

d.velop documents in Microsoft Outlook: Administrator

Table of Contents

1. d.velop documents in Microsoft Outlook (Cloud) 4
1.1. Basic information on the application and the manual 4
1.1.1. About d.3one 4
1.1.2. Useful things to know about storing and displaying e-mails in d.3one 4
1.2. Installation and uninstallation 6
1.2.1. Preparing for installation 6
1.2.2. Installing the add-in for d.3one in Microsoft Outlook 7
1.2.3. Locally installing the add-in for d.velop documents in Microsoft Outlook 8
1.2.4. Distributing the add-in for d.velop documents in Microsoft Outlook using Active Directory software distribution 8
1.2.5. Distributing the add-in for Microsoft Outlook in the web browser (OWA) 12
1.3. Configuring d.velop documents in Microsoft Outlook 12
1.3.1. Preparing for the authentication of the Groupware app with OAuth 2.0 and EWS in Azure Active Directory 12
1.3.2. Preparing for the authentication of the Groupware app with OAuth 2.0 and Microsoft Graph in Azure Active Directory 13
1.3.3. Specifying the registry information from Azure Active Directory for authentication with OAuth 2.0 14
1.3.4. Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft EWS 14
1.3.5. Setting up multiple connections to the Microsoft Exchange server with Exchange Online and Microsoft Graph 15
1.3.6. Creating your own sources for mappings 16
1.3.7. Creating your own categories for mappings 17
1.3.8. Creating a "Store in" function 17
1.3.9. Creating a "Go to" function 18
1.3.10. Creating a "Move to folder" function 19
1.3.11. Creating a "Search for" function 19
1.3.12. Changing the file format from DGIX to EML for archiving with Microsoft Exchange 20
1.3.13. Storing items when Microsoft Exchange services are not configured 20
1.4. Tips and tricks 20
1.4.1. Configuring the settings for accessing the d.velop documents in Microsoft Outlook administration with single sign-on 20
1.4.2. Configuring the authentication for the Offline Store 21
1.4.3. Preparing the check for duplicates 21
1.4.4. Enabling the check for duplicates 21
1.4.5. Configuring post-processing of e-mails 22
1.4.6. Adding additional mailboxes for storing items from other mailboxes 22
1.4.7. Adjusting the level of logging in Microsoft Outlook 23
1.4.8. Displaying BCC recipients in the e-mail preview 23
1.4.9. Disabling d.velop documents in Microsoft Outlook UI components 23
1.4.10. Enabling the function for storing all the e-mails in a conversation 23
1.4.11. Preventing documents with S/MIME encryption from being stored 24
1.5. Preventing documents with DRM protection from being stored 24
1.6. Frequently asked questions 24
1.6.1. Why does it take so long to store an e-mail using the "Send and store" function in cache mode? 24
1.6.2. Why can't I store delivery reports or read receipts using the "Store all e-mails of the conversation" function? 25
1.6.3. Why are items that I already deleted still available in the Offline Store? 25
1.6.4. Why are some DGIX files or embedded images not displayed in an e-mail? 25
1.6.5. What is the Offline Store? 25

1.6.6. What are the differences between the web add-in and the COM add-in for Microsoft Outlook? 25
1.6.7. What are categories? 26
1.6.8. What are sources? 26
1.6.9. What are mappings? 27
1.6.10. Which properties can I use when creating sources as custom fields for Microsoft Exchange? 27
1.6.11. Which field names are mapped to which source properties? 27
1.6.12. How do I enable the post-processing options? 31
1.6.13. How do I change the settings for the "Send and store" function? 31
1.6.14. How do I create a "Go to" function for opening e-mail content in web applications? (Example of use) 32
1.6.15. How do I create a "Go to" function for searching for a document in d.3 smart explorer? (Example of use) 32
1.6.16. How do I create a "Search for" function for searching a domain? (Example of use) 32
1.6.17. How do I create a "Search for" function for searching in sender information? (Example of use) 32
1.6.18. How do I check for duplicates of encrypted or signed e-mails? 33
1.6.19. How can I use categories to create mappings for specific customer scenarios? (Example of use) 33
1.6.20. How can I use sources to create mappings for specific customer scenarios? (Example of use) 33
1.6.21. Which properties of an e-mail are analyzed for duplicate checking? 34
1.7. Additional information sources and imprint 34

1. d.velop documents in Microsoft Outlook (Cloud)

1.1. Basic information on the application and the manual

This documentation describes the installation, configuration and updating of d.3one 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.3one 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.3one

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. Useful things to know about storing and displaying e-mails in d.3one

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 following list to understand which types of e-mails d.velop documents processes 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.

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.

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.

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. 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
```

1.2.2. Installing the add-in for d.3one 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

You can download the add-in installation package via the configuration.

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 **Client integrations** under **Context menus and functions**.
3. Click on **Upload add-in setup**.

1.2.3. Locally installing 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**

1.2.4. 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.3one 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 entry **Software\d.velop\dvelop.Client.Outlook.Integration**.
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

1.2.5. Distributing the add-in for Microsoft Outlook in the web browser (OWA)

If you also want to use the app for Microsoft Outlook in the web browser (OWA), for example, you must set up a connection for the add-in in the integration settings. You can then distribute the add-in to your users with Microsoft Exchange Admin Center.

This is how it works

1. Open the **Configuration** feature from the start page and navigate to **Web settings** in the **Miscellaneous** category.
2. In the **Allowed Domains** section, add the entry **https://outlook.office.com**.
3. Go to Microsoft Exchange Admin Center to distribute the add-in.
4. Go to **Organization > Add-Ins** and enter the following URL: **https://<BaseUri>/groupware/clients/outlookaddin/manifest**

With the add-in distribution configuration as the basis, your users can then use d.3one in Outlook in the web browser.

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

> **Warning**
> Microsoft will disable Exchange Web Services (EWS) for all external applications in Exchange Online as of October 1, 2026. This change will also affect the d.velop components d.ecs groupware and d.ecs content crawler. Neither application will be able to access Exchange Online via EWS anymore. Instead, a switch to the Microsoft Graph API is required.

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**
  - **MailboxSettings.ReadWrite** (This permission is required in order to use a color for each category.)

  - **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 Exchange Online and Microsoft EWS

> **Warning**
> Microsoft will disable Exchange Web Services (EWS) for all external applications in Exchange Online as of October 1, 2026. This change will also affect the d.velop components d.ecs groupware and d.ecs content crawler. Neither application will be able to access Exchange Online via EWS anymore. Instead, a switch to the Microsoft Graph API is required.

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

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

> **Warning**
> Microsoft will disable Exchange Web Services (EWS) for all external applications in Exchange Online as of October 1, 2026. This change will also affect the d.velop components d.ecs groupware and d.ecs content crawler. Neither application will be able to access Exchange Online via EWS anymore. Instead, a switch to the Microsoft Graph API is required.

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

1.3.6. 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

1.3.7. 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

1.3.8. 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.

1.3.9. 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

1.3.10. 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.

1.3.11. 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

1.3.12. 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 DGIX 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.

1.3.13. 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.

1.4. 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. 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.

1.4.4. Enabling the check for duplicates

You can avoid storing unnecessary duplicates in the d.3 repository by enabling the check for duplicates in the Groupware app.

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.

1.4.5. 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.

> **Note**
> You can assign colors to categories (available starting with version 1.32.0 of d.ecs groupware). If you are using the Microsoft Graph API and have granted the **MailboxSettings.ReadWrite** permission in the Azure Active Directory app registration, the color for the category is automatically applied to the mailbox. If the permission has not been granted, the category is still created without a color assignment, and a warning is logged.

1.4.6. 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.

1.4.7. 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.

1.4.8. 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.

1.4.9. 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.

1.4.10. 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.

1.4.11. 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.

1.5. 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 **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.

1.6. Frequently asked questions

You can find answers to frequently asked questions in this section.

1.6.1. 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.

1.6.2. 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.

1.6.3. 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.

1.6.4. 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.

1.6.5. 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.3one 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

1.6.6. 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

1.6.7. 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

> **Note**
> You can assign colors to categories (available starting with version 1.32.0 of d.ecs groupware). If you are using the Microsoft Graph API and have granted the **MailboxSettings.ReadWrite** permission in the Azure Active Directory app registration, the color for the category is automatically applied to the mailbox. If the permission has not been granted, the category is still created without a color assignment, and a warning is logged.

1.6.8. What are sources?

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

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

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

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

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

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

- **Standard - Microsoft Exchange e-mail**
- **Standard - Microsoft Exchange attachment**
- **Standard - Microsoft Exchange journal e-mail**
- **Standard - IBM Notes e-mail**
- **Standard - IBM Notes attachment**
- **Standard - IBM Notes journal e-mail**

- **Standard - appointment/meeting**

See also:

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

1.6.9. What are mappings?

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

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

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

See also:

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

1.6.10. 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.

1.6.11. 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.

1.6.12. 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.

1.6.13. 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.

1.6.14. 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.

1.6.15. 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.

1.6.16. 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.

1.6.17. 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.

1.6.18. 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.

1.6.19. 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

1.6.20. 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

1.6.21. 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

1.7. 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.