

smart FIX

E-Mail-Import

Produktversion 6 SP 01

© Insiders Technologies GmbH, Kaiserslautern 2024

Alle Rechte vorbehalten

Nachdruck und sonstige Verwertung, auch auszugsweise, sind nur zulässig mit schriftlicher Genehmigung von Insiders Technologies GmbH.

Stand: 27.09.2024

Diese Unterlage wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Insiders schließt jegliche Haftung betreffend der Vollständigkeit, Verwendungsfähigkeit, Richtigkeit und Aktualität der Dokumentinhalte aus. Insiders behält sich das Recht vor, dieses Dokument jederzeit zu verändern oder zu aktualisieren.

Maßgebend ist stets die jeweilige vertragliche Vereinbarung.

Die Dokumentationen beschreiben alle verfügbaren Funktionen, Basisprodukte und Zusatzkomponenten, die bausteinartig für individuelle Kundenlösungen zusammengesetzt werden können. Wir weisen darauf hin, dass somit bestimmte Funktionen eine eigene Lizenzierung erfordern.

Ein Teil der verwendeten Namen sind geschützte Handelsnamen und/oder Marken der jeweiligen Hersteller.

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter.

Insiders Technologies GmbH

Brüsseler Str. 1

67657 Kaiserslautern

GERMANY

Tel: +49(0)631/92081-1700

Fax: +49(0)631/92081-1711

E-Mail: support@insiders-technologies.de

Internet: <https://www.insiders-technologies.de>

Inhalt

1	Einleitung	5
1.1	Überblick	6
2	Verarbeitung elektronischer Dokumente	7
2.1	Grundlegendes zur Verarbeitung	8
2.1.1	Direkt verarbeitbare Dateien	8
2.1.2	Von Microsoft Office verarbeitete Dateien	8
2.1.3	Von LibreOffice verarbeitete Dateien	9
2.2	Verarbeitung elektronischer Dokumente	9
2.2.1	Windows 64-Bit-Betriebssystem	9
2.2.2	Microsoft Office Dokumente in neueren Versionen	9
2.2.3	Activator als Dienst	10
2.3	Weitere Konfigurationsmöglichkeiten	10
3	E-Mail-Import	11
3.1	Begriffe	12
3.2	Voraussetzungen für den E-Mail-Import	13
3.2.1	E-Mail-Clients	13
3.2.2	Registrierung der Anwendung für EWS OAuth2	13
3.2.3	Registrierung der Anwendung für Microsoft Graph als Benutzer	15
3.2.4	Zusätzliche Konfiguration für Gruppenpostfächer	16
3.2.5	Registrierung der Anwendung für Microsoft Graph als Anwendung	18
3.2.6	Registrierung der Anwendung für IMAP OAuth2 mit Gmail	20
4	Arbeitsweise des E-Mail-Import	22
4.1	Ablauf des E-Mail-Import	23
4.2	Auswahl der zu importierenden E-Mails	24
4.3	Erzeugen von Bildstapeln	24
4.3.1	Erzeugte PDFs	25
4.3.2	Konvertierung in PDF-Dateien mit LibreOffice	25
4.3.3	Behandlung von Anhängen	26
4.3.4	Externe Quellen in HTML-Dateien	28
4.3.5	E-Mails im Aussteuerungsordner	29
4.3.6	Fehlerbehandlung bei der Konvertierung	29
4.4	Dokumenttrennung	29
4.5	Klassifikation des E-Mail-Bodys	30
4.5.1	Verarbeitung bei kurzen Texten	30
5	Konfiguration des E-Mail-Import	31
5.1	Konfiguration der E-Mail-Profiles	32
5.2	Schnittstellen zum E-Mail-Server	32

5.2.1	EWS.....	32
5.2.2	EWS OAuth2	33
5.2.3	IMAP	33
5.2.4	IMAP OAuth2	33
5.2.5	Graph User.....	34
5.2.6	Graph App.....	34
5.3	Weitere Konfigurationsmöglichkeiten	34
5.4	Importer	36
6	Kundenspezifische Anpassungen	37
6.1	Ablauf des SPL-Programms	38
6.2	Überschreibbare Funktionen	39
6.2.1	E-Mail-Profile	39
6.2.2	Version der IMAP-Bibliothek Chilkat.dll	39
6.2.3	Aufgabennamen	39
6.2.4	Anhänge.....	40
6.2.5	Aussteuerung.....	42
6.2.6	Dateinamen	44
6.2.7	E-Mail-Kopfdaten.....	45
6.2.8	Externe Vorgangs-ID	45
6.2.9	Felder.....	45
6.2.10	Filter für Klassifikation des E-Mail-Bodys	47
6.2.11	Konfigurationen.....	49
6.2.12	Aufgabenattribute	52
6.2.13	Steuerdateinamen	52
6.2.14	EML-Dateien	53
6.2.15	Übernahme der Empfänger in die Kopfdaten einer E-Mail	53
7	Glossar	54
7.1	Bezeichnungen und Erklärungen	55

1 Einleitung

Das Kapitel gibt einen Überblick über den Ablauf der Dokumentverarbeitung.

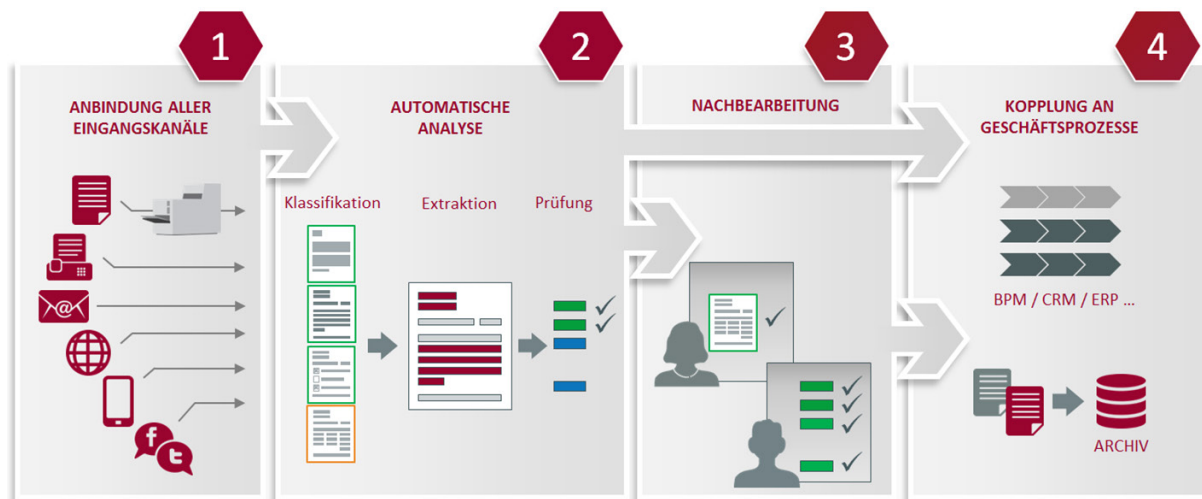
1.1 Überblick

Das System verarbeitet Daten aus unterschiedlichen Eingangskanälen und Medien. Das können elektronische Dokumente wie E-Mails, aber auch Briefpost und Faxe sein.

Während der automatischen Analyse wird die Dokumentklasse ermittelt. Anhand der durch die Dokumentklasse vorgegebenen Informationsstrukturen werden die Inhalte des Dokuments extrahiert. Anschließend werden die extrahierten Daten nach vorgegebenen Kriterien automatisch geprüft und bewertet.

Daten, die nicht zweifelsfrei ermittelt werden konnten, können manuell kontrolliert und ggf. angepasst werden.

Nach Abschluss der Dokumentverarbeitung können die extrahierten Daten an nachgelagerte Systeme exportiert werden.



Zur Verarbeitung von E-Mails steht der *E-Mail-Import* zur Verfügung, mit dem E-Mails und deren Anhänge von einem E-Mail-Server in das System übertragen werden.

Der *E-Mail-Import* ist in *SPL* realisiert und bietet so die Möglichkeit, die Verarbeitung kundenspezifisch anzupassen.

Hinweis

Wenn die *smartblocks E-Mail-Import* und *Standard-XML-Import* gleichzeitig aktiviert werden, muss jeder Importer im *Configurator* über den Dialog *Komponente ändern* im Textfeld *Parameter* mit dem Kommandozeilenparameter „-SPLImport <Importmodus>“ auf einen Importmodus eingeschränkt werden.

Für den *E-Mail-Import* ist eine separate Lizenz erforderlich.

2 Verarbeitung elektronischer Dokumente

Das Kapitel beschreibt Grundlegendes zur Verarbeitung elektronischer Dokumente und gibt einen Überblick über die Voraussetzungen und Konfigurationsmöglichkeiten.

2.1 Grundlegendes zur Verarbeitung

Elektronische Dokumente werden beim Import in das PDF-Format konvertiert und in diesem Format vom System verarbeitet. Dabei werden verschiedene Dateitypen unterschieden:

- Dateien, die direkt konvertiert werden können (Bild-, PDF-, Text-, HTML-Dateien)
- Microsoft Office Dateien, für deren Konvertierung die Installation der jeweiligen Office-Anwendung erforderlich ist
- Dateien, die über einen Druckvorgang konvertiert werden (z. B. OpenOffice Dateien)

2.1.1 Direkt verarbeitbare Dateien

Nachfolgende Formate unterstützt das System direkt und wandelt diese bei Bedarf entsprechend um, das heißt es ist keine Installation einer weiteren Anwendung erforderlich:

Suffix	Format
BMP	MS Windows Bitmap
GIF	Gif Image
HTML	HyperText Markup Language
JIF	JFIFJPEG
JPG	JFIFJPEG
PDF	Portable Document Format
PNG	Png Image
TIF	TIFF
TXT	Textdatei

2.1.2 Von Microsoft Office verarbeitete Dateien

Mit Microsoft Office und OpenOffice erstellte Dateien werden beim Import über die jeweilige Microsoft Office Anwendung in das PDF-Format konvertiert.

Die Konvertierung der Dateien erfolgt über die Funktion *Speichern* der jeweiligen Anwendung.

Format	Anwendung
*.doc, *.docx, *.txt, *.rtf, *.odt	MS Word
*.xls, *.xlsx, *.ods	MS Excel
*.ppt, *.pps, *.pptx, *.ppsx, *.odp	MS PowerPoint

Bei der Konvertierung sollte als Standarddrucker kein Netzwerkdrucker, sondern ein lokaler oder virtueller Drucker eingerichtet sein.

Konfiguration

Für kundenspezifische Anpassungen stehen die folgenden Konfigurationseinträge zur Verfügung.

- smartFIX / Edoc / OfficeExtensions / SupportedExcelExtensions
- smartFIX / Edoc / OfficeExtensions / SupportedPowerPointExtensions
- smartFIX / Edoc / OfficeExtensions / SupportedWordExtensions

2.1.3 Von LibreOffice verarbeitete Dateien

Mit LibreOffice erstellte Dateien werden beim Import in das PDF-Format konvertiert.

Folgende Dateiendungen werden von LibreOffice unterstützt:

*.doc, *.docx, *.txt, *.rtf, *.odt, *.xls, *.xlsx, *.ods, *.ppt, *.pps, *.pptx, *.ppsx und *.odp

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Edoc / LibreOffice / SupportedLibreOfficeExtensions

Verwandte Themen**Konvertierung in PDF-Dateien mit LibreOffice25****2.2 Verarbeitung elektronischer Dokumente**

Für die Verarbeitung elektronischer Dokumente sind verschiedene Voraussetzungen erforderlich, die in den folgenden Abschnitten beschrieben sind.

2.2.1 Windows 64-Bit-Betriebssystem

Bei Windows 64-Bit-Systemen kann es aufgrund eines Fehlverhaltens in der *Microsoft COM* Infrastruktur erforderlich sein, den folgenden Ordner anzulegen:

- %WINDIR%\SysWOW64\config\systemprofile\Desktop

2.2.2 Microsoft Office Dokumente in neueren Versionen

Dokumente, die mit einer neueren Version von Microsoft Office erstellt wurden, können importiert und verarbeitet werden.

Um einen korrekten Speicher- oder Druckvorgang über Word sicherzustellen, ist in Word die Option *Dateiformatkonvertierung beim Öffnen bestätigen* zu deaktivieren.

Die Option erreichen Sie folgendermaßen:

1. Wählen Sie die Registerkarte *Datei* aus.
2. Betätigen Sie im linken Bereich die Schaltfläche *Optionen*.

Der Dialog *Word-Optionen* wird geöffnet.

3. Betätigen Sie die Schaltfläche *Erweitert*.
4. Deaktivieren Sie im Bereich *Allgemein* das Ankreuzkästchen *Dateiformatkonvertierung beim Öffnen bestätigen*.

2.2.3 Activator als Dienst

Wenn der *Activator* auf dem Rechner als Dienst installiert und gestartet ist, müssen folgende Voraussetzungen erfüllt sein:

- Der Dienst „DCOM-Server-Prozessstart“ ist gestartet.
- Dem Dienstbenutzer müssen ggf. die Benutzerrechte „Start- und Aktivierungsberechtigungen“ für folgende Programme zugewiesen werden:
 - *Microsoft Excel* Anwendung
 - *Microsoft PowerPoint* Präsentation
 - *Microsoft Word* Dokument

Tipp

Wenn der Dienstbenutzer auf dem Rechner über lokale Administratorrechte verfügt, ist in der Regel keine weitere Anpassung der Benutzerrechte erforderlich. Sollte eine Berechtigung fehlen, wird im Event-Log eine entsprechende Meldung ausgegeben.

Die Benutzerrechte werden über den Dialog *Start- und Aktivierungsberechtigungen* zugewiesen. Den Dialog erreichen Sie über *Start > Systemsteuerung > Verwaltung > Komponentendienste > Computer > Arbeitsplatz > DCOM-Konfiguration > Kontextmenüpunkt Eigenschaften > Dialog Eigenschaften von <Anwendungsname> > Registerkarte Sicherheit > Bereich Start- und Aktivierungsberechtigungen > Option Anpassen > Schaltfläche Bearbeiten....*



2.3 Weitere Konfigurationsmöglichkeiten

Zur Konvertierung der elektronischen Dateien stehen folgende Konfigurationseinträge zur Verfügung:

- smartFIX / Edoc / ExtensionsNotToDisplay
- smartFIX / Edoc / KillProclds
- smartFIX / Edoc / HtmlConversion / FontsToReplace
- smartFIX / Edoc / HtmlConversion / LoadExternalResources
- smartFIX / Edoc / HtmlConversion / MinHtmlFontSize
- smartFIX / Edoc / HtmlConversion / TargetFont
- smartFIX / Edoc / NoPrintExtensions
- smartFIX / Edoc / UseImprovedHtmlRendering
- smartFIX / Edoc / HtmlConversion / WrapPreformattedText

3 E-Mail-Import

In diesem Kapitel sind einige Begriffe erläutert, die in den weiteren Abschnitten des Handbuches verwendet werden. Weiterhin sind die Voraussetzungen, die für den *E-Mail-Import* erforderlich sind, beschrieben.

3.1 Begriffe

Begriff	Erläuterung
Eingangsordner	Ordner auf dem E-Mail-Server, aus dem die zu importierenden E-Mails gelesen werden
Zielordner	Ordner auf dem E-Mail-Server, in den die E-Mails verschoben werden, wenn sie in das System importiert wurden
Aussteuerungsordner	Ordner auf dem E-Mail-Server, in den E-Mails verschoben werden, die nicht importiert werden können
E-Mail-Profil	Kombination aus Benutzernamen, Passwort, Eingangsordner, Zielordner, Aussteuerungsordner und bestimmten Optionen für den Import
Schnittstelle	E-Mail-Protokoll, das für die Kommunikation mit dem E-Mail-Server verwendet wird
EWS	Abkürzung für Exchange Web Services Schnittstelle für den Zugriff auf Microsoft Exchange Server
IMAP	Abkürzung für Internet Message Access Protocol Schnittstelle, über die auf andere E-Mail-Server als Microsoft Exchange Server zugegriffen werden kann
EWS OAuth2	Abkürzung für Exchange Web Services Open Authorization 2 Schnittstelle für den mit OAuth2 authentifizierten Zugriff auf Microsoft Office 365 Exchange Konten
IMAP OAuth2	Abkürzung für Internet Message Access Protocol Open Authorization 2 Schnittstelle für den mit OAuth2 authentifizierten Zugriff auf andere Konten als Microsoft Office 365
Graph User	Schnittstelle für den mit OAuth2 authentifizierten Zugriff auf Microsoft Office 365 Konten über Microsoft Graph Die Anmeldung erfolgt als Benutzer
Graph App	Schnittstelle für den mit OAuth2 authentifizierten Zugriff auf Microsoft Office 365 Konten über Microsoft Graph Die Anmeldung erfolgt als Anwendung

3.2 Voraussetzungen für den E-Mail-Import

Zur Verarbeitung elektronischer Dokumente sind zusätzlich nachfolgende Voraussetzungen erforderlich.

Der *E-Mail-Import* unterstützt zur Kommunikation mit E-Mail-Servern folgende Schnittstellen:

- EWS (Exchange Web Services)
- IMAP (Internet Message Access Protocol)
- Graph User (Microsoft Graph für Microsoft Office 365 mit einer Anmeldung als Benutzer)
- Graph App (Microsoft Graph für Microsoft Office 365 mit einer Anmeldung als Anwendung)

Für den Import von E-Mails im EML-Format aus einem Dateiverzeichnis steht die Schnittstelle File zur Verfügung.

3.2.1 E-Mail-Clients

Lotus Notes

- Die Eigenschaft *Sperren von Dokumenten* muss deaktiviert sein, da sie im IMAP-Protokoll nicht vorgesehen ist und vom *E-Mail-Import* nicht unterstützt wird.

Verwandte Themen

Windows 64-Bit-Betriebssystem.....	9
Microsoft Office Dokumente in neueren Versionen	9
Activator als Dienst	10

3.2.2 Registrierung der Anwendung für EWS OAuth2

Um ein E-Mail-Profil mit der Schnittstelle EWS OAuth2 im *Configurator* erstellen zu können, muss eine Anwendungs-ID vorliegen. Diese wird von Microsoft bei der Registrierung der Anwendung über Microsoft Azure auf der Webseite <https://aad.portal.azure.com> vergeben. Hierfür sind Administrationsrechte erforderlich. Gehen Sie wie folgt vor:

1. Melden Sie sich auf der Webseite <https://aad.portal.azure.com> an.
2. Wählen Sie in der linken Navigationsleiste *Alle Dienste* aus.
Die Navigation wird erweitert.
3. Wählen Sie in der erweiterten Navigation *App-Registrierung* aus.
Die Seite *App-Registrierung* wird geladen.
4. Betätigen Sie die Schaltfläche *Neue Registrierung*.
Die Seite *Anwendung registrieren* wird geöffnet.
5. Geben Sie im Textfeld *Name* einen passenden Namen ein, beispielsweise Insiders Technologies GmbH smart-FIX EWS OAuth2-based Connection.
6. Aktivieren Sie im Bereich *Supported account types* das Ankreuzkästchen *Accounts in any organizational directory (Any Azure AD directory - Multitenant)*.
7. Aktivieren Sie im Bereich *Platform configuration(optional)* das Ankreuzkästchen *Client Application (Web, iOS, Android, Desktop+Devices)*.

8. Betätigen Sie die Schaltfläche *Registrieren*.
Die Anwendung wird registriert.
9. Wechseln Sie zur Registerkarte *Authentication*.
10. Betätigen Sie die Schaltfläche *Add a platform*.
Der Dialog *Configure platforms* wird geöffnet.
11. Wählen Sie die Option *Mobile and desktop applications* aus.
12. Aktivieren Sie im Bereich *Redirect URI* das Ankreuzkästchen <https://login.microsoftonline.com/common/oauth2/nativeclient>.
13. Geben Sie im Feld *Custom redirect URIs* den Wert `urn:ietf:wg:oauth:2.0:oob` ein.
14. Bestätigen Sie die Eingaben mit *Configure*.
15. Wechseln Sie zur Registerkarte *API permissions*.
16. Betätigen Sie die Schaltfläche *Add a permission*.
17. Wählen Sie im Bereich *Supported legacy APIs* die Option *Exchange* aus.
18. Wählen Sie die Option *Delegated permissions* aus.
19. Navigieren Sie zum Eintrag *EWS*.
20. Aktivieren Sie das Ankreuzkästchen *EWS.AccessAsUser.All*.
21. Betätigen Sie die Schaltfläche *Add permissions*.
22. Die Berechtigung wird hinzugefügt.

Hinweis

Falls der Bereich *Supported legacy APIs* oder das Ankreuzkästchen *EWS.AccessAsUser.All* nicht angezeigt werden, navigieren Sie in den Bereich *Manifest* und erweitern Sie den Eintrag *requiredResourceAccess* folgendermaßen:

```
{
  "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
  "resourceAccess": [
    {
      "id": "3b5f3d61-589b-4a3c-a359-5dd4b5ee5bd5",
      "type": "Scope"
    }
  ]
}
```

Beachten Sie, dass mehrere Einträge mit Komma voneinander getrennt werden.

23. Navigieren Sie in die Registerkarte *Overview*.
Im Textfeld *Application (client) ID* wird die benötigte Anwendungs-ID angezeigt.
24. Notieren Sie sich die Anwendungs-ID.

Außerdem muss die Tenant-ID vorliegen. Diese ist ebenfalls im Azure Active Directory Admin Center unter <https://aad.portal.azure.com> einsehbar. Gehen Sie wie folgt vor:

1. Wählen Sie in der linken Navigationsleiste *Azure Active Directory* aus.
Die Seite *Azure Active Directory* wird geladen.



2. Wählen Sie im Bereich *Verwalten* die Schaltfläche *Einstellungen* aus.
Die Seite *Eigenschaften* wird geladen.
Im Textfeld *Verzeichnis-ID* wird die Tenant-ID angezeigt.
3. Notieren Sie sich die Tenant-ID und fahren Sie mit der Konfiguration des E-Mail-Profiles im *Configurator* fort.

3.2.3 Registrierung der Anwendung für Microsoft Graph als Benutzer

Tipp

Es wird empfohlen, die Schnittstelle Microsoft Graph als Benutzer zu konfigurieren. Die Schnittstelle ist auch als Graph User oder Graph OAuth2 bekannt. Authentifiziert wird die Schnittstelle durch ein Microsoft Office 365 Konto mittels OAuth2. Dabei wird ein Token generiert, der in *smart FIX* hinterlegt und für die künftige Authentifikation für Microsoft Office 365 genutzt wird. Bevor man die Schnittstelle Microsoft Graph als Benutzer startet, muss auf der Plattform Microsoft Azure eine entsprechende App registriert werden. Die Berechtigungen werden bei der Authentifikation durch *smart FIX* angefordert und müssen während der Registrierung der App nicht gesetzt werden. Die Schnittstelle unterstützt Impersonation.

Falls der E-Mail-Import auf einem System mit einer Firewall ausgeführt wird, müssen für die korrekte Nutzung von Microsoft Graph OAuth2 mindestens die folgenden Einträge in der Firewall freigeschaltet werden:

- <http://graph.microsoft.com/>*
- https://*.microsoftonline.com/*
- https://*.msauth.net/*

Um ein E-Mail-Profil mit der Schnittstelle Graph User im *Configurator* erstellen zu können, muss eine Anwendungs-ID und eine Zertifizierungsstellen-URI vorliegen. Beide werden bei der Registrierung der Anwendung auf der Plattform Azure auf der Webseite des Drittanbieters Microsoft vergeben. Für die Plattform Azure sind Administrationsrechte erforderlich.

Hinweis

Die Oberfläche der Plattform Azure ist abhängig von der verwendeten Version.

Dokumentation

Nähere Informationen können der Dokumentation des folgenden Drittanbieters entnommen werden.

- Dokumentation der Plattform Azure von Microsoft

Beachten Sie die folgenden Punkte:

1. Melden Sie sich auf der Webseite <https://aad.portal.azure.com> an.
2. Navigieren Sie in die Ansicht *App registrations*.
3. Legen Sie eine neue Registrierung an.
4. Geben Sie im Textfeld *Name* einen passenden Namen ein, beispielsweise *smart FIX Exchange Cloud Anbindung*.
5. Aktivieren Sie das Ankreuzkästchen *Accounts in this organizational directory only (<Your company name> - Single tenant)*.
6. Wählen Sie im Listenfeld im Bereich *Redirect URI* den Wert *Public client/native (mobile & desktop)* aus und tragen Sie im Textfeld den Wert *urn:ietf:wg:oauth:2.0:oob* ein.



7. Registrieren Sie die Anwendung.
8. Navigieren Sie zur Ansicht *API permissions*.
In dieser Ansicht werden Berechtigungen vergeben.
9. Stellen Sie sicher, dass für die angelegte Registrierung nur die Berechtigung *User.Read* vergeben ist.
10. Navigieren Sie zur Ansicht *Overview*.
11. Notieren Sie den Wert, der für *Application (client) ID* hinterlegt ist.
Dieser Wert wird für die Anwendungs-ID benötigt.
12. Notieren Sie den Wert, der für *Directory (tenant) ID* hinterlegt ist.
Dieser Wert wird für die Tenant-ID der Zertifizierungsstellen-URI benötigt.

3.2.4 Zusätzliche Konfiguration für Gruppenpostfächer

Um Gruppenpostfächer für Exchange Online nutzen zu können, muss eine sogenannte Impersonation eingerichtet werden. Das bedeutet ein technischer Benutzer simuliert einen Einzelbenutzer, so dass mehrere Benutzer auf dieses Postfach zugreifen können.

Hinweis

Die folgenden Schritte zum Einrichten der Impersonation können für Exchange Online über das Exchange Management Center eingerichtet werden, es wird jedoch empfohlen hierfür eine 64-bit PowerShell mit Administratorrechten zu nutzen. Beim Konfigurieren der Impersonation für On-Premises Exchange Server achten Sie auf das korrekte Einrichten des Management Scopes und des ManagementRoleAssignments.

Führen Sie zum Einrichten der Impersonation für Exchange Online über eine PowerShell die folgenden Befehle aus:

1. Starten Sie eine 64-Bit PowerShell mit Administratorrechten.
2. Installieren Sie das Exchange Online Management Modul in der Version 2.0.5:

```
Install-Module -Name ExchangeOnlineManagement -RequiredVersion 2.0.5
```

3. Bestätigen Sie die Installation mit der Eingabe des Buchstabens J.
4. Importieren Sie das installierte Exchange Online Management Modul:

```
Import-Module ExchangeOnline Management
```

5. Stellen Sie eine Verbindung zu Microsoft Exchange Online her:

```
Connect-ExchangeOnline
```

6. Der Dialog *Bei Ihrem Konto anmelden* wird geöffnet.
7. Melden Sie sich als Benutzer mit Administratorrechten an.
Eine Verbindung zu Microsoft Exchange Online wird hergestellt.

8. Legen Sie eine Distribution Group an:

```
New-DistributionGroup -Name "NameDerDistributionGroup" -Type security
```

9. Lassen Sie sich Informationen zu der neu angelegten Gruppe anzeigen:

```
Get-DistributionGroup NameDerDistributionGroup | fl
```

10. Notieren Sie den Wert des Parameters *DistinguishedName*, dieser wird später benötigt.



11. Fügen Sie alle Postfächer von Benutzern zu der Distribution Group hinzu, die Zugriff auf das Gruppenpostfach benötigen:

```
Add-DistributionGroupMember -Identity NameDerDistributionGroup -Member  
BenutzernameDesPostfachs
```

Mit folgendem Befehl können Sie sich die Mitglieder der Distribution Group anzeigen lassen:

```
Get-DistributionGroupMember NameDerDistributionGroup
```

12. Legen Sie einen neuen Management Scope an:

```
New-ManagementScope -Name NameDesManagementScopes -  
RecipientRestrictionFilter:"MemberOfGroup -eq 'WertDesParametersDistinguishedName'"
```

Mit folgendem Befehl können Sie sich vorhandene Management Scopes anzeigen lassen:

```
Get -ManagementScopes
```

13. Erstellen Sie mit folgendem Befehl eine Rollenzuweisung:

```
New-ManagementRoleAssignment -Name:NameDerRollenzuweisung -  
Role:ApplicationImpersonation -CustomRecipientWriteScope NameDesManagementScopes -  
User:TechnischerBenutzerFuerImpersonation
```

Mit folgendem Befehl können Sie die Rollenzuweisung überprüfen:

```
Get-ManagementRoleAssignment: NameDerRollenzuweisung
```

Tipp

Um zu testen, ob die Impersonation erfolgreich ist, kann das Drittanbietertool EWSEditor eingesetzt werden.



Führen Sie in Microsoft Outlook folgende Schritte aus, um das Postfach eines technischen Benutzers als Gruppenpostfach mit Impersonation freizugeben:

1. Melden Sie sich in Outlook als der technische Benutzer für das Gruppenpostfach an.
2. Wählen Sie die Ordner aus, auf die den Benutzern Zugriff gewährt werden soll.
3. Führen Sie einen Rechtsklick auf den Ordner aus.
Ein Kontextmenü öffnet sich.
4. Wählen Sie im Kontextmenü *Eigenschaften* aus.
5. Der Dialog *Eigenschaften* wird geöffnet.
6. Öffnen Sie die Registerkarte *Berechtigungen*.
7. Betätigen Sie die Schaltfläche *Hinzufügen*.
8. Wählen Sie nun die Benutzer aus, die Zugriff auf das Gruppenpostfach haben sollen.
9. Wählen Sie im Bereich *Berechtigungen* im Listenfeld *Berechtigungsstufe* den Wert *Veröffentlichender Bearbeiter* aus.
10. Bestätigen Sie Ihre Eingaben mit *OK*.

3.2.5 Registrierung der Anwendung für Microsoft Graph als Anwendung

Tipp



Die Schnittstelle ist auch als Graph Application bekannt. Authentifiziert wird *smart FIX* als Anwendung bei Microsoft Office 365. Mit dieser Schnittstelle kann auf alle Postfächer der Organisation zugegriffen werden. Um den Zugriff auf eine bestimmte Gruppe einzuschränken, führen Sie folgende Schritte in der PowerShell mit vorliegender Anwendungs-ID als Administrator von Microsoft Office 365 aus:

1. Laden Sie das Exchange Online Management Modul:

```
Install-Module -Name ExchangeOnlineManagement -Scope CurrentUser
```

2. Verbinden Sie sich mit Exchange Online, wobei das User Principal Name-Format genutzt werden muss:

```
Connect-ExchangeOnline -UserPrincipalName <UserPrincipalName>
```

3. Erstellen Sie eine neue Richtlinie für den Zugriff eines Gruppenpostfachs auf die Anwendung:

```
New-ApplicationAccessPolicy -AppId <Anwendungs-ID> -PolicyScopeGroupId  
<Gruppenpostfach> -AccessRight RestrictAccess -Description "Restrict this app to  
members of distribution group <Gruppenpostfach>."
```

4. Testen Sie, ob die Anwendung Zugriff auf das Postfach eines Benutzers aus der Gruppe <Gruppenpostfach> hat:

```
Test-ApplicationAccessPolicy -Identity <Benutzerpostfach> -AppId <Anwendungs-ID>
```

Bevor die Schnittstelle Microsoft Graph als Anwendung gestartet wird, muss auf der Plattform Microsoft Azure eine entsprechende App registriert werden. Dabei müssen die erforderlichen Berechtigungen zum Abrufen von E-Mails konfiguriert und von einem Administrator von Microsoft Azure freigegeben werden. Es wird empfohlen Microsoft Graph als Benutzer einzurichten.

Falls der E-Mail-Import auf einem System mit einer Firewall ausgeführt wird, müssen für die korrekte Nutzung von Microsoft Graph OAuth2 mindestens die folgenden Einträge in der Firewall freigeschaltet werden:

- <http://graph.microsoft.com/>*
- https://*.microsoftonline.com/*
- https://*.msauth.net/*

Um ein E-Mail-Profil mit der Schnittstelle Graph App im *Configurator* erstellen zu können, muss ein Client-Secret, eine Anwendungs-ID und eine Tenant-ID vorliegen. Diese werden bei der Registrierung der Anwendung auf der Plattform Azure auf der Webseite des Drittanbieters Microsoft vergeben. Für die Plattform Azure sind Administrationsrechte erforderlich.

Hinweis

Die Oberfläche der Plattform Azure ist abhängig von der verwendeten Version.



Dokumentation



Nähere Informationen können der Dokumentation des folgenden Drittanbieters entnommen werden.

- Dokumentation der Plattform Azure von Microsoft

Beachten Sie die folgenden Punkte:

1. Melden Sie sich auf der Webseite <https://aad.portal.azure.com> an.
2. Navigieren Sie in die Ansicht *App registrations*.
3. Legen Sie eine neue Registrierung an.

4. Geben Sie im Textfeld *Name* einen passenden Namen ein, beispielsweise smart FIX Exchange Cloud Anbindung.
5. Aktivieren Sie das Ankreuzkästchen *Accounts in this organizational directory only (<Your company name> - Single tenant)*.
6. Wählen Sie im Listenfeld im Bereich *Redirect URI* den Wert *Public client/native (mobile & desktop)* aus und tragen Sie im Textfeld den Wert *urn:ietf:wg:oauth:2.0:oob* ein.
7. Registrieren Sie die Anwendung.
8. Navigieren Sie zur Ansicht *Certificates & secrets*.
9. Legen Sie ein neues Client-Secret an.
10. Geben Sie im Textfeld *Description* eine passende Beschreibung ein und wählen Sie im Listenfeld *Expires* einen Zeitraum aus, nachdem das Client-Secret abläuft.

Nachdem das Client-Secret erstellt wurde, wird im Bereich *Value* der Wert des Client-Secrets angezeigt.

11. Notieren Sie das Client-Secret.

Hinweis

Der Wert des Client-Secret kann später nicht mehr eingesehen werden.

12. Navigieren Sie in die Ansicht *API permissions*.
13. Vergeben Sie für Microsoft Graph Berechtigungen vom Typ *Application permissions*.
14. Wählen Sie die Berechtigungen *Mail.ReadWrite* und *Mail.Send* aus.
15. Bestätigen Sie die Einstellungen mit *Add permissions*.

Für die Anwendung sollten nun die Berechtigungen *User.Read*, *Mail.ReadWrite* und *Mail.Send* vergeben sein.

Hinweis

Die Vergabe der Berechtigungen für *Mail.ReadWrite* und *Mail.Send* muss durch einen Administrator bestätigt werden. Außerdem muss sichergestellt werden, dass die Anwendung nur Zugriff auf die benötigten Postfächer hat. Dies kann nur mit Administratorrechten über die PowerShell ausgeführt werden. Falls noch nicht geschehen, installieren Sie die Azure CLI und verbinden sich mit Exchange Online mit dem folgenden Befehlen:

```
Install-Module -Name ExchangeOnlineManagement -Scope CurrentUser  
Connect-ExchangeOnline -UserPrincipalName <UserPrincipalName>
```

Führen Sie danach die folgenden Befehle als Administrator aus:

```
New-ApplicationAccessPolicy -AppId <AppId> -PolicyScopeGroupId "My Graph User Group" -AccessRight  
RestrictAccess -Description "Restrict this app to members of distribution group My Graph User Group."  
Test-ApplicationAccessPolicy -Identity <MyGraphUser> -AppId <AppId>
```

Genauere Informationen hierzu sind der Dokumentation des Herstellers Microsoft zu entnehmen.

16. Navigieren Sie zur Ansicht *Overview*.
17. Notieren Sie den Wert, der für *Application (client) ID* hinterlegt ist.
Dieser Wert wird für die Anwendungs-ID benötigt.
18. Notieren Sie den Wert, der für *Directory (tenant) ID* hinterlegt ist.
Dieser Wert wird für die Tenant-ID benötigt.

3.2.6 Registrierung der Anwendung für IMAP OAuth2 mit Gmail

Um ein E-Mail-Profil mit der Schnittstelle IMAP OAuth2 mit Gmail im *Configurator* erstellen zu können, muss eine Client-ID und ein Clientschlüssel vorliegen. Diese werden von Google bei der Registrierung der Anwendung über die Google Developer Console auf der Webseite <https://code.google.com/apis/console#access> vergeben. Hierfür sind Administrationsrechte erforderlich. Gehen Sie wie folgt vor:

1. Melden Sie sich auf der Webseite <https://code.google.com/apis/console#access> an.
2. Navigieren Sie in den Bereich *Ressourcen verwalten*.
3. Betätigen Sie die Schaltfläche *Projekt erstellen*.
Ein neues Projekt wird angelegt.
4. Geben Sie im Textfeld *Projektname* einen Projektnamen ein.
5. Falls gefordert, wählen Sie im Listenfeld *Organisation* den Suffix der Domäne aus.
6. Falls gefordert, wählen Sie im Listenfeld *Speicherort* den Suffix der Domäne aus.
7. Betätigen Sie die Schaltfläche *Erstellen*.
Das neue Projekt wird erstellt.
Die Seite zum Anlegen eines neuen Projekts wird geschlossen.
8. Navigieren Sie im Menü zum Bereich *APIs & Dienst*.
9. Betätigen Sie die Schaltfläche *Bibliothek*.
Ein Suchdialog wird geöffnet.
10. Geben Sie im Suchdialog *Gmail API* ein.
11. Selektieren Sie den Wert *Gmail API*.
12. Betätigen Sie die Schaltfläche *AKTIVIEREN*.
Die API für Gmail ist aktiviert.
13. Navigieren Sie im Menü zum Bereich *APIs & Dienst*.
14. Betätigen Sie die Schaltfläche *OAuth-Zustimmungsbildschirm*.
15. Kontrollieren Sie, ob das Projekt mit dem in Schritt 4 erstellten Projektnamen selektiert ist.
16. Wählen Sie im Listenfeld *User Type* den Wert *Intern* aus.
17. Betätigen Sie die Schaltfläche *Erstellen*.
18. Geben Sie im Textfeld *Name der Anwendung* einen Namen ein.
19. Navigieren Sie zum Bereich *Bereiche for Google APIs*.
20. Betätigen Sie die Schaltfläche *Bereich hinzufügen*.
21. Wählen Sie im Listenfeld *Gmail API* den Wert <https://mail.google.com/> aus.
22. Betätigen Sie die Schaltfläche *Hinzufügen*.
23. Betätigen Sie die Schaltfläche *Speichern*.
24. Navigieren Sie zum Bereich *APIs & Dienst*.
25. Betätigen Sie die Schaltfläche *Anmeldedaten*.
26. Betätigen Sie die Schaltfläche *ANMELDEDATEN ERSTELLEN*.
27. Wählen Sie *OAuth-Client-ID* aus.

28. Wählen Sie im Listenfeld *Anwendungstyp* den Wert *Desktopanwendung* aus.

29. Wählen Sie einen passenden Namen aus.

30. Betätigen Sie die Schaltfläche *ERSTELLEN*.

Die OAuth2-Client-ID wird erstellt.

Eine Meldung wird angezeigt, dass der OAuth-Client erstellt wurde. Die Client-ID und der Clientschlüssel werden angezeigt.

31. Notieren Sie sich die Client-ID und den Clientschlüssel und fahren Sie mit der Konfiguration des E-Mail-Profiles im *Configurator* fort.

4 Arbeitsweise des E-Mail-Import

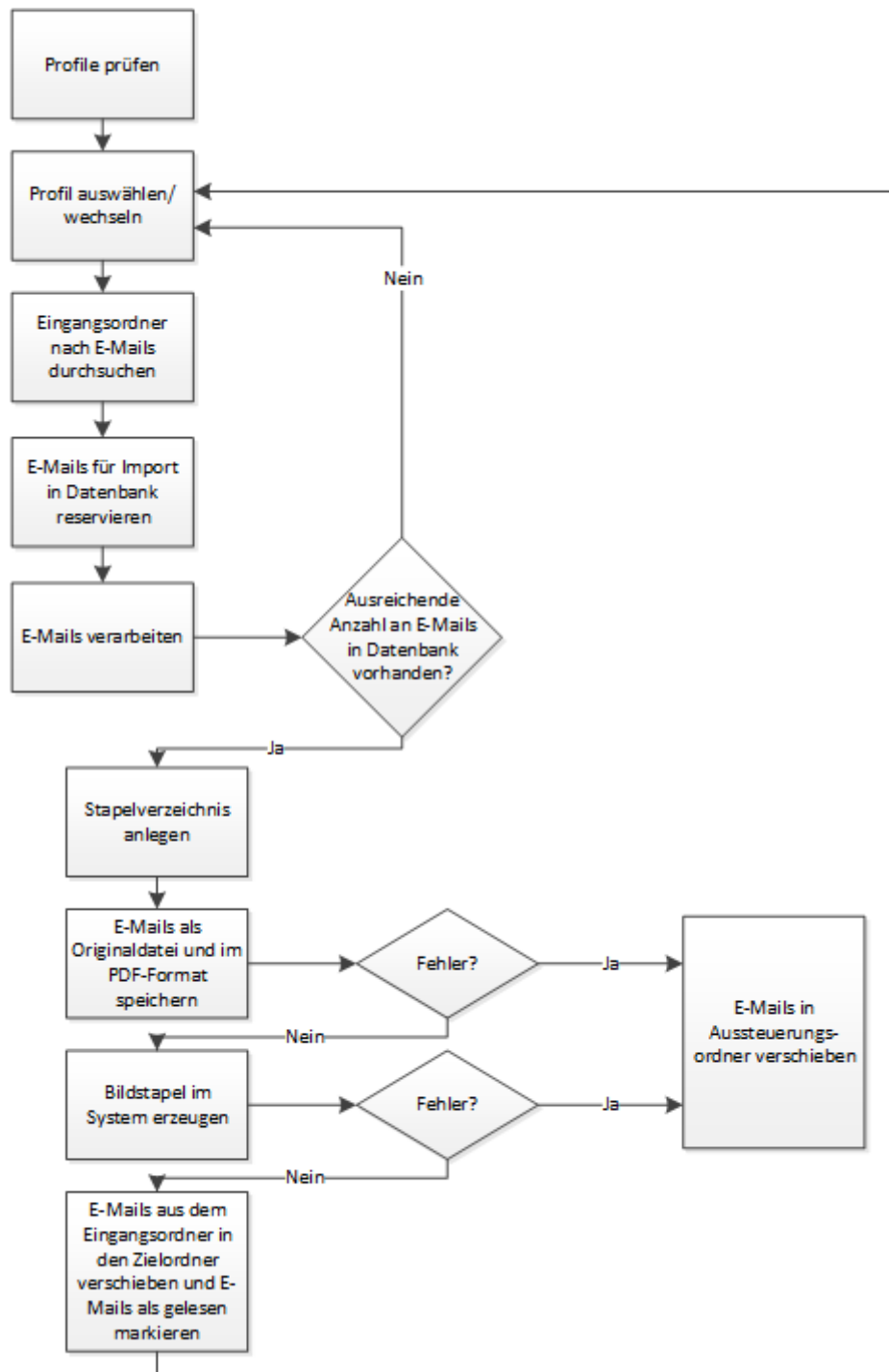
In diesem Kapitel sind die wesentlichen Abläufe beim *E-Mail-Import* in der Standardkonfiguration erläutert.

4.1 Ablauf des E-Mail-Import

Der *E-Mail-Import* ist ein Betriebsmodus des *Importer*. Wenn eine entsprechende Lizenz vorhanden ist, kann diese im *DocumentManager* über den *smartblock E-Mail-Import* aktiviert werden.

E-Mail-Bodys und E-Mail-Anhänge können in diversen Formaten verarbeitet und als PDF für die Weiterverarbeitung im System gespeichert werden.

Bei der Verarbeitung werden im Wesentlichen die folgenden Schritte durchlaufen:



4.2 Auswahl der zu importierenden E-Mails

Die zu importierenden E-Mails werden anhand der im *Configurator* hinterlegten Benutzerprofile ausgewählt.

Dabei werden vom *E-Mail-Import* die einzelnen Profile nacheinander durchgegangen und die E-Mails reserviert, die sich für den Import in den jeweiligen Eingangsordnern befinden. Hierfür wird die E-Mail mit folgenden Informationen in die Datenbanktabelle SF_MAIL_IMPORT der *Control-DB* geschrieben:

- Profilname
- Eindeutige ID der E-Mail
- Name des Clients für den *E-Mail-Import*
- Verarbeitungszustand (Waiting, Processing started, Processed)
- Zeitstempel

4.3 Erzeugen von Bildstapeln

Wenn in der Datenbanktabelle SF_MAIL_IMPORT der *Control-DB* eine ausreichende Anzahl an reservierten E-Mails existiert, wird für die jeweiligen E-Mails ein Stapelverzeichnis mit folgendem Namen angelegt:

- MAIL_<yyyymmdd>_<Fortlaufende Nummerierung>
z. B. MAIL_20120629_000014

Hinweis

Es werden maximal 200 zu analysierende Seiten pro Dokument und 2000 Seiten pro Bildstapel unterstützt.

In diesem Stapelverzeichnis werden die E-Mail-Bodys und E-Mail-Anhänge als Originaldateien und als PDF abgelegt. Für die Originaldateien wird im Stapelverzeichnis ein Ordner OriginalFiles erzeugt. Die PDFs werden direkt im Stapelverzeichnis gespeichert.

Die Größe der Stapel ist konfigurierbar.

Konfiguration

Für kundenspezifische Anpassungen stehen die folgenden Konfigurationseinträge zur Verfügung.

- smartFIX / Import / ExchangeDirectory
- smartFIX / Import/Mail / MaxEmailsPerStack



4.3.1 Erzeugte PDFs

Je nach Konfiguration werden die Inhalte der E-Mails entweder in eine oder in mehrere PDFs konvertiert.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Import/Mail / SinglePdfPerMail



4.3.2 Konvertierung in PDF-Dateien mit LibreOffice

Für die Konvertierung in PDF-Dateien kann neben Microsoft Office auch die frei verfügbare Software LibreOffice eingesetzt werden. Eine lauffähige Version von LibreOffice ist im Verzeichnis %SF_ROOT_DIR%\System\lib\LibreOfficePortable abgelegt. Im systemweiten Konfigurationseintrag smartFIX / Edoc / LibreOffice / SupportedLibreOfficeExtensions werden die Dateitypen eingetragen, die mit LibreOffice konvertiert werden. Während der Konvertierung wird LibreOffice automatisiert im Hintergrund gestartet und beim Beenden der Komponente sowie im Fehlerfall beendet. Im Fehlerfall wird zusätzlich eine entsprechende Fehlermeldung ausgegeben.

Jede Komponente des Dokumentanalyse-Systems kann maximal einen zugeordneten Prozess von LibreOffice ausführen, wobei mehrere Komponenten gleichzeitig ausgeführt werden können. Einmal gestartete Prozesse werden wiederverwendet. Jeder Prozess belegt etwa 320 MB Arbeitsspeicher. Der gestartete Prozess läuft unter demselben Benutzer wie die Komponente, durch die der Prozess gestartet wurde. Daher hat der Prozess Zugriff auf alle Dateien, auf die auch der Benutzer der Komponente Zugriff hat. Alle Benutzer des Clients auf dem der Prozess läuft, können den Prozess ansprechen und damit Zugriff auf die Dateien erhalten. Die Rechte für den Dateizugriff und die Benutzung der Clients sind entsprechend einzuschränken.

Für jede Komponente wird ein freier Port benötigt. Die Ports werden im Konfigurationseintrag smartFIX / Edoc / LibreOffice / LibreOfficePorts hinterlegt. Für die Kommunikation über das Netzwerk wird das Protokoll TCP verwendet. Aus Sicherheitsgründen ist darauf zu achten, dass die Firewall so eingestellt ist, dass die für LibreOffice konfigurierten Ports nicht nach außen geöffnet sind. Sollte dies nicht geschehen, könnte der Prozess von LibreOffice von allen Clients aus dem Netzwerk verwendet werden.

Bei der Konvertierung von Dateien mit LibreOffice ist Folgendes zu beachten:

- Makros werden immer deaktiviert.
- Eine Anpassung der Seitengröße an eine Druckausgabe erfolgt nicht.
- Initiale werden von LibreOffice nicht erkannt.

Bei der Konvertierung von Textdateien ist Folgendes zu beachten:

- Text aus Kommentaren wird zwar entsprechend in Kommentare konvertiert, allerdings nicht von der OCR weiterverarbeitet.
- LibreOffice konvertiert keine Textlayer aus Textfeldern.
- Bei Bildern mit dazugehörigem Text wird der Text nach der Konvertierung nicht extrahiert.

Bei der Konvertierung von Tabellen ist Folgendes zu beachten:

- Filter werden immer entfernt.
- Gruppen werden ausgeklappt, solange sie nicht als unsichtbar markiert sind.
- Die Größe von Zellen wird an den Inhalt angepasst.

- Spalten, die größer als die druckbare Seitengröße sind, werden auf die Seitengröße begrenzt und umgebrochen. Die Seitengröße wird dabei aus dem Dokument übernommen.
- Bei der Extraktion von Text aus Excel-Dateien wird jede Zelle in eine Zeile übertragen.
- Das Layout von Excel-Dateien kann sich verändern.
- Aus Excel-Dateien wird langer Text in Diagrammen über die Begrenzung der Diagramme hinaus gedruckt.

Bei der Konvertierung von PowerPoint-Dateien ist Folgendes zu beachten:

- Die Titelleiste der PDF-Datei entspricht dem Inhalt des Dokuments, nicht dem Dateinamen.

Konfiguration

Für kundenspezifische Anpassungen stehen die folgenden Konfigurationseinträge zur Verfügung.

- smartFIX / Edoc / LibreOffice / SupportedLibreOfficeExtensions
- smartFIX / Edoc / LibreOffice / LibreOfficePorts
- smartFIX / Edoc / LibreOffice / LibreOfficeFontSubstitutions
- smartFIX / Edoc / LibreOffice / SysTargetPdfFormat
- smartFIX / Edoc / LibreOffice / TargetPdfFormat



4.3.3 Behandlung von Anhängen

Je nach Konfiguration können E-Mail-Anhänge in diversen Formaten verarbeitet werden.

Wenn Anhänge, die selbst eine E-Mail darstellen, verarbeitet werden, ist Folgendes zu beachten:

- EWS, Microsoft Graph
 - Angehängte E-Mails werden wie „normale“ E-Mails behandelt.
 - Enthält eine angehängte E-Mail wiederum eine E-Mail, wird sie nicht verarbeitet, sondern in den Aussteuerungsordner verschoben.
- IMAP
 - Angehängte E-Mails werden in den Aussteuerungsordner verschoben.

Angehängte EML-Dateien werden wie normale E-Mails behandelt. Enthält eine angehängte EML-Datei wiederum eine E-Mail oder EML-Datei als Anhang, wird diese in den Aussteuerungsordner verschoben.

Konfiguration

Für kundenspezifische Anpassungen stehen die folgenden Konfigurationseinträge zur Verfügung.

- smartFIX / Import/Mail / AcceptArchiveSuffixes
- smartFIX / Import/Mail / AcceptSuffixes
- smartFIX / Import/Mail / IgnoreSuffixes



Anhänge im MSG-Format

Falls konfiguriert, können E-Mail-Anhänge im MSG-Format verarbeitet werden.

Ist der Dateityp nicht im Konfigurationseintrag hinterlegt, werden E-Mails mit MSG-Dateien im Anhang in den Aussteuerungsordner verschoben.

Das Verarbeiten von Anhängen in MSG-Dateien ist nicht möglich.

Tipp

MSG-Dateien können von Outlook nicht im PDF-Format gespeichert werden, weshalb diese im Temp-Verzeichnis als HTML-Dateien zwischengespeichert werden. Diese HTML-Dateien werden dann in das PDF-Format konvertiert. Um Probleme beim Zugriff zu vermeiden, sollte die Indizierung auf dem Temp-Verzeichnis ausgeschaltet werden.

Die Indizierung des Temp-Verzeichnisses kann folgendermaßen ausgeschaltet werden:

Öffnen Sie über den Kontextmenüpunkt *Eigenschaften* des Verzeichnisses den Dialog *Eigenschaften von <Verzeichnisname>*.

1. Aktivieren Sie die Registerkarte *Allgemein*.
2. Selektieren Sie im Bereich *Attribute* auf die Schaltfläche *Erweitert...*
Der Dialog *Erweiterte Attribute* wird geöffnet.
3. Deaktivieren Sie im Bereich *Archiv- und Indexattribute* das Kontrollkästchen *Zulassen*, so dass für Dateien in diesem Ordner Inhalte zusätzlich zu Dateieigenschaften indiziert werden.
4. Bestätigen Sie den Dialog mit *OK*.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Import/Mail / AcceptSuffixes

Eingebettete Anhänge von E-Mails im HTML-Format

E-Mails im HTML-Format können einen `<base>`-Tag enthalten, das die URL für externe Quellen, z. B. eingebettete Anhänge enthält, die im HTML-Code verlinkt sind. Diese URL entspricht nicht dem Verzeichnis, in dem eingebettete Anhänge beim Import abgelegt werden. Dadurch werden die Anhänge nicht gefunden und können nicht konvertiert werden. In diesem Fall werden in der konvertierten PDF „Ersatzbilder“ in Form eines Fragezeichens angezeigt.

Geschützte PDF-Anhänge

Geschützte PDFs sind Dateien mit bestimmten Sicherheitseinstellungen, welche die Berechtigungen der Benutzer regeln. Dies können beispielsweise ein Passwortschutz oder verschiedene Berechtigungen zum Bearbeiten oder Drucken der Datei sein. Mit Ausnahme von passwortgeschützten Dateien können diese geschützten PDFs über den *E-Mail-Import* importiert werden.

Beim Import der E-Mails wird der geschützte Anhang erkannt und wenn möglich automatisch über die Funktion `CONVERT_TO_PDF()` in ein ungeschütztes PDF konvertiert. Dabei werden die einzelnen Seiten der geschützten PDF in Bilder konvertiert und zu einer neuen ungeschützten PDF zusammengefasst.

Hinweis

E-Mails mit passwortgeschützten PDF-Anhängen werden in den Aussteuerungsordner verschoben.

Durch die Konvertierung kann sich die Verarbeitungszeit für geschützte PDFs erhöhen.

Platzhalterdokumente

Falls konfiguriert werden E-Mail-Anhänge, die nicht konvertiert werden aber im *Verifier* und im Export zur Verfügung stehen sollen, durch Platzhalterdokumente ersetzt.

Das konfigurierte Platzhalterdokument wird importiert und mit dem Bild-Flag *P* versehen. Die Originaldateien werden in den Ordner OriginalFiles des Stapelverzeichnisses kopiert und können im *Verifier* über den Menüpunkt *Ansicht > Originaldokument anzeigen (Strg+Umschalt+P)* angezeigt werden.

Konfiguration

Für kundenspezifische Anpassungen stehen die folgenden Konfigurationseinträge zur Verfügung.

- smartFIX / Import/Mail / SubstituteSuffixes
- smartFIX / Import/Mail / SubstitutionDocumentPath
- smartFIX / Import/Mail / SubstituteInconvertibleAttachments

4.3.4 Externe Quellen in HTML-Dateien

HTML-Dateien werden beim Import automatisch in das PDF-Format konvertiert.

Hinweis

Zur Konvertierung externer Ressourcen benötigt der Rechner, auf dem der E-Mail-Import läuft, eine Internet-Verbindung.

Falls die HTML-Dokumente externe Quellen beinhalten, z. B. eingebettete Bilder, die sich auf einem Webserver befinden, werden diese standardmäßig beim Import heruntergeladen und konvertiert.

Wenn die externen Quellen innerhalb einer bestimmten Zeitspanne nicht geladen werden können, was beispielsweise der Fall sein kann, wenn die Internetverbindung abbricht, wird das HTML-Dokument ohne die eventuell noch ausstehenden externen Quellen in ein PDF konvertiert. Im *Coordinator* wird eine entsprechende Warnung ausgegeben.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Edoc / HtmlConversion / LoadExternalResources

4.3.5 E-Mails im Aussteuerungsordner

Wenn E-Mails nicht verarbeitet werden können, werden diese in den Aussteuerungsordner verschoben.

Dies ist im Einzelnen der Fall, wenn

- drei Versuche, die E-Mail zu importieren fehlgeschlagen sind (z. B. bei einem überschrittenen Timeout oder bei einem Absturz des *Importer*)
- im Anhang eine nicht zulässige Datei oder eine Datei mit einem nicht unterstützten Format enthalten ist
- der E-Mail-Body aufgrund der Konfiguration unberücksichtigt bleibt und die E-Mail keinen Anhang enthält
- beim Import über IMAP ein eingebetteter Anhang enthalten ist, dessen Dateiname unter Windows nicht gültig ist
- es sich um eine angehängte E-Mail handelt, die als Anhang ebenfalls eine E-Mail enthält
- eine E-Mail einen passwortgeschützten PDF-Anhang enthält
- es sich um einen vom E-Mail-Server automatisch versendeten NDR (Non Delivery Report) handelt
- die E-Mail aufgrund bestimmter Bedingungen ausgefiltert wird. Die Filterung erfolgt mithilfe der *SPL*-Funktion *mimSpamMail()*.
- es sich um eine digital signierte E-Mail handelt (nur IMAP).

Konfiguration

Für kundenspezifische Anpassungen stehen die folgenden Konfigurationseinträge zur Verfügung.

- smartFIX / Import/Mail / MailProfiles
- smartFIX / Import/Mail / CreateClearingComment



4.3.6 Fehlerbehandlung bei der Konvertierung

Bei der PDF-Konvertierung einer Datei über die native Applikation kann es z. B. durch den Indexierungsdienst von Windows zu Fehlern bei Schreibzugriffen auf die Dateien kommen. Da diese Fehler oft nur temporärer Art sind, werden nach einem Fehler weitere Konvertierungsversuche durchgeführt.

Scheitern auch diese Konvertierungsversuche, wird die E-Mail in den Aussteuerungsordner verschoben und eine entsprechende Warnung in die Tabelle SF_LOG der *Result-DB* geschrieben.

4.4 Dokumenttrennung

Jede E-Mail stellt einen Vorgang dar, d. h. die Vorgangstrennung ist extern vorgegeben.

Die Dokumenttrennung wird nur für die E-Mail-Bodys vorgegeben und ist konfigurierbar. Jeder E-Mail-Body bildet ein separates Dokument. Bei den Anhängen wird die Dokumenttrennung vom *Analyser* vorgenommen.

Bezüglich der Manipulation der Dokument- und Seitenreihenfolge per Drag-and-Drop im *Verifier*, Oberfläche *Bildstapel korrigieren* ist zu beachten, dass diese gemischte Dokumenttrennung wie eine extern vorgegebene Dokumenttrennung behandelt wird.

Bei E-Mails, die als Anhang weitere E-Mails enthalten, wird die Dokumenttrennung analog zu dieser Konfiguration verwendet.

Konfiguration



Für kundenspezifische Anpassungen stehen die folgenden Konfigurationseinträge zur Verfügung.

- smartFIX / Import/Mail / DocumentSeparationMode
- Verifier / DocumentImageMatrix / DragAndDropOnGivenDocsSeparation

4.5 Klassifikation des E-Mail-Bodys

In der Regel sind bei E-Mail-Bodys nur die Texte und nicht die Signaturen relevant. Um die Klassifikation und das Training mit dem *AutoClassifier* auf den E-Mail-Text zu beschränken, ist ein Filtermechanismus integriert, über den Signaturen herausgefiltert werden.

Dieser Filtermechanismus ist über *SPL* realisiert und kann kundenspezifisch über verschiedene überschreibbare Funktionen angepasst werden. Das *SPL*-Programm wird im Slot `OnAnalyserAutoClassifyImage()` aufgerufen. Der Filtermechanismus ist aktiv, wenn der *smartblock E-Mail-Import* aktiviert ist.

Die Klassifikation erfolgt bei E-Mail-Bodys immer auf den gefilterten Inhalten aller Seiten.

4.5.1 Verarbeitung bei kurzen Texten

Der Schwärzungsgrad für die Leerseitenerkennung bei der Analyse kann definiert werden.

Je nach Konfiguration werden E-Mail-Bodys, die nur wenig Text beinhalten, nicht übersprungen. Diese E-Mail-Bodys werden konvertiert und auch als relevante Seiten angesehen, wenn der Schwärzungsgrad unter dem definierten liegt.

Eine Seite, die aus einem E-Mail-Body konvertiert wurde, wird nur dann als Leerseite angesehen, wenn der Schwärzungsgrad den Wert „0“ hat, d. h. wenn die Seite komplett leer ist.

Für die Anhänge von E-Mails wird der definierte Schwärzungsgrad für die Leerseitenerkennung berücksichtigt.

Konfiguration



Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Analyser / SkipEmptyPages

5 Konfiguration des E-Mail-Import

In diesem Kapitel sind die Konfigurationsmöglichkeiten des *E-Mail-Import* beschrieben.

5.1 Konfiguration der E-Mail-Profile

Die Konfiguration der E-Mail-Profile kann bei aktiviertem *smartblock E-Mail-Import* über den *Configurator* vorgenommen werden.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Import/Mail / MailProfiles



5.2 Schnittstellen zum E-Mail-Server

Es werden folgende Schnittstellen zur Kommunikation mit E-Mail-Servern durch den *E-Mail-Import* unterstützt:

- EWS (Exchange Web Services)
- IMAP (Internet Message Access Protocol)
- EWS OAuth2 (Exchange Web Services, mit OAuth2 Authentifizierung für Microsoft Office 365 Konten)
- IMAP OAuth2 (Internet Message Access Protocol, mit OAuth2 Authentifizierung)
- Graph User (Microsoft Graph für Microsoft Office 365, angemeldet als Benutzer)
- Graph App (Microsoft Graph für Microsoft Office 365, angemeldet als Anwendung)

Tipp

Für den Import von E-Mails im EML-Format aus einem Dateiverzeichnis steht die Schnittstelle File zur Verfügung.



5.2.1 EWS

EWS ist eine Schnittstelle für den Zugriff auf den Microsoft Exchange Server.

Auf der Seite des Exchange Servers übernimmt der *IIS* (Internet Information Server) des Betriebssystems die Kommunikation mit der *EwsAdapter.dll*.

Tipp

Wenn mehrere *Importer* gleichzeitig E-Mails importieren, wird empfohlen auf dem *IIS* die maximale Anzahl der Arbeitsprozesse für die EWS auf „2“ zu erhöhen. Diese Einstellung kann im *IIS-Manager* über *Anwendungspools* > *MSExchangeServicesAppPool* > *Erweiterte Einstellungen* > *Maximale Anzahl von Arbeitsprozessen* angepasst werden.



5.2.2 EWS OAuth2

EWS OAuth2 ist eine Schnittstelle für den Zugriff auf den Microsoft Exchange Service mit einem Office 365 Konto. Mit OAuth2 kann eine authentifizierte Verbindung aufgebaut werden. Dafür muss auf Microsoft Azure eine Registrierung der Anwendung durchgeführt werden. Danach kann im *Configurator* ein E-Mail-Profil eingerichtet werden. Auf der Konfigurationsseite der E-Mail-Profile im *Configurator* oder mithilfe des SPL-Befehls EWS_AUTHENTICATE_OAUTH2 kann dann ein Token lokal abgespeichert werden.

Beim Sichern des Mandanten oder Erstellen eines Supportarchives werden Token aus Sicherheitsgründen nicht gespeichert. In beiden Fällen muss beim Einspielen der Daten ein neuer Token generiert werden.

Zu beachten ist, dass der Token nach 90 Tagen Inaktivität ungültig wird. In diesem Fall muss ein neuer Token angelegt werden. Mit der Anwendung AzureAD PowerShell können Token widerrufen werden.

5.2.3 IMAP

IMAP ist eine Schnittstelle, über die auch auf andere E-Mail-Server als Microsoft Exchange Server zugegriffen werden kann.

Um IMAP verwenden zu können, muss Chilkat über die mitgelieferte Installationsdatei Chilkat ImapActiveX.msi installiert werden.

Der *E-Mail-Import* greift auf IMAP über die Chilkat.dll zu. Diese DLL stellt dem SPL-basierten *E-Mail-Import* eine COM-Schnittstelle zur Verfügung und kommuniziert ihrerseits über IMAP mit dem E-Mail-Server.

Die Version der Bibliothek Chilkat.dll kann über die überschreibbare Funktion milmapGetChilkatObjectName() kundenspezifisch angepasst werden.

Wenn Sie Lotus Notes als E-Mail-Client verwenden, beachten Sie bitte, dass die Eigenschaft *Sperren von Dokumenten* deaktiviert sein muss, da sie im IMAP-Protokoll nicht vorgesehen ist und vom *E-Mail-Import* nicht unterstützt wird.

5.2.4 IMAP OAuth2

IMAP OAuth2 ist eine Schnittstelle, mit der auch auf andere E-Mail-Server als Microsoft Exchange Server zugegriffen werden kann. Der E-Mail-Import greift auf das IMAP über die Chilkat.dll zu. Durch die DLL wird dem SPL-basierten E-Mail-Import eine COM-Schnittstelle zur Verfügung gestellt, die über IMAP mit dem E-Mail-Server kommuniziert. Die Version der Bibliothek Chilkat.dll kann über die überschreibbare Funktion milmapGetChilkatObjectName() kundenspezifisch angepasst werden.

Mit OAuth2 kann eine authentifizierte Verbindung aufgebaut werden. Dafür muss beim E-Mail-Anbieter eine Registrierung der Anwendung durchgeführt werden. Danach kann im *Configurator* ein E-Mail-Profil eingerichtet werden und auf der Konfigurationsseite der E-Mail-Profile im *Configurator* kann dann ein Token lokal abgespeichert werden.

Beim Sichern des Mandanten oder Erstellen eines Supportarchives werden Token aus Sicherheitsgründen nicht gespeichert. In beiden Fällen muss beim Einspielen der Daten ein neuer Token generiert werden.

Hinweis

Bei der Verwendung von Microsoft Office 365 wird weiterhin die Nutzung der Schnittstelle EWS OAuth2 empfohlen.

Verwandte Themen

E-Mail-Clients 13



5.2.5 Graph User

Graph User ist eine Schnittstelle für den Zugriff auf Konten von Microsoft Office 365 über Microsoft Graph. Die Anmeldung des E-Mail-Profiles erfolgt als Benutzer mit den entsprechenden Rechten.

Die Profile können so eingerichtet werden, dass auf die Postfächer anderer Benutzer zugegriffen werden kann. Für diese Konfiguration müssen zusätzlich Berechtigungen über das Outlook-Konto des Benutzers eingerichtet werden, auf dessen Ordner zugegriffen werden soll. Es ist nötig für jeden Ordner, auf den ein Zugriff durch einen zweiten Benutzer erfolgen soll, diesen zweiten Benutzer über die Eigenschaften des Ordners in den Berechtigungen hinzuzufügen. Als Berechtigungsstufe muss „Veröffentlichender Bearbeiter“ angegeben werden.

Authentifiziert wird die Verbindung über OAuth2. Dafür muss über die Plattform Azure des Drittanbieters Microsoft eine Registrierung der Anwendung durchgeführt werden.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Import/Mail / MailProfiles

Dokumentation

Nähere Informationen können der folgenden Dokumentation entnommen werden.

- *Configurator*



5.2.6 Graph App

Graph App ist eine Schnittstelle für den Zugriff auf Konten von Microsoft Office 365 über Microsoft Graph. Die Anmeldung des E-Mail-Profiles erfolgt als Anwendung mit eigenen Berechtigungen, ohne dass ein Benutzer angemeldet werden muss. Authentifiziert wird die Verbindung über OAuth2. Dafür muss über die Plattform Azure des Drittanbieters Microsoft eine Registrierung der Anwendung durchgeführt werden.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Import/Mail / MailProfiles

Dokumentation

Nähere Informationen können der folgenden Dokumentation entnommen werden.

- *Configurator*



5.3 Weitere Konfigurationsmöglichkeiten

Bei aktiviertem *smartblock E-Mail-Import* stehen weitere mandantenspezifische Konfigurationseinträge zur Verfügung:

- smartFIX / Import/Mail / AcceptArchiveSuffixes
- smartFIX / Import/Mail / AcceptSuffixes
- smartFIX / Import/Mail / CreateClearingComment
- smartFIX / Import/Mail / DocumentSeparationMode

- smartFIX / Import/Mail / HtmlMailFontFamily
- smartFIX / Import/Mail / HtmlMailFontSize
- smartFIX / Import/Mail / IgnoreEmbeddedAttachmentsInTextBody
- smartFIX / Import/Mail / IgnoreSuffixes
- smartFIX / Import/Mail / MailProfiles
- smartFIX / Import/Mail / MaxEmailsPerStack
- smartFIX / Import/Mail / MaxWaitTime
- smartFIX / Import/Mail / ProcessMailBodiesAsText
- smartFIX / Import/Mail / RejectMailsWithEmptyBody
- smartFIX / Import/Mail / SaveEmlFile
- smartFIX / Import/Mail / SetWriteProtectionForOriginalFiles
- smartFIX / Import/Mail / SinglePdfPerMail
- smartFIX / Import/Mail / SubstituteSuffixes
- smartFIX / Import/Mail / SubstitutionDocumentPath
- smartFIX / Import/Mail / SubstituteInconvertibleAttachments

Hinweis

Für den Import von E-Mails im EML-Format aus einem Dateiverzeichnis haben die Konfigurationseinträge smartFIX / Import/Mail / CreateClearingComment und smartFIX / Import/Mail / MaxWaitTime keine Auswirkungen. Für die Schnittstelle IMAP hat der Konfigurationseintrag smartFIX / Import/Mail / CreateClearingComment keine Auswirkung.

Der Konfigurationseintrag smartFIX / Import/Mail / AcceptArchiveSuffixes beinhaltet standardmäßig die folgenden Dateiendungen der Archivformate: 7z, bz2, cab, gz, iso, rar, tar, wim, xz und zip.

Weiterhin steht zur Anpassung des *E-Mail-Import* folgender globaler Konfigurationseintrag zur Verfügung:

- smartFIX / Importer / ImportTimeout

Für die Konfiguration der verwendeten Sicherheitsprotokolle für eine Kommunikation über .NET steht der folgende Konfigurationseintrag zur Verfügung:

- smartFIX / Security / PermittedSecurityProtocols



5.4 Importer

Abhängig von den kundenspezifischen Anforderungen können mehrere *Importer* zur Verarbeitung eingesetzt werden.

- Hochvolumige Postfächer

Für hochvolumige Postfächer können mehrere *Importer* eingesetzt werden, die dann gleichzeitig aus demselben Eingangsordner importieren.

- Mehrere *Importer* auf einem Rechner

Zur Erhöhung des Durchsatzes oder der Ausfallsicherheit können bei EWS, IMAP und Microsoft Graph mehrere *Importer* auf einem Rechner eingesetzt werden.

Durch eine prozessübergreifende Synchronisation der *Importer* wird gewährleistet, dass dieser nicht gleichzeitig Dateien derselben Microsoft Office-Anwendung bearbeitet. Wird durch einen *Importer* z. B. gerade eine Word-Datei bearbeitet, warten weitere *Importer* mit der Bearbeitung von Word-Dateien bis die laufende Konvertierung abgeschlossen ist. Bei der Konvertierung mit LibreOffice entfällt diese Einschränkung. Es können mehrere Dateien mit mehr als einem *Importer* gleichzeitig konvertiert werden.

Dieses Szenario ist dann sinnvoll, wenn der Posteingang unterschiedliche Dateiformate enthält. Werden beispielsweise nur Word-Dateien importiert, sollten die *Importer* auf mehrere Rechner verteilt werden. Bei der Konvertierung mit LibreOffice entfällt diese Einschränkung.

- *Importer* für spezielle E-Mail-Profile

Über den Kommandozeilenparameter „-MailProfiles“ kann ein *Importer* spezifischen E-Mail-Profilen zugeordnet werden. Mehrere E-Mail-Profile werden durch | voneinander getrennt.

- *E-Mail-Import* parallel zu *Standard-XML-Import*

Wenn parallel zum *E-Mail-Import* auch über den *Standard-XML-Import* importiert wird, kann dem *Importer* zur Beschränkung auf den *E-Mail-Import* der Kommandozeilenparameter „-SPLImport MaillImport“ übergeben werden.

6 Kundenspezifische Anpassungen

In diesem Kapitel ist der Ablauf des *SPL*-Programms erläutert und die Optionen für kundenspezifische Anpassungen beschrieben.

6.1 Ablauf des SPL-Programms

Die spezifische Logik des *E-Mail-Import* ist unter anderem in der Datei *MailImport.spl* realisiert. Als Einsprungspunkte dienen die folgenden Funktionen:

- `mimOnImporterImportStack()`
- `mimOnImporterCommitStack()`
- `mimOnImporterRollbackStack()`

`mimOnImporterImportStack()`

Die Funktion wird aufgerufen, wenn ein neuer Stapel importiert werden soll. In der Funktion werden im Wesentlichen folgende Verarbeitungsschritte abgearbeitet:

1. Konsistenzprüfung aller konfigurierten Profile
2. Suche eines Profils mit genügend E-Mails
3. Reservierung der E-Mails in der Datenbanktabelle `SF_MAIL_IMPORT` der *Control-DB*
4. Anlegen eines Stapelverzeichnisses im konfigurierten Austauschverzeichnis
5. Lesen und Konvertieren der E-Mails (E-Mail-Bodys und Anhänge) in das PDF-Format
 - Verschieben von E-Mails in den Aussteuerungsordner, falls sie nicht gelesen werden können
6. Alle Informationen zum Bilden der Stapel werden in einem Dictionary zusammengefasst und an den *Importer* zurückgegeben.

`mimOnImporterCommitStack()`

Die Funktion wird aufgerufen, nachdem der *Importer* einen neuen Stapel gebildet hat. Hier werden vor allem die importierten Mails aus dem Eingangsordner in den Zielordner verschoben und die vom *E-Mail-Import* verwendete Trigger-Datei von `.sf_import_working` nach `.sf_import_finished` umbenannt.

`mimOnImporterRollbackStack()`

Die Funktion wird aufgerufen, wenn das Erzeugen eines neuen Stapels gescheitert ist. Dies ist z. B. dann der Fall, wenn die Funktion `mimOnImporterImportStack()` bei der Konvertierung abgestürzt ist. Hauptaufgaben dieser Funktion sind das Verschieben der problematischen E-Mails in den Aussteuerungsordner und das Löschen des Stapelverzeichnisses.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- `smartFIX / Import / ExchangeDirectory`



6.2 Überschreibbare Funktionen

Zum Anpassen des *E-Mail-Import* an kundenspezifische Erfordernisse stehen *SPL*-Funktionen zur Verfügung, die im Kundenbereich überschrieben werden können. Die Funktionen sind in den nachfolgenden Abschnitten kurz erläutert.

6.2.1 E-Mail-Profile

Die für ein Profil relevanten Konfigurationen werden in einem Dictionary gespeichert. Mit der folgenden Funktion können im Dictionary weitere kundenspezifische Konfigurationen übergeben werden.

- `micAddConfigs(profile, configs)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<profile>` ist das E-Mail-Profil.
- `<configs>` ist ein Dictionary mit kundenspezifischen Konfigurationsmöglichkeiten.

Mit der folgenden Funktion kann das Dictionary für ein Profil ausgelesen werden:

- `micGetProfileSpecificConfigs(profile)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<profile>` ist das E-Mail-Profil.

6.2.2 Version der IMAP-Bibliothek Chilkat.dll

Der *E-Mail-Import* greift auf die Schnittstelle IMAP über die Bibliothek Chilkat.dll zu.

Die Version der Bibliothek Chilkat.dll kann mit der folgenden Funktion angepasst werden:

- `milmapGetChilkatObjectName()`

6.2.3 Aufgabennamen

Aufgabennamen können mit der folgenden Funktion angepasst werden:

- `mimMailStackName(user, inputFolder, category)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<user>` ist der Benutzername.
- `<inputFolder>` ist Eingangsordner.
- `<category>` ist die Eingangskategorie.

Die Funktion gibt den Aufgabennamen zurück. In der Standardimplementierung setzt sich dieser aus dem Präfix „MAIL“ dem Datum und einer fortlaufenden Nummerierung zusammen (MAIL_yyyymmdd_nnnnnn).

Der aktuell gültige Aufgabenname kann mit der Funktion `mimMailStackName()` ausgelesen werden.

6.2.4 Anhänge

Nachfolgend sind die *SPL*-Funktionen zur Behandlung von Anhängen erläutert.

Anlagengröße bei EWS mit Exchange Server 2010

Die maximale zulässige Größe von E-Mail-Anhängen kann mit der folgenden Funktion angepasst werden:

- `muGetMaxAttachmentSize()`

Eingebettete Anhänge von E-Mails im HTML-Format

E-Mails im HTML-Format können einen `<base>`-Tag enthalten, der die URL für externe Quellen, z. B. eingebettete Anhänge enthält, die im HTML-Code verlinkt sind. Diese URL entspricht nicht dem Verzeichnis, in dem eingebettete Anhänge beim Import abgelegt werden. Dadurch werden die Anhänge nicht gefunden und können nicht konvertiert werden. In diesem Fall werden in der konvertierten PDF „Ersatzbilder“ in Form eines Fragezeichens angezeigt.

Um festzulegen, dass der `<base>`-Tag ignoriert werden soll, steht die folgende überschreibbare Funktion zur Verfügung:

- `milgnoreHtmlBaseTags()`

Wenn die Funktion den Wert `TRUE` hat, werden die `<base>`-Tags beim Import nicht berücksichtigt.

Geschützte PDF-Anhänge

Zum Konvertieren geschützter PDFs steht die folgende überschreibbare Funktion zur Verfügung:

- `mimConvertSecuredPdf(sourceFileName, targetFileName, append, dpi)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<sourceFileName>` ist der Dateiname der geschützten Quelldatei.
- `<targetFileName>` ist der Dateiname der Zieldatei.
- `<append>` gibt an, ob eine bereits vorhandene Zieldatei erweitert (`TRUE`) oder ersetzt werden soll (`FALSE`).
- `<dpi>` ist die Auflösung der Zieldatei `<tagetFileName>`.

Die Funktion wird aufgerufen, wenn es sich bei einem E-Mail-Anhang um eine geschützte PDF handelt (`IS_SECURED_PDF(path)`).

Bei passwortgeschützten PDF-Anhängen wird eine Fehlermeldung ausgegeben und die betreffende E-Mail wird in den Aussteuerungsordner verschoben.

Zu beachten ist, dass die Verarbeitungszeit geschützter PDFs erheblich höher ist als die von ungeschützten PDFs, da diese mittels Rasterisierung in ein Bitmap-Format konvertiert werden.

Ignorierte Anhänge

Zur kundenspezifischen Weiterverarbeitung ignoriierter Anhänge steht die folgende überschreibbare Funktion zur Verfügung:

- `mimHandleIgnoredFile(convertedImages, attachmentName, mailIdx)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<convertedImages>` ist ein Dictionary mit Informationen zu den erzeugten Bildern und PDFs der E-Mail, die sich aktuell in Verarbeitung befindet.
- `<attachmentName>` ist der Name des Anhangs, der anhand der Dateiendung als „zu ignorieren“ erkannt wurde.
- `<mailIdx>` ist eine fortlaufende Nummerierung der E-Mails innerhalb eines Importvorgangs.

Die Funktion wird für jeden Anhang aufgerufen, der, je nach Konfiguration, als „zu ignorieren“ erkannt wird.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- `smartFIX / Import/Mail / IgnoreSuffixes`



Platzhalterdokumente

Zum Anpassen des Verhaltens beim Ersetzen bestimmter Anhänge durch Platzhalterdokumente stehen die folgenden überschreibbaren Funktionen zur Verfügung:

- `mimIsFileToSubstitute(name)`
- `mimIsFileToAccept(name)`
- `mimIsFileToIgnore(name)`

Der Parameter der Funktionen hat folgende Bedeutung:

- `<name>` ist der Name des Anhangs.

Die Funktion `mimIsFileToSubstitute(name)` ermittelt, ob der Anhang `<name>` durch ein Platzhalterdokument ersetzt werden soll. Die Funktionen `mimIsFileToAccept(name)` und `mimIsFileToIgnore(name)` ermitteln, ob der Anhang zu verarbeiten oder zu ignorieren ist.

Reihenfolge der Anhänge

Die Anhänge einer E-Mail werden standardmäßig in der Reihenfolge importiert, in der sie auf dem E-Mail-Server vorliegen.

Um die Sortierung der Anhänge anzupassen, steht die folgende überschreibbare Funktion zur Verfügung:

- `muSortAttachments(attachments)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<attachments>` ist ein Vektor mit Informationen zu den einzelnen Anhängen. Der Aufbau des Vektors entspricht dem des Elements 'attachments' im Rückgabe-Dictionary der *SPL*-Funktion `EWS_LIST`.

6.2.5 Aussteuerung

Nachfolgend sind die *SPL*-Funktionen zur Aussteuerung von E-Mails beschrieben.

Aussteuerungskriterien

Zum Anpassen der Kriterien, unter denen eine E-Mail ausgesteuert werden soll, steht die folgende überschreibbare Funktion zur Verfügung:

- `mimMailHasToBeMovedToClearing(mailDict)`

Der Parameter der Funktion hat folgende Bedeutung:

- `<mailDict>` ist ein Dictionary mit den Informationen der E-Mail. Der Aufbau des Dictionary entspricht dem Rückgabewert der *SPL*-Funktion `EWS_LIST`.

Wenn der Rückgabewert der Funktion `TRUE` ist, wird die E-Mail nicht importiert, sondern in den Aussteuerungsordner verschoben.

E-Mails mit leerem E-Mail-Body

Zum Aussteuern von E-Mails mit leerem E-Mail-Body können die beiden überschreibbaren Funktionen `mimMailBodyIsInvalid(mail)` und `micRejectMailsWithEmptyBody(profile)` genutzt werden.

Mit `micRejectMailsWithEmptyBody(profile)` kann der Wert des Konfigurationseintrags `smartFIX / Import/Mail / RejectMailsWithEmptyBody` zurückgegeben werden.

Zur Identifikation von E-Mails mit leerem E-Mail-Body, die ausgesteuert werden sollen, steht die folgende überschreibbare Funktion zur Verfügung:

- `mimMailBodyIsInvalid(mail)`

Der Parameter der Funktion hat folgende Bedeutung:

- `<mail>` ist ein Dictionary mit den Informationen der E-Mail.

Die Funktion gibt `TRUE` zurück, wenn die E-Mail nicht im `MSG`-Format vorliegt, der E-Mail-Body leer ist und die Funktion `micRejectMailsWithEmptyBody(profile)` den Wert `TRUE` hat.

Fehlgeschlagener Import

E-Mails werden standardmäßig ausgesteuert, wenn drei Versuche sie zu importieren (z. B. bei einem überschrittenen Timeout oder bei einem Absturz des *Importer*) fehlgeschlagen sind. Die Anzahl der fehlgeschlagenen Importversuche wird in die Tabelle `SF_MAIL_TRIES` der *Control-DB* geschrieben.

Zum Anpassen der Anzahl der maximal zulässigen Importversuche steht die folgende überschreibbare Funktion zur Verfügung:

- `mimMaxTries()`

Nicht unterstützte Dateiformate

Zum Aussteuern von Dateien, die in einem nicht unterstützten Format vorliegen, steht die folgende Funktion zur Verfügung:

- `mimIsUnsupportedFileFormat(path)`

Der Parameter der Funktion hat folgende Bedeutung:

- `<path>` ist der Dateipfad.

Die Funktion wird vor der Konvertierung zu PDF aufgerufen und entscheidet anhand des übergebenen Pfades und des Dateiinhaltes, ob die Datei in einem Format vorliegt, das vom System verarbeitet werden kann. Ist dies nicht der Fall, wird die Datei ausgesteuert.

Non Delivery Reports

Wenn eine E-Mail nicht zugestellt werden kann, wird vom E-Mail-Server automatisch eine Antwort in Form eines Non Delivery Report (NDR) verschickt.

NDRs können in zwei verschiedenen Ausprägungen auftreten:

- Spezielle Statusmeldung entsprechend dem Standard RFC 3461
Diese Statusmeldungen werden vom *E-Mail-Import* standardmäßig ausgesteuert.
- Standard-E-Mail mit entsprechenden Fehlertext

Zum Anpassen dieses Verhaltens steht die folgende überschreibbare Funktion zur Verfügung:

- `mimIsInvalidNonDeliveryReport(mail)`

Der Parameter der Funktion hat folgende Bedeutung:

- `<mail>` ist ein Dictionary mit den Informationen der E-Mail.
Eines der Elemente des Dictionarys ist 'messageClass'. Das Element kann die Werte 'Email', 'NonDeliveryReport' und 'Other' haben.

Die Funktion gibt TRUE zurück, wenn es sich bei der E-Mail um einen NDR handelt, der ausgesteuert werden soll.

Protokollierung ausgesteuerter E-Mails

Für den Zugriff auf Kommentare ausgesteuerter E-Mails steht die folgende Funktion zur Verfügung:

- `miHandleClearingComment(comment, mail)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<comment>` ist der Kommentartext, der den Grund für das Verschieben angibt.
- `<mail>` ist ein Dictionary mit den Informationen der E-Mail.

Die Funktion wird aufgerufen, wenn eine E-Mail in den Aussteuerungsordner verschoben wird.

Spam-Filter

Mit der folgenden Funktion kann ein Spam-Filter eingerichtet werden:

- `mimIsSpamMail(mailDict)`

Der Parameter der Funktion hat folgende Bedeutung:

- `<mailDict>` ist ein Dictionary mit den Informationen der E-Mail. Der Aufbau des Dictionary entspricht dem Rückgabewert der *SPL*-Funktion `EWS_LIST`.

Die Funktion wird für jede E-Mail aufgerufen und gibt TRUE zurück, wenn die E-Mail als Spam-Mail identifiziert wurde. E-Mails, die aufgrund der angegebenen Kriterien als Spam identifiziert werden, verschiebt der *E-Mail-Import* in den Aussteuerungsordner.

In der Standardimplementierung findet keine Filterung statt.

6.2.6 Dateinamen

Zum Anpassen der Namen der zu verarbeitenden Dateien stehen folgende überschreibbare Funktionen zur Verfügung:

- `mimGetImageName(mailIdx, nbImages, fileName)`
- `mimMaxOriginalFileName()`
- `mimNameOfConvertedFile(fileName)`
- `mimIsMailBody(DICT('EdocPath -> edocPath, 'Flags' -> flags))`

Hinweis

Da diese Funktionen in Abhängigkeit zueinander stehen, müssen bei kundenspezifischen Anpassungen gegebenenfalls alle Funktionen überschrieben werden.

`mimGetImageName(mailIdx, nbImages, fileName)`

Die Funktion legt eindeutige Namen für die Originaldateien (E-Mail-Body und Anhänge) fest.

Die Parameter der Funktion haben folgende Bedeutung:

- `<mailIdx>` ist eine fortlaufende Nummerierung der E-Mails innerhalb eines Importvorgangs.
- `<nbImages>` ist eine eindeutige Nummerierung der Originaldateien innerhalb einer E-Mail.
- `<fileName>` ist ein String zum Bilden des Namens (z. B. Mailbody.<Originaler Name des Anhangs>).

In der Standardimplementierung werden die Originaldateien mit ihren Originalnamen in folgendem Verzeichnis abgelegt:

`<Austauschverzeichnis>\<MAIL_<yyyymmdd>_<Fortlaufende Nummerierung>\OriginalFiles`

`mimMaxOriginalFileName()`

Mit dieser Funktion kann die Länge der generierten Originaldateinamen angepasst werden. In der Standardimplementierung werden 48 Zeichen der Originaldateien der E-Mail für die Namensbildung zugrunde gelegt.

Tipp

Originaldateinamen sollten möglichst kurz gehalten werden, da diese in der Statusleiste des *Verifier* angezeigt werden.

Beim Ändern der Zeichenlänge ist Folgendes zu beachten:

- Die Dateinamenlänge von Bildern in der Datenbanktabelle SF_IMAGES (Spalte IMAGE_ID) auf 120 Zeichen beschränkt.
- Für die verschiedenen Optionen der Dateierweiterungen, z. B. bei Multipage-Dateien (':ddd') müssen insgesamt 12 Zeichen als reserviert angesehen werden.

Hinweis

Die Anzahl der Zeichen kann maximal auf 108 erhöht werden.

`mimNameOfConvertedFile(fileName)`

Die Funktion generiert Namen für die konvertierten PDFs.

Der Parameter der Funktion hat folgende Bedeutung:

- `<fileName>` ist der über `mimImageGetName` festgelegte Name.

Die Vergabe des Dateinamens ist konfigurierbar.

mimIsMailBody(DICT('EdocPath' -> edocPath, 'Flags' -> flags))

Mit der Funktion wird geprüft, ob es sich bei einem Dateinamen um einen E-Mail-Body handelt.

Der Parameter der Funktion ist ein Dictionary mit den beiden folgenden Elementen:

- 'EdocPath' ist der Pfad zur Originaldatei des E-Mail-Bodys.
- 'Flags' ist ein SET mit Bild-Flags.

Mögliche Werte sind: 'MailBody' und 'Placeholder'

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Import/Mail / SinglePdfPerMail

**6.2.7 E-Mail-Kopfdaten**

Zum Erzeugen der Kopfdaten einer E-Mail stehen folgende überschreibbare Funktionen zur Verfügung:

- mimCreateMailHeader(mailDict)
- mimCreateHtmlMailHeader(mailDict)

Der Parameter der Funktion hat folgende Bedeutung:

- <mailDict> ist ein Dictionary mit den Informationen der E-Mail. Der Aufbau des Dictionary entspricht dem Rückgabewert der *SPL*-Funktion EWS_LIST.

Die Funktion mimCreateHtmlMailHeader(mailDict) gibt einen *SPL*-String zurück, der mit „<html>“ eingeleitet und mit „</html>“ beendet wird.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- smartFIX / Import/Mail / ProcessMailBodiesAsText

**6.2.8 Externe Vorgangs-ID**

Zum Anpassen der Vorgangs-ID steht folgende überschreibbare Funktion zur Verfügung:

- mimCreateProcId(mailIdx, mailDict)

Die Parameter der Funktion haben folgende Bedeutung:

- <mailIdx> ist eine fortlaufende Nummerierung der E-Mails innerhalb eines Importvorgangs.
- <mailDict> ist ein Dictionary mit den Informationen der E-Mail. Der Aufbau des Dictionary entspricht dem Rückgabewert der *SPL*-Funktion EWS_LIST.

Standardmäßig wird aus <mailIdx> eine vierstellige Vorgangs-ID erzeugt. Hat <mailIdx> z. B. den Wert „34“, wird die Vorgangs-ID „0034“ generiert. Die Funktion wird für jede E-Mail aufgerufen, sobald diese konvertiert wurde.

6.2.9 Felder

Felder können über die folgende Funktion vorbelegt werden:

- `mimSetFieldImport(importedFields, scope, infoDict)`

Die Parameter der Funktion haben folgende Bedeutung:

- `<importedFields>` ist ein Vektor, in dem alle zu importierenden Felder gesammelt werden.
- `<scope>` gibt den Gültigkeitsbereich des Feldes an ('Process', 'Document' oder 'Stack').
- `<infoDict>` stellt Informationen zur Verfügung, die zur Vorbelegung genutzt werden können. Die Informationen sind abhängig von dem Wert, den der Parameter `<scope>` besitzt:

Wert 'Stack'

```

DICT('StackId'      -> stackId,
     'User'         -> user,
     'InputFolder'  -> inputFolder
    );

```

Wert 'Process'

```

DICT('StackId'      -> stackId,
     'User'         -> user,
     'InputFolder'  -> inputFolder,
     'ProcID'       -> processId,
     'Mail'         -> DICT('id' -> i, 'date' -> d, ...),
    );

```

Wert 'Document'

```

DICT('StackId'      -> stackId,
     'InputFolder'  -> inputFolder,
     'ProcID'       -> processId,
     'Mail'         -> DICT('id' -> i, 'date' -> d, ...),
     'DocID'        -> documentId,
     'IsAttachment' -> isAttachment,
    );

```

Zum Einfügen eines Feldimports in das Dictionary `<importedFields>` steht die folgende Funktion zur Verfügung:

- `mimSetField(importedFields, scope, id, name, value, rating)`

Hinweis

Die Länge des Feldwertes darf 250 Zeichen nicht überschreiten.

Neben dem Dictionary `<importedFields>` und dem Wert `<scope>` müssen die zum Scope gehörige ID, der Feldname, der Feldwert, und das Rating als Parameter übergeben werden.





Beispiel

```
FUNCTION mimSetFieldImport(importedFields, scope, infoDict)
{
  IF scope = 'Stack' THEN
  {
    mimSetField(importedFields, scope, '', 'Field1', infoDict['MessageStore'],
    'ok');
  }
  IF scope = 'Process' THEN
  {
    mimSetField(importedFields, scope, infoDict['ProcID'], 'Field2',
    infoDict['Mail']['subject'], 'ok');
  }
  IF scope = 'Document' THEN
  {
    mimSetField(importedFields, scope, infoDict['DocID'], 'Field3',
    infoDict['Mail']['subject'], 'ok');
  }
}
```

6.2.10 Filter für Klassifikation des E-Mail-Bodys

Bei der Klassifikation von E-Mail-Bodys werden vor der Klassifikation Signaturen herausgefiltert.

Realisiert ist der Filtermechanismus über die Bibliothek MailDissection.spl, die im Slot OnAnalyserAutoClassifyImage() aufgerufen wird.

Ablauf der Analyse bei der Vorfilterung

Bei der Vorfilterung der für die Klassifikation relevanten Inhalte der E-Mail-Bodys werden bei der Analyse im Wesentlichen folgende Schritte durchlaufen:

1. Der *Analyser* startet die Verarbeitung eines E-Mail-Stapels.
2. Bei einer Datei des Stapels erkennt der *Analyser*, dass diese mit dem *AutoClassifier* zu klassifizieren ist.
3. Der *Analyser* ruft den *SPL*-Slot OnAnalyserAutoClassifyImage() auf und übergibt dem Slot die Image-IDs von Dateien mit identischer DocID.
4. Der Slot prüft, ob es sich um einen E-Mail-Body handelt (z. B. anhand des ImageFlags „MailBody“):
 - Handelt es sich um einen E-Mail-Body, ermittelt der Slot den für die Klassifikation relevanten Text und liefert ihn an den *Analyser* zurück.

Mit diesem Text ruft der *Analyser* den *AutoClassifier* auf.

Der *AutoClassifier* ermittelt anhand des Textes die Dokumentklasse und wendet diese auf alle Seiten des Dokuments an.

Sollte keine Klassifikation möglich sein, erhält die Datei die Dokumentklasse „Unklassifiziert“.

- Handelt es sich um einen E-Mail-Body, der allerdings über keinen brauchbaren Text verfügt, liefert der Slot einen „leeren“ Text zurück.

Der *Analyser* klassifiziert die Datei auf die Klasse „Unklassifiziert“.

- Handelt es sich um keinen E-Mail-Body, gibt der Slot diese Information an den *Analyser* zurück, der die Datei ohne Berücksichtigung des Slots analysiert.

OnAnalyserAutoClassifyImage

Die Slot-Funktion wird zur Aufbereitung des Dokumentinhaltes für die Klassifikation über *AutoClassifier* genutzt.

Wenn über den *AutoClassifier* klassifiziert wird, übergibt der *Analyser* der Slot-Funktion die Image-IDs von Dateien mit identischer Dokument-ID.

Die Slot-Funktion liefert ein Dictionary mit den Elementen 'Action' und 'Text' zurück.

- 'Action'

Mögliche Werte sind:

- 'Ignored': Der Text wurde nicht verändert.
- 'Filtered': Der Text wurde verändert. Die Klassifikation soll nur auf dem veränderten Text erfolgen

- 'Text'

Veränderter Text, der zur Klassifikation genutzt werden soll

Überschreibbare Funktionen zum Vorfiltern

Zum Anpassen des Filtermechanismus stehen verschiedene überschreibbare Funktionen sowie ein Thesaurus mit internationalisierbaren Schlüsselwörtern zur Verfügung.

Einige Thesaurusbegriffe und -synonyme sind bereits in der Datei System/Product/ThesaurusMail.tdb hinterlegt und können im Kundenbereich entsprechend angepasst und erweitert werden. Weiterhin können mit verschiedenen überschreibbaren Funktionen die Gewichte und die Suchbereiche für die Synonyme angepasst werden. Die Funktionen hierfür werden in der Funktion SEARCH_THES übergeben.

Die überschreibbaren Funktionen stehen in der Bibliothek MailDissection.spl zur Verfügung:

- mdProcessEmail(imagelds)
Haupteinstiegspunkt für die Aufbereitung der E-Mails
- mdExtractTextFromMail(imagelds)
Liefert den extrahierten Text aus dem E-Mail-Body zurück
- mdLineDelimiter()
Trennzeichen zwischen zurückgelieferten Zeilen
- Gewichtung und Suchbereiche der Thesaurussynonyme:
 - mdThesSubjectRating()
Gewichtung der Thesaurussynonyme des Thesaurusbegriffs „Subject“
 - mdThesNonSubjectRating()
Gewichtung der Thesaurussynonyme des Thesaurusbegriffs „nonSubject“
 - mdThesGreetingsRating()

Gewichtung der Thesaurussynonyme des Thesaurusbegriffs „Greetings“

- mdThesNonGreetingsRating()

Gewichtung der Thesaurussynonyme des Thesaurusbegriffs „nonGreetings“

- mdGreetingLeftMargin() und mdGreetingRightMargin()

Suchbereich für die Thesaurussynonyme des Thesaurusbegriffs „Greetings“

- mdSubjectLeftMargin() und mdSubjectRightMargin()

Suchbereich der Thesaurussynonyme des Thesaurusbegriffs „Subject“

6.2.11 Konfigurationen

Für komplexe Konfigurationen stehen verschiedene *SPL*-Funktionen zur Verfügung. In der Standardimplementierung geben die Funktionen den jeweiligen Wert des Konfigurationseintrages zurück.

micMaxEmailsPerStack(profile)

- smartFIX / Import/Mail / MaxEmailsPerStack

Maximale Anzahl an E-Mails pro Stapel

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micMaxWaitTime(profile)

- smartFIX / Import/Mail / MaxWaitTime

Zeitüberschreitung für die Verweildauer einer E-Mail im Postfach

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micIgnoreSuffixes(profile)

- smartFIX / Import/Mail / IgnoreSuffixes

Dateitypen, die nicht importiert werden sollen

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micAcceptSuffixes(profile)

- smartFIX / Import/Mail / AcceptSuffixes

Dateitypen, die importiert werden sollen

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micSubstituteSuffixes(profile)

- smartFIX / Import/Mail / SubstituteSuffixes

Dateitypen, die durch ein Platzhalterdokument ersetzt werden sollen

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micSubstitutionDocumentPath(profile, originalName, attachment)

- smartFIX / Import/Mail / SubstitutionDocumentPath

<profile> ist das E-Mail-Profil.

<originalName> ist der Dateiname des Platzhalterdokuments.

<attachment> ist die angehängte Datei.

Die Parameter der Funktionen haben folgende Bedeutung:

- <profile> ist das E-Mail-Profil.
- <originalName> ist der Name der Originaldatei.

micProcessMailBodiesAsText(profile)

- smartFIX / Import/Mail / ProcessMailBodiesAsText

Importformat von E-Mail-Bodys

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micHtmlMailFontSize()

- smartFIX / Import/Mail / HtmlMailFontSize

Schriftgröße

micHtmlMailFontFamily

- smartFIX / Import/Mail / HtmlMailFontFamily

Schriftart

micIgnoreInlineAttachmentsInTextBody(profile)

- smartFIX / Import/Mail / IgnoreEmbeddedAttachmentsInTextBody

Behandlung eingebetteter Anhänge in E-Mail-Bodys

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micRejectMailsWithEmptyBody(profile)

- smartFIX / Import/Mail / RejectMailsWithEmptyBody

Aussteuerung von E-Mails mit leeren E-Mail-Bodys

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micCreateClearingComment(profile)

- smartFIX / Import/Mail / CreateClearingComment

Kommentar für E-Mails, die in den Aussteuerungsordner verschoben werden

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micSinglePdfPerMail(profile)

- smartFIX / Import/Mail / SinglePdfPerMail

Konvertierung des E-Mail-Inhalts in eine oder mehrere PDFs

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micExchangeDirectory(profile)

- smartFIX / Import / ExchangeDirectory

Konfiguration des Austauschverzeichnisses

Der Parameter der Funktion hat folgende Bedeutung:

<profile> ist das E-Mail-Profil.

micDpi()

- smartFIX / KnowledgeDB / SystemDpi

Konfiguration der Auflösung

micSaveEmlFile()

- smartFIX / Import/Mail / SaveEmlFile

Speichern von E-Mails als EML-Dateien im Stapelverzeichnis

6.2.12 Aufgabenattribute

Aufgabenattribute können über die folgende Funktion vorbelegt werden:

- mimStackAttributes(user, inputFolder)

Die Parameter der Funktionen haben folgende Bedeutung:

- <user> ist der Benutzername.
- <inputFolder> ist der Eingangsordner.

Die Funktion gibt einen Vektor mit den standardmäßigen Aufgabenattributen des E-Mail-Stapels zurück. In der Standardimplementierung sind keine Aufgabenattribute vorbelegt, allerdings wird das Aufgabenattribut \$StackDir automatisch gesetzt, falls es nicht in der eventuell überschriebenen Funktion gesetzt wurde. \$StackDir wird vom *CoordinatorKernel* zum Löschen von Aufgabenverzeichnissen benötigt.

Die überschriebene Funktion muss einen Vektor zurückliefern, der die vorbelegten Aufgabenattribute enthält. Der Vektor hat folgende Syntax:

```
VECTOR( DICT('Name' ->name_1, 'Value'->value_1),
        ...,
        DICT('Name' ->name_n, 'Value'->value_n)
);
```

6.2.13 Steuerdateinamen

Zum Anpassen der Suffixe der Steuerdateien stehen folgende überschreibbare Funktionen zur Verfügung:

- mimWorkingTriggerFileSuffix()
- mimFinishedTriggerFileSuffix()

Die beiden Funktionen liefern die gewünschten Suffixe für die Steuerdateien des *E-Mail-Import*. In der Standardimplementierung besitzen die Steuerdateien die Suffixe „sf_import_working“ und „sf_import_finished“.

6.2.14 EML-Dateien

Falls konfiguriert, werden importierte E-Mails als EML-Dateien gespeichert.

Zum Anpassen des Speicherortes steht die folgende überschreibbare Funktion zur Verfügung:

- `mimGetEmlFilePath()`

Die Funktion liefert den Speicherort und den Dateinamen für die EML-Dateien zurück. In der Standardimplementierung werden die EML-Dateien im Verzeichnis `ExchangeDir\StackId\OriginalFiles` mit dem Dateinamen „Mail_Original.eml“ gespeichert.

Mehrere E-Mails pro Bildstapel werden über die Funktion `mimGetUniqueFileName(basePath, fileName, fileExtensions)` benannt.

Konfiguration

Für kundenspezifische Anpassungen steht der folgende Konfigurationseintrag zur Verfügung.

- `smartFIX / Import/Mail / SaveEmlFile`



6.2.15 Übernahme der Empfänger in die Kopfdaten einer E-Mail

Um zu konfigurieren, ob die Empfänger im Feld Cc in die Kopfdaten einer E-Mail übernommen werden, steht die folgende überschreibbare Funktion zur Verfügung:

- `mimIsCcRequired()`

Beispiel

```
FUNCTION mimIsCcRequired()  
{  
    RETURN TRUE;  
}
```



7 Glossar

Dieses Kapitel gibt einen Überblick über spezifische Bezeichnungen und Begriffe.

7.1 Bezeichnungen und Erklärungen

Nachfolgend finden Sie Erklärungen zu spezifischen Bezeichnungen und Begriffen, die in dieser Dokumentation verwendet werden.

Activator

Der *Activator* ist eine Systemkomponente. Er hat die Aufgabe, Programme auf dem lokalen Rechner zu starten und zu beenden. Der *Activator* muss auf jedem Rechner laufen, auf dem der *CoordinatorKernel* oder eine andere Client-Server-Komponente ein Programm starten soll.

Analyser

Der *Analyser* ist eine Systemkomponente. Auf Basis der im *DocumentManager* definierten Dokumentklassen klassifiziert er Dokumente, extrahiert die gewünschten Informationen und führt eine interne Prüfung und Korrektur durch.

Dokument

Ein Dokument ist ein elektronisches Abbild eines Blatts, z. B. ein eingescanntes Blatt Papier.

Aufgabe

Eine Aufgabe ist eine Menge von elektronischen Dokumenten.

Aufgabenzustand

Der Bildstapelzustand beschreibt den nächsten Verarbeitungsschritt, den eine Aufgabe im System durchlaufen soll.

COM

COM (Component Object Model) ist eine von Microsoft entwickelte Spezifikation, welche die Entwicklung von Softwarekomponenten beschreibt, die sich in Programme einbauen oder sich zum Zweck einer vergrößerten Funktionalität auch bestehenden Programmen hinzufügen lassen.

Configurator

Der *Configurator* ist eine Systemkomponente. Er dient der Konfiguration mehrerer Bereiche wie des Systems, der Komponenten und Komponententypen, des Workflows und der Benutzerverwaltung.

Coordinator

Der *Coordinator* ist eine Komponente. Er stellt Administrationsfunktionalitäten für den Client-Server-Betrieb des Systems zur Verfügung. Dieser bietet eine Laufzeitüberwachung der übrigen Komponenten und zeigt deren Zustände und Meldungen an. Er ist in zwei Teile gegliedert: den *CoordinatorKernel* und die Oberfläche *Coordinator*.

Control-DB

Die *Control-DB* ist eine systeminterne Datenbank. Sie enthält und verwaltet Informationen über die momentan im System befindlichen Aufgaben, Vorgänge und Dokumente.

DocumentManager

Der *DocumentManager* ist eine Systemkomponente. Er stellt Funktionen zum Definieren, Testen und Optimieren neuer Dokumentklassen bereit. Für jede Dokumentklasse werden dabei Strukturen zur Klassifikation, Informationsextraktion sowie zur automatischen Prüfung und Korrektur angelegt.

Dokument

Ein Dokument besteht aus einer oder mehreren Seiten, die inhaltlich zusammengehören.

Dokumentklasse

Eine Dokumentklasse beschreibt die Klassifikations- und Informationsstruktur gleichartiger Dokumente. Dokumentklassen werden im *DocumentManager* definiert. In der Klassifikationsphase ordnet der *Analyser* Dokumente der Dokumentklasse zu. Anschließend werden anhand der Informationsstrukturen die Informationen aus dem Dokument extrahiert.

Feld

Ein Feld ist ein Bereich in einem Dokument, aus dem bestimmte Informationen extrahiert werden.

Importer

Der *Importer* ist eine Systemkomponente. Er liest gescannte Aufgaben z. B. aus einem Dateisystem oder einem Archivsystem, legt sie auf dem Server ab und stellt Informationen über die Aufgabe in der Datenbank zur Verfügung.

Klassifikation

Klassifikation ist der Schritt der Analyse, bei dem ein Dokument einer oder mehreren Dokumentklassen zugeordnet wird. Hierfür suchen die Klassifikatoren *FormClass*, *PatternClass*, *AutoClassifier* und *PageSizeClass* nach Klassifikationsmerkmalen im Dokument, die einer definierten Dokumentklasse entsprechen.

Result-DB

Die *Result-DB* ist eine systeminterne Datenbank. Sie wird durch den *Exporter* mit Statistikinformationen gefüllt. Weiterhin werden hier die Log-Ausgaben gespeichert, die im *Coordinator* angezeigt werden.

SPL

SPL (smart FIX Programming Language) ist eine integrierte Programmiersprache, mit der Abläufe, die sich nicht über Feldverbünde abbilden lassen, realisiert werden können.

Vorgang

Ein Vorgang ist eine Menge von Dokumenten, die inhaltlich zusammengehören. z. B. ein Anschreiben mit Anlagen.

Vorgangs-ID

Die Vorgangs-ID ist der eindeutige Bezeichner eines Vorgangs innerhalb einer Aufgabe.