

Produktbeschreibung

SECMENDO.connect Azure AD



IBsolution GmbH

Im Zukunftspark 8

D-74076 Heilbronn

Version 1.0

IBsolution GmbH

Im Zukunftspark 8 | 74076 Heilbronn | Telefon +49 (7131) 2711-3000 | www.ibsolution.de

Registergericht: Stuttgart HRB 108247 | Geschäftsführer: Oliver Donner, Loren Heilig, Andreas Mayer

Inhaltsverzeichnis

1	Beschreibung.....	3
2	Liefergegenstand.....	4
3	Vorraussetzungen.....	5

1 Beschreibung

Der SECMENDO.connect Azure AD Connector erlaubt das Auslesen von Benutzer- und Gruppeninformationen aus Microsoft Azure AD sowie die Änderung der Daten innerhalb Microsoft Azure AD über SAP Identity Management Standard Prozesse.

Die bereitgestellten Funktionen sind für Benutzer:

- Auslesen der Benutzerdaten aus Microsoft Azure AD
- Anlegen, Ändern, Löschen von Benutzern in Microsoft Azure AD
- Identifizierung von onPremise bzw. Cloud Benutzern

Gruppen:

- Auslesen der Gruppendaten aus Microsoft Azure AD
- Anlegen, Ändern, Löschen von Gruppen in Microsoft Azure AD
- Zuweisung von Benutzer Mitgliedschaften zu Gruppen in Microsoft Azure AD
- Identifizierung von onPremise bzw. Cloud Gruppen

Der Azure AD Connector benutzt die Azure Active Directory Graph API sowie das Microsoft Graph Java SDK.

- <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-graph-api>
- <https://github.com/microsoftgraph/msgraph-sdk-java>

Der Connector läuft auf dem SAP Identity Management Runtime Server und wird mittels der Java Runtime ausgeführt. Dieser Runtime Server muss eine HTTPS Verbindung zu dem Microsoft Azure AD Tenant aufbauen können, um die Daten lesen und schreiben zu können.

2 Liefergegenstand

Connector (Java Library / JAR Files) zur Einbindung in SAP Identity Management Runtime zum Aufruf der Microsoft Graph API.

SAP Identity Management Package Export zum Aufrufen der Connector Funktionalität.

3 Voraussetzungen

- SAP Identity Management
 - Version 8.0 aktuelles SP
 - Datenbank Plattform: siehe PAM (Microsoft Server und Oracle)
 - SAPJDK 8
 - Runtime Plattform: siehe PAM (Microsoft Server oder Linux)

- Offene HTTPS Verbindung von Runtime Server zu Microsoft Azure AD Tenant

- Microsoft Azure AD Tenant
 - App Registration mit Application (Client) ID und Secret
 - Application Permissions
 - Directory.ReadWrite.All (Read and write directory data)
 - Group.ReadWrite.All (Read and write all groups)
 - User.ReadWrite.All (Read and write all users' full profiles)