Quadrotech Archive Shuttle 11.1
Planning Guide

Contents

Introduction

This guide contains information that will help you plan your Quadrotech Archive Shuttle migrations.

Key terms

The following table introduces the terminology that is used throughout Archive Shuttle documentation, videos, and the user interface.

TERM	ITEM + DESCRIPTION
Link	**Enterprise Vault** A Link is a Vault Store **Exchange** A Link is an Exchange database **Office 365** A connection to Office 365 **PST** A connection to a PST Output Area **Proofpoint** A connection to a Proofpoint output area **EAS** A connection to an EAS IIS Server **Metalogix** A connection to a Metalogix server
Container	**Enterprise Vault** A Container is a Vault / Archive **Exchange** A Container is an Exchange mailbox **Office 365**

TERM	ITEM + DESCRIPTION
	A Container is an Office 365 mailbox or Personal Archive **PST** A container is a PST file **Proofpoint** A container currently has no applicable context **EAS** A container is an archive relating to a user. **Metalogix** A container is an archive
Item	**Enterprise Vault** An Item is an archived Item. **Exchange** An Item is an item in the mailbox **Office 365** An Item is an item in the mailbox or personal archive **PST** An item is an item inside a PST file **Proofpoint** An item currently has no applicable context **EAS** An item is a message in the archive **Metalogix** An item is a message in the archive

2

Modules

Archive Shuttle has several modules that it uses to communicate with different systems to complete tasks. For best performance, modules are usually installed on the systems they interact with. Information relating to where each module should be installed is given in a later section of this document.

The following table describes each of the Modules which are available with Archive Shuttle:

MODULE	DESCRIPTION
Active Directory Collector Module	The Active Directory Collector Module is responsible for resolving SIDs in AD and for retrieving all necessary data about a user (e.g., department) that might be necessary to filter data. It also collects information about the Exchange configuration of users (For example, on which Exchange Server / Database Availability Group (DAG) the user has a mailbox, if the mailbox has an Exchange Archive Mailbox enabled or not, and so on)
Enterprise Vault Collector Module	The Enterprise Vault Collector Module interacts with an Enterprise Vault Directory and is responsible for collecting all necessary metadata about Vault Stores, Archives, Items' in each Archive and Enterprise Vault shortcuts in a mailbox.
Enterprise Vault Provisioning Module	The Enterprise Vault Provisioning Module creates new temporary archives for ingestion. It is able to map a temporary Archive to a User and can enable, disable, rename and ZAP existing Archives. This module utilizes EVPM to perform many tasks.
Enterprise Vault Export Module	The Enterprise Vault Export Module is responsible for exporting data from Enterprise Vault. It is multi-threaded and uses the Enterprise Vault APIs for accessing archived items. The exported data is stored on a Windows Network Share (SMB/CIFS). Npte that SMB 2 and SMB 3 are supported.
Enterprise Vault Import Module	The Enterprise Vault Import Module is responsible for ingesting data into the newly created or mapped archives in the target Enterprise Vault environment. It is multi-threaded and uses the Enterprise Vault APIs to ingest data. The data to import is read from the export location (SMB/CIFS Share). Note that SMB 2 and SMB 3 are supported.

MODULE	DESCRIPTION
Enterprise Vault Shortcut processing Module	After migration has finished, the Enterprise Vault shortcuts in a users' mailbox will be updated so that they refer to the migrated archive. Note: Non-shortcut items, such as calendar items, are also updated.
Exchange Import Module	The Exchange Import Module ingests data into a users' mailbox. This can be the primary mailbox or an Exchange Personal Archive mailbox.
Metalogix Export Module	This module collects data from Metalogix Archive Manager and extracts data from that system.
Office 365 Module	The Office 365 Module processes data relating to migrations to Office 365. It collects metadata from Office 365, ingests items into Office 365 mailboxes or Personal Archives, and post processes the target to remove Enterprise Vault shortcuts and pending items.
Native Format Import Module	The Native Format Import Module allows for data to be exported to PST file format. The resultant files are stored on a configurable destination folder (UNC path) and the files can be split at predetermined sizes. The filenames can also be customized if required.
Proofpoint Module	This module takes exported source environment data and prepares the data for Proofpoint ingestion.
EAS Module	This module collects data from Zantaz EAS and extracts data from that system.
PST Export Module	This module collects data from PST files and extracts the data from them.
Dell Archive Manager Module	This module collects data from DAM and extracts the data from that system.
SourceOne Module	This module collects data from SourceOne and extracts the data from that system.
Storage Import Module	This module writes native archive output files to the desired storage location. It optionally converts MSG files to EML and writes them to a storage provider of choice at scale and speed. This enables ingestion to Azure, Amazon S3, and UNC.

Planning for migrations

> **NOTE:** Before proceeding with a migration, you need to determine the priority of your migration waves. Archive Shuttle recommends that leavers, journals and larger archives should be prioritized first. Projects with complex sources also need careful consideration.

Planning for migrations to Amazon S3

If you plan to migrate data to Amazon S3, install the Storage Import Module before beginning.

When setting up your Amazon S3 account(s) using the Credential Editor, makes sure the AWS Region matches your Amazon S3 account.

You'll use the Storage Import and Storage Provider target when configuring the workflow policy, mapping wizard, etc.

While setting up the migration, use the Storage Import Module tab of the System Configuration page to, for example, set item/archive parallelism, set up conversion of MSG to EML, fail items permanently on specified errors, etc.

This is how the migrated archive and messages look on the storage provider (Amazon S3):

Planning for migrations to Azure Blob

If you plan to migrate data to Azure Blob, install the Storage Import Module before beginning.

You'll use the Storage Import and Storage Provider target when configuring the workflow policy, mapping wizard, etc.

While setting up the migration, use the Storage Import Module tab of the System Configuration page to, for example, set item/archive parallelism, set up conversion of MSG to EML, fail items permanently on specified errors, etc.

Planning for migrations to Enterprise Vault

When migrating data to an Enterprise Vault environment, it is essential that the option in the provisioning group to "Automatically enable mailboxes" is turned off. If it is not turned off, there is the possibility that duplicate archives may be created in the target.

Planning for migrations to Exchange

As with the ingestion in to Office 365, ingestion in to Exchange may be subject to throttling limits within Microsoft Exchange. A knowledge base article has been created which can help raise these limits.

By default the Exchange Import Module will attempt to ingest items into the chosen target mailbox or personal archive three times using AIP and then will fall back to trying Exchange Web Services (EWS). If they all fail, then the ItemRoutingErrorCount will be incremented, and the item will be counted as failed (and it will be visible on the Failed Items screen, and retried from time to time).

Planning for Office 365 migrations

Microsoft throttles connections and bandwidth usage to their cloud service – Office 365.

http://technet.microsoft.com/en-us/library/exchange-online-limits.aspx

There are some steps that can be taken to improve the throughput and performance when migrating to Office 365. These are described in this section. In addition it is recommended that Microsoft be contacted and a request made to increase the throttling limits whilst the data migration is being undertaken.

Mailbox or Personal Archive

When planning your Office 365 migration, it's important to discuss if you are migrating to either a mailbox or a personal archive. If you're migrating to a personal archive, this must be enabled previously to your migration.

Remember that there might be different size and item limits on either choice.

Item size limits

There may be size limits set by Microsoft on your mailboxes when being ingested into Office 365. For more information on this, including how to increase mailbox size limits, see Size Limits When Ingesting into Office 365.

Authorization

You must use OAuth to authenticate when using Archive Shuttle. For more on OAuth, click here.

Throttling

You may need to lift throttling restrictions for your project. Restrictions are set by Microsoft, but lifting them for a set period of time (30, 60 or 90 days) is a straight forward process. Check out more on this here.

Mailbox or Personal Archive

When planning your Office 365 migration, it's important to discuss if you are migrating to either a mailbox or a personal archive. If you're migrating to a personal archive, this must be enabled previously to your migration.

Remember that there might be different size and item limits on either choice.

Item size limits

There may be size limits set by Microsoft on your mailboxes when being ingested into Office 365. You can, however, increase the size of the mailbox. There may be size limits set by Microsoft on your mailboxes when being ingested into Office 365. For more information on this, including how to increase mailbox size limits, click here.

Journal Transformation/Journal Splitting

Migrating journals requires thought on whether you would like to process them as Journal Transformation, or journal splitting. For more on this, click here.

Migrating leavers

Migrating leavers to Office 365 takes further consideration. For more on this, click here.

Size limits when ingesting into Office 365

For quite some time there has been a limit imposed by Microsoft on the size of individual items that can be ingested into Office 365 by third parties. This limit was 25 Mb. The limits for system-provided applications has been increased, and now, the limits for third parties has also been increased. This section explains how to take advantage of this increase.

Details

The default limit on a new Office 365 tenant is still 25 Mb, but this can be increased per user, or across the board for all users.

To increase the limit for an individual user:

In the Office 365 Admin Center, locate the user and change the max send and max receive sizes:
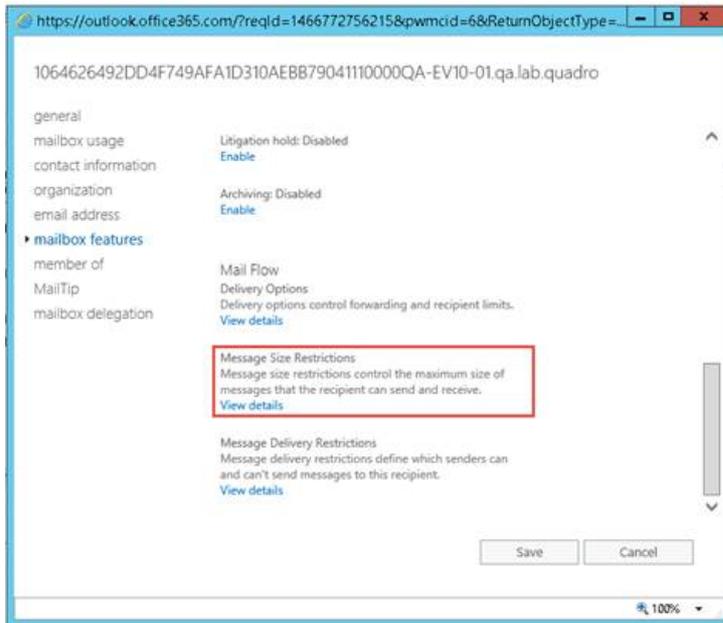
To increase the size for multiple users:

To edit size for multiple users. Shift + Click to select multiple recipients, then click the Update… link on the right side to modify those user's message size restrictions.
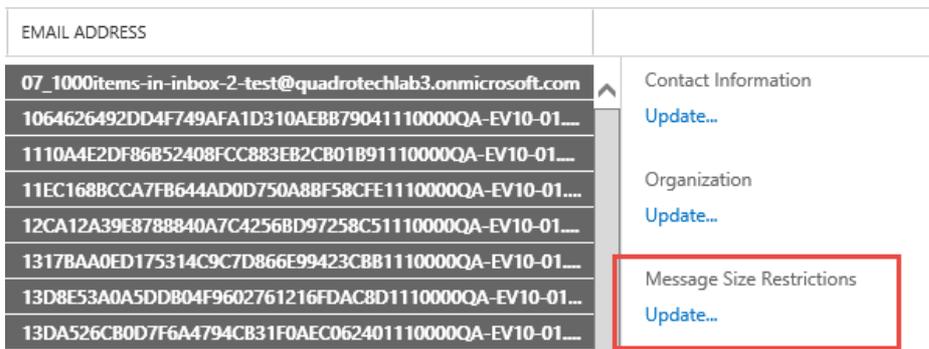
To increase the limit across the board:

Go to Recipients, Mailboxes, Click … and choose Set default message size restrictions
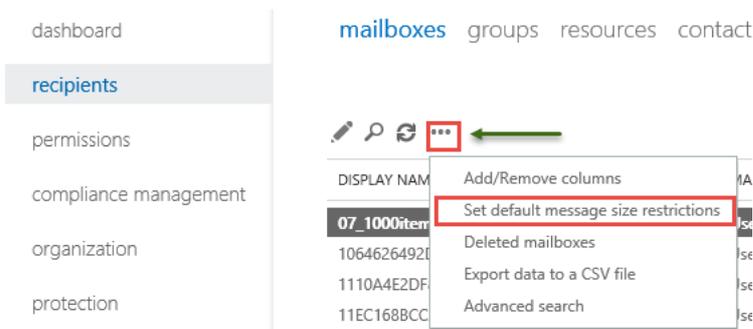
To increase the limits via PowerShell:

Limits can also be changed by PowerShell as follows:

For a single user:

```
Set-Mailbox -identity user@somedomain.com -MaxSendSize 75Mb -MaxReceiveSize 75Mb
```

For multiple mailboxes:

```
{"alias","alias2","alias3") | % {Set-Mailbox -identity $_ -MaxSendSize 75Mb -MaxReceiveSize 75Mb}
```

For all mailboxes:

```
Get-Mailbox | Set-Mailbox -MaxSendSize 75Mb -MaxReceiveSize 75Mb
```

To change the default:

```
Get-MailboxPlan | Set-MailboxPlan -MaxSendSize 75Mb -MaxReceiveSize 75Mb
```

> **i** | **NOTE:** Archive Shuttle has seen items more than 120 Mb ingest successfully after making these changes.

Using OAuth Authentication

Archive Shuttle can be configured to use OAuth to authenticate with Microsoft Office 365, using a Certificate and/or Secret. Read the step-by-step guide below on how to configure OAuth using Secret and a certificate. For more on this, click here.

Considerations when using OAuth

- OAuth is currently supported over both Exchange Online and PowerShell endpoints.

- If you would like to use OAuth without a Global Administrator account, a certificate with thumbprint needs to be configured together with an installed Exchange Online PowerShell v3 module. Otherwise, a Global Administrator account is required. Click here for more information.

- You cannot utilize more than one service account when using OAuth.

- Basic authentication in Windows Remote Manager (WinRM) only needs to be enabled when a project's scope includes mapping source retention categories to retention labels in Exchange Online. Click here for more information.

Credential Editor

An account with Global Administration rights from Archive Shuttle 10.3 and below in Credential Editor. A Global Admin account is not required in later versions.

Considerations when using the Credential Editor

- This is only when using a certificate thumbprint with installed Exchange Online PowerShell v3 (EXO v3). Click here for more information.

- An account with Global Administration rights when using the Credential Editor is still required when using an Application Secret or using certificate thumbprint without installed Exchange Online Powershell v3 module.
- For more on configuring OAuth for GCC and GCC High tenants by configuring the Credential Editor, click here.

- If using Microsoft Graph, ensure that the Azure App Registration section has been filled, regardless if OAuth is being used. If Azure App Registration is left empty, an error will occur.

Minimum permissions required for the account are listed on the *Quadrotech Archive Shuttle Installation Guide.*

Configuring OAuth with a Secret

Step 1: Create a new Registered Application in Azure
To get an application ID:
1. Go to https://portal.azure.com and log in to your Office 365 tenant with an administrator account.
2. From the left menu, select **Azure Active Directory** > **App registrations**.
3. Click **New registration**.
4. Enter a name.
5. From the **Supported account types,** select *Supported Account Type – Single tenant*.
6. Don't enter anything for **Redirect URI (optional).** Leave it as it is.
7. Click **Register.**
8. Copy the **Application (client) ID** and save it somewhere secure that you will remember. You will need it later.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

| AS_oAuth | ✓ |

Supported account types

Who can use this application or access this API?

- ◉ Accounts in this organizational directory only (Quadrotech Solutions AG - LAB only - Single tenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

| Web ⌄ | e.g. https://myapp.com/auth |

Step 2: Configure Permissions, Roles and Secret

Configure Application Permissions: Return to the Azure portal and access **Azure Active Directory** > **App registrations** > **owned applications**. Then find the application you created in Step 1 above.

1. Select your application, and then select **API Permissions**.
2. Click **Add a Permission.**
3. In the **Request API permissions** section > Select **APIs my organization uses**, search for **Office 365 Exchange Online** and select this API.
4. Click **Application Permissions**
5. In the **Permissions** list section, select the **full_access_as_app** listed in this section.
6. Click **Add permissions.**
7. Click **Grant Admin consent**.

Assign **User Administrator** role to the registered Application:
1. Navigate to **Active Directory - Roles and Administrators**
2. Find and open the **User Administrator** role
3. Click on **Add Assignments**
4. Search for the registered application (by Display Name)
5. Select the application and click **Add**.

The application is now recognized as Service Principal for the User Administrator role.

You can also use Exchange Online groups for basic migration scenarios. For more on this, click here.

NOTES:

- An Azure Active Directory Premium license is required for these steps.

- This role is mandatory to collect mailboxes. For more on this role, click here.

Configure Application Secret:

1. Go to Certificates & Secrets and click the **New Client Secret** button.
2. Enter a descriptive name.
3. Choose an Expiry duration for the Secret (it is recommended to set the secret to not expire)
4. Click **Add**.
5. Copy the **Secret** created and save it somewhere. You will need it later.

Step 3: Add your Application ID and Secret on the server running the Archive Shuttle Office 365 Import module.

To do this:

1. In Archive Shuttle, open the Credential Editor while logged in as the account the module is running under.
2. Select the **Office 365 OAuth** tab and click **Add**.
3. Enter the **Name (free format text)**, **Application ID**, **Tenant** (eg. tenant.onmicrosoft.com) and **Secret Value.**
4. Save and close the Credential Editor.
5. Restart the Office 365 module to force settings to take immediate effect.

Configuring OAuth with a certificate

Step 1: Create a new Registered Application in Azure

To get an application ID:

1. Go to https://portal.azure.com and log in to your Office 365 tenant with an administrator account.
2. From the left menu, select **Azure Active Directory** > **App registrations**.
3. Click **New registration**.
4. Enter a name.
5. From the **Supported account types,** select *Supported Account Type – Single tenant*.
6. Don't enter anything for **Redirect URI (optional).** Leave it as it is.
7. Click **Register.**
8. Copy the **Application (client) ID** and save it somewhere you will remember and securely. You will need it later.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

AS_oAuth ✓

Supported account types

Who can use this application or access this API?

- ⦿ Accounts in this organizational directory only (Quadrotech Solutions AG - LAB only - Single tenant)
- ◯ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ◯ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ◯ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ⌄	e.g. https://myapp.com/auth

Step 2: Add a certificate to the server running the Office 365 module.

To add an untrusted certificate to your bridgehead server's local certificate store:

1. Access the server where the Office 365 module is installed.
2. Open the certificates manager by **start/run certlm.msc**
3. Expand **Trusted Root Certificate Authorities** > **Certificates.**
4. Right-click **Certificates** and select **All Tasks > Import...** to launch the **Certificate Import Wizard**.
5. Locate the (.cer) certificate file and follow the wizard prompts.
6. Supply password, if required.
7. Right-click Certificates and select **All Tasks** > **Import...** to launch the **Certificate Import Wizard**.
8. Locate the (.pfx) certificate file and follow the wizard prompts.
9. Supply the password, if required.

Step 3: Configure Permissions and Roles

Configure Application Permissions: Return to the Azure portal and access **Azure Active Directory** > **App registrations** > **owned applications**. Then find the application you created in Step 1 above.

1. Select your application, and then select **API Permissions**.
2. Click **Add a Permission.**
3. In the **Request API permissions** section > Select **APIs my organization uses**, search for **Office 365 Exchange Online** and select this API.
4. Click **Application Permissions**
5. In the **Permissions** list section, select the **full_access_as_app** listed in this section.
6. Click **Add permissions.**
7. Click **Grant Admin consent**.

Assign **User Administrator** role to the registered Application:
1. Navigate to **Active Directory - Roles and Administrators**
2. Find and open the **User Administrator** role
3. Click on **Add Assignments**
4. Search for the registered application (by Display Name)
5. Select the application and click **Add**.

The application is now recognized as Service Principal for the User Administrator role.

You can also use Exchange Online groups for basic migration scenarios. For more on this, click here.

i NOTES:

- An Azure Active Directory Premium license is required for these steps.

- This role is mandatory to collect mailboxes. For more on this role, click here.

Step 4: Get a Thumbprint
To get a thumbprint:
1. Go to Certificates & Secrets and click the **Upload Certificate** button.
2. Upload your certificate file from Step 2.
3. Copy the certificate **Thumbprint** and save it somewhere. You will need it later.

i NOTE: OAuth supports the Exchange Online Powershell Module v3. This can be used to authenticate the use of a certificate and thumbprint in the case of a Global Administrator not being present to connect to Office 365. Application secret is NOT supported via this method.

Step 5: Add your Application ID and Thumbprint on the server running the Archive Shuttle module.
To do this:
1. In Archive Shuttle, open the Credential Editor while logged in as the account the module is running under.
2. Select the **Office 365 OAuth** tab and click **Add**.
3. Enter the **Name (free format text)**, **Application ID**, **Thumbprint**, and **Tenant** (eg. tenant.onmicrosoft.com)
4. Save and close the Credential Editor.
5. Restart the Office 365 module to force settings to take immediate effect.

Required API permissions for to use modern authentication (oAuth)

Below are required API permissions for Archive Shuttle.

As Global Administrator

Office 365 Exchange Online (1)		
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes

For Exchange Online

Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

Office 365 Exchange Online (2)		
Exchange.ManageAsApp	Application	Manage Exchange as Application
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes

Using Exchange Online PowerShell module

Connecting to Office 365 using OAuth supports the Exchange Online Powershell Module v3. This can be used to authenticate the use of a certificate and thumbprint. This is useful in the case of a Global Administrator account not being present to connect to Office 365.

Visit this article from Microsoft for more about the module.
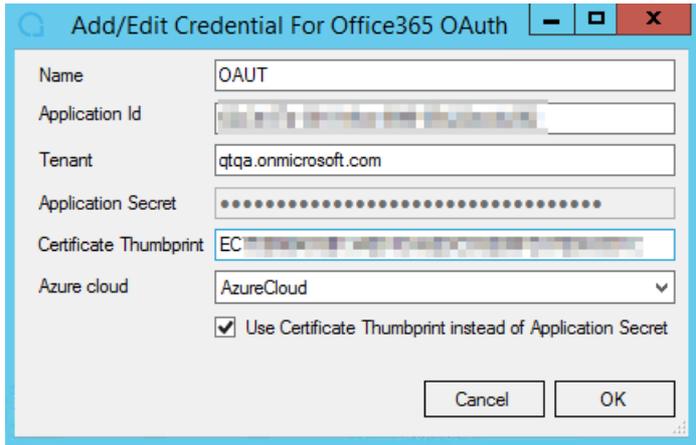
ℹ **NOTE:** Application secret is NOT supported via this method.

Installing the Exchange Online Management module

You first need to download the Exchange Online Management module. This needs to be on the same machine as the Office 365 module.

ℹ **PRE-REQUISITES:**

- PowerShell 5.1 and later are supported.

- Minimum requirements: EXO v3 installed on machine where module is located.

- PowerShell command: *Install-Module ExchangeOnlineManagement* on machine where module is located.

- A self-signed certificate can be used. Certificates issued with SHA 1 or SHA 2 can also be used. Azure permits only .cer, .pem and .crt public keys. For more about Azure requirements for certificates, click here. View this section and this page for more information.

1. Install the certificate into the Personal and Trusted Root Certification Authorities folder stores on a virtual machine where the Office 365 module is running.

2. Open the **Azure Active Directory portal**, and go to **Active Directory**.

3. Select **App registrations**, then **New registration**.

4. Give the application a name, and select **Accounts in this organizational directory only**.

5. Set **Redirect URI** to **Web,** and leave the URL blank. Then click **Register.**

6. Next, we need to configure the Application permissions. Select **API Permissions.**

7. *User Read* should appear as default. Click **Add a permissions,** and locate **Office 365 Exchange Online** from the **APIs my organization uses** tab.

8. Select **Application permissions.** In the next screen, expand **Exchange**, and check **full_access_as_app** and **Exchange.ManageAsApp.** Then click **Add permissions.**

9. Now we need to grant administration consent. Click **Grant admin consent for <tenant>**. When this is completed, the *Status* column for **full_access_as_app** and **Exchange.ManageAsApp** permissions should read **Granted for <tenant>.**
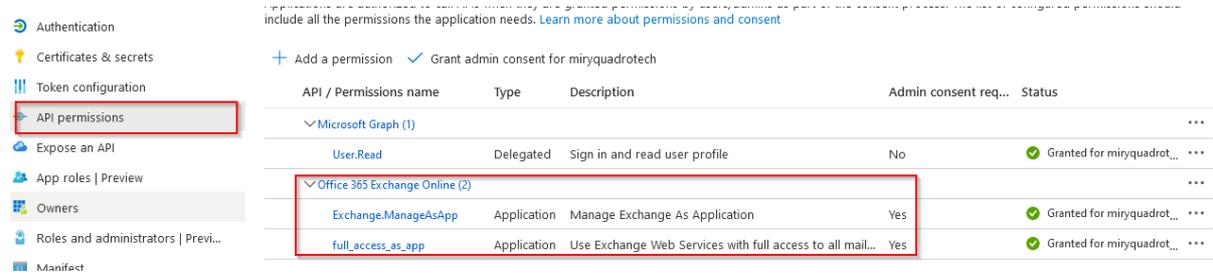
10. Select **Certificates & Thumbprints,** and upload the certificate you previously created.

> ℹ **NOTE:** Check that the certificate (that is on the same virtual machine as the Office 365 module) is in the .cer format. .pfx is not supported.
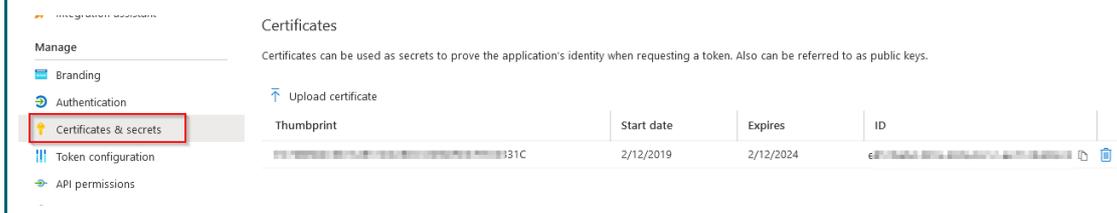
11. Navigate to **Active Directory - roles and administrators.**

12. Find the **Global Reader** role and open it.

13. Click on the **Add assignments** button.
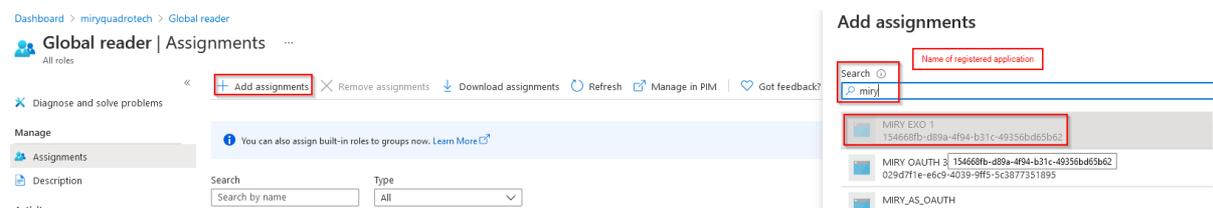
14. Select the registered application from step 4 as the ServicePrincipal for the Global Reader role.

15. Repeat steps 12 and 13 for the **Exchange Administrator** and **User Administrator** roles.

Setup application using Exchange Online role groups

Prerequisites

This method is supported only in Exchange Online PowerShell, and only when you connect in the REST API mode (do not use the UseRPSSession switch in the Connect-ExchangeOnline command).

This configuration is only compatible with the following scenarios:

- collection of mailboxes

- owner migration scenarios

> **i** **NOTE:** Archive Shuttle's leaver, virtual journals and other user provisioning operations require Azure Active Directory roles.

Steps

1. Register your application in Azure Active Directory

2. Select **Created application registration** -> **Certificate & secrets** -> **upload certificate**

3. Select **API permissions**

4. Configure permissions based on the following:

API/Permissions Name	Type	Description	Admin consent required?
Microsoft Graph (2)			
Organization.Read.All	Application	Read organization information	Yes
User.Read.All	Application	Read all users' full profiles	Yes
Office 365 Exchange Online (2)			
Exchange.ManageAsApp	Application	Manage Exchange As Application	Yes
full_access_as_app	Application	Use Exchange web Services with full access to all mailboxes.	Yes

5. Navigate to the **Exchange Admin center**

6. Select **Roles** -> **Admin roles**

7. Add the Role group with the necessary roles

Roles:

+ −

NAME ▲
Mail Recipients
Mailbox Import Export
Mailbox Search

8. Start PowerShell and connect to Azure Active Directory as an administrator

9. Connect to Exchange Online as an administrator

10. Run the following cmdlets:

```
# Get registered application and create service principal

$appFromAzure = Get-AzureADServicePrincipal -
SearchString"YourRegisterApplicationName"

New-ServicePrincipal -AppId $appFromAzure.AppId -ServiceId
$appFromAzure.ObjectId -DisplayName "NameForServicePrincipal"

$SP = Get-ServicePrincipal -Identity "NameForServicePrincipal"

# Assign service principal to RoleGroup
Add-RoleGroupMember -Identity "YourRoleGroup" -Member $SP.Identity

# Check result
Get-RoleGroup -Identity " YourRoleGroup"
```

Supported Office 365 features when basic RBAC setup is used	
Feature	**Supported?**
Sync Office 365 mailboxes	Yes
Sync cloud-only Office 365 mailboxes	Yes
Get licenses	Yes
Get mailbox quota	Yes

Supported Office 365 features when basic RBAC setup is used	
Ingest data into mailbox (normal users, journal transformation)	Yes
Process shortcuts on Office 365 mailboxes (delete, convert, fix, restore)	Yes
Virtual journal and leavers provisioning	No
Journal transformation leavers	No
Collect retention labels and tags	No

Scoping the application access policy (creating scoped accounts)

ℹ️ **NOTE:** This process can only be used when configuring Archive Shuttle using a certificate.

Creating an application registration using a certificate

1. Create a new registered application with Azure using a certificate. Use the instructions as seen in step 1, under the *Configuring OAuth with a certificate* section here.

2. Upload a certificate by going to **Certificates & secrets**, and under **Certificates**, click **Upload certificate**.

3. Select the required certificate, enter a description if needed, and click **Add.**

4. On **API Permissions**, click **Add a permission**, and enter the API permissions as seen under the *For Exchange Online* section here. Do NOT grant admin consent at this time.

Adding administrative roles

5. On the **Roles and administrators** tab in the Azure Active Directory admin center, and in the text field, search for the role titled Exchange recipient administrator or global reader. Click on its name.

ℹ️ **NOTE:** The global reader role will allow you to read any attribute, but not update attributes.

6. Click **Add assignments**, then search for the application registration you created earlier, then click **Add.**

Creating an Exchange security group

7. You now need to create an Exchange security group. Go to the Exchange admin center.

8. Under **Recipients > Groups**, click **Add a group.**

9. On the **Group type** page, select **Mail-enabled security,** and click **Next.**

10. On the **Basics** page, enter a group name and, optionally, a description. Once created, this is the group where you will need to add the mailboxes that you want the app registration to have write access to write to. Once this is done, click **Next.**

11. On the **Settings** page, enter a group email address. This could be the same name as the group name, and click **Next.**

12. Review the group you have created. Once you are satisfied, click **Create group**. It may take a few minutes for the group to appear in the group list.

ℹ **NOTE:** You may want to remove access to emails being sent to the group directly. To do this, click on the group name under **Mail-enabled security**, and under **Settings**, check the **Hide this group from the global address list.**

13. You will now need to add users to the group. Select the group under **Mail-enabled security,** and under **Members**, select **View all and manage members.** Enter the members by selecting their checkbox, and click **Add** until all your desired members have been added.

Connecting to the tenant

14. Open the PowerShell module, and connect to the Exchange module using the following command: Connect-ExchangeOnline. Then click the **Run Selection** button.

15. Sign into the module using a global administration account. Connecting may take up to a minute.

Creating the application access policy

16. Use the following command in PowerShell to create the application policy. Replace the fields in bold with your own credentials:

New-ApplicationAccessPolicy -Description "**Policy Name**" -AppId '**OAuth App Registration ID** ' -AccessRight RestrictAccess -PolicyScopeGroupId '**Mail Enabled Security Group Email Address**'

Then click **Run Selection.** The output to the command should appear below.

ℹ **NOTES:**

- Once the command has been ran, it may take up to one hour for the command to take effect. It is recommended that you wait this full period to ensure application of this command. Click here for more information.

- You can test whether the application of the command has been successful by using the following command. Replace the fields in bold with your own credentials:

Test-ApplicationAccessPolicy -Identity **SMTP address** -AppId **Outh App Registration ID**

Grant admin consent

17. Go back to the API permissions for your application registration, and click **Grant admin consent for <tenant>,** and click **Yes.**

i | **NOTE:** Using this process may result in certain features not functioning as expected, such as leavers and virtual journal migrations. If this occurs, please contact support.

Adding credentials for Office 365 ingest account in Credential Editor

If you want to add/change credentials for Office 365 ingest account, you must be logged in as the local service account under which the Services (particularly Office 365 module) runs. Use the Archive Shuttle Credentials Editor for adding/changing of the credentials for Office 365 ingest account.

The tool is called *ArchiveShuttle.Module.CredentialsEditor.exe* and is by default located in: *C: \Program Files (x86)\QUADROtech\Archive Shuttle Modules\CredentialsEditor\.*

Then, follow these steps:

1. Run the tool, click Add and specify the valid UPN account and the valid password. Then, click OK and save the credentials.

2. Restart the module.

3. Verify connectivity using the **Test connection** button.

At least one service account is required per import module. One service account needs to have configured Global Administrator rights and rest of the accounts should have Application Impersonation rights configured.

i | **NOTES:**

- When ingest accounts are not visible in the Health page, you have to restart the Office 365 module service first and then Core service to have accounts from Credential Editor loaded to that page.

- Service accounts must be unique and cannot repeat across additional module instances.

OAuth support for GCC and GCC High tenants

You may experience an issue where it is claimed that OAuth is not supported with GCC and GCC High tenants. This issue can be resolved using the Credentials Editor.

1. Go the the **Credentials Editor**, then the **Office 365 Auth tab**.

2. Click **Edit**.

3. On the Azure cloud drop down list, select:

   a. *AzureCloud* for GCC tenants

   b. *AzureUSGovernment* for GCC High tenants.

4. Click **OK**.

Using Microsoft Graph

Use of Microsoft Graph is enabled automatically from Archive Shuttle 11.0.

If using Microsoft Graph, ensure that the Azure App Registration section has been filled in the Credentials Editor, regardless if OAuth is being used. If Azure App Registration is left empty, an error will occur.

Microsoft Graph commands and permissions

List users

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	User.ReadBasic.All, User.Read.All, Directory.Read.All
Delegated (personal Microsoft account)	Not supported.
Application	User.Read.All, Directory.Read.All

Get a user

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	User.Read, User.ReadBasic.All, User.Read.All, Directory.Read.All
Delegated (personal Microsoft account)	User.Read
Application	User.Read.All, Directory.Read.All

List subscribedSkus

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	Organization.Read.All, Directory.Read.All
Delegated (personal Microsoft account)	Not supported.
Application	Organization.Read.All, Directory.Read.All

user: assignLicense

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	User.ReadWrite.All, Directory.ReadWrite.All
Delegated (personal Microsoft account)	Not supported.
Application	User.ReadWrite.All, Directory.ReadWrite.All

Update user

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	User.ReadWrite, User.ReadWrite.All, User.ManageIdentities.All, Directory.ReadWrite.All
Delegated (personal Microsoft account)	User.ReadWrite
Application	User.ReadWrite.All, User.ManageIdentities.All, Directory.ReadWrite.All

Delete a user

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	User.ReadWrite.All
Delegated (personal Microsoft account)	Not supported.
Application	User.ReadWrite.All

Permanently delete item

One of the following permissions is required to call this API. To learn more, including how to choose permissions, see Permissions.

For applications:

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	Application.ReadWrite.All, Directory.ReadWrite.All
Delegated (personal Microsoft account)	Not supported.
Application	Application.ReadWrite.OwnedBy, Application.ReadWrite.All

The requestor needs to have one of the following roles: **Global Administrator** or **Application Administrator**.

For users:

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	User.ReadWrite.All
Delegated (personal Microsoft account)	Not supported.
Application	Not supported.

The signed-in user needs to have one of the following roles: **Global Administrator** or **User Administrator**.

For groups:

Permission type	Permissions (from least to most privileged)
Delegated (work or school account)	Group.ReadWrite.All

Permission type	Permissions (from least to most privileged)
Delegated (personal Microsoft account)	Not supported.
Application	Not supported.

The requestor needs to have one of the following roles: **Global Administrator** or **Groups Administrator**.

Global Administrator consent for app-only permissions

Any app-only permission requires a global administrator of the directory to give consent to the application. Select one of the following options, depending on the role:

Global tenant administrator

For a global tenant administrator:

1. Go to **Enterprise applications** in the Azure portal

2. Select the app registration, and select **Permissions** from the **Security** section of the left pane.

3. Select the button labeled **Grant admin consent for {Tenant Name}** (where {Tenant Name} is the name of the directory)

Standard user

For a standard user of your tenant, ask a global administrator to grant admin consent to the application. To do this, provide the following URL to the administrator:

```
https://login.microsoftonline.com/Enter_the_Tenant_Id_Here/adminconsent?
client_id=Enter_the_Application_Id_Here
```

In the URL:

- Replace Enter_the_Tenant_Id_Here with the tenant ID or tenant name (for example, contoso.microsoft.com)

- Enter_the_Application_Id_Here is the application (client) ID for the registered application

- **NOTE:** The error 'AADSTS50011: No reply address is registered for the application' may be displayed after you grant consent to the app by using the preceding URL. This error occurs because the application and the URL do not have a redirect URI. This can be ignored.

Planning for migrations to PST

In order to perform a migration of Enterprise Vault data to PST, a PST File Name policy can be defined. The file name policy is defined with tokens, as shown in the table below:

Token	Description
username	Username of the owning user (sAMAccount Name)
firstname	First name of the owning user
lastname	Last name of the owning user
fullname	Full name of the owning user
email	E-mail address of the owning user
upn	User principal name of the owning user
pstid	ID of the PST file; continuous integer over all PST files
pstnumber	Number of PST file; continuous integer per user
archivename	Name of the archive
archiveID	The Enterprise Vault Archive ID associated with the archive

The tokens can be used to construct filenames and paths.

Planning for migrations to UNC

If you plan to migrate data to UNC, install the Storage Import Module before beginning.

You'll use the Storage Import and Storage Provider target when configuring the workflow policy, mapping wizard, etc.

While setting up the migration, use the Storage Import Module tab of the System Configuration page to, for example, set item/archive parallelism, set up conversion of MSG to EML, fail items permanently on specified errors, etc.

4

Planning component installation

Where to set up Archive Shuttle components

The core Archive Shuttle Components include the following:

- Archive Shuttle Core Web Interface

- Archive Shuttle Core Web Services

- Archive Shuttle Core Service

It is recommended to install these components on the same server. For a production environment, this must be a dedicated server (physical or virtual). They can; however, be installed on separate servers.

See the chapter Hardware requirements for Archive Shuttle Core Server for more information about prerequisites.

Archive Shuttle also has the following Modules:

- Archive Shuttle Active Directory Collector Module

- Archive Shuttle Enterprise Vault Collector Module

- Archive Shuttle Enterprise Vault Export Module

- Archive Shuttle Enterprise Vault Import Module

- Archive Shuttle Enterprise Vault Provisioning Module

- Archive Shuttle Enterprise Vault Shortcut Processing Module

- Archive Shuttle Exchange Import Module

- Archive Shuttle Office 365 Module

- Archive Shuttle Native Format Import Module

- Archive Shuttle EAS Module

- Archive Shuttle Metalogix Module

- Archive Shuttle PST Export Module

- Archive Shuttle Dell Archive Manager Module

- Archive Shuttle SourceOne Module

Depending on the migration scenario, some or all of these modules have to be installed.

The following table provides a guideline on where to install these modules:

MODULE	NUMBER OF MODULES	NOTES
Active Directory Collector Module	One per Active Directory forest	Needs to be installed on a Server in the Active Directory Forest where data is to be collected from. The account that it is running under must have privileges to read Active Directory and its objects – a normal user account is sufficient.
Enterprise Vault Collector Module	Minimum: One per source Enterprise Vault environment Recommended: One per Enterprise Vault Server hosting a Vault Store. Note: If performing an EV to EV migration, this module is also needed in the target environment to gather site settings (HTTP/HTTPS) used when running 'Fix Shortcuts'.	There needs to be at least one Enterprise Vault Collector Module installed in the source Enterprise Vault environment. It is recommended to install this component near the SQL Server that hosts the Vault Store databases. Care should be taken when additional Enterprise Vault Collector Modules are installed. Performance might not necessarily be increased, the limiting factor is usually the time it takes to retrieve data from the Vault Store databases.
Enterprise Vault Provisioning Module	One per source Enterprise Vault environment, and one per target Enterprise Vault environment.	There needs to be one Enterprise Vault Provisioning Module per Enterprise Vault environment, i.e. per Enterprise Vault Directory Database. This module uses EVPM. It is recommended to install this component on the least busy Enterprise Vault server.
Enterprise Vault Export Module	Minimum: One per source Enterprise Vault environment	There needs to be at least one Enterprise Vault Export Module installed in the source Enterprise Vault environment.

MODULE	NUMBER OF MODULES	NOTES
	Recommended: One per Enterprise Vault Server hosting a Vault Store.	It is recommended to install the Enterprise Vault Collector module on each Enterprise Vault server that hosts Vault Store partition data, in the source environment. This module requires the Enterprise Vault API. If this module is to be installed on a non-Enterprise Vault server, then the Enterprise Vault API Runtime needs to be installed.
Enterprise Vault Import Module Note: This module is only required if the migration scenario includes migration to an Enterprise Vault environment.	Minimum: One per target Enterprise Vault environment. Recommended: One per target Enterprise Vault Server hosting a Vault Store.	There needs to be at least one Enterprise Vault Import Module per target Enterprise Vault environment, i.e., Enterprise Vault Directory. It is recommended to install an Enterprise Vault Import Module on each Enterprise Vault Server where the Vault Store to import to is hosted. This module requires the Enterprise Vault API. If this module is to be installed on a non-Enterprise Vault server, then the Enterprise Vault API Runtime needs to be installed.
Shortcut Processing Module	Minimum: One per target environment.	There needs to be at least one Shortcut Processing Module per target environment. This module must be installed on a Server with Microsoft Outlook 2007/2010/2013 (32 bit). Note: An optional change in the System Configuration can change this module to use EWS rather than MAPI

MODULE	NUMBER OF MODULES	NOTES
		(however the installation of the module still requires Outlook)
Exchange Import Module Note: This module is only required if the migration scenario includes migration to an Enterprise Vault environment.	Minimum: One per target Exchange environment.	There needs to be at least one Exchange Import Module per target Exchange environment. This module requires Microsoft Outlook to be installed. It is not supported to install the module on an Exchange Server. It is recommended to install this module on a dedicated physical or virtual machine. To improve performance, multiple Exchange Import Modules can be installed. It is recommended to start with one module and add more modules (up to one per Exchange database) if required.
Office 365 Module	One per environment	There needs to be an Office 365 module in order to migrate containers to Office 365. This module collects data about Office 365 mailboxes, as well as migrating data into the target container and post-processing the ingested data to remove Enterprise Vault shortcuts and pending items. The module connects to Office 365 using the credentials specified in the Credential Editor, which is installed by the module.
Native Format Import Module	One per environment	One Native Format Import Module is required in order to take extracted data and create

MODULE	NUMBER OF MODULES	NOTES
		PST files. This module will split PST files at predetermined sizes and store them with a name defined by policy into a UNC accessible staging area which is defined per link. This module must be installed on a Server with Microsoft Outlook 2007/2010/2013 (32 bit).
Proofpoint Module	One per environment	One Proofpoint Module is required in order to take extracted data and prepare/construct the data required for Proofpoint ingestion. This module must be installed on a Server with Microsoft Outlook 64-bit. This module also requires a 64-bit JRE. Additional information is available in the Installation Overview.
EAS Zantaz Module	One per environment	One EAS Module is required on a machine which can communicate with an EASIIS Server which has access to all the required Document Repositories.
Metalogix	One per environment	One Metalogix Module is required on a machine which can communicate with an Metalogix Server which has access to all the required Document Repositories.
PST Export Module	One per environment	One PST Export Module is required, and can process a number of UNC paths to

MODULE	NUMBER OF MODULES	NOTES
		extract data from PST files which are located there.
Dell Archive Manager Module	One per environment	One Dell Archive Manager module is required for the source environment.
SourceOne Module	One per environment	One SourceOne module is required for the source environment.

Planning for the Archive Shuttle databases

Archive Shuttle uses the following Databases:

- The Archive Shuttle Directory database. There is just one of these; it hosts all configuration and non-item based metadata.

- The Archive Shuttle Item database(s). There is one of these for each source Link (e.g. one per Vault Store). These databases do not have to be on the same SQL Server as the Archive Shuttle Directory database. Each Item Database can be on a separate SQL Server, if required.

Microsoft SQL Server must be installed and set up before you install Archive Shuttle. The collation requirement for the SQL Server installation must be case-insensitive, accent-sensitive (CI, AS); case-sensitive and accent-insensitive installations are not supported.

Microsoft SQL Server must be on a dedicated server, either physical or virtual. It is not supported to have it on the same server as the Archive Shuttle Core server. It is not supported to have the Microsoft SQL Server shared with any other software, for production use.

Before installing the Archive Shuttle Core Components, make sure the account that will be used has "dbcreator" rights in Microsoft SQL Server.

ℹ️ **NOTE:** SQL is only relevant within your environment when installing **Core** (see *Quadrotech Archive Shuttle Compatibility Guide* for more). If you are installing within the cloud, Quadrotech maintains SQL for you.

SQL versions

To see which versions of SQL Server are supported, go to the *Quadrotech Archive Shuttle Compatibility Guide*.

ℹ️ **NOTE:** Having the latest service pack installed is recommended.

SQL editions

Although Enterprise Edition of Microsoft SQL Server is recommended, Standard Edition may be used if the SQL instance uses the recommended (not minimum) resources associated with the size of migration you are performing. Planning for additional time will be required to accommodate regularly required offline maintenance.

Planning export/import storage

Sizing the staging location

The Archive Shuttle Export and Import Modules require a location to store the extracted data. Sizing of this location should be carefully considered.

Consider the following options when sizing the storage area:

- Local and Network Attached Storage is supported.

- Modifying the export/import schedules for the required modules can mean that the data to be migrated flows through the storage area with only a small amount being present at any time.

- Modifying the container mappings and 'batching' the migration will also lead to a smaller amount of data residing in the export/import location.

i | **NOTE:** Export will stop if the free space on the staging area drops to 20 Gb or lower.

It is recommended to allow for between 50 and 100 Gb per source link. For example, with Enterprise Vault that would be 50 to 100 Gb per source Vault Store. Other sources may vary.

i | **NOTE:** If the migration will send the data to PST files, additional space may be required in the staging area since, by default, temporary PSTs are created in the staging area before they're moved to the PST Output Path. The temporary location can be changed, or the space needed per source link should be increased to at least double the recommendations above.

The System Health dashboard provides an administrator with an overview of storage and other health parameters which may affect the migration being undertaken. The following information is displayed:

Item	Description
Module Health	Displays information relating to all modules in the Archive Shuttle environment.
Unmapped Retentions	Any retention categories that are not mapped to a target environment are displayed here.
Link Health	Detailed information relating to each of the links will be displayed here. The links can be filtered so that only particular types of link are shown (e.g., Enterprise Vault, Exchange)

Item	Description
	This part of the dashboard will also show if an Enterprise Vault link is backup mode. This will affect any ingests to that Link (they will be suspended while the link is in backup mode)

Free space on a staging area location is color coded as shown in the following table:

Highlighting	Reason
No highlighting	Free space is above 100 Gb
Yellow	Free space is below 100 Gb
Red	Free space is below 50 Gb

In addition, the System Health page gives an overview of any modules which are deactivated or otherwise not running. This is shown at the top left of the screen in the Admin Interface.

The Link information at the bottom of the page also highlights the 'Used' space on each link. Used space is defined as the amount of data that has been exported, but not yet imported. This too is color coded for ease of identifying a potential problem, as follows:

Highlighting	Reason
No highlighting	Used space is within normal parameters
Yellow	Used space is between 75% and 90% of the maximum allowed
Red	Used space is above 90% of the maximum allowed

If the Used Space reaches 100% on a link, exporting of data will be stopped until data has been imported, even if there is still free disk space available on disk. This is further illustrated as follows:

Staging Area free Space 100GB	
Link usage Space 10GB	Link 1 20GB High Watermark
Link usage Space 15GB	Link 2 20GB High Watermark
Link usage Space 10GB	Link 3 20GB High Watermark
Link usage Space 5GB	Link 4 20GB High Watermark
60 GB Free Space	
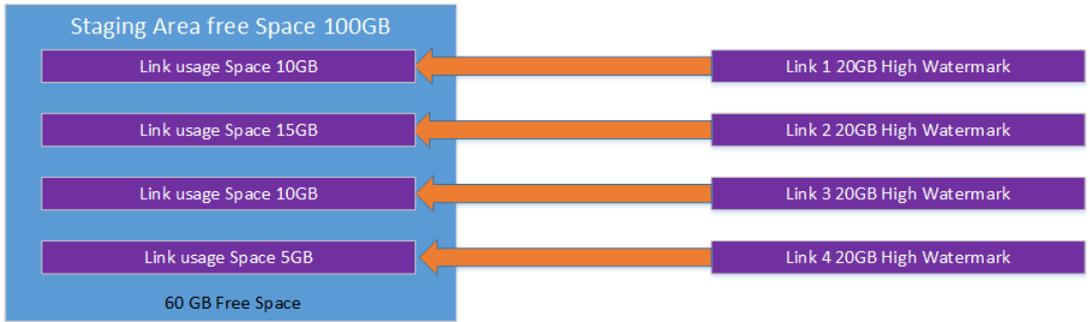
Export will function normally

Staging Area free Space 100GB	
Link usage Space 10GB	Link 1 20GB High Watermark
Link usage Space 15GB	Link 2 20GB High Watermark
Link usage Space 10GB	Link 3 20GB High Watermark
Link usage Space 20GB	Link 4 20GB High Watermark
45 GB Free Space	
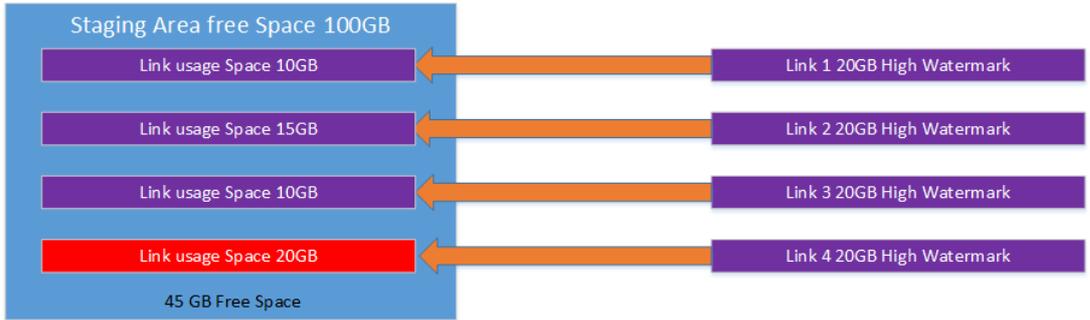
Export for the highlighted link will stop, because the watermark has been reached – even though plenty of free space on the Staging Area.

Permissions/access requirements for complex deployments

In complex environments crossing domains, organizations and forests, consideration must be given to the permissions / access requirements of the Archive Shuttle export and import modules that are required for the migration.

The basic requirement is that the Active Directory account that the export module runs under needs to be able to read/write to the storage location. In addition, the required import module also requires read/write access to the storage location.

i | **NOTE:** The export/import storage location is specified as a UNC. Hidden shares are supported.

Sizing the PST output location

If Archive Shuttle is being used to extract data to PST files, the sizing of the PST Output location is important and should be carefully considered.

Consider the following options when sizing the storage area:

- It does not have to be locally attached storage to the Native Format Import Module. Network attached storage is supported.

- No data is written to the location until Stage 2 is activated for the chosen containers.

- Typically the space required for a PST file export of an archive will be almost double the size of the source archive.

i | **NOTES:**

- PST files will be created by default of about 2 GB in size. A lower size can be set in the UI if required.

- The export item size estimate when importing using the Native Format Import module may be larger in the UI than the estimated size in the database.

How to change folder translations

By going to **System Configuration > General > Folder**, you are able to add, remove and change the translation for new and existing folders.

Clicking on the **Edit** button brings up a pop-up menu, showing the list of labels of folders. Clicking one gives you a list of translations on the right pane.

You can edit the translations on the right hand pane by selecting one, or add a new translation by selecting the end of a translation and pressing **Enter.** You can edit as many folders as you wish, and once you are done, click **Save,** then **Save** in the top right. This is logged in the database **dbo.MailboxFolderTranslation.**

i | **NOTES:**

- Folder Translation is working only for Exchange 2013 and higher versions of Exchange mailboxes, as well as for Exchange Online mailboxes.

- Folder Translation is working only for root folders, not for split folders, therefore all split folders will use language of the source archive.

Preserving the Chain of Custody

Archive Shuttle performs a number of operations in order to preserve and verify the Chain of Custody of data items during a migration. This section explains some of those which need to be taken into account in a migration.

Item level hashing

When an item is exported from a source environment. a hash is generated for that item and stored in the Archive Shuttle Item database. Sometime later, when the item is ingested, the hash is recomputed and compared with that stored value.

If the hashes do not match, a Chain of Custody violation is logged and the item will by default be re-exported and re-migrated.

ℹ **NOTE:** If a significant number of Chain of Custody alerts are reported, it is likely that anti virus is touching the files after they have been stored on the staging area.

Migration-level hashing

As Archive Shuttle is performing the hashing on the items as mentioned in the previous section, a hash is generated on the whole message file, in order to avoid tampering during the migration.

Watermarks

When migrating from EV to EV Archive Shuttle adds a custom index entry to migrated item. This entry contains:

- Migration Time UTC
- Source Archive ID
- Source Transaction ID
- Archive Shuttle Version

When migrating from EV to Exchange, Archive Shuttle adds the same information to each migrated item as MAPI properties.

Retained databases

Following the migration, in case of Chain of Custody queries, you may consider retaining the Archive Shuttle SQL databases.

Migrating leavers data and journal archives

When performing a migration with Archive Shuttle a question which arises and needs to be addressed is whether to migrate leavers data if journal migration is being performed.

Journal archives contain messages from everyone inside the organization, and all inbound and outbound communications. It has messages from everyone in the company now, and everyone that left the company over the preceding years. The tricky part is determining when journal archiving was turned on. That can affect whether or not you need to migrate just the journal archive, or the journal archive and leavers data.

Let's look at a couple of examples.

Example 1

Let's say Bob works for the organization now, and has been working for the organization for 3 years. Jane doesn't work for the company any more, she joined about 18 months ago and left 3 months ago.

Journal archiving has been in place for 5 years.

In this example, the data which would be in Bob's archive will be in the journal archive. The data which would be in Jane's 'leaver' archive will also be in the journal archive. Therefore, the organization could make the decision that they do not need to migrate that leaver archive.

Example 2

Let's say Sarah has been working for the company for 6 months. Let's say David is a leaver, he left 3 months ago, and has been working for the company for 7 years.

Journal archiving has been in place for 5 years.

In this example the data in Sarah's archive will be in the journal archive, but not all of the data in David's 'leaver' archive will be in the journal archive. Therefore, the organization could make the decision that they do need to migrate David's data as well as the journal archive.

This comparison would need to be done across all leaver archives before an overall decision could be reached, and ultimately it's the organizations decision to migrate the data or not.

Naming conventions for leaver archives

An important consideration when migrating leaver archives with Archive Shuttle is the naming convention (or naming standard) to use for the mailboxes which Archive Shuttle will create.
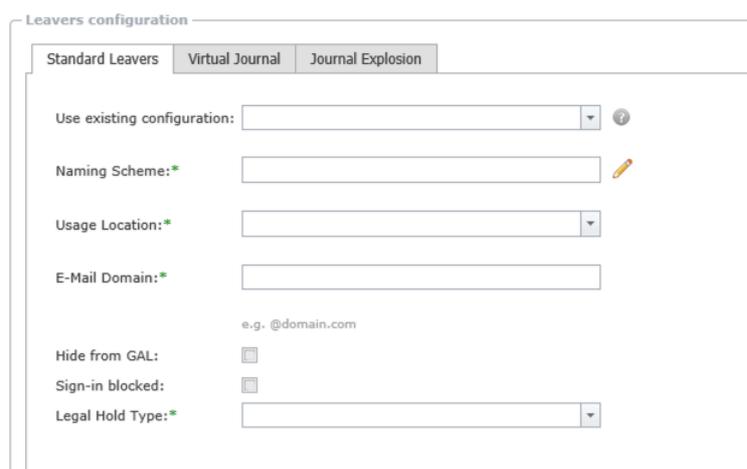
The above screenshot shows where the configuration / selection is made in Archive Shuttle. There are many tokens that can be used to help form the name such as:

- Archive ID
- Archive Name
- Container Mapping iD, and more.

It's important to remember that there should not be any overlap or collision with existing names in the target.

In selecting 'archive name', problems will be encountered when someone exists and a leaver has the same name. For example, if there is already an active mailbox owned by John Smith, and Archive Shuttle tries to process a lever called John Smith.

Ultimately, the naming scheme should be unique. Often the name will have a prefix; they will all appear in the directory in the same sort of place (compared with postfixing a token). Here is an example:

AL-*archivename*

Considerations when using special characters for naming leavers

Archive Shuttle will replace special characters in leaver naming tokens (for example letters with diacritics), with an underscore (_) (for example Aimée to Aim_e), in cloud only mailboxes. For more information, visit "Invalid user name" when you try to create a user name that contains a

special character in Microsoft 365 and Microsoft 365 email address contains an underscore character after directory synchronization.

Tuning a Migration

There are many aspects of a migration that can be tuned with Archive Shuttle, some of these are manual tuning mechanisms, others can be automatic if required.

Scheduling module operation

Each Archive Shuttle module can be supplied with a specific schedule. For example, if extraction is allowed only during the evening, so as to lessen the load on the source environment, the export modules can be configured to have an evening-only schedule.

Configuring schedules should be done with careful consideration of the impact on the space requirements on the Staging Area. If exports are occurring all night long, but ingests are not scheduled, the staging area may fill up rapidly.

Tuning module parallelism

Each of the modules used in an Archive Shuttle migration operates on a number of containers in parallel and within that a number of items in parallel. The defaults for each module have been chosen following testing in many different environments. They can be adjusted to higher or lower values in the System Configuration. The changes made will take effect the next time the module checks in with the Archive Shuttle Core (approximately once per minute)

For reference:

Container level parallelism

For example, Office 365 Mailbox Parallelism. This is the number of containers that will be operated on simultaneously by the module

Item level parallelism

For example, EXC Import Item Parallelism. This is the number of items that will be operated on simultaneously per container.

When changing the parallelism, it is advised to make changes in small steps and then observe the impact that this has had on migration performance.

EV ingest specific tuning

An option in the System Configuration allows the EV Import Module to pause if Enterprise Vault is in a scheduled archiving window. Pausing the ingestion during this time lessens the load on the target environment.

In addition, backup mode is checked per target Vault Store every 5 minutes.

When ingesting data the EV Import module will only send data to a Vault Store that is not in backup mode.

Finally, the number of items that are not yet marked as indexed in the target environment is captured per Vault Store once per minute. This is displayed on the System Health page in the Archive Shuttle Admin Interface.

> **i** | **NOTE:** A large index backlog might indicate that the target environment has a problem relating to indexing is indexing slowly.

Native Format Import (NFI) specific tuning

An option in the System Configuration allows the Native Format Import module to rename (i.e., move) temporary PST files from the Staging Area to the PST Output Path during Stage 1. Normally, the finalization of PSTs is not performed until Stage 2 is running for a container mapping, but this can lead to increased pressure for storage requirements on the Staging Area.

Enabling the option in the System Configuration can mean that this pressure is reduced because completed PST files are moved out of the Staging Area and placed in their final location.

Office 365 specific tuning

Additional throughput can be achieved by the Office 365 module by setting up and configuring additional service accounts that have application impersonation rights within Office 365. These accounts can then be added to the credential editor, and the Office 365 module will use them for ingesting data in a round-robin fashion.

Item batching

The Exchange and Office 365 modules both utilize an intelligent batching mechanism which groups together items based on size, folder and whether the item has an attachment or not.

> **i** | **NOTE:** This can be deactivated on a per-module basis, if required.

About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com. The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request

- View Knowledge Base articles

- Sign up for product notifications

- Download software and technical documentation

- View how-to videos

- Engage in community discussions

- Chat with support engineers online

- View services to assist you with your product