HIVE BDC: MICROSOFT 365 SETUP

App registrations for mail and SharePoint

Document

Setup guide for IT administrators, version 1.0
12 October 2026

Product

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. All rights reserved. Changes to this document require the written consent of Balsoft GmbH. Reproduction of this document and disclosure to third parties are permitted only with the consent of Balsoft GmbH.

Contents

1 Overview 3

2 Before you start 3

2.1 Roles 3

2.2 What to have ready 3

2.3 Where to run the scripts 4

3 Download the scripts 4

4 SharePoint app 4

4.1 Step 1: create the app registration 4

4.2 Step 2: assign the permissions 5

5 Mail app 5

5.1 Step 1: create the app registration 5

5.2 Step 2: assign the permissions 5

6 Client secrets 6

7 Enter the values in Hive BDC 6

8 Troubleshooting 6

8.1 Support 7

1 Overview

Hive BDC can mail each document to its recipient and file it in SharePoint. For both it signs in to Microsoft 365 with an app registration in your Microsoft Entra ID. This guide sets up the two app registrations it needs. You only need the ones for the features you use: no mail, no mail app; no SharePoint, no SharePoint app.

There are two registrations so that each one holds only the permission it needs, and each permission is narrowed down further: the SharePoint app can write only to the sites you name, the mail app can send only as the one mailbox you name.

App registration	Permission	Limited to
Hive BDC SharePoint	Sites.Selected (application)	Write access on the sites you name (chapter 4)
Hive BDC Mail	Application Mail.Send in Exchange Online	Sending as one mailbox (chapter 5)

Each app is set up in two steps: step 1 creates the app registration without any permission, step 2 assigns its permissions. The steps can be done by different administrators. Each script shows the tenant it is signed in to and asks before it changes anything. It skips what already exists, so you can run it again at any time, for example to add a SharePoint site. With -WhatIf it only shows what it would do. The scripts never store a client secret; you create it in chapter 6.

2 Before you start

2.1 Roles

Each step needs these Microsoft Entra roles. One Global Administrator covers all of them except the site membership.

Step	Role
Step 1: create an app registration	Application Administrator (or Application Developer)
Step 2, SharePoint: admin consent for Sites.Selected	Global Administrator, or Privileged Role Administrator
Step 2, SharePoint: access to a site	SharePoint Administrator, and member of that site
Step 2, mail: send as one mailbox	Exchange Administrator (Organization Management in Exchange)

2.2 What to have ready

- SharePoint: the address of each site Hive BDC uploads to, for example https://contoso.sharepoint.com/sites/Invoices. The address of a library or folder in the site works as well.
- Mail: the mailbox the documents are sent from, for example invoices@contoso.com. It has to exist in Exchange Online; a shared mailbox is fine and needs no licence.

- Mail: one or more test recipients. Documents from a test system go to them instead of to customers or vendors.

2.3 Where to run the scripts

Use Azure Cloud Shell. It runs in the browser, is already signed in with your account, and has everything the scripts need: Azure CLI and the Exchange Online module. Nothing is installed on your computers.

1. Sign in to https://portal.azure.com with an administrator account of your tenant.
2. Open Cloud Shell with the terminal icon in the top bar, and choose PowerShell.
3. On the first start, Cloud Shell asks about storage. "No storage account required" is enough for these scripts.

Note: Step 2 signs in once more (SharePoint: for the site access, mail: for Exchange Online). Cloud Shell has no browser, so there that sign-in uses a code you enter at microsoft.com/devicelogin. Many organisations block sign-in by code with Conditional Access ("You don't have access to this"). Then run step 2 on your own computer: Windows PowerShell 5.1 or PowerShell 7 with Azure CLI installed, where the sign-in opens a browser. The mail script also needs the Exchange Online module there (Install-Module ExchangeOnlineManagement).

3 Download the scripts

Each app has two scripts, one per step. Paste the lines for the app you set up into Cloud Shell; they download the scripts into the current folder.

App	Step 1: create	Step 2: permissions
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
```

All scripts are plain text. You can read them before you run them on the Hive BDC page at balsoft.de, or with code New-HiveBDCMailApp.ps1 in Cloud Shell. The source is also public at github.com/balsoft-gmbh/hive-bdc in the scripts folder.

4 SharePoint app

4.1 Step 1: create the app registration

```
./New-HiveBDCSharePointApp.ps1
```

The script shows the tenant and your account and asks whether to continue; answer y. It creates the app registration "Hive BDC SharePoint" and its service principal (the enterprise application), without any permission. At the end it prints the Directory (tenant) ID, the Application (client) ID and the command for step 2. Note both IDs for chapter 7.

4.2 Step 2: assign the permissions

Run the script with the client ID from step 1 and the sites Hive BDC uploads to. Separate several sites with a comma.

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

1. Shows the tenant, the app and the sites, and asks whether to continue. Answer y.
2. Adds the permission Sites.Selected and grants admin consent. Sites.Selected alone gives access to no site at all.
3. Gives the app write access on each site. For this step the script signs in once more, because it needs the permission Sites.FullControl.All for your account: open the address shown, enter the code, sign in, and accept the permission request.

Another site later: run step 2 again with that site; everything else is skipped.

Note: With -AllSites instead of -SiteUrl the app gets Sites.ReadWrite.All and can write to every site in the tenant. Use it only if your security policy allows it; per-site access is the safer default.

5 Mail app

5.1 Step 1: create the app registration

```
./New-HiveBDCMailApp.ps1
```

As in chapter 4.1, for the app registration "Hive BDC Mail". Note the client ID.

5.2 Step 2: assign the permissions

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

1. Shows the tenant, the app and the mailbox, and asks whether to continue. Answer y.
2. Signs in to Exchange Online (address and code as in chapter 4.2) and allows the app to send as the one mailbox: the role Application Mail.Send, limited to a management scope that contains only this mailbox (RBAC for Applications).

The app deliberately gets no Mail.Send permission in Entra ID: that permission would allow sending as every mailbox of the tenant, and the Exchange limit would not narrow it. A Mail.Send consent that already exists is removed. Exchange Online needs up to 30 minutes to apply the limit; until then a test send can fail with ErrorAccessDenied, which is not an error in the setup.

Note: Custom Exchange scopes need a one-time switch that tenants which never customised Exchange have off. The script turns it on (Enable-OrganizationCustomization). Exchange then

needs up to an hour to apply it; if the script stops with that message, run it again later with the same parameters.

Note: In tenants without RBAC for Applications the script falls back to an application access policy: Mail.Send is consented in Entra ID and restricted to a mail-enabled security group that contains the mailbox.

6 Client secrets

Each app needs a client secret. Create it in the Microsoft Entra admin center and enter it directly in the Hive BDC dashboard (chapter 7). Please do not send it by mail or put it in a ticket.

1. Open https://entra.microsoft.com, then Applications, App registrations, All applications.
2. Select "Hive BDC SharePoint" (or "Hive BDC Mail"), then Certificates & secrets, New client secret.
3. Enter a description, for example HiveBDC, choose the validity (24 months is the longest offered), and add it.
4. Copy the Value at once. It is shown only this one time.

Note: Put a reminder in your calendar for the expiry date. Before it expires, create a new secret the same way and enter it in the dashboard; then delete the old one.

7 Enter the values in Hive BDC

Open the Hive BDC dashboard on the server, then Settings and the Connections tab.

Section	Field	Value
SharePoint	Tenant ID, Client ID, Client secret	Directory (tenant) ID and Application (client) ID of "Hive BDC SharePoint", and its secret
Document mail	Client ID, Client secret	Application (client) ID of "Hive BDC Mail", and its secret
Document mail	Tenant ID	Empty when it is the same tenant as SharePoint
Document mail	Send from	The mailbox from chapter 5
Document mail	Test recipients	The addresses that receive documents from a test system

Save, then press Test SharePoint and Test mail. Both check the sign-in and the target without uploading or sending anything. The secrets are stored encrypted on the server and are never shown again.

8 Troubleshooting

What you see	What to do
Insufficient privileges, or Authorization_RequestDenied	Your account lacks one of the roles in chapter 2.1. Activate it (for example in Privileged Identity Management) and run the script again.
A site is listed under NOT granted	Your account needs SharePoint Administrator and must be a member of that site. Add yourself to the site and run the script again.
There are 2 app registrations named ...	An app with that name exists twice. Delete the one you do not use, or create yours with another -AppName.
... has no service principal	Step 1 was not completed for this client ID. Run step 1 again; it creates what is missing.
The mailbox ... was not found	Check the address. It has to be a mailbox in Exchange Online, not a distribution list.
Test mail works, sending fails with ErrorAccessDenied	Wait up to 30 minutes after the script, then try again.
Azure CLI (az) was not found	Run the script in Azure Cloud Shell (chapter 2.3).

8.1 Support

Balsoft GmbH, Herler Str. 109, 51067 Köln. Mail support@balsoft.de, web www.balsoft.de. Please include the full output of the script when you contact us; it contains no secrets.