PST Flight Deck 9.2.3

Deployment Guide

© 2026 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

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.
10801 N. Mopac Expressway
Building 3, Suite 400
Austin, TX 78759

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.

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

PST Flight Deck
Updated June 2026
Version 9.2.3

Contents

Introduction **4**

Pre-Installation Requirements **5**

Overview of Licensing 5

Production License 5

Trial License 5

Obtaining a license file 6

Installers 6

Installation **7**

Core 7

Installation Considerations 8

Core Post-Installation Tasks 8

Enable BITS 8

Active Directory Synchronization 9

Next Steps 9

Migration Agent 9

Agent Version 9

Interactive Installation 10

Command Line Installation 10

Next Steps 12

Application Streaming Wrapper 12

Overview 13

Installation 13

Configuration 13

Next Steps 15

Central Upload Agent 15

Overview 15

Installation 15

Content Scanner 16

Installation 16

Configuration 16

Next Steps 17

Shared Scanner **18**

Installation 18

Configuration 19

Management Console **20**

Installation 20

1

Introduction

This guide describes important steps to deploy PST Flight Deck in a general configuration on supported systems. It is written for a technical audience. All installation, configuration, and support should be performed by a PST Flight Deck qualified architect. The goal of this guide is to provide an overview of the installation process. If a comprehensive evaluation of the best deployment for a specific environment is required, a PST Flight Deck architect will need to be engaged.

PST Flight Deck is a scalable enterprise-capable solution designed to address decades of unmanaged PST file creation, utilization, and proliferation throughout an organization. The objective of this solution is to identify and migrate the content of PST files into a target environment to permit the content to be subject to regulatory, retention, and organizational requirements.

The scalability and customization of the solution permits a vast number of suitable configurations and designs. The purpose of this document is to provide a general installation guidance. This document is not intended to provide guidance on PST Flight Deck deployment design. If a comprehensive evaluation of the best deployment for a specific environment is required, a PST Flight Deck architect will need to be engaged.

2

Pre-Installation Requirements

Review the PST Flight Deck requirements document in addition to this guide before installing the software. It will give you a better understanding of the process and requirements needed to successfully implement PST Flight Deck.

All prerequisites discussed in the PST Flight Deck requirements document must be implemented before you attempt to install any of the PST Flight Deck components. In addition, the following items or information will be required during the installation:

- Valid PST Flight Deck license file for the features and domain where the product is installed
- Current version of PST Flight Deck installation media
- Workstation(s) available meeting minimum requirements
- PST Flight Deck Migration Agent installation media for the version of Outlook installed on the workstation(s)
- Name of SQL server which is accessible and configured for PST Flight Deck
- Known desired target system/type connection information

Overview of Licensing

PST Flight Deck uses a license file which is bound to the domain name where the PST Flight Deck Core server is installed. A license file containing the required features and number of accounts that are to be migrated must be obtained prior to the installation.

The following pages are types of PST Flight Deck licenses that are available.

Production License

A production license has no, or vast, time limits associated with it and has the amount of user licenses which have been purchased. It is designed to be the only license required through the life of the project.

Trial License

A trial license allows the full functionality of a license for a limited time. When the license expires, the software continues to run with reduced functionality. This results in changed behavior within the UI and product. This type of license is commonly issued for proof-of-concept installations or during the initial setup and testing of PST Flight Deck.

Obtaining a license file

PST Flight Deck and ScanIt license files are issued by e-mail upon purchase. Trial license files may be issued for proof-of-concept installations through our sales team. If a trial license is required and unavailable, please contact your sales representative directly or the sales team via our site.

If you need to replace a license file, please reference our knowledge base article on how to update a PST Flight Deck license file.

Installers

There are several features available in PST Flight Deck. Depending on your deployment and license, all features may not be offered or appropriate. The installers for the current public version of PST Flight Deck can be downloaded from our site and are as follows:

Feature	Filename
PST Flight Deck Server	PST Flight Deck.msi
Migration Agent x86 version	Migrationagent_x86.msi
Migration Agent x64 version	Migrationagent_x64.msi
Central Upload Agent	CentralUploadAgent.msi
Content Scanner	ContentScanner.msi
Share Scanner / Content Scanner / Central Upload Agent	SharedScanner.msi
PST Flight Deck Admin Console	ManageUI.msi

3

Installation

PST Flight Deck has many components that can be installed to best suit a project's requirements. The following discusses the installation of many of these components.

Core

The Core server is responsible for several aspects required for a functional PST Flight Deck system. In a typical configuration, the Core server hosts the PST Flight Deck Core service, the IIS instance hosting PST Flight Deck files, the Background Intelligent Transfer Service (BITS) upload directory, and any number of modules which may be installed. The Core service is responsible for communication with the PST Flight Deck system database and execution of scheduled operations. All deployed agents also check in and update the system through the Core server. Essentially, the Core service acts as the conductor of the entire solution.

A typical deployment of PST Flight Deck begins with the installation of a Core server. In most deployments, you will have more than one PST Flight Deck server, however for non-production installations it is possible to deploy all the components on a single server. It is not recommended to perform production migrations in a single server configuration.

For a successful installation, it is important that all of the requirements have been met prior to starting. If you have not done so, please review the Requirements Guide and this document to ensure all criteria for installation and configuration are met.

To install the first PST Flight Deck server:

1. Log into the PST Flight Deck server as the PST Flight Deck service account
2. Execute the PST Flight Deck MSI installer.
3. Follow installer prompts to provide the following information:
    b. Review and accept the Agreement
    c. Determine features to install and desired installation location
    d. Select and validate the PST Flight Deck license file
    e. Define the SQL server or instance to be used for the PST Flight Deck system database and validate access to the resource
    f. Provide the PST Flight Deck service account and validate it
    g. Provide Core PST Flight Deck server name or alias and method of communication to the server
    h. Select the target and associated configuration for the project
    i. Select the storage locations to be used for the PST Flight Deck modules
4. Select Install to begin the installation
5. Monitor to completion and select Finish to complete the installation wizard

Any additional node may be installed using the same installer but only selecting the modules desired for installation on that node. Typically, Extraction and Repair modules are installed locally to the BITS Upload directory for each Location.

Installation Considerations

Some organization's security requirements do not permit interactive logons for service accounts. In these cases, it is necessary to have an additional account used as an installation account. If an alternate account is required to be used for installation, equivalent rights will be required for the installation account at the point of installation.

It is important to differentiate between the PST Flight Deck service account and other accounts which may be used as part of your PST Flight Deck deployment. Generally speaking, the PST Flight Deck service account is used during installation and is the account the services run as. When targeting an Enterprise Vault system for migration, the PST Flight Deck service account will be the same as the Enterprise Vault service account. Some targets, such as Exchange or Exchange Online, require multiple accounts with various elevated rights. Typically these accounts are not the same as the PST Flight Deck service accounts. For more information on the accounts required for your deployment, please refer to the Requirements Guide.

PST Flight Deck is designed to be able to function when using HTTPS to encrypt all module and client traffic to the PST Flight Deck server.

> **NOTE:** the customer will have to supply and configure appropriate machine or domain associated SSL certificates within IIS on the Core server.

It is recommended to have the BITS upload location on a separate high performance disk from the remainder of the PST Flight Deck modules' working directories. Doing so will promote improved performance and stability in all operations throughout your migration.

Core Post-Installation Tasks

Once the PST Flight Deck installer has completed, a few system configuration changes are needed to ensure proper functionality of the PST Flight Deck server.

Enable BITS

PST Flight Deck leverages the Background Intelligent Transfer Service (BITS) to centralize PST files from Migration Agent machines to a desired PST Flight Deck server. For this process to work as expected, BITS must be enabled on the Core server's IIS instance using the following process:

1. Open the IIS Manager
2. Expand the PST Flight Deck BITS Website and select the Uploads virtual directory
3. In the Features View center panel of the IIS management console, scroll to the bottom and double-click BITS Uploads
4. In the resultant options, select Allow clients to upload files and hit the Apply link in the "Actions" panel.

More details related to BITS can be found on the Microsoft MSDN site.

Active Directory Synchronization

PST Flight Deck must obtain information from Active Directory (AD) related to domains and user accounts. Upon initial synchronization, information related to all domains are added to the PST Flight Deck databases. After installation has completed and before using the product, this synchronization should complete.
To confirm AD synchronization has been initiated:

1. Launch the PST Flight Deck Admin Console
2. Select Settings > Scheduled Tasks
3. Confirm the “Synchronize Active Directory” task’s “Last Run” time is populated

Depending on the environment, collecting all the required information from a domain can take some time. The process can be observed in the PST Flight Deck Administrator or Management Console under the Users section of the Manage screen. To learn how to enable logging in PST Flight Deck please visit our knowledgebase article on the topic.

Next Steps

Upon completion of the Core installation and configuration, the main part of your PST Flight Deck installation will be complete. To validate the installation is working as expected, install at least one Migration Agent on a workstation and perform an initial test ensuring the test file completes processing from one end of the migration to the other. If the migration did not complete successfully, it is a good idea to validate the configuration of your PST Flight Deck installation prior to performing any other troubleshooting.

Migration Agent

PST Flight Deck leverages a component installed on end-user workstations called the Migration Agent. This agent is critical for discovering PST files, providing meta-data to help to determine PST file ownership, managing the user interaction with the PST files, and uploading PST files to a centralized location throughout a migration project.

The Migration Agent has a lightweight footprint and is supported on many client operating systems. Prior to installation, a workstation should be confirmed to meet the system requirements for the Migration Agent. For details as to the requirements to install the agent please refer to the Requirements Guide.

Agent Version

The version of the agent that will be installed will coincide with the architecture of Outlook which is installed. For example, if a client has the 64 bit version of Outlook installed, the installer will automatically detect and choose to install the 64 bit version of the Migration Agent.

Interactive Installation

Although most installations will be automated, initial tests of the Migration Agent installations are frequently performed interactively. This approach is not suitable for production deployments of the agent over multiple workstations.

To install the PST Flight Deck Migration Agent interactively on a desired workstation:

1. Log into a workstation with an account that has local administrative permissions.
2. Download the appropriate Migration Agent installer to the applicable workstation
   b. Current 32-bit installer
   c. Current 64-bit installer
3. Execute the Migration Agent MSI installer: Migrationagent_xNN.msi (Where "xNN" represents the architecture)
4. Follow installer prompts to provide the following information:
   b. Review and accept the License Agreement
   c. Supply the location where the Migration Agent will be installed
   d. Supply the PST Flight Deck Core's fully qualified web service address and method of communication to the server*
   e. Determine if you wish to enable the Discovery Scanner upon user logon
5. Select Install to begin the installation
6. Select Finish to complete the installation wizard.

* For production Migration Agents, it is strongly encouraged to use a DNS alias for the PST Flight Deck server rather than an actual server name.

Command Line Installation

For a production environment, the Migration Agent is typically installed on every workstation within an organization. Performing an interactive installation to accomplish this is typically unrealistic. For deployment to a large number of workstations, a command line installation (CLI) is frequently required.

Overview

In addition to the options available for installation via the MSIEXEC command, PST Flight Deck has several properties that are passed to the installer to configure the Migration Agent during installation. A CLI is also used to configure properties that are not exposed during an interactive installation. It is always recommended to build a CLI command and test it on a local workstation prior to using the command for a mass Migration Agent deployment.

Syntax

The following is the syntax used when building a command line installation for the Migration Agent. In the examples below, “xNN” represents the architecture of the agent being installed. Below is the general syntax of the command:

```
msiexec /i MigrationAgent_xNN.msi [WEBSERVICESERVERNAME=<SERVERNAME>]
[REGISTERFILESCANNER="1"] [USE_HTTPS="1"] [WEBSERVICEAPPNAME=<PST
Flight DeckWS>]
```

Options

Although only a single property needs to be passed to the PST Flight Deck Migration Agent for a successful installation, there are many options available when installing from a command line.

Property	Required	Description
WEBSERVICESERVERNAME	Yes	The server where PST Flight Deck IIS instance is hosted. Typically, the Core server is the desired target. DNS alias is preferred for this value.
REGISTERFILESCANNER	No	Inform Migration Agent install if PST Flight Deck Discovery Agent is to be started at user logon. To disable the file scanning set this property to “0”.
USE_HTTPS	No	For use when agents are required to communicate to PST Flight Deck using HTTPS. Specify “1” to enable this feature.
WEBSERVICEAPPNAME	No	Used to specify an alternate IIS hosted web application location other than the default one. Specify the name of the desired web application to enable this feature.

Examples

There are a number of configuration scenarios under which you may use a CLI in the deployment of a PST Flight Deck migration agent. The following examples utilize the MSIEXEC command and its

switches to install and suppress any visibility of the installation (/q /i). For more information on options available to the MSIEXEC command, please refer to the Microsoft MSDN article on MSIEXEC.

Below are some common examples of CLI syntax using "xNN" to represent the architecture of the Migration Agent being installed, "PST Flight DeckAlias.somedomain.local" to represent the alias of the server where the PST Flight Deck IIS instance is hosted, and "X:\Path\To\" representing a path valid to the workstation where the installation is occurring.

The following example shows a standard installation of the Migration Agent. Typically, the Core server is the desired target of the WEBSERVICESERVERNAME and a DNS alias is preferred for this value.

```
msiexec /q /i "X:\Path\To\MigrationAgent_xNN.msi"
WEBSERVICESERVERNAME=PST Flight DeckAlias.somedomain.local
```

The next example shows how to specify communication to be performed over the HTTPS protocol:

```
msiexec /q /i "X:\Path\To\MigrationAgent_xNN.msi"
WEBSERVICESERVERNAME=PST Flight DeckAlias.somedomain.local
USE_HTTPS=1
```

This final example shows a basic and typical installation which produces logging for troubleshooting:

```
msiexec /q /i "X:\Path\To\MigrationAgent_xNN.msi"
WEBSERVICESERVERNAME=PST Flight DeckAlias.somedomain.local /l*x "X:
\Path\To\InstallLog.txt"
```

Once the installation has completed you will see the Migration Agent represented amongst the installed applications on the workstation. The Migration Agent will not be functional until the next successful user logon to that workstation. For the Migration Agent to be immediately functional, you may wish to force a reboot as part of the installation process.

Next Steps

Once the first Migration Agent has been installed and a user has logged back in successfully, no user interaction is required to begin the discovery process. It is recommended to go through some initial testing to confirm the Migration Agent is working as expected. The installer should validate the installation and configuration settings of the Migration Agent prior to executing future deployments. This testing will typically culminate in a successful end to end test to confirm full system functionality.

Application Streaming Wrapper

The PST Flight Deck Application Streaming Wrapper (ASW) is designed for environments that utilize virtual application streaming to provide Outlook to users. Due to the way application streaming is performed, a typical agent approach cannot be used. The system requirements of ASW are minor and typically covered by the requirements of the streaming solution and the Outlook application being streamed.

Overview

The ASW works as a wrapper for Outlook on an application streaming solution. Upon launch, it checks to see if a user is enabled for migration. If they are enabled, it quickly closes open connections to PST files associated with the user's Outlook profile during that streaming session. Once it has completed, it launches Outlook and maintains the standard user experience without any of the PST files connected. There is no interaction required from users streaming Outlook but their experience will be impacted as PST files will no longer be attached to their streamed Outlook instance. The ASW is frequently used in conjunction with the Central Upload Agent to enable discovered files to be uploaded from shared resources without the use of a traditional Migration Agent.

Installation

The ASW is currently only available by contacting Quest.

The installation for the ASW is a manual process. The ASW installation media contains a number of files. The following table shows the files and their functions:

Component	Description
MigrationAgentCitrixClient.exe	Outlook wrapper published via streaming solution
MigrationAgentCitrixClient.exe.config	Configuration file for the wrapper
NLog.config	Configuration file for logging
NLog.dll	ASW required library
Profman.dll	ASW required library

Installation of the ASW involves copying the above files to the streaming solution server and completing the applicable configuration for the wrapper.

Configuration

After manual installation of the ASW has completed, there are several areas that should be evaluated for configuration.

Wrapper

Configuration of the ASW is required prior to use. All configuration changes to the ASW takes place in the MigrationAgentCitrixClient.exe.config file with the exception of logging. The format of this file is standard XML format and can be edited in any text editor.

Configuration parameters available are as follows:

- OutlookPath – Local Path of the Outlook.exe on the streaming server

- DisconnectSession – Controls behavior of the session after PST file detachment
- DisconnectSessionCommand – Command issued upon session disconnection
- DisconnectSessionMessage – Text informing user of change, forced session disconnection, and the need to reconnect to continue working
- DisconnectSessionCaption – Text used for title bar of DisconnectSessionMessage
- endpoint address – The AdvancedClient.svc endpoint hosted by the IIS instance on the PST Flight Deck server.

Below are some configuration options and examples:

Property	Accepted Value	Example Value
OutlookPath	Valid local path to Outlook.exe	C:\Program Files (x86) \Microsoft Office\Office14\Outlook.exe
DisconnectSession	TRUE/FALSE	TRUE
DisconnectSessionCommand	Any command line directive executable by user initiating session *	shutdown /l /f
DisconnectSessionMessage	Plain text	Your Outlook profile has been changed. Please restart your session
DisconnectSessionCaption	Plain text	Session Disconnected
endpoint address	Full URL to the PST Flight Deck Server hosted AdvancedClient.svc	http://pstflightdeckalias/PSTFlightDeckWS/AdvancedClient.svc

* Omitting the logoff command (/l) may result in the host machine shutting down. We recommend using the force command (/f).

Logging

Logging for the application configuration wrapper is configured separately than the wrapper itself. By default, logging is enabled at an “Info” level and configured to write to the %TEMP %/Quadrotech/MigrationAgent.log location. There is typically no need to make changes to the default logging. The NLog.config file contains the configuration to modify logging if required.

Outlook

The ASW replaces Outlook as the published application within your streaming solution. The icon and name can be changed to give the appearance to the end user that Outlook is still the application being published. To cease publication of Outlook and publish the ASW consult your streaming solution’s documentation.

Depending on the utilization of Outlook on your application streaming host, you may also wish to set registry keys governing how Outlook handles PST files. Unlike the Migration Agent, the ASW has no ability to manage the utilization of the PST files. For information regarding the registry keys the Migration Agent sets when a user is enabled for migration, please refer to the knowledge base article.

Next Steps

Once installed and configured, the ASW is fully functional. When an enabled user launches the published ASW application over the streaming solution's interface, any PST files that are attached to that user's profile will be disconnected if the user is enabled for migration.

Central Upload Agent

The Central Upload Agent (CUA) is a component frequently utilized in a PST Flight Deck environment. The primary role of the CUA is to upload files stored on centralized repositories more rapidly without having to use a workstation's Migration Agent. This can result in quicker processing for users that are separated from their PST storage location by a slow WAN link, users without a Migration Agent, or PST Files with no clear owner. Prior to installation, the system requirements for the CUA should be met. For more information related to the system requirements for the CUA please review the Requirements Guide.

Overview

The CUA is usually installed on a low resource server or workstation located near user file servers, project shares, or other centralized locations where PST files are typically stored. Once a CUA is configured, file servers can be designated as "Central Servers" that the CUA will use to copy files from their original location to the PST Flight Deck server's upload location and resume a typical workflow. With sufficient rights, the CUA can also be used for a "Forced Migration". This will expedite uploading a user's PST files and bypass the Migration Agent.

The CUA may be used for either Transparent or Disconnect modes of migration.

Installation

The CUA needs sufficient permissions to access, copy, and remove PST files from their original location. On file shares, the account will need read/write share and file system access. If you intend to use the CUA to perform "Forced Migrations" the account used to run the CUA will need sufficient rights to access the administrative share on locations where PST files are located. To ensure stability and supportability, ensure the system requirements are met prior to installing the CUA.

To install the Central Upload Agent:

1. Log onto the machine where the CUA will be installed as an account with sufficient rights to perform the installation.
2. Execute the CUA MSI installer: CentralUploadAgent.msi

3. Follow installer prompts to provide the following information:
    b. Review and accept the License Agreement
    c. Provide credentials with sufficient rights to access and remove PST files from their discovered locations
    d. Select Check and Next when available
    e. Provide the desired installation path of the CUA
    f. Provide the Core PST Flight Deck server name or alias and method of communication to the server
    g. Specify the UNC path of the BITS upload location
    h. Select Install to begin the installation
    i. Monitor the installation and select Finish once completed

Content Scanner

One of the largest challenges of a PST migration project is identifying the proper owner for each of the PST files that have been found on a shared file server. PST Flight Deck Content Scanner is used to scan PST files marked as “Ownerless” or those files located on specific fileservers, and associate ownership based on the contents of the file. This component is specifically useful when scanning project or departmental shares where PST files identified may not have clear owners associated with them.

Installation

The Content Scanner can be installed on the Core server as described above or on another machine using the installer available. All requirements, including proper account access rights, of the Content Scanner should be met prior to installation. For instructions on how to install the Content Scanner on the Core server, please refer to the installation section above.

To install the Content Scanner on a server other than the Core server:

1. Log into the machine where you will be installing the Content Scanner as an account with sufficient rights to perform the installation.
2. Execute the Content Scanner MSI installer: ContentScanner.msi
3. Complete installer prompts providing the following information:
    b. Review and accept the License Agreement
    c. Supply and validate the account that will be used to run the Content Scanner module
    d. Provide Core PST Flight Deck server name or alias and method of communication to the server
    e. Select Install to begin the installation
    f. Monitor the installation and select Finish once completed

Configuration

The Content Scanner will attempt to scan any PST file which is marked as Ownerless. The content scanner can also be set to scan all files from a given target regardless of ownership association. This can be useful for project shares that have files which may have been discovered from a number of users or perhaps a single unique user.

To specify targeted servers:

1. Launch Admin Console and select Settings > Computers
2. Highlight the file servers desired for target
3. Under the Content Scanner section, select Set to target those servers
4. Refresh view to confirm the targeting

Next Steps

Once installed and configured, the Content Scanner attempts to scan all PSTs found on a targeted server or associated with the configured “Ownerless Account”. The Content Scanner identifies the owner of a PST file by scanning the sender and recipient information of its content. It is able to help determine ownership of a PST file by documenting when the most frequently occurring sender or recipient within a PST file matches for over 50% of items within a PST file. The results of the content scanner become visible in the Management or Admin Consoles under Manage > Owners.

4

Shared Scanner

The Share Scanner is a supplemental component that can be used in conjunction with a Core installation. The purpose of the Share Scanner is to enable resources such as file servers and project shares to be scanned for PST files contained on those resources. Identified files are sent to the Core server for inclusion in the PST migration project.

Installation

The Share Scanner is able to be installed via an MSI available on our FTP site. The Share Scanner should be installed with a dedicated account that would never naturally be associated with any PST files. The account will need sufficient rights on the file servers and other resources it is intended to scan. Several file servers can be associated with a single Share Scanner.

The installer for the Share Scanner includes the following components that can be installed:

Feature	Description
Content Scanner Module	Used to scan PST files to aid in ownership discovery
Central Upload Agent	Agent used as an alternate means to transfer PST files to the upload location
File Scanner	Primary feature of installer. Used to discover PST files located on file servers or project shares

To install the Share Scanner on a supported server:

1. Log into the machine where you will be installing the Share Scanner as an account with sufficient rights to perform the installation
2. Execute the Share Scanner MSI installer: SharedScanner.msi
3. Complete installer prompts providing the following information:
   b. Review and accept the License Agreement
   c. Select the components to be installed on the machine
   d. Supply and validate the account that will be used to run the selected components
   e. Provide Core server name or alias and method of communication to the server
   f. Provide the UNC location for the BITS upload directory for the location the Central Upload Agent will write to
   g. Select Install to begin the installation
   h. Monitor the installation and select Finish once completed

Configuration

Share scanner configuration is performed by editing the config.xml file located in the specified installation location. The configuration file is fully commented with examples on how to edit the configuration. Minimally, the server section needs to be modified to reflect all project drives desired for scanning. In the example below, two source locations are shown. The Share Scanner can be used to scan dozens of source resources.

Example of <server> section configuration:

```
<server>
<Path>P:\</Path>
<Pattern>*.pst</Pattern>
</server>
<server>
<Path>\\FS001\d$</Path>
<Pattern>*.pst</Pattern>
</server>
```

When appropriately configured, the scanned results should appear in the Console shortly after they are identified.

5

Management Console

PST Flight Deck has a powerful GUI which grants control and reporting options for your migration called the PST Flight Deck Management Console (Management Console). With it you can manage migrations, communications to end users, and generate reports related to the progress and performance of your environment.

Installation

The Management Console is available via a standalone installer. Review the Requirements Guide for the minimum requirements and supported systems for installation.

To install the Management Console:

1. Log into the machine where you will be installing the Management Console as an account with sufficient rights to perform the installation.
2. Execute the Management Console MSI installer: ManageUI.msi
3. Follow installer prompts to provide the following information:
   b. Review and accept the License Agreement
   c. Confirm or alter the installation location
   d. Provide the PST Flight Deck SQL instance being used and confirm access
   e. Provide Core server name or alias and method of communication to the server
   f. Select Install to begin the installation
   g. Monitor the installation and select Finish once completed

Once installed you can launch the Management Console from the start menu with an account with sufficient access to the PST Flight Deck database.