Quest

Binary Tree Migrator Pro for Exchange 20.11.1

Installation and Configuration Guide

© 2023 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

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

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

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are 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.

Binary Tree Migrator Pro for Exchange 20.11.1 – Installation and Configuration Guide
Updated – November 2023
Version – 20.11.1

Table of Contents

1. Introduction 4
1.1 Purpose 4
1.2 Audience 4
1.3 Getting More Information 4
1.4 About Migrator Pro for Exchange 4

2. Installing Migrator Pro for Exchange 5
2.1 Upgrading Migrator Pro for Exchange from an Earlier Version 5
2.2 Necessary Pre-Installation Preparations 5
2.3 Migrator Pro for Exchange *Default Installation* 8
2.4 Migrator Pro for Exchange *Advanced Installation* or *Upgrade* 11
2.5 Uninstalling Migrator Pro for Exchange 17

3. Configuring Migrator Pro for Exchange 18
3.1 Defining an Office 365 (Tenant) Target Forest 19
3.2 Defining a Local Exchange Target Forest 21

4. Installing Migrator Pro for Exchange Public Folder Workers 25

5. Components of Migrator Pro for Exchange 28
5.1 MCP Windows Service 28
5.2 Admin Portal 28
5.3 User Portal 29

6. Introduction to the Admin Portal 30

Appendix A. STIG Environments 32
SQL Express 32
Additional Information 32

Appendix B. Deployment in FIPS Environment 33
Cryptographic usage 33
Background 33
Prerequisites 34
Installation and operation 34
References 35

1. Introduction

1.1 Purpose

The purpose of this document is to provide information on how to get started using Binary Tree Migrator Pro for Exchange including prerequisites, installation and configuration instructions, and an introduction to the Admin Portal.

1.2 Audience

This document assumes the reader has some experience using Microsoft Exchange and some basic Administration skills. If Outlook Client and Exchange Administration topics mentioned in this document are not understood, please reference the Microsoft Outlook and Exchange System Administration documentation.

1.3 Getting More Information

The Migrator Pro for Exchange *User Guide* provides information on how to use Binary Tree Migrator Pro for Exchange to perform a migration from Microsoft to Microsoft Exchange or Microsoft Office 365 Exchange Online.

For additional resources, refer to Support: https://support.quest.com

1.4 About Migrator Pro for Exchange

Migrator Pro for Exchange enables migration from one version of Microsoft Exchange to another. It combines a backend policy engine with front-end management components, which give project managers and administrators more control across their Exchange upgrades.

Key Features and Functions

- The workflow engine allows administrators to create migration tasks, select objects, schedule jobs, and provide user self-service.
- The unified console enables flexible filtering and selection of mailbox objects.
- Content included in the mailbox is moved in one transaction, therefore mailbox security and permissions (delegates) are retained.
- Reports on object state and migration status feed into the console to reduce the effort required to create tasks.
- Does not require server hosted agents for any of its functionality.
- Public Folder migration support for Exchange 2003, Exchange 2007, Exchange 2010, Exchange 2013, Exchange 2016, and Office 365.
- Support for migrations to Office 365, resource forest migrations, and Outlook 2003 profile updates.

2. Installing Migrator Pro for Exchange

This section provides information for:

- Upgrading Migrator Pro for Exchange from an Earlier Version
- Necessary Pre-Installation Preparations
- Migrator Pro for Exchange *Default Installation*
- Migrator Pro for Exchange *Advanced Installation* or *Upgrade*
- Uninstalling Migrator Pro for Exchange

2.1 Upgrading Migrator Pro for Exchange from an Earlier Version

Migrator Pro for Exchange can be easily upgraded to a newer version by running the installation wizard for the new release. The wizard will detect any previous version and offer you the option to upgrade. The previously existing SQL database and configuration settings are preserved when upgrading.

Migrator Pro for Exchange provides a direct upgrade path only from its most recent prior GA version (and any subsequent minor releases). If you want to upgrade from an earlier version, we recommend incremental upgrades, one version at a time.

If the Migrator Pro for Exchange Installer detects a previous version of Migrator Pro for Exchange, it will skip the screen that offers the *Default Installation* option (as described in section 2.3 below), and will perform an upgrade using the *Advanced Installation* (as described in section 2.4 below).

Even if a prior Migrator Pro for Exchange version has been uninstalled, the Installer will still perform the installation as an upgrade (by an Advanced *Installation*) if it finds this entry remaining in the Windows registry:

HK_Local_Machine\Software\Binary Tree\E2E

If you have uninstalled a prior Migrator Pro for Exchange version and now want to run the *Default Installation* option for the new version, you must first remove that entry from the registry.

2.2 Necessary Pre-Installation Preparations

The Migrator Pro for Exchange server should be installed in one of the following locations:

- For Intra-org (same forest) or Office 365 installations the Migrator Pro for Exchange server should be installed in the Source forest.
- For Inter-org (cross forest) migrations, the Migrator Pro for Exchange server should be installed in the Target forest.
- For migrations to an Exchange resource forest, the Migrator Pro for Exchange server should be installed in the resource forest.

Prior to installing Migrator Pro for Exchange, you need to identify the primary Exchange 2010 and/or Exchange 2013 servers utilized as the PowerShell hosts.

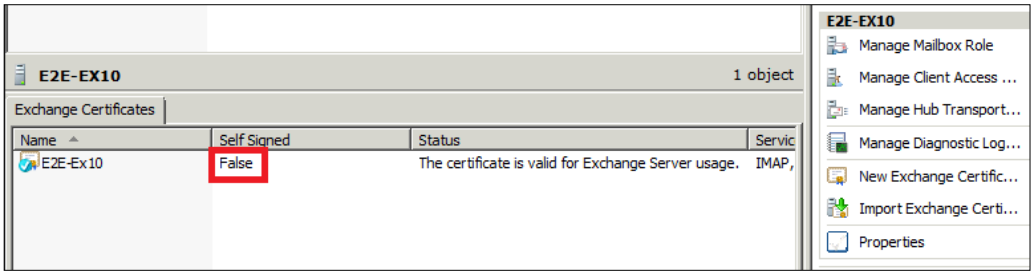
Note also that Outlook must be installed on the Migrator Pro for Exchange server to facilitate MAPI transport for migrations. See the Migrator Pro for Exchange *Requirements* document for supported versions and other relevant notes.

NOTE !

Migrator Pro for Exchange supports either non-SSL or SSL mode for the PowerShell provider. If you want to utilize non-SSL, then no further action is required; however, if you want to utilize SSL mode for the PowerShell provider, you must make sure that the Migrator Pro for Exchange system trusts the certificate on your Exchange server.

Migrator Pro for Exchange requires a non-self-signed certificate on the Exchange 2010 and/or 2013 servers that will host PowerShell. This can be a public certificate (i.e., VeriSign) or a private certificate (i.e. Windows Certificate Services). The PowerShell host servers need not also be a Client Access Server (CAS) host.

The image below displays the Exchange Certificates in Exchange 2010. The interface in other versions of Exchange is different.



It is recommended that the PowerShell host servers be under-utilized servers, so that any additional load on the production Exchange server can be avoided.

Note also that your remote PowerShell connection will require port 5985 be open for http, and port 5986 for https.

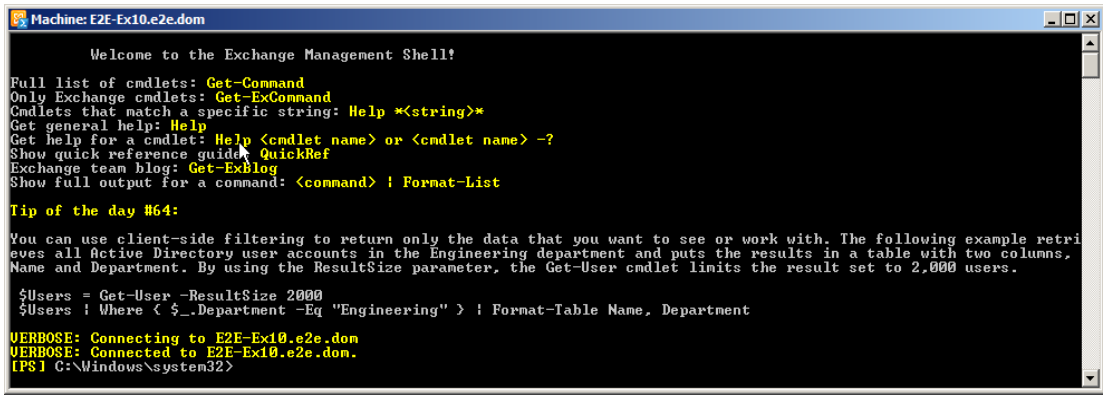
Once the PowerShell machine is identified, perform the following prerequisite PowerShell commands. This applies to both SSL and non-SSL modes.

To execute these commands, launch the Exchange Management Shell:

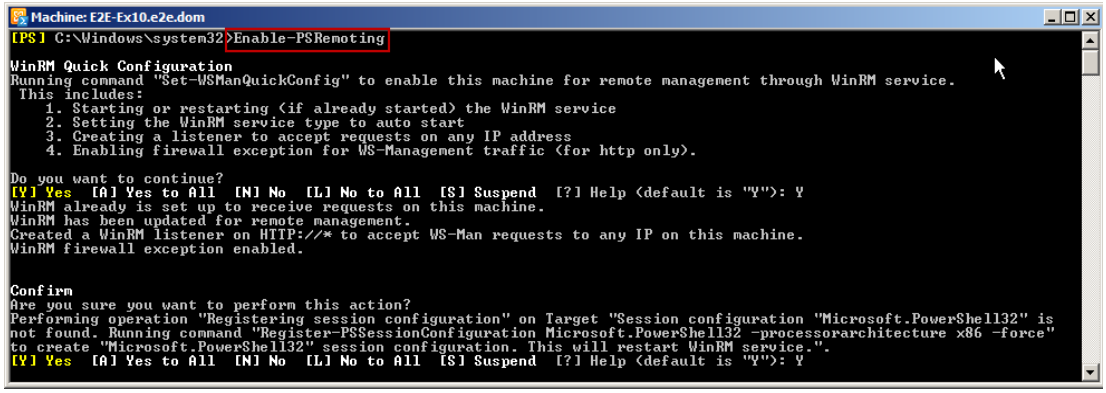
1. Click Start, and then point to All Programs. Expand Microsoft Exchange Server 2010 (shown in the image below), Microsoft Exchange Server 2013, or Microsoft Exchange Server 2016 and then click Exchange Management Shell.
2. In the Exchange Management Shell window, execute the following command:

   Enable-PSRemoting

   This command configures the machine on which it is run, to receive Windows PowerShell remote commands.



3. Press <***Y***> to continue.
4. Press <***Y***> again to confirm.

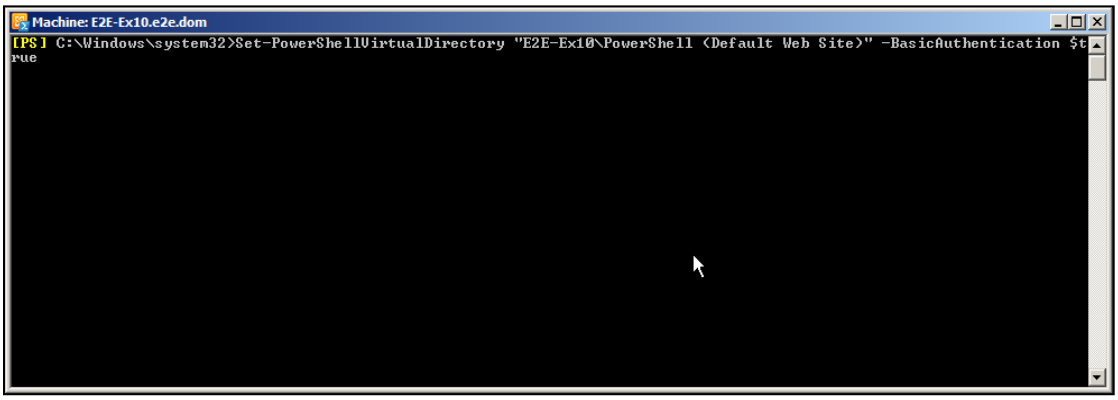


5. The next command lets you authenticate against the server being used as the remote PowerShell host server:

   Set-PowerShellVirtualDirectory "<Exchange Server name>\PowerShell (Default Web Site)" –BasicAuthentication $true

   If using non-SSL mode, Windows Authentication should also be enabled using this command that includes the additional Windows Authentication command:

   Set-PowerShellVirtualDirectory "<Exchange Server name>\PowerShell (Default Web Site)" –BasicAuthentication $true-WindowsAuthentication $true



When the command is executed, even though it configures the system for basic authentication, all the data, including passwords, are encrypted using SSL.

Default Installation vs. Advanced Installation

Migrator Pro for Exchange is installed by an Installation wizard. The Installation wizard offers you a choice of two installation types:

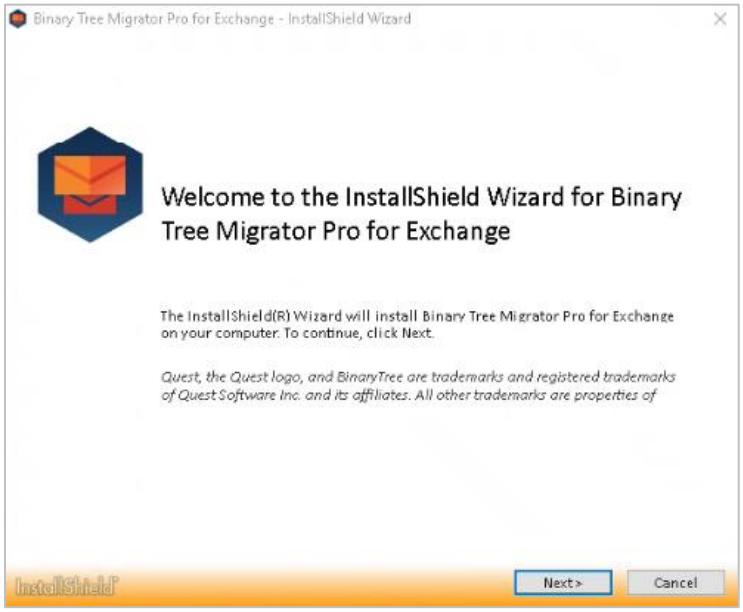
- **Default Installation:** The wizard will scan your environment to determine the information necessary for installation, and then will install according to those specifications. This option will automatically install SQL Express if no SQL server is detected on the local machine.
- **Advanced Installation:** The wizard will lead you through a series of screens for you to specify where you want to install Migrator Pro for Exchange, and the names, locations, and access credentials for certain network and program components, and will then perform the installation to those specifications.

The *Default Installation* option will suit most organizations. The *Advanced Installation* will be appropriate if you want to specify particular components other than those the wizard would find and use by default. The two options are described separately in the next two sections below.

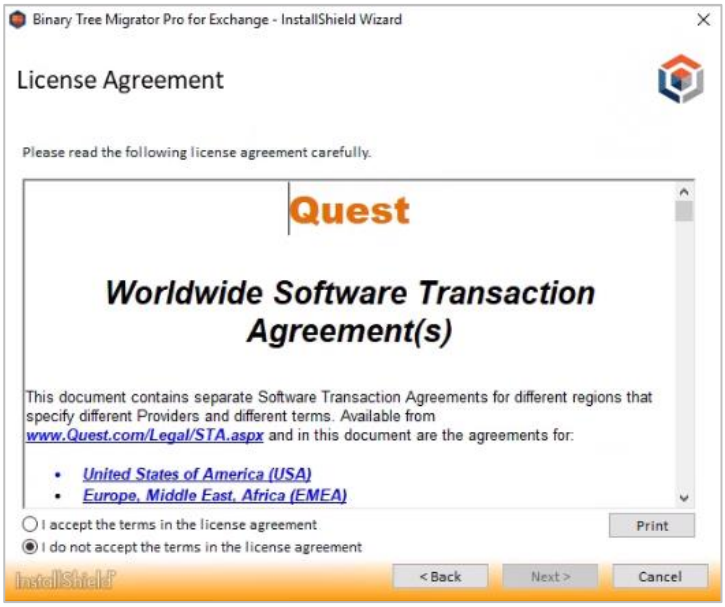
2.3 Migrator Pro for Exchange *Default Installation*

To run the *Default Installation* option in the Installation wizard:

1. Once the PowerShell commands are successfully executed, navigate to the folder where you saved the Migrator Pro for Exchange Installation files, then right-click on the *Migrator Pro for Exchange Install* file and select to **Run as Administrator**.
2. Click **Run** on the security warning, and then click **Next** on the *Welcome* screen:



3. The wizard then prompts you to review and accept the Migrator Pro for Exchange license and maintenance agreement. To accept the agreement, select the **I accept…** radio button and click **Next**.



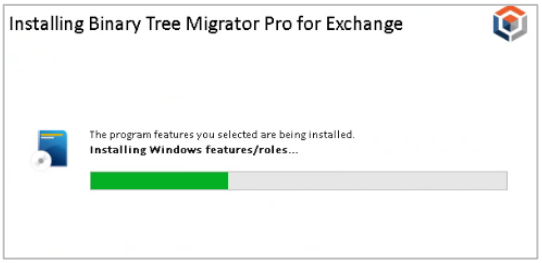
4. If you accept the license terms the wizard then prompts you to choose between **Default Installation** and **Advanced Installation**. Click on the **Default Installation** option.

If the Migrator Pro for Exchange Installer detects a previous version of Migrator Pro for Exchange, it will skip this screen that offers the *Default Installation* option, and will perform an upgrade using the *Advanced Installation* process. Even if a prior Migrator Pro for Exchange version has been uninstalled, the Installer will still perform the installation as an upgrade (by an *Advanced Installation*) if it finds this entry remaining in the Windows registry:

HK_Local_Machine\Software\Binary Tree\E2E

If you have uninstalled a prior Migrator Pro for Exchange version and now want to run the *Default Installation* option for the new version, you must first remove that entry from the registry.

The wizard then scans your environment to gather the information it needs, and to determine whether you need to install any of several required accessory applications. A progress meter shows the wizard's progress:



These accessory components are required for the Migrator Pro for Exchange installation:

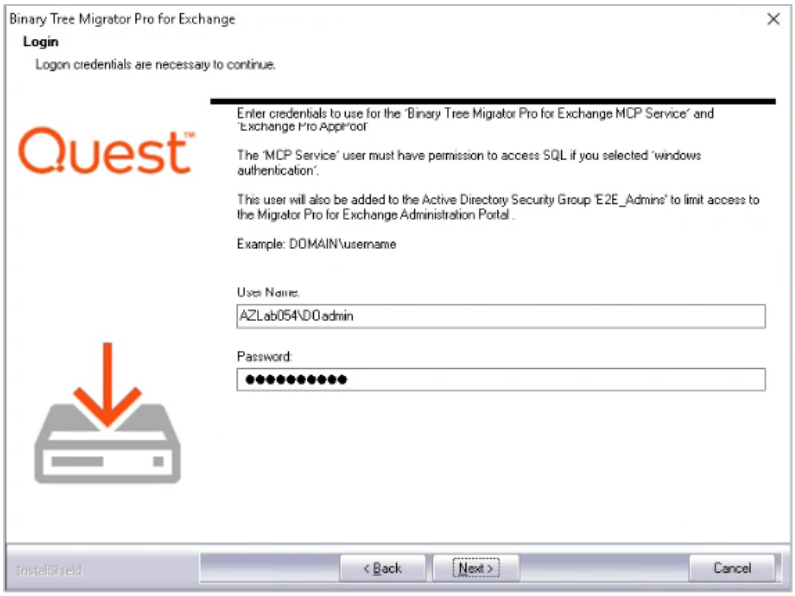
- Windows features IIS and .NET Framework 4.8 full

- SQL Server 2017 Express
    - [local]\SQLEXPRESS installs as a named instance using the format *servername\SQLExpress*
    - Installs in Mixed mode with install account as SA, and local SA password is *Password1*
- Microsoft Online Sign-on assistant
- Azure AD PowerShell module

If you already have these accessory apps installed, you can just skip ahead to the next step below. Otherwise, the Migrator Pro for Exchange installer will prompt you to authorize the installation of the ones you need. In that case, click the **Install** button to accept. If you have to install Microsoft .NET 4.8 Framework, you may also be prompted to accept Microsoft's license agreement. If so, mark the checkbox for **I have read and accept…**, and click **Install**.

The installation of accessory applications may take several minutes. Some of the newly installed components may then require a system reboot, in which case the wizard will also prompt you to authorize the reboot. Click **Yes** to authorize the reboot. If you do have to reboot, the wizard will automatically resume at the next screen in this process (next step below).

5. The wizard then prompts you for the login credentials Migrator Pro for Exchange should use for its MCP Service and the Migrator Pro for Exchange AppPool. Enter the credentials and click **Next**.



The installation resumes when you click **Next**, and a progress meter shows the progress, and notifies you when the installation is complete:

6. Click the **Finish** button to close this portion of the wizard. Another progress meter shows the process progress through this last phase of the installation, and the wizard then notifies you when the process is complete:
7. Click this **Finish** button to close the Migrator Pro for Exchange Installer.

Now that the physical installation is complete, see section 3 below to configure Migrator Pro for Exchange for your environment and purposes. The first time you run the Migrator Pro for Exchange Admin Portal after this installation, Migrator Pro for Exchange will prompt you to define your target forest.

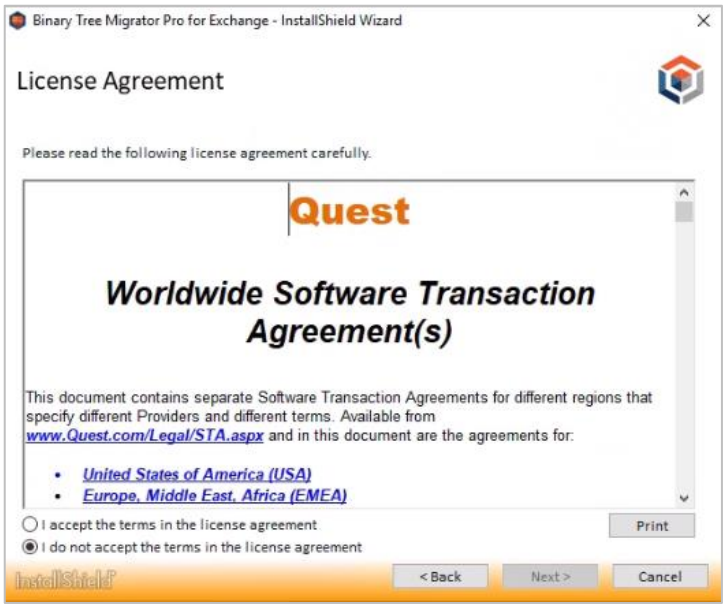
2.4 Migrator Pro for Exchange *Advanced Installation* or *Upgrade*

To run the *Advanced Installation* option in the Installation wizard (for either a fresh installation or an upgrade):

1. Once the PowerShell commands are successfully executed, navigate to the folder where you saved the Migrator Pro for Exchange Installation files, then right-click on the *Migrator Pro for Exchange Install* file and select to **Run as Administrator**.

2. Click **Run** on the security warning, and then click **Next** on the *Welcome* screen:

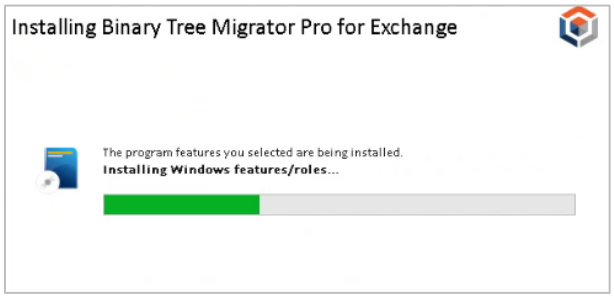
3. The wizard then prompts you to review and accept the Migrator Pro for Exchange license and maintenance agreement. To accept the agreement, select the **I accept…** radio button and click **Next**.



4. If you accept the license terms the next prompt asks you to choose between **Default Installation** and **Advanced Installation**. Click on the **Advanced Installation** option.

If the Migrator Pro for Exchange Installer detects a previous version of Migrator Pro for Exchange, it will skip this screen that offers the *Default Installation* option, and will perform an upgrade using the *Advanced Installation* process.

The wizard then scans your environment to gather the information it needs for installation, and to determine whether you also need to install any required accessory applications. A progress meter shows the progress:



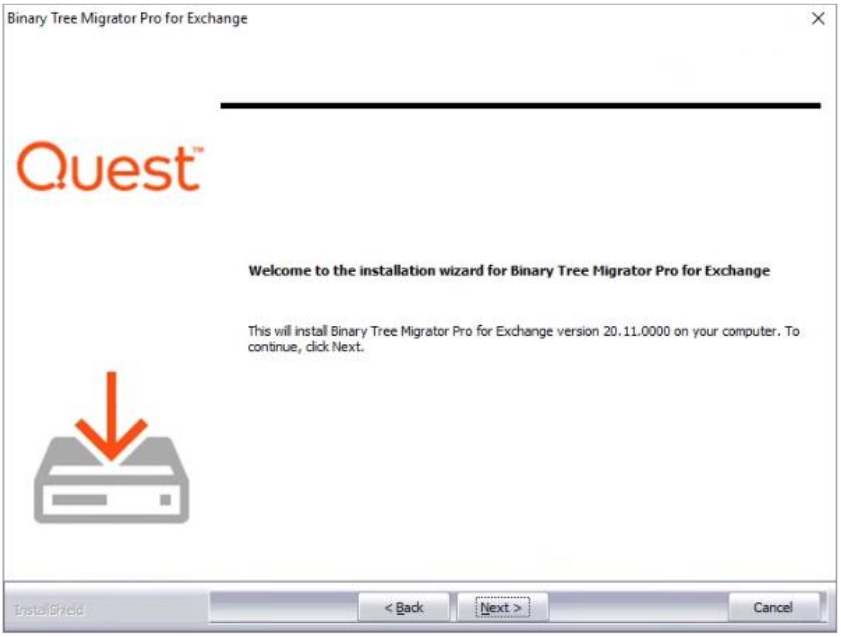
These accessory components are required for the Migrator Pro for Exchange installation:

- Windows features IIS and .NET Framework 4.8 full
- Microsoft Online Sign-on assistant
- Azure AD PowerShell module

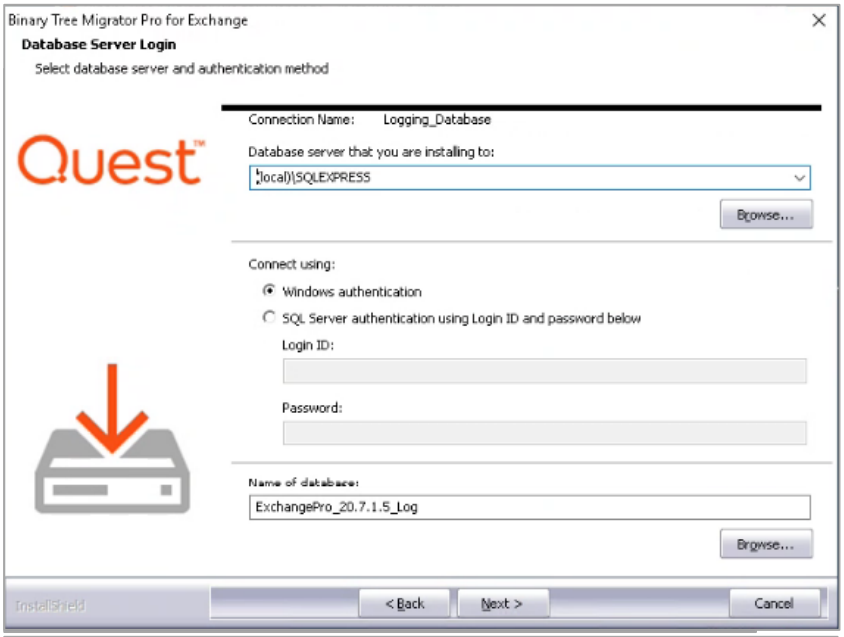
If you already have these accessory apps installed, you can just skip ahead to the next step below. Otherwise, the Migrator Pro for Exchange installer will prompt you to authorize the installation of the ones you need. In that case, click the **Install** button to accept. If you have to install Microsoft .NET 4.8 Framework, you may also be prompted to accept Microsoft's license agreement. If so, mark the checkbox for **I have read and accept…**, and click **Install**.

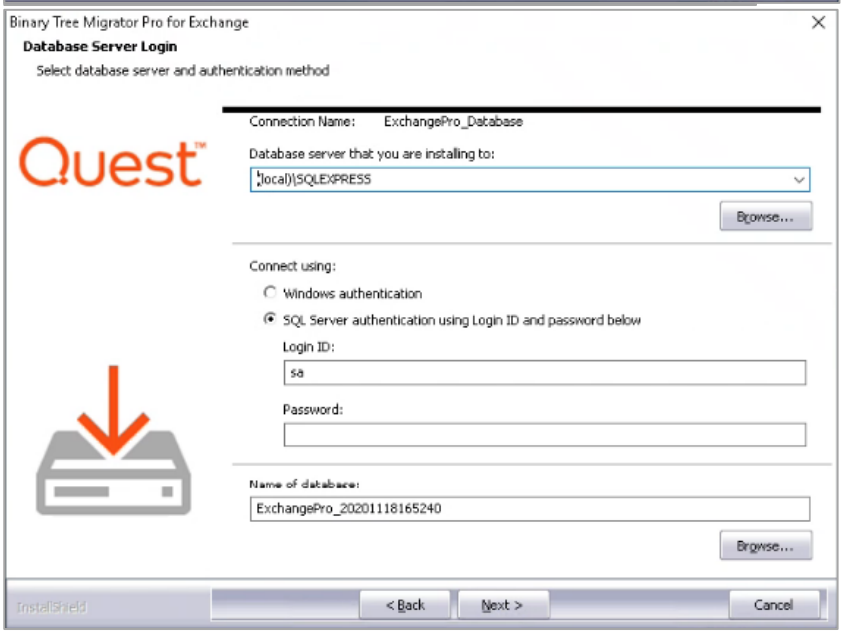
The installation of accessory applications may take several minutes. Some of the newly installed components may then require a system reboot, in which case the wizard will also prompt you to authorize the reboot. Click **Yes** to authorize the reboot. If you do have to reboot, the wizard will automatically resume at the next screen in this process (next step below).

5. On the installation wizard *Welcome* screen, click **Next**.



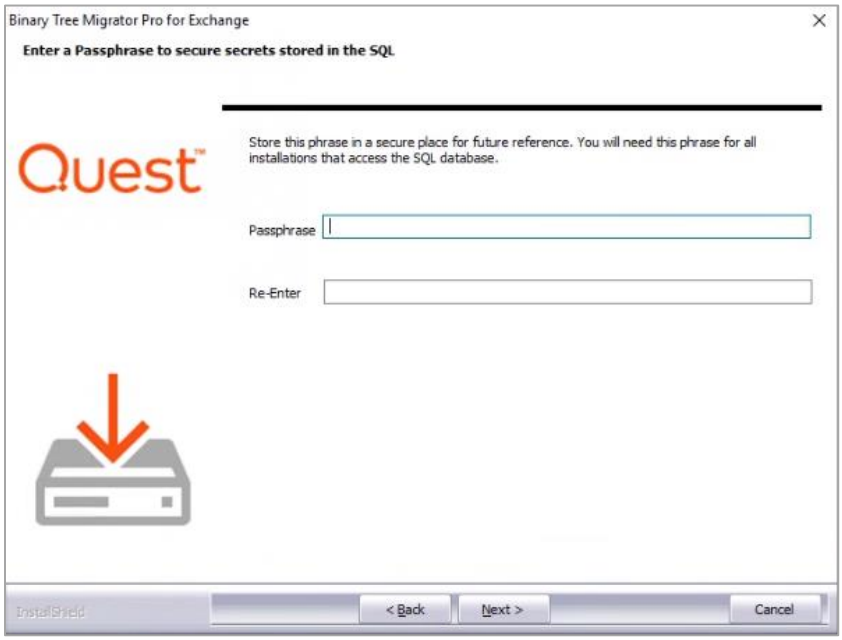
6. On the *Destination Location* screen, select the destination folder for the installation and then click **Next**.
7. On the *Database Server Login* screen, select or browse to the Migrator Pro for Exchange database server you are installing to, select the connection authentication method, and enter the **Name of database** (or **Browse** to it and select it). Then click **Next**.
8. The *Database Server Login* screen appears again, this time for the Migrator Pro for Exchange Logging Database. Select or browse to the logging database server you are installing to, select the connection authentication method, and enter the **Name of database** (or **Browse** to it and select it).



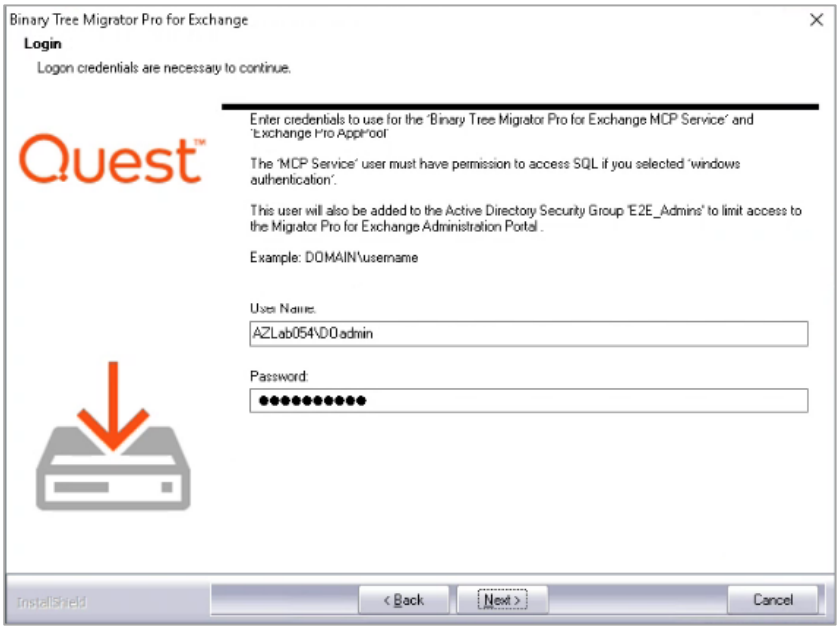


Then click **Next**.

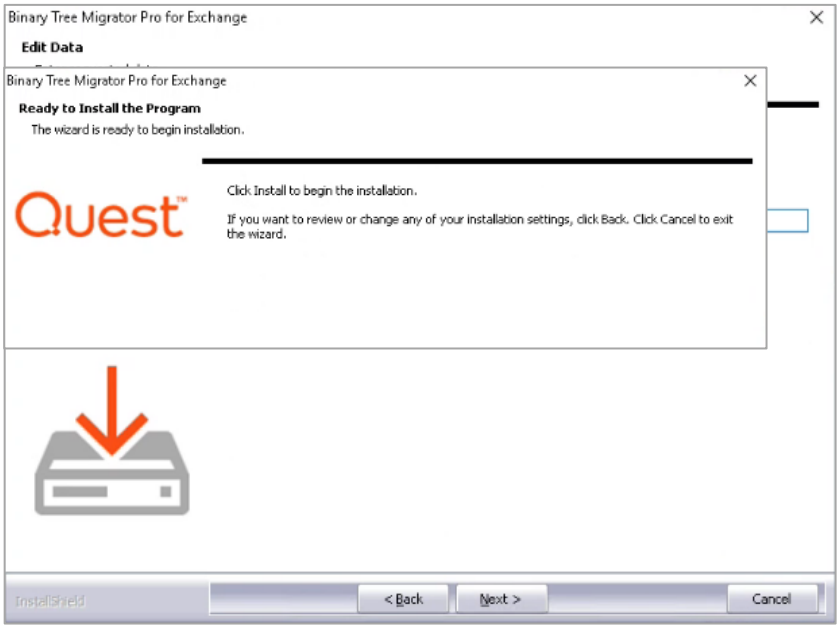
9. On the *Passphrase* screen, enter a passphrase to secure secrets stored in the SQL database. Then click **Next**. Store this phrase in a secure place for future reference. This phrase will be needed for all installations that access the SQL database.



10. On the *Login* screen, enter the **User Name** and **Password** to use for the Binary Tree Migrator Pro for Exchange MCP Service and Migrator Pro for Exchange AppPool and then click **Next**.



11. On the *Migrator Pro for Exchange Administrative Group* screen, enter an Active Directory Security Group to limit access to the Migrator Pro for Exchange Admin Portal, and then click **Next**. Note that *E2E_Admins* is the default group but a different group name can be entered.



12. On the *Ready to Install the Program* screen, click **Install**.

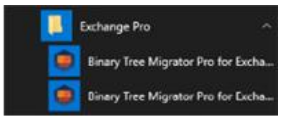
    The installation process may take a few minutes, and the window shows a progress meter while you wait.

    Click **Cancel** if you want to cancel. The installer will first check to determine if the server has adequate disk space, and will alert you if there is not enough space available for installation.

13. When installation is complete, the wizard Complete screen appears. Click **Finish** to close the installer program and return to the Migrator Pro for Exchange Installer.

14. And click **Finish** again to close the Installer.

When the installation completes, the wizard creates a shortcut icon on the Desktop to launch **Migrator Pro for Exchange**. This entry is also added to the Windows **Start** menu along with entries for the **Migrator Pro for Exchange Worker**.



Now that the physical installation is complete, see section 3 below to configure Migrator Pro for Exchange for your environment and purposes. The first time you run the Migrator Pro for Exchange Admin Portal after this installation, Migrator Pro for Exchange will prompt you to define your target forest.

2.5 Uninstalling Migrator Pro for Exchange

To uninstall Migrator Pro for Exchange, go to *Programs and Features* from the Windows *Control Panel*:

1. Click **Start**, and then click **Control Panel.**
2. Click **Programs and Features**, and then select **Migrator Pro for Exchange** from the list.
3. Click **Uninstall**. Uninstalling Migrator Pro for Exchange also uninstalls Migrator Pro for Exchange Worker that is installed on the Migrator Pro for Exchange console.

If other Migrator Pro for Exchange Workers have been setup on other machines, they may need to also be uninstalled.

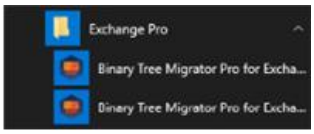
4. Click **Yes**.
5. Click **Finish**.

3. Configuring Migrator Pro for Exchange

The first time you run the Migrator Pro for Exchange Admin Portal after installing the software (in section 2 above), Migrator Pro for Exchange will prompt you to define your target forest. Your target forest can reside in a local Exchange environment, or may be a tenant forest in Office 365.

Use the New Forest wizard to define your target forest.

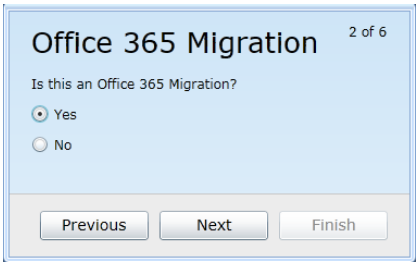
Double-click the Migrator Pro for Exchange shortcut on the Desktop, or Migrator Pro for Exchange in the Windows **Start** menu.



The Admin Portal opens, and Migrator Pro for Exchange starts its New Forest wizard with the **Migrator Pro for Exchange License** screen:

Click **Browse** to locate your license file (**.lic*) or copy and paste the license key and click **Add License**. Then click **Next**. Migrator Pro for Exchange then validates the license file and displays the license details. Click **Next**.

Migrator Pro for Exchange then begins a series of screens for you to define your target forest.



This screen asks whether your target forest is a local Exchange forest, or a tenant forest in Office 365.

If you are migrating to an Office 365 target forest: Click the **Yes** option, then click **Next**, and continue this procedure in section 3.1.1 below.

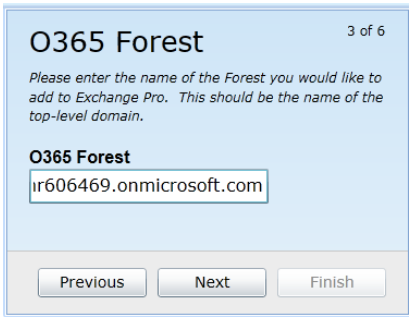
If you are migrating to an on-premises Exchange forest: Click the **No** option, then click **Next**, and continue this procedure in section 3.1.2 below.

If you are migrating to Office 365 but you don't configure the O365 forest now, you can configure an on-premises Exchange forest first, and then the O365 forest later, and Migrator Pro for Exchange will automatically switch the two. That is, Migrator Pro for Exchange will correctly configure the on-premises forest as the source and the O365 forest as the target.

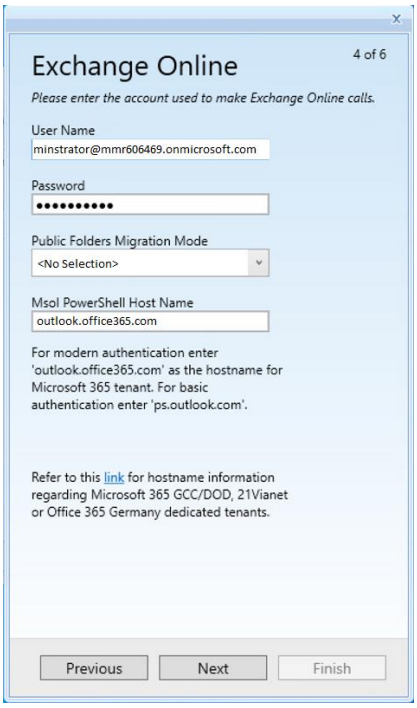
3.1 Defining an Office 365 (Tenant) Target Forest

If your target forest is in a local Exchange environment (not in Office 365), skip ahead to section 3.1.2 below.

Continuing this procedure from the Office 365 Migration screen, where you clicked **Yes** to begin defining an Office 365 Tenant forest:



Enter the name of the tenant target forest, and click **Next**.



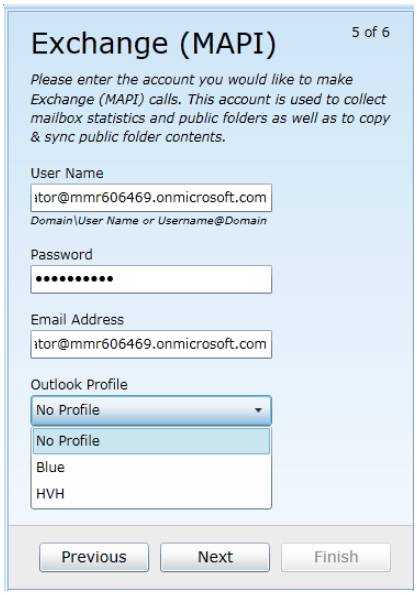
These *Exchange Online* settings are required for Migrator Pro for Exchange program access to Office 365.

Enter the **User Name** and **Password** for the account Migrator Pro for Exchange should use to access Office 365.

Specify a **Public Folders Migration Mode** from the drop-down list. *PowerShell* and *MAPI* are the two available methods. If the **Migration Mode** is not specified here, Migrator Pro for Exchange will use the *MAPI* migration method by default.

For **Msol PowerShell Host Name**, enter the Office 365 endpoint URL. The default Msol Host Name value is outlook.office365.com. Refer to this link for hostname information regarding Microsoft 365 GCC/DOD, 21Vianet or Office 365 Germany dedicated tenants.

When you have entered the requested information, click **Next**.



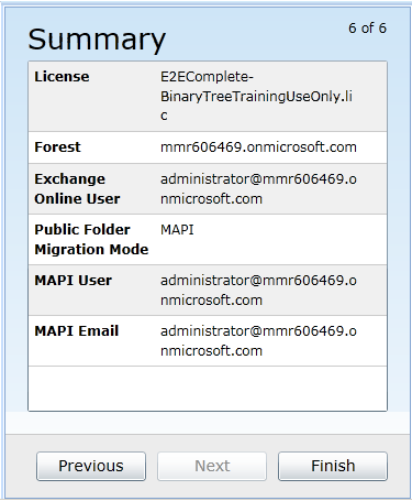
These *Exchange (MAPI)* settings are required only when migrating public folders in cross-forest migrations where no trusts exist.

Enter the **User Name**, **Password** and **Email Address** for the account Migrator Pro for Exchange should use for program calls to Exchange (MAPI), and specify the **Outlook Profile** the program should use.

When you have entered the requested information, click **Next**.

If Migrator Pro for Exchange is installed on a Windows 2012 server with Outlook 2010 as the MAPI provider: You ***must*** use an **Outlook Profile** to connect to a secondary forest.

If the MAPI provider is Outlook 2013: Both trusted and non-trusted Exchange 2013 forests can be reached without an Outlook Profile.



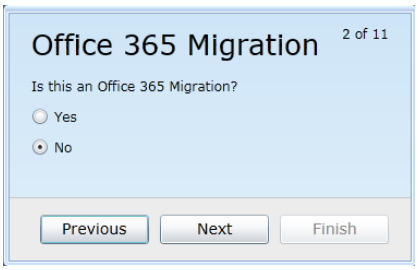
The *Summary* screen shows the settings and choices you have entered to configure your tenant target forest. Review the settings to make sure they are correct for the designated tenant forest. (If you want to change anything you can click **Previous** to return to an earlier screen.)

When these Summary screen values appear as they should, click **Finish** to save the forest configuration information.

When the forest configuration is saved, it appears on the *Configuration Settings* screen of the Migrator Pro for Exchange Admin Portal.

3.2 Defining a Local Exchange Target Forest

This section 3.2 applies only if your target forest is in a local Exchange environment (not in Office 365). A local Exchange target forest is defined when migrating Intra-org (no other forests would be needed), or when migrating Inter-org (a source forest would be defined).

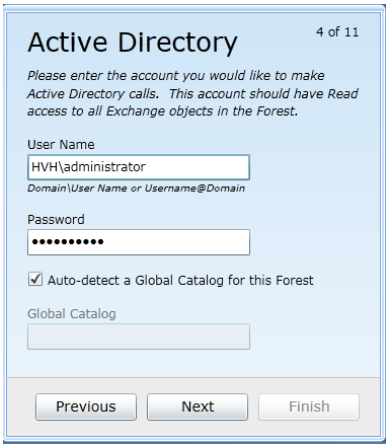


Continuing this procedure from the Office 365 Migration screen, where you clicked **No** (as shown here) to begin defining a target forest in your local Exchange environment.

The first screen in this sequence to define a local target forest is this *Target Forest* screen. Enter the name of the **Target Forest** (top-level domain).

If the target forest you specify is configured as an Exchange Resource Forest environment, select the **Resource Forest** check box to create a "Linked User" relationship between the source and target account. This option applies only for an inter-org migration where the target Exchange environment is located in a resource forest. For more information about resource forests, see Microsoft's article http://technet.microsoft.com/en-us/library/aa998031.aspx and other Microsoft resources.

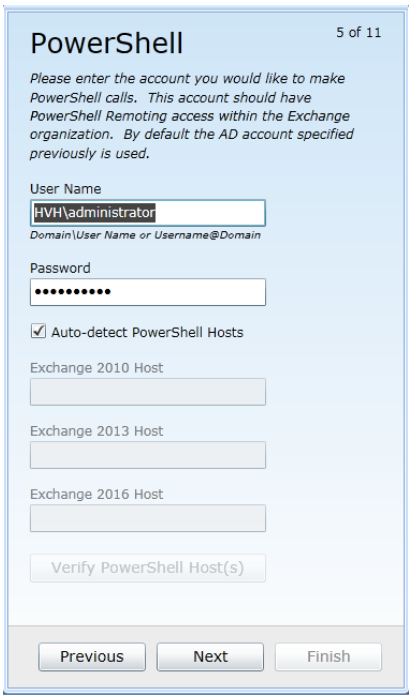
Click **Next**.



In this *Active Directory* screen: Enter the **User Name** (in *Domain\Username* format) and **Password** of the account to use for Active Directory calls.

You can either automatically select a global catalog by selecting the **Auto-Detect a Global Catalog for this Forest** checkbox, or manually specify one in the Global Catalog field.

Click **Next**.

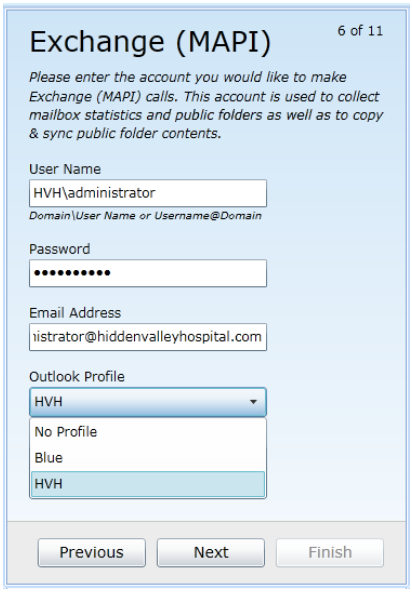


In this *PowerShell* screen: Enter the **User Name** and **Password** of the account to use for PowerShell calls. By default, the program sets these values to the **User Name** and **Password** specified on the previous *Active Directory* screen, but you can change them here.

You can either automatically select the PowerShell hosts by keeping the **Auto-detect the PowerShell Hosts** checkbox selected, or deselect it to manually specify the **Exchange 2010 Host**, **Exchange 2013 Host**, and **Exchange 2016 Host**. If specifying the hosts manually, click the **Verify PowerShell Host(s)** button to validate connectivity to the PowerShell host servers.

Click **Next**.

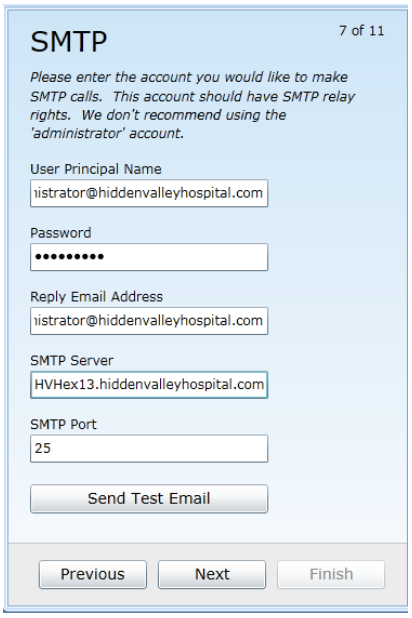
When specifying a PowerShell Host manually, you must use a Fully Qualified Domain Name (FQDN). If you use an IP address, it will generate an SSL certificate error.



In this *Exchange (MAPI)* screen: Enter the **User Name**, **Password** and **Email Address**, and specify the **Outlook Profile** of the account to use for Exchange (MAPI) calls.

Click **Next**.

If Outlook is installed on the Migrator Pro for Exchange Server, an **Outlook Profile** should be used.



In this *SMTP* screen: Enter the **User Principal Name**, **Password**, **Reply Email Address** (e.g., *user@domain.com*), **SMTP Server**, and **SMTP Port** of the account to use for SMTP calls.

Click **Next**.

NOTE !

Specifying SMTP information is not required at the time of configuration.

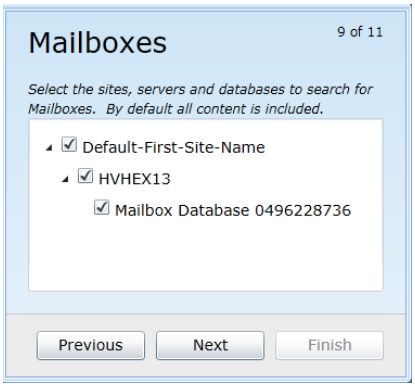
You must specify the **User Principal Name** (*user@domain.com*) and **Password** for the account that will be used to send email communications to end users.

By default, the Exchange 2010/2013 Simple Mail Transfer Protocol (SMTP) receives connector rejects mail from any “well known accounts” such as *Administrator*. We recommend you designate a different account for this purpose.

Make sure the service account being used has access to the Exchange 2003/2007 and 2010/2013/2016 servers.

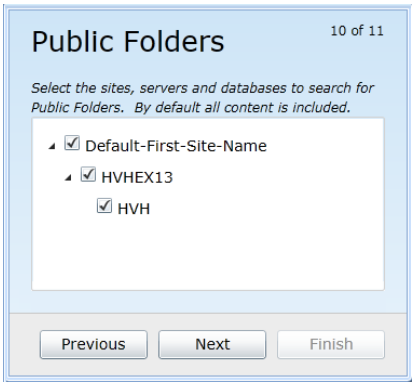
On this *Staged Migrations* screen: Specify the Exchange 2010 or Exchange 2013 staging server/database that Migrator Pro for Exchange should use when migrating from Exchange 2003 to Exchange 2013, or from Exchange 2007 to Exchange 2016.

Click **Next**.



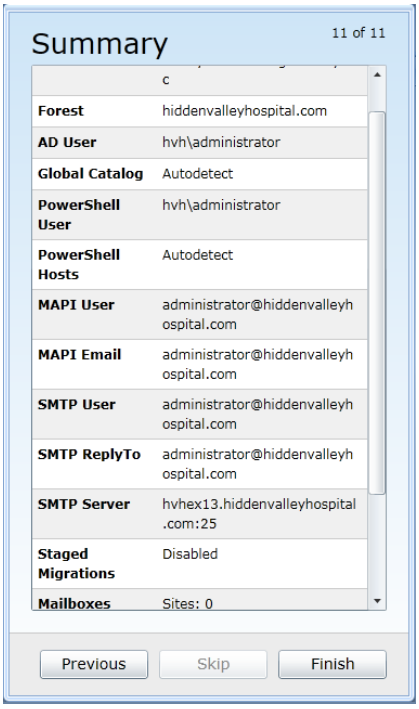
On this *Mailboxes* screen: Select the sites, servers, and databases to search for mailboxes. All content is selected by default. Right-click in the list area to select options to expand/collapse the list or select/deselect all items.

Click **Next**.



In this *Public Folders* screen: Select the sites, servers, and databases to search for Public Folders. All content is selected by default. Right-click in the list area to select options to expand/collapse the list or select/deselect all items.

Click **Next**.



The *Summary* screen shows the settings and choices you have entered to configure your local target forest. Review the settings to make sure they are correct for the designated forest. (If you want to change anything you can click **Previous** to return to an earlier screen.)

When these *Summary* screen values appear as they should, click **Finish** to save the forest configuration information.

NOTE ! In a non-English locale, the date-time format of the operating system must be set to *mmddyyyy* (rather than *ddmmyyyy*) for Migrator Pro for Exchange to rationalize Office 365 mailboxes.

When the forest configuration is saved, it appears on the *Configuration Settings* screen of the Migrator Pro for Exchange Admin Portal.

4. Installing Migrator Pro for Exchange Public Folder Workers

This section includes instructions for the installing Migrator Pro for Exchange Public Folder Workers. Public Folder Workers can be used to allow distribution of Public Folder processing. Public Folder Workers can be assigned specific Public Folder processing roles including provisioning, content sync, change detection, and reporting.

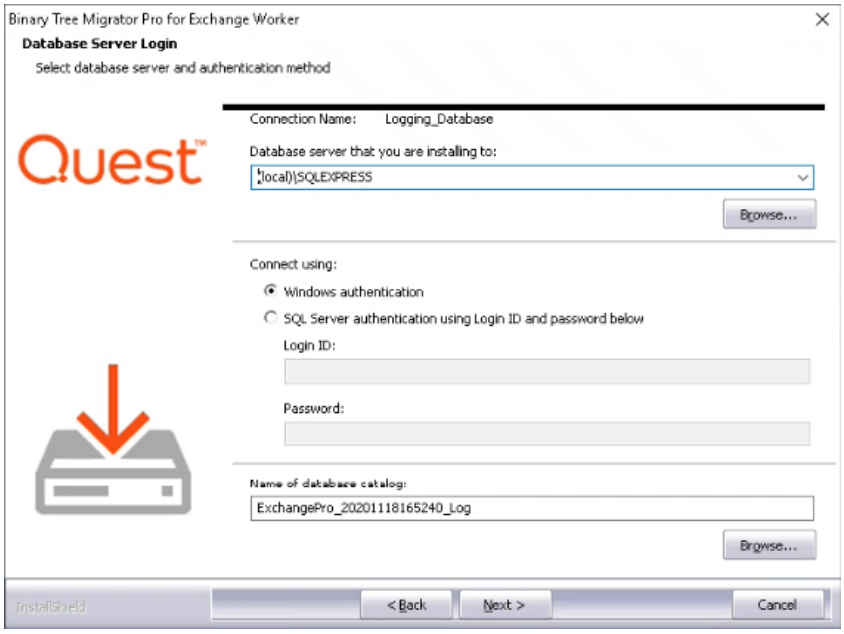
To install the Migrator Pro for Exchange Public Folder Worker:

1. Download or copy the Migrator Pro for Exchange Public Folder Worker installation executable (*Migrator Pro for Exchange Worker Installer*) to the device that will be used as a Public Folder Worker.
2. Right-click on the *Migrator Pro for Exchange Worker Installer* file and select to **Run as Administrator**. Click **Run** on the security warning.
3. The installer then scans your environment to gather the information it needs for installation, and to determine whether you need to install any of several required accessory applications.

   If these accessory apps are already installed, just skip ahead to the next step below. Otherwise, the Migrator Pro for Exchange installer will prompt you to authorize the installation of the ones you need. In that case, click the **Install** button to accept. If you have to install Microsoft .NET 4.8 Framework, you may also be prompted to accept Microsoft's license agreement. If so, mark the checkbox for **I have read and accept…**, and click **Install**.

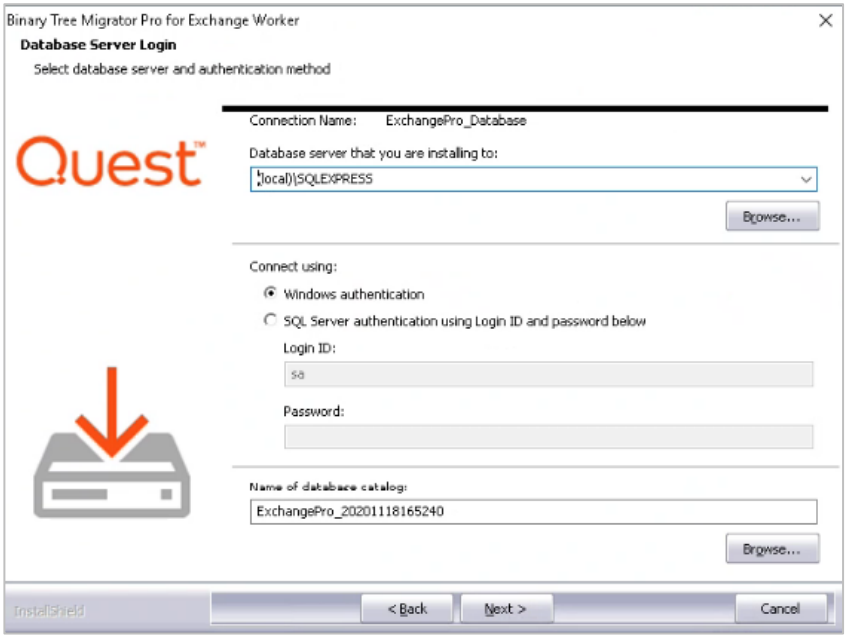
   The installation of accessory applications may take several minutes.
4. When the accessory components are installed, the Migrator Pro for Exchange Worker installer *Welcome* screen appears. Click **Next**.

5. On the *Choose Destination Location* screen, you may **Browse** to an installation location and then click **Next**.



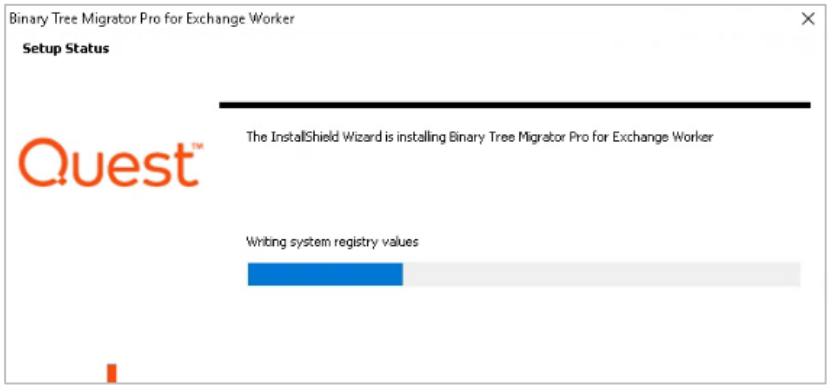
6. On the *Database Server Login* screen, select or browse to the Migrator Pro for Exchange database server you are installing to and select the connection authentication method. Then, in the **Name of database catalog** field, browse to and select the database configured for Migrator Pro for Exchange (Do not enter a new name). Click **Next**.

7. The *Database Server Login* screen appears again, this time for Migrator Pro for Exchange logging database. Select or browse to the logging database server you are installing to, select the connection authentication method, and enter or browse to the database. The logging database name should be specified in the Name of database catalog field. Click **Next**.

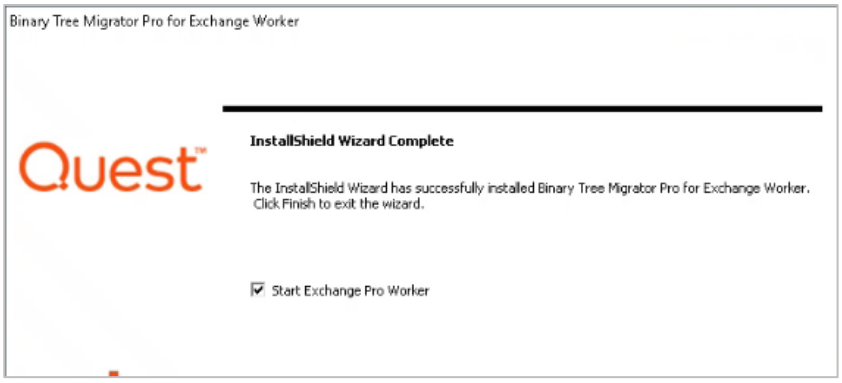


8. On the *Ready to Install* screen, click **Install**.

9. Wait while the installation proceeds. This may take a few minutes. A dialog box displaying installation progress will appear. Click **Cancel** if you want to cancel.



10. When installation is complete, the *wizard Complete* screen appears. Click **Finish** to close.



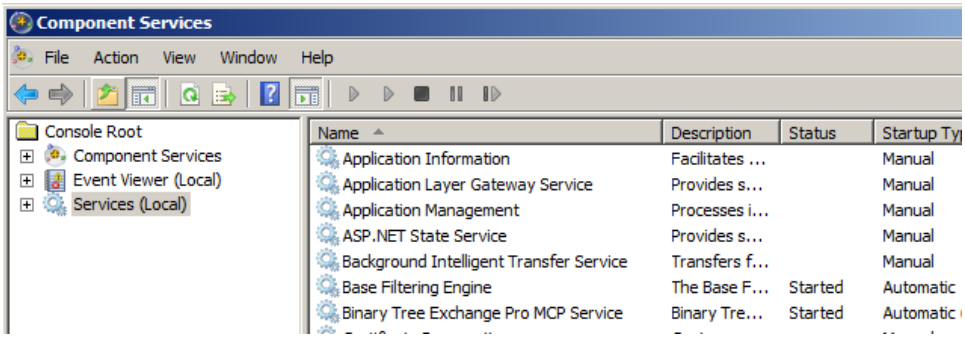
When the installation completes, it creates a shortcut icon on the Desktop to launch Migrator Pro for Exchange Worker. This Migrator Pro for Exchange Worker icon is also added to the toolbar.

5. Components of Migrator Pro for Exchange

The main components of Migrator Pro for Exchange are: the MCP Windows Service, the Admin Portal, and the User Portal.

5.1 MCP Windows Service

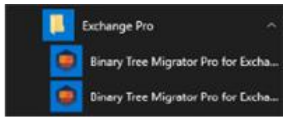
The MCP Windows Service (BinaryTree Migrator Pro for Exchange MCP Service) is the controlling service for all Migrator Pro for Exchange functions. This service should automatically start. Make sure that BinaryTree Migrator Pro for Exchange MCP Service is started in Windows Services.



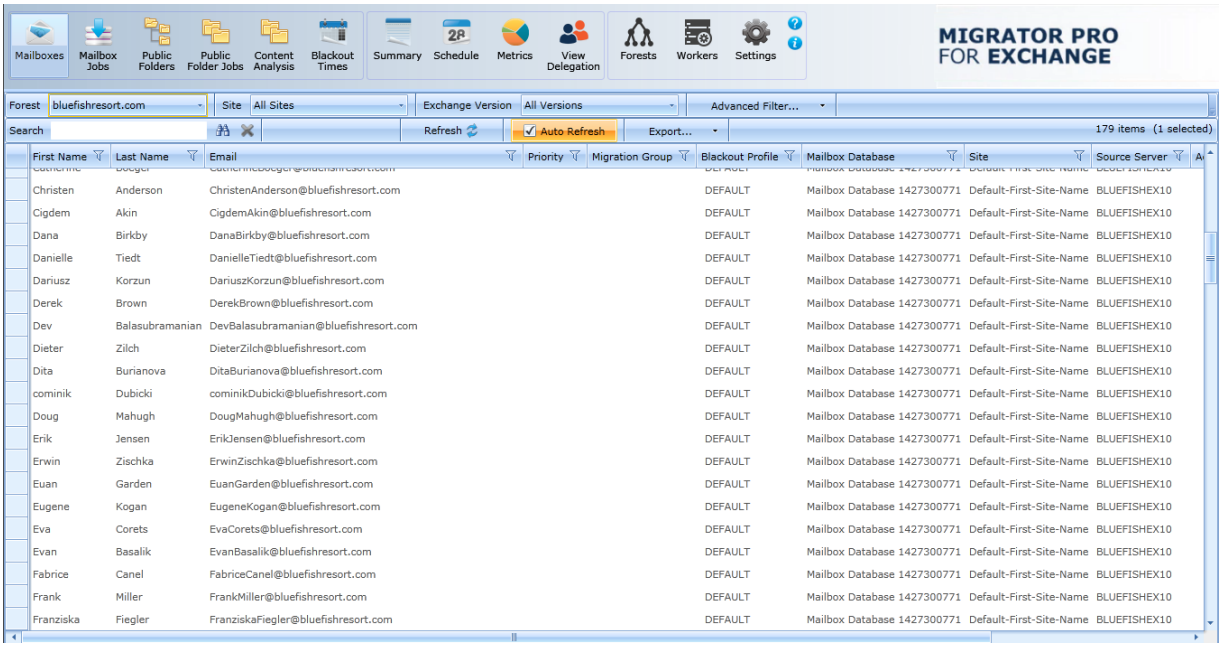
5.2 Admin Portal

Migrator Pro for Exchange's Admin Portal is a friendly user interface that lets you configure and execute most administrative tasks associated with a migration.

To launch the Admin Portal, double-click the **Migrator Pro for Exchange** shortcut on your Windows desktop, or select **Migrator Pro for Exchange** from the Windows **Start** menu:



The Admin Portal opens in a browser window. Migrator Pro for Exchange supports Internet Explorer 8 or later and Firefox.



The Admin Portal launches with http://localhost/exchangepro/admin/default.aspx. You can use *localhost*, <*machinename*>, or the IP address to access the Admin Portal.

5.3 User Portal

The User Portal is available for users to postpone and schedule blackouts for their migrations and to provide alternative notification capabilities.

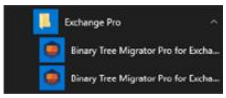
- The User Portal is located at: *http://<MachineName>/exchangepro/user/default.aspx*
- Windows Authentication is enabled for this virtual application. When performing cross-forest migrations, if the users in the source forest attempt to connect to the Migrator Pro for Exchange server in the target forest and a trust has not been established between the two forests, the users will be prompted for their target credentials.

6. Introduction to the Admin Portal

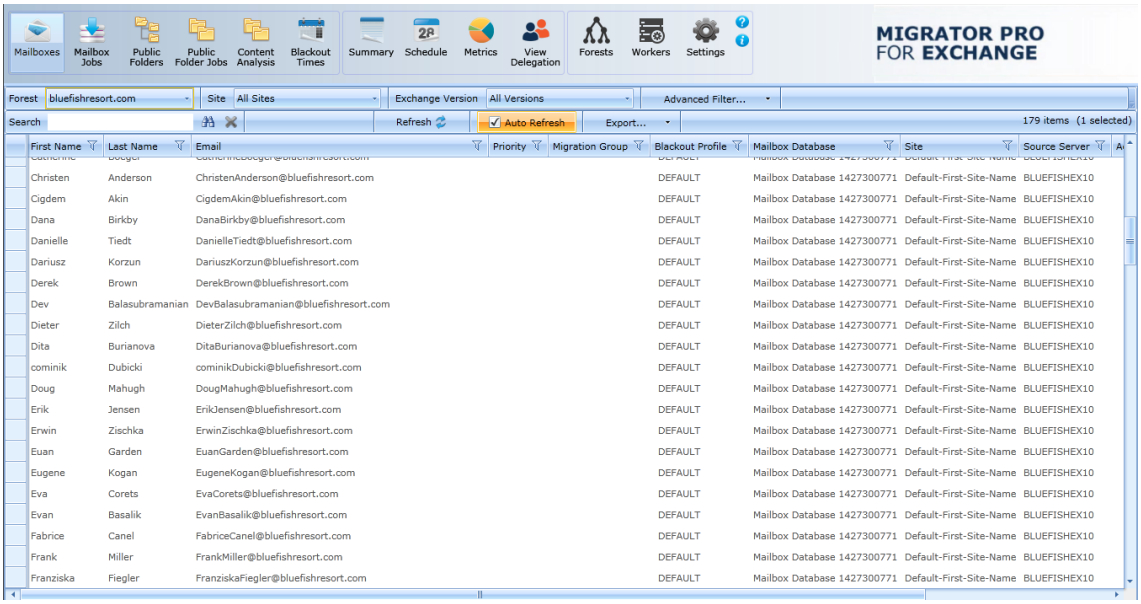
Migrator Pro for Exchange's Admin Portal is a friendly user interface that lets you control various administrative tasks related to Exchange mailbox migration.

The first time you run the Admin Portal after installing Migrator Pro for Exchange, the program leads you through a series of screens for you to enter your Migrator Pro for Exchange license key and configure Migrator Pro for Exchange communications with other programs and hardware. After that initial configuration, the Admin Portal lets you update configuration data, define new forests to Migrator Pro for Exchange, designate mailboxes and public folders for migration, schedule and execute migrations, pause and resume migrations, review migration statistics, and so forth.

To access the Admin Portal, double-click the **Migrator Pro for Exchange** shortcut on your Windows desktop, or select **Migrator Pro for Exchange** from the Windows **Start** menu:



The Admin Portal opens as a new tab in your browser called *Migrator Pro for Exchange*:



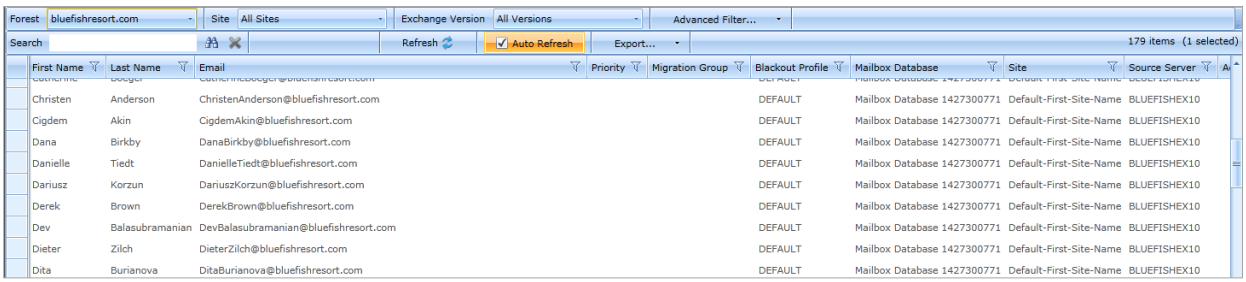
Migrator Pro for Exchange's Main Toolbar appears across the top of the browser tab:

The toolbar buttons let you change the view of the Admin Portal, to show different types of information and different groups of available features below the Main Toolbar:

- **Mailboxes:** Lists mailboxes from all the sites in the specified forest. In addition, it allows you to sort, group, search, and select mailboxes to add to the migration queue.
- **Mailbox Jobs:** Manages the sequence of migration requests for the selected migration destination site.

- **Public Folders:** Displays the Public Folder tree from the selected Source and Target forest. In addition, it allows you to sort, group, search, and select public folders to add to the migration queue. Public folder migration is only enabled during on-premises cross forest migration projects.
- **Public Folder Jobs:** Manages the sequence of migration requests for the selected migration destination. Public folder migration is only enabled during on-premises cross forest migration projects.
- **Content Analysis:** Allows Public Folder content information collection and analysis in SQL for data remediation.
- **Blackout Times:** Allows the configuration of time periods when mailboxes cannot be migrated for the selected migration site.
- **Summary:** Displays high-level accounting of mailbox migrations, which allows you to view all status levels.
- **Schedule:** Displays estimated migration sequence for the selected migration site. It is a read-only view.
- **Metrics:** Provides historical data and throughput measurements of migrations in a graphical format.
- **View Delegation:** Displays delegation data, so you can migrate mailboxes associated by delegation rights together (to preserve delegation rights after the migration).
- **Forests:** Configure global forest settings, add new forest, etc.
- **Workers:** Administer Public Folder migration workers.
- **Settings:** Configure general settings, activities, mailboxes, Public Folders, workers, scripts, notification templates, and licenses.
- **Help:** Open a browser window of information and field notes about the currently active Migrator Pro for Exchange screen or tab.
- **About:** Displays version information about the Migrator Pro for Exchange product.

In addition to the Main Toolbar, the Admin Portal also contains a Data Panel that displays data depending on the button that is currently selected.



Detailed information about the Admin Portal is available in the Migrator Pro for Exchange *User Guide*.

Appendix A. STIG Environments

Please note the following considerations for STIG environments.

SQL Express

The SQL Express option should not be chosen when installing Migrator Pro for Exchange. SQL Express does not include the following settings or features needed for STIG environments:

- SQL Server must be monitored to discover unauthorized changes to stored procedures. (SQL Agents is not part of SQL Express) 41403, 41404, 41405

A dedicated SQL Server (full version) should be used.

Additional Information

Microsoft SQL Server 2012 Database Security Technical Implementation Guide (stigviewer.com)

Microsoft SQL Server 2012 Database Instance Security Technical Implementation Guide (stigviewer.com)

MS SQL Server 2016 Instance Security Technical Implementation Guide (stigviewer.com)

MS SQL Server 2016 Database Security Technical Implementation Guide (stigviewer.com)

Appendix B. Deployment in FIPS Environment

Binary Tree Migrator Pro for Exchange 20.11.1 can be successfully deployed in a FIPS environment by following the procedure described in this document.

The audience for this section is technical implementation consultants deploying Migrator Pro for Exchange.

Cryptographic usage

Migrator Pro for Exchange relies on the following Third-Party cryptographic libraries for its cryptographic needs.

Cryptographic usage	Cryptographic algorithm	Cryptographic parameters
Communication – Website User Interface	SSL TLS 1.2	
Communication – SQL Server	SSL TLS 1.2	
Communication – (LDAP/Kerberos)	AES128_HMAC_SHA1, AES256_HMAC_SHA1	SESSION: Signing & Sealing
Symmetric encryption of bulk data	AES256 CBC Mode	KEY: 256-bit PBKDF2 (Constant) IV: 128-bit PBKDF2 (Constant)
Symmetric encryption of bulk data – Additional Entropy	RNG	64-bits (Random per encrypted value)
Symmetric encryption of secrets – (DPAPI) Configuration Parameters	AES256 CBC Mode	SCOPE: LocalMachine
Symmetric encryption of secrets – Additional Entropy	RNG	256-bits (Constant per node)
Hashing – (PBKDF2) Generation of encryption KEY/IV	HMACSHA1	HASH SIZE: 160-bit
Hashing – (DPAPI)	SHA512	HASH SIZE: 523-bit

Background

To execute in a FIPS compliant mode, a Windows environment requires the Microsoft Policy “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” setting enabled.

Microsoft states that “This policy is only advisory to applications. Therefore, if you enable the policy, it does not make sure that all applications will comply”.

Migrator Pro for Exchange leverages Microsoft’s CryptoAPI (CAPI) and CryptoAPI Next Generation (CNG) for its cryptographic needs

Microsoft Product Relationship with CNG and CAPI libraries is documented here:
https://technet.microsoft.com/en-us/library/cc750357.aspx

“Rather than validate individual components and products, Microsoft chooses to validate only the underlying cryptographic modules. Subsequently, many Windows components and Microsoft products are built to rely on the Cryptographic API: Next Generation (CNG) and legacy Cryptographic API (CAPI) FIPS 140 validated cryptographic

modules. Windows components and Microsoft products use the documented application programming interfaces (APIs) for each of the modules to access various cryptographic services.

Prerequisites

External to Migrator Pro for Exchange, the following server configurations are necessary to set up the environment for FIPS Mode.

1. Windows Server 2012 R2 or later must be installed and up to date.
2. The following group policies must be enabled:
    a. System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.
        i. Ensure this policy is enabled.
    b. Network Security: Configure encryption types allowed for Kerberos.
        i. Ensure the “AES128_HMAC_SHA1” and “AES256_HMAC_SHA1” values are selected.
        ii. NOTE: Authentication of target accounts with synchronized passwords requires Kerberos encryption type “RC4_HMAC_MD5” to be allowed for participating devices.
3. Insecure SCHANNEL Server protocols must be disabled.
    a. SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1
4. SSL certificate for Web Hosting issued by a trusted certificate authority.
5. SQL Server Encrypted Connections must be enabled.
    a. See reference links for configuration details

Installation and operation

For environments with existing Migrator Pro for Exchange installations, the installation must be upgraded to version 20.11 or later. If the existing installation is configured with remote Migrator Pro for Exchange Workers, the remote Workers need to be upgraded to version 20.11 or later.

For new installations, Migrator Pro for Exchange 20.11 enforces all FIPS mode requirements, no additional steps are required.

WEBSITE SSL CERTIFICATE INSTALLATION

1. Ensure the certificate and CA certificate chain has been installed on the server.
2. Open Internet Information Services (IIS) Manager.
3. Expand the Sites node in the Connections pane.
4. Right-click the “Default Web Site” website node and choose “Edit Bindings…”.
    a. If the site has an “https” binding, select it and click “Edit…”
    b. If the site does not have an “https” binding, click “Add…”

i. From the “Type” drop-down, select “https”.

c. From the “SSL certificate” drop-down, select the appropriate certificate.

d. Click OK.

e. Remove the “http” binding.

5. In the IIS Manager Features View pane, double-click “SSL Settings”.

   a. Check the “Require SSL” checkbox and click “Apply” in the Actions pane.

6. Validate the website can be accessed and the bowers is indicating the certificate is valid and trusted.

References

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

Network security: Configure encryption types for Kerberos

Windows Server SCHANNEL Protocol Settings

Internet Information Services (IIS) 7.0 Set Up SSL Certificates

Internet Information Services (IIS) 8.0 Centralized SSL Certificates

Enable encrypted connections - SQL Server | Microsoft Docs

KB3135244 - TLS 1.2 support for Microsoft SQL Server