i-net HelpDesk

26.4.130

Office 365

Konfiguration / Kommunikation / OAuth-Verbindung / Office 365

Mit Office 365 verbinden

Eine authentifizierte *Verbindung zu Office 365* ist erforderlich, um auf E-Mails oder Dateien von Microsofts Services zuzugreifen. Beim Herstellen einer Verbindung zu Office 365 wird das Konfigurationsdialogfeld angezeigt, wie in der Abbildung unten zu sehen ist. Dort müssen Sie die fehlenden Informationen eingeben.

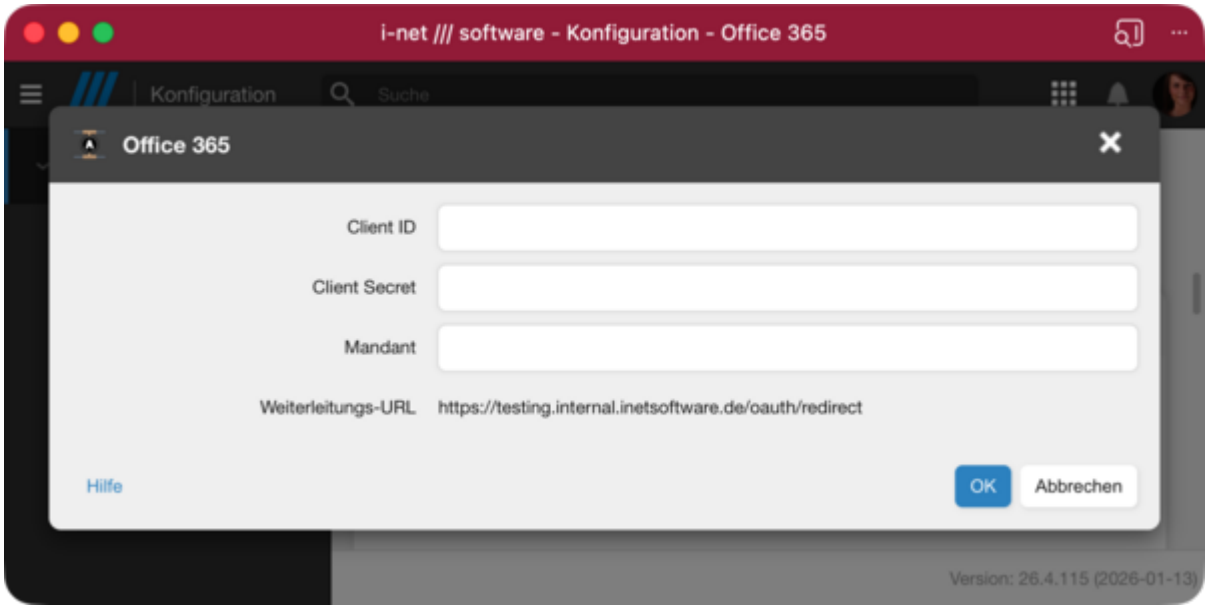


Abbildung 1: Konfigurationsdialog

Dieser Leitfaden ist eine Anleitung zum Erstellen einer OAuth-Anwendungsverbindung, basierend auf Microsofts Schnittstelle im Jahr 2025. Er konzentriert sich auf die allgemeine Verbindung, die für die Standardbenutzerauthentifizierung erforderlich ist. Microsoft Office 365 bietet eine alternative *App-Only*-Authentifizierungsmethode, die aufgrund weniger restriktiver Polling-Limits die Ausfallsicherheit von E-Mail-Verbindungen verbessern kann. Bitte überprüfen Sie auch die erforderlichen Einstellungen für E-Mail-Integration.

Hinweis: Alle Änderungen, die in den Microsoft-Portalen vorgenommen werden, brauchen gelegentlich einige zehn Minuten, bis sie greifen und von i-net HelpDesk korrekt verwendet werden können.

Voraussetzung

Die folgenden Voraussetzungen müssen für eine erfolgreiche Verbindung zum Microsoft Office 365 Authentifizierungsdienst erfüllt sein:

- Der i-net HelpDesk-Server muss mit HTTPS gesichert sein
- Der i-net HelpDesk-Server und der Browser-Client müssen in der Lage sein, die Webseite https://login.microsoftonline.com/ zu erreichen.
- Sie müssen berechtigt sein, eine *Azure Entra ID Anwendung* unter https://entra.microsoft.com zu erstellen.
- Für die E-Mail-Integration überprüfen Sie die entsprechende Voraussetzung.

E-Mail-Abruf

Wird mit diesem Profil ein E-Mail-Abruf oder -Versand initiiert, sind die folgenden Voraussetzungen zu erfüllen:

- Der Server muss in der Lage sein, die folgenden Domänen aufzurufen:
  - Für MSN-Verbindungstyp: smtp-mail.outlook.com, imap-mail.outlook.com
  - Für Office 365-Verbindungstyp: outlook.office365.com, smtp.office365.com.

Erstellen der Azure-Entra-ID-Anwendung

Sie werden jetzt eine neue Anwendung erstellen. Diese Anwendung wird die Authentifizierungsdaten für die OAuth-Verbindung bereitstellen, die wir zu i-net HelpDesk hinzufügen möchten.

- Gehen Sie auf die Webseite https://entra.microsoft.com und melden Sie sich an.
- Wählen Sie App-Registrierungen aus dem Menü in der Seitenleiste
- Klicken Sie im Menü auf Neue Registrierung.

Auf der neu geöffneten Seite müssen Sie Ihre Anwendung konfigurieren (siehe Abbildung unten):

- Geben Sie einen aussagekräftigen *Namen* ein, um diese Anwendung von einer anderen zu unterscheiden
- Wählen Sie die *unterstützten Kontotypen*. Es gibt einen *Entscheidungshilfe...*-Link, der die Unterschiede zwischen den Optionen beschreibt. Normalerweise sollte die erste Option (einzelner Mandant) ausreichen.
- Geben Sie die *Umleitungs-URI* ein, die im Konfigurationsdialog des i-net HelpDesk-Servers als *Weiterleitungs-URL* angezeigt wird, in dem eine neue Verbindung erstellt wird (siehe oben). Vergewissern Sie sich, dass Sie Web als Typ der Umleitungs-URL ausgewählt haben.
- Klicken Sie auf Registrieren am Ende des Dialogs

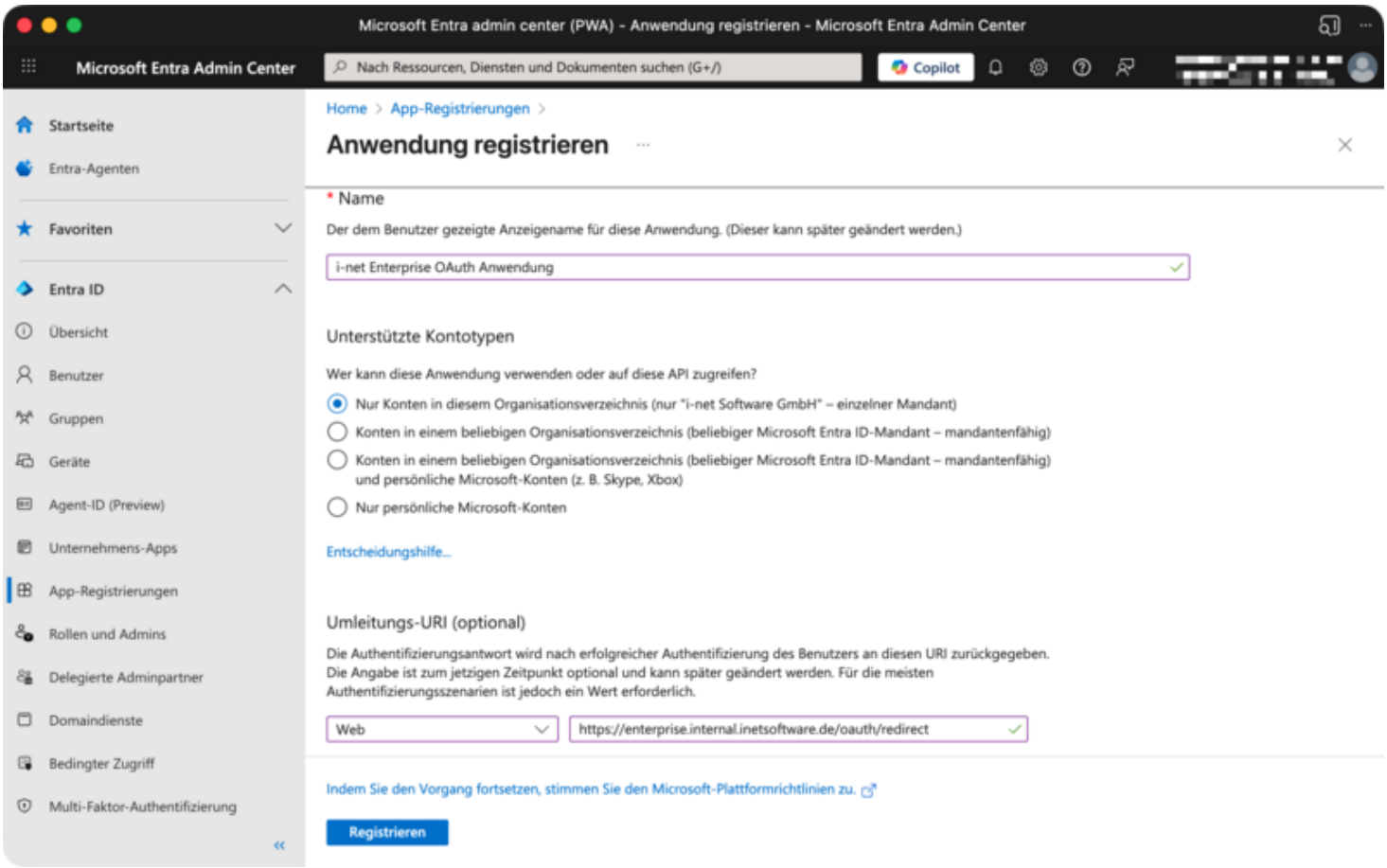


Abbildung 2: Azure Entra ID Anwendungsregistrierung

Hinweis: Nach dem Erstellen der Anwendung lautet die Standard-API-Berechtigung für die Microsoft Graph-API User.Read. Diese Berechtigung reicht für die Authentifizierung gegenüber dieser Anwendung aus.

Office 365-Konfiguration

Nachdem Sie die Anwendung vorbereitet haben, können Sie nun die erforderlichen Informationen im Konfigurationsdialog eingeben.

Hinweis: Wenn Sie bei der Konfiguration des Kontotyps *Einzelner Mandant* ausgewählt haben, müssen Sie die ID des Mandanten in das entsprechende Feld der Konfiguration eintragen. Andernfalls sollte es leer gelassen werden.

Abrufen der Client- und Mandanten-ID

Die *Client- und Mandanten-IDs* werden in der Übersicht direkt nach dem Erstellen der Anwendung angezeigt. Sie werden als Anwendungs-ID (Client) und Verzeichnis-ID (Mandant) im Abschnitt *Zusammenfassung* der Anwendung direkt unter dem Anwendungsnamen angezeigt. Fügen Sie die *Client- und Mandanten-ID* in das Dialogfeld *OAuth-Verbindung* ein.

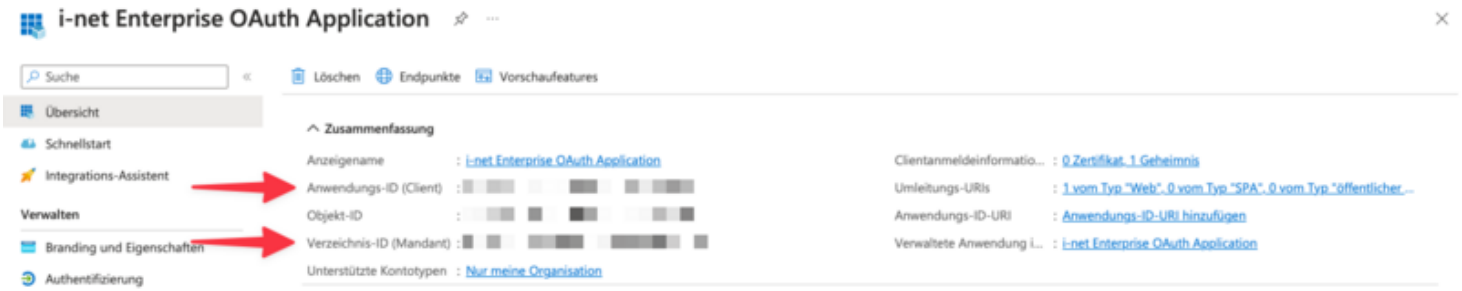


Abbildung 3: Azure Entra ID Anwendungsübersicht

Abfrage des Client-Secrets

Das *Client-Secret* muss separat erstellt werden. Sie können den Link Zertifikat oder Geheimnis hinzufügen im Abschnitt Essentials verwenden, um dorthin zu gelangen.

- Navigieren Sie zum Abschnitt *Zertifikate & Geheimnisse* der Anwendung.
- Klicken Sie auf "Neuer geheimer Clientschlüssel" in der Registerkarte *Geheime Clientschlüssel*.
- Geben Sie eine *Beschreibung* ein und legen Sie die *Ablaufzeit* in der Seitenleiste fest.
- Klicken Sie auf Hinzufügen.

Sie müssen nun den neuen Eintrag aus der Spalte Wert aus der Tabelle kopieren und in den *OAuth-Verbindung*-Dialog einfügen.

Hinweis: Das *Client-Secret* gilt als Passwort, bewahren Sie es also bitte an einem sicheren Ort auf.

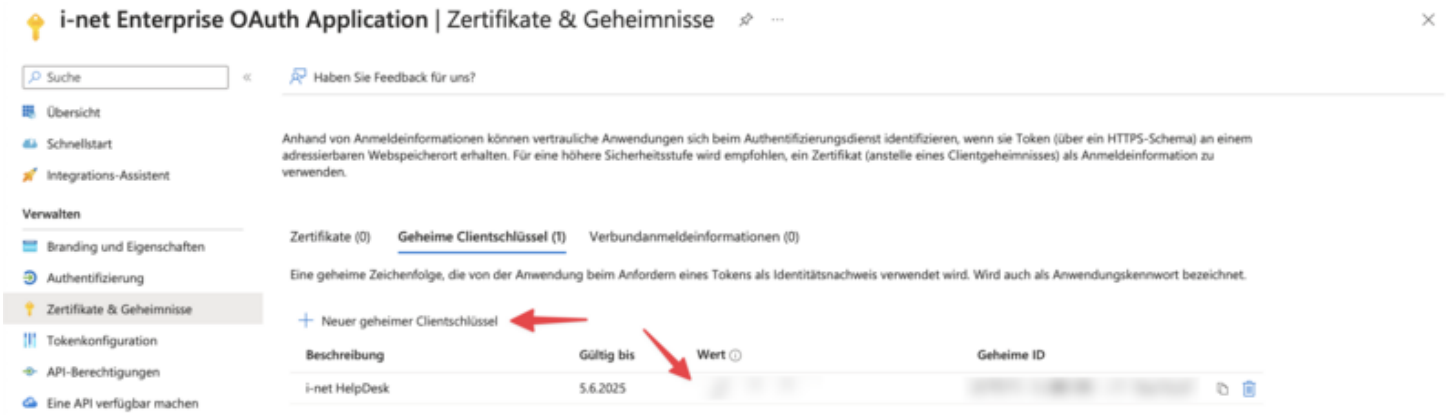


Abbildung 4: Azure Entra ID Anwendungszertifikate

E-Mail-Integration

Die OAuth-Verbindung kann auch zur Authentifizierung bei Office 365-E-Mail-Diensten zum Senden und Empfangen von E-Mails verwendet werden. Die folgenden zusätzlichen Anforderungen müssen erfüllt sein:

- Der Server muss die folgenden Domänen aufrufen können:
  - Für den Verbindungstyp MSN: smtp-mail.outlook.com, imap-mail.outlook.com
  - Für den Verbindungstyp Office 365: outlook.office365.com, smtp.office365.com.
- Das Protokoll SMTP AUTH muss für Ihre Organisation aktiviert sein.
- Sie müssen Organisationsadministrator mit Berechtigung zur Konfiguration im Exchange Admin Center sein.

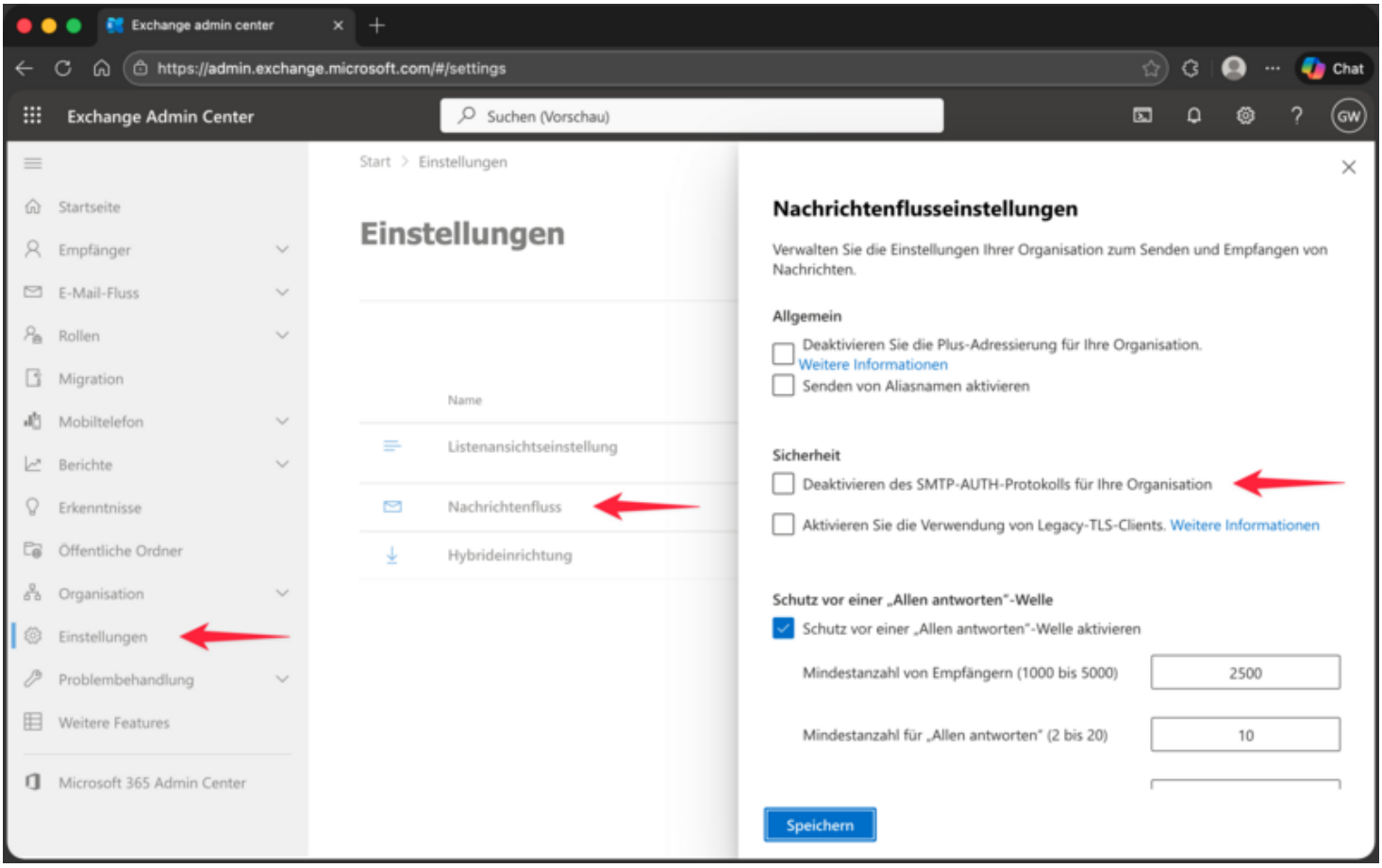
Die oben genannte Standardeinrichtung kann sowohl für den benutzerbasierten als auch für den App-Only-basierten Authentifizierungsablauf verwendet werden. Die beiden Methoden unterscheiden sich wie folgt:

- **Benutzerbasiert**: Beim Erstellen der Verbindung für eingehende oder ausgehende E-Mails muss die Verbindung durch Anmelden beim jeweiligen E-Mail-Kontobenutzer hergestellt werden. Klicken Sie dazu auf die Schaltfläche OAuth-Verbindung einrichten, nachdem Sie den Anbieter Office 365 (als Benutzer) ausgewählt haben. Bei dieser Methode wird ein bestimmter Benutzer direkt mit den Einstellungen für eingehende oder ausgehende E-Mails verbunden.
- **App-Only**: Der Authentifizierungsablauf App-Only erfordert keine direkte Kontoverbindung. Hier muss die Verbindung der im Microsoft-Portal registrierten Anwendung mit dem jeweiligen E-Mail-Konto mithilfe zusätzlicher PowerShell-Befehle konfiguriert werden. Der Authentifizierungsablauf App-Only hat weniger restriktive Polling-Beschränkungen, was zu weniger Verbindungsausfällen führt.

SMTP-Authentifizierung

Die OAuth-Verbindung kann auch für die Authentifizierung gegenüber SMTP verwendet werden. Es ist jedoch zu beachten, dass nur die moderne SMTP-Authentifizierung unterstützt wird, nicht die Graph-API-Methode zum Versenden von E-Mails. Daher müssen Sie entweder Ihre Organisation oder das für den Versand von E-Mails verwendete Konto so konfigurieren, dass es SMTP-AUTH unterstützt.

Dazu müssen Sie auf das Microsoft Exchange Admin Portal zugreifen, zu Mail Flow navigieren und die Option Turn off SMTP AUTH protocol for your organization deaktivieren.



Benutzerbasierter Authentifizierungsablauf

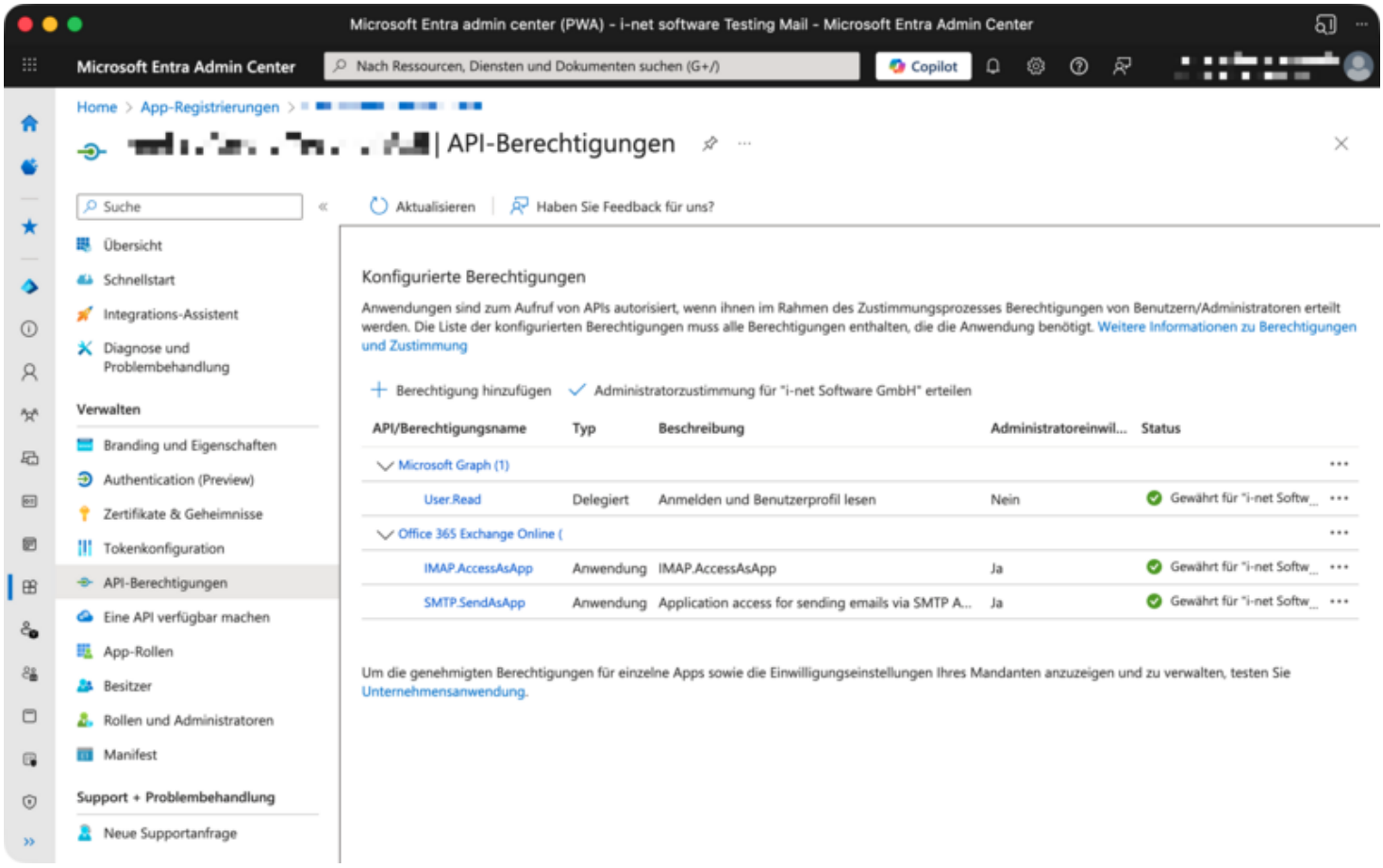
Wie bereits erwähnt, müssen Sie für die Einrichtung der E-Mail-Integration mit benutzerbasierter Authentifizierung über die entsprechende Schaltfläche die OAuth-Verbindung einrichten. Nach der Einrichtung ändert sich die Schaltfläche zu OAuth-Verbindung erneuern. Es wird empfohlen, diese Einrichtung in einem privaten Browser-Tab vorzunehmen, damit Sie sich mit dem Benutzer des jeweiligen E-Mail-Kontos authentifizieren können.

App-only-Authentifizierungsablauf

Der *App-only-Authentifizierungsablauf* erfordert zusätzliche Einstellungen für den Empfang von E-Mails über IMAP. Das jeweilige E-Mail-Konto muss vorab authentifiziert werden. Dazu müssen Sie folgende Schritte ausführen:

- In Ihrer *Anwendungsregistrierung*, die Sie gerade erstellt haben (siehe oben).
- Klicken Sie auf API-Berechtigungen und Berechtigung hinzufügen.
- Wählen Sie die Registerkarte Von meiner Organisation verwendete APIs, suchen Sie nach Office 365 Exchange Online und wählen Sie diese Option aus.
- Wählen Sie Anwendungsberechtigungen.
- Suchen Sie nach IMAP.AccessAsApp und SMTP.SendAsApp und wählen Sie diese Optionen aus.
- Klicken Sie auf Berechtigungen hinzufügen.
- Die Berechtigungen wurden nun hinzugefügt. Möglicherweise ist ein weiterer Schritt erforderlich:
  - Klicken Sie auf Administratorzustimmung für ... erteilen.

Das Ergebnis sollten die zugewiesenen API-Berechtigungen sein, wie im Screenshot zu sehen.



Hinweis: Die Anweisungen sind abgeleitet und gekürzt aus den Microsoft IMAP/POP/SMTP OAuth-Anweisungen.

Registrieren Sie Dienstprinzipale in Exchange

Die Vorabauthentifizierung findet im Microsoft Exchange Admin Portal statt. Sie müssen dazu ein Organisationsadministrator sein. Öffnen Sie die Cloud Shell mit PowerShell. Diese Shell enthält alle Exchange-Online-Tools vorinstalliert.

- Öffnen Sie https://admin.exchange.microsoft.com/
- Nach kurzer Wartezeit sollte die Cloud Shell als Icon in der Toolbar erscheinen (siehe unten).
- Wählen Sie, falls nötig, die PowerShell als Arbeitsumgebung.
- Führen Sie die nachstehenden Befehle aus.

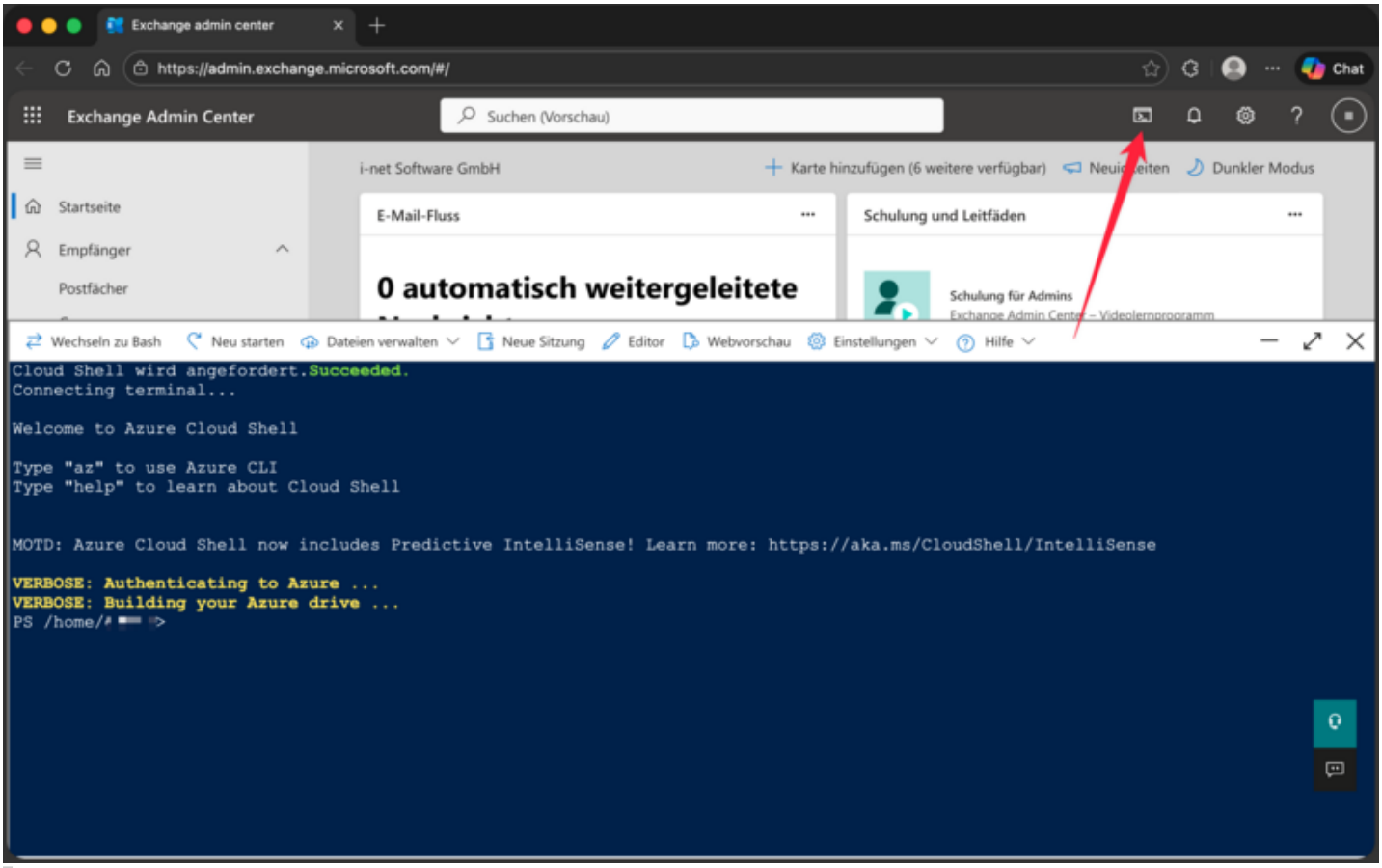


Abbildung 5: Exchange Admin Center Cloud Shell

```
# Verbinden Sie Ihren Mandanten mit der Konsole.
Connect-ExchangeOnline
  # APPLICATION_ID - Die App-Registrierungsanwendung/Client-ID (siehe 'Abrufen der Client- und Mandanten-ID')# OBJECT_ID - Die Objekt-ID aus dem Link 'Verwaltete Anwendung im lokalen Verzeichnis' im Abschnitt 'Essentials'
New-ServicePrincipal -AppId <APPLICATION_ID> -ObjectId <OBJECT_ID>
  # ACCOUNT_EMAIL - Das E-Mail-Konto des Benutzers, von dem Sie E-Mails senden/empfangen# SERVICE_PRINCIPAL_ID - Die ObjectId aus dem Ergebnis des vorherigen Befehls
Add-MailboxPermission -Identity "ACCOUNT_EMAIL" -User <SERVICE_PRINCIPAL_ID> -AccessRights FullAccess
```

Hinweis: Die Anweisungen sind unter Microsoft IMAP/POP/SMTP OAuth-Anweisungen aufgeführt. Sie sind jedoch so formuliert, dass Sie sie von einem lokalen Computer-PowerShell aus statt vom Online-PowerShell ausführen können.