d.velop

d.ecs content crawler: Administrator

Table of Contents

1. d.ecs content crawler

1.1. Imprint/Legal Notices

Contact d.velop AG Schildarpstraße 6-8 48712 Gescher, Germany

Phone +49 2542 9307-0d-velop.de or info@d-velop.de

Represented by: Sebastian Evers (Co-CEO), Rainer Hehmann (Co-CEO), Dr. Stephan Held (CFO), Christoph Pliete (CAO) Chairman of the Supervisory Board: Dr. Helmut Bäumer Commercial register: Coesfeld District Court, no. HRB 4903 Sales tax identification number: DE 813062165

If you have any questions about this documentation or the software, please contact us. Tel: +49 2542 9307-6000

support@d-velop.de

This document was last revised on 12/01/2022 and relates to d.ecs content crawler version 1.13.5.

Document name: decscontentcrawler_admin.pdf (build number: 20221201).

1.2. Basic information on the application and the manual

This documentation describes how to install, configure and update d.ecs content crawler and is aimed at administrators.

To fully comprehend the information in this document, it is helpful to have knowledge of Microsoft Windows and Microsoft Outlook and/or HCL Notes. You can find more information about operating d.3one integrations in the quick guide for d.3one e-mail integration.

1.2.1. About d.ecs content crawler

With the help of d.ecs content crawler, you can store e-mails centrally in your d.3ecm system environment in a rule-based, legally secure and audit-proof manner and make them available to your users.

You can use the journaling function in Microsoft Exchange and HCL Domino to save the e-mails from your journal in a legally secure and audit-proof manner in your d.3 repository.

In addition, you can map the e-mails to files and processes or simply save e-mails in a legally compliant manner in the d.3 repository.

d.ecs content crawler is a primary component of the following solution packages:

- dbs | journal archiver for Microsoft Exchange
- dbs | journal archiver for IBM Domino
- dbs | mailbox archiver for Microsoft Exchange
- dbs | mailbox archiver for IBM Domino

If your users have not purchased d.3one in Microsoft Outlook or d.3one in IBM Notes, they can use an add-in or widget to restore e-mails and save items locally if necessary. Further information on this topic can be found in the section on the license-dependent scope of functions of the d.3one integrations.

1.2.2. Architecture of a d.3ecm system environment

We in d.velop AG focus on a modern software architecture based on microservices among other things.

For example, d.3one is a collection of single microservices that interact and provide the user with DMS functionality in the user interface. Each microservice is a standalone application.

In the d.3ecm architecture, a microservice is referred to as an app.

Each d.velop product consists of its own apps which are specific for the product and which are installed using a product-specific setup. If, for example, an app was installed several times as separate app instances (e.g. for cluster operations or scaling purposes), all apps must have the same version.

Based on this architecture, you can decide freely according to the requirements of your server environment, which app should be install on which host how many times in the d.3ecm environment. This architecture design offers you maximum freedom to cover your specific requirements for the IT environment.

Besides the product-specific apps, there are the core apps that you need to consider separately.

Core apps in the d.3ecm architecture

There are a number of apps that are of crucial importance for many d.velop AG products in the d.3ecm system landscape. All the apps below are installed as **infrastructure** products using d.velop software manager and are not part of other d.velop products:

d.ecs http gateway

The d.ecs http gateway app is the core HTTP interface to all app in a d.3ecm environment. Any HTTP communication is done using this app. From a technical point of view, this is a reverse proxy. Each app is registered in the d.ecs http gateway app. The newly registered app can then be accessed by all the other apps under https://<BaseUri>/<AppName>. If you have to run several d.ecs http gateway apps in a d.3ecm environment, all d.ecs http gateway apps must be accessed under the identical base address. For each d.3ecm environment, there must be only a single base address.

d.ecs jstore

The d.ecs jstore app is a NoSQL database that caches frequently requested data from the d.3 server in the memory of the application server; such data includes, for instance, property values for frequently used documents. Thus the requested database accesses on the d.3 database are reduced and therefore the performance of the whole system is increased.

In addition, d.ecs jstore is used by the different d.velop components (e.g. d.3one, d.ecs monitor) to store data permanently.

d.ecs jstore is based on Redis (Remote Dictionary Server) and replaces Couchbase as cache storage, which was used until d.3ecm Version 8.0. Among other things, the app is easier to configure and, thus provides considerable advantages compared to the latest solution.

The d.ecs jstore app is installed on each Windows host on which a d.velop app is run.

In a d.3ecm environment, each single d.ecs jstore instance on a Windows host must be clustered in order to allow data communication.

d.ecs identity provider

The d.ecs identity provider app authenticates the users on behalf of each app. You can use systems like the Windows Active Directory service for authentication. The authorization of a user is done by each app.

d.ecs shell

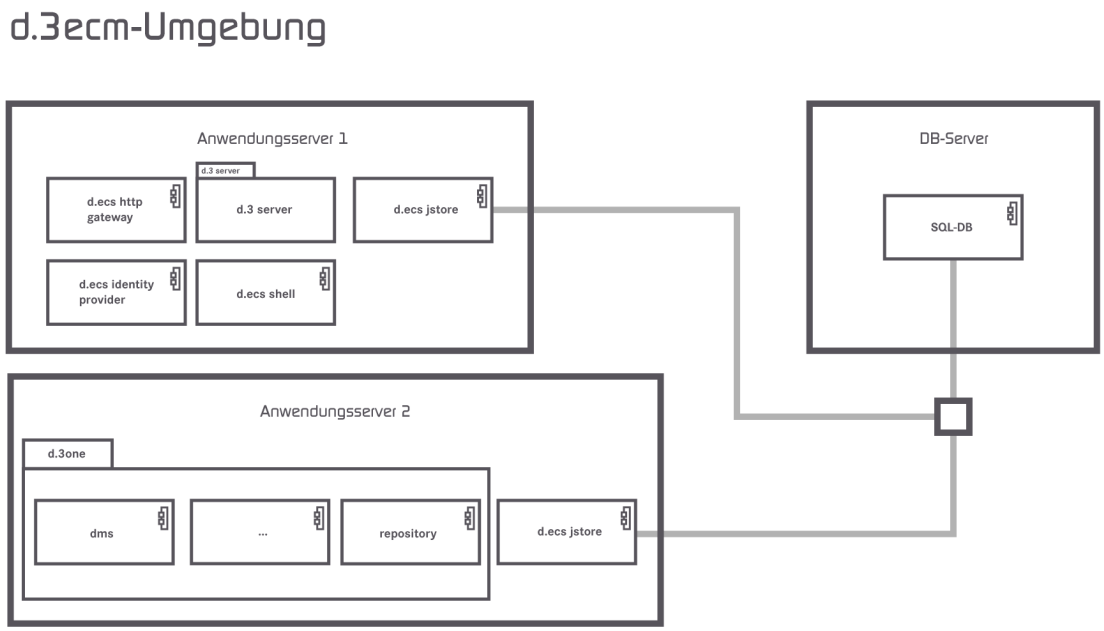
The d.ecs shell app provides the common frame for the HTML interface of each app and implements a uniform look & feel user experience so that the interface of the apps is consistent and appears to be made in one piece. The app also provides access to the native functions of the host. In this context a host may be, for example, an e-mail application, an ERP application or even a browser.

Potential scenarios for a d.3ecm environment with d.3one

You can design your d.3ecm environment especially according to the requirements of your enterprise or organization. You can either use one single core application server at minimum or distribute the apps on different application servers. You can choose how to organize your d.3ecm environment based on your needs and requirements for your IT environment.

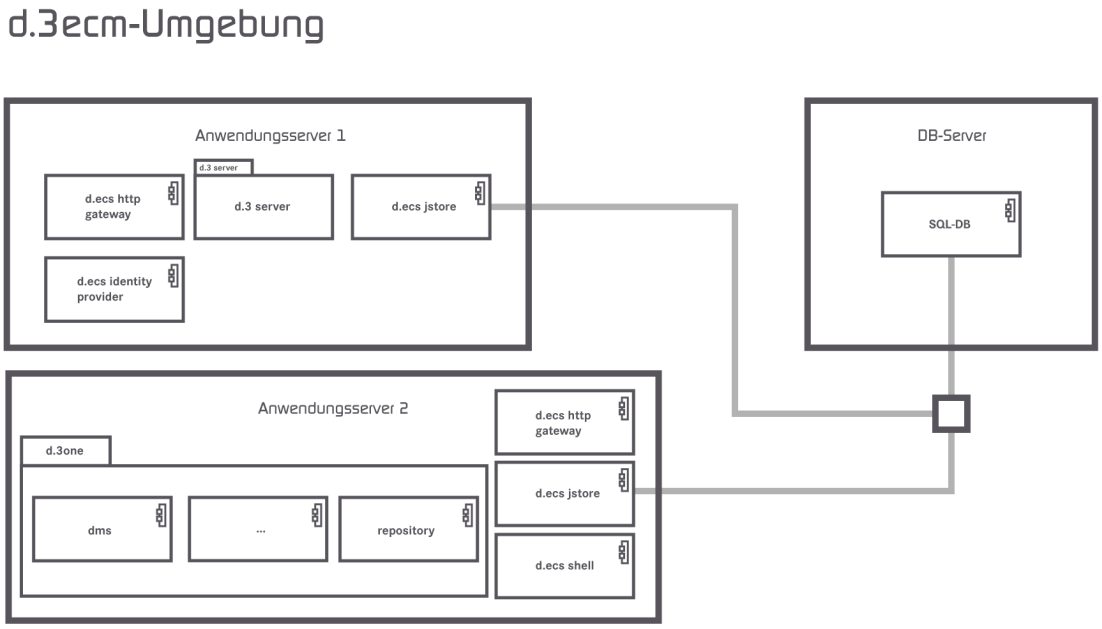
Example 1

The core apps were installed on a single application server, while the product-specific apps are installed on a different application server.



Example 2

The core apps are distributed on two application servers and the d.ecs http gateway app exists two times in the d.3ecm environment.



If there are questions regarding the cluster operation or scaling, contact your d.velop representative.

1.2.3. Useful things to know about d.3one licenses

With d.3one as their integrating application, users can easily use d.3 functions in other applications, such as:

- Browsers
- Microsoft Outlook
- Microsoft Office
- HCL Notes
- SAP ERP
- Customer-specific integrations

Each integration must be licensed for each user. The number of users of individual products can vary within a d.3one installation; for instance, 200 users can use d.3one in the browser, but only 50 users can use d.3one in Microsoft Outlook. In contrast to a d.3ecm system environment, d.3one is a separate integration application.

When a user uses d.3one in the browser or as an integration, license information is retrieved from the d.3 repository. With each access, each d.3one user is allocated a user license in the d.3ecm system environment. Make sure that enough basic licenses are available for all users that use the d.3ecm system environment directly or indirectly. We recommend using named user licenses as standard.

> **Note**
> Before you install d.3one or the integrations, make sure that enough d.3 client access licenses (d.3 CALs) are available. We recommend using a consistent named user license model in which sufficient d.3 client access licenses are available for every d.3one user.

The functions available to you for the e-mail integrations vary based on the product purchased.

If you have any additional questions about d.3one licensing, contact your d.velop contact person.

See also: Detailed information about named-user licenses

1.2.4. Useful information about the license-dependent scope of functions of the d.3one integrations

The d.3one integrations for Microsoft Outlook and HCL Notes are included in the delivery with d.ecs content crawler. You can distribute the add-in or widget to your users as needed. Further information can be found in the administration manuals for d.3one in Microsoft Outlook and d.3one in IBM Notes.

The scope of functions of the integrations are based on the licenses purchased. You can use the list below to track which functions are available to you with the various licenses.

No license

- Restoring an item from a d.3 repository
- Offline Store

Basic license

- Restoring an item from a d.3 repository
- Offline Store
- Storing e-mails and attachments using the context menu
- Searching in the d.3 repository

Full license

- Restoring an item from a d.3 repository
- Offline Store
- Storing e-mails and attachments using the context menu
- Searching in the d.3 repository
- Storing items in dossiers using drag & drop
- Sending and simultaneously storing items in a d.3 repository with the **Send and store** function
- Opening e-mail content in different applications using the **Go to** function
- Tasks and messages
- Context-sensitive search using the **Search for** function
- Using the d.3one functions
- Opening d3l reference files
- Sending an item by e-mail as an original file or PDF file
- Creating a new version of a document with alteration text
- Updating document properties
- Displaying documents during editing
- Displaying the properties of an archived e-mail
- Exporting the properties of multiple items
- Exporting documents as PDF files

1.2.5. Useful things to know about the system architecture and operating principles of d.ecs content crawler

This section contains information on the structure and operation of d.ecs content crawler so that you can better understand the functions of d.ecs content crawler and adapt your system environment.

The following diagram shows how profiles or configurations for journal archiving are processed by d.ecs content crawler:

d.ecs content crawler processes profiles that can be configured according to your needs. With the help of the profiles, you can determine which mail databases, mailboxes or journal mailboxes are processed by d.ecs content crawler. In addition, you can individually define the maximum number of profiles or documents that can be processed, for example.

In d.ecs content crawler, a profile controller processes a configuration document and determines the required number of mail databases. A profile worker instance is created for each mail database or mailbox. If there are more mailboxes to be processed than there are processing instances, the mailboxes are evenly distributed among the instances. The journal configuration also counts as a profile.

The profile worker instance identifies the documents to be archived based on the rules defined in the profile. The number of documents is determined for each cycle.

Each profile worker instance generates the necessary number of document workers. The determined number of documents to be archived per database is distributed evenly to the existing document workers.

Based on a previously created mapping, the document workers save the documents using the groupware app and the DMS app in the d.3 repository with the corresponding e-mail properties and d.3 properties.

See also: Example of a d.ecs content crawler configuration

1.3. Installation and uninstallation

This section provides information on installing, updating, and uninstalling d.ecs content crawler and the necessary components.

1.3.1. System requirements

Please refer to the central system requirements for d.velop products (on-premises). You can find deviating or more extensive system requirements in the documentation.

If you are using Microsoft Exchange Online, archived e-mails in the mailboxes (stubs) are not subject to full-text indexing. The stubs are not found during a full-text search by Microsoft Outlook. The stubs are displayed as usual in the folders. Full-text indexing occurs if the Microsoft Outlook category is specified instead of the archive message class.

You have the following options for ensuring that your users can search for archived content in a Microsoft Outlook application installed on-premises:

- Enable cache mode in Microsoft Outlook.
- Use the advanced search in Microsoft Outlook (**Home > Filter Email > More Filters > Search Tools > Advanced Find**).
- Provide your users with a start page folder that can be used to search for archived e-mails in the d.3 repository (direct link to the result list).

1.3.2. Preparing to install d.ecs content crawler

Before installing d.ecs content crawler, you need to carry out some preparatory steps. You must complete the following tasks before installing d.ecs content crawler:

- Install and configure the d.3one application server with the appropriate groupware app components.
- Install the d.velop infrastructure components. Information on installing the central infrastructure apps can be found in the configuration guide for d.velop infrastructure components. If you want to use Kerberos, you must install and configure the d.ecs identity provider before installing Kerberos.
- Make sure that the rights for **Status transfer processing** and **Status transfer release** are granted in the d.3 administration.
- Create a test environment for e-mail archiving projects. Configure the test environment so that you can simulate errors in the production system. A test environment can help you to test new functions before installing a new version for the production system.

Useful things to know about using d.ecs content crawler with HCL Domino

If you are using d.ecs content crawler with HCL Domino, we recommend that you do not install the d.ecs domino service on the productive mail server or on a highly frequented HCL Domino server. Create a separate server or use an underutilized server to ensure productive operation.

> **Warning**
> Using the d.ecs domino service can have a negative impact on the functionality of the HCL Domino Server. We therefore strongly advise against using the d.ecs domino service for a company-critical HCL Domino system. Deploy the HCL Domino server as a stand-alone server to process e-mails with the d.ecs domino service. You can also use the d.ecs domino service with the d.3one application server, for example.

Granting permissions for Microsoft Exchange Server

To ensure the connectivity of Microsoft Exchange Server, you must specify a user account that has access permission for all Microsoft Exchange Server mailboxes in your organization. Ensure that the certificate for the URL is valid.

The user account for the EWS (Exchange Web Services) connector should be the same user account that you used to install d.3one.

You must ensure that the user account has the necessary permissions for Microsoft Exchange Server, particularly the right **Exchange Impersonation** (role **Exchange Impersonation**). This right can be used to perform actions on all the mailboxes on behalf of the relevant owner.

You only require a Microsoft Exchange mailbox for the user account for the impersonation if you are using d.ecs content crawler. For d.3one in Microsoft Outlook, a Microsoft Exchange mailbox for the impersonation is not required.

You can change the permissions with the following PowerShell command:

```
New-ManagementRoleAssignment –Name:impersonationAssignmentName –
Role:ApplicationImpersonation
```

If you only want to grant rights for specific mailboxes to the user account, you can restrict the permissions using a filter for a regular, filtered recipient scope (**RecipientRestrictionFilter**).

For example, you can enter a PowerShell command to grant an Exchange impersonation for the service account to mailboxes 1 and 2.

Example

```
New-ManagementScope -Name d3oneImpersonationScope
-RecipientRestrictionFilter { (Name -eq "Mailbox1") -or (Name -eq
"Mailbox2") }
New-ManagementRoleAssignment -Name d3oneImpersonation -Role
ApplicationImpersonation -User "serviceAccount" -CustomRecipientWriteScope
d3oneImpersonationScope
```

Alternatively, you can configure the Exchange impersonation in Office 365 or Microsoft Exchange Online under **Exchange Admin Center > Permissions**.

You can find more information about filtering under “Understanding management role scope filters” in the Exchange Server 2013 documentation on the Microsoft Docs website.

Assigning throttling policies for the service user in Microsoft Exchange Server

To ensure that d.3one in Microsoft Outlook works in combination with Microsoft Exchange Server, you must create and assign a special throttling policy for the service user with the role **ApplicationImpersonation** on the server with Microsoft Exchange Server.

For Microsoft Exchange version 2010

Create the following policy in the Microsoft Exchange management console.

```
New-ThrottlingPolicy d3onepolicy
Set-ThrottlingPolicy d3onepolicy -RCAMaxConcurrency $null
-RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null
-RCAPercentTimeInMailboxRPC $null -EWSMaxConcurrency $null
-EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null
-EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null
-EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null
-CPAMaxConcurrency $null -CPAPercentTimeInCAS $null
-CPAPercentTimeInMailboxRPC $null -CPUStartPercent $null
```

Assign the policy to the service user.

```
Set-Mailbox "user name" -ThrottlingPolicy d3onepolicy"
```

Microsoft Exchange Version 2013 or higher

Create the following policy in the Microsoft Exchange management console.

```
New-ThrottlingPolicy -Name d3onepolicy -ThrottlingPolicyScope Regular
-IsServiceAccount -MessageRateLimit unlimited -RcaCutoffBalance Unlimited
-RcaMaxBurst unlimited -RcaRechargeRate unlimited -RcaMaxConcurrency
unlimited -RecipientRateLimit unlimited -EwsMaxConcurrency
unlimited -CpaMaxConcurrency unlimited -EwsCutoffBalance unlimited
-EwsMaxSubscriptions unlimited
```

Assign the policy to the service user.

```
Set-ThrottlingPolicyAssociation -Identity "user name" -ThrottlingPolicy
d3onepolicy
```

1.3.3. Installing d.ecs content crawler

You install the software exclusively with d.velop software manager. If an application is required for different products, the corresponding software packages are also installed automatically.

For further information on installing the software, see the d.velop software manager manual.

Install the d.ecs content crawler app on the d.3one application server. With a basic installation (maximum of ten mailboxes) or a test environment, you can also install the Windows service from d.ecs content crawler on the d.3one application server. For larger systems with increased workload, we recommend installing d.ecs content crawler on dedicated servers.

Install the following components for the setup of d.ecs content crawler:

- d.ecs groupware
- d.ecs mail converter
- d.ecs content crawler app
- d.ecs domino service setup
- DGI2HTML
- DGI2EML

In addition to d.ecs content crawler, the integrations for Microsoft Outlook and HCL Notes are included in the delivery. The functionality of the integrations depends on the licenses purchased. If necessary, you can distribute the integrations to your users. Further information on distributing the integrations can be found in the administration manuals for d.3one in Microsoft Outlook and d.3one in IBM Notes.

In the case of a new installation, data from a previous installation may still be entered. This data was not deleted during the previous uninstallation. If necessary, amend the data accordingly.

1.3.4. Uninstalling d.ecs content crawler

The software you installed using d.velop software manager can only be uninstalled with d.velop software manager. If the software to be uninstalled has dependencies with other software packages, you must resolve these conflicts accordingly.

For further information on uninstallation, see the d.velop software manager manual.

1.3.5. Rolling back an installation of d.ecs content crawler

You can restore an earlier version of the software that you installed with d.velop software manager. During this process, the software is only reset to a previous version.

For further information on rolling back to an earlier version, see the d.velop software manager manual.

1.3.6. Enabling the default port for d.ecs content crawler

- The port for d.ecs content crawler is determined dynamically by default. However, you can also define a port.

1.3.7. Installing updates for d.ecs content crawler

The default method for installing updates for d.ecs content crawler is with the d.velop software manager.

If an earlier version other than the immediately previous version is installed in your system environment, contact your d.velop contact person.

1.4. Configuring d.ecs content crawler

This section provides information on configuring d.ecs content crawler and the necessary components.

1.4.1. Preparing for the authentication of the Groupware app with OAuth 2.0 in Azure Active Directory

If you want to use Microsoft Office 365 in combination with the Groupware app, you should specify that the Groupware app be authenticated with OAuth 2.0. This method of authentication is recommended by Microsoft.

To use authentication with OAuth 2.0, you must first adjust the configuration in Azure Active Directory. Then, adjust the settings in the Groupware app as required.

You must perform the following preparatory tasks for authentication with OAuth 2.0 in Azure Active Directory:

- **Registering the Groupware app in Azure Active Directory**: Create a new app registration for the Groupware app. Select **Accounts in this organizational directory only** as the supported account types. Enter the base address of the d.3one system environment as a redirect URI.
- **Configuring the API permissions**: Add the following permission for the API permissions: **Use Exchange Web Services with full access to all mailboxes (full_access_as_app)**
- **Creating a client secret**: Create a new client secret. Copy the secret directly to the clipboard to paste the secret in the Groupware app afterward.
- **Determining the application ID and the directory ID**: Copy the IDs from the app registration overview of the Groupware app to the clipboard to paste them to the Groupware app later.

Additionally, create an access policy for the Groupware app in Microsoft 365. For more information, see the following article in our knowledge base: https://kb.d-velop.de/s/article/000001683

You then need to adjust the corresponding settings in the Groupware app for authentication with OAuth 2.0.

1.4.2. Preparing for the authentication of the Groupware app with OAuth 2.0 and Microsoft Graph in Azure Active Directory

If you are using Microsoft Office 365 in combination with the Groupware app and Microsoft Graph, ensure that the Groupware app is authenticated with OAuth 2.0.

> **Note**
>
> The Microsoft Graph interface does not support the following functions:
>
> - Access to public folders
> - Access to the online archive
> - Importing and exporting the complete data of the message classes **Tasks** (**IPM.Task**) and **Distribution list** (**IPM.DistList**)
> - Specifying colors for a category (each user sets the color individually)
>
> If you are using d.ecs content crawler, the following additional restrictions apply:
>
> - Journal archiving is not supported.
> - Only e-mail items can be restored from the d.3one results list.

To use authentication with OAuth 2.0, you must first adjust the configuration in Azure Active Directory. Then, adjust the settings in the Groupware app as required.

You must perform the following preparatory tasks for authentication with OAuth 2.0 in Azure Active Directory:

- **Registering the Groupware app in Azure Active Directory**: Create a new app registration for the Groupware app. Specify which accounts can access the API. Enter the base address of the d.3one system environment as a redirect URI.

- **Configuring the API permissions**: Add the following API permissions from the area **Microsoft Graph > Application permissions**:
  - **Group.Read.All**
  - **GroupMember.Read.All**
  - **Mail.ReadWrite**
  - **MailboxSettings.Read**
  - **Member.Read.Hidden**
  - **User.Read.All**
- **Creating a client secret**: Create a new client secret. Copy the secret directly to the clipboard to paste the secret in the Groupware app afterward.
- **Determining the application ID and the directory ID**: Copy the IDs from the app registration overview of the Groupware app to the clipboard to paste them to the Groupware app later.

Additionally, create an access policy for the Groupware app in Microsoft 365. For more information, see the following article in our knowledge base: https://kb.d-velop.de/s/article/000001683

You then need to adjust the corresponding settings in the Groupware app for authentication with OAuth 2.0.

1.4.3. Specifying the registry information from Azure Active Directory for authentication with OAuth 2.0

Once you have registered the Groupware app in Azure Active Directory and copied the necessary IDs and client secret, you must make the appropriate adjustments to the settings in the Groupware app.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Microsoft Exchange** under **E-mail management**.
3. Select **OAuth 2.0 (Microsoft Office 365)** under **Exchange Web Services authentication method** in the **Connection settings** perspective.
4. Enter the directory ID that you previously copied to the clipboard in Azure Active Directory under **Office 365 Directory ID**.
5. Enter the application ID that you previously copied to the clipboard in Azure Active Directory under **Office 365 Application ID for d.ecs groupware**.
6. Enter the client secret that you previously copied to the clipboard in Azure Active Directory under **Office 365 API Access Key for Exchange Web Services**.
7. Add the impersonation user in Exchange Web Services.
8. Save your entries and restart the Groupware app.

1.4.4. Setting up multiple connections to the Microsoft Exchange server with Microsoft Exchange (on-premises)

You can define the connection to the Microsoft Exchange server and connect multiple different Exchange servers to the Groupware app.

To connect a Microsoft Exchange server, make sure that the SSL certificate is qualified and valid.

The following conditions apply for the impersonation user:

- For Exchange Online in Microsoft 365: the user needs a mailbox (EWS and OAuth 2.0).
- Microsoft Exchange server (on-premises): the user needs a mailbox (EWS and Basic) if they are to access public folders.
- Enter the SMTP address as the user name to allow access to public folders.

For an additional Microsoft Exchange connection, you can select between Microsoft Exchange (on-premises) and Exchange Online. For Microsoft Exchange (on-premises), only Microsoft EWS is permitted. Exchange Online can use Microsoft EWS or Microsoft Graph.

If you want to delete a Microsoft Exchange configuration, make sure that the configuration is no longer used.

Let's assume you want to configure the connection settings for the Microsoft Exchange server and add Microsoft Exchange (on-premises) as an additional connection.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Microsoft Exchange** under **E-mail management**.
3. Go to the **Connection settings** perspective.
4. Select **Enable Microsoft Exchange services**.
5. Enter all necessary parameters for the first connection.
6. Click the plus sign to add the parameters as an additional connection.
7. Enter the accepted domains for the Microsoft Exchange server. Separate the domains with a comma.
8. Under **Exchange API**, select **Microsoft EWS** as the interface.
9. Under **Exchange Web Services server**, enter the fully qualified name of your Exchange server (on-premises) in the format <name of server>.<name of domain>.
10. Select your port under **Exchange Web Services port**. The default value is **443**.
11. Set the appropriate version under **Exchange Web Services version**. The default value is **Autodetect**.
12. Set the authentication method for Exchange Web Services. For Microsoft Exchange (on-premises), only **Basic** is permitted.
13. Enter the impersonation user and the password.
14. If necessary, select the option **Open mailboxes via AutoDiscovery (hybrid environments)**.

See also:

- Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft EWS
- Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft Graph

1.4.5. Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft EWS

You can define the connection to the Microsoft Exchange server and connect multiple different Exchange servers to the Groupware app.

To connect a Microsoft Exchange server, make sure that the SSL certificate is qualified and valid.

The following conditions apply for the impersonation user:

- For Exchange Online in Microsoft 365: the user needs a mailbox (EWS and OAuth 2.0).
- Microsoft Exchange server (on-premises): the user needs a mailbox (EWS and Basic) if they are to access public folders.
- Enter the SMTP address as the user name to allow access to public folders.

For an additional Microsoft Exchange connection, you can select between Microsoft Exchange (on-premises) and Exchange Online. For Microsoft Exchange (on-premises), only Microsoft EWS is permitted. Exchange Online can use Microsoft EWS or Microsoft Graph.

If you want to delete a Microsoft Exchange configuration, make sure that the configuration is no longer used.

Let's assume you want to configure the connection settings for Exchange Online and use Microsoft EWS as an additional connection.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Microsoft Exchange** under **E-mail management**.
3. Go to the **Connection settings** perspective.
4. Select **Enable Microsoft Exchange services**.
5. Enter all necessary parameters for the first connection.
6. Click the plus sign to add the parameters as an additional connection.
7. Enter the accepted domains for the Microsoft Exchange server. Separate the domains with a comma.
8. Under **Exchange API**, select **Microsoft EWS** as the interface.
9. Click **Microsoft 365** under **Exchange Web Services server**, which causes the system to enter outlook.office365.com.
10. Enter the Exchange Web Services port and the appropriate version under **Exchange Web Services version**. The default value is **Autodetect**.
11. Set the authentication method for Exchange Web Services. For **OAuth 2.0 (Microsoft 365)**, enter the Microsoft 365 directory ID, the Microsoft 365 application ID for d.ecs groupware, the Microsoft 365 API access key for Exchange Web Services, and the impersonation user for Exchange Web Services from Azure Active Directory. For **Basic**, enter the impersonation user and the password.

See also:

- Setting up multiple connections to the Microsoft Exchange server with Microsoft Exchange (on-premises)
- Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft Graph

1.4.6. Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft Graph

You can define the connection to the Microsoft Exchange server and connect multiple different Exchange servers to the Groupware app.

To connect a Microsoft Exchange server, make sure that the SSL certificate is qualified and valid.

The following conditions apply for the impersonation user:

- For Exchange Online in Microsoft 365: the user needs a mailbox (EWS and OAuth 2.0).
- Microsoft Exchange server (on-premises): the user needs a mailbox (EWS and Basic) if they are to access public folders.
- Enter the SMTP address as the user name to allow access to public folders.

For an additional Microsoft Exchange connection, you can select between Microsoft Exchange (on-premises) and Exchange Online. For Microsoft Exchange (on-premises), only Microsoft EWS is permitted. Exchange Online can use Microsoft EWS or Microsoft Graph.

If you want to delete a Microsoft Exchange configuration, make sure that the configuration is no longer used.

Let's assume you want to configure the connection settings for Exchange Online and use Microsoft Graph as an additional connection.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Microsoft Exchange** under **E-mail management**.
3. Go to the **Connection settings** perspective.
4. Select **Enable Microsoft Exchange services**.
5. Enter all necessary parameters for the first connection.
6. Click the plus sign to add the parameters as an additional connection.
7. Enter the accepted domains for the Microsoft Exchange server. Separate the domains with a comma.
8. Under **Exchange API**, select **Microsoft Graph** as the interface.
9. Enter the Microsoft 365 directory ID, the Microsoft 365 application ID for d.ecs groupware, and the Microsoft 365 API access key from Azure Active Directory. The Exchange connection is entered under outlook.office365.com (accepted domains).

See also:

- Setting up multiple connections to the Microsoft Exchange server with Microsoft Exchange (on-premises)
- Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft EWS

1.4.7. Establishing a connection between the d.3one application server and d.ecs domino

For d.3one in IBM Notes to function properly, you need to ensure communication between the HCL Domino server, the client PCs running HCL Notes and the d.3one application server. You can configure the connection data on the HCL Domino server where d.ecs domino is installed. You must be logged in with a Windows administrator account to configure the connection data.

Let's assume you want to configure the connection data on the HCL Domino server for communication between the servers.

This is how it works

1. In the data directory, open the **d3onecfg.nsf** database using HCL Notes or a browser and navigate to **Settings**. Make sure that the **d3onecfg.nsf** file is stored in the root directory of the databases. The file must not be stored in a subdirectory.
2. On the **d.3one server** tab, enter the host name of the server where d.3one is installed (base address). You have to enter the fully qualified domain name (FQDN) of the d.3one application server in order for Kerberos authentication to work properly in the Windows domain, e.g. **d.3one.contoso.com**.
3. Enter the port for the d.3one application server.
4. Go to the **d.ecs domino** tab and select the log level for d.ecs domino under **Log level**.
5. Enter the path to the log file under **Log path**.
6. Enter the name of the log file under **Log file**.
7. Under **Work path**, enter the file path where the temporary files for d.ecs domino are stored (e.g. for converting e-mails). If you do not enter a path, the **Temp** system folder will be used.
8. Under **SSL port**, enter the port for the encrypted connection for d.ecs domino. The default port is **8182**.
9. Go to the **Certificate** tab and enter the file path of the Java Keystore under **Keystore file path**. The Java Keystore stores the key to be used for the secure connection.
10. Enter the password for the Java Keystore under **Keystore password**.
11. If necessary, enter the password for the key stored in the Java Keystore under **Key password**.

If your users retrieve their mail databases from different servers, you may need to replicate the database on the mail servers so that your settings for d.3one on the server can also be used for the client PCs running HCL Notes.

After you have set the connection data, you have to set the connection data in d.3one as well.

1.4.8. Setting the d.ecs domino connection data in d.3one

If you have set the connection data for d.ecs domino on the HCL Domino server, you also have to set the connection data in d.3one for the connection between the d.3one application server and d.ecs domino.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **IBM Domino** under **E-mail management**.
3. Select **Enable IBM Domino services**.
4. Under **d.ecs domino service server**, enter the host name of the client PC where d.ecs domino is installed.
5. Under **d.ecs domino service port**, enter the port for d.ecs domino. The default port is **8182**.
6. Save your entries and restart the Groupware app.

1.4.9. Specifying the common settings of d.ecs content crawler

After you have installed d.ecs content crawler, you need to configure d.ecs content crawler. You can configure d.ecs content crawler for rule-based processing of e-mails or journal archiving. You can also adjust the processing speed.

> **Warning**
> We do not advise using d.link for lotus notes in parallel with d.ecs content crawler as this may cause problems in the mailbox.

You can find the common settings for d.ecs content crawler in the **Configuration** feature on the start page in the **Document management** category under **E-mails** by selecting the **Archiving options** entry under **E-mail archiving**. Alternatively, you can use the **d.ecs content crawler** feature.

For example, in the common settings you can define the maximum number of profiles to be processed simultaneously. Values are already specified by default. If necessary, you can individually adjust the values.

> **Note**
> If you are using the Microsoft Graph interface, halve the maximum number of profiles to be processed simultaneously as well as the instances per profile. Microsoft has defined a strict throttling policy for the Microsoft Graph interface that cannot be changed.

When you have finished configuring the common settings for d.ecs content crawler, restart d.ecs content crawler in d.3 process manager.

If Microsoft Exchange Server or HCL Domino Server are not available for a certain period of time, e.g. because of a maintenance window for updates or for data backup, restart d.ecs content crawler in d.3 process manager as soon as the mail server is available again.

1.4.10. Configuring the database server

d.ecs content crawler creates a job for every e-mail to be processed, which contains all the necessary information. You need to define a database to manage the jobs.

The database tables are created with the prefix **GWCR_**. You can use the database of a d.3 repository for d.ecs content crawler.

> **Note**
> If you want to use an internal database, you can no longer install d.ecs content crawler in a distributed manner. Only one instance may be registered and executed with d.ecs http gateway.

For example, suppose you want to configure a database server to manage jobs.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Archiving options** under **E-mail archiving**.
3. Switch to the **Database** perspective.
4. Select the appropriate type of database.
5. Under **Server**, enter the appropriate host name or the IP address of the database server.
6. Enter the name of the database you want to use.
7. Enter the name of the database user.
8. Enter the user's password and save your details.

1.4.11. Configuring journal archiving

With d.ecs content crawler, you have the option of journal archiving for certain items with Microsoft Exchange and HCL Domino. For example, you can save journal e-mails or meeting requests with journal archiving. This does not apply to appointments, for example, if you enabled the **Storing format: EML instead of DGIX** option in the Groupware app. You will find the option in the **Configuration** feature in the **Document management** category under **E-mails** if you select the **Microsoft Exchange** entry under **E-mail management** and navigate to the **Process settings** perspective.

In addition, you can use compliance archiving without journaling enabled for Microsoft Exchange 2016 and Microsoft Exchange Online.

To store e-mails from the journal of your e-mail system in a legally secure and audit-proof manner, you can use dbs | journal archiver instead of purchasing a full license for d.ecs content crawler. To be able to use and configure journal archiving, you must have dbs | journal archiver or dbs | mailbox archiver licensed for your e-mail system.

Specifying the common settings for journal archiving

With d.ecs content crawler, you can enable journaling for Microsoft Exchange or HCL Domino.

Suppose you want to use journal archiving for Microsoft Exchange.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Archiving options** under **E-mail archiving**.
3. Go to the **Processing settings** perspective.
4. Enable journaling for Microsoft Exchange.
5. Select the repository in which to save the journal e-mails.
6. Under **Journal mailbox**, enter the SMTP address of the mailbox in which the journal e-mails are stored, e.g. **journal@<domainname>.com**. If you want to specify multiple mailboxes, separate the entries with a comma.
7. Select the days and the durations for the time control.
8. Save your entries.

If you change the configuration for journal archiving, you then need to restart the d.ecs content crawler service.

Configuring compliance archiving without journaling enabled for Microsoft Exchange 2016 and Microsoft Exchange Online

Compliance archiving is only supported in combination with Microsoft Exchange 2016 and Microsoft Exchange Online. If you are using an earlier version of Microsoft Exchange Server, your configurations will be ignored.

If you want to use compliance archiving without journaling enabled, you must note the following:

- You must enable litigation hold on Microsoft Exchange Server. If you enable litigation hold, a copy is made in the **Versions** folder every time an item is changed. Make sure that the folder is not unnecessarily filled with copies.

  > **Warning**
  > d.ecs content crawler does not check whether litigation hold is enabled in Microsoft Exchange. If litigation hold is disabled, Microsoft Exchange Server automatically deletes the items after a specified period of time, or the user of that item is permanently deleted.
  >
  > For more information, see “Recoverable items folder in Exchange Server” in the Exchange Server 2019 documentation on the Microsoft Docs website.

- You have to adjust the settings for a profile in d.ecs content crawler. Enter**Microsoft Exchange** as the source system and select the **Enable archiving of deleted elements** option. In this case, e-mails that are saved under **Recoverable items** in the **Deletions** or **Purges** folders are also taken into account. The items from the corresponding folders are processed based on your configurations for the profile.
- The items are not automatically deleted by d.ecs content crawler. If necessary, you must specify automatic deletion in the profile.

If you change the configuration for journal archiving, you then need to restart the d.ecs content crawler service.

Configuring journal archiving for HCL Domino

When performing journal archiving for HCL Domino, note the following:

- The archiving service can process a maximum of one journal database. If you want to process more than one journal database, you have to install several d.ecs content crawler apps or several groupware apps (d.3one application server).
- Make sure that one of the following categories (document types) is specified in the HCL Domino Server administration in the **Form** field: **Message**, **Memo**, **Reply**, **Notice**, **Appointment**, **Report**, **Non-Delivery Report**, **Recall Response**, **Recall Request**, **Return Receipt** or **Personal Stationery**. Only these categories may be transferred to the journal database.
- To be able to assign the properties of e-mails to d.3 properties, you must create a mapping. We recommend using a separate category for journal e-mails, otherwise the mapping for saving e-mails in HCL Notes is also used in d.3one.

Configuring journal archiving for Microsoft Exchange

When performing journal archiving for Microsoft Exchange, note the following:

- Journal archiving can also archive documents which have been delivered directly and have no envelope. We recommend that you configure journaling for Microsoft Exchange in such a way that only e-mails from Microsoft Exchange are accepted (Microsoft Exchange PowerShell Commandlet **Set-Mailbox** in conjunction with **AcceptMessagesOnlyFromSendersOrMembers**).
- Within the journal, only e-mails with the message classes **IPM.Note***, **IPM.Schedule.Meeting***, **IPM.Report.Recall***, **IPM.Outlook.Recall*** and **REPORT.IPM*** are processed. E-mails that deviate from these specifications are moved to the **d.3ecm unprocessable** folder in the journal mailbox.

- To be able to assign the properties of e-mails to d.3 properties, you must create a mapping. When mapping, the values are not determined from the envelope e-mail, but from the document to be saved. We recommend using a separate category (document type) for journal e-mails, otherwise the mapping for saving e-mails in Microsoft Outlook is also used in d.3one.

Microsoft Office 365 (Microsoft Exchange Online) currently only supports external mailboxes as journal mailboxes. External mailboxes are mailboxes that are not Microsoft Office 365 mailboxes. For journal archiving with d.ecs content crawler, the external mailbox must be accessible using the Exchange Web Services (EWS). It doesn't matter whether it is a cloud mailbox or an on-premises mailbox.

Saving meeting requests

You can save other items from journaling in addition to e-mails. You can select the source **Calendar entry/meeting** when mapping these items.

You can save the following items in addition to e-mails:

- Meeting requests
- Responses to meeting requests (**Acceptance**, **Rejection**, **Tentative acceptance**)
- Rejection of meetings

You can additionally adopt the following values:

- All SMTP addresses (participant, organizer) or all participant names
- Start time and end time
- Meeting organizer's name
- Names of the required participants, optional participants, rooms, or resources
- Location
- Meeting organizer's SMTP address
- SMTP addresses of the required or optional participants, rooms or resources
- SMTP addresses of all participants

1.4.12. Configuring rule-based archiving

With d.ecs content crawler, you can archive e-mails based on rules by creating profiles. In these profiles, you specify sources, rules and process steps to determine how the items are to be processed.

You can also configure sources, rules and process steps when creating the profile using the appropriate context actions without having to exit the profile configuration.

If you want to create a profile for rule-based archiving, you must create a category and specify the mapping for this category. You can create the category and the mapping in the groupware app configuration and the **Mapping** feature before creating a profile. Alternatively, when creating a process step collection, you can switch to the configuration using the appropriate context actions without having to leave the process step configuration.

Enabling rule-based archiving

In order to archive e-mails based on rules, you have to enable the option in d.ecs content crawler.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Archiving options** under **E-mail archiving**.
3. Go to the **Processing settings** perspective.
4. Enable the option for rule-based processing and save your details.

Creating your own sources for mappings

Pre-configured sources for creating mappings are available to you as standard with the integrations and d.ecs content crawler. However, you can also create your own sources with additional custom fields.

You do not need to define sources for journal archiving because you can use the applicable standard source.

> **Note**
> If a source is being used for a configuration, you can no longer change or delete the source.

Let's assume you want to define your own source for a mapping.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Sources** under **E-mail management**.
3. In the source overview, choose the context action **Create new source**.
4. Enter a unique name for the source.
5. Select the base source from which you want the source to obtain basic information.
6. If necessary, select **Add or edit custom field** to define additional custom fields for the source.
7. Enter the name of the custom field as the name appears in the source system.
8. Enter a display name for the custom field.
9. Under **Type**, select a file type for the custom field.
10. Click **Add**.

You can now add, edit and delete custom fields as required or save your entries to use the source for a mapping.

See also:

- Detailed information about sources
- Detailed information about categories
- Detailed information about mappings

Creating your own categories for a mapping

You must define at least one category to create a mapping.

You do not need to define categories for journal archiving because you can use the applicable default category.

> **Note**
> If a category is being used for a configuration, you cannot delete the category.

Let's assume you want to define your own category for a mapping.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Categories** under **E-mail management**.
3. In the category overview, choose the context action **Create new category**.
4. Enter a unique name for the category and save your entries.

See also:

- Detailed information about categories
- Detailed information about sources
- Detailed information about mappings

Creating a profile

To e.g. archive e-mails from your mailboxes in a rule-based manner, you need a profile. Before you can create a profile, you need at least the following:

- A configured connection to the source system (Microsoft Exchange or HCL Domino)
- A mapping with a source and a category

All other necessary components of the profile (sources collection, rule collection, process step collection) can also be created in advance or directly from the profile settings.

Suppose you want to create a profile.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Profiles** under **E-mail archiving**.
3. Create a new profile by clicking the plus symbol.
4. Enter a unique name and a description for the profile.
5. Specify which e-mail system should process the profile under **Source system**, e.g. **Microsoft Exchange**.
6. Select a Microsoft Exchange connection if you selected **Microsoft Exchange** under **Source system**.

> **Note**
> You can also specify several configured Microsoft Exchange servers. This means that the same profile can be used to process mailboxes that are partially configured in Microsoft Exchange On-Premises and in Exchange Online (hybrid scenario).
>
> You can find more information on this in the following chapters:
>
> - Setting up multiple connections to the Microsoft Exchange server with Microsoft Exchange (on-premises)
> - Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft EWS
> - Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft Graph

7. Select a sources collection for the profile. Alternatively, use **Create source collection** to add a new sources collection.
8. Select a rule collection for the profile. Alternatively, use **Create rule collection** to add a new rule collection.
9. Select a process step collection for the profile. Alternatively, use **Create process step collection** to add a new process step collection.
10. Specify whether the profile is a prioritized profile.
11. Select the days and the durations for the profile's time control.
12. Save your entries.

See also:

- Detailed information on profiles
- Detailed information about mappings
- Creating your own sources for mappings

Creating a sources collection

You need a sources collection to create a profile.

For example, suppose you want to create a new sources collection.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Sources** under **E-mail archiving**.
3. Click the plus icon to add a new sources collection.
4. Provide a unique name and description for the sources collection.
5. Add a source, e.g. the type **User**.
6. Enter a name for the source, e.g. **Administrator**.
7. Click **Add**.
8. If necessary, add further sources and save your information.

You can then use the new sources collection to create your profile.

See also: Detailed information on sources collections

Creating a rule collection

You need a rule collection to create a profile.

> **Note**
> In order to process e-mails, you must configure the **Documents not archived** or **Documents archived** rule as a minimum.

For example, suppose you want to create a new rule collection.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Rules** under **E-mail archiving**.
3. Click the plus icon to add a new rule collection.
4. Select the context action to add a new rule collection.
5. Provide a unique name and description for the rule collection.
6. Add a rule, e.g. **Documents archived**.
7. Click **Add**.
8. If necessary, add further rules and save your information.

You can then use the new rule collection to create your profile.

See also: Detailed information on rule collections

Creating a process step collection

You need a process step collection to create profiles.

Suppose you want to add an **Archive document** process step to a new process step collection.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Under **E-mail archiving**, select the entry **Process steps**.
3. Click the plus icon to add a new process step collection.
4. Provide a unique name and description for the process step collection.
5. Add the process step **Archive document**.
6. Select a repository.
7. Select a source.
8. Select a category.
9. If necessary, add a post-processing action, e.g. specify that attachments should be linked.
10. Select a profile-related check for duplicates, if necessary.
11. If necessary, enable **Process dbs | case manager data**.
12. Click **Add**.
13. If necessary, add further process steps and save your information.

You can then use the new process steps collection to create your profile.

See also: Detailed information on process step collections

1.4.13. Configuring a service user

To be able to work with d.ecs content crawler, you need a service user. This user is used to save documents in the d.3 repository, for example.

The service user must meet the following requirements:

- The user must be assigned to the administrative group that you have specified as the administrative group in d.ecs identity provider.
- The user must have rights to read documents with **Read processing**, **Read verification** or **Read public** status in the d.3 administration.
- The user must have the right to import a document in the d.3 administration.

1.4.14. Configuring error jobs

External dependencies can result in network failures, for example. To ensure correct operation, error jobs are created for all actions in d.ecs content crawler. In the event of errors, the jobs are given a corresponding status.

You can define how error jobs are processed. For example, you can define how often error jobs should be restarted in order to search for the cause of the error manually and to restart the jobs manually. You can also specify an interval for restarting the error jobs. You can combine the options for the maximum number of restarts and the interval.

Suppose you want to specify that error jobs are restarted a maximum of seven times. You also want to define a specific day and time when error jobs should be restarted.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Archiving options** under **E-mail archiving**.
3. Switch to the **Error handling** perspective.
4. Enable the Automatic restarts of error jobs option.
5. Enter **7** for the maximum number of restarts.

6. Enable **Reset error jobs on service restart**.
7. Select the appropriate day.
8. Click **Add time**.
9. Enter the appropriate value.
10. Click **Add** and save your entries.

1.4.15. Configuring change logging

Change logging records changes made to the system in a central location. You can view detailed information about the changes, if required.

Enabling change logging

Suppose you want to enable change logging. Note that the action of disabling change logging will also be logged.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Archiving options** under **E-mail archiving**.
3. Switch to the **Error handling** perspective.
4. Enable the **Change logging** option.
5. Save your entries.

Displaying the change log

Suppose you want to view the details of logged changes.

This is how it works

1. Select the **d.ecs content crawler** feature from the start page.
2. Click **Change logging**.
3. Click an entry to display the detailed view.

1.5. Tips and tricks

This topic provides you with useful tips on functions and tips for making your work easier.

1.5.1. Enabling HTTPS for secure communication between d.ecs http gateway and the app instances (optional)

The communication of the d.3one integrations with the browser and d.ecs http gateway is generally encrypted with HTTPS. The communication between the d.ecs http gateway app and the d.ecs content crawler app is unencrypted with HTTP. Apps that are hosted on Internet Information Services (IIS) are excluded. Communication for these apps is already encrypted using the TLS protocol (Transport Layer Security Protocol).

You can also encrypt the communication between the d.ecs http gateway app and d.ecs content crawler with a certificate that uses the TLS protocol. The protocol used corresponds to the security standard, with SSL (Secure Sockets Layer) being used synonymously with TLS.

In order to encrypt the communication, you have to assign a fixed port to enable TLS for d.ecs content crawler. In addition, you need the hash value of the certificate and the application identifier to link the certificate to the port.

Determining the hash value of the certificate to be linked

If you have defined a port for the d.ecs content crawler app, you need to determine the hash value of the certificate that you want to link.

In addition to the hash value, you need an application identifier (app ID). You can use any valid GUID in the format **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX**. Using the hash value and the application identifier, you can link the certificate to the app port.

You can use the same certificate that you use in IIS. If you want to use a different certificate, you can use the properties of the certificate to determine the hash value (finger print). Remove any space characters.

Suppose you want to find out the hash value of the certificate.

This is how it works

1. Start the Windows command prompt as administrator.
2. Enter the command **netsh http show sslcert ipport=0.0.0.0:<Port>**. Replace **<Port>** with the port number you specified when installing d.3one (**3401** by default).
3. Copy the value for **Certificate hash**, e.g. into a text editor.

Specifying the port in the d.ecs content crawler app

In order to encrypt communication between the apps, you have to enable TLS in the d.ecs content crawler app and assign a fixed port to the app.

This is how it works

1. Open the **bin** folder in the installation directory of the d.ecs content crawler app (e.g.: C:\d3\d.3 content crawler\bin).
2. Open the **dvelop.GroupwareCrawler.App.exe.config** file with a text editor.
3. In the **appSettings** area, enter the value **https** for **protocol** (e.g.: **<add key="protocol" value="https">**).
4. Enter a fixed value for **port lower bound** and **port upper bound** (e.g.: **<add key="port lower bound" value="4010" /><add key="port upper bound" value=4010" />**).
5. Save the file.
6. Restart the service in the **d.3content crawler app**.

Linking the certificate and port of the d.ecs content crawler app

Once you have specified a port and determined the certificate, you can link the certificate to the port of the d.ecs content crawler app.

This is how it works

1. Start the Windows command prompt as administrator.
2. Enter the command **netsh http add urlacl url=https://*:<Port>/ user=<User>**. Replace **<Port>** with the port number and **<User>** with the user running the app.
3. Enter the command **netsh http add sslcert ipport=0.0.0.0:<Port> certstorename=<storename> certhash=<hash> appid={<appid>}**. Replace **<storename>** with the certificate store, **<Port>** with the port number, **<hash>** with the saved hash value and **<appid>** with the application ID.
4. Confirm the command.

If the port was linked successfully, you can view the linked port in the Windows command prompt using the command **netsh http show sslcert**. You can also directly display the linked port using the command **netsh http show sslcert ipport=0.0.0.0:<Port>**. Replace **<Port>** with the port number.

Then restart the relevant apps to ensure that the apps use HTTPS instead of HTTP when registering at the d.ecs http gateway app.

Example

```
netsh http show sslcert ipport=0.0.0.0:3401
netsh add urlacl url=https://*:4000/ user=SYSTEM netsh http add urlacl
```

```
url=https://*:4000/ user=SYSTEM
netsh http add sslcert ipport=0.0.0.0:4000 certstorename=Root
certhash=e31c06568e4b222a92c8434eaa770b26f09a31a3 appid={2131f4cd-
d05b-4308-9af1-9caa44b2c74a}
```

See also: Checking the registration in d.ecs http gateway

1.5.2. Adjusting the logging level in d.ecs content crawler

You can adjust the logging level in the groupware app and the d.ecs content crawler app to suit your needs.

In d.ecs content crawler, you can also enable extended logging in order to receive more detailed information in the event of an error. If you enable extended logging, you can display information about a job and identify the associated document more quickly.

Suppose you want to use the d.ecs content crawler to display all messages in the central d.3 log and enable extended logging.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Archiving options** under **E-mail archiving**.
3. Switch to the **Error handling** perspective.
4. Under **Log level**, select **All**.
5. Enable **Extended logging** and save your details.

See also: Detailed information about logging

1.5.3. Preparing the check for duplicates

You can avoid storing unnecessary duplicates in the d.3 repository using the Groupware app.

To ensure that the check for duplicates works properly, you must ensure that the items in the repository are imported and stored with the appropriate d.3 status. For example, if you want to enable importing and storing with a status when creating a mapping for the item **E-mail**, you must define the value **No** for the following parameters in the d.3 admin configuration:

- **IGNORE_DUPS_IN_A**: For checking items that are stored directly with the status **Archive**.
- **IGNORE_DUPS_IN_B_P**: For checking items that are stored directly with the status **Processing** or **Verification**.

For more information about the parameters and the check for duplicates, see the d.3 admin manual.

1.5.4. Enabling the check for duplicates

You can avoid storing unnecessary duplicates in the d.3 repository by enabling the check for duplicates in the Groupware app. You can enable the function for d.3one and d.ecs content crawler.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Management options** under **E-mail management**.
3. In the **Groupware settings** perspective, select the option for checking for duplicates.
4. Save your entries.

1.5.5. Configuring a permission check

When you save e-mails in the d.3 repository, all the recipients and the sender of the e-mail are written to a d.3 system field (**dvelop.groupware.mail.restrictions**). With d.3 server version 8, you have the option

of setting a permission check using restriction sets. Existing groups in the recipient list are retroactively resolved.

> **Note**
> If the X.500 address of internal recipients or the internal sender cannot be resolved, an error message is written to the log. In addition, the d3 system field **d.velop.groupware.mail.restrictions.resolve.error** is filled with the value **1** to ensure that you can identify and correct the affected document easily.

Furthermore, when saving from the e-mail application, the following values are written to d.3 system fields and can be used for your permission check:

- **dvelop.groupware.messageID**: The message ID of the e-mail. The ID is also entered when saving attachments.
- **dvelop.groupware.attachmentid**: The attachment ID when saving an individual attachment.
- **dvelop.groupware.recoverableItem**: If the saved document is based on an e-mail that is marked as deleted in Microsoft Exchange, the value is **1**.
- **dvelop.groupware.attachments.count**: The number of attachments is entered when saving an e-mail.
- **d.velop.groupware.attachments.name**: The file name for the attachment when an e-mail is saved.
- **dvelop.groupware.attachments.extension**: The file extension, including the period, for the attachment when an e-mail has been saved.
- **d.velop.groupware.attachments.index**: The internal index of attachments when saving e-mails. Specify the parameter if you want to create a retrieval link.
- **dvelop.groupware.attachments.size**: The file size of the attachments when saving the e-mail.
- **dvelop.groupware.attachments.type**: The display of the attachment type. If the value is **EMBEDDED**, the attachment is embedded. If the value is **FILE**, the attachment is an attached file.
- **dvelop.groupware.mail.restrictions**: A table that contains all the recipients and the sender of the e-mail (permission control).
- **dvelop.groupware.cm.token**: If the option **dbs | case manager-data process** is enabled in d.ecs content crawler, the dbs | case manager token is entered.
- **dvelop.groupware.mail.conversationid**: The conversation ID (message header: **Thread-Index**).

The following system fields are written only if the check for duplicates is disabled.

- **dvelop.groupware.exchange.mailbox.objectguid**: The unique object GUID of the d.3one user that saved the item in the d.3 repository.
- **dvelop.groupware.exchange.mailbox.userguid**: The unique object GUID of the mailbox user from d.ecs identity provider.
- **d.velop.groupware.exchange.mailbox.name**: The name of the Microsoft Exchange mailbox where the saved e-mail is located.

1.5.6. Enabling the function to restore multiple e-mails at the same time

You can restore multiple e-mails at the same time with d.ecs content crawler.

DGIX, MSG, NZIP and EML formats are supported when restoring e-mails. If the target system is HCL Domino, you can only select e-mails that were saved with the Domino service when restoring.

To be able to restore e-mails, you have to enable the option in d.ecs content crawler.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Archiving options** under **E-mail archiving**.
3. Go to the **Processing settings** perspective.

4. In the **Restore** area, enable the **Restore e-mails** option.

1.5.7. Restoring multiple e-mails from the results list of a search

If you have enabled the option to restore e-mails, you can use the search in d.3one to restore several e-mails from the results list of a search at the same time. You can then specify a destination for the restored e-mails.

If you select HCL Domino as the target system, enter the name of the physical HCL Notes database as the database (**mail\user1.nsf**).

If you select Microsoft Exchange as the target system, enter an SMTP address or a user name as the target mailbox. In Microsoft Exchange, you can also specify macros as the target folder. If necessary, you can enable the option **Microsoft Exchange in-place archive** if the e-mails are to be imported into the in-place archive.

Suppose you want to restore multiple e-mails from a results list.

This is how it works

1. Carry out a search in the **Search** feature that contains the e-mails you want to restore.
2. Select the **Restore e-mails** context action.
3. Select individual or all e-mails from the results list and click on **Restore e-mails**.
4. Enter a description for the job.
5. Select a target system.
6. Specify a target mailbox or database.
7. Enter a target folder. The sub-folder will be created automatically.
8. Start the restore process.

A job is created in the **Restore** profile for each e-mail to be restored.

1.5.8. Monitoring d.ecs content crawler with d.ecs monitor

If you want to use d.ecs monitor to monitor d.ecs content crawler, you have to install d.ecs monitor agent in the respective d.3ecm system environments. If the d.ecs monitor agent already exists in your d.3ecm system environment, the agent will be recognized automatically and the d.ecs monitor agent will send the status information to d.ecs monitor.

With d.ecs monitor you receive general information about the status of d.ecs content crawler, e.g. CPU usage, memory consumption or the number of threads. The d.ecs content crawler app also sends the number of faulty jobs to d.ecs monitor. You can view the jobs under **Monitoring object**. By default, an alarm is triggered in d.ecs monitor once there are 100 jobs with an error status. You can adjust the value if necessary.

Further information on d.ecs monitor can be found in the d.ecs monitor administration manual.

1.5.9. Monitoring journal archiving

If you want to monitor the journaling function, we advise that you include the journal mailbox of the e-mail application. You can then identify unprocessed e-mails faster and take action.

Alternatively, you can run PowerShell scripts regularly.

1.5.10. Defining a different port and HTTP protocol

The app port is determined dynamically by default. If necessary, you can also change the port and the HTTP protocol.

This is how it works

1. In the app installation directory, create a folder with the name **conf**.
2. Create a file with the name **appsettings.config**.
3. Define the port by entering the same value for both the upper and lower bounds.
4. Enter a value for **protocol**, such as **http** or **https**.
5. Restart the app.

```
<?xml version="1.0" encoding="utf-8"?>
<appSettings>
  <add key="port lower bound" value="4000" />
  <add key="port upper bound" value="4200" />
  <add key="protocol" value="http" />
</appSettings>
```

However, you can also configure the search for a free port:

- **port lower bound**: Indicates the lower bound above which you want the app to search for a free port.
- **port upper bound**: Indicates the upper bound below which you want the app to search for a free port.
- **protocol**: Indicates the protocol through which you want the app to establish connections. The possible values are **http** or **https**.

1.6. Frequently asked questions

In this section, you can find answers to frequently asked questions.

1.6.1. From which folders are deleted elements archived if I have litigation hold or in-place hold enabled?

If you have litigation hold or in-place hold enabled, the **Deletions** and **Purges** folders are archived when you archive deleted items. The folders are not archived from the archive folder.

For more information, see “Recoverable items folder in Exchange Server” in the Exchange Server 2019 documentation on the Microsoft Docs website.

1.6.2. Which message classes are suitable for journaling, mailbox archiving or manual storage with the Microsoft Outlook add-in?

The IDs in the following list help you to understand which message classes are suitable for journaling or mailbox archiving in d.ecs content crawler. In addition, you will learn which message classes support manual storage in the d.3one integration in Microsoft Outlook.

IPM.Activity

- Name: Journal entries
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM.Appointment

- Name: Appointments
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Contact

- Name: Contacts
- Journaling: No

- Mailbox archiving: No
- Manual storage: No

IPM.DistList

- Name: Distribution list (stored as ZIP containers with individual vCards)
- Journaling: Yes (as attachment to an e-mail)
- Mailbox archiving: Yes (as attachment to an e-mail)
- Manual storage: Yes (as attachment to an e-mail, is not considered an attachment when saving)

IPM.Document

- Name: Documents
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM.OLE.Class

- Name: Exceptional items deviating from the batch pattern
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM

- Name: Items for which the specified form was not found
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM.Note

- Name: E-mails
- Journaling: Yes
- Mailbox archiving: Yes
- Manual storage: Yes

IPM.Note.IMC.Notification

- Name: Reports from Internet Mail Connector (Microsoft Exchange Server gateway to the Internet)
- Journaling: Yes
- Mailbox archiving: Yes
- Manual storage: Yes

IPM.Note.Rules.Oof.Template.Microsoft

- Name: Templates for automatic replies
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: Yes

IPM.Post

- Name: Providing notes in a folder
- Journaling: Yes
- Mailbox archiving: No

- Manual storage: No

IPM.StickyNote

- Name: Creating notes
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM.Recall.Report

- Name: Message recall reports
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM.Outlook.Recall

- Name: Revoking sent messages from the mailbox of a user
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM.Remote

- Name: Remote mail message header
- Journaling: No
- Mailbox archiving: No
- Manual storage: No

IPM.Note.Rules.ReplyTemplate.Microsoft

- Name: Templates for automatic replies
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: Yes

IPM.Report

- Name: Status reports for items
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Resend

- Name: Sending a faulty message again
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Schedule.Meeting.Canceled

- Name: Meeting cancellations
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Schedule.Meeting.Request

- Name: Meeting requests
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Schedule.Meeting.Resp.Neg

- Name: Responses to cancellations of meeting requests
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Schedule.Meeting.Resp.Pos

- Name: Responses to the acceptance of meeting requests
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Schedule.Meeting.Resp.Tent

- Name: Responses to the acceptance of meeting requests
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Note.Secure

- Name: Digitally signed notes to other persons
- Journaling: Yes
- Mailbox archiving: Yes
- Manual storage: Yes

IPM.Note.Secure.Sign

- Name: Encrypted notes to other persons
- Journaling: Yes
- Mailbox archiving: Yes
- Manual storage: Yes

IPM.Task

- Name: Tasks
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.TaskRequest.Decline

- Name: Responses to acceptance of a task request
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.TaskRequest

- Name: Task requests
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.TaskRequest.Update

- Name: Update to requests
- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.conflict.message

- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.sharing

- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

Report.report.ipm.note.ipnrn.ndr

- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

IPM.Schedule.Meeting.Notification

- Journaling: Yes
- Mailbox archiving: No
- Manual storage: No

1.6.3. Why do I not see the option to archive deleted elements when creating a profile?

When creating a profile, the **Enable archiving of deleted elements** option is only available if you select **Microsoft Exchange** as the source system. The option is supported by d.ecs content crawler with Microsoft Exchange 2016 or higher.

1.6.4. What is the difference between deleting and resetting jobs?

In the d.ecs content crawler feature, you can navigate to the **Job overview** area under **Statistics overview** to mark jobs and, if necessary, delete or reset them with the appropriate context actions. If you want to delete a profile, make sure that there are no more jobs for that profile in the database.

If you delete the marked jobs, the jobs are deleted from the database and the underlying documents are reset.

If you reset the marked jobs, the jobs and the underlying documents are reset. These jobs are then processed again immediately with the profile.

1.6.5. What is a named user license?

A named user license is used to assign a dedicated user to a product or an integration. Due to this assignment, a license is reserved for one user and the license cannot be used by any other user.

The first time that each d.3one integration is started, named user licences are assigned for the user and the d.3one integration. For example, if a user logs into d.3one in the browser or integration, a license is reserved for this user and for this product in d.ecs license server.

See also: Detailed information about d.3one licenses

1.6.6. What are categories?

You can help your users with their daily work by defining categories for storing items. By default, there are no predefined categories. However, you can create your own categories in the administration.

You can classify sources (e.g. e-mails or attachments) for storage in the repository using d.3 categories (document types). Furthermore, you can also use the Groupware app to define your own categories in which items are stored. You can use a category to map a source to multiple d.3 categories.

You can customize the categories, because the categories are independent of the repository and the source.

See also:

- Creating categories
- Detailed information about sources
- Detailed information about mappings

1.6.7. What are profiles?

To use rule-based archiving, you must create profiles. A profile has three central components: sources, rules and process steps.

Sources, rules and process steps are combined into collections. You can use these collections to determine which items are archived and, if necessary, post-processed based on which rules.

To ensure that the properties of e-mails can be assigned to the corresponding d.3 properties, you must create a mapping.

See also:

- Creating profiles
- Detailed information on sources collections
- Detailed information on rule collections
- Detailed information on process step collections

1.6.8. What are sources?

Mappings let you link any source system (e.g. an e-mail application or ERP system) with a d.3 repository.

A source system can specify multiple sources, such as e-mails and attachments. The sources describe an item with specific properties and categories in the source system.

In the case of archiving profiles, sources are data pools from which items are read, such as Microsoft Exchange users, groups, or public folders.

In the context of the Groupware app, sources are items to be processed, such as e-mails or attachments. The app identifies the properties of the source (e.g. sender, subject or recipient) and generates the document file to be stored.

You can use a mapping to link the properties of a source with specific d.3 property fields (repository fields). You can define your own sources for mappings.

You can also further classify the sources by creating categories. The categories are independent of the categories (document types) in the d.3 repository.

The e-mail integrations and d.ecs content crawler provide you with default sources for creating mappings:

- **Standard - Microsoft Exchange e-mail**
- **Standard - Microsoft Exchange attachment**
- **Standard - Microsoft Exchange journal e-mail**
- **Standard - IBM Notes e-mail**
- **Standard - IBM Notes attachment**
- **Standard - IBM Notes journal e-mail**
- **Standard - appointment/meeting**

See also:

- Creating sources
- Detailed information about categories
- Detailed information about mappings

1.6.9. What are sources collections?

For rule-based archiving, you must specify the sources that are to be archived in each profile. The sources are mailboxes or mail databases from which items are archived. A sources collection can consist of several sources. To specify the mailboxes or mail databases to archive for a profile, create and configure a sources collection.

Depending on the source added, certain special features apply, e.g.:

- **User**:
  - The mailboxes are determined automatically using the specified user name.
  - Since the address book is searched, several mailboxes from different users may be found for one entry.
- **Group**:
  - The mailboxes are determined automatically using the specified group.
  - Groups can also be broken down into groups.
  - For Microsoft Exchange, you must provide the group's SMTP address. The group must be visible in the Microsoft Exchange address book in order to be resolved.
- **Microsoft Exchange public folder**:
  - The mailboxes are determined using the specified file path.
  - If you want to prevent sub-folders from also being archived, select the **Folder restriction** rule.
- **Microsoft Exchange in-place archive**:
  - The mailboxes are determined using the specified Microsoft Exchange in-place archive.
  - With Microsoft Exchange, you must provide the SMTP address of the in-place archive.
  - Make sure that in-place archiving is enabled for the mailbox.

See also:

- Creating sources collections
- Detailed information on profiles
- Detailed information on rule collections
- Detailed information on process step collections

1.6.10. What are rule collections?

In each profile you have to specify a set of rules. The rules are used to determine which items are archived. Several rules are linked with AND relations and are combined into a rule collection. To define the archiving rules for a profile, create and configure a rule collection.

Depending on the rule added, certain special features apply, e.g.:

- **Folder restriction**:
  - You can set folder inclusions or folder exclusions for Microsoft Exchange or HCL Domino.
  - A rule can only contain inclusion rules or exclusion rules.
  - Enter sub-folders with a backslash (\). For example, if you also want to archive a sub-folder called **Invoices**, enter **Inbox\Invoices** as the folder inclusion.
  - Using the option **Include sub-folders**, you can specify for each folder whether the sub-folders are also archived. For example, if you do not want to archive any items from the **Deleted items** folder or its sub-folders, enter **Deleted items** as the folder exclusion and enable **Include sub-folders**.
  - You can reference the inbox for HCL Domino using the **$Inbox** macro. You can also use the macro to reference the folders you have created with the appropriate names.
  - Various macros are also available for Microsoft Exchange. Including sub-folders may increase the load on the Microsoft Exchange Server or the HCL Domino Server.
- **External rule check**:
  - You can choose to check an item with an external application instead of a previously created rule. Enter the URI for the rule check.
  - The external rule check is always carried out as the last step after all preceding rules. For more information on the structure of the HTTP calls and the data to be transmitted, for example, see the sections on configuring the external rule check.
- **Check for subject**:
  - The content of the subject is used to check which items will be archived. You can include or exclude e-mails by subject.
  - When entering search terms, please note that they are case-sensitive.
  - If you enable the option **Match all**, all search terms must appear in the subject (AND relation).
  - If you enable the option **Match any**, at least one search term must appear in the subject (OR relation).
- **Using a regular expression on subject**: You can choose to include or exclude subjects from e-mails using a regular expression. To exclude items, select the option **No processing**.
- **Only external mails**: Only items that have at least one external recipient or sender are identified. Senders or recipients are considered internal if they contain the domain. If the item contains only internal addresses, the item will not be processed.

See also:

- Creating rule collections
- Detailed information on profiles
- Detailed information on sources collections
- Detailed information on process step collections
- Detailed information on the external rule check
- Detailed information on the external rule check with d.ecs script

1.6.11. What are process step collections?

In each profile, you must specify the process steps in order to define how the archived items will be processed. To determine which steps are to be used during processing, you can create and configure a process step collection.

Depending on the process step added, certain special features apply, e.g.:

- **Archive document**:
  - All identified items are archived.
  - You can also define the post-processing of the items.
  - We recommend the delete option only for monitoring functional mailboxes.
  - You can delete items that have already been archived at a later date by creating a profile with the post-processing action Delete.

  - If you enable the option **Process dbs | case manager data**, the processing speed of the e-mail archiving may be affected. Use this option only for dbs | case manager functional mailboxes. You cannot use this process step with the **Documents archived** rule.
- **Save in file system**:
  - All identified items are transferred to the file system in EML format.
  - If necessary, you can enable **No sub-folders** to specify that only the top-level folders are archived.
  - If you enable the option for processing PEC e-mails, the attached EML e-mails are transferred to the file system and the attachments are saved separately. You cannot use this process step with the **Documents archived** rule.
  - You can specify a static or dynamic path. For a static path, enter the full path in the "Path" field. For a dynamic path, enter the macro **<SMTPADDRESS>** anywhere in the path, e.g. **C:\export\<SMTPRADDRESS>**. Create a regular expression for the macro that can determine a piece of text from an SMTP address. This piece of text is inserted at the location of the **<SMTPADDRESS>** macro. Example:
    - Path: **C:\export\<SMTPRADDRESS>**
    - Input: **Smith@Domain.com**
    - Regular expression: **(?<=@)[^.]+(?=\.)**
    - Output path: **C:\export\Domain**
  - If you are using HCL Domino, the system does not determine the SMTP address but rather provides the name of the e-mail database for performance reasons. Therefore, you need to create a regular expression for a dynamic path as follows:
    - Path: **C:\export\<SMTPRADDRESS>**
    - Input: **mail\\bbenutze**
    - Regular expression: **[a-zA-Z]{8}**
    - Output path: **C:\export\bbenutze**
- **Storage with d.velop inbound**:
  - The option **Pass PDF attachments to d.velop inbound** extracts attachments in PDF format and transfers the attachments to d.velop inbound.
  - You can use the option **Pass entire mail to d.velop inbound** only if you have a subscription for d.velop inbound in the d.velop cloud.
- **Post-processing action**:
  - You can specify how items that have already been archived are processed.
  - Attachments are only removed and replaced with HTTP links if it is evident that the attachment can be removed. With certain e-mail formats, it is not always clear whether the attachments can be removed, e.g. MIME formats. The corresponding e-mails are still saved in full in the d.3 repository.
  - To reduce the e-mail load and ensure suitable formatting, check the settings of your mail gateway.
  - You cannot apply this process step at the same time as the **Documents not archived** rule.
- If you select multiple processing steps, the following dependencies result:
  - You can create only one processing step with post-processing enabled. The processing step with post-processing is always executed as the last step after all previous processing steps.
  - You can select the option **Storage with d.velop inbound** only once.
  - You can select only one post-processing action.
  - You can use the options **Archive document** and **Save in file system** multiple times for different parameters.

See also:

- Creating process step collections
- Detailed information on profiles
- Detailed information on sources collections
- Detailed information on rule collections

1.6.12. What are mappings?

A mapping lets you link a source system (e.g. an e-mail application) with a destination (a d.3 repository).

Each e-mail has certain standard properties, such as the sender, recipient or subject. You can map the standard properties to a d.3 category and the appropriate d.3 properties. If you create appropriate mappings, your users no longer have to specify these properties manually.

You can find additional information about creating and managing mappings in the d.3one administration manual.

See also:

- Detailed information about sources
- Creating sources
- Detailed information about categories
- Creating categories

1.6.13. What authentication options do I have when configuring a database server?

SQL Server authentication is the only authentication mechanism supported. Other options such as Windows authentication are not available.

1.6.14. Which jobs are processed when I change a rule-based archiving profile?

If you change profiles for rule-based archiving, the changes will be adopted the next time the d.ecs content crawler is run without restarting.

Jobs are processed immediately with the new profile configuration.

1.6.15. Which source properties are mapped to which field names in HCL Notes or Microsoft Outlook?

In this list, you can find information about the source properties for creating mappings. You can use the list to see which source properties are mapped to which field names in Microsoft Outlook and HCL Notes.

All recipient names (To, Cc and Bcc)

- HCL Notes: Calculated value
- Microsoft Outlook: Calculated value
- Meaning: List of all recipients (To, CC and BCC) as display names (if available)

All recipient SMTP addresses (To, Cc and Bcc)

- HCL Notes: Calculated value
- Microsoft Outlook: **RecipientTable**
- Meaning: List of all recipients (To, CC and BCC) as e-mail addresses (if available). If the online e-mail address is unavailable in the Domino Directory, the value from the e-mail is used.

Text body

- HCL Notes: **Body**
- Microsoft Outlook: **PR-BODY**
- Meaning: Defined text content from the e-mail content. In unencrypted e-mails, the text content cannot be read and is therefore transmitted as empty. In unencrypted e-mails, the text cannot be read. As a result, mapping always results in an empty value.

Created on

- HCL Notes: **Created** document property
- Microsoft Outlook: **PR_CREATION_TIME**

- Meaning: Date that the e-mail was created

Received on

- HCL Notes: **DeliveredDate**
- Microsoft Outlook: **PR_MESSAGE_DELIVERY_TIME**
- Meaning: Date that the e-mail was delivered

Last modification time

- HCL Notes: **$Revisions**
- Microsoft Outlook: **PR_LAST_MODIFICATION_TIME**
- Meaning: Date that the e-mail was last changed

Message ID

- HCL Notes: **$MessageID**
- Microsoft Outlook: **PR_INTERNET_MESSAGE_ID**
- Meaning: Unique message ID for the e-mail

Message size in bytes

- HCL Notes: Calculated value
- Microsoft Outlook: **Size**
- Meaning: Size of the e-mail

Recipient names

- HCL Notes: **SendTo**
- Microsoft Outlook: Calculated value
- Meaning: List of the recipients as display names (if available)

Recipients' SMTP addresses

- HCL Notes: **SendTo**
- Microsoft Outlook: Calculated value
- Meaning: List of the recipients as e-mail addresses

Recipient names (Bcc)

- HCL Notes: **BlindCopyTo**
- Microsoft Outlook: **RecipientTable**
- Meaning: List of the blind copy recipients as display names (if available)

Recipients' SMTP addresses (Cc)

- HCL Notes: **CopyTo**
- Microsoft Outlook: **RecipientTable**
- Meaning: List of the copy recipients as e-mail addresses

All SMTP addresses (From, To, Cc and Bcc)

- HCL Notes: Calculated value
- Microsoft Outlook: **RecipientTable**
- Meaning: List of all SMTP addresses

Sender name

- HCL Notes: **From**
- Microsoft Outlook: **PR_SENDER_NAME**
- Meaning: Name of the sender

SMTP address of the sender

- HCL Notes: **From**
- Microsoft Outlook: **PR_SENDER_EMAIL_ADDRESS**
- Meaning: SMTP address of the sender

Subject

- HCL Notes: **Subject**
- Microsoft Outlook: **PR_SUBJECT**
- Meaning: Subject line of the e-mail

Sent on

- HCL Notes: **PostedDate**
- Microsoft Outlook: **PR_CLIENT_SUBMIT_TIME**
- Meaning: Date that the e-mail was sent

Number of attachments

- HCL Notes: Calculated value
- Microsoft Outlook: Calculated value
- Meaning: Number of attachments

Sent on behalf of (SMTP address)

- Microsoft Outlook: **PR_RCVD_REPRESENTING**
- Meaning: SMTP address of the deputy sender

Sent on behalf of (name)

- Microsoft Outlook: **PR_RECEIVED_BY**
- Meaning: Name of the deputy sender

Time (received/sent on/created)

- HCL Notes: Calculated value
- Microsoft Outlook: Calculated value
- Meaning: Delivery date (if available). If the delivery date is unavailable, either the submission date (Submit) or creation date (Create) is used. The creation date is always available.

Mailbox ID

- Microsoft Outlook: **MBADGUID**
- Meaning: Mailbox ID in the Active Directory. The mailbox ID can be used to control authorization, for example.

Mailbox name

- Microsoft Outlook: Calculated value
- Meaning: Name of the Microsoft Exchange mailbox (the SMTP address by default)

Folder name (last level)

- HCL Notes: Calculated value
- Microsoft Outlook: Calculated value
- Meaning: Folder containing the e-mail. With HCL Notes e-mails, the folder path can be determined only if the folder references in the mail database have been activated and the e-mail has been received or moved following the activation. Do not use backslashes (\) when mapping folder names. Backslashes are required to map **Folder path (split)**.

Folder path

- HCL Notes: **$FolderRefs**
- Microsoft Outlook: **PR_FOLDER_PATH**
- Meaning: Complete path of the folder containing the e-mail.

Folder path (split)

- HCL Notes: Calculated value
- Microsoft Outlook: Calculated value
- Meaning: List of folders containing the e-mail, calculated from the folder path.

For attachments:

File name

- HCL Notes: Calculated value
- Microsoft Outlook: **PR_ATTACH_FILENAME**
- Meaning: Original file name of the attachment

File size in bytes

- HCL Notes: Calculated value
- Microsoft Outlook: **PR_ATTACH_SIZE**
- Meaning: Size of the file in bytes

File extension

- HCL Notes: Calculated value
- Microsoft Outlook: **PR_ATTACH_EXTENSION**
- Meaning: The file extension

For user information, you can select the login name of the Windows user that is assigned to the mailbox using the **Mailbox SAM account name** display name. The SAM account name can be identified only if you have configured an Active Directory in d.ecs identity provider. Furthermore, you must specify a user with the SMTP address of the mailbox, which is not always possible with Microsoft Office 365.

1.6.16. How do I archive PST files based on rules?

The processing of PST files is indirectly supported by d.ecs content crawler. We recommend importing a PST file into an in-place archive. Follow the method stipulated by Microsoft. You can archive the in-place archive with d.ecs content crawler.

To archive an in-place archive, you must select a **Microsoft Exchange in-place archive** source library as the source and specify the mailbox to be processed. The post-processing corresponds to the processing of other source types. You can adapt all rules and process steps to your needs.

For more information about in-place archives, see “In-place archiving in Exchange Server” in the Exchange Server 2019 documentation on the Microsoft Docs website.

For more information about importing PST files, see “Procedures for mailbox imports from .pst files in Exchange Server” in the Exchange Server 2019 documentation on the Microsoft Docs website.

1.6.17. How do I archive in a legally compliant manner with Microsoft Exchange Online without an external mailbox?

If you want to archive in a legally compliant manner with Microsoft Exchange Online without an external mailbox, you can enable the option **Archive deleted elements** for rule-based archiving in d.ecs content crawler. In this case you need the dbs | mailbox archiver solution package.

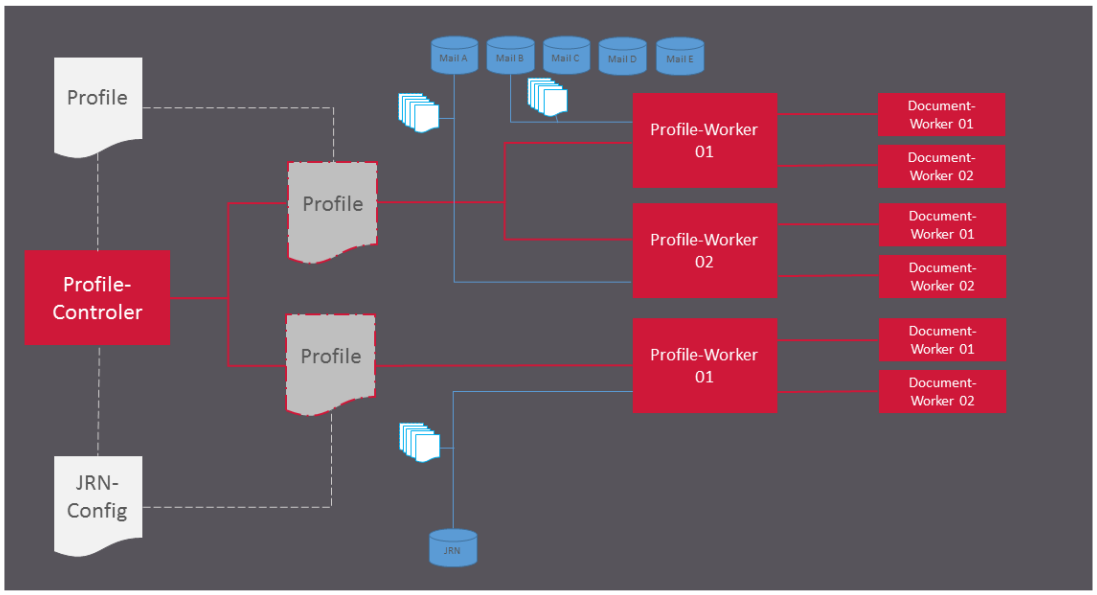
1.6.18. How can a d.ecs content crawler configuration be structured? (Example)

You can adapt the configuration of d.ecs content crawler for rule-based archiving of items and journal archiving to suit your needs.

Example

A customer would like to archive five mailboxes based on rules in a d.3 repository. The customer also wants to use journal archiving for a journal mailbox.

The following diagram shows you what the sample configuration could look like:



d.velop

The administrator creates a mapping for the properties of the e-mails to be archived and certain d.3 properties. In addition, the administrator creates a profile for rule-based archiving and a configuration for journal archiving.

A profile worker is created within d.ecs content crawler for journal archiving. Two document workers are created for the profile worker. The profile worker processes the journal mailbox.

Two profile workers are created for the profile for rule-based archiving. Two document workers are created for each profile worker. The profile workers process the five mailboxes based on the rules of the profile created.

In each cycle, 100 documents are processed which are evenly distributed to the document workers. Based on the mapping, the document workers save the documents in the d.3 repository with the corresponding properties.

1.6.19. How can I use d.ecs content crawler without a d.3one application server?

You can also use d.ecs content crawler without a d.3one application server. In this case, the items are exported to the file system. In this mode, you have access to the complete set of rules.

In order to use this mode, you still have to install the d.velop infrastructure components.

The following restrictions apply to this mode:

- Saving items in a d.3 repository is not possible.
- When saving items in a d.3 repository, it is not possible to replace attachments with links.
- When post-processing items, only the complete deletion of the item is possible.

1.6.20. How can I display and filter detailed information on jobs?

You can display information about your jobs in the d.ecs content crawler feature in the **Statistics overview** area. If you click on the number of jobs in the corresponding status, you will receive more detailed information about these jobs under **Job overview**. You can filter the jobs if necessary.

In the **Overall status** area, information such as pending jobs or jobs completed since the last restart is displayed.

In the **Profile status** area, you can display an analysis of each profile.

1.6.21. How can I define the rule-based linking of embedded attachments when I use HCL Domino?

If you are using HCL Domino and want to use the **Link attachments and embedded files** post-processing action on a process step collection, embedded files are not replaced with HTTP links in this case. This post-processing action is only supported for regular attachments.

1.6.22. How do I configure e-mail archiving for different domains?

If you configure e-mail archiving for different domains in your organization, we recommend a separate d.3one application server for processing for each domain.

1.6.23. How do I configure an external rule check?

In individual customer-specific cases, the standard rules of d.ecs content crawler may not be sufficient to check an object and mark it for further processing. In this case, you can use the external rule check. Using a simple HTTP interface, you can create individual rules to check an object in as much detail as you want.

> **Warning**
> With d.ecs content crawler, you can use an external script for rule evaluation. d.velop AG does not assume any liability or responsibility for the called script and/or the results, which may arise from the execution of the script.

The external rule check must be an application that can receive, evaluate and send HTTP calls.

The external rule check process is as follows:

1. d.ecs content crawler is already creating jobs and identifying objects. d.ecs content crawler transfers the jobs and objects to the external rule check.
2. The external rule check accepts the HTTP calls and sends back a confirmation.
3. Confirmed jobs are set to a queued status. Errors are also marked accordingly.
4. The external rule check executes the rules for the objects and reports the result back to d.ecs content crawler using the appropriate callbacks.
5. If a response is received, the corresponding job is marked and processed further with the next cycle or processing is canceled.

Communication takes place exclusively through HTTP POST calls. Data is transferred as **application/json**.

In the following section you will find further important information on the structure of the HTTP calls and the data to be transmitted for the external rule check.

POST data for the transfer of d.ecs content crawler to the external rule check

```
{
  "uri": "http://server.domain.com:2000/",
  "groupwareItemIdentifier": null,
  "jobId": null,
  "successCallback": null,
  "errorCallback": null,
  "isTest": true
}
```

- **uri**: The URI of the external rule check.
- **groupwareItemIdentifier**: The ID of the object that will be submitted to the external rule check. The IDs for HCL Domino objects and Microsoft Exchange objects are different.
- **jobId**: The ID of the job passed to the external rule check.
- **successCallback**: The URI of the callback if the check is a success. The callback must take place when the external rule check has been successfully completed.
- **errorCallback**: The URI of the callback if the check is a failure. The callback must take place if an error has occurred during the external rule check that prevents further processing. The callback should be logged in the job.
- **isTest**: If the value is **true**, the transmitted data is only used for the connection test. If the value is **false**, the data belongs to a job and is processed. Since the default value is **false**, you can omit the value.

GroupwareItemIdentifier (HCL Domino)

```
{
    "type": "DOMINO",
    "server": "dominoserver/domain",
    "database": "mail/mailuser.nsf",
    "replicaId": "C1257CB700273AAF",
    "noteId": "39CA",
    "universalId": "84A717A82EDD701DC12580ED0051F49D",
    "attachmentIdentifier": null
}
```

- **type**: Determines whether an object belongs to an HCL Domino system or a Microsoft Exchange system.
- **server**: The name of the HCL Domino server on which the database and object reside. Use the standard abbreviation **<Server>/<Domain>**.
- **database**: The path name and file name of the database in which the object is contained. The information is always relative to the data directory of the HCL Domino server.
- **replicaId**: The replica ID of the database.
- **noteId**: The note ID of the object in the database.
- **universalId**: The universal ID of the object in the database.
- **attachmentIdentifier**: If you complete this entry, an attachment within an object is identified with this entry. Since this entry is not used in d.ecs content crawler, the value is always **zero**.

GroupwareItemIdentifier (Microsoft Exchange)

```
{
    "type": "EXCHANGE",
    "exchangeStoreType": 0,
    "mailbox": "ttes@so.training",
    "parentFolderId": null,
```

```
    "entryId":
"AAMkADQyMzc0YTZmLWIyM2QtNDFkOC04MDJhLWRmZDUxMTAxMDMyZQBGAAAAAAAZMnZybIySRbt
8MxDtMGQbBwCUhE5mmOtWRbVwYoiZpwRcAAAAZwNIAAAhPwfg1f9rTqKq29vpQTqcAAATGKY5AAA
=",
    "attachmentId": -1,
    "entryIdFormat": 1,
    "isDeletedElement": false
}
```

- **type**: Determines whether an object belongs to an HCL Domino system or a Microsoft Exchange system.
- **exchangeStoreType**: The type of mailbox. A value of **0** is the user's primary mailbox. A value of **1** is the user's archive mailbox. A value of **2** is a public folder.
- **mailbox**: The mailbox that contains the object. The format is the SMTP address.
- **parentFolderId**: The ID of the folder containing the object.
- **entryId**: The ID of the object in the mailbox.
- **attachmentId**: If you complete this entry, an attachment within an object is identified with this entry. Since this entry is not used in d.ecs content crawler, the value is always **-1**.
- **entryIdFormat**: The format of the entry ID. A value of **0** is the MAPI format. A value of **1** is the EWS format. Using the Exchange Web Services, you can convert the entry IDs from the MAPI format to the EWS format.
- **isDeletedElement**: Specifies, if the object is contained in the folder **Recoverable Items**. This is usually not relevant.

POST data for the transfer of the external rule check to d.ecs content crawler

```
{
  "uri": "http://server.domain.com:2000/",
  "groupwareItemIdentifier":
"{\"type\":\"DOMINO\",\"server\":\"dominoserver/
domain\",\"database\":\"mail/
mailuser.nsf\",\"replicaId\":\"C1257CB700273AAF\",\"noteId\":\"39CA\",\"univ
ersalId\":\"84A717A82EDD701DC12580ED0051F49D\",\"attachmentIdentifier\":null
}",
  "jobId": "dfd1a0ef-bbee-477a-936f-d43342abfe75",
  "status": 4,
  "statusMessage": "Task for externally checking job dfd1a0ef-
bbee-477a-936f-d43342abfe75 successfully created"
}
```

- **uri**: The URI of the external rule check.
- **groupwareItemIdentifier**: The ID of the object that will be submitted to the external rule check. The IDs for HCL Domino objects and Microsoft Exchange objects are different.
- **jobId**: The ID of the job passed to the external rule check.
- **status**: The status that the external rule check reports back to d.ecs content crawler. The following values are allowed:
  - **0 Unknown**: You must not use this value. The value is used for internal testing.
  - **1 Continue**: This value indicates that the job can be further processed by d.ecs content crawler.
  - **2 Abort**: This value indicates that further processing of the job by d.ecs content crawler should be canceled and that the object should be reset.
  - **3 Error**: This value indicates that the external rule check failed.
  - **4 Received**: This value indicates that the external rule check has received the data from d.ecs content crawler and a callback from the external rule check is pending.
  - **999 TestSuccess**: This value is required for the connection test and indicates that a connection for the external rule check was successfully established.

- **statusMessage**: An optional message that is displayed in the overview of jobs by d.ecs content crawler. You should enter a value, especially in the event of an error.

If an object is not processed by an external rule, the object must be flagged accordingly and moved to a folder that is not monitored. During subsequent processing by d.ecs content crawler, this object will not be processed again.

In Microsoft Exchange, you must complete the designated property **DXJOB** (Type: **PT_UNICODE**) with the value **SCP**.

In HCL Domino, you must complete the **D3IMPORT** field (Type: **Text**) with the value **SCP**.

1.6.24. How do I configure an external rule check with d.ecs script?

In individual customer-specific cases, rules may be required to check an object and to mark it for further processing in addition to the standard rules of d.ecs content crawler. In this case, you can use d.ecs script. In d.ecs script, you can create your own scripts for your application.

The external rule check process is as follows:

1. d.ecs content crawler is already creating jobs and identifying objects. d.ecs content crawler transfers the jobs and objects to d.ecs script.
2. d.ecs script executes the script specified in the d.ecs content crawler set of rules. The script must result in a callback to determine whether the corresponding object should be processed.
3. If a response is received, the corresponding job is marked and processed further with the next cycle or processing is canceled.

In the following section you will find further important information on the structure of the HTTP calls and the data to be transmitted for the external rule check with d.ecs script.

The following object is transferred from d.ecs content crawler in JSON format to d.ecs script and can be used in a script for rule checking:

```
{
    "GroupwareItemIdentifier" : null,
    "JobId" : null,
    "Status" : 0,
    "StatusMessage" : null
}
```

- **GroupwareItemIdentifier**: The ID of the object that is sent to d.ecs script. The rule check must identify the object and make it available. The IDs for HCL Domino objects and Microsoft Exchange objects are different.
- **JobId**: The ID of the job that is sent to d.ecs script.
- **Status**: The status that, with further processing, determines the object. You need to set the status in the script. The following values are allowed:
  - **1 Continue**: This value indicates that the job can be further processed by d.ecs content crawler.
  - **2 Abort**: This value indicates that further processing of the job by d.ecs content crawler should be canceled and that the object should be reset.
  - **3 Error**: This value indicates that an error has occurred in the script.
  - **4 Deleted**: This value indicates that the object was deleted in the script. The job is also deleted immediately.
- **StatusMessage**: An optional message that is displayed in the job overview of d.ecs content crawler. You can set the message in the script to provide more detailed information on the status.

GroupwareItemIdentifier (HCL Domino)

```
{
    "type": "DOMINO",
```

```
    "server": "dominoserver/domain",
    "database": "mail/mailuser.nsf",
    "replicaId": "C1257CB700273AAF",
    "noteId": "39CA",
    "universalId": "84A717A82EDD701DC12580ED0051F49D",
    "attachmentIdentifier": null
}
```

- **type**: Determines whether an object belongs to an HCL Domino system or a Microsoft Exchange system.
- **server**: The name of the HCL Domino server on which the database and object reside. Use the standard abbreviation **<Server>/<Domain>**.
- **database**: The path name and file name of the database in which the object is contained. The information is always relative to the data directory of the HCL Domino server.
- **replicaId**: The replica ID of the database.
- **noteId**: The note ID of the object in the database.
- **universalId**: The universal ID of the object in the database.
- **attachmentIdentifier**: If you complete this entry, an attachment within an object is identified with this entry. Since this entry is not used in d.ecs content crawler, the value is always **zero**.

GroupwareItemIdentifier (Microsoft Exchange)

```
{
    "type": "EXCHANGE",
    "exchangeStoreType": 0,
    "mailbox": "ttes@so.training",
    "parentFolderId": null,
    "entryId":
"AAMkADQyMzc0YTZmLWIyM2QtNDFkOC04MDJhLWRmZDUxMTAxMDMyZQBGAAAAAAAZMnZybIySRbt
8MxDtMGQbBwCUhE5mmOtWRbVwYoiZpwRcAAAAZwNIAAAhPwfg1f9rTqKq29vpQTqcAAATGKY5AAA
=",
    "attachmentId": -1,
    "entryIdFormat": 1,
    "isDeletedElement": false
}
```

- **type**: Determines whether an object belongs to an HCL Domino system or a Microsoft Exchange system.
- **exchangeStoreType**: The type of mailbox. A value of **0** is the user's primary mailbox. A value of **1** is the user's archive mailbox. A value of **2** is a public folder.
- **mailbox**: The mailbox that contains the object. The format is the SMTP address.
- **parentFolderId**: The ID of the folder containing the object.
- **entryId**: The ID of the object in the mailbox.
- **attachmentId**: If you complete this entry, an attachment within an object is identified with this entry. Since this entry is not used in d.ecs content crawler, the value is always **-1**.
- **entryIdFormat**: The format of the entry ID. A value of **0** is the MAPI format. A value of **1** is the EWS format. Using the Exchange Web Services, you can convert the entry IDs from the MAPI format to the EWS format.
- **isDeletedElement**: Specifies, if the object is contained in the folder **Recoverable Items**. This is usually not relevant.

Example script (process all objects)

```
param([string]$scriptDto)

$dto = $scriptDto | ConvertFrom-Json
```

```
$dto.Status = 1

$Obj = @{ }

$Obj.ReturnCode = 0
$Obj.ScriptDto = $dto | ConvertTo-Json

return $ResultObj = (New-Object PSObject -Property $Obj)
```

If an object is not processed by an external rule, the object must be flagged accordingly and moved to a folder that is not monitored. During subsequent processing by d.ecs content crawler, this object will not be processed again.

In Microsoft Exchange, you must complete the designated property **DXJOB** (Type: **PT_UNICODE**) with the value **SCP**.

In HCL Domino, you must complete the **D3IMPORT** field (Type: **Text**) with the value **SCP**.

1.6.25. How do I open the configuration of the connection to Microsoft Exchange or HCL Domino?

You can call up the configuration of the connection to Microsoft Exchange or HCL Domino under <base address>/groupware.

1.6.26. How do I open the configuration of d.ecs content crawler if the feature is not displayed on the start page?

If the **d.ecs content crawler** feature is not available on the start page, you can call up the configuration under <base address>/groupwarecrawler.

1.6.27. How do I check for duplicates of encrypted or signed e-mails?

A check for duplicates is not performed for encrypted e-mails.

1.6.28. After linking the certificate and port, how do I check whether the apps use HTTPS when registering with the d.ecs http gateway?

If you have linked a certificate to a port to encrypt communication between the apps, you can check in the d.ecs http gateway administration how the apps register with the d.ecs http gateway app.

This is how it works

1. Open the d.ecs http gateway app administration with **https://<Computername>:4280/httpgateway/ui** or select the **d.ecs http gateway admin** entry in the Windows start menu in the d.velop program group.
2. In the **Apps** area, click the relevant app.
3. Click the app to view the app's properties.
4. Under **Destination URL**, check whether the URL begins with HTTPS.

See also: Linking the certificate and port for inter-app communication with HTTPS

1.6.29. How do I prevent encrypted e-mails from being archived?

You can exclude encrypted e-mails from automatic archiving. Add the corresponding rule to a rule collection.

> **Note**
> The attachments of an encrypted e-mail cannot be detached from the e-mail, even if you have enabled the post-processing option **Link attachments** in the process step collection. The encrypted e-mail is archived together with the attachments.

1.6.30. How do I manually move database entries to jobs if the jobs still exist after changing my database?

If you made changes to the database you were using while configuring the database server, the jobs may still exist in the database. In this case, you have to move the database entries manually.

Exit d.ecs content crawler. You can then move all tables with the prefix **GWCR_** to the new database.

See also: Configuring the database server

1.6.31. How are e-mails without jobs processed by d.ecs content crawler?

E-mails with the status **Prepared-Rule** or **Error** without an associated job are automatically reset in order to be processed again. A check is carried out beforehand to determine whether the e-mails have been moved.

1.6.32. How are e-mails processed by d.ecs content crawler when the e-mails have been moved?

If e-mails are moved during processing, the e-mails are given a new ID in Microsoft Exchange Server. d.ecs content crawler reports that the item cannot be found. The associated job is recorded as an error (error number 40).

An asynchronous process cyclically searches for jobs with the error number 40 and tries to find the respective e-mail. If the e-mail is found, the job is corrected, reset, and the item is processed. If the item is not found, the job is deleted.

1.6.33. What is the purpose of logging?

For logging, the d.3one integration writes to the central d.3 log. If an error occurs, all the necessary information is logged so that the cause of the error can be identified quickly.

By default, the integration only logs errors. If you require more information, you can adjust the logging level to your requirements.

See also: Adjusting the logging level in d.ecs content crawler

1.6.34. How do I map a d.3 repository ID to a repository ID?

If you have configured multiple repositories that have the same d.3 repository ID, you can map a d.3 repository ID to a repository ID in the Groupware app if necessary.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **E-mails** in the **Document management** category.
2. Select the entry **Management options** under **E-mail management**.
3. Go to the **Repository mapping** perspective.
4. Enter the relevant d.3 repository ID.
5. Select the repository ID that you want to map to the d.3 repository ID.
6. Click **Add** and save your entries.

1.6.35. How do I reset the counter for jobs?

You can display information about your jobs and the created profiles in the **d.ecs content crawler** feature in the **Statistics overview** area. In the context menu of a profile, you can use **Reset statistics** to reset the number of successfully processed jobs.

1.6.36. What are prioritized profiles and how do I use them?

You can assign a priority to profiles so that they are processed faster.

A prioritized profile can help you if you e.g. have many profiles for bulk archiving and few time-critical profiles for processing incoming invoices. Due to the high load, the profiles for bulk archiving are processed first. As a result, time-critical e-mails may be imported into the system too late.

With prioritized profiles, you can ensure that the respective profiles are processed alongside regular profile processing and thus time-critical emails are in the system on time.

By default, profiles are not prioritized. Prioritize only as many profiles as necessary. If all profiles are time-critical, we recommend that you do not prioritize any profile.

1.7. Additional information sources

If you want to deepen your knowledge of d.velop software, visit the d.velop academy digital learning platform at https://dvelopacademy.keelearning.de/.

Our E-learning modules let you develop a more in-depth knowledge and specialist expertise at your own speed. A huge number of E-learning modules are free for you to access without registering beforehand.

Visit our Knowledge Base on the d.velop service portal. In the Knowledge Base, you can find all our latest solutions, answers to frequently asked questions and how-to topics for specific tasks. You can find the Knowledge Base at the following address: https://kb.d-velop.de