Table of Contents

[1. First Time Enablement 2](#_Toc197072626)

[1.1 Register Vault Application in Entra Admin Center 2](#_Toc197072627)

[1.2 Create SharePoint Site and Enable Collaborative Authoring with PowerShell 3](#_Toc197072628)

[1.3 SharePoint Site Hardening – Option 1 – in SharePoint 3](#_Toc197072629)

[1.4 SharePoint Site Hardening - Option 2 - with PowerShell 4](#_Toc197072630)

[1.5 Authorize Connection between Vault and Office 365 5](#_Toc197072631)

[2. Enablement in Additional Vault(s) 6](#_Toc197072632)

[2.1 Add Redirect URI(s) to the App Registration 6](#_Toc197072633)

[2.2 Authorize Connection between Vault and Office 365 6](#_Toc197072634)

[3. Re-enablement after a Vault Refresh 7](#_Toc197072635)

[3.1 Re-authorize the Connection between Vault and Office 365 7](#_Toc197072636)

[4. External User Setup 8](#_Toc197072637)

[4.1 Grant Application Registration Permissions for Automated Guest Invitations (Optional) 8](#_Toc197072638)

[4.2 Enable External Collaboration at the SharePoint Tenant Level 8](#_Toc197072639)

[4.3 Enable External Collaboration at the Root & Site Collection Level 8](#_Toc197072640)

[4.4 Invite External Users to Azure (Optional) 9](#_Toc197072641)

[4.5 Add User(s) to Vault 9](#_Toc197072642)

[5. Security Token Renewal 9](#_Toc197072643)

[5.1 Generate New Security Token in Entra 10](#_Toc197072644)

[5.2 Re-authorize Connection between Vault and Office 365 10](#_Toc197072645)

[6. Powershell Script Variables 10](#_Toc197072646)

# First Time Enablement

|  |  |  |
| --- | --- | --- |
| Register Vault Application in Entra Admin Center | | |
| **Step** | **Completed** | **Comments** |
| Navigate to Vault Admin > Settings > Checkout Settings and click **Edit** |  |  |
| In a separate window, login as Admin to Entra Admin Center |  |  |
| Click on **App Registrations** |  |  |
| Click on **New Registration** |  |  |
| Give it a name and enter a redirect URI  (format must be  https://Your Vault DNS/ui/clientTiles/office365/oauth2) |  |  |
| Click **Register** |  |  |
| Copy and paste the newly created *Directory (tenant) ID* and *Application (client) ID* from Entra into Vault Checkout Settings |  | Directory (tenant) ID:  ­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Application (client) ID:  ­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| From the Entra app page, click **API permissions** |  |  |
| Click **Add a permission** |  |  |
| Click **Microsoft Graph** and then **Application Permissions** |  |  |
| Under Sites section, check off:   * Sites.Selected   Under Users section, check off:   * User.ReadBasic.All\*   Under Users section, check off:   * User.Invite.All \*\*   Under Directory section, check off:   * Directory.ReadWrite.All \*\*   \*This permission is required if using collaborative authoring workflow actions  \*\*These permissions are for the optional Auto Invite External Users feature |  |  |
| Click **Add permissions** |  |  |
| Click **Grant admin consent for <Tenant Name>** |  |  |
| From the Entra app page, click **Certificates & secrets** |  |  |
| Click **New client secret** |  |  |
| Add a description and pick the longest acceptable expiration period (*recommended – Never*) |  |  |
| Click **Add** |  |  |
| Copy and paste your newly created **Secret Value** from Azure into Vault Checkout Settings |  | Secret Value:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Create SharePoint Site and Enable Collaborative Authoring with PowerShell | | |
| **Step** | **Completed** | **Comments** |
| Install PowerShell (at least version 7) |  |  |
| Open PowerShell and install PnP PowerShell Module with the following command:  Install-Module PnP.PowerShell -RequiredVersion 2.12 |  |  |
| Download and open the PowerShell scripts provided in [Vault Help](https://platform.veevavault.help/en/lr/56840/#granting-the-app-access-to-the-sharepoint-team-site) |  |  |
| Prepare the variables in the SitePnP.ps1 script. Each variable must be in a quote. Example: $alias = "Alias"  $adminUrl = “The URL of the SharePoint Admin Center”  $siteBaseUrl = “The base URL for SharePoint sites in the tenant”  $siteTitle = “The title of the new SharePoint site”  $owner = “The email address of the site owner”  $alias = “The unique alias for the SharePoint site”  $tenantUrl = “The tenant domain name used for Entra app registrations”  $appId = “The App ID of the Entra App created in 1.1”  $displayName = “The name of the Azure App created in 1.1”  $siteUrl = “The full URL of the SharePoint site constructed using $siteBaseUrl + $alias”  $entraIDApp = “ID of the Azure Admin App that grants Collaborative Authoring Azure App access to the SharePoint site. If left blank, it will be dynamically created upon running this script”.  $adminAppName = "Veeva CA Admin App"  Important: See [Powershell Script Variables](#_Powershell_Script_Variables) for more information on how to set and use these variables. |  |  |
| Go the folder where you saved the PowerShell script.  Run the ‘SitePnP.ps1’ script in PowerShell command prompt as follows. If you have updated the name and the new name includes spaces or special characters, it is recommended to specify the entire file name within double quotes to avoid any issues with spaces & characters in the file name.  .\SitePnP.ps1 |  |  |
| Navigate to the newly Created SharePoint site’s **Documents** Library |  |  |
| Copy and paste the URL from SharePoint into Vault Checkout Settings |  | URL:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| SharePoint Site Hardening – Option 1 – in SharePoint | | |
| **Step** | **Completed** | **Comments** |
| Login to SharePoint as the administrator user who created the site in **1.2** |  |  |
| Navigate to the site created in **1.2** |  |  |
| From the site Settings, click **Site permissions** |  |  |
| Click **Change how members can share** |  |  |
| Select*Only site owners can share files, folders, and the site* and **disable** Allow access requests |  |  |
| Click **Save** |  |  |
| Verify that the Site Owner group only includes the administrator who created the site in **1.2** |  |  |
| Select **Advanced Site Permissions** |  |  |
| Select **Permission Levels** |  |  |
| Select **Contribute Permission Level** |  |  |
| Disable the **Delete Items** list permission |  |  |
| Click **Submit** |  |  |
| Click **Documents** |  |  |
| Open Settings |  |  |
| Click **Library Settings** |  |  |
| Click **Permissions for this document library** |  |  |
| Select *Site Members* and *Site Visitors,* click **Remove User Permissions,** and confirm the prompt |  |  |
| Return to the **Documents** library |  |  |
| Copy and paste the URL from SharePoint into Vault Checkout Settings |  |  |
| SharePoint Site Hardening - Option 2 - with PowerShell | | |
| **Step** | **Completed** | **Comments** |
| Download SharePoint Online Client Components SDK from Microsoft’s [Download Center](https://www.microsoft.com/en-us/download/details.aspx?id=42038) |  |  |
| Open PowerShell and install PnP PowerShell Module with the following command:  Install-Module -Name Microsoft.Online.SharePoint.PowerShell |  |  |
| Prepare the variables in the SiteHardening.ps1 script  $siteTitle = “The title of the new SharePoint site”  $siteUrl = “The full URL of the SharePoint site constructed using $siteBaseUrl + $alias” |  |  |
| Run the SiteHardening .ps1 script in SharePoint Online Management Shell  .\ sitehardening.ps1 |  |  |
| Authorize Connection between Vault and Office 365 | | |
| **Step** | **Completed** | **Comments** |
| Within Vault Checkout Settings, click **Authorize** |  |  |
| Once your Integration Status is verified within Vault Checkout Settings, click **Save** |  |  |

# Enablement in Additional Vault(s)

|  |  |  |
| --- | --- | --- |
| Add Redirect URI(s) to the App Registration | | |
| **Step** | **Completed** | **Comments** |
| Login as Admin to Entra Admin Center |  |  |
| Click on **App Registrations** |  |  |
| Find the App Registration initially created for Collaborative Authoring in **1.1** |  |  |
| From the Entra app page, click **Authentication** |  |  |
| Click **Add a platform** |  |  |
| Select **Web** as the application type |  |  |
| Enter a **Redirect URI** (format must be  https://Your Vault DNS/ui/clientTiles/office365/oauth2) |  |  |
| Click **Configure** |  |  |
| Authorize Connection between Vault and Office 365 | | |
| **Step** | **Completed** | **Comments** |
| Navigate to Vault Admin > Settings > Checkout Settings and click **Edit** |  |  |
| Copy and paste the *Directory (tenant) ID* and *Application (client) ID* from **1.1** into Vault Checkout Settings |  |  |
| Copy and paste your **Secret Value** from **1.1** into Vault Checkout Settings |  |  |
| Copy and paste the URL from **2** into Vault Checkout Settings |  |  |
| Click **Authorize** |  |  |
| Once your Integration Status is verified within Vault Checkout Settings, click **Save** |  |  |

# Re-enablement after a Vault Refresh

|  |  |  |
| --- | --- | --- |
| Re-authorize the Connection between Vault and Office 365 | | |
| **Step** | **Completed** | **Comments** |
| Navigate to Vault Admin > Settings > Checkout Settings and click **Edit** |  |  |
| Copy and paste the *Directory (tenant) ID* and *Application (client) ID* from **1.1** into Vault Checkout Settings |  |  |
| Copy and paste your **Secret Value** from **1.1** into Vault Checkout Settings |  |  |
| Copy and paste the URL from **1.2** into Vault Checkout Settings |  |  |
| Click **Authorize** |  |  |
| Once your Integration Status is verified within Vault Checkout Settings, click **Save** |  |  |

# External User Setup

External users are collaborators with email addresses from different domains. When using Collaborative Authoring with external users, you can enable automatic invitations through Azure in your Vault. Once automatic invitations are enabled, Vault will send external users an email invitation when they click Edit, automatically adding them to the session.

|  |  |  |
| --- | --- | --- |
| Grant Application Registration Permissions for Automated Guest Invitations (Optional) | | |
| **Step** | **Completed** | **Comments** |
| Login as Admin to Entra Admin Center |  |  |
| Click on **App Registrations** |  |  |
| Find the App Registration initially created for Collaborative Authoring in **1.1** |  |  |
| From the Entra app page, click **View API permissions** |  |  |
| Click **Add a permission** |  |  |
| Click **Microsoft Graph** and then **Application Permissions** |  |  |
| Under Sites section, check off:   * Sites.Selected   Under Users section, check off:   * User.Invite.All \*\*   Under Directory section, check off:   * Directory.ReadWrite.All \*\*   \*\*These permissions are for the optional Auto Invite External Users feature |  |  |
| Click **Add permissions** |  |  |
| Enable External Collaboration at the SharePoint Tenant Level | | |
| **Step** | **Completed** | **Comments** |
| Login to the Office365 Admin Center |  |  |
| Navigate to SharePoint Admin |  |  |
| Under Policies, Click **Sharing** |  |  |
| Within the *External sharing > Content can be shared with:* section, allow for sharing with external users by making a selection other than **Only people in your organization** |  |  |
| Enable External Collaboration at the Root & Site Collection Level | | |
| **Step** | **Completed** | **Comments** |
| Click **Sites** |  |  |
| Click **Active Sites** |  |  |
| Locate **Root** site  (ex. Site name: *Company Team Site*   URL: *company.sharepoint.com*) |  |  |
| Click on **Site Name** |  |  |
| Click on the **Policies** tab |  |  |
| Click Edit under External Sharing |  |  |
| Within the *External sharing > Site content can be shared with:* section, allow for sharing with external users by making a selection other than **Only people in your organization** |  |  |
| Click **Save** |  |  |
| Click **Active Sites** |  |  |
| Locate the site that you created in **1.2** |  |  |
| Click on the **Policies** tab |  |  |
| Click Edit under External Sharing |  |  |
| Within the *External sharing > Site content can be shared with:* section, allow for sharing with external users (*recommended –* **Existing guests only**) |  |  |
| Click **Save** |  |  |
| Invite External Users to Azure (Optional) | | |
| Skip this step if you are not using Vault to Automate Invites. | | |
| **Step** | **Completed** | **Comments** |
| Navigate to your Entra Admin Center |  |  |
| Click **Users** |  |  |
| Click **New Guest User** |  |  |
| Ensure *Invite User* is selected and enter guest user information |  |  |
| Click **Invite** |  |  |
| Add User(s) to Vault | | |
| **Step** | **Completed** | **Comments** |
| Navigate to Vault Admin > Users & Groups |  |  |
| Click **Create** |  |  |
| Add user details and ensure that the user’s email address exactly matches the email in Entra |  |  |
| Click **Save** |  |  |

# Security Token Renewal

Security tokens created in Azure are typically assigned an expiration date. The steps below outline the process whereby new tokens can be generated for the integration. This step can be completed prior to the secret expiring minimizing any disruption on checkout documents.

|  |  |  |
| --- | --- | --- |
| Generate New Security Token in Entra | | |
| **Step** | **Completed** | **Comments** |
| Navigate to Vault Admin > Settings > Checkout Settings and click **Edit** |  |  |
| In a separate window, login as Admin to Entra Admin Center |  |  |
| Click on **App Registrations** |  |  |
| Find the App Registration initially created for Collaborative Authoring in **1.1** |  |  |
| From the Azure app page, click **Certificates & secrets** |  |  |
| Click **New client secret** |  |  |
| Add a description and pick the longest acceptable expiration period (*recommended – Never*) |  |  |
| Click **Add** |  |  |
| Copy and paste your newly created **Secret Value** from Azure into Vault Checkout Settings |  | Secret Value:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Re-authorize Connection between Vault and Office 365 | | |
| **Step** | **Completed** | **Comments** |
| Within Vault Checkout Settings, click **Authorize** |  |  |
| Once your Integration Status is verified within Vault Checkout Settings, click **Save** |  |  |

For more information on Collaborative Authoring, visit [Vault Help](http://vaulthelp2.vod309.com/wordpress/admin-user-help/documents-admin-user-help/configuring-collaborative-authoring-with-microsoft-office/) & [Collaborative Authoring Resource Hub](https://www.veeva.com/products/vault-platform/collaborative-authoring/).

# Powershell Script Variables

*$adminUrl = "https://test-admin.sharepoint.com"*

You can get this URL by navigating to your SharePoint Admin center, and copying the first part of the URL there:

A screenshot of a computer

AI-generated content may be incorrect.

*$siteBaseUrl = "https://test.sharepoint.com/sites/"*

You can get this URL by navigating to any existing SharePoint site and the URL will be up through “/sites/”:

A screenshot of a browser

AI-generated content may be incorrect.

Note: it is important that it end with a forward slash

*$siteTitle = "Site Title"*

This can be defined however is preferred, i.e. “Vault Collaboration”

*$owner = "owner@domain.com"*

This would be the Microsoft username for the administrator who is running the script (i.e. “michaelferrell@devopsveeva.onmicrosoft.com”)

*$tenantUrl = "domain.com"*

You can get this URL by navigating to the Microsoft Entra Admin Center, and the Overview tab. The URL needed is the Primary Domain field:

A screenshot of a computer

AI-generated content may be incorrect.

*$appId = "appId"*

This is the Application (client) ID for the app registration for your Vaults:

A screenshot of a computer

AI-generated content may be incorrect.

*$displayName = "Display Name"*

This is the Display Name for the app registration for your Vaults:

A screenshot of a computer

AI-generated content may be incorrect.

*$siteUrl = “https://test.sharepoint.com/sites/siteAlias”*

If you are setting up a net new site, nothing is needed for this variable (the script will create this using $siteBaseUrl and $alias. If you’re updating an existing site:

This is the URL for your existing SharePoint site, which you can get by navigating to the site in the SharePoint Admin center and copying the Site Address:

A screenshot of a computer

AI-generated content may be incorrect.

*$adminAppName = "Admin App Name"*

The script will create a Entra Admin ID App with the name you specify in this variable. This new app will get ‘AllSites.FullControl’ permission, and you can give this app any name that you prefer. This site permission is needed to grant your existing application permission to manage your SharePoint site (without a Service Account).

The first time you run the script, this variable should be used and the $entraIDApp variable should be commented out. For subsequent uses of the script, the newly created Entra Admin ID app can be used to configure Collaborative Authoring in other Vault environments in your organization. Record the app Id for future use and comment this variable out if you are planning to run this script again for other Vault environments.

This admin app is required to update permissions, but once all updates are made to existing app registrations and SharePoint sites, this app can be deleted.

*$entraIDApp = "entraIdApp"*

If you already have an Entra Admin app created using the above variable $adminAppName (that has the AllSites.FullControl permission), then comment out the variable $adminAppName and enter the Application (client) ID for that Entra Admin ID app here, rather than using $adminAppName to create a new Entra Admin App again.