d.velop documents in Microsoft Outlook: Administrator

Table of Contents

1. d.velop documents in Microsoft Outlook: Administrator

1.1. Basic information on the application and the manual

This documentation describes the installation, configuration and update of the d.velop documents integration in Microsoft Outlook and is intended for administrators.

To fully comprehend the information in this document, it is helpful to have in-depth knowledge of Microsoft Windows and Microsoft Outlook. You can find more information about operating d.velop documents in Microsoft Outlook in the quick guide for d.velop documents e-mail integration.

The sample repositories and archives used are based on the Microsoft Demonstration Platform and the fictional company Contoso.

1.1.1. About d.velop documents

d.3one is an innovative modern product suite with the philosophy of focusing on the end users and supporting them from wherever they would like to access ECM information, Be it Microsoft Outlook, Microsoft Office, IBM Notes, or simply the browser.

Seamless integration and simple handling

You can define a few areas for your users so that they can access the required information with a URL, without detours and without many clicks.

The innovative search supports you step by step in finding information and data using the facets. In this way, you also quickly gain an overview when you have large quantities of data. Importing documents into dossiers is accomplished quickly with drag & drop, whether it is one document or several.

An intelligent check for duplicates protects you from importing identical data multiple times. You can change document contents and properties at any time. You can also edit contents of Microsoft Office documents natively and straightforwardly in Microsoft Office.

As a team and across the organization, you communicate directly in d.3one using Tasks and Messages as well as with integrate forms, so that everyone can participate in digital business processes.

Expandability and adaptation

You can expand and adapt d.3one individually with functions, tailored to your requirements.

d.3one is an innovative tool that allows you to collaborate with the d.3ecm world.

1.1.2. 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

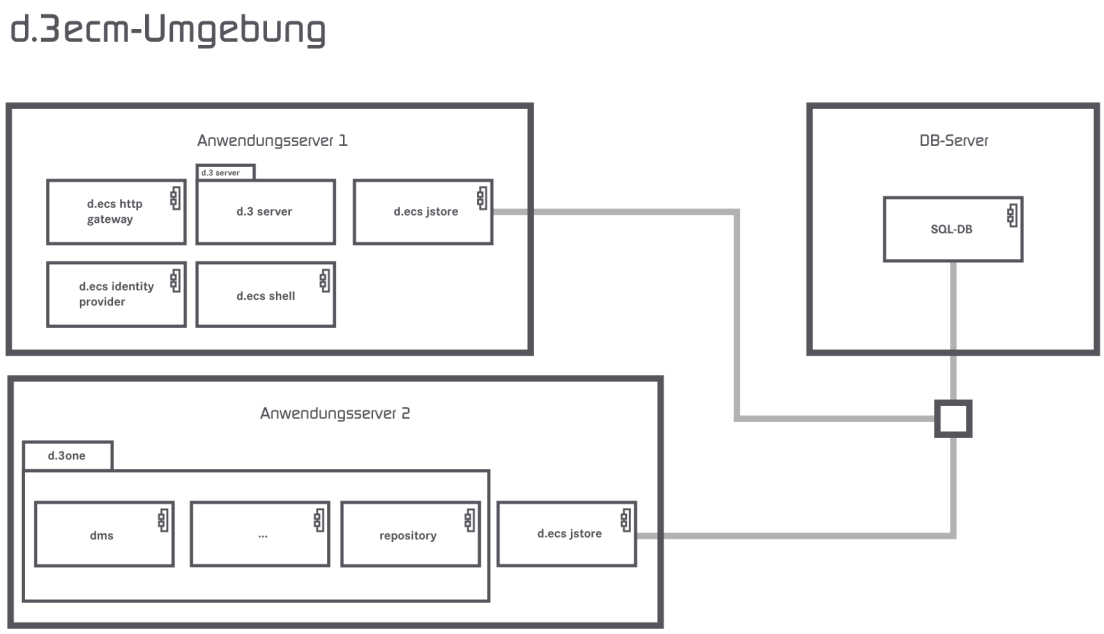
The d.ecs shell app provides the common frame for the HTML interface of each app and implements a uniform look & feel user experience so that the interface of the apps is consistent and appears to be made in one piece. The app also provides access to the native functions of the host. In this context 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.

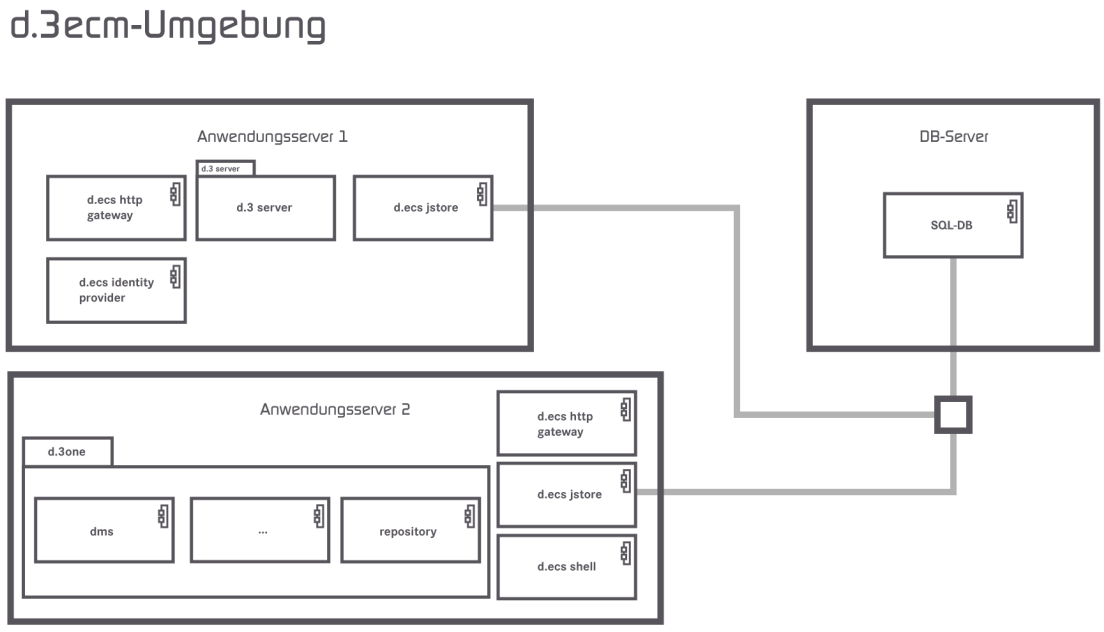
Example 1

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.

1.1.3. Useful things to know about d.velop documents licenses

With d.velop documents 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.velop documents installation; for instance, 200 users can use d.velop documents in the browser, but only 50 users can use d.velop documents in Microsoft Outlook. In contrast to a d.3ecm system environment, d.velop documents is a separate integration application.

When a user uses d.velop documents in the browser or as an integration, license information is retrieved from the d.3 repository. With each access, each d.velop documents 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.velop documents 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.velop documents 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.velop documents licensing, contact your d.velop contact person.

See also: Detailed information about named-user licenses

1.1.4. Useful things to know about the license-dependent scope of functions of d.velop documents in Microsoft Outlook

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.velop documents 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

See also: Assigning full licenses

1.1.5. Useful things to know about storing and displaying e-mails in d.velop documents

Viewing, displaying and restoring e-mails and different file formats between applications usually involves visual "losses" and possibly even lost information. To prevent display problems or the potential loss of information caused by switching applications (e.g. from the e-mail application to the d.3ecm system environment), the standards and standardized policies of d.velop AG are applied.

The processing that occurs while saving e-mails in HCL Notes or Microsoft Outlook is to a great extent provider-independent, because the e-mails are stored in a standardized XML format in the d.3 repository. Thanks to the XML format, information from e-mails and provider-specific information is available at all times, which means that the information can be restored in HCL Notes or Microsoft Outlook at any time. However, if the provider redesigns the proprietary templates or forms (e.g. **Memo**) for e-mails, an e-mail may be displayed differently after the restore than it was when it was stored in the d.3 repository.

When processing e-mails, the IETF specifications, which have been defined in the Requests for Comments in RFC 2045, RFC 2046, RFC 2047, RFC 2048 and RFC 2049 and are a continuation of RFC 822, are used by default.

Since RFC 2048 has been classified by the Internet Engineering Task Force (IETF) as Best Practice, RFC 2048 is the applicable policy for the processing of e-mails. In particular, RFC 2048 is the best method for displaying e-mails that are not displayed with HCL Notes or Microsoft Outlook (e.g. the result list in the d.velop documents integration for HCL Notes).

The display of e-mails or converted documents in another long-term format (e.g. PDF or TIFF) may differ visually from the display in HCL Notes or Microsoft Outlook. In terms of content, all the information is displayed as per RFC 822 and RFC 2048.

You can find more information about this topic on the IETF website, for example.

You can use the list below to track which types of e-mails are processed by d.velop documents and how the e-mails are stored.

Plain text

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed without restrictions.

HTML

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed without restrictions.

MIME

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed without restrictions.

S/MIME-based encryption (internal)

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed without restrictions.

S/MIME-based encryption (external)

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed without restrictions.

PGP-based encryption (internal)

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed without restrictions.

PGP-based encryption (external)

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed without restrictions.

S/MIME-based signature (internal)

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed with restrictions.
- Comment: e-mails stored with HCL Notes integration require more storage space in the repository store than the original file.

S/MIME-based signature (external)

- Microsoft Exchange: processed without restrictions.
- HCL Domino: processed with restrictions.
- Comment: e-mails stored with HCL Notes integration require more storage space in the repository store than the original file.

HCL Notes-based signature (internal)

- Microsoft Exchange: cannot be processed. Storing is denied or not possible.
- HCL Domino: processed without restrictions.
- Comment: restoring can only be done in HCL Domino. Display in the d.3ecm system environment is possible only with conditions. The saved file is larger than the original file.

HCL Notes-based signature (external)

- Microsoft Exchange: cannot be processed. Storing is denied or not possible.
- HCL Domino: processed without restrictions.
- Comment: restoring can only be done in HCL Domino. Display in the d.3ecm system environment is possible only with conditions. The saved file is larger than the original file.

E-mails with DRM protection

- Microsoft Exchange: processed without restrictions.
- HCL Domino: cannot be processed.
- Comment: If you store e-mails with DRM protection, these e-mails may become unreadable.

If e-mails are encrypted and signed, it is sometimes only possible to show that the e-mails are encrypted, because the signature is also encrypted.

You have the option of storing an e-mail you want to save with encryption or decrypting the open e-mail before saving it.

You cannot store attachments from encrypted or signed e-mails. However, you can store the whole e-mail.

1.2. Installation and uninstallation

This topic provides you with information about installing, updating and uninstalling d.velop documents in Microsoft Outlook and the components required.

1.2.1. System requirements

The system requirements for d.velop documents apply to d.velop documents in Microsoft Outlook. Further information on d.velop documents is available in the d.velop service portal: https://service-portal.d-velop.de/de/products/dvelop-documents

Supplementary information

- The Microsoft Outlook add-in requires Microsoft Edge WebView2 Runtime.
- The authentication method is provided by d.ecs identity provider. You must configure the LDAP support for each d.3 repository. Otherwise, a login is not possible. In d.ecs identity provider, enter the provider **LDAP**.
- 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 continue to be displayed in the folders. Full-text indexing occurs if the Microsoft Outlook category is specified instead of the archive message class. The following options are available to you to ensure that 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 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).
- Microsoft Outlook is not supported in combination with IBM Mail Support for Microsoft Outlook (IMSMO).

Correct display of d.velop documents in Microsoft Outlook

The screen requires a minimum bit depth of 16 bits.

Pop-up blockers

If you are using a restrictive pop-up blocker, the integration may not open workflows correctly. We recommend allowing pop-ups for the d.velop documents application server and d.3 presentation server.

1.2.2. Preparing for installation

In this topic, you can find information about all the tasks involved in preparing for the installation. You can then begin with the installation.

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.velop documents.

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.velop documents 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 -User <impersonationAssignmentUser>
```

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.velop documents 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.

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
```

1.2.3. Installing d.velop documents in Microsoft Outlook

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.

1.2.4. Installing the add-in for d.velop documents in Microsoft Outlook

There are two ways to install the add-in for d.velop documents in Microsoft Outlook on all your client PCs:

- Installing the add-in locally
- Installing the add-in using Active Directory software distribution

1.2.5. Local installation of the add-in for d.velop documents in Microsoft Outlook

You can install the MSI package for the add-in using d.velop software manager. By default, the setup file is located in the folder <installation path>\outlookaddin.

Any user can locally install the setup for the add-in on a client PC.

The following requirements must be fulfilled to locally install the add-in:

- The client PC users must be logged in as administrators.
- The system requirements for the client PC must be fulfilled.
- Microsoft Outlook has to be closed for the installation.

The setup wizard guides you through the installation step by step. Check each step and choose the appropriate options for your requirements. You must agree to the license terms to install the add-in.

You can access the add-in once it is installed.

You can also install the MSI packages without a user interface. If you want to change the installation path, add the parameter **APPLICATIONFOLDER** to the target directory. Otherwise, the default path is used. You can also add the parameter **SERVERADDRESS** to the base address of the d.ecs http gateway server.

Example: **d.3one_microsoft_outlook_integration-1.8.0.0.msi APPLICATIONFOLDER="C:\<Installation directory> SERVERADDRESS="https://<Base address>" /q**

1.2.6. Distributing the add-in for d.velop documents in Microsoft Outlook using Active Directory software distribution

Once you have completed the installation of d.velop documents in Microsoft Outlook, you can automatically distribute the add-in within your organization using AD software distribution.

This is how it works

1. Create a new folder in the domain controller, e.g. **<Installation path>\Software distribution**.
2. Copy the setup file for d.velop documents in Microsoft Outlook (**d.3one_microsoft_outlook_integration*.msi**) and add the file to the new folder.
3. Share the folder.
4. Give everyone read access to the folder.

You then have to create a security group with a group policy and create the new MSI package with the setup for the d.velop documents in Microsoft Outlook add-in.

If you want to install an MSI package with AD software distribution with an English-language server operating system, you must enable the switch **Ignore language when deploying this package** under **Advanced Deployment Options**.

Defining settings for d.velop documents using Active Directory software distribution

If you have created a group policy for AD software distribution for the add-in for a group of users, you can create a registry item for using d.velop documents.

The registry item is read out from **HKEY_CURRENT_USER**. If a value is unavailable, the item from **HKEY_LOCAL_MACHINE** is used.

Let's assume you want to create a registry item for using d.velop documents with a latency of 30 seconds.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Settings > Windows Settings > Registry** to select the registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Under **Action**, select the entry **Replace**.
6. Under **Hive**, select the entry **HKEY_CURRENT_USER** or **HKEY_LOCAL_MACHINE**.
7. Under **Key Path**, specify the applicable path for the operating system:
   - For 32-bit client operating systems, enter the path **HKLM\Software\d.velop\dvelop.Client.Outlook.Integration**.
   - For 64-bit client operating systems, enter the path **HKLM\Software\WOW6432Node\d.velop\dvelop.Client.Outlook.Integration**.
   - For mixed operation of 32-bit and 64-bit clients, enter the two paths above.
8. Under **Value name**, specify the entry **ServerAddressMailSystem**.
9. Under **Value type**, select **REG_SZ**.
10. Under **Value data**, specify the entry **https://<d.velop documents server>|30|30** and save your entries.

Creating a security group for AD software distribution for the add-in

To distribute the MSI package software, you must create a new security group containing the users for Active Directory software distribution.

This is how it works

1. Open **Control Panel > Administrative Tools > Active Directory Users and Computers**.
2. Select the domain.
3. Choose **Action > New > Group** to create a new group.
4. Enter a name for the security group under **Group name**.
5. Under **Group scope**, select the option **Global**.
6. Under **Group type**, select the option **Security**. Save your entries.

Creating a group policy for AD software distribution for the add-in

If you have created a security group for the MSI package setup, you must define a group policy for the group in the domain controller.

This is how it works

1. Open **Control Panel > Administrative Tools > Group Policy Management**.
2. Select the domain.

3. Select **Action > Create a GPO in this domain, and link it here**.
4. Enter a name for the group policy.
5. Select the created policy.
6. Enter the created group under **Security Filtering** and save your entries.

Creating a software package for AD software distribution for the add-in

If you have created a security group and a group policy for a group of users, you must create a new software package for the MSI package setup in the Group Policy Management Editor.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Policies > Software Settings > Software Installation** to select the software installation.
4. Click **Action > New > Package** to add the setup. It must be possible to reference all the packages as UNC paths.
5. Select the package and open the package properties.
6. Go to the **Software Deployment** tab.
7. Under **Deployment type**, select the option **Assigned**.
8. Under **Deployment options**, select the options **Uninstall this application when it falls out of the scope of management** and **Install this application at logon**.
9. Under **Installation user interface options**, select **Basic**.
10. Log into the client PC again.

Enabling synchronization with the Offline Store using the AD software distribution for the add-in

If you have created a group policy for a group of users for AD software distribution for the add-in, you can use a registry item to enable the synchronization of items to be stored locally with the Offline Store. You can use the Offline Store to define a local path for the items, for example, or exclude folders from the synchronization.

To enable synchronization, create an appropriate registry item.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Settings > Windows Settings > Registry** to select the registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Under **Action**, select the entry **Replace**.
6. Under **Tree**, select the entry **HKEY_LOCAL_MACHINE**.
7. Under **Key Path**, specify the entry **Software\d.velop\dvelop.Client.Outlook.Integration**.
8. Under **Name**, enter **OFFLINESTOREENABLED**.
9. Under **Value type**, enter **REG_DWORD 1/0**. Save your entries.

Synchronization is now enabled and you can set additional configurations using registry items if necessary.

See also:

- Detailed information about the Offline Store
- Configuring the authentication for the Offline Store

Excluding Microsoft Outlook folders from synchronization with the Offline Store using the AD software distribution for the add-in

If you have created a group policy for a group of users for AD software distribution for the add-in and synchronization with the Offline Store is enabled, you can use a registry item to define Microsoft Outlook folders that you want to exclude from the synchronization with the Offline Store.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Settings > Windows Settings > Registry** to select the registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Under **Action**, select the entry **Replace**.
6. Under **Hive**, select the entry **HKEY_LOCAL_MACHINE**.
7. Under **Key Path**, specify the entry **Software\d.velop\dvelop.Client.Outlook.Integration**.
8. Under **Name**, enter **OFFLINESTOREEXCLUDEFOLDERS**.
9. Under **Value type**, select **REG_MULTI_SZ**.
10. Under **Value data**, enter the Microsoft Outlook folders to be excluded. Save your entries.

See also: Detailed information about the Offline Store

Defining the local path for storage with the Offline Store using the AD software distribution for the add-in

If you have created a group policy for a group of users for AD software distribution for the add-in, you can use a registry item to define a local path for the items to be stored for the Offline Store.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Settings > Windows Settings > Registry** to select the registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Under **Action**, select the entry **Replace**.
6. Under **Hive**, select the entry **HKEY_LOCAL_MACHINE**.
7. Under **Key Path**, specify the entry **Software\d.velop\dvelop.Client.Outlook.Integration**.
8. Under **Name**, enter **OFFLINESTOREPATH**.
9. Under **Value type**, select **REG_SZ**.
10. Under **Value data**, specify the local directory and save your entries.

See also: Detailed information about the Offline Store

Defining the maximum age of items for local storage with the Offline Store using the AD software distribution for the add-in

If you have created a group policy for AD software distribution for the add-in for a group of users, you can use a registry item to define the maximum age for items. Items that exceed this age are no longer stored locally by the Offline Store.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Settings > Windows Settings > Registry** to select the registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Under **Action**, select the entry **Replace**.

6. Under **Hive**, select the entry **HKEY_LOCAL_MACHINE**.
7. Under **Key Path**, specify the entry **Software\d.velop\dvelop.Client.Outlook.Integration**.
8. Under **Value name**, specify the entry **OFFLINESTOREMAXAGE**.
9. Under **Value type**, select **REG_DWORD**.
10. Under **Value data**, specify the maximum age for the items to be stored in days and save your entries.

See also: Detailed information about the Offline Store

Defining a maximum memory space limit for the Offline Store using the AD software distribution for the add-in

If you have created a group policy for AD software distribution for the add-in for a group of users, you can use a registry item to define a maximum storage limit for items on the local disk. When the limit is reached, synchronization stops.

> **Note**
> Specify the maximum storage limit in bytes. The value is displayed in MB on the configuration interface.

To define a storage limit, you create a registry item.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Settings > Windows Settings > Registry** to select the registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Under **Action**, select the entry **Replace**.
6. Under **Hive**, select the entry **HKEY_LOCAL_MACHINE**.
7. Under **Key Path**, specify the entry **Software\d.velop\dvelop.Client.Outlook.Integration**.
8. Under **Value name**, specify the entry **OFFLINESTOREMINFREEDISCSPACE**.
9. Under **Value type**, select **REG_QWORD**.
10. Under **Value data**, specify the local directory and save your entries.

See also: Detailed information about the Offline Store

1.2.7. Distributing the add-in for Microsoft Outlook in the web browser (OWA) or for the new Outlook

If you also want to use the add-in for Microsoft Outlook in the web browser (OWA) or the new Outlook for Windows, it is necessary for you to set up a connection for the add-in in d.ecs http gateway. You can then distribute the add-in to your users for Exchange on-premises in Microsoft Exchange admin center or for Exchange Online in Microsoft 365 admin center.

This is how it works

1. Open the d.ecs http gateway configuration screen and select **Configuration**.
2. Make sure that the **Content-Security-Policy** header line is available. If the header line isn't available yet, click on **Add header** and enter **Content-Security-Policy** as the name.
3. Enter one of the following values for the header line:
   - If you are using Microsoft 365: **frame-ancestors 'self' outlook.office.com;** or **frame-ancestors 'self' outlook.office365.com;**
   - If you are using Microsoft Exchange on-premises: **frame-ancestors 'self' <Name of domain>;**
4. Save your changes and restart d.ecs http gateway.
5. Distribute the add-in:
   - If you are using Microsoft Exchange on-premises: Open the Microsoft Exchange admin center and navigate to **Organization > add-ins**. Upload the manifest file provided. You can find the

manifest file under <Installation path>\groupware\bin\wwwroot\outlookaddin\manifest\OutlookAddin.xml.
- If you are using Microsoft Exchange Online: Open the Microsoft 365 admin center and navigate to **Settings > Integrated apps**. Upload the manifest file provided. You can find the manifest files under <Installation path>\groupware\bin\wwwroot\outlookaddin\manifest\OutlookAddin-M365.xml.

> **Note**
> On earlier versions, it was necessary to create the header line **X-Frame-Options** with the value **ALLOW-FROM**. It isn't necessary to create this header line any more.

You can find an overview of the supported Outlook client versions here.

Once you've distributed the add-in, your users can use d.velop documents in Outlook in their web browser or in the new Outlook for Windows.

1.2.8. Installing the DGIX viewer to display e-mails

In the integration, data and information from the e-mail application are stored in a special format for long-term archiving. A DGIX file is a type of ZIP file that contains an XML file with the useful data and a folder for any available file attachments.

You require a special view to display files in DGIX format. There are two variants for the viewer: DGI2EML and DGI2HTML. You can use these tools to display DGIX files in the e-mail application.

A setup program for installing the DGIX viewer is provided in the d.velop documents setup program. There are two ways to install the DGIX viewer on all your client PCs:

- Installing the DGIX viewer locally
- Installing the DGIX viewer using Active Directory software distribution

See also:

- Detailed information about how DGI2EML works
- Defining call parameters for DGI2EML
- Detailed information about how DGI2HTML works
- Defining call parameters for DGI2HTML

1.2.9. Installing the DGIX viewer locally

You can install the MSI package for DGIX Viewer using d.velop software manager. By default, the setup file is located in the folders <installation path>\dgi2eml and <installation path>\dgi2html. The steps for installing the DGIX viewers DGI2HTML and DGI2EML are the same. Since both DGIX viewers are registered for the file extension ***.dgix**, the most recent DGIX viewer installed always opens. Choose one of the two viewers.

To ensure that your users can locally install the setup for the DGIX viewer on the client PCs, the following requirements must be fulfilled:

- The client PC users must be logged in as administrators.
- The system requirements for the client PC must be fulfilled.

The setup wizard guides you through the installation step by step. Check each step and choose the appropriate options for your requirements.

You can use the DGIX viewer immediately following the installation.

You can also install the MSI packages without a user interface. If you want to change the installation path, add the parameter **APPLICATIONFOLDER** to the target directory. Otherwise, the default path is used.

Example: **DGI2HTMLSetup_1.8.0.0.msi APPLICATIONFOLDER="C:\<Installation directory>" /q**

1.2.10. Installing the DGIX viewer using Active Directory software distribution

Once you complete the installation in d.velop software manager, the setup files for installing the DGIX viewer locally are created automatically. The default location for the setup files is in the folders <installation path>\dgi2eml and <installation path>\dgi2html. The steps for installing the DGIX viewers DGI2HTML and DGI2EML are the same. Since both DGIX viewers are registered for the file extension ***.dgix**, the most recent DGIX viewer installed always opens. Choose one of the two viewers.

Let's assume you want to install the DGIX viewer using AD software distribution.

This is how it works

1. Create a new folder in the domain controller (e.g. **<installation path>\Software distribution**.
2. Copy the setup file for the DGIX viewer and add the file to the new folder.
3. Share the folder.
4. Grant read access to the folder to every user.

You then have to create a security group with a group policy and create the new MSI package with the DGIX viewer setup.

If you want to install an MSI package with AD software distribution with an English-language server operating system, you must enable the switch **Ignore language when deploying this package** under **Advanced Deployment Options**.

Creating a group policy for AD software distribution for the DGIX viewer

If you have created a security group for the MSI package setup, you must define a group policy for the group in the domain controller.

This is how it works

1. Open **Control Panel > Administrative Tools > Group Policy Management**.
2. Select the domain.
3. Select **Action > Create a GPO in this domain, and link it here**.
4. Enter a name for the group policy.
5. Select the created policy.
6. Enter the created group under **Security Filtering** and save your entries.

You then have to create the new MSI package with the DGIX viewer setup.

Creating a security group for AD software distribution for the DGIX viewer

To distribute the MSI package software, you must create a new security group containing the users for Active Directory software distribution.

This is how it works

1. Open **Control Panel > Administrative Tools > Active Directory Users and Computers**.
2. Select the domain.
3. Choose **Action > New > Group** to create a new group.
4. Enter a name for the security group under **Group name**.
5. Under **Group scope**, select the option **Global**.
6. Under **Group type**, select the option **Security**. Save your entries.

You then have to create a group policy and the new MSI package with the DGIX viewer setup.

Creating a software package for AD software distribution for the DGIX viewer

If you have created a security group and a group policy for a group of users, you must create a new software package for the MSI package setup in the Group Policy Management Editor.

This is how it works

1. Select the created group policy in Group Policy Management.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Policies > Software Settings > Software Installation** to select the software installation.
4. Click **Action > New > Package** to add the setup. It must be possible to reference all the packages as UNC paths.
5. Select the package and open the package properties.
6. Go to the **Software Deployment** tab.
7. Under **Deployment type**, select the option **Assigned**.
8. Under **Deployment options**, select the options **Uninstall this application when it falls out of the scope of management** and **Install this application at logon**.
9. Under **Installation user interface options**, select **Basic**.
10. Log into the client PC again.

If you have installed the DGIX viewer using AD software distribution, you can find the DGIX viewer in the Control Panel under **Programs and Features** after restarting.

If the entry is not displayed, enter the command **gpupdate /force** in the command prompt. Then restart the client PCs.

1.2.11. Installing updates for d.velop documents in Microsoft Outlook

When you install an update using d.velop software manager, select the option **Update installed products** in d.velop software manager. The configuration of the earlier version is retained.

1.2.12. Installing updates for version 1.18.0 when using HTTPS

You can specify that communication between the Groupware app and d.ecs http gateway is secured by HTTPS. If you perform an update from version 1.18.0 to a higher version, the configuration is not fully transferred automatically in this case.

You therefore have to adapt the configuration manually to ensure that the Groupware app works correctly.

To do so, open the file **conf/appsettings.json** in the installation directory. The settings for the port and protocol have been transferred from the previous installation automatically. Example:

```
{
  "port lower bound": "4205",
  "port upper bound": "4205",
  "protocol": "https"
}
```

Add the certificate to be used. Example:

```
{
  "port lower bound": "4205",
  "port upper bound": "4205",
  "protocol": "https",
  "Kestrel": {
    "Certificates": {
```

```
      "Default": {
        "Subject": "d3one1.dev.local",
        "Store": "My",
        "Location": "LocalMachine"
      }
    }
  }
}
```

1.2.13. Uninstalling d.velop documents in Microsoft Outlook

Before you uninstall d.velop documents on the server, you should first locally uninstall the d.velop documents integration on the client PCs. This ensures that d.velop documents is not called by a client PC even though the integration was already uninstalled on the server.

Once you have uninstalled all the components, you can start the uninstall program to uninstall d.velop documents.

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.

1.2.14. Uninstalling d.velop documents in Microsoft Outlook with group policies

To uninstall d.velop documents in Microsoft Outlook on the server, you must uninstall the integration locally on the client PCs using the group policies.

Let's assume you want to uninstall d.velop documents in Microsoft Outlook using group policies.

This is how it works

1. Open **Control Panel > Administrative Tools > Group Policy Management** and select the relevant group policy.
2. Click **Action > Edit** to open the Group Policy Management Editor.
3. Click **User configuration > Policies > Software Settings** and select the entry **Software installation**.
4. In the editor area, select the entry **d.3one**.
5. Right-click to open the context menu and choose **All Tasks > Remove**.
6. In the **Remove Software** dialog box, select the option **Immediately uninstall the software from users and computers**.

You can then uninstall d.velop documents in Microsoft Outlook on the server.

1.2.15. Rolling back an installation of d.velop documents in Microsoft Outlook

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.

1.2.16. Enabling the default port for d.velop documents in Microsoft Outlook

- The port for the integration in d.velop documents is determined dynamically by default. However, you can also define a port.

1.3. Configuring d.velop documents in Microsoft Outlook

This topic provides you with information about configuring d.velop documents in Microsoft Outlook and the components required.

1.3.1. Preparing for the authentication of the Groupware app with OAuth 2.0 and EWS 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.velop documents 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.

1.3.2. 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. This method of authentication is recommended by Microsoft.

> **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.velop documents result 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.velop documents 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**
- **Granting administrator consent**: Select **Grant admin consent for <tenant name>** for the relevant API permissions.
- **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.

1.3.3. 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.

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

1.3.5. 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

1.3.6. 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

1.3.7. Defining call parameters for DGI2EML

You can use the tool DGI2EML to specify various call parameters. You can also specify the parameters when calling the program. The order is irrelevant. You specify the path to the DGIX file directly without parameters.

The following parameters are available to you:

-silent

- Meaning: You use the parameter to specify that all the user interfaces are suppressed and only the conversion of the DGIX file is performed.
- Value: **true** or **false**
- Default value: **false**
- Example: **-silent=true**

-temp

- Meaning: You use the parameter to define the directory in which the conversion is performed.
- Value: **"<Path to the directory>"**
- Default value: Temporary directory of Windows
- Example: **-temp="C:\test"**

Sample call: **DGI2EML.exe "C:\E-Mail.dgix" -silent=true -temp="C:\temp"**

See also:

- Installing the DGIX viewer
- Detailed information about how DGI2EML works

1.3.8. Defining call parameters for DGI2HTML

You can use the tool DGI2HTML to specify various call parameters. You can also specify the parameters when calling the program. The order is irrelevant. You specify the path to the DGIX file directly without parameters.

The following parameters are available to you:

-silent

- Meaning: You use the parameter to specify that all the user interfaces are suppressed and only the conversion of the DGIX file is performed.
- Value: **true** or **false**
- Default value: **false**
- Example: **-silent=true**

-temp

- Meaning: You use the parameter to define the directory in which the conversion is performed.
- Value: **"<Path to the directory>"**
- Default value: Temporary directory of Windows
- Example: **-temp="C:\test"**

-lang

- Meaning: You use this value to specify the language for the conversion.
- Value: **"<Language>"**
- Default value: Language of the operating system
- Example: **-lang="en-US"**

-renditionMode

- Meaning: You use this value to define a special page for the rendering (for example, to ensure that no links are created for attachments).
- Value: **true** or **false**
- Default value: **false**
- Example: **-renditionMode=true**

-renderBccRecipient

- Meaning: You use this parameter to specify whether you want to display the BCC recipients.
- Value: **true** or **false**
- Default value: **false**
- Example: **-renderBccRecipient=true**

Sample call: **DGI2HTML.exe "C:\E-Mail.dgix" -silent=true -temp="C:\temp" -lang="en-US" -renditionMode=true**

See also:

- Installing the DGIX viewer
- Detailed information about how DGI2HTML works

1.3.9. Configuring the Internet Explorer browser settings for viewing e-mail attachments

To ensure that your users can also view e-mail attachments stored in the d.3 repository separately in their e-mail application, you must configure settings in Internet Explorer. Internet Explorer is only supported by the feed for d.3 8.1.0. The Current feed no longer supports Internet Explorer.

The changes in Internet Explorer are required because the attachments are no longer included in the e-mail, but are now linked. It may not be possible to open the relevant e-mail with Internet Explorer because the files cannot be saved.

We recommend distributing the settings using the group policies in the domain.

To ensure that your users can view attachments in Internet Explorer, you must allow encrypted pages to be saved in Internet Explorer.

This is how it works

1. In Internet Explorer, open **Tools > Internet Options**.
2. Go to the **Advanced** tab.
3. Go to **Security** and deactivate the option **Do not save encrypted pages to disk**.

1.3.10. Preparing a hybrid environment with Microsoft Exchange

In a hybrid environment, some of your organization's mailboxes are on an on-premises Microsoft Exchange server. Other mailboxes are in Microsoft Exchange Online. This is always the case if you migrate all your organization's mailboxes to Microsoft Exchange Online (Office 365).

You can find more information about hybrid operation in the Exchange documentation for hybrid deployments on the Microsoft Docs website.

You must perform the following preparatory tasks to ensure that access to the mailboxes works properly:

- Set up the autodiscover function in Microsoft Exchange.
- Make sure that the on-premise Active Directory is synchronized with the Azure Active Directory or with Azure AD Connect. You can find more information about Azure AD Connect on the Microsoft Docs website by searching for "What is hybrid identity with Azure Active Directory?".
- Make sure that EWS impersonation users with the same password can log in on the on-premises Microsoft Exchange server and Microsoft Exchange Online (password synchronization).

If you have configured the Groupware app for the hybrid environment, the appropriate Microsoft Exchange server (on-premises or Microsoft Exchange Online) is dynamically determined for each mailbox. Since the determination can take several seconds, the assignment of the mailbox to Microsoft Exchange Server is stored for twelve hours and then redetermined. If you restart the Groupware app, all the stored mappings are deleted immediately.

You can also simply configure multiple Microsoft Exchange connections for the same domain. The connection for a mailbox is then automatically determined from the existing mailboxes. This also gives you the advantage of being able to mix the EWS API and Microsoft Graph API. For instance, you can connect the Microsoft Exchange server (on-premises) using the EWS API and basic authentication. On the other hand, you can connect Microsoft Exchange Online using the Microsoft Graph API and OAuth 2.0.

1.3.11. 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.

For Microsoft Exchange, you can only specify named properties of the type **Public Strings**, **Common** and **Internet Headers** as custom fields. It must be possible to reference the named properties using a name.

See also:

- Detailed information about sources
- Example of the use of sources
- Detailed information about categories
- Detailed information about mappings

1.3.12. Creating your own categories for mappings

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
- Example of the use of categories
- Detailed information about sources
- Detailed information about mappings

1.3.13. Creating a "Store in" function

You can use a **Store in** function to help your users with their daily work. Define a d.3 repository and a d.3 category in which your users can store items using the **Store in** context menu. When your users save items, the repository and category are already selected.

Let's assume you want to create a new **Store in** function.

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 **'Store in' functions** under **Context menus and functions**.
3. Select the context action **Create new 'Store in' function**.
4. Enter a name for the function and add a description.
5. Select the repository that you want to be automatically selected for your users.
6. Select a source to be used to save the items.
7. Select the category that you want to be automatically selected for your users.
8. Enter a display name for the context menu for the required language.
9. If necessary, select a post-processing action that your users will see by default when saving.
10. If necessary, define the users or user groups that you want to see the context menu. If you want to provide the **Store in** function for all users, leave the field empty.
11. Save your entries.

To ensure that your users can use the **Store in** function you created, you must restart the user e-mail applications.

1.3.14. Creating a "Go to" function

You can use a **Go to** function to help your users with their daily work. Your users can then open e-mails easily in a different application (e.g. an ERP system).

You can create a **Go to** function for any third-party provider application that can be accessed with a URL.

When you create the function, you can also define whether the other application is displayed in the inbox on the sidebar or opened in a browser window, for example. Make sure that the relevant resource can be integrated. If your resource prevents integration, select the option for displaying it in a separate browser window.

Let's assume you want to create a new **Go to** function.

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 **'Go to' functions** under **Context menus and functions**.
3. Then choose the context action **Create new 'Go to' function**.
4. Enter a name for the regular expression and add a description if necessary.
5. Under **Menu entry**, enter a display name for the context menu. If necessary, add the placeholder **<DOCVALUE>** to the display name. The placeholder is filled with the result of the regular expression. If you want to use the result of the regular search, omit the placeholder.
6. Under **Group for authorized users**, you can define specific groups that you want to see the context menu, if necessary. If you want to provide the **Go to** function for all users, leave the field empty.
7. Enter a regular expression for the search in the repository and, if necessary, click the pen icon to test the regular expression. For example, if you use the regular expression **D[0-9]{8}**, a document ID such as **D00000191** is found and the result of the search is provided in the placeholder **<DOCVALUE>**.
8. Choose the elements for which the regular expression is to be used.

9. Under **Open URL**, enter the URL that you want to open for the result of the regular expression. If necessary, add the placeholder **<DOCVALUE>** to the URL. Only one individual result from the regular expression is ever used. You can also use a path to an application in the form of a URL.
10. Choose whether you want to display the **Go to** function in the sidebar or in a separate browser window.
11. Save your entries.

To ensure that your users can use the **Go to** function you created, you must restart their e-mail applications.

See also:

- Example of use for opening e-mail content in web applications
- Example of use for searching for a document in d.3 smart explorer

1.3.15. Creating a "Move to folder" function

You can centrally define a folder to which items are directly moved when storing them in the d.3 repository.

Let's assume you have created the sub-folder **Order confirmations** for your users, so that order confirmations can be collected centrally in the mailbox. You want to enable your users to move e-mails directly to the folder when storing them in the d.3 repository.

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, enable the option for moving items to specific folders.
4. Enter **<file path>\Order confirmations** under **Folder path** and save your entries.

You can also exclude folders using macros, so that the folder name is not language-specific.

1.3.16. Creating a "Search for" function

You can use a **Search for** function to help your users with their daily work. Your users can then quickly and easily search for a search term within the context of an e-mail, for example to find the relevant customer file directly in the d.3 repository.

You can also enable the fully automated context-sensitive search. When your users select an e-mail, the search starts automatically after a short time (3 seconds). The automatic search is performed only if a result is found for the regular expression. The search is not performed if a storage dialog is displayed.

Define a regular expression (RegEx) for the context-sensitive search. If the regular expression results in a search term with more than 500 characters, only the first 500 characters are used for the search. You can truncate the view in the context menu to fewer than 500 characters by adding three periods (...) to the menu entry.

Let's assume you want to create a new **Search for** function.

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 **'Search for' functions** under **Context menus and functions**.
3. Then choose the context action **Create new 'Search for' function**.
4. Enter a name for the regular expression and add a description if necessary.
5. Select the repository to be searched.

6. Select the d.3 categories to which the search is to be restricted. If you want to search in all categories, leave the field empty.
7. Under **Group for authorized users**, you can define specific groups that you want to see the context menu, if necessary. If you want to provide the **Search for** function for all users, leave the field empty.
8. Enter a regular expression for the search in the repository and, if necessary, click the pen icon to test the regular expression. For example, if you use the regular expression **D[0-9]{8}**, a document ID such as **D00000191** is found and the result of the search is provided in the placeholder **<DOCVALUE>**.
9. Choose the e-mail elements for which the regular expression is to be used.
10. If necessary, activate the **Automatic search** option.
11. Under **Menu entry**, enter a display name for the context menu. If necessary, add the placeholder **<DOCVALUE>** to the menu entry. The placeholder is filled with the result of the regular expression. If you want to use the result of the regular search, omit the placeholder.
12. Save your entries.

To ensure that your users can use the **Search for** function you created, you must restart the user e-mail applications.

See also:

- Example of use for searching for domains
- Example of use for searching in sender information

1.3.17. Changing the file format from DGIX to EML for archiving with Microsoft Exchange

For Microsoft Exchange, you can choose to archive an item as a DGIX file or EML file. When installing the Groupware app, archiving is automatically enabled in EML format.

Let's assume that you want to use the EML format for archiving.

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 **Processing settings** perspective.
4. Select the option **Storing format: EML instead of DGIX**.

If you are also using d.ecs content crawler, you then restart d.ecs content crawler.

1.3.18. Storing items when Microsoft Exchange services are not configured

If the Microsoft Exchange services are not activated, you can still store e-mails and attachments with d.velop documents in Microsoft Outlook. In this scenario, the client sends the items to be processed directly to the Groupware app.

If this option is activated, encrypted e-mails can also now be stored decrypted from the Outlook client.

If you want to use d.ecs content crawler, you must activate and configure Microsoft Exchange services under all circumstances.

The following restrictions apply if you are working without Microsoft Exchange services:

- The **Flag stored e-mails for all recipients** function is not available to you.
- If a category is defined during post-processing, only the text can be defined. The color cannot be specified.
- Groups in the recipient lists are not resolved (mappings and authorization control).
- The mappings for the mailbox user ID (**OBJECTGUID**) and mailbox SAM account name (**SAM_ACCOUNT_NAME**) are not available to you.

1.3.19. Things to know about checking for duplicates

The check for duplicates helps you avoid unnecessary copies of items in the d.3 repository.

The function is available to you for journaling and rules-based storage of items in d.ecs content crawler. If, for example, an e-mail is imported once through journaling and once based on rules, the Groupware app identifies the e-mail as a duplicate and prevents a duplicate from being saved.

The check also works when manually storing items. If the check is activated, the Groupware app passes the hash to the DMS app. The d.3 server then checks whether there is already a stored item with the same hash. It does not matter how the item is stored. However, the check for duplicates is performed only when storing items with the status Release.

1.4. Tips and tricks

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

1.4.1. Configuring the settings for accessing the d.velop documents in Microsoft Outlook administration with single sign-on

If you want to call the administration in the integration using single sign-on (SSO), you must configure the appropriate settings in the internet options of your operating system (individually or with group policies). You must add the d.velop documents base address in the internet options for the **Local intranet** security zone.

This is how it works

1. Open the Windows control panel and select **Internet Options**.
2. Go to **Security** and select **Local intranet**.
3. Click **Sites > Advanced**.
4. Under **Add this website to the zone**, add the d.velop documents base address and choose **Add** to confirm.

You can choose **Custom level** and go to **User Authentication** to define whether the login data is sent from the client PC to the server (SSO) or whether the user is asked for his or her user name and password. **Automatic log in only in Intranet zone** is enabled by default, which means that single sign-on should be enabled.

1.4.2. Configuring the authentication for the Offline Store

If you or your users want to use the Offline Store in Microsoft Outlook, you must ensure that basic authentication is enabled for Microsoft Exchange Server. The Windows user account that is currently logged in is used for authentication. Due to this restriction, the Windows user account must also have the mailbox.

To use the Offline Store, you can only use the EWS interface in combination with basic authentication.

If you are using Microsoft Office 365, you must synchronize the on-premises Active Directory with the Azure Active Directory so that the users are identified by both directory services.

See also: Detailed information about the Offline Store

1.4.3. Assigning enhanced named user licenses for user groups

With the aid of user groups, you can specify which users can use all the functions of an integration and which users are to receive only a basic license.

Let's assume you want to make all the functions of an integration available to a group of users.

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 under **Group for users with advanced license**, select the relevant user group.
4. Save your entries.

See also: Detailed information about the license-dependent scope of functions of the integration

1.4.4. 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.

1.4.5. 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.

The check for duplicates is also dependent on the document status in the d.3 administration. Therefore, check the values for **TEST_FOR_DUPLICATES**, **IGNORE_DUPS_IN_B_P**, **IGNORE_DUPS_IN_A** and **IGNORE_DUPS_IN_OTHER_DOCTYPES**.

You can enable the function for d.velop documents 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.

1.4.6. Configuring post-processing of e-mails

You can specify, for example, that an icon is displayed for your users in the Microsoft Outlook mailbox once an item is successfully archived. You can also specify that the item is assigned to a specific category and color in the mailbox following archiving.

You can display an icon after archiving unencrypted and unsigned e-mails and a category for encrypted and signed e-mails. Alternatively, you can specify that a category is assigned for all e-mails (including unencrypted and unsigned e-mails) if necessary. An icon is not displayed in this case.

Let's assume you want an icon to be displayed for your users after archiving an item. In addition, you want to assign signed or encrypted e-mails to a **Purchasing** category with the color yellow in the mailbox.

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 **Processing settings** perspective.
4. Select the **Set icon** option.
5. Enable **Set category for signed or encrypted e-mails**.
6. For the category, go to **Text** and enter **Purchasing**.
7. Under **Color**, choose **Yellow**. Save your entries.

If a user has not used categories in the Microsoft Outlook mailbox before, a configuration is automatically created for categories in the mailbox. It therefore may no longer be possible for users to use the default categories. To apply the changes, the Groupware app and d.ecs content crawler must be restarted.

1.4.7. Adding additional mailboxes for storing items from other mailboxes

You can store items from other users' mailboxes that have been added to Microsoft Outlook in the d.3 repository.

This is the only way to archive items from other mailboxes with the integration.a

This is how it works

1. Open the Windows Control Panel and select the entry **Mail** for Microsoft Outlook.
2. Choose **Email Accounts**.
3. Choose **Change** to edit your primary Microsoft Exchange account.
4. Choose **More Settings**.
5. Go to the **Advanced** tab and enter the additional mailboxes from Microsoft Exchange Server.
6. Click **Add** and save your entries.

1.4.8. 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.velop documents 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.

1.4.9. Enabling the function for flagging saved e-mails for all recipients

You can specify that e-mails that your users save in the d.3 repository are flagged as "stored" for all the recipients.

This function can only be used to flag e-mails for all recipients. Attachments cannot be flagged with this function.

Furthermore, you cannot combine this function with the **Send and store** function. If you save e-mails with the **Send and store** function, the e-mail is not flagged as "stored" for all the recipients.

You cannot flag e-mails in public folders.

> **Note**
> The function massively increases the load on the server. We recommend that you use this function only with caution.

Let's assume you want to enable the flagging function.

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 **Processing settings** perspective.
4. Enable **Flag stored e-mails for all recipients (Microsoft Exchange)** and save your entries.

1.4.10. Adjusting the level of logging in the Groupware app

To identify the causes of errors, you can adjust the level of logging in the Groupware app to your requirements.

Let's assume you want to specify that all messages are logged in the central d.3 log.

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 **Logging** perspective.
4. Under **Log level**, select the entry **All**. Save your entries.

See also: Detailed information about logging

1.4.11. Adjusting the level of logging in Microsoft Outlook

To identify the causes of errors, you can adjust the level of logging in Microsoft Outlook to your requirements.

Let's assume you want to specify that all the messages in the log file **d3oneOutlook.log** of the add-in are to be displayed in order to identify the causes of errors.

This is how it works

1. On the Microsoft Outlook menu ribbon, choose **File** and then **Options**.
2. In the dialog box, click **Add-ins > Add-in Options**.
3. Under **Log level**, select the entry **All** and confirm your settings.
4. Restart Microsoft Outlook.

See also: Detailed information about logging

1.4.12. Adjusting the settings for the cache

The cache is used to optimize the storage of items in the d.3 repository and to restore and display e-mails, for example. You can adjust the cache settings to fit your needs. You can specify a cache directory, a maximum cache size and the cache time.

Let's assume you want to increase the maximum cache size to 1500 MB and define the cache time as one day.

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 **Cache settings** perspective.
4. Under **Maximum cache size (MB)**, enter the value **1500**.
5. Under **Cache time in minutes**, enter the value **1440**.

1.4.13. Displaying BCC recipients in the e-mail preview

You can specify that BCC recipients are also displayed in the e-mail preview.

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, enable the option **Show BCC recipients in e-mail preview**.
4. Save your entries.

The DGIX files and the BCC recipient are then displayed in the e-mail preview.

1.4.14. Disabling d.velop documents in Microsoft Outlook UI components

You can specify that the integration starts without UI components. Disabling UI components is useful, for example, if your users only use functions that are still available when there is no internet connection (e.g. the Offline Store).

To make only the offline functions available to your users, you must create a suitable registry item.

This is how it works

1. Select **Control Panel > Administrative Tools > Group Policy Management**.
2. Select the corresponding group policy and click **Action > Edit** to open the group policy editor.
3. Click **User configuration > Policies > Settings > Windows Settings > Registry** to select a registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Select **HKEY_CURRENT_USER / HKEY_LOCAL_MACHINE** under **Tree**.
6. Select **Software\d.velop\dvelop.Client.Outlook.Integration** under **Key Path**.
7. Under **Name**, enter the value **DisableUI**.
8. Under **Value type**, select **REG_DWORD**.
9. Under **Value data**, enter **1** to hide the UI.

1.4.15. Enabling the function for storing all the e-mails in a conversation

You can make the function **Store all e-mails of the conversation** available to your users in the Microsoft Outlook menu ribbon. This function lets your users store multiple e-mails that are part of a conversation in one step in the d.3 repository. You must enable this function to make it available.

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 **Processing settings** perspective.
4. Under **Client-side settings**, enable the option **Enable storing of all e-mails in a conversation**.

Your users can then select the function on the **Home** tab in the Microsoft Outlook menu ribbon.

1.4.16. Temporarily restoring e-mails and attachments using a service user

You can define a service user for temporarily restoring items that have been stored with the integration or d.ecs content crawler in the d.3 repository. In this case, the Windows user that is logged into the client PC is not used for authentication; instead, the service user is.

> **Warning**
> We recommend not using this function continuously. All the permission structures in your d.velop documents system environment are bypassed. All users with access to the HTTP link for the item can access the object. By changing the link, every document can be accessed without a permission check.

Let's assume you have to restore items that have been stored in the repository using the integration.

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 **Restore** perspective.
4. Enable the **Restore via service user** option.
5. Enter the name, domain and password of the service user.

1.4.17. Preventing documents with S/MIME encryption from being stored

If necessary, you can prevent your users from storing documents with S/MIME encryption in the d.3 repository.

This is how it works

1. Go to **Configuration > Document management > E-mails > E-mail management**.
2. Select **Microsoft Exchange**.

3. Go to **Post-processing settings**.
4. Enable **Do not store S/MIME encrypted documents (client-side storing only)**.
5. Save your setting.

You have successfully prevented documents with S/MIME encryption from being stored. When saving documents with S/MIME encryption, your users receive a warning message stating that saving is not allowed and the save operation will be cancelled.

Only senders and recipients can read documents with S/MIME encryption in plain text. Microsoft Outlook (desktop version) is required to do so. If you do not prevent saving and you archive documents with S/MIME encryption, these documents may become unreadable. Furthermore, a rendition cannot be created in this case.

1.4.18. Preventing documents with DRM protection from being stored

If necessary, you can prevent your users from storing documents with DRM protection in the d.3 repository.

This is how it works

1. Go to **Configuration > Document management > E-mails > E-mail management**.
2. Select **Microsoft Exchange**.
3. Go to **Post-processing settings**.
4. Enable **Do not store DRM protected documents (client-side storing only)**.
5. Save your setting.

You have successfully prevented documents with DRM protection from being stored. When saving documents with DRM protection, your users receive a warning message stating that saving is not allowed and the save operation will be cancelled.

Documents with DRM protection are provided with digital permissions (e.g. do not forward, do not print, etc.) by an external Microsoft service. Only senders and recipients can read documents with DRM protection in plain text. Microsoft Outlook (desktop version) is required to do so. If you do not prevent saving and you archive documents with DRM protection, these documents may become unreadable. Furthermore, a rendition cannot be created in this case.

1.4.19. 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.

Let's assume you want to define the port and use **http** for the 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.json**.
3. Define the port by entering the same value for both the upper and lower bounds.
4. For **protocol**, enter the value **http**. Example:

```
{
  "port lower bound": "4100",
  "port upper bound": "5000",
  "protocol": "http"
}
```

5. Restart the app.

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**.

If you use **https**, enter the certificate in the file **appsettings.json**. To use a certificate from the Windows certificate store, you can define the following information in the file, for example:

```
{
  "port lower bound": 4100,
  "port upper bound": 4100,
  "protocol": "https",
  "Kestrel": {
    "Certificates": {
      "Default": {
        "Subject": "d3one1.dev.local",
        "Store": "My",
        "Location": "LocalMachine"
      }
    }
  }
}
```

You can use the table below to see how the entries in the Windows certificate store relate to the entries in the file **appsettings.json** and the corresponding PowerShell scripts:

Windows certificate store	"appsettings.json"	PowerShell
Local Computer	**LocalMachine**	**get-childitem -path Cert:\LocalMachine**
Current User	**CurrentUser**	**get-childitem -path Cert:\CurrentUser**
Personal	**My**	**get-childitem -path Cert:\LocalMachine\My**
Trusted Root Certification Authority	**Root**	**get-childitem -path Cert:\LocalMachine\Root**
Subject	**Subject**	Not available

1.4.20. Using Microsoft Edge in d.velop documents in Microsoft Outlook

To use the Microsoft Edge browser in the integration, you have to download a Microsoft Edge version from the Microsoft Insider Channel or the Microsoft Edge Runtime.

The official build of Microsoft Edge is not supported.

To use the Microsoft Edge browser in the integration, you need Microsoft Windows 10, Microsoft Outlook 2019 or Microsoft Outlook for Microsoft 365 at minimum.

We recommend installing Microsoft Edge Runtime.

> **Note**
> All versions in the Microsoft Insider Channels are pre-release versions.

For more information about the Microsoft Insider Channels and Microsoft Edge Runtime, see the Microsoft website.

1.4.21. Using Internet Explorer instead of Microsoft Edge in d.velop documents in Microsoft Outlook

If you have Microsoft Edge Runtime installed (WebView2), Microsoft Edge Runtime is used as the integrated browser instead of Internet Explorer. If you still want to use Internet Explorer, enable the settings accordingly in a registry item. Internet Explorer is only supported by the feed for d.3 8.1.0. The Current feed no longer supports Internet Explorer.

Let's assume you want to disable Microsoft Edge Runtime with a registry item in order to use Internet Explorer.

This is how it works

1. Select **Control Panel > Administrative Tools > Group Policy Management**.
2. Select the corresponding group policy and click **Action > Edit** to open the group policy editor.
3. Click **User configuration > Policies > Settings > Windows Settings > Registry** to select a registry.
4. Click **Action > New > Registry Item** to create a new registry item.
5. Select **HKEY_CURRENT_USER / HKEY_LOCAL_MACHINE** under **Tree**.
6. Select **Software\d.velop\dvelop.Client.Outlook.Integration** under **Key Path**.
7. Enter **UseEdge** under **Name**.
8. Under **Value type**, select **REG_DWORD**.
9. Enter **0** under **Value Data** and save your entries.

Microsoft Internet Explorer is now permanently enabled in d.velop documents in Microsoft Outlook.

1.4.22. How can I store an encrypted or signed e-mail?

You have the option of storing an e-mail you want to save with encryption or decrypting the open e-mail before saving it.

You cannot store attachments from encrypted or signed e-mails. However, you can store the whole e-mail.

1.5. Frequently asked questions

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

1.5.1. Why does it take so long to store an e-mail using the "Send and store" function in cache mode?

If you have activated cache mode in Microsoft Outlook and then use the **Send and store** function, it can take up to 30 seconds after sending your e-mail for the form for storing it to be displayed.

1.5.2. Why can't I store delivery reports or read receipts using the "Store all e-mails of the conversation" function?

You can use the **Store all e-mails of the conversation** function to store multiple e-mails from a conversation in the d.3 repository. Although delivery reports and read receipts are part of a conversation, these items do not belong to the **IPM.Note** message class and therefore cannot be stored in the repository.

1.5.3. Why are items that I already deleted still available in the Offline Store?

The Offline Store performs a daily check of whether there are still corresponding stubs (e-mails reduced to header information) for items in the Offline Store in the mailbox. If no stubs are available for items, the items are deleted from the Offline Store. As a result, items that were already synchronized and then deleted in Microsoft Outlook may not be removed from the Offline Store until 24 hours later.

1.5.4. Why are some DGIX files or embedded images not displayed in an e-mail?

If you restore and display DGIX files in Microsoft Outlook, the Microsoft Outlook settings are used to display them. If a group policy is used to specify that attachments cannot be larger than 50 MB, any attachment larger than 50 MB is not displayed in the e-mail. Embedded images may be displayed with a delay in the e-mail if automatic reloading of images is not permitted.

> **Note**
> In the latest version of Microsoft Outlook 2013, there is a bug in the display of EML files. Due to this bug, no CC recipients are displayed for EML files.

1.5.5. What is the Offline Store?

You or your users can use the Offline Store to store archived e-mails locally.

If you are often away on business, for example, it is useful to store archived e-mails locally on your mobile device. You can then access your e-mails even if you do not have an internet connection.

If you want to save archived e-mails locally, you can also save only items from within a specific time period. The date on which the items are received or sent is used to calculate the period.

You or your users can also customize the Offline Store by reserving memory space on the local disk for the Offline Store.

You can find more information about configuring the Offline Store in the quick guide for d.velop documents e-mail integrations.

See also:

- Enabling synchronization with the Offline Store using AD software distribution
- Excluding Microsoft Outlook folders from synchronization with the Offline Store using AD software distribution
- Defining the local path for storage with the Offline Store using AD software distribution
- Defining the maximum age for storage with the Offline Store using AD software distribution
- Defining a maximum memory space limit for the Offline Store using AD software distribution
- Configuring the authentication for the Offline Store

1.5.6. 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.velop documents integration is started, named user licences are assigned for the user and the d.velop documents integration. For example, if a user logs into d.velop documents 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.velop documents licenses

1.5.7. What can I do if the display of DGIX files as HTML pages does not work properly?

An incorrect data extension causes problems displaying DGIX files. If an image has the file extension for bitmaps (***.bmp**), for example, but is actually a JPEG file (***.jpg**), the image is not displayed.

The DGIX viewer (DGI2HTML) uses Internet Explorer embedded on the client PC to display the DGIX file as an HTML page. Internet Explorer (embedded) displays an error when displaying local images because the images have the incorrect file extension.

In this case, you can display DGIX files using the DGI2EML viewer instead of the DGI2HTML viewer.

1.5.8. What can I do if I cannot download an e-mail stored as a DGIX file directly using the add-in in Internet Explorer?

If you have used the add-in in Internet Explorer to store an e-mail in DGIX format, it may not be possible to download the e-mail directly using the add-in in the web browser.

In this case, you can refresh the page with **F5** or use a different web browser (e.g. Microsoft Edge or Google Chrome).

1.5.9. What are the differences between the web add-in and the COM add-in for Microsoft Outlook?

Note the following differences between the web add-in and the COM add-in:

- The COM add-in only works in Microsoft Outlook on Windows desktops.
- If users replace e-mail attachments with HTTP links when they save an e-mail, it is not possible to restore the attachments in the web add-in by double-clicking.
- If users use Apple MacOS, no Archive icon is displayed in the web add-in.

An overview of the features of d.velop documents in Microsoft Outlook in the various add-ins is available here: https://serviceportal.d-velop.de/de/news/funktionsueberblick-d3one-in-microsoft-outlook-fuer-das-neue-outlook

1.5.10. 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

1.5.11. 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 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

1.5.12. 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

1.5.13. Which properties can I use when creating sources as custom fields for Microsoft Exchange?

For Microsoft Exchange, you can only specify named properties of the type **Public Strings**, **Common** and **Internet Headers** as custom fields. It must be possible to reference the named properties using a name.

1.5.14. Which field names are mapped to which source properties?

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.

Unresolved recipient names (To, Cc)

- HCL Notes: Calculated value
- Microsoft Outlook: Calculated value
- Meaning: List of all unresolved recipient names (To, Cc)

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

Recipients' SMTP addresses from message header

- Microsoft Outlook: Calculated value
- Meaning: List of the recipients as e-mail addresses, taken from the message header

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

Recipients' SMTP addresses (Cc) from message header

- Microsoft Outlook: Calculated value
- Meaning: List of copy recipients as e-mail addresses, taken from the message header

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

Senders' SMTP address from message header

- Microsoft Outlook: Calculated value
- Meaning: SMTP address of the sender, extracted from the message header

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.

Category

- Microsoft Outlook: **PidNameKeywords**
- Meaning: Name of the Outlook category

For attachments:

File name

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

File index

- HCL Notes: Calculated value
- Microsoft Outlook: **PR_ATTACH_NUM**
- Meaning: Index 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.

1.5.15. Which languages can I use as call parameters for the DGI2HTML viewer?

If you want to specify a call parameter for the DGI2HTML viewer, the following languages with the following values are available to you:

- English: **en-US**
- German: **de-DE**
- Czech: **cs-CZ**
- Danish: **da-DK**
- Spanish: **es-ES**
- French: **fr-FR**
- Croatian: **hr-HR**
- Italian: **it-IT**
- Dutch: **nl-NL**
- Polish: **pl-PL**
- Serbian: **sr-Cyrl**

1.5.16. Are e-mails flagged as "stored" for all recipients if the Groupware service is closed?

If the Groupware app service is closed while flagging e-mails as "stored" for all the recipients or if the system is restarted, the system does not automatically start flagging these e-mails again.

1.5.17. How do I enable the post-processing options?

When storing items in the d.3 repository, your users can use the post-processing options to replace attachments in the mailbox with HTTP links, for example, or to select the folder to which the items are to be moved.

The post-processing options are enabled by default. If an option is not automatically enabled, you can enable the option later.

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. Select **Enable post-processing**.
4. Save your entries.

1.5.18. How do I change the settings for the "Send and store" function?

You can use the **Send and store** function to help your users with their daily work. The function lets your users send e-mails and attachments while storing them in a suitable category in the d.3 repository at the same time.

The function is available only for the primary mailbox in Microsoft Outlook. The sent items must be stored in the **Sent Items** folder in Microsoft Outlook.

The function is enabled by default. Where necessary, they can change the source and category for the function or use the context actions to create new sources and categories directly.

Let's assume you want to change the source and category for the **Send and store** function.

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 **'Send and store' functions** under **Context menus and functions**.
3. Select a source.
4. Select a category and save your entries.

To ensure that your users can use the modified **Send and store** function, you must restart their e-mail applications.

1.5.19. How do I permit the storage of e-mails that have been archived using d.link for microsoft exchange?

You can specify that your users can store e-mails that have been archived using d.link 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 **Microsoft Exchange** under **E-mail management**.
3. Go to the **d.link for microsoft exchange settings** perspective.
4. Enable the option **Enable client-side storing of e-mails archived using d.link for microsoft exchange**.

For example, your users can then use the relevant context menus or drag & drop to store the e-mails again.

1.5.20. How do I create a "Go to" function for opening e-mail content in web applications? (Example of use)

You can use a **Go to** function to map different scenarios (for example, for opening the content of e-mails in third-party provider applications) using URLs.

Example

You want to enable your users to open e-mail content for customer numbers (e.g. **KN00451**) in an internal CRM application.

To make this function available to your users, you can create a **Go to** function. Under **Open URL**, enter a URL template for the internal CRM application (e.g. **https://crm.company.com/customer/**) as the URL.

When the specified URL is subsequently accessed, **https://crm.company.com/KN00451** is then retrieved as the result of the search and opened as a URL in your users' web browser.

See also:

- Creating **Go to** functions
- Creating **Go to** functions for searching for documents in d.3 smart explorer (example of use)

1.5.21. How do I create a "Go to" function for searching for a document in d.3 smart explorer? (Example of use)

You can use a **Go to** function to map different scenarios (for example, for searching for a document in d.3 smart explorer) using URLs. In this case, you must ensure that d.3 smart explorer is installed on your users' client PCs.

Example

You want to enable your users to search for specific document IDs (e.g. **D00000191**) in d.3 smart explorer. The result of the search is stored in the placeholder **<DOCVALUE>**.

To make this function available to your users, you can create a **Go to** function. Under **Open URL**, enter **d3://d3explorer/idlist=<DOCVALUE>** as the URL.

When the specified URL is subsequently called, **d3://d3explorer/idlist=D00000191** is then retrieved as the result of the search. This URL is used to start d.3 smart explorer on your users' client PCs and perform a search for the document ID.

See also:

- Creating **Go to** functions
- Creating **Go to** functions for opening e-mail content in web applications (example of use)

1.5.22. How do I create a "Search for" function for searching a domain? (Example of use)

With a **Search for** function, you can use a regular expression to specify that a domain is read for the search.

Example

To read the relevant domain, enter the following regular expression while creating a **Search for** function: **@[a-z.-]+\.[a-z]{2,}**

When the search is then performed, the regular expression finds the domain.

See also:

- Creating **Search for** functions
- Creating **Search for** functions for sender information (example of use)

1.5.23. How do I create a "Search for" function for searching in sender information? (Example of use)

With a **Search for** function, you can use a regular expression to specify that the search term is read out from the sender information.

Example

You want to specify that the SMTP address is also read during the search.

To extend the search to the SMTP address, enter the following regular expression while creating a **Search for** function: **[a-z0-9\-_]?[a-z0-9.\-_]+[a-z0-9\-_]?@[a-z.-]+\.[a-z]{2,}**

When the search is then performed, the regular expression finds the relevant SMTP address.

See also:

- Creating **Search for** functions

- Creating **Search for** functions for domains (example of use)

1.5.24. How does DGI2EML work?

You can use the DGI2EML tool to display DGIX files in your e-mail application. The EML format is a standardized format for displaying e-mails and is supported by many e-mail applications, such as Microsoft Outlook and HCL Notes.

The tool creates a temporary EML file from the DGIX file. The temporary EML file is used for the display in the e-mail application. When the DGIX file is opened, the e-mail application starts and displays the e-mail as usual. Your users can edit, send or forward e-mails as usual.

Aspects to note

- Encrypted or signed e-mails may be displayed differently from their originals.
- If you respond to a temporarily restored e-mail or forward this e-mail, this information is not written to the archived document.

See also:

- Installing the DGIX viewer
- Defining call parameters for DGI2EML

1.5.25. How does DGI2HTML work?

You can use the DGI2HTML tool installed on the client side to display DGIX files on your system. The tool enables a view that is independent of d.velop documents.

The tool temporarily creates an HTML file based on the DGIX file. The temporary HTML file is used for displaying in DGI2HTML.

Displaying signed e-mails

You can identify a signed e-mail by the signature symbol  . The signature is not checked.

Displaying encrypted e-mails

You can identify an encrypted e-mail by the lock symbol  . The text body of an encrypted e-mail cannot be displayed with the DGI2HTML viewer.

Aspects to note

- Although you can use the DGI2HTML viewer to display stored e-mails and attachments, you cannot edit or forward the e-mails.
- Encrypted or signed e-mails may be displayed differently from their originals.

See also:

- Installing the DGIX viewer
- Defining call parameters for DGI2HTML

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

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

In the integration in Microsoft Outlook, a check for duplicates is not performed for signed e-mails.

1.5.27. How can I use categories to create mappings for specific customer scenarios? (Example of use)

You can define your own categories to create specific mappings for your organization.

Example

An employee receives a variety of different e-mails. One part of these e-mails is correspondence for purchasing. The other part of these e-mails is correspondence for sales. The categories (document types) **CorrPurchase** and **CorrSales** are available in the d.3 repository.

The **Department** property must be defined based on the e-mail type (purchasing or sales). However, only the employee can decide which type of e-mail it is. Nevertheless, when storing e-mails, the employee should only have to change the storage form in a small number of exceptional cases. In the ideal scenario, the employee stores the e-mails directly in the repository so that the relevant processes can be started within the organization.

The administrator for the organization defines two new categories in the Groupware app configuration: **Purchasing correspondence** and **Sales correspondence**.

The administrator uses one of the default sources as the source.

The administrator creates two new **Store in** functions in the Groupware app configuration. For one function, the administrator selects the newly created category for the correspondence for purchasing. For the other function, the administrator selects the newly created category for the correspondence for sales.

Two new context menus for storing items in the d.3 repository are then available to the employee. With the aid of the context menus, the employee can directly decide whether an e-mail is to be stored for Sales or Purchasing.

See also:

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

1.5.28. How can I use sources to create mappings for specific customer scenarios? (Example of use)

You can define your own sources to create specific mappings for your organization.

Example

An employee receives a variety of different e-mails. One part of these e-mails is correspondence for purchasing. The other part of these e-mails is correspondence for sales. However, only the category (document type) **Correspondence** is available in the d.3 repository.

The **Department** property must be defined based on the e-mail type (purchasing or sales). However, only the employee can decide which type of e-mail it is. Nevertheless, when storing e-mails, the employee should only have to change the storage form in a small number of exceptional cases. In the ideal scenario, the employee stores the e-mails directly in the repository so that the relevant processes can be started within the organization.

The administrator for the organization defines two new sources in the Groupware app configuration: **Purchasing correspondence** and **Sales correspondence**.

The administrator defines two new mappings for the two sources. Most of the source and target properties in the mapping table are the same. For the **Department** property, the administrator provides the value **PUR** in the mapping for the **Purchasing correspondence** source. In the mapping for the **Sales correspondence** source, the administrator enters the value **SALES** for the **Department** property.

The administrator creates two new **Store in** functions. For one function, the administrator selects the newly created **Purchasing correspondence** source. For the other function, the administrator selects the newly created **Sales correspondence** source.

Two new context menus for storing e-mails in the d.3 repository are then available to the employee. With the aid of the context menus, the employee can directly decide whether an e-mail is to be stored for Sales or Purchasing.

See also:

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

1.5.29. How can I temporarily restore stubs for d.link for microsoft exchange and d.link for microsoft outlook?

You can temporarily restore stubs for d.link for microsoft exchange or d.link for microsoft outlook without executing a d.link for microsoft exchange service or installing a d.3 integrating application. The Groupware app acts as the HTTP server for d.link for microsoft exchange and resolves the HTTP links. Stubs generated with d.link for microsoft outlook are resolved without further settings.

If the HTTP links were not generated using a DNS alias, you may have to install the Groupware app on the same client PC where the d.link for microsoft exchange service was running. In this case, you must also install d.ecs jstore and include d.ecs jstore in a cluster.

> **Note**
> If you enable temporary restoring, you must uninstall d.link for microsoft exchange, d.link for microsoft outlook and the OnTheFly form.

Let's assume you want to restore stubs for d.link for microsoft exchange and d.link for microsoft outlook.

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. In the **d.link for microsoft exchange settings** perspective, enable the option **Resolve d.link for microsoft exchange stubs via HTTP**.
4. Under **Port of web server**, enter the port with which the d.link for microsoft exchange web server originally ran.
5. Enter the user name, domain and password for the domain user that has the right to export the relevant e-mails.
6. If necessary, enable the option for the hash value check if "Secure Hash Value Generation" was enabled in d.link for microsoft exchange.
7. Restart the **d.ecs groupware** service.

The d.3 repository is then referenced in the stubs and HTTP links using the d.3 repository ID. To resolve the stubs, the Groupware app automatically determines the repository ID from the d.3 repository ID. If you have configured multiple repositories with the same d.3 repository ID, create a fixed mapping for a d.3 repository ID and a repository ID.

See also: Mapping a d.3 repository ID to a repository ID

1.5.30. 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.

1.5.31. What is the purpose of logging?

For logging, the d.velop documents 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 level of logging in the Groupware app
- Adjusting the level of logging in Microsoft Outlook

1.5.32. Can users access an e-mail if importing copies is prevented by the check for duplicates?

The check of duplicates prevents importing of copies of the same e-mail. That is why duplicates are located only in the mailboxes of the people who sent or received the e-mail in this case.

If you follow our recommendation and define the permissions on e-mails via d.3 system fields, all users have access to their own e-mails. Storing the e-mail once is sufficient. Users can still find the e-mail.

1.5.33. Which properties of an e-mail are analyzed for duplicate checking?

When an email is stored, the Groupware app calculates a hash from certain parts of the e-mail. The hash contains the following criteria:

- Message ID
- E-mail address of the person who sent the e-mail
- Subject
- Body of the e-mail
- E-mail addresses of all people who received the e-mail
- Display name of the attachments
- Hash of the attachments

For signed and encrypted e-mails, the following additional criteria are processed:

- Hash of the original EML file (**content.eml**)
- Flag indicating that it is a signed e-mail

For meetings and appointments, the following criteria are also processed:

- Start time
- End time

- Location

1.6. Additional information sources and imprint

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/

Find the central imprint at https://www.d-velop.com/imprint.