E-Mail-Versand der Lohnabrechnungen mit moderner Authentifizierung (Service & MFA)

Inhalt

1 Moderne Authentifizierung (Service & MFA) im Dialog Lohn

Ab Oktober 2022 wurde von Microsoft die **SMTP-Authentifizierungen** deaktiviert. Seither müssen neue ***«moderne Authentifizierungen»*** verwendet werden. Diese bieten viele Vorteile und Verbesserungen bezüglich Sicherheit. Ebenfalls wird das Aktivieren der ***mehrstufigen Authentifizierung (MFA)*** vereinfacht zur Verfügung gestellt.

In dieser Anleitung wird beschrieben, wie Sie diese modernen Authentifizierungen für den ***Versand von Lohnabrechnungen per E-Mai im Dialog Lohn*** verwenden können.

1.1 Ausgangslage (Problematik)

Es genügt nicht mehr nur eine E-Mail-Adresse und ein Password zu kennen, um E-Mails verschicken zu können.
Es gibt aber eine Lösung:

- Man **registriert eine Applikation beim Provider** (zB. im Azure AD für Microsoft Office365) und gibt dieser Applikation die nötigen Rechte. Im Dialog Lohn verwenden wir diese Registrierung der Applikation.
  Dies durch die zwei ID's die aus der Registrierung entstehen:
  - die **Application-ID**
  - die **Mandant-ID**
  um Dialog Lohn gegenüber den SMTP Server mit dieser App als «Benutzer» anzumelden

- Dann erfolgt die Anmeldung und man kann die E-Mails auch von Dialog Lohn aus verschicken

Microsoft hat diese Beschränkung nicht sofort in Kraft gesetzt, sondern in Phasen:

- für einige Kunden funktioniert es noch und für andere nicht
- mit der Zeit werden alle Kunden blockiert und die Registrierung der Applikation (Dialog Lohn) muss durchgeführt werden

Der Kunde registriert die Applikation bei seinem Provider und gibt beide ID's im Dialog Lohn ein.
Das funktioniert so seit einiger Zeit und ohne Probleme.

Vor kurzem wurde Microsoft noch strenger und erfordert MFA (Multi-Factor-Authentification).
Mit einem solchen Konto funktioniert der E-Mail-Versand im Dialog Lohn nicht mehr (auch nicht mit der Registrierung der Applikation).

Wir haben aber ebenfalls eine Lösung gefunden, damit auch für diesen Fall E-Mails weiterhin aus Dialog Lohn verschickt werden können.

1.2 Registrierung der Applikation (dies muss Ihre IT durchführen)

Kunden mit Office365 die in Dialog Lohn mit moderner Authentifizierung arbeiten wollen, müssen die Applikation Dialog Lohn in ihrem eigenen Azure Account zuerst registrieren.

Dafür haben wir ein Skript erstellt. Mit Hilfe dieses Skripts wird die Registrierung der Applikation automatisch durchgeführt. Einzige Voraussetzung ist, dass die Person/Benutzer, der dieses Skript ausführt, auch ein Administrator in Azure ist.

Der Kunde muss von Dialog Lohn Support folgende Dateien verlangen:

- manifest.json
- Publishing-DialogLohn-Client.ps1
- Start- Publishing-DialogLohn-Client.cmd

Alle drei Dateien müssen in einen Ordner zusammen sein.
Der Azure Administrator startet Start-Publishing-DialogLohn-Client.cmd.
Der Rest passiert automatisch.

Das aktuelle Skript mit den notwendigen Dateien finden Sie in unserem **Downloadbereich Dialog Lohn.**

Da diese Authentifizierung mit der Zeit, und je Dienstleister, anders oder noch einfacher funktionieren kann, sind diese Dateien nicht immer notwendig oder aktuell. Diesbezüglich konsultieren Sie bitte die Dokumentation Ihres Dienstleisters für den E-Mail-Versand.

1.2.1 Notwendige Komponente (Windows/Azure CLI)

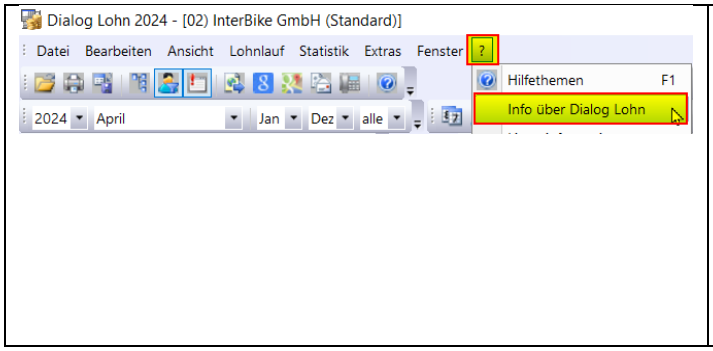
Bei der Registrierung unter Windows mit Azure muss die Komponente Azure CLI bereits installiert sein.
Link für Download: https://learn.microsoft.com/en-us/cli/azure/install-azure-cli

1.3 Konfiguration im Dialog Lohn

1.3.1 Prüfen Version 2025.0.2.1

Bitte prüfen Sie, dass auf ihrem System Dialog Lohn mit Version **2025.0.2.1** (oder höher) installiert ist.

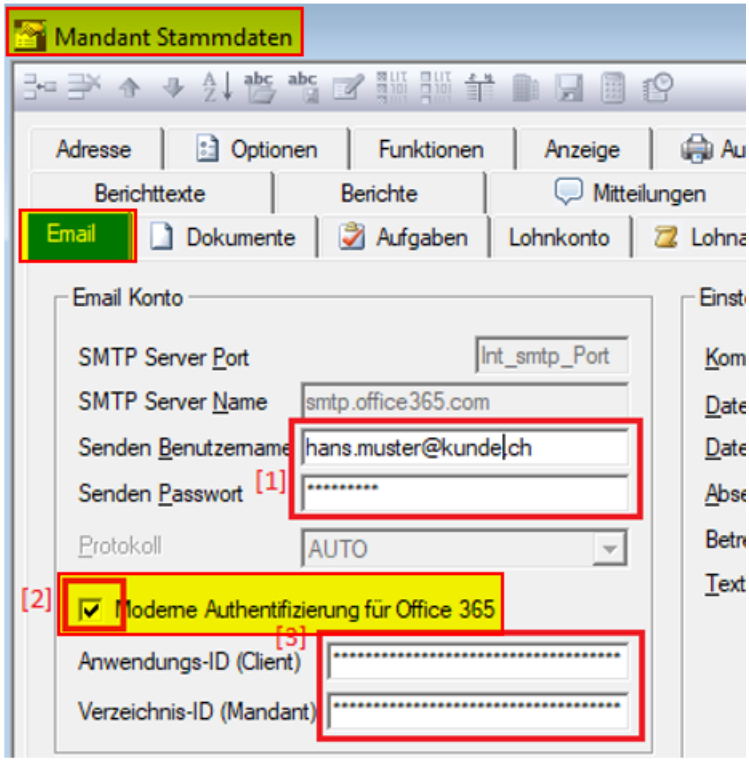
Dies prüfen Sie am besten im Dialog Lohn unter Menu **?** und Info über Dialog Lohn:



Die aktuellen Versionen finden Sie in unserem **Downloadbereich Dialog Lohn**.

1.3.2 Einstellungen im Dialog Lohn

Die notwendigen Einstellungen werden in den Stammdaten zum Mandanten im Register **E-Mail** vorgenommen:



[1] Benutzer-Konto und Passwort

[2] Auschecken um sich via App anzumelden

[3] Application-ID und Mandant-ID

1.3.2.1 Moderne Authentifizierung im Dialog Lohn aktivieren

Falls die moderne Authentifizierung auf dem GUI nicht ersichtlich ist (siehe **[2]**), dann können Sie diese wie folgt aktivieren. Es gibt 3 Varianten:

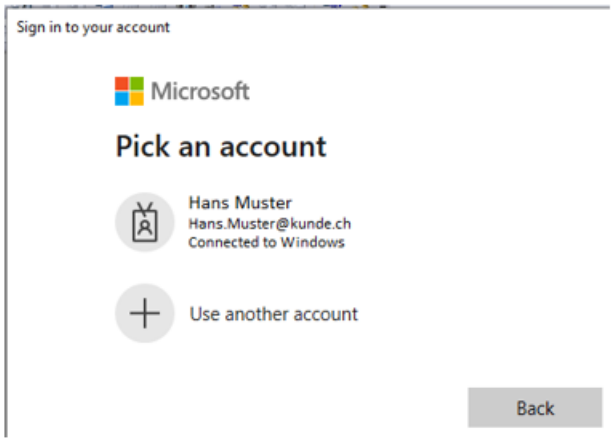
- Command-Line Parameter (für Aufruf Dialog Lohn)
  /SHOWOAUTH

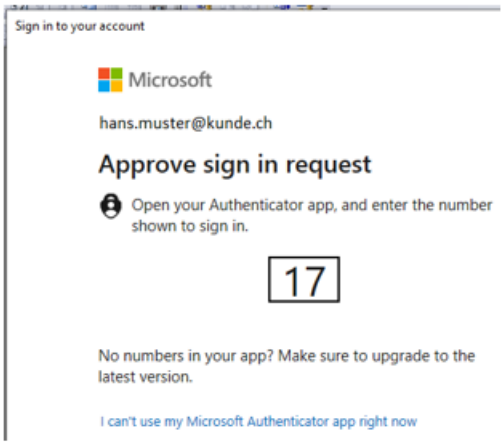
- Command-Line Parameter (für Aufruf Dialog Lohn)
  /SERVICE

- Parameter in Datei Local.INI (befindet sich im Programmverzeichnis Dialog Lohn)
  [Setup]
  oAuth=1

1.3.3 Anwendung mit Lohnabrechnung per E-Mail

Mit zusätzlicher MFA, muss zuerst der Benutzer bestätigt werden und danach die Zusatzinformationen, z.B. Code per Handy oder per E-Mail (je nach MFA-Einstellung) eingeben werden.





Danach sollte das E-Mail korrekt verschickt werden.

1.4 Was machen bei Fehler?

Da Dialog Lohn andere Systemkomponenten aufruft, können Fehler an vielen Orten auftreten.
Für Fehleranalysen bieten sich folgende Möglichkeiten an:

- Windows Ereignisanzeige
  Bei Fehlern reagiert Windows in der Regel mit Einträgen in der Ereignisanzeige, welche danach gesichtet und untersucht werden können.

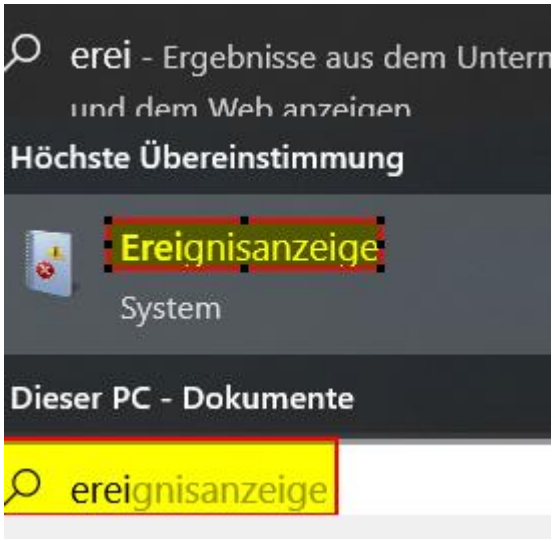
- Erweitertes Fehlerprotokoll im Dialog Lohn aktivieren
  Für weitere Analysen von Fehlern kann auch im Dialog Lohn ein detailliertes Protokoll aktiviert werden, welches
  - die Verarbeitungsschritte sequenziell und mit erweiterten Details auflistet
  - bei Fehlern allenfalls weitere Informationen liefert

Dialog Lohn verwendet die allgemein, von Windows erstellten Fehlerinformationen (Stacktraces). Es kann seitens Dialog Lohn nicht garantiert werden, dass diese zusätzlichen Informationen für eine effiziente Fehlersuche in jedem Fall genügen.

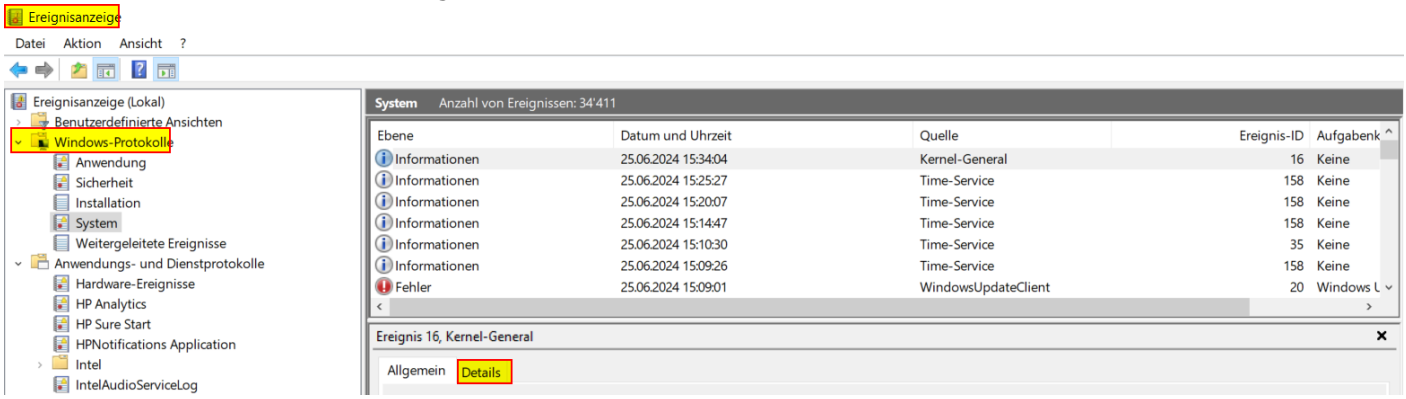
Mehrere erfolgreiche Installationen auf Kundensystemen bestätigen uns aber eine erfolgreiche Umsetzung der Serviceauthentifizierung mit MFA.

1.4.1 Ereignisanzeige (Windows)

Suchen Sie im Windows mit «Ereignisanzeige» (Deutsch) oder mit «Event Log» (Englisch):



Danach werden Ihnen die verschiedenen «Windows-Protokolle» angezeigt. Die Meldungen werden klassifiziert von einfachen Informationen, zu Warnungen bis zu Fehlern:



SICHTEN SIE **ALLE MELDUNGEN** IN **ALLEN WINDOWS-PROTOKOLLEN** FÜR DAS BETROFFENE ZEITFENSTER.

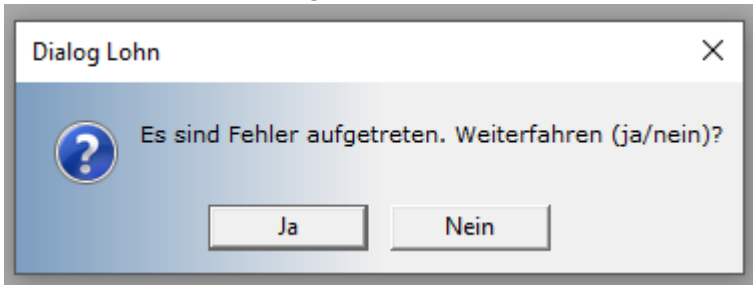
1.4.2 Fehlerprotokoll im Dialog Lohn aktivieren

Um dieses Protokoll zu aktivieren, muss man mit **administrativen Rechten** einen Windows Command-Prompt (Eingabeaufforderung) starten und folgende Linie eingeben:

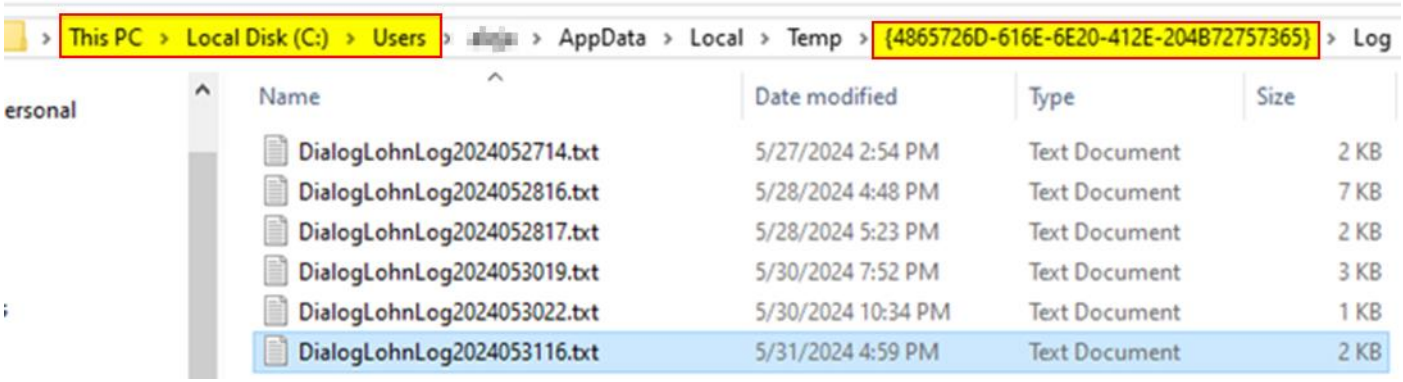
```
C:\Windows\system32>set logdebugmax=5/31/2024 16:00
```

Mit Datum/Zeit, ab wann es starten soll.
Nach 2 Tagen wird dies wieder automatisch beendet und müsste nochmals gestartet werden.

Im Fehlerfall meldet Dialog Lohn einen Fehler:



Danach kann das detaillierte Fehlerprotokoll in folgendem Verzeichnis gesichtet werden:
c:\Users**\<username>**\AppData\Local\Temp\{4865726D-616E-6E20-412E-204B72757365}\DialogLohnLog<**date-time**>.txt



1.5 Verschlüsselung für den Versand

Wir empfehlen die Lohnabrechnung **verschlüsselt (mit Passcode)** zu versenden.
Dies muss von der IT im **Admin-Center von Exchange** konfiguriert werden.

Hier ein (mögliches) Beispiel: