HIVE BDC: EINRICHTUNG IN MICROSOFT 365

App-Registrierungen für Mail und SharePoint

Dokument

Einrichtungshandbuch für IT-Administratoren, Version 1.0
12. Oktober 2026

Produkt

Hive BDC 1.2, by Balsoft
Microsoft 365: Entra ID, SharePoint Online, Exchange Online

Balsoft GmbH
Herler Str. 109
51067 Köln
HRB 121678 Amtsgericht Köln, USt-IdNr. DE452983132

Copyright © 2026 Balsoft GmbH. Alle Rechte vorbehalten! Änderungen an diesem Dokument bedürfen der schriftlichen Zustimmung der Balsoft GmbH. Die Vervielfältigung dieses Dokumentes, sowie die Weitergabe an Dritte ist nur mit Zustimmung der Balsoft GmbH erlaubt.

Inhalt

1 Überblick 3

2 Vorbereitung 3

2.1 Rollen 3

2.2 Was Sie bereithalten 4

2.3 Wo Sie die Skripte ausführen 4

3 Skripte herunterladen 4

4 SharePoint-App 5

4.1 Schritt 1: App-Registrierung anlegen 5

4.2 Schritt 2: Berechtigungen zuweisen 5

5 Mail-App 5

5.1 Schritt 1: App-Registrierung anlegen 5

5.2 Schritt 2: Berechtigungen zuweisen 6

6 Geheime Clientschlüssel 6

7 Werte in Hive BDC eintragen 6

8 Fehlersuche 7

8.1 Support 7

1 Überblick

Hive BDC kann jeden Beleg per Mail an den Empfänger senden und in SharePoint ablegen. Für beides meldet es sich mit einer App-Registrierung in Ihrem Microsoft Entra ID bei Microsoft 365 an. Dieses Handbuch richtet die beiden App-Registrierungen ein. Sie brauchen nur die für die Funktionen, die Sie nutzen: ohne Mailversand keine Mail-App, ohne SharePoint keine SharePoint-App.

Es sind zwei Registrierungen, damit jede nur die Berechtigung hat, die sie braucht, und jede Berechtigung ist zusätzlich eingeschränkt: Die SharePoint-App darf nur in die Sites schreiben, die Sie nennen, die Mail-App darf nur als das eine Postfach senden, das Sie nennen.

App-Registrierung	Berechtigung	Eingeschränkt auf
Hive BDC SharePoint	Sites.Selected (Anwendung)	Schreibzugriff auf die genannten Sites (Kapitel 4)
Hive BDC Mail	Application Mail.Send in Exchange Online	Senden als ein Postfach (Kapitel 5)

Jede App wird in zwei Schritten eingerichtet: Schritt 1 legt die App-Registrierung ohne Berechtigungen an, Schritt 2 weist ihre Berechtigungen zu. Die Schritte können verschiedene Administratoren ausführen. Jedes Skript zeigt den Mandanten, an dem es angemeldet ist, und fragt, bevor es etwas ändert. Was schon vorhanden ist, überspringt es, Sie können es also jederzeit erneut ausführen, zum Beispiel um eine weitere SharePoint-Site hinzuzufügen. Mit -WhatIf zeigt es nur, was es tun würde. Die Skripte speichern keinen geheimen Clientschlüssel; den legen Sie in Kapitel 6 an.

2 Vorbereitung

2.1 Rollen

Jeder Schritt braucht diese Microsoft-Entra-Rollen. Ein Globaler Administrator deckt alle ab, ausgenommen die Mitgliedschaft in der Site.

Schritt	Rolle
Schritt 1: App-Registrierung anlegen	Anwendungsadministrator (oder Anwendungsentwickler)
Schritt 2, SharePoint: Administratorzustimmung für Sites.Selected	Globaler Administrator oder Administrator für privilegierte Rollen
Schritt 2, SharePoint: Zugriff auf eine Site	SharePoint-Administrator und Mitglied dieser Site
Schritt 2, Mail: als ein Postfach senden	Exchange-Administrator (Organization Management in Exchange)

2.2 Was Sie bereithalten

- SharePoint: die Adresse jeder Site, in die Hive BDC hochlädt, zum Beispiel https://contoso.sharepoint.com/sites/Rechnungen. Die Adresse einer Bibliothek oder eines Ordners in der Site geht ebenfalls.
- Mail: das Postfach, aus dem die Belege versendet werden, zum Beispiel rechnung@contoso.de. Es muss in Exchange Online vorhanden sein; ein freigegebenes Postfach genügt und braucht keine Lizenz.
- Mail: eine oder mehrere Testadressen. Belege aus einem Testsystem gehen an sie statt an Kunden oder Lieferanten.

2.3 Wo Sie die Skripte ausführen

Verwenden Sie Azure Cloud Shell. Sie läuft im Browser, ist bereits mit Ihrem Konto angemeldet und bringt alles mit, was die Skripte brauchen: Azure CLI und das Exchange-Online-Modul. Auf Ihren Rechnern wird nichts installiert.

1. Melden Sie sich mit einem Administratorkonto Ihres Mandanten an https://portal.azure.com an.
2. Öffnen Sie Cloud Shell über das Terminal-Symbol in der oberen Leiste und wählen Sie PowerShell.
3. Beim ersten Start fragt Cloud Shell nach einem Speicher. „Kein Speicherkonto erforderlich" genügt für diese Skripte.

Hinweis: Schritt 2 meldet sich noch einmal an (SharePoint: für den Site-Zugriff, Mail: bei Exchange Online). Cloud Shell hat keinen Browser, dort geschieht diese Anmeldung mit einem Code auf microsoft.com/devicelogin. Viele Organisationen sperren die Anmeldung per Code mit bedingtem Zugriff („Sie haben keinen Zugriff"). Führen Sie Schritt 2 dann auf Ihrem eigenen Rechner aus: Windows PowerShell 5.1 oder PowerShell 7 mit installiertem Azure CLI, dort öffnet die Anmeldung einen Browser. Das Mail-Skript braucht dort zusätzlich das Exchange-Online-Modul (Install-Module ExchangeOnlineManagement).

3 Skripte herunterladen

Jede App hat zwei Skripte, eines pro Schritt. Fügen Sie die Zeilen für die App, die Sie einrichten, in Cloud Shell ein; sie laden die Skripte in den aktuellen Ordner.

App	Schritt 1: anlegen	Schritt 2: Berechtigungen
SharePoint	New-HiveBDCSharePointApp.ps1	Grant-HiveBDCSharePointAccess.ps1
Mail	New-HiveBDCMailApp.ps1	Grant-HiveBDCMailAccess.ps1

```
Invoke-WebRequest https://balsoft.de/downloads/hive-bdc/New-HiveBDCSharePointApp.ps1 -OutFile New-HiveBDCSharePointApp.ps1

Invoke-WebRequest https://balsoft.de/downloads/hive-bdc/Grant-HiveBDCSharePointAccess.ps1 -OutFile Grant-HiveBDCSharePointAccess.ps1

Invoke-WebRequest https://balsoft.de/downloads/hive-bdc/New-HiveBDCMailApp.ps1 -OutFile New-HiveBDCMailApp.ps1
```

Invoke-WebRequest https://balsoft.de/downloads/hive-bdc/Grant-HiveBDCMailAccess.ps1 -OutFile Grant-HiveBDCMailAccess.ps1

Alle Skripte sind reiner Text. Sie können sie vor dem Ausführen auf der Hive-BDC-Seite unter balsoft.de lesen oder mit code New-HiveBDCMailApp.ps1 in Cloud Shell. Der Quelltext ist auch öffentlich unter github.com/balsoft-gmbh/hive-bdc im Ordner scripts.

4 SharePoint-App

4.1 Schritt 1: App-Registrierung anlegen

./New-HiveBDCSharePointApp.ps1

Das Skript zeigt den Mandanten und Ihr Konto und fragt, ob es weitergehen soll; antworten Sie mit y. Es legt die App-Registrierung „Hive BDC SharePoint" und ihren Dienstprinzipal (die Unternehmensanwendung) an, ohne Berechtigungen. Am Ende gibt es die Verzeichnis-ID (Mandant), die Anwendungs-ID (Client) und den Befehl für Schritt 2 aus. Notieren Sie beide IDs für Kapitel 7.

4.2 Schritt 2: Berechtigungen zuweisen

Starten Sie das Skript mit der Client-ID aus Schritt 1 und den Sites, in die Hive BDC hochlädt. Mehrere Sites trennen Sie mit Komma.

./Grant-HiveBDCSharePointAccess.ps1 -AppId <client-id> -SiteUrl https://contoso.sharepoint.com/sites/Invoices

1. Zeigt den Mandanten, die App und die Sites und fragt, ob es weitergehen soll. Antworten Sie mit y.
2. Fügt die Berechtigung Sites.Selected hinzu und erteilt die Administratorzustimmung. Sites.Selected allein gibt noch auf keine Site Zugriff.
3. Gibt der App Schreibzugriff auf jede Site. Für diesen Schritt meldet sich das Skript noch einmal an, weil es für Ihr Konto die Berechtigung Sites.FullControl.All braucht: Öffnen Sie die angezeigte Adresse, geben Sie den Code ein, melden Sie sich an und bestätigen Sie die Berechtigungsanfrage.

Später eine weitere Site: Führen Sie Schritt 2 mit dieser Site erneut aus; alles andere wird übersprungen.

Hinweis: Mit -AllSites statt -SiteUrl erhält die App Sites.ReadWrite.All und darf in jede Site des Mandanten schreiben. Nutzen Sie das nur, wenn Ihre Sicherheitsrichtlinie es erlaubt; Zugriff pro Site ist die sicherere Vorgabe.

5 Mail-App

5.1 Schritt 1: App-Registrierung anlegen

./New-HiveBDCMailApp.ps1

Wie in Kapitel 4.1, für die App-Registrierung „Hive BDC Mail". Notieren Sie die Client-ID.

5.2 Schritt 2: Berechtigungen zuweisen

./Grant-HiveBDCMailAccess.ps1 -AppId <client-id> -SenderMailbox invoices@contoso.com

1. Zeigt den Mandanten, die App und das Postfach und fragt, ob es weitergehen soll. Antworten Sie mit y.
2. Meldet sich bei Exchange Online an (Adresse und Code wie in Kapitel 4.2) und erlaubt der App, als das eine Postfach zu senden: die Rolle Application Mail.Send, beschränkt auf einen Verwaltungsbereich, der nur dieses Postfach enthält (RBAC für Anwendungen).

Die App erhält bewusst keine Mail.Send-Berechtigung in Entra ID: Diese würde das Senden als jedes Postfach des Mandanten erlauben, und die Exchange-Beschränkung würde sie nicht einengen. Eine bereits vorhandene Mail.Send-Zustimmung wird entfernt. Exchange Online braucht bis zu 30 Minuten, bis die Beschränkung gilt; bis dahin kann ein Testversand mit ErrorAccessDenied scheitern, ein Fehler in der Einrichtung ist das nicht.

Hinweis: Eigene Exchange-Bereiche brauchen einen einmaligen Schalter, der in Mandanten, die Exchange nie angepasst haben, aus ist. Das Skript schaltet ihn ein (Enable-OrganizationCustomization). Exchange braucht danach bis zu einer Stunde, bis er wirkt; hält das Skript mit diesem Hinweis an, starten Sie es später mit denselben Parametern erneut.

Hinweis: In Mandanten ohne RBAC für Anwendungen weicht das Skript auf eine Anwendungszugriffsrichtlinie aus: Mail.Send wird in Entra ID zugestimmt und auf eine E-Mail-aktivierte Sicherheitsgruppe mit dem Postfach beschränkt.

6 Geheime Clientschlüssel

Jede App braucht einen geheimen Clientschlüssel. Legen Sie ihn im Microsoft Entra Admin Center an und tragen Sie ihn direkt im Hive-BDC-Dashboard ein (Kapitel 7). Bitte senden Sie ihn nicht per Mail und tragen Sie ihn nicht in ein Ticket ein.

1. Öffnen Sie https://entra.microsoft.com, dann Anwendungen, App-Registrierungen, Alle Anwendungen.
2. Wählen Sie „Hive BDC SharePoint“ (oder „Hive BDC Mail“), dann Zertifikate & Geheimnisse, Neuer geheimer Clientschlüssel.
3. Geben Sie eine Beschreibung ein, zum Beispiel HiveBDC, wählen Sie die Gültigkeit (24 Monate ist die längste) und fügen Sie ihn hinzu.
4. Kopieren Sie sofort den Wert. Er wird nur dieses eine Mal angezeigt.

Hinweis: Tragen Sie sich das Ablaufdatum als Erinnerung ein. Legen Sie vor dem Ablauf auf demselben Weg einen neuen Schlüssel an und tragen Sie ihn im Dashboard ein; danach löschen Sie den alten.

7 Werte in Hive BDC eintragen

Öffnen Sie das Hive-BDC-Dashboard auf dem Server, dann Settings und den Reiter Connections.

Bereich	Feld	Wert
SharePoint	Tenant ID, Client ID, Client secret	Verzeichnis-ID und Anwendungs-ID von „Hive BDC SharePoint" und ihr Schlüssel
Document mail	Client ID, Client secret	Anwendungs-ID von „Hive BDC Mail" und ihr Schlüssel
Document mail	Tenant ID	Leer, wenn es derselbe Mandant wie bei SharePoint ist
Document mail	Send from	Das Postfach aus Kapitel 5
Document mail	Test recipients	Die Adressen, die Belege aus einem Testsystem erhalten

Speichern Sie und drücken Sie dann Test SharePoint und Test mail. Beide prüfen die Anmeldung und das Ziel, ohne etwas hochzuladen oder zu versenden. Die Schlüssel werden verschlüsselt auf dem Server gespeichert und nie wieder angezeigt.

8 Fehlersuche

Was Sie sehen	Was Sie tun
Insufficient privileges oder Authorization_RequestDenied	Ihrem Konto fehlt eine der Rollen aus Kapitel 2.1. Aktivieren Sie sie (zum Beispiel in Privileged Identity Management) und starten Sie das Skript erneut.
Eine Site steht unter NOT granted	Ihr Konto braucht die Rolle SharePoint-Administrator und muss Mitglied dieser Site sein. Fügen Sie sich der Site hinzu und starten Sie das Skript erneut.
There are 2 app registrations named ...	Eine App dieses Namens gibt es zweimal. Löschen Sie die nicht genutzte oder legen Sie Ihre mit einem anderen -AppName an.
... has no service principal	Schritt 1 wurde für diese Client-ID nicht abgeschlossen. Führen Sie Schritt 1 erneut aus; er legt an, was fehlt.
The mailbox ... was not found	Prüfen Sie die Adresse. Es muss ein Postfach in Exchange Online sein, keine Verteilerliste.
Test mail klappt, der Versand scheitert mit ErrorAccessDenied	Warten Sie nach dem Skript bis zu 30 Minuten und versuchen Sie es erneut.
Azure CLI (az) was not found	Starten Sie das Skript in Azure Cloud Shell (Kapitel 2.3).

8.1 Support

Balsoft GmbH, Herler Str. 109, 51067 Köln. Mail support@balsoft.de, Web www.balsoft.de. Bitte senden Sie die vollständige Ausgabe des Skripts mit; sie enthält keine geheimen Schlüssel.