

Technische Dokumentation

SEPPmail Outlook Add-In v1.6.0

In diesem Dokument wird dargelegt, wie das SEPPmail Outlook Add-in funktioniert, und welche Einstellungen vorgenommen werden können.

Inhalt

| | | |
|-----|---|----|
| 1 | Einleitung..... | 3 |
| 2 | System-Anforderungen | 4 |
| 3 | Installation | 5 |
| 3.1 | Installation mit User-Interface..... | 5 |
| 3.2 | Installation ohne User-Interface | 7 |
| 4 | Registry | 10 |
| 4.1 | Local Machine..... | 10 |
| 4.2 | Current User | 11 |
| 5 | Versand von Mails..... | 12 |
| 6 | Interne Verschlüsselung..... | 12 |
| 7 | Berechtigungssteuerung per LDAP..... | 12 |
| 8 | Automatische Verarbeitung von E-Mails durch das Add-in..... | 14 |

1 Einleitung

Das SEPPmail Outlook Add-In (Add-In) kann auf PC-Systemen mit Microsoft Outlook installiert werden. Die Installation kann silent oder mit Benutzeroberfläche erfolgen. Je nach gewählter Installation stehen unterschiedliche Einstellungen (Parameter) zur Verfügung, um die Funktionalität des Add-Ins zu beeinflussen.

Das Add-in selbst stellt in jeder Art von Mail-Fenster (zum Verfassen einer E-Mail) Buttons zur Verfügung. Abhängig von den bei der Installation gewählten Einstellungen sind es unterschiedlich viele Buttons, mit unterschiedlicher Standard-Einstellung (gedrückt / nicht gedrückt).

Die Zustände der Haupt-Buttons beim späteren Versenden der Mail werden in Form von Steuer-Informationen in die Mail integriert.

Ein (optionaler) Button ruft eine Hilfe-Seite im Standard-Browser auf.

Durch eine (optionale) Einstellung kann eine Warnung beim Versenden von unverschlüsselten und unsignierten Mails erscheinen.

Die Anwendung ist mehrsprachig und passt sich der Sprache der Outlook-Oberfläche an. Ist diese nicht verfügbar, wird Englisch als Sprache für das Add-in festgelegt.

Im Folgenden werden technische Details zu System-Anforderungen, zur Installation, zu den Abläufen in der Registry und zum Versand von Mails beschrieben.

2 System-Anforderungen

Microsoft Windows:

Eines der folgenden Betriebssysteme:

Windows Vista, Windows 7, 8 und 10 (32 bit und 64 bit) oder Windows Terminal Server

Microsoft Outlook:

Eine der folgenden Outlook Versionen:

Outlook 2007, Outlook 2010 (32 bit und 64 bit), Outlook 2013 (32 bit und 64 bit)

.NET Framework:

Das .NET Framework muss in der Version 4.0 Client Profile oder neuer vorhanden sein. Fehlt dieses, versucht die Installationsroutine diese Komponente automatisch aus dem Internet zu beziehen und zu installieren.

3 Installation

Die Installation besteht aus zwei Dateien:

Setup.exe

- Ist erforderlich um auf Windows Vista, Windows 7 und Windows 8, bei eingeschaltetem UAC, per Rechtsklick „Als Administrator“ auswählen zu können.
- Prüft vor dem Ausführen der .msi-Datei ob die Voraussetzungen für die Installation (z.B. NET Framework) vorhanden sind.

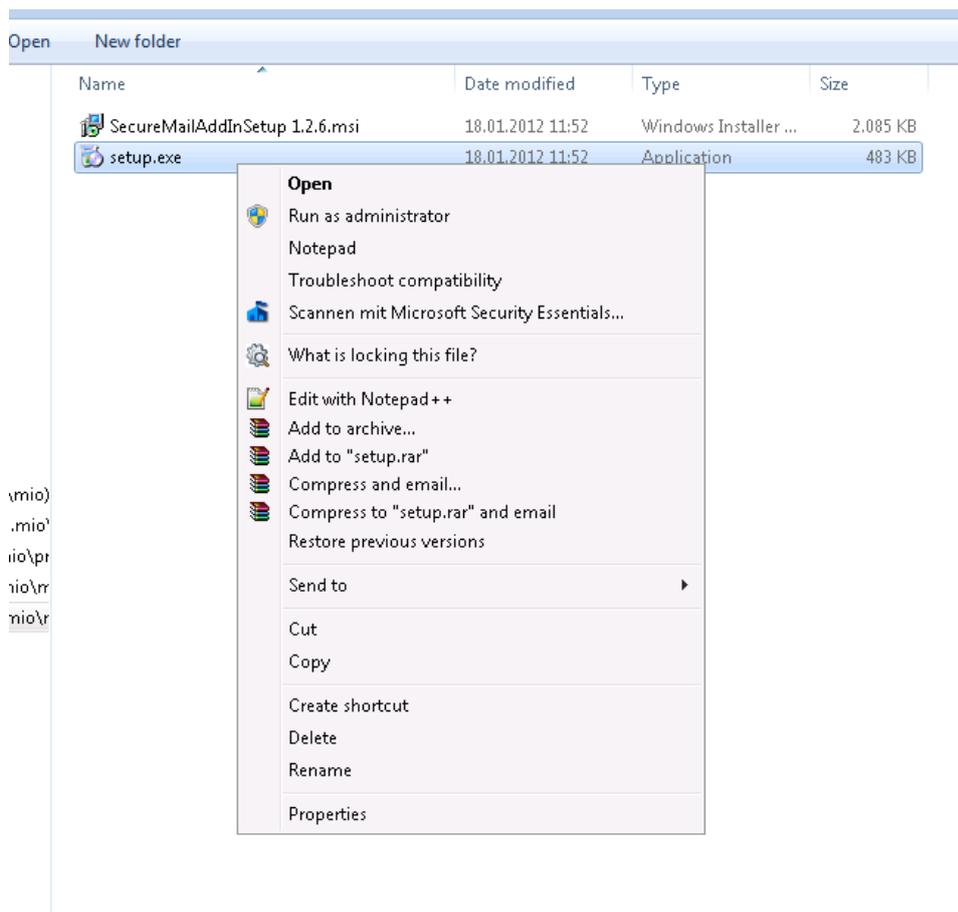
SEPPmailOutlookAddInSetup.msi

- Führt die eigentliche Installation durch.
- Kann auch direkt gestartet werden, wenn entsprechende Rechte vorhanden sind (z.B. inaktives UAC und Admin-Rechte).
- Kann auch für die automatisierte Software-Verteilung verwendet werden.

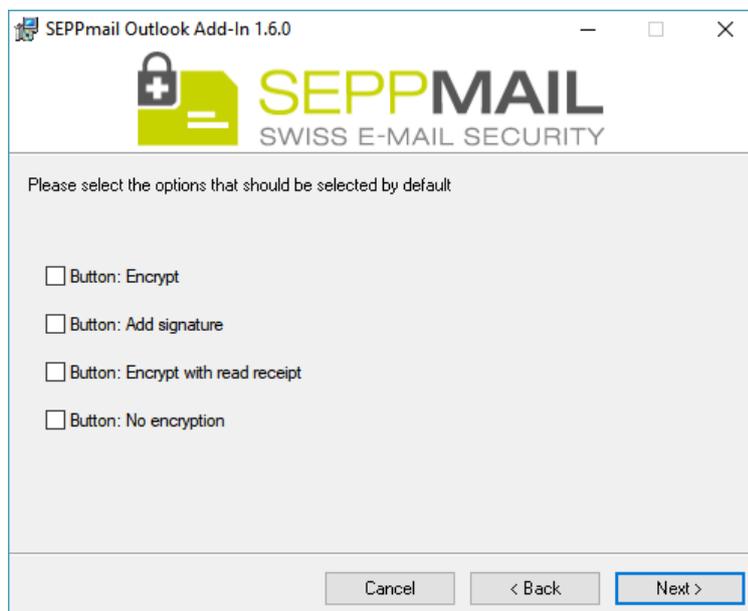
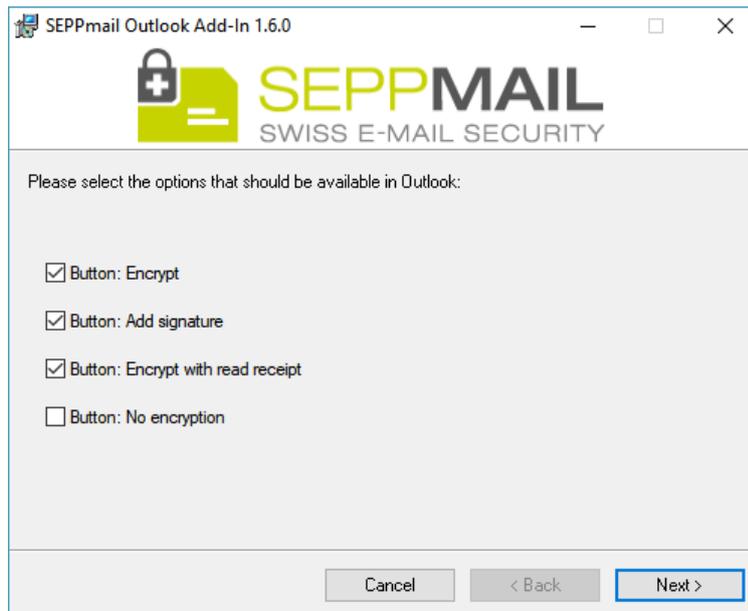
3.1 Installation mit User-Interface

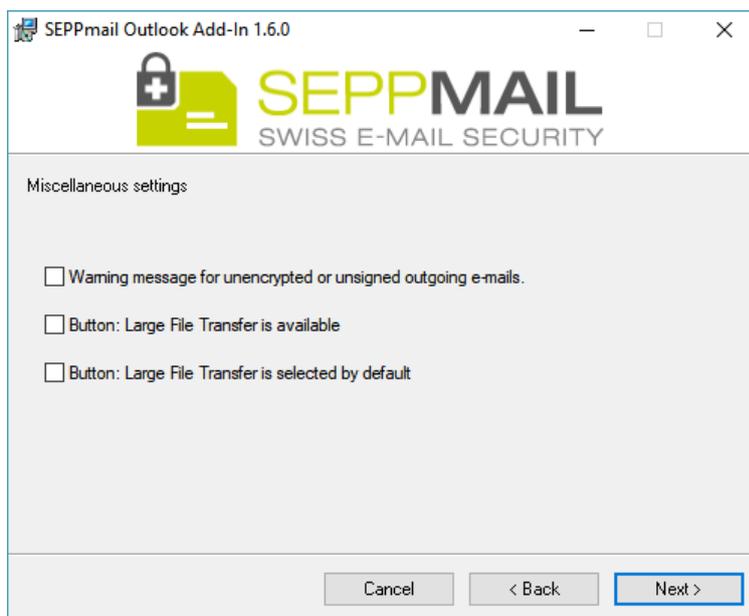
Beispiel:

1. Rechtsklick auf setup.exe und „Als Administrator ausführen“ bzw. „Run as administrator“ auswählen.



2. Die Sicherheitsabfrage von Windows mit „Ja“ beantworten, um die Installation zu starten.
3. Im Folgenden erscheinen die folgenden Bildschirme auf denen der Benutzer Wahlmöglichkeiten
 - a. zu den später angezeigten Buttons
 - b. zum Ein/Ausschalten einer Warnung beim Versand von unverschlüsselten und unsignierten Mails.
 - c. Zu den Standard Button-Zuständen bei Öffnen eines Mail-Fensters





3.2 Installation ohne User-Interface

Alternativ kann die Installation über die Kommandozeile mit diversen Parametern gestartet werden.

Wichtiger Hinweis: Die Kommandozeile muss als Administrator gestartet werden!

Beispiel:

```
msiexec /q /i "SecureMailAddInSetup 1.2.6.msi" SMWarning=false
SMEncrypt=true SMSign=true SMWebmail=true SMHelp=true
SMEncryptSelected=false SMSignSelected=false
SMWebmailSelected=false /li .\log.txt
```

Msiexec-Parameter:

```
/q           Installation ohne User-Interface
/i           Installation eines msi-Pakets
/li .\log.txt log.txt erzeugen mit Basis-Infos im aktuellen Verzeichnis
```

MSI-Parameter

| Parameter | Standard | Beschreibung |
|-----------------------------|----------|---|
| SMWarning | False | Warnung bei Plain-Mails ein-/ausschalten |
| SMEncrypt | True | „Verschlüsseln“ ein-/ausschalten |
| SMLargeFileTransfer | False | „Large File Transfer“ ein-/ausschalten |
| SMSign | True | „Signieren“ ein-/ausschalten |
| SMWebmail | True | „Verschlüsseln mit Lesebestätigung“ ein-/ausschalten |
| SMNoEncryption | False | „Unverschlüsselt“ ein-/ausschalten |
| SMHelp | False | „Hilfe“ ein-/ausschalten |
| SMEncryptSelected | False | „Verschlüsseln“ Standard: aktiv/inaktiv |
| SMLargeFileTransferSelected | False | „Large File Transfer“ Standard: aktiv/inaktiv |
| SMSignSelected | False | „Signieren“ Standard: aktiv/inaktiv |
| SMWebmailSelected | False | „Verschlüsseln mit Leseb.“ Standard: aktiv/inaktiv |
| SMNoEncryptionSelected | False | „Unverschlüsselt“ Standard: aktiv/inaktiv |
| Tooltips | False | Tooltips für Buttons ein/aus |
| LMonly | False | Registry-Werte nur in „Local Machine“ speichern |
| Subject-mod | False | Wird die Subject-Ergänzung aktiviert, werden keine Header-Felder geschrieben, |

| | | |
|--------------------------|-------|--|
| | | <p>sondern Steuerbefehle als Zeichenfolgen an den Betreff ergänzt.</p> <p>Beim Senden werden zunächst evtl. noch vorhandene Steuerbefehle (z.B. „[confidential]“, etc.) aus dem Betreff entfernt und anschließend gemäß der durch die Schaltflächen im Add-in vorgenommenen Einstellungen an den Betreff ergänzt.</p> <p>Der Benutzer sieht den erweiterten Betreff im Ordner „Gesendete Objekte“ und kann die Steuerbefehle für jede E-Mail nachvollziehen.</p> <p>Im Local Machine Teil der Registry werden die folgenden Werte ergänzt, mittels derer die Zeichenfolgen, die als Steuerbefehle verwendet werden sollen, konfiguriert werden können:</p> <p><i>s-smenc = “[confidential]”</i></p> <p><i>s-smsign = “[sign]”</i></p> <p><i>s-smwebmail = “[priv]”</i></p> |
| PlaceSubjectFlagsAtStart | False | <p>Legt fest, ob Steuerbefehle am Anfang des Betreffs eingefügt werden. Standardmäßig (false) werden Steuerbefehle am Ende des Betreffs angefügt.</p> <p>Diese Einstellung ist nur relevant, wenn “subject-mod” aktiviert ist.</p> |

4 Registry

4.1 Local Machine

Bei der Installation werden nur Werte in den Zweig „Local Machine“ geschrieben, da die Installation des Add-Ins für alle Benutzer eines PCs/Terminal Servers erfolgt.

Folgende Werte werden standardmäßig geschrieben:

| | | |
|---|-----------|---|
|  InternalRecipient | REG_SZ | ime@imepseudodomain.local |
|  LMonly | REG_DWORD | 0x00000000 (0) |
|  PlaceSubjectFlagsAtStart | REG_DWORD | 0x00000000 (0) |
|  SMCrypt | REG_DWORD | 0x00000001 (1) |
|  SMCryptSelected | REG_DWORD | 0x00000000 (0) |
|  SMHelp | REG_DWORD | 0x00000000 (0) |
|  SMInternalEncryption | REG_DWORD | 0x00000000 (0) |
|  SMLargeFileTransfer | REG_DWORD | 0x00000000 (0) |
|  SMLargeFileTransferSelected | REG_DWORD | 0x00000000 (0) |
|  SMNoEncryption | REG_DWORD | 0x00000000 (0) |
|  SMNoEncryptionSelected | REG_DWORD | 0x00000000 (0) |
|  SMSign | REG_DWORD | 0x00000001 (1) |
|  SMSignSelected | REG_DWORD | 0x00000000 (0) |
|  SMWarning | REG_DWORD | 0x00000001 (1) |
|  SMWebmail | REG_DWORD | 0x00000001 (1) |
|  SMWebmailSelected | REG_DWORD | 0x00000000 (0) |
|  s-smenc | REG_SZ | [confidential] |
|  s-smifm | REG_SZ | [ifm] |
|  s-smnoenc | REG_SZ | [noenc] |
|  s-smsign | REG_SZ | [sign] |
|  s-smwebmail | REG_SZ | [priv] |
|  subject-mod | REG_DWORD | 0x00000000 (0) |
|  Tooltips | REG_DWORD | 0x00000001 (1) |
|  UsageTimeStamp | REG_SZ | |
|  Web Site | REG_SZ | http://www.seppmail.ch |

Der Pfad in der Registry lautet:

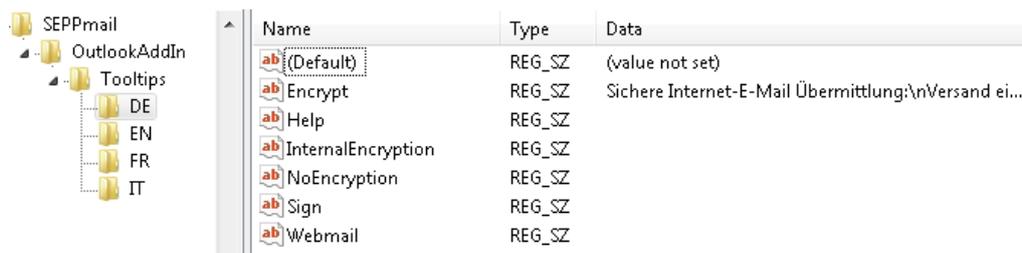
HKEY_LOCAL_MACHINE\SOFTWARE\SEPPmail\OutlookAddIn

Auf 64bit-Systemen wird (da das Setup-Paket im 32-bit Modus läuft) der folgende Pfad verwendet:

HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\SEPPmail\OutlookAddIn

In diesem Registry-Key existiert ein Unterordner / Key mit dem Namen Tooltips

Hier werden in Ordnern pro Sprache die Tooltips für die Buttons hinterlegt:



| Name | Type | Data |
|--------------------|--------|--|
| (Default) | REG_SZ | (value not set) |
| Encrypt | REG_SZ | Sichere Internet-E-Mail Übermittlung:\nVersand ei... |
| Help | REG_SZ | |
| InternalEncryption | REG_SZ | |
| NoEncryption | REG_SZ | |
| Sign | REG_SZ | |
| Webmail | REG_SZ | |

4.2 Current User

Wenn die Option LMOnly = false gesetzt ist (Standard-Wert), dann wird beim Start von Outlook geprüft, ob bereits Registry-Werte für das Add-In im Bereich

HKEY_CURRENT_USER\Software\SEPPmail\OutlookAddIn

bzw.

HKEY_CURRENT_USER\Software\Wow6432Node\SEPPmail\OutlookAddIn

vorhanden sind.

Wenn ja, wird der Timestamp (UsageTimeStamp) zwischen den Einstellungen aus Local Machine mit denen aus Current User verglichen.

Sind die Einstellungen aus Local Machine neuer (oder keine Werte in Current User vorhanden) dann werden die folgenden Einstellungen aus Local Machine nach Current User kopiert:

| | | |
|---|-----------|--------------------|
|  SMEncrypt | REG_DWORD | 0x00000001 (1) |
|  SMEncryptSelected | REG_DWORD | 0x00000000 (0) |
|  SMHelp | REG_DWORD | 0x00000000 (0) |
|  SMLargeFileTransfer | REG_DWORD | 0x00000000 (0) |
|  SMLargeFileTransferSelected | REG_DWORD | 0x00000000 (0) |
|  SMNoEncryptionSelected | REG_DWORD | 0x00000000 (0) |
|  SMSign | REG_DWORD | 0x00000001 (1) |
|  SMSignSelected | REG_DWORD | 0x00000000 (0) |
|  SMWarning | REG_DWORD | 0x00000001 (1) |
|  SMWebmail | REG_DWORD | 0x00000001 (1) |
|  SMWebmailSelected | REG_DWORD | 0x00000000 (0) |
|  UsageTimeStamp | REG_SZ | 2017,1,31,13,45,59 |

Der UsageTimeStamp in Current User wird dabei mit der aktuellen zeit belegt.

Hierdurch wird ermöglicht, dass die Einstellungen zu den Buttons individuell für den User eingestellt werden könnten, ohne dass dies die Einstellungen für andere Benutzer beeinträchtigt.

Ist der UsageTimeStamp von Current User neuer als der in Local Machine, werden immer die Werte aus Current User vom Add-In verwendet.

5 Versand von Mails

Beim Versand von Mails, werden die folgenden Felder, je nach Zustand der Buttons, in den Header der Mail eingebaut:

| Tag | Value |
|-------------|--------|
| x-smenc | yes/no |
| x-smsign | yes/no |
| x-smwebmail | yes/no |
| x-smplain | yes/no |

6 Interne Verschlüsselung

Mit der Funktion „Interne Verschlüsselung“ können E-Mails an ein internes Postfach umgeleitet werden, dass die E-Mail (intern) Server-seitig verschlüsselt.

Dazu müssen einige Voraussetzungen erfüllt sein. Der Registry-Konfigurationswert „InternalRecipient“ muss die E-Mail-Adresse enthalten, unter der das Postfach, über das die Server-seitige Verschlüsselung durchgeführt wird, erreichbar ist.

Abhängig davon, ob dieser Wert den Standardeintrag „ime@imepseudodomain.local“ oder einen anderen Wert enthält, werden unterschiedliche Abläufe angewendet.

1. InternalRecipient = „ime@imepseudodomain.local“

Beim Versand einer E-Mail werden die ursprünglich in der E-Mail eingetragenen Empfänger (To, CC, BCC) entfernt und in Header-Feldern ("X-SM-ORIGTO", "X-SM-ORIGCC" und "X-SM-ORIGBCC") abgelegt und stattdessen die konfigurierte Server-Postfach-Adresse („InternalRecipient“) als Empfänger eingesetzt.

Der Server ist dann dafür zuständig, die E-Mails, die in diesem Postfach eingehen, zu verschlüsseln, anschließend die ursprünglichen Empfänger aus den genannten Header-Feldern wiederherzustellen und die E-Mail an den eigentlichen Empfänger zu versenden.

2. InternalRecipient enthält anderen Wert

Wird die interne Verschlüsselung aktiviert, dann legt das Add-in beim Versand die verfasste E-Mail in eine Container-E-Mail, die dann an die für die SEPPmail Appliance konfigurierte „InternalRecipient“-Adresse.

Falls entsprechende Zertifikate vorhanden sind, wird die Container-E-Mail zusätzlich signiert und verschlüsselt.

Der Server hat dann die Aufgabe, die E-Mails, die in diesem Postfach eingehen, aus der Container-E-Mail zu entpacken, zu verschlüsseln, und die E-Mail an den eigentlichen Empfänger zu versenden.

7 Berechtigungssteuerung per LDAP

Falls gewünscht kann eine Berechtigungssteuerung aktiviert werden, bei der abhängig vom ausgewählten Absender-Postfach die Verwendung der SEPPmail

Verschlüsselungsfunktionen gesperrt wird. Dazu wird über eine per Registry konfigurierbare LDAP-Abfrage geprüft, ob die jeweils ausgewählte Absender-Adresse für die Verschlüsselungsfunktionen berechtigt ist.

Die Berechtigungsprüfung wird über die folgenden Registry-Schlüssel gesteuert bzw. konfiguriert:

| Name | Typ | Beschreibung | Beispiel |
|---------------------------|-----------|---|--|
| LDAPPermissionCheckActive | REG_DWORD | Steuert, ob die Berechtigungssteuerung grundsätzlich aktiviert ist. | 0x1 |
| LDAPServerAddress | REG_SZ | Die Adresse des LDAP Servers | „test.server.com“ |
| LDAPUsername | REG_SZ | Der Benutzername, mit dem die LDAP Abfrage durchgeführt wird | „user“ |
| LDAPPassword | REG_SZ | Das Passwort für den Benutzer, mit dem die LDAP Abfrage durchgeführt wird | „password“ |
| LDAPAuthenticationTypes | REG_SZ | Das zu verwendende Authentifizierungsverfahren für die LDAP-Anmeldung. Mehrere Werte können Komma-separiert angegeben werden. Mögliche Werte sind unter https://msdn.microsoft.com/de-de/library/system.directory.services.authenticationtypes(v=vs.110).aspx aufgelistet. Ist der Eintrag nicht vorhanden oder leer wird eine NTLM-Authentifizierung („Secure“) verwendet. | „Secure,FastBind“ |
| LDAPOrganizationalUnit | REG_SZ | Die LDAP Organisations-Einheit, für die die Abfrage ausgeführt wird | “OU=Managed,OU=Users,DC=test,DC=server,DC=com” |
| LDAPQuery | REG_SZ | Die LDAP Abfrage, in der anstelle des Platzhalters „{0}“ die ausgewählte Absender-Adresse eingesetzt wird, und die ein Ergebnis liefern muss, | „(&(mail={0})(SEPPmailPermission=*))“ |

| | | | |
|--|--|---|--|
| | | wenn die Adresse berechtigt ist, und kein Ergebnis liefern darf, wenn die Adresse nicht berechtigt ist. | |
|--|--|---|--|

8 Automatische Verarbeitung von E-Mails durch das Add-in

Folgende Verarbeitungsschritte werden automatisch durch das Add-in durchgeführt:

- Wird eine E-Mail mit interner Verschlüsselung versendet, dann wird (wie bereits beschrieben) die ursprüngliche, verfasste Mail in eine Container-E-Mail gelegt, diese mit einer technischen Markierung „Interne Verschlüsselung“ versehen und an den in der Einstellung „InternalRecipient“ hinterlegten Empfänger versendet.
- Geht eine E-Mail im Posteingang ein, die in ihrem Header die Kennung „X-ESWmail-InternalEncrypt-sentcopy“ gesetzt hat, dann wird die technische Markierung „Interne Verschlüsselung“ entfernt und die E-Mail in den Ordner „Gesendete Elemente“ verschoben.
- Wird eine E-Mail im Ordner „Gesendete Elemente“ abgelegt und ist an dieser E-Mail noch die technische Markierung „Interne Verschlüsselung“ gesetzt, so wird die E-Mail gelöscht.