PST Flight Deck 9.2

Requirements Guide

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest and the Quest are trademarks and registered trademarks of Quest Software Inc. and its affiliates. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are the property of their respective owners.

Legend

! CAUTION: A caution icon indicates potential damage to hardware or loss of data if instructions are not followed.

i IMPORTANT, NOTE, TIP, MOBILE OR VIDEO: An information icon indicates supporting information.

PST Flight Deck
Updated April 2024
Version 9.2

Contents

1

Introduction

This guide defines the system requirements that must be met in order to successfully install and operate PST Flight Deck. The target audience for this guide is professional system administrators. The information included pertains to the operation and configuration of PST Flight Deck. All installation, configuration, and support should be performed by PST Flight Deck qualified administrators.

This guide provides minimum and recommended system requirements.

2

System Requirements

The PST Flight Deck server should meet the following requirements.

Hardware Requirements

PST Flight Deck is a robust system designed to be scalable and meet the needs of organizations of any size. You should consider project requirements when evaluating the systems to allocate to the PST Flight Deck solution. The hardware requirements we recommend are meant to provide a general guidance for proper hardware configuration.

Core Server and Nodes

We recommend the following hardware requirements for the PST Flight Deck Core server and Nodes. These may be physical or virtual machines.

	CPU Cores	RAM
Minimum	6	8 Gb
Recommended	8	12 Gb

The size or requirements of a project can dictate the hardware required. It is best to review sizing for a specific project to ensure the solution meets the project requirements.

It is possible to put a full, or any portion of a deployment on Azure resources. For information on deployment of a full Core in Azure please contact a PST Flight Deck Architect to appropriately size, configure, and deploy your environment.

Additional Module or Ingestion Nodes

PST Flight Deck is able to be expanded to include additional Nodes for scalability or to otherwise accommodate the needs of a project. The following hardware requirements are for additional Modules or Ingestion Nodes. These may be physical or virtual machines.

	CPU Cores	RAM
Minimum	4	8 Gb

	CPU Cores	RAM
Recommended	8	12 Gb

It is also possible to expand an environment onto Azure instances. Minimum instance types are D2 for Module Nodes and DS2 for Nodes containing an upload location and Extraction module. Migrations for over 1000 users should consult a PST Flight Deck architect to design a solution that best suits their needs.

Under most circumstances, it is advised to run Extraction and Repair modules local to the Upload directory for a given location to ensure sufficient IOPS are available to facilitate and optimal processing time of a PST file.

Requirements for Additional Server Components

PST Flight Deck is a scalable and flexible product that supports a number of configurations to suit the needs of any PST file elimination or migration initiative. There are several components that could be installed on separate hardware to support the needs of a migration project. Examples of these components are:

- Active Directory Scanner
- Share Scanner
- Central Upload Agent

Generally speaking, a minimal system is required to support these components. They can, and frequently are installed on the same machine. In environments where a modest use of these components is needed, the following specifications are recommended:

- 4 Core CPU
- 8 GB RAM
- 10 GB of dedicated disk space

The Active Directory Scanner (AD Scanner) is a very lightweight component that, under normal conditions, does not require many resources. A single core machine with 4 GB or RAM is typically sufficient for a production AD Scanner.

Project requirements or constraints could result in an increase in hardware requirements.

Requirements for Consoles

Consoles are typically run from the Core server, but can be installed on any supported operating system. Any system running a console requires the following:

- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 4.5
- Display resolution of 1440 x 900 or higher
- Low-latency connection to the Microsoft SQL Server hosting the system database

- Consoles are used to manage, configure, monitor, and administer PST Flight Deck PST file elimination and migration projects. A minimum supported display resolution is 1440 x 900, but it is recommended that machines used to manage projects have a resolution of 1920 x 1080 or higher.
- The console must be run by an account with read/write access to the system database.

Storage

Storage is based on the PST volume and processing rate. The following table outlines general considerations. Storage is required for the upload directory per location and several modules prospectively running on any number of nodes configured in the environment.

Area	Recommended size	Recommended speed
Uploads	3-5 times the daily ingest volume	Fast disks with high IOPS is required, preferably SSD
Backup	Daily upload volume multiplied by the number of days to keep the data	Standard disk speed requirements
Filter	Usually more than 1% of the total data. Volume may change dependent on filter configuration	Standard disk speed requirements
Hash Tables	Hash data is usually about 0.2% of total space in scope	Mid-range disks required due to frequent reads
Cleanup	Volume of storage is dependent on the target and data quality. Office 365 and Exchange migrations are usually 2-6% and other targets are less.	Standard disk speed requirements
Park	If managed, the size of the Park Area can be small since it is only used as a waiting area while PST file ownership is determined.	Standard disk speed requirements

If you're only estimates of the volume of data are available, make sure to re-evaluate the total volume after the discovery process of the project takes place.

Cloud Storage

PST Flight Deck can use Azure storage for the Backup and Cleanup module storage locations. It has been tested with standard, locally redundant blob storage. All access tiers have been used for this sort of storage and it is suggested to select the one that best suits the requirements of the project.

For more information on how to create and configure Azure storage for PST Flight Deck, please reference the appropriate article.

Software

The PST Flight Deck server can be installed on several different operating systems.

Version	Supported?
Windows 2008 R2	Yes
Windows 2012	Yes
Windows 2012 R2	Yes
Windows Server 2016	Yes
Windows Server 2019	Yes
Windows Server 2022	Yes

All server components require the following server-based features to be installed:

- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 4.5
- BITS
- Internet Information Server with ASP.Net enabled It is recommended the required components be installed using PowerShell commands. (See below)

For required versions of Outlook, click here.

i **NOTE:** Microsoft Office 365 is supported.

SQL Server

PST Flight Deck uses a SQL Server database to track the migration project. The minimum configuration for this server is:

	CPU Cores	RAM
Minimum	4	8 Gb
Average	8	12 Gb

- 10 GB Disk Space on a fast disk for the database
- Adequate space to accommodate log growth between maintenance cycles.

The following versions of SQL Server are supported:

Version	Supported?
SQL 2008	No
SQL 2008 R2	No
SQL 2012	No *1
SQL 2014	Yes
SQL 2016	Yes
SQL 2019	Yes
SQL 2022 RC1	Yes

Permissions/Security

The PST Flight Deck service account requires local Administrator access to all PST Flight Deck servers, full read/write access to the BITS upload share and the storage location that the share points at, and also active SQL ‘dbcreator’ permissions during the installation process.

For migrations to an Enterprise Vault target, the account used as the PST Flight Deck service account needs to be the Vault Service account used for the applicable Enterprise Vault server(s).

All accounts used during the operation of a PST Flight Deck project require the ability to access applicable servers, and to have full read/write access to the PST Flight Deck SQL database. Any account used during the operation of PST Flight Deck must be configured as an “Expert” in PST Flight Deck to have full control over Console functions.

Accounts running services that provide supplemental functionality, such as the Share Scanner or Central Upload Agent, require permission sufficient to access the resources they are acting against. For some of the more advanced features of the Central Upload Agent, this may include access to local workstation administrative shares. Typically these components run under accounts other than the service account.

Ports

The following ports must be open for communication between PST Flight Deck and its dependencies.

Source	Destination	Port	Description
Workstation	PST Flight Deck Server	80/443	Agent communication

Source	Destination	Port	Description
PST Flight Deck Core	SQL Server	1433	SQL access
Module Node	PST Flight Deck Core	80/443, 445 (SMB)	Module to core communication
Ingest Node	PST Flight Deck Core, and target system	80/443, 445 (SMB)	Module to core communication
Workstation	Upload location server	81/444	File transfer (BITS)*

* In addition to the Default Web Site, PST Flight Deck uses a separate PST Flight Deck BITS Website. The Default Web Site's communication passes via port 80/443, whereas the BITS website is preconfigured to use port 81/444. Having this as separate website makes it possible to limit bandwidth immediately when the server is in OFF STATE (because of a full disk for upload) while communication to the Default Web Site continues. All ports can be changed manually, if needed.

Additional Requirements

PST Flight Deck has a highly extendable architecture. As this is the case, the requirements per deployment may change. The following section stipulates the additional requirements needed for supplemental components used within a deployment.

For Ingestion into Exchange or Office 365

Two types of accounts are required in PST Flight Deck when ingesting. Any account used for these targets will need to be assigned “application impersonation” rights. To use some of the advanced functionality available to Exchange or Office 365 targets,

To migrate data for people who have left the organization to an Office 365 target, an account with additional permissions is required. In addition to having “application impersonation” rights assigned, the Exchange Administrator and User Management Administrator roles are also required in order to apply the licenses necessary for this type of migration.

i **NOTE:** GCC and GCC High tenants are supported.

For Ingestion into Enterprise Vault

If the intended target system of a PST migration is Enterprise Vault, additional requirements are needed to accomplish the ingestion.

The current Enterprise Vault Service Account is required for installation and to run the services responsible for any Enterprise Vault related function.

The API associated with version of Enterprise Vault being ingested to is also required. This is typically included in the Enterprise Vault installation media (e.g. “X:\Symantec Enterprise Vault\API Runtime\” where “X:\” is the drive letter of the Enterprise Vault installation media). Frequently, customers choose to install the Enterprise Vault Admin Console instead of the API. this is an acceptable and supported configuration.

For migrations requiring Enterprise Vault shortcut creation, the account running the shortcut module will require “Application Impersonation” rights in the target Exchange environment.

Adding/changing the credentials for Office 365 ingest account

To add or change credentials for Office 365 ingest account, you must use OAuth in order to authenticate with Microsoft Office 365. The main steps of this approach can be found here.

For Shortcut Rehydration

PST Flight Deck includes the ability to restore Enterprise Vault shortcuts found within PST files in the upload area prior to the ingestion into a desired target.

The current Enterprise Vault Service Account associated with the shortcuts being restored is required to run the service responsible for any Enterprise Vault related function, including shortcut rehydration. The Enterprise Vault server associated with the shortcuts must be running and able to successfully retrieve the items associated with the shortcuts via API calls to the source server.

The API for the version of Enterprise Vault being retrieved from is also required. This is typically included in the Enterprise Vault installation media (e.g. “X:\Symantec Enterprise Vault\API Runtime\” where “X:\” is the drive letter of the Enterprise Vault installation media). Frequently, customers choose to install the Enterprise Vault Admin Console instead of the API. This is an acceptable and supported configuration.

For Repair

PST Flight Deck includes the ability to identify and repair corrupted PST files where ever possible.

To facilitate this functionality, PST Flight Deck leverages the native repair utility for Outlook. Outlook 2016 x64 or later (including click to run versions) is required to be installed on any machine running a Repair module.

Using OAuth Authentication

PST Flight Deck can be configured to use OAuth in order to authenticate with Microsoft Office 365.

ℹ **NOTE:** OAuth is currently supported over the EWS endpoints.

Step 1: Create a new Registered Application in Azure (steps can be found here)
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 **Microsoft Entra ID** > **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.

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 **Microsoft Entra ID** > **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.**
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.

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.

Step 5: Add your Application ID and Thumbprint on the server running the PST Flight Deck Office 365 ingest module

1. In PST Flight Deck, open the Credential Editor. Click Credential Editor for more.
2. Select the **Office 365** tab and click **Add**.
3. Enter the Application ID, Thumbprint, and Tenant (eg. tenant.onmicrosoft.com).
4. Save and close the Credential Editor.

Creating the App registration for OAuth

To create an application registration in Azure for OAuth, follow these steps:

1. Log into your Azure portal and select the “App Registration” option located in your dashboard, or type the name into the search bar.

2. In the app registration, select the **New Registration** option.

3. Fill the following columns:

Name – Name the application after your custom preferences

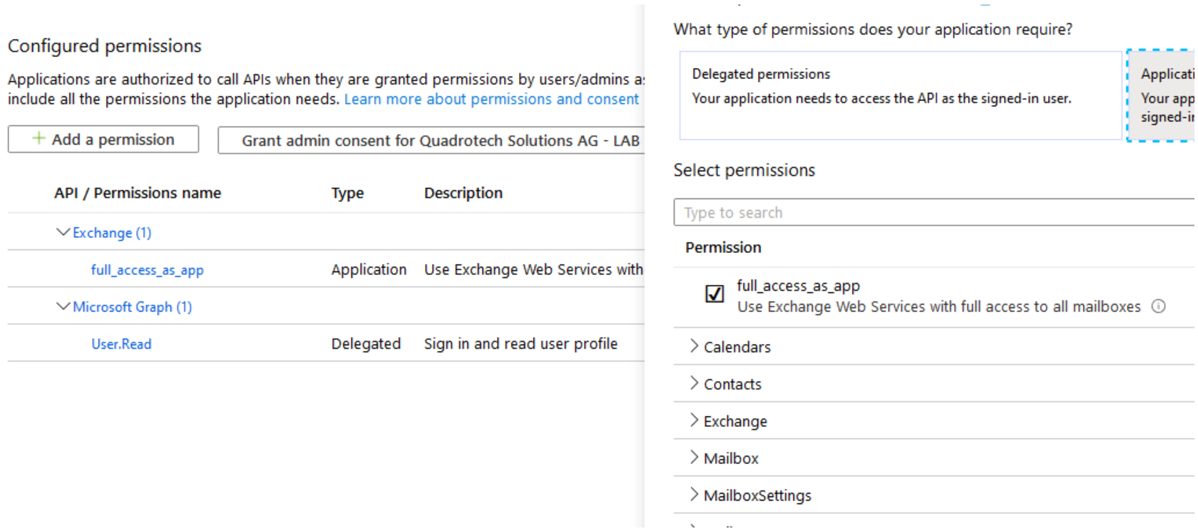
Supported account types – choose the account type that fits most of your organization

Redirect URI – http://localhost

4. Click **Register**.

Your App registration is now complete. When the application is created, the API permissions must be configured. This can be via the API Permissions bookmark on the left panel in the Azure portal by clicking on the **Add a permission** button.

From the permissions, select **Exchange** > **Application Permissions** > **full_access_as_app.**



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins a include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
∨ Exchange (1)		
full_access_as_app	Application	Use Exchange Web Services with
∨ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

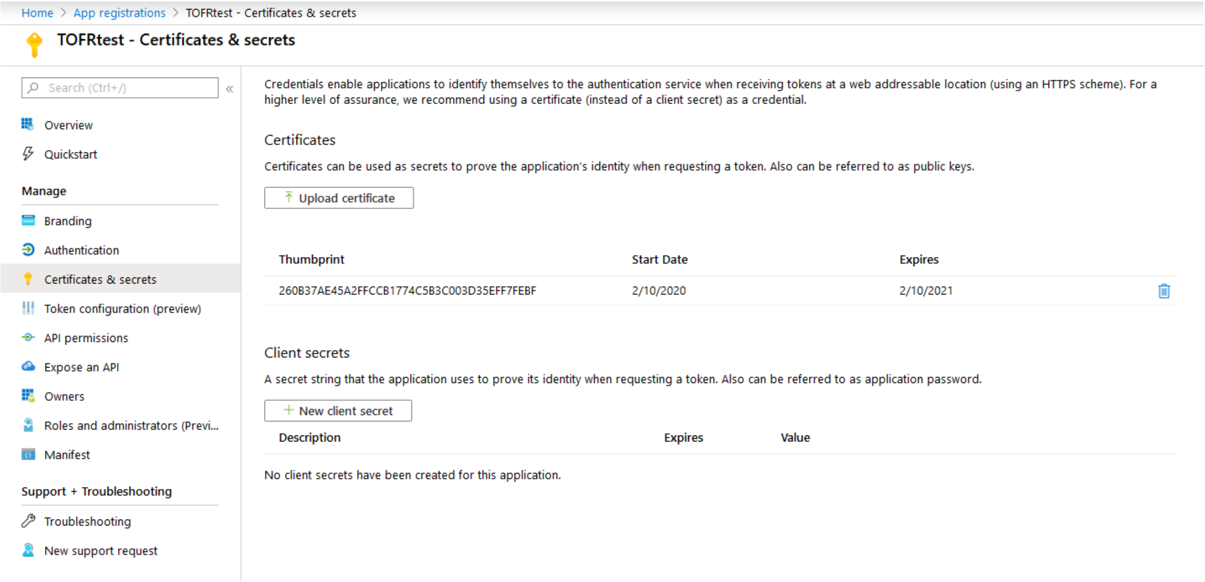
Applicati
Your app
signed-i

Select permissions

Permission

☑ full_access_as_app
Use Exchange Web Services with full access to all mailboxes ⓘ

To upload the certificate that has been previously generated in your PST Flight Deck server machine within the app registration you have just created, navigate to **App registrations** > **Certificates & secrets**:



Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start Date	Expires
260B37AE45A2FFCCB1774C5B3C003D35EFF7FEBF	2/10/2020	2/10/2021

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been created for this application.

By clicking **Upload certificate**, you are able to load the certificate into your Azure application.

These steps are mandatory to configure the Credentials Editor, which uses OAuth as described here.

To create a self-signed certificate for testing purposes, you can follow the steps described in the article here.

PowerShell for Software Components

The following PowerShell commands will install the required components for the installation and operation of PST Flight Deck:

Windows 2008 R2 Service Pack 1

```
Import-module servermanager
Add-windowsfeature application-server, web-server, bits, web-asp-net,
Web-Windows-Auth
```

Windows 2012 and Windows 2012 R2

```
Install-WindowsFeature Application-Server, Web-Server, Web-Windows-
Auth, BITS
Install-WindowsFeature Net-Framework-Features
Install-WindowsFeature Web-Net-Ext45, Web-Asp-Net, NET-WCF-HTTP-ion45
```

Windows Server 2016

```
Install-WindowsFeature Web-Server, Web-Windows-Auth, BITS
Install-WindowsFeature Net-Framework-Features
Install-WindowsFeature Web-Net-Ext45, Web-Asp-Net, NET-WCF-HTTP-
Activation45
```

It may be necessary to utilize the –Source switch to specify the Sources directory on your installation media depending on your OS setup. For additional information, please read the following article: https://support.microsoft.com/en-us/kb/2913316.

How to use PowerShell to verify and grant Application Impersonation permissions

When performing a migration interfacing with Exchange Online or on-premises either directly as a target or in support of post-processing operations, Application Impersonation permissions are frequently required. This section discusses how to use PowerShell to validate these settings and how you can set them if you have sufficient permissions to do so.

Remote connection via Powershell

To execute a PowerShell command in an Exchange Online environment, you will need to establish a remote PowerShell session with the Exchange server. This is also possible with local deployments of Exchange. The following will provide an example using Exchange Online.

1. Launch PowerShell from a local computer and execute the following command: `$Cred = Get-Credential`
2. This will produce a Windows authentication prompt for credentials to be securely stored for the remote session. Populate the prompt with appropriate credentials.
3. Initialize the remote session by issuing the following command: `$ExOnline = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $Cred -Authentication Basic –AllowRedirection`
4. Import the connection to Exchange Online with the following command: Import-PSSession $ExOnline

Verifying Permissions

Once connected, it may be useful to validate that the correct permissions are associated with an account. To verify that an account has the required role association use the following Command: `Get-ManagementRoleAssignment -Role ApplicationImpersonation`

If permissions are validated as expected, make sure to close your PowerShell connection to prevent future issues. Instructions to do so are found below.

Assigning Permission

If required, run the following PowerShell command to assign “application impersonation” rights to the account(s) used for ingestion: `New-ManagementRoleAssignment –Name “Mig Import User” –User “User@ExampleDomain.local” –Role ApplicationImpersonation`

Closing the Session

Once your work in the remote PowerShell session has concluded, you should close the open session using the following command: `Remove-PSSession $ExOnline`

For additional information about connecting to Exchange Online using remote PowerShell, please read the following document:

http://technet.microsoft.com/en-us/library/jj984289(v=exchg.150).aspx

For information on how to remotely connect to PowerShell on an Exchange server, please read the following document:

https://technet.microsoft.com/en-us/library/dd335083(v=exchg.160).aspx

4

Antivirus Exclusions

PST Flight Deck is a product designed to move large quantities of data from client workstations to a desired target. This involves a high level of processing against a given file. If not appropriately excluded, antivirus software can cause file locks, missing data, and performance-related issues that can impact the functionality of PST Flight Deck. The following should be excluded from antivirus scanning.

Modules

PST Flight Deck can be deployed in a number of configurations. It is expandable and customizable to suit the specific needs of any enterprise it is deployed in. Several areas are used to read and write data in a PST Flight Deck environment. Since these areas are frequently in use as part of PST file processing, we recommend that you exclude applicable directories for all of the following services:

- Backup
- Cleanup
- Filter/Extraction
- Park
- Uploads
- Hash table

Fileservers and Workstations

PST files are frequently centralized, migrated, and then deleted. The following are recommended exclusions for workstations and file servers containing PST files that you want to migrate.

- %Temp% location for authenticating users
- Files ending in a *.PST extension