Dell Migration Manager for PSTs 1.2.1

Quick Start Guide

Migration Manager for PSTs Quick Start Guide
Updated - February 2016
Software Version - 1.2.1

Legend

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

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

Contents

1

Migrating With MMP

Product overview

This Quick-Start Guide has been prepared to get you started with Dell™ Migration Manager for PSTs (MMP). It orients you to its basic purposes and features, and then to help you install it. The Quick-Start Guide is written for network administrators, consultants, analysts, and any other IT professionals who will install the product, use its administration tools, or contribute to migration project planning. Additional migration scenarios and advanced installation types are covered in the *Migration Manager for PSTs User Guide*.

Migration Manager for PSTs lets you migrate PST files from a supported source system to mailboxes in Exchange 2016, Exchange 2013, Exchange 2010, or Microsoft Office 365 Exchange

Online. This can be accomplished through the Migration Manager for PSTs web GUI, or the PowerShell command-line interface. Simple migration scenarios using both of these approaches are documented in this Quick-Start Guide.

Supported PSTs and Message Types

Along with standard messages in PSTs, MMP supports the following:

- Microsoft Outlook encrypted or signed S/MIME messages
- Password protected PSTs
- Locked PSTs
- PSTs where the UNC path to the file is longer than the supported Windows max path length.
- Non-Unicode PSTs, such as PSTs created in Outlook 97 or Outlook XP.

By default, hidden messages are not migrated. Optionally, hidden messages can be migrated using the Start-MMPMigrationTask cmdlet and the -MigrateAssociatedItems parameter. This parameter is documented in the *PowerShell Cmdlets* chapter of the *MMP User Guide*.

Product components

- **Configuration Console:** This Windows utility allows you to configure the SQL connection website settings, agent settings and logging settings for MMP. You need to run this on every MMP server on which you install an MMP component. You may also use the Configuration Console later to change these settings.
- **Web Service and Scheduling Agent:** The Web UI and the service layer providing data to the MMP Web UI, Agents, PowerShell Cmdlets, and the windows service that manages scheduled tasks for processing by other MMP agents.
- **Discovery agent:** The windows service that performs discovery of users and computers within Active Directory domains, as well as file scanning of those computers for PST files.
- **Migration agent:** The windows service that handles migration of PST file data into Microsoft Office 365 or Exchange.
- **PowerShell Cmdlets:** The Powershell command line interface for MMP.
- **Dell Log Viewer:** The Dell Log Viewer simplifies the viewing and interpretation of program log files, which document events and warnings in Dell programs.

System requirements

The following sections list the supported versions of software required to run the Migration Manager for PSTs.

Administration migration server(s)

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

SQL server

An existing SQL Server may be used, or you can set up a new server to use with MMP.

- SQL Server 2014
- SQL Server 2012 SP2
- SQL Server 2012
- SQL Server 2008
- SQL Server 2008 R2

Target servers

- Exchange 2016
- Exchange 2013 SP1
- Exchange 2013
- Exchange 2010 SP2 and later
- Office 365 Exchange Online (O365)

End user workstations

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows XP
- Windows Vista
- Windows Server 2012R2
- Windows Server 2012
- Windows Server 2008 x86
- Windows Server 2008 x64
- Windows Server 2008R2

Internet Information Services

IIS is not needed for an agent-only installation.

- IIS8
- IIS7
- Windows Authentication
- The SQL Server Native Client must be installed on the IIS server, to allow communication with the SQL Server instance where the MMP database will be created.
- If you want to use HTTPS to encrypt the data from the MMP website with SSL, then you will need to obtain or create an SSL certificate and bind it to the MMP website. You may use a self-signed certificate or an authoritative certificate purchased from a certificate authority.
- The WebDAV feature must be disabled on your IIS server.
- ASP.NET 4.5

NOTE: It is recommended that you install IIS before installing .NET 4.5.1. ASP.NET 4.5 may not be properly registered with IIS when .NET Framework 4.5.1 is installed before installing IIS.

To verify that ASP.NET 4.5 is installed and registered with IIS, complete the following steps:

1. Open IIS Manager and browse to Application Pools.
2. Check for ASP.NET v4.0 - if this is listed, then ASP.NET 4.5 is installed and registered with IIS.

To register ASP.NET 4.5 with IIS after it is installed on Server 2012 R2 or 2012, complete the following steps:

1. In the Windows Server Manager, navigate to the **Add Roles and Features Wizard**.
2. Select **Server Roles** from the left-hand menu.
3. In the Roles box, under WebServer (IIS)|Web Server|Application Development, select the **ASP.NET 4.5 (Installed)** checkbox.

To register ASP.NET 4.5 with IIS after it is installed on Server 2008R2:

1. Open a Windows Shell.
2. Change to the directory of the latest .NET folder. For example: `C:\Windows\Microsoft.Net\Framework\v4.0.30319`)
3. Execute the command: `aspnet_regiis.exe -i`

.NET framework

- .NET 4.5.1

PowerShell

- 2.0 or later. For Windows Server 2008 R2, this can be installed from the Microsoft Management Framework.

NOTE: In order to run the MMP cmdlets, MMP will add or modify **powershell.exe.config** upon installation in the following locations:

- System32\WindowsPowerShell\v1.0\
- SysWow64\WindowsPowerShell\v1.0\

For installations of the 32 bit installer on a 32 bit machine, it will add/modify in the System32 directory.

For installations of the 32 bit installer on a 64 bit machine, it will add/modify in the SysWOW64 directory.

For installations of the 64 bit installer on a 64 bit machine, it will add/modify in both directories.

Supported browsers

- Internet Explorer 11 and 10 for Windows
- Firefox 21, 20, and 19 for Windows or Mac OS X.
- Chrome 26, 25 and 24 for Windows.

Installation and configuration permissions

The user installing the software must be a local administrator and have the following rights:

- Rights to create a website in IIS.
- Rights to create a database in SQL.
    - SQL Server Roles:
        - dbcreator
        - sysadmin
- Member of Local Administrators

Post-installation and configuration permissions

SQL Permissions

After installation and configuration, you do not need the dbcreator and sysadmin SQL Server roles. You will need the rights listed below.

- Rights to maintain the MMP database in SQL:
    - Server Role: bulkadmin (recommended)
    - Database Roles: db_owner

Web Authorization

The users and groups that have access to the MMP Website can be configured through the .NET Authorization Rules settings in IIS.

The .NET Authorization settings can be found under the ASP.NET section of the IIS Manager. By default, the only rule set is an "Allow" for "All Users". This indicates that any user that can authenticate to the website using Windows Authentication can access this website.

New rules can easily be added, by selecting **Add Allow Rule** and **Add Deny Rule** in the right-hand panel.

For more details on how to set up authorization in the IIS Manager, please view the Microsoft documentation on this located at http://technet.microsoft.com/library/hh831722.aspx.

Migration agent service

In order to migrate locked PST files on remote machines, the migration agent service must run as a domain administrator account instead of local system.

Migration sources

Migration sources require connection credentials and may have limits on the number of source connections. This limit does not occur during discovery. It may occur when attempting to migrate multiple PSTs from a single client.

Connection credentials

The migration source connection must have the following connection credentials:

- Rights to query Active Directory.
- Administrator credentials to access the administrator folder shares and access files and temp directories on any computer, including the migration server, during discovery and migration. The format must be username@domain or domain\username.

Limits on source connections

There may be a limit on the number of source connections that you can have. This depends on the operating system of the client computer hosting the PST file. If you exceed the number of connections, the task will be retried later.

Exchange 2010/2013/2016 target credentials

The following sections explain how to configure your Exchange 2010 SP2, 2013 or 2016 target system.

Enabling Application Impersonation Rights

To migrate data to Exchange 2010/2013/2016, your administrator accounts must have Application Impersonation rights, which means the accounts must be assigned to a Role-Based Access Control group that has Application Impersonation rights. Because no groups have Application Impersonation rights by default, you need to add Application Impersonation rights to an existing group or create a new group. One way to do this is by using the Exchange Management Shell with PowerShell cmdlets. The cmdlets to run can be found here.

To create a role group for impersonation, use the PowerShell cmdlets from the article above. To create the impersonation role and assign a user to that role:

1. Log on to your Exchange server, or to a computer that has the Exchange Administration tools installed on it as an Exchange administrator.
2. Go to Start | All Programs | Microsoft Exchange Server 2010/2013/2016 | Exchange Management Shell.
3. Run the cmdlet to create the management role group and assign the **ApplicationImpersonation** role to that group, and then assign the user you want to use as a migration administrator.

   In the following example, we are using the user pst_migration_admin@sitraka.com.

```
New-RoleGroup -Name MigrationImpersonation -Roles
ApplicationImpersonation
-Members pst_migration_admin@sitraka.com
```

You can add multiple users using commas to separate each user.

Accessing the Mail Server

Make sure that Outlook Web Access (OWA) is accessible from the internet. MMP uses Exchange Web Services (EWS) to access your mail server from the internet. The OWA server name can be used for accessing your Exchange server with EWS. If you are not using HTTPS for OWA, you will need to enter the full URL for your EWS service which follows the format *http://servername/EWS/Exchange.asmx*.

You can find the URL for your EWS server using PowerShell. From the Exchange Management Shell, execute the following command:

```
Get-WebServicesVirtualDirectory | Select name, *url* | fl
```

The EWS server URL will be returned in the ExternalUrl value. To access the mailboxes slated for migration, the migrator needs to have an account with the **ApplicationImpersonation** role.

Office 365 target credentials

Connections to O365 may be limited to 10 per credential. If this number is exceeded, additional credentials are needed. By default, a single migration agent runs 5 threads, which will open 5 connections. If you have multiple migration agents or have changed the default to more than 10 threads, additional credentials should be entered.

To migrate data to Office 365, your administrator accounts must have Application Impersonation rights, which means the accounts must be assigned to a Role-Based Access Control group that has Application Impersonation rights. Because no groups have Application Impersonation rights by default, the first step is to sign in as an organization administrator to the Office 365 portal (http://portal.microsoftonline.com) and either add this right to an existing role group or to a new role group that you create.

It is recommended that you create a new role group named “Migration Impersonation” and add the Application Impersonation right to it.

Role groups are created in the Role Groups page of the Office 365 portal.

1. After logging in, go to the Options menu, select **See All Options....**
2. Then from the **Options: Manage Myself** menu, select **My Organization**.
3. Lastly, select the **Roles & Auditing** item and click **New**.

Hardware requirements

The following hardware is required for optimal performance of MMP. The workstation may be a virtual machine, but a dedicated machine will enhance migration performance.

Standard Migration:

- 3 GHz dual-core processor, 4GB memory, 50GB free disk space

High-volume Migration Recommendations:

- 3 GHz quad-core processor, 16GB memory, 100GB free disk space
- 1 Gbps NIC, and 1 Gbps or faster network connections

Getting started

The following sections walk you through installing Migration Manager for PSTs and running a migration through the GUI or PowerShell.

Installing Migration Manager for PSTs

Migration Manager for PSTs can be installed through the **autorun.exe** GUI, which provides helpful information and links to download required software.

The following files are provided on the installation media:

- autorun.exe
- **DellMMPInstaller (x86).msi:** The installer for 32-bit Windows
- **DellMMPInstaller (x64).msi:** The installer for 64-bit Windows
- MMPUserGuide.pdf
- MMPQStartGuide.pdf
- MMPReleaseNotes.pdf

Prerequisites Checker for a full installation

The Prerequisites Checker is a program that you can use to verify that you have all of the required prerequisites installed prior to installing Migration Manager for PSTs.

To run the Prerequisites Checker for a full installation, complete the following steps:

1. Open the **autorun.exe** program provided in your installation media.
2. Select the **Prerequisites** menu.
3. In the Check for Installed Prerequisites section, go to the **Prerequisites Checker for Web Server/Full Product Install** box.
4. Click **Run** to open the Prerequisites Checker.
5. On the Exchange Login screen, enter the Administrator Credentials.
    - **Email:** The administrator email account.
    - **Password:** The password for the administrator email account.
6. On the SQL Server screen, enter the SQL Server credentials.
    - **Host name:** The host name of the computer where the SQL instance is located.
    - **Authentication mode:** Select either Windows Authentication or SQL Authentication.

    For SQL Authentication, enter the Username and Password.

        - **Username:** The name of the user account that will be used to connect to the SQL server.
        - **Password:** The password for the user account that will be used to connect to the SQL server.
7. The Report screen displays the list of items that will be checked. Click **Run** to start the Prerequisites Checker. The list of prerequisites includes:
    - Installed Software

- Autodiscover Server
- .NET Framework
- Microsoft Internet Information Services
- Operating System
- Windows Management Framework
- Hardware
- Microsoft SQL Server

Icons next to each prerequisite in the Prerequisites Checker display the status:

- **Green box with checkmark:** Success
- **Red circle with x:** Error
- **Yellow triangle with exclamation point:** Warning

8 Click the arrow next to any prerequisite to expand the list of items under that prerequisite.

9 Information regarding the status of each prerequisite is displayed to the right of each line item. Any additional information about each prerequisite may be displayed by clicking on a line item and then clicking **View Details** next to the information icon at the top of the screen.

10 Correct any errors prior to installing Migration Manager for PSTs.

Prerequisites Checker for an agent-only installation

The Prerequisites Checker is a program that you can use to verify that you have all of the required prerequisites installed prior to installing Migration Manager for PSTs.

To verify that required prerequisites are installed correctly prior to running Migration Manager for PSTs, complete the following steps:

1 Open the **autorun.exe** program provided in your installation media.

2 Select the **Prerequisites** menu.

3 In the Check for Installed Prerequisites section, go to the **Prerequisites Checker for Agent-Only Install** box.

4 Click **Run** to open the Prerequisites Checker.

5 On the Exchange Login screen, enter the Administrator Credentials.

- **Email:** The administrator email account.
- **Password:** The password for the administrator email account.

6 The Report screen displays the list of items that will be checked. Click **Run** to start the Prerequisites Checker. The list of prerequisites includes:

- Autodiscover Server
- .NET Framework
- Operating System
- Windows Management Framework
- Hardware

Icons next to each item in the Prerequisites Checker display the status:

- **Green box with checkmark:** Success
- **Red circle with x:** Error
- **Yellow triangle with exclamation point:** Warning

7 Click the arrow next to any prerequisite to expand the list of items under that prerequisite.

8 Information regarding the status of each prerequisite is displayed to the right of each line item. Any additional information about each prerequisite may be displayed by clicking on a line item and then clicking **View Details** next to the information icon at the top of the screen.

9 Correct any errors prior to installing Migration Manager for PSTs.

Installation Steps

Complete the following steps to run the installation wizard for Migration Manager for PSTs. This section describes how to do a simple installation of all MMP components. For distributed setup guidance and for instructions on installing MMP components from the command line, please see the *Migration Manager for PSTs User Guide*.

1 From the autorun.exe GUI, run the appropriate 32- or 64-bit MSI file and launch the Setup Wizard on the computer you have selected to use for the component(s) you are installing.

2 On the Welcome screen, click **Next** to start the setup process.

3 On the Transaction Product Agreement screen, read the license agreement and then click **I accept the terms of the license agreement**.

4 On the Custom Setup screen, select the MMP components you want to install. For the simple installation, select them all.

- Web Services and Scheduling Agent
- PowerShell Cmdlets
- Discovery Agent
- Migration Agent
- Dell Log Viewer

5 On the Destination Folders screen, in the **Install Dell Migration Manager for PSTs to:** box, use the default directory **C:\Program Files\Dell\Migration Manager for PSTs\,** or click **Change** to select a different directory.

6 On the Ready to install Dell Migration Manager for PSTs screen, click **Install** to begin the installation.

7 On the Installing Dell Migration Manager for PSTs screen, a status is displayed during the installation. Click **Cancel** to cancel the installation.

8 On the Completed the Dell Migration Manager for PSTs Setup Wizard screen, you have the option to launch the Configuration Console to configure MMP on your server. This is the default option. If you wish to finish configuring MMP on your server later, you can uncheck this option. Now click **Finish** to exit the Setup Wizard.

Using the Configuration Console

After you have installed the MMP product files, you can use the Configuration Console to configure MMP. The Configuration Console is an MMP utility that lets you configure MMP with your SQL server and IIS server. You will need to run this at least once on your MMP server. You can run it again later if you need to make changes to your SQL and IIS connections.

You can launch the Configuration Console from the final screen of the installer, or from the Windows Start Menu. The first time you run the Configuration Console, it runs in a wizard mode where you must navigate through all of the configuration screens in order by clicking **Next** after each screen. After you have saved your configuration settings the first time, the Configuration Console runs in a free mode where you can navigate to any screen, configure your settings, and then click **Apply** on the Summary screen to save them.

If you run the Configuration Console again, it displays the previously saved settings.

Welcome

The Welcome screen lists information you need to gather prior to starting your configuration. Review the list and gather the necessary information.

MMP requires a valid DLV license for migration. If you have previously installed using an ASC license, the Welcome screen provides a link to http://license.quest.com/upgrade to obtain a new license.

Website

On the Website screen, enter the following web service connection information. If you are using SSL, make sure that your IIS server has been configured with the necessary certificates.

- **Website address:** The address for the Migration Manager for PSTs website. For example, **wspst01.sitraka.com**
- **Port:** The port for the Migration Manager for PSTs website. If the port number you enter is in use, it cannot be used for website installation. An error message prompts you to select a different port. For example, you may choose **443** if you will select SSL encryption, or **8080** if you want to use an alternate port.
- **Use SSL encryption (https) to connect:** This checkbox is selected by default. This option is recommended, though if you use SSL a valid certificate will need to be installed in IIS for secure communication.
- **Allow use of a self-signed certificate:** Allow use of a user-generated identify certificate.

Once you have entered the Web Site settings, the URL for your MMP website is displayed.

If you have selected the Use SSL option, then the URL to your MMP website will be in the format **https://<web server name>:<port>**. Using the examples above, the URL to the website would be **https://wspst01.sitraka.com:443** or just **https://wspst01.sitraka.com**.

If you have not selected the Use SSL option, then the URL to your MMP website will be in the format **http://<web server name>:<port>**. Using the examples above, the URL to the website would be **http://wspst01.sitraka.com:8080**.

If you wish to copy this URL to the Windows Clipboard, you can do so.

SQL Server

NOTE: If the MMP Web Server is installed on a separate machine from the one running Migration Manager for PSTs, the SQL Server screen will not be displayed in the Configuration Console on the Migration Manager for PSTs server. The SQL Server screen will be displayed when running the Configuration Console on the MMP Web Server machine.

On the SQL Server screen, enter the SQL Server Name and Authentication method for the Migration Manager for PSTs database. The user must have a valid login on the SQL Server and will be assigned correct roles to access the database. These SQL Server credentials do not require system administrator privileges.

- **Server name:** The name of the SQL server to be used for the connection.

If you are using a local SQL Server Express installation, then your Server name is **.\SQLEXPRESS**. If you are connecting to the default instance of a regular SQL Server, then the name could be the fully qualified domain name of the SQL Server or the instance name that can be resolved from your MMP server to the SQL Server instance. For example, **SQLServer01** or **SQLServer01.sitraka.com**.

- **Authentication:** Select either SQL Server Authentication or Windows Authentication.

  Windows Authentication will use the Application Pool Identity credentials from the Migration Manager for PSTs web service.

- **Username:** Only used for SQL Server Authentication. The name of the user account that will be used to connect to the SQL server.
- **Password:** Only used for SQL Server Authentication. The password for the user account that will be used to connect to the SQL server.

Enter credentials that have sysadmin privileges in the section below. These credentials are used for creating, upgrading and assigning database roles during the configuration and are not saved.

- **Authentication:** Select either SQL Server Authentication or Windows Authentication.

Windows Authentication will use the credentials of the currently logged in user. This user must have a valid SQL login with sysadmin privileges on the SQL server.

To give a user SQL **dbcreate** and **sysadmin** privileges on the SQL server, complete the following steps:

1. Open SQL Management Studio.
2. Connect to the SQL Server instance hosting the MMP database.
3. Expand the Security folder in the tree view.
4. Expand the Logins folder in the tree view.
5. Select the user and open their properties.
6. Select the Server Roles option and verify that the **sysadmin** role is checked for the user account that will be used to connect to the SQL server.

NOTE: The user set in the AppPool must have a SQL login. A public role is sufficient. The system administrator credentials are used to add this user to the MMP database with db_owner privileges.

Web Server

Enter credentials for the web service application pool. These credentials will be used to access the database if **Windows Authentication (web service credentials)** was selected on the SQL Server screen.

NOTE: If the MMP Web Server is installed on a separate machine from the one running Migration Manager for PSTs, the Web Server screen will not be displayed in the Configuration Console on the Migration Manager for PSTs server. The Web Server screen will be displayed when running the Configuration Console on the MMP Web Server machine.

- **Username:** The name of the user account that connects to the database if Windows Authentication is used.
- **Password:** The password for the user account that connects to the database if Windows Authentication is used.

Agent

The Agent screen allows you to configure local agents and global migration settings. Enter the following information in the Local Agent Settings section:

- **Agent:** Discovery Agent, Migration Agent, or Schedule Agent.

- **Restore Defaults:** Restore the settings below to their defaults.
- **Poll time (seconds):** The frequency for the agents to look for tasks to run.
- **Task count:** The number of concurrent tasks the agent runs.

  This option is not displayed under the schedule agent.
- **Request Timeout for all agents (milliseconds):** The time before all agents time out.

Sometimes situations occur in which a PST file cannot be migrated at first. A common scenario that occurs is a locked PST file resulting from a user having a PST file open in Outlook. In this case, the PST file will be retried later.

Enter the following information in the Global Migration Agent Settings section:

- **Retry delay (minutes):** The minimum time to wait before the first attempt to retry the PST file migration. The wait time automatically doubles with each retry after the first until the number of retries set in the Retry attempts field is reached.
- **Retry attempts:** The number of retries to attempt before failing the migration.
- **Max Message Size:** Enter the maximum message size allowed for the migration. The default is 10MB.

If the PST file still fails to migrate, the PST file is placed into a failed PST migrations collection. See the Collections for failed PST migrations section.

License

MMP requires a valid DLV license for migration.

- **License File:** Browse to enter a valid license for migration.

If there is an existing license, adding a new license replaces the existing license. You can view the existing license by clicking the information icon at the top right-hand corner of the page and selecting the Licenses tab.

Logging

The Logging screen allows you to select a component and configure its logging settings. Only messages of the selected log level and higher will be logged.

- **Product Component:** From the drop-down list, select **Discovery Agent**, **Migration Agent**, **Schedule Agent**, **Web Service**, or **Windows PowerShell**.
- **Restore Defaults:** This button sets the currently-selected component's log settings to the default settings.
- **Apply to All:** This button applies the settings of the currently-selected component to the rest of the components.

In the Migration Agent Log Settings box, enter the following settings for the selected agent:

- **Log Level:** Select the desired log level from the drop-down list. Log levels include:

All	Info	Error
Verbose	Notice	Fatal
Debug	Warning	Off

- **Maximum size of each log file (MB):** Enter the maximum size for each log file. The default is 25 MB.
- **Number of files to keep:** The maximum number of log files. The default is 10.
- **Error Context Logging:** Select this checkbox to log the context of previous messages leading up to an error, including debug-level messages.

Summary screen

The Summary screen lists the configuration changes that will be made. Click **Finish** to save and apply your configuration settings if this is the first time you have run the Configuration Console and it is operating in wizard mode. Click **Apply** to save and apply your changes if you have run the Configuration Console before. If there is a problem with your configuration settings, the Configuration Console will display a warning.

Configuring the MMP website to use SSL (optional)

To use SSL to encrypt the data exchanged with the MMP website using HTTPS, you will need to obtain and bind a SSL certificate to the MMP website. If you wish to use a self-signed certificate, you can follow these instructions.

1. Open IIS Manager and browse to the server running the MMP website.
2. Open the **Server Certificates** feature for the website in the right panel.
3. Click **Create Self-Signed Certificate** in the **Actions** pane.
    1. Enter a name for your new certificate in the **Specify a friendly name for the certificate** field.
    2. Click **OK** to create the new certificate.
4. Expand the **Sites** tree and select the MMP website, to secure it with the new SSL certificate.
5. Click **Bindings** from the Action panel.
6. Click **Add…** to open the **Add Site Binding** dialog.
    1. Select **https** in the **Type** chooser.
    2. Select **All Unassigned** or the IP address of the MMP website in the **IP Address** field.
    3. Set the **Port** to 443
    4. Select your new SSL certificate in the **SSL Certificate** chooser.
    5. Click **OK** to complete the SSL certificate installation.

Your Migration Manager for PSTs website is now configured to use HTTPS on port 443. On the Website tab of the Configuration Console, make sure that **Allow use of a self-signed certificate** is selected.

Upgrading from a previous version

Upgrading from a previous version is done through the Migration Manager for PSTs installer. There is no need to uninstall the currently-installed version. Your configuration settings are preserved in the new version. You still need to run the Configuration Console to update the database and apply your settings to the MMP website and web server.

To upgrade from a previous version of Migration Manager for PST, complete the following steps:

> **NOTE:** If you selected Windows Authentication, enter your Web Server credentials. The user must have a valid login on the SQL Server and will be assigned correct roles to access the database.

NOTE: If the MMP Web Server is installed on a separate machine from the one running Migration Manager for PSTs, the SQL Server screen and the Web Server screen will not be displayed in the Configuration Console on the Migration Manager for PSTs server. These screens will be displayed when running the Configuration Console on the MMP Web Server machine.

NOTE: When upgrading from a 1.0.3.18 or a prior version only, you must set the configuration logs to their default settings on the Logging screen in the Configuration Console in order for the logs to get advanced logging features. On the Logging screen, select a component and click **Restore Defaults**. Then click **Apply to All**. Then click **Apply** to save the configuration settings to the upgraded version.

1. Run the installation wizard provided for the latest version of Migration Manager for PSTs. Instructions for running the installation wizard are provided in the Installation Steps section of this chapter.
2. Launch the Configuration Console. Configuration settings from your previous installation are loaded in the Configuration Console.

   For information about the Configuration Console, see the Using the Configuration Console section of this chapter.
3. If you selected Windows Authentication to configure the SQL server connection, continue to step 4. If you selected SQL Authentication, continue to step 5.
4. For Windows Authentication, enter credentials on the Web Server screen.
5. It is recommended that you review the configuration settings using the tabs on the left pane of the Configuration Console.
6. Click **Apply** to save the configuration settings to the upgraded version.
7. Exit the Configuration Console.

To configure your upgrade using PowerShell cmdlets, please follow the full example scripts listed in the *Upgrading from a previous version* section of the User Guide.

The Migration Web UI

The Migration Web UI Home page contains the following links for performing the steps of a migration. These links are explained in the sections below. The URL to the MMP website is defined by the choices you made during setup, with specific examples given in the previous section, such as **https://wspst01.sitraka.com**.

Home
Sources
Discover
- Users
- Computers
- PSTs

Collections
Targets
Migrate
Events

Home

The information icon at the top right-hand corner of the home page opens the About box. This box contains the About, Licenses, and Contact tabs.

About

The About contains information about the product version, and other legal information such as trademarks and the copyright.

Licenses

The licenses tab displays information about your migration license, including:

- **License:** The name of the product license.
- **Type:** The type of license purchased. For example, Beta, Term, etc.
- **Expires:** The expiration date for the license.
- **Seats licensed:** The number of seats purchased under the license agreement.
- **Seats used:** The number of seats used under the license agreement.

Licenses can be added or replaced in the Configuration Console. If there is an existing license, adding a new license replaces the existing license.

Contact

The Contact tab displays information for contacting Dell about this product.

Viewing help topics

Each web page displays a help menu that you can click to access help.

- **Help Topics:** This link takes you to Epic, an online system where you can view your product documentation. It provides access to documentation from anywhere, on any internet-enabled device.
- **Search Support Portal and Knowledge Base:** This link takes you to the support Knowledge Base. You can search the Knowledge Base by product or key word. The support portal also provides links to other useful information.
- **Visit the Community:** Communities provide information about specific products such as documents or discussions on particular topics.
- **Check for Updates:** This link takes you to a support page where you can download software updates.

Sources

The Sources link displays connections used to connect to Active Directory. By default, source connections are sorted alphabetically by name. You can change the sort order by clicking the column headings.

New Source

The New Source button contains the following fields:

- **Source name:** The source name for the connection.
- **Admin name:** The name of the administrator account.
- **Password:** The password for the administrator account.

Hiding and unhiding source connections.

Once a source connection is created it cannot be deleted. The source connections can be hidden and unhidden from view as needed.

To hide source connections:

- Click the **Hide** icon ( ) on a source connection to hide it from view.

To view hidden source connections:

- Select the **View Hidden** checkbox above the source connection list.

To unhide hidden source connections:

1. Select the **View Hidden** checkbox above the source connection list to view the hidden source connections.
2. Click the **Unhide** icon ( ) on the hidden source connections you want to unhide.

To view source connections after they are unhidden:

- Deselect the **View Hidden** checkbox to display the unhidden source connections.

Discover

The Discover link is used to create a new discovery task or manage existing discovery tasks. By default, discovery tasks are sorted by last run time. You can change the sort order by clicking the column headings. You can filter the results displayed in the Name, Status, and Last Ran columns.

Discovery results can be exported to a CSV file. This allows you to work with the results in a spreadsheet and create adhoc reports. While not all fields collected from the Active Directory scan are displayed in the Migration Web UI, every field that is collected from the Active Directory scan is output to the CSV file.

You can also export discovery results to a CSV file using PowerShell cmdlets. See the Exporting Discovery Tasks and Events to a CSV File section.

The Discovery link contains the following buttons to create discovery tasks:

- New User Discovery
- New Computer Discovery
- New PST Discovery on Computers
- New PST Discovery on Network Shares

New User Discovery

The Settings tab contains the following fields:

- **Name:** The user discovery task name.
- **Source:** The source connection to use for the discovery task.

Advanced Discovery Filters

- **Containers:** Select containers to restrict the scope of discovery.

The Schedule tab contains the following fields:

- **Run Now:** Start the discovery now.
- **Run Once:** Start the discovery on the specified date and time.
- **Run Recurring:** Start the discovery on the specified days, time, and range of recurrence.

New Computer Discovery

The Settings tab contains the following fields:

- **Name:** The computer discovery task name.
- **Source:** The source connection to use for the discovery task.

Advanced Discovery Filters

- **Containers:** Select containers to restrict the scope of discovery.

The Schedule tab contains the following fields:

- **Run Now:** Start the discovery now.
- **Run Once:** Start the discovery on the specified date and time.
- **Run Recurring:** Start the discovery on the specified days, time, and range of recurrence.

New PST Discovery on Computers

The Settings tab contains the following fields:

- **Name:** The PST file discovery task name.
- **Source:** The source connection to use for the discovery task.
- **Relative path:** The comma-delimited list of paths to the PST files. Leave the field blank to search the entire computer for PST files. This can include drives.
- **Recurse:** Search all directories under the specified path(s) to the PST file.
- **Exclude system files:** Do not search system files.

The Computers tab contains the following fields:

- **Filter available computers:** Filter by name.
- **Filter by OU:** Filter by organization unit from the drop-down list.

The Schedule tab contains the following fields:

- **Run Now:** Start the discovery now.
- **Run Once:** Start the discovery on the specified date and time.
- **Run Recurring:** Start the discovery on the specified days, time, and range of recurrence.

New PST Discovery On Network Shares

The Settings tab contains the following fields:

- **Name:** The PST file discovery task name.
- **Source:** The source connection to use for the discovery task.
- **Relative path:** The comma-delimited list of paths from the network share root. Leave the field blank to search all relative paths.
- **Recurse:** Search all directories under the specified path to the PST file.
- **Exclude system files:** Do not search system files.

The Network Shares tab contains the following fields:

- **Filter available network shares:** Filter by name.

Discovered Items

The Discover link contains the following subpages for: Users • Computers • PSTs

Users

Click this link to view a complete list of the discovered users. By default, users are sorted alphabetically by name. You can change the sort order by clicking the column headings. You can filter results displayed in the Name, Email, Mailbox Enabled, OU, and Discovered columns.

The following information is provided:

- **Name:** The name of the discovered user.
- **Email:** The target email address.
- **Mailbox Enabled:** Indicates whether the user is mailbox enabled.
- **OU:** The organizational unit of the discovered user.
- **Discovered:** The date and time stamp of the discovery.

MMP uses several attributes in Active Directory to determine if a user is mailbox enabled. MMP filters out non mailbox-enabled users from the Collection wizard in the website and in migration tasks. If any of the following Active Directory user attributes are set, MMP considers the user to be mailbox enabled:

- homeMTA
- homeMDB
- msExchHomeServerName
- msExchMailboxGuid

Computers

Click this link to view a complete list of the discovered computers. By default, computers are sorted alphabetically by name. You can change the sort order by clicking the column headings. You can filter the results displayed in the Name, Host, OU, Type, and Discovered columns.

The following information is provided:

- **Name:** The name of the discovered computer.
- **Host:** The host name of the discovered computer.
- **OU:** The organizational unit of the discovered computer.
- **Type:** The computer or network share.
- **Discovered:** The date and time stamp of the discovery.

You can filter results displayed in the Name, Host, OU, Type, and Discovered columns.

Click **New Network Share** to add a network share.

- **Name:** The network share name.
- **Source:** The source connection to access the network share.
- **Path:** The path to the network share.

PSTs

Click this link to view a complete list of the discovered PSTs. By default, PSTs are sorted by discovered time. You can change the sort order by clicking the column headings. You can filter results displayed in the Name, Owner, Location, Path, Size, and Discovered columns.

The following information is provided:

- **Name:** The name of the PST file.
- **Owner:** The name of the person who owns the PST file.

  The owner of a PST file is determined by the Access Control List (ACL) on the source system. To change the owner, follow the instructions below.
- **Location:** The name of the computer or network share on which the PST file was discovered.
- **Path:** The relative path to the computer where the discovered PST is located.
- **Size:** The size of the PST file.
- **Discovered:** The date and time stamp of the discovery.

To change the owner of a PST file, complete the following steps:

1. On the PSTs page, hover over the owner of the PST in the Owner column to activate the Edit icon.
2. Click anywhere in the **Owner** box.
3. In the Owner box, type at least 2 characters of the owner name to display the drop-down list.
4. Select an owner for the PST file from the drop-down list.
5. Repeat this process for each PST owner you wish to change on the web page.

   When the owner of a PST file has been changed, a red marker is displayed by the owner of the PST file.
6. If you have changed the owner of 1 or more PST files, the **Apply Changes** link at the top of the page is activated. Click **Apply Changes** to save your changes. Or, click **Cancel Changes** to remove any changes that you have made to the owners of PST files.

NOTE: Changes to the owner of a particular PST file on a web page must be saved before navigating to another page. If you attempt to navigate off the web page prior to saving your changes, the following message is displayed: You have unsaved changes. Do you want to save your changes before continuing?

You can also change the owner of the PST after discover with the **Set-MMPPstFileOwner** cmdlet.

Collections

The Collections link allows you to create collections of users or one or more PSTs for migration. By default, collections are sorted by alphabetically by name. You can change the sort order by clicking the column headings. You can filter results displayed in the Name, Type, and Label columns.

New User collection

On the Settings tab, enter the following information:

- **Name:** The collection name.
- **Label:** The collection label.

On the Users tab, select the users that you wish to include in the collection and move them to the table on the right.

New PST collection

On the Settings tab, enter the following information:

- **Name:** The collection name. Hover over the Name field to display the UNC path.
- **Label:** The collection label.

On the **PSTs** tab, select the PSTs you wish to include in the collection and move them to the table on the right.

Hiding and unhiding collections.

Once a collection is created it cannot be deleted. Collections can be hidden and unhidden from view as needed.

To hide collections:

- Click the **Hide** icon ( ) on a collection to hide it from view.

To view hidden collections:

- Select the **View Hidden** checkbox above the collection list.

To unhide hidden collections:

1. Select the **View Hidden** checkbox above the collection list to view the hidden collections.
2. Click the **Unhide** icon ( ) on the hidden collections you want to unhide.

To view collections after they are unhidden:

- Deselect the **View Hidden** checkbox to display the unhidden collections.

Collections for failed PST migrations

When situations occur in which a PST file cannot be migrated at first and it meets the retry criteria, the PST will be retried for migration. MMP will attempt to migrate the PST file again based on the number of retries entered in the **Retry attempts** box on the Migration Agent Configuration page in the Configuration Console.If the PST file still fails to migrate, the PST file is placed into a failed PST migrations collection.

To migrate a failed PST migrations collection:

1. Go to the migration task that contains the failed PST file and edit the task.
2. In the **Name** field, rename the task to a unique name. Renaming the original task instead of creating a new task allows you to keep the settings from the original task.
3. Under **Collection**, locate the collection with -failed appended to the name of the original collection that contained the failed PST file.
4. Make sure that the target is set correctly in the **Target** field.
5. Click **Next** and review the previous settings on the **Migration Settings** and **Schedule** tabs and proceed with the migration.

Targets

The Targets link allows you to enter the credentials that you use to connect to the target system. See additional details in the Migration Workflow section below. By default, target connections are sorted by alphabetically by name. You can change the sort order by clicking the column headings.

New Target

The New Target button contains the following fields:

- **Target Name:** The name to use for the target connection.
- **System:** The target system.
    - **Use auto-discovery** (checkbox): Select this checkbox if you want Migration Manager for PSTs to use the target system's auto-discover service to find the target server name (URL). If you leave this checkbox unmarked, you must specify the **Server name/URL** in the next field below.
- **Server name/URL:** The name —or— URL of the target server.
- **Use SSL** (checkbox): Select this checkbox if you want MMP to use SSL for its connections to the target server.
- **Admin name:** The name of the administrator account used to connect to the target.
- **Password:** The password for the administrator account.
- **Add Additional Credential:** Add an additional administrator account to use for the connection.

Hiding and unhiding target connections.

Once a target connection is created it cannot be deleted. The target connections can be hidden and unhidden from view as needed.

To hide target connections:

- Click the **Hide** icon () on a target connection to hide it from view.

To view hidden target connections:

- Select the **View Hidden** checkbox above the target connection list.

To unhide hidden target connections:

1. Select the **View Hidden** checkbox above the target connection list to view the hidden target connections.
2. Click the **Unhide** icon () on the hidden target connections you want to unhide.

To view target connections after they are unhidden:

- Deselect the **View Hidden** checkbox to display the unhidden target connections.

Migrate

The Migrate link allows you to create a new migration task or manage your existing migration tasks. By default, migration tasks are sorted by last run time. You can change the sort order by

clicking the column headings. You can filter the results displayed for the Name, Status, Progress, and Last Ran columns.

New Migration

The New Migration button contains the following fields:

- **Name:** The migration task name.
- **Collection:** The collection to use for the migration task.
- **Target:** The target system to use for the migration.

Details

Click the Details icon for a migration task to view the Details screen. The Details screen displays the list of PSTs contained in the migration task. By default, the PSTs in a migration task are sorted by Name. You can filter the results displayed by Name, Owner, OU, Status, Estimated Percent Complete, or Completed columns. The Status, Estimated Percent Complete, and Completed columns are continuously updated as the PSTs migrate.

The Migration Details section shows live information for the selected PST. This includes statistics on messages, appointments, tasks, and contacts.

It also displays details about the current migration task. This includes information about the PSTs during and after the migration, including the log location and troubleshooting tips. The screen provides the option to export log file to a CSV file.

Events

The Events link takes you to the Events page, which shows the complete list of events generated during discovery and migration. The top of the page displays the number of errors, warnings, and information messages. By default, events are sorted by timestamp. You can change the sort order by clicking the column headings. You can filter results displayed in the Type, Task, Message, Log Location, and Timestamp columns.

The following information is displayed:

- **Type:** The type of event message: error, warning, or information as indicated by the icons.
- **Task:** The task name for which the event is generated.
- **Message:** The event message content.
- **Log Location:** The path for the log file.
- **Timestamp:** The time the event message was generated.

Click on any event to display information about it in the Event details box. A brief synopsis of the event is shown in the box. Click **Details** to display the full message content of the event. The following information is also displayed:

- **Task:** The name of the task for which the event was generated. You can get the task ID by hovering over the task name.
- **Log Location:** Lists the location and name of the log file that contains the event.
- **Troubleshoot:** Click the link to query the Knowledge Base for informational articles about the event message.

Events can be exported to a CSV file from the Migration Web UI. This allows you to work with the results in a spreadsheet and create ad hoc reports.

You can also export events to a CSV file using PowerShell cmdlets. See the Exporting Discovery Tasks and Events to a CSV File section.

Dashboard widgets

The Migration Web UI home page contains widgets that display statistics for the most recent migration of each PST. Widgets are automatically refreshed every 10 minutes and can be manually refreshed by clicking the refresh button. Widgets include the following:

Migration Status

The Migration Status widget displays the status of recent PST migrations:

- **Pending:** Number of the most recent migrations, per PST, waiting to be processed.
- **In Progress:** Number of the most recent migrations, per PST, currently processing.
- **Completed:** Number of the most recent migrations, per PST, that have completed processing.
- **Completed with errors:** Number of the most recent migrations, per PST, that have completed processing, but had errors.
- **Failed:** Number of the most recent migrations, per PST, that could not be processed.
- **Canceled:** Number of the most recent migrations, per PST, that have been stopped.

Migration Progress

The Migration Progress widget shows a snapshot of the PST migration tasks each day for the last 7 days. Hover over the bars to see the migration task count for each date. These counts are not cumulative.

The Migration Progress widget shows the following information about the PST files selected for migration:

- Migrated PSTs
- Warnings
- Errors

Discovery Progress

The Discovery Progress widget shows a snapshot of the new PST files discovered each day for the last 7 days. Hover over the bars to see the discovered PST file count for each date. These counts are not cumulative.

The Discovery Progress widget shows the following information about the PST files:

- Discovered PSTs
- Warnings
- Errors

Events

The Events widget shows the number of events generated and the number of minutes since those events were generated. You can hover over any event to view the details of that event. To view all event messages, click **Show All**.

Migration Statistics

The Migration Statistics widget shows statistics about the migration or migrations to date, including:

- **First Migration Start:** The date and time that the first migration was started.
- **PSTs Migrated:** The number of PST migrations to date.
- **Messages Migrated:** The number of messages migrated to date.
- **Appointments Migrated:** The number of appointments migrated to date.
- **Tasks Migrated:** The number of tasks migrated to date.
- **Contacts Migrated:** The number of contacts migrated to date.
- **Errors:** The number of errors generated during the migration(s).
- **Data Migrated:** The amount of data migrated.
- **Current Rate:** The data migrated per hour for currently active tasks.

Migration History

The Migration History widget shows a series of migration task status snapshots for the last 7 days. Hover over the bars to see the status information for each date. To view the counts for each category, hover over the appropriate color for the category you want to view. Each snapshot is a cumulative status of all migration tasks run to that date.

The Migration History widget shows the following information about the PST files selected for migration:

- Pending: The number of migration tasks that are waiting to be processed.
- **In Progress:** The number of migration tasks currently processing.
- **Completed:** The number of migration tasks that have completed processing.
- **Completed with errors:** The number of migration tasks that have completed processing, but had errors.
- **Failed:** The number of migration tasks that could not be processed.
- **Canceled:** The number of migration tasks that have been stopped.

Other pages

The following pages display useful information about your migration.

Collections Dashboard

You can view the dashboard for a particular collection by completing the following steps:

1 Under **Collections**, find the name of the collection for which you want to view the dashboard.

2 Click **Details** for that collection.

The widgets display the information for the collection you are viewing.

Targets Dashboard

You can view the dashboard for a particular collection by completing the following steps:

1 Under **Targets**, find the name of the target for which you want to view the dashboard.

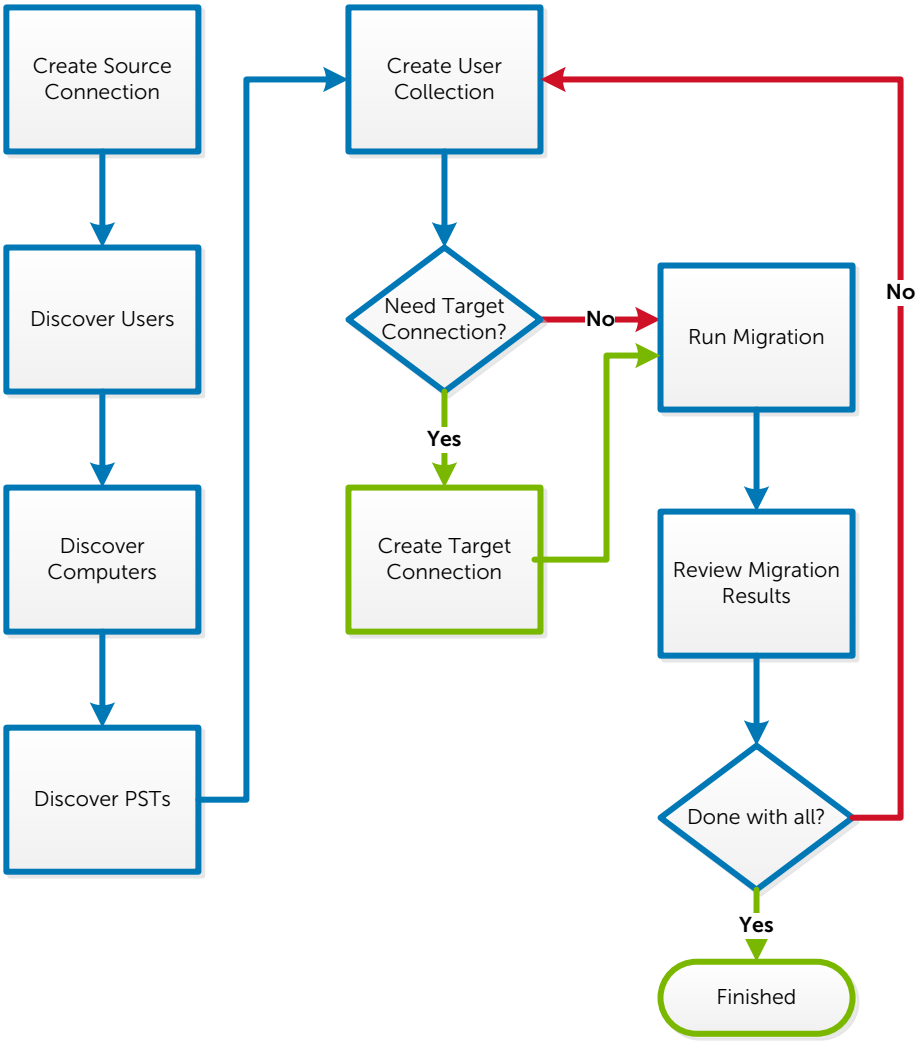
2 Click **Details** for that target.

The widgets display the information for the target you are viewing.

Migration workflow

The following sections provide instructions for performing a simple migration to an Exchange or O365 target system. First, you discover what is available for migration, then you choose what to migrate, then choose where to migrate it, then you migrate the PSTs to their Exchange target or O365 mailboxes. A high-level diagram of the migration project work flow for a simple migration is shown below.

Note that Migration Manager for PSTs does not create mailboxes in Exchange. You must create the mailboxes in Exchange before migrating PSTs.



The following sections, describing the migration using the MMP website and using the MMP PowerShell cmdlets will follow this basic work flow. More details are given in the *Migration Manager for PSTs User Guide*.

Sample GUI Migration Scenario

The following migration scenario shows the steps to migrate to an Exchange or O365 target using the MMP website.

Create a New Source Connection

A "source connection" defines all the information required to successfully connect MMP to a given Active Directory source domain for data retrieval of users, computers and PSTs.

Complete the following steps to define a new connection to a migration source:

1 Click the **Sources** link and then click **New Source**.

2 In the **Source Name** box, enter the desired name for your source connection.

3 In the **Admin Name** box, enter credentials for an Administrator that can open Administrator folder shares and access files and temp directories on any computer, including the migration server, during discovery and migration. The format must be username@domain or domain\username.

4 In the **Password** box, enter the password for the administrator entered in the **Admin Name** box.

5 Once you have entered all of the source information, click the **Test** link in the **Test Connection** box to test the connection to the source domain.

6 If the connection is valid, click **Save**.

7 If needed, repeat the steps above to create multiple source connections.

Create discovery tasks

Complete the following steps to connect to Active Directory to discover users, computers, and PST files to be migrated to mailboxes:

1 Click the **Discover** link and then click **New User Discovery**.

2 On the **Settings** tab in the **Name** box, enter a name for the User Discovery Task Name.

3 In the **Source** box, select the desired source connection.

4 Optionally, in the **Advanced Discovery Filters** section of the screen, select containers to restrict the scope of discovery.

5 On the **Schedule** tab, click a radio button to select the schedule on which to run New User Discovery: **Run Now** or **Run Once** or **Run Recurring**

6 Click **Run** to start new user discovery.

7 Select **Discover/New Computer Discovery**.

8 On the **Settings** tab in the **Name** box, enter a name for the Computer Discovery Task Name.

9 In the **Source** box, select the desired source connection.

10 Optionally, in the **Advanced Discovery Filters** section of the screen, select containers to limit the scope of discovery.

11 On the **Schedule** tab, click the radio button to select the schedule on which to run the Computer Discovery: **Run Now** or **Run Once** or **Run Recurring**

12 Click **Run** to start new computer discovery.

Note: Computer discovery must be completed before running PST discovery.

13 Optionally, add a network share.

14 Click the **Discover/Computers links** and then click **New Network Share**.

15 Enter a network share name.

16 Select a source that has credentials to access the network share from the drop-down list.

17 Enter the path for the network share and optionally add subfolders to refine the directories that can be scanned by this network share.

18 Click **Test** to confirm that the selected credentials can access the network share.

19 Click **Save**.

20 Select **Discover/New PST Discovery**.

21 On the **Settings** tab in the **Name** box, enter the PST discovery task name.

22 In the **Source** box, select the desired source connection.

23 To narrow your search, in the **Relative Path** box, enter the path to search for PSTs. Otherwise, leave this field blank to search the entire computer. The **Relative Path** can be specified as a comma-delimited list of directories that exist under the network share path. Examples of valid relative paths include:

- foldername, foldername, foldername\subfoldername
- foldername\subfoldername

UNC paths are not allowed in the relative path.

24 Under **Search Options**, if you select the **Recurse** checkbox, then MMP will search through subfolders of the paths entered in the **Relative Path** box.

Select the **Exclude system files** checkbox if you want to exclude system files from the network share search.

25 On the **Computers** tab, the **Filter available computers** field allows you to optionally **Filter by computer name** and/or **Filter by an OU**. In the **Filter by Computer name box**, enter a computer name to narrow down the list of computers displayed on the left. This makes it easier to select which ones to move to the right to be searched in that particular PST Discovery task. In the Filter by an OU drop-down list, filter by selecting an organizational unit.

26 On the **Schedule** tab, click the radio button to select the schedule on which to run the PST Discovery: **Run Now** or **Run Once** or **Run Recurring**

27 Click **Run** to start new PST discovery.

As files are discovered, the owner of the PST files is determined by the Access Control List (ACL) on the source system. To change the owner, change the owner in the ACL on the source system and perform discovery again to update it. You can also change the owner of the PST after discovery with the Set-MMPPstFileOwner cmdlet.

Create a new user or PST collection

A collection is a grouping of discovered users or PSTs that MMP can perform migration operations upon. Collections can be made up of users or PSTs from a single source connection, or from multiple source connections.

Note: User discovery must be completed before creating a user collection, and PST discovery must be completed before creating a PST collection.

Complete the following steps to create a collection:

1 Click the **Collections** link and then click **New User Collection** or **New PST Collection**.

2 On the **Settings** tab in the **Name** box, enter a name for the collection.

3 In the **Label** box, enter a descriptive word or phrase for the collection.

4 On the **Users** tab, you can optionally filter by **Name** or **Email**. On the **PSTs** tab, you can optionally filter by **Name** or **Owner**.

5 Select the users or PSTs that you want to include in the collection, move them to the right, and click **Close**.

Create a target connection

A target connection defines all of the information required to successfully connect MMP to a given Exchange target system for data exchange and import.

Complete the following steps to specify how to define a new connection to a migration target:

1. Click the **Targets** link and then click **New Target**.
2. In the **Target Name** box, enter a name for the target system.
3. In the **System** drop-down list, select **Exchange 2016**, **Exchange 2013**, **Exchange 2010**, or **O365**.
4. In the **Admin name** box, enter the administrator name with rights to connect to all of the target mailboxes that will be used for migration. The format must be username@domain or domain\username.
5. In the **Password** box, enter the password for the Admin name you entered above.
6. To work around Exchange and O365 limits on concurrent connections, you can use the **Add Additional Credential** box to specify additional accounts to be used for migration
7. Once you have entered all of the target information, enter the name of a target mailbox that you will be migrating to and click the **Test** link in the **Test Connection** box to test the connection.
8. Click **Save**.

Create a migration task

Complete the following steps to create a new migration task:

1. Click the **Migration** link and then click **New Migration**.
2. On the **Task Settings** tab in the **Name** box, enter a name for the migration task.
3. In the **Collection** box, select the name for the collection of users for which you will migrate PSTs.
4. In the **Target** box, select the name of the target connection you set up to connect to target mailboxes.
5. On the **Migration Settings** tab, select the destination:
    - **Migrate to Primary:** Migrate PSTs to users' primary mailboxes.
    - **Migrate to Archive:** Migrate PSTs to an archive.
    - **Migrate to Subfolder:** Migrate PSTs to a subfolder of users' primary mailboxes or archive.

    Then, select the checkboxes next to the items you intend to migrate:
    - Email
    - Contacts
    - Calendar
    - Tasks

    If you select email, also select the following options:

    Date Range:
    - All email
    - Last modified date

    To increase migration performance:
    - Exclude Deleted Items
    - Exclude Junk Mail

- Exclude Sent Mail

Exclude specific folders:

- Enter folder names to exclude, separated by commas.

6 On the **Schedule** tab, select the schedule to run the migration(s): **Run Now** or **Run Once** or **Run Recurring**

7 Click **Run** to start the migration task.

PowerShell command-line interface

The following migration scenario shows the steps to migrate to an Exchange 2013 target using a PowerShell command-line interface. To view a list of the available MMP commands, enter the following command:

```
Get-Command -Module PSTMigratorModules
```

Sample PowerShell migration scenario

To complete a PST migration using the PowerShell command-line interface, complete the following steps:

1 Import the PowerShell modules.

```
Import-Module PSTMigratorModules
```

2 Create a connection to an Active Directory source and add it to the MMP database.

```
$SourceName = 'My Active Directory Source'
$SourceConnection = New-MMPConnection -Name $SourceName
$SourceConnection = Add-MMPConnection -InputObject $SourceConnection
```

3 Create credentials and assign them to the source connection:

```
$SourceCredentials = New-MMPCredential -ConnectionId
$SourceConnection.Id -Credentials (Get-Credential)
$SourceCredentials = Add-MMPCredential -InputObject $SourceCredentials
```

4 Discover users for the source and view the results. Get-MMPDiscoveredUser will not return results until the discovery has completed.

```
Start-MMPUserDiscoveryTask -Name 'My User Discovery' -SourceConnectionId
$SourceConnection.Id
Get-MMPDiscoveredUser
```

5 Discover computers for the source and view the results. Get-MMPDiscoveredComputer will not return results until the discovery has completed.

```
Start-MMPComputerDiscoveryTask -Name 'My Computer Discovery'
   -SourceConnectionId $SourceConnection.Id
Get-MMPDiscoveredComputer
```

6 Discovery PST files on all computers in the MMP database and view the results. Get-MMPDiscoveredFile will not return results until the discovery has completed.

```
$ComputersToSearch = Get-MMPDiscoveredComputer
Start-MMPPstFileDiscoveryTask -Name 'My PST Discovery'
   -SourceConnectionId $SourceConnection.Id -Computers
$ComputersToSearch
Get-MMPDiscoveredPstFile
```

7 Create a collection and add it to the MMP database.

A collection is a grouping of discovered users or PSTs that MMP can perform migration operations upon. Collections can be made up of users or PSTs from a single source connection, or from multiple source connections. The default is to create a user collection Discovery must be completed before creating a collection.

To create a user collection:

```
$CollectionName = 'My User Collection'
$CollectionLabel = 'MMP'
$UserCollection = New-MMPCollection -Name $CollectionName -Label
$CollectionLabel
$UserCollection = Add-MMPCollection -InputObject $UserCollection
$User1 = Get-MMPDiscoveredUser | Where Object {$_.Name -eq 'John Smith'}
Add-MMPCollectionMember -User $User1 -Collection $UserCollection
```

To create a PST file collection:

```
$CollectionName = 'My PST Collection'
$CollectionLabel = 'MMP'
$FileCollection = New-MMPCollection -Name $CollectionName -Label
   -CollectionType PSTFile $CollectionLabel
$FileCollection = Add-MMPCollection -InputObject $FileCollection
$PstFile1 = Get-MMPDiscoveredPSTFile | Where Object {$_.Name -eq 'Inbox'}
Add-MMPCollectionMember -PstFile $PstFile1 -Collection $FileCollection
```

8 Assign discovered users or PSTs to the collection. User collections and PST file collections are mutually exclusive. If you attempt to add a PST file to a user collection or vice versa, an error is generated.

```
$UserCollection = Get-MMPCollection | Where-Object {$_.Name -eq 'user
collection name'}
Add-MMPCollectionMember -User $User1 -Collection $UserCollection
$FileCollection = Get-MMPCollection | Where-Object {$_.Name -eq 'file
collection name'}
Add-MMPCollectionMember -PstFile $PstFile1 -Collection $FileCollection
```

9 Create a connection to the Exchange 2013 target and add it to the MMP database.

```
$TargetName = "My Exchange 2013 Target"
$TargetUrl = "Exchange2013.sitraka.com"
$TargetKind = Exchange2013
$TargetConnection = New-MMPConnection -TargetConnection -Name
$TargetName -EwsUrl $TargetUrl -ServerKind $TargetKind
$TargetConnection = Add-MMPConnection -InputObject $TargetConnection
```

10 Create credentials and assign them to the target connection.

```
$TargetCredentials = New-MMPCredential -ConnectionId
$TargetConnection.Id -Credentials (Get-Credential)
$TargetCredentials = Add-MMPCredential -InputObject $TargetCredentials
```

11 Queue a migration task for processing by the MMP agents.

```
$MigrationName = "My Migration"
Start-MMPMigrationTask -Name $MigrationName -CollectionId $Collection.id
   -SourceConnectionId $SourceConnection.Id -TargetConnectionId
$TargetConnection.Id -MigrateToSubfolder -MigrateEmail -MigrateCalendar
   -MigrateTasks -MigrateContacts -MigrateToArchive
```

12 View the status of the migration task and its subtasks.

```
Get-MMPTask | Where-Object {$_.Name -eq $MigrationName}
   $MigrationTask = Get-MMPTask | Where-Object {$_.Name -eq
$MigrationName}
```

13 Stop a Migration

```
Stop-MMPMigrationTask -Id $MigrationTask.Id
Get-MMPTask -Id $MigrationTask.Id -Detailed
```

14 Check current license usage.

```
Get-MMPLicense
```

Upload a new license:

```
Add-MMPLicense -Filename '\\server02.sitraka.com\share\license.asc'
```

Viewing events with PowerShell

Events can be viewed in the log files, or enter the following command:

```
Get-MMPEvent
```

Exporting Discovery Tasks and Events to a CSV File

Any of the following results can be exported to a CSV file. This allows you to work with the results in a spreadsheet and create adhoc reports.

- Get-MMPDiscoveredUser
- Get-MMPDiscoveredPstFile
- Get-MMPDiscoveredComputer
- Get-MMPEvent

For example, to export events to a CSV file, use the following command:

```
Get-MMPEvent | Export-Csv -Path C:\example.csv
```

2

Pre-migration Checklist

Prior to performing the migration, administrators need to gather information about the source and target systems used in the migration. The checklist below provides a guide to gathering that information. If needed, print out this form and fill in the information.

What user account will install the product?

The installing user must have permission to create a website and SQL database (SQL Server Authentication may be used to create the database).

Is a supported version of Windows Server installed on the migration server?

See the System Requirements section for supported versions.

Is a supported version of Exchange installed on the target server?

See the System Requirements section for supported versions.

Is a supported version of .NET Framework installed on the migration server?

See the System Requirements section for supported versions.

Is a supported version of PowerShell installed on the migration server?

See the System Requirements section for supported versions.

What is the SQL Server name?

During installation you will need the name of the SQL server to install the MMP database.

Is a supported version of SQL Server installed on the migration server?

See the System Requirements section for supported versions.

Is a supported version of IIS installed on the server?

See the System Requirements section for supported versions.

What is the IIS web server name?

If you are using SSL, it must match the certificate.

Do you have Windows Authentication enabled in IIS?

Do you have ASP.NET enabled in IIS?

Do you know which port you will use to host the website for MMP?

This port may not be in use at the time of installation.

It is recommended that you use SSL on the website. Do you have a certificate? Self-signed or third party are accepted.
Is a supported browser installed on the computer that will be used to view the Migration Manager for PSTs website? See the System Requirements section for supported versions.
What user will be used to view the MMP website and/or run the PowerShell cmdlets? The user must have permissions to access the IIS default folders.
What is the FQDN of your Domain Controller? This will be used to gather user and computer data for PST discovery when creating a source connection.
What account will you use to set up a source connection to Active Directory? This account must be able to query Active Directory as well as access to the administrative shares on any PCs where PSTs will be discovered.
What is the name of your Exchange server, on premises or O365? This server will be used to create a target connection to connect and perform the migration (if configured autodiscover may be used if this in unknown).
What user account will be used to perform the migration? This account needs the Application Impersonation Role in order to place mail in user's mailboxes.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

For sales or other inquiries, visit http://software.dell.com/company/contact-us.aspx or call 1-949-754-8000.

Technical Support Resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.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. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to http://software.dell.com/trials.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer

Third-Party Contributions

This product contains some third-party components (listed below). Copies of their licenses may be found by referencing http://software.dell.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.dell.com.

Table 1. List of third-party contributions

Component	License or Acknowledgment
AlphaFS 2.0.1	MIT License
Angular.js 1.2.16	MIT License
AutoMapper 3.2.1	MIT License
Backbone.js 1.0.0	MIT License
Common.Logging 2.1.2	Apache 2.0 License
Google APIs Client Library for .NET 1.8.2	Apache 2.0 License
Google Data API SDK (1.8.0.0) Setup 1.8	Apache 2.0 License
Google Data API SDK (2.2.0.0) Setup 2.2.0.0	Apache 2.0 License
JQuery 1.7.1	MIT License
JQuery 1.8.2	MIT License
JQuery 2.1.0	MIT License
JQuery Form 3.46	MIT License
jQuery-Placeholder 2.0.7	MIT License
Json.net 6.0.8	MIT License
Log4Net 2.0.3	Apache 2.0 License
Moment.js 2.6.0	MIT License
Newtonsoft.Json.dll 6.0.5	MIT License
Newtonsoft.Json.dll 6.0.8	MIT License
Quartz.NET 2.2.3	Apache 2.0 License
RestSharp 105.0.1	Apache 2.0 License
RestSharp 105.2.3	Apache 2.0 License
Select2 3.4.8	Apache 2.0 License
spin.js 1.2.4	MIT License
Twitter Bootstrap 2.1.1	Apache 2.0 License
Twitter Bootstrap 2.3.1	Apache 2.0 License
Underscore.js 1.5.1	MIT License
Underscore.string 2.3.0	MIT License
WebGrease 1.3	Apache 2.0 License
ZimbraCSharpClient 5.0.96.0	Mozilla Public License (MPL) 1.1