Table of Contents

[1. First Time Enablement 2](#_Toc191398211)

[1.1 Register Vault Application in Azure Active Directory 2](#_Toc191398212)

[1.2 Create SharePoint Site and Enable Collaborative Authoring with PowerShell 2](#_Toc191398213)

[1.3 SharePoint Site Hardening with PowerShell 3](#_Toc191398214)

[1.4 Authorize Connection between Vault and Office 365 4](#_Toc191398215)

[2. Enablement in Additional Vault(s) 5](#_Toc191398216)

[2.1 Add Redirect URI(s) to the App Registration 5](#_Toc191398217)

[2.2 Authorize Connection between Vault and Office 365 5](#_Toc191398218)

[3. Re-enablement after a Vault Refresh 6](#_Toc191398219)

[3.1 Re-authorize the Connection between Vault and Office 365 6](#_Toc191398220)

[4. External User Setup 7](#_Toc191398221)

[4.1 Grant Application Registration Permissions for Automated Guest Invitations (Optional) 7](#_Toc191398222)

[4.2 Enable External Collaboration at the SharePoint Tenant Level 7](#_Toc191398223)

[4.3 Enable External Collaboration at the Root & Site Collection Level 7](#_Toc191398224)

[4.4 Invite External Users to Azure (Optional) 8](#_Toc191398225)

[4.5 Add User(s) to Vault 8](#_Toc191398226)

[5. Security Token Renewal 9](#_Toc191398227)

[5.1 Generate New Security Token in Azure 9](#_Toc191398228)

[5.2 Re-authorize Connection between Vault and Office 365 9](#_Toc191398229)

# First Time Enablement

|  |  |  |
| --- | --- | --- |
| Register Vault Application in Azure Active Directory | | |
| **Step** | **Completed** | **Comments** |
| Navigate to Vault Admin > Settings > Checkout Settings and click **Edit** |  |  |
| In a separate window, login as Admin to Azure Portal and open Azure Active Directory |  |  |
| 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 Azure into Vault Checkout Settings |  | Directory (tenant) ID:  ­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Application (client) ID:  ­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| From the Azure 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.Invite.All \*\*   Under Directory section, check off:   * Directory.ReadWrite.All \*\*   \*\*These permissions are for the optional Auto Invite External Users feature |  |  |
| Click **Add permissions** |  |  |
| Click **Grant admin consent for <Tenant Name>** |  |  |
| 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:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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 |  |  |
| 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 Azure app registrations”  $appId = “The App ID of the Azure 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. |  |  |
| Run the SitePnP.ps1 script in PowerShell  .\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 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 Azure Portal and open Azure Active Directory |  |  |
| Click on **App Registrations** |  |  |
| Find the App Registration initially created for Collaborative Authoring in **1.1** |  |  |
| From the Azure 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 Azure Portal and open Azure Active Directory |  |  |
| Click on **App Registrations** |  |  |
| Find the App Registration initially created for Collaborative Authoring in **1.1** |  |  |
| From the Azure 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 Azure Active Directory 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 Azure Active Directory |  |  |
| 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 Azure | | |
| **Step** | **Completed** | **Comments** |
| Navigate to Vault Admin > Settings > Checkout Settings and click **Edit** |  |  |
| In a separate window, login as Admin to Azure Portal and open Azure Active Directory |  |  |
| 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/).