



Migrator Pro for Exchange 20.11.4

Installation and Configuration Guide



© 2025 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

20 Enterprise Ste 100

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.

Contents

Introduction	5
Purpose	5
Audience	5
Getting More Information	5
About Migrator Pro for Exchange	6
Key Features and Functions	6
Installing Migrator Pro for Exchange	7
Upgrading Migrator Pro for Exchange from an Earlier Version	7
Necessary Pre-Installation Preparations	7
Migrator Pro for Exchange Default Installation	10
Migrator Pro for Exchange Advanced Installation or Upgrade	13
Uninstalling Migrator Pro for Exchange	16
Configuring Migrator Pro for Exchange	17
Defining a Microsoft 365 (Tenant) Target Forest	18
Entra ID App Registration	18
Manually registering the Migrator Pro for Exchange application with the Microsoft Azure portal	18
Configuring Migrator Pro for Exchange for Microsoft 365	21
Defining a Local Exchange Target Forest	23
Installing Migrator Pro for Exchange Public Folder Workers	27
Components of Migrator Pro for Exchange	29
MCP Windows Service	29
Admin Console	29
User Portal	29
Introduction to the Admin Console	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
About us	36
Technical support resources	36

Introduction

Purpose

This document describes how to get started using Migrator Pro for Exchange including prerequisites, installation and configuration instructions, and an introduction to the Admin Console.

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.

Getting More Information

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

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

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 2010, Exchange 2013, Exchange 2016, Exchange 2019, and Office 365.
- Support for migrations to Office 365, resource forest migrations, and Outlook profile updates.

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

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.

i **NOTE:** 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).

i **NOTE:** 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.

i **IMPORTANT:** If you are connecting to Microsoft 365 and are upgrading from the previous Migrator Pro for Exchange release, you **must** complete the Entra ID App Registration process. It is not possible to use the previous username/password authentication method to migrate to Microsoft 365 with this release of Migrator Pro for Exchange. Microsoft enforces MFA on all new tenants and will begin enforcing it on existing tenants.

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 Microsoft 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.

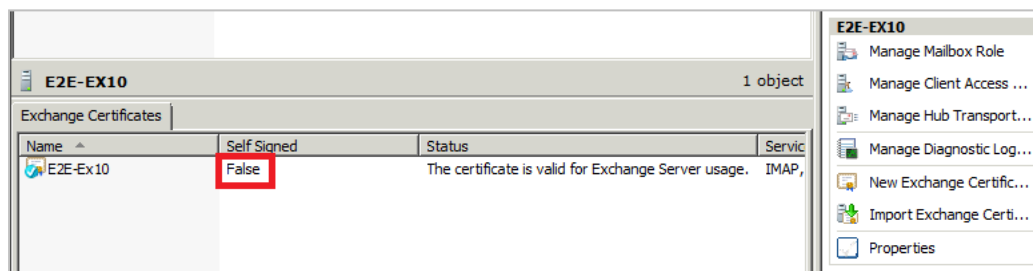
Prior to installing Migrator Pro for Exchange, you need to identify the primary Exchange servers utilized as the PowerShell hosts.

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.

i **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 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, Microsoft Exchange Server 2016, or Microsoft Exchange Server 2019 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.

```

Machine: E2F-Fx10.e2e.dom
Welcome to the Exchange Management Shell!
Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> ! Format-List

Tip of the day #64:
You can use client-side filtering to return only the data that you want to see or work with. The following example retrieves all Active Directory user accounts in the Engineering department and puts the results in a table with two columns, Name and Department. By using the ResultSize parameter, the Get-User cmdlet limits the result set to 2,000 users.

$Users = Get-User -ResultSize 2000
$Users | Where { $_.Department -Eq "Engineering" } | Format-Table Name, Department

VERBOSE: Connecting to E2E-Ex10.e2e.dom
VERBOSE: Connected to E2E-Ex10.e2e.dom.
PS1 C:\Windows\system32>

```

4. Press <Y> again to confirm.

```

Machine: E2F-Fx10.e2e.dom
PS1 C:\Windows\system32> Enable-PSRemoting
WinRM Quick Configuration
Running command "Set-WSManQuickConfig" to enable this machine for remote management through WinRM service.
This includes:
1. Starting or restarting (if already started) the WinRM service
2. Setting the WinRM service type to auto start
3. Creating a listener to accept requests on any IP address
4. Enabling firewall exception for WS-Management traffic (for http only).

Do you want to continue?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
WinRM already is set up to receive requests on this machine.
WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
WinRM firewall exception enabled.

Confirm
Are you sure you want to perform this action?
Performing operation "Registering session configuration" on Target "Session configuration "Microsoft.PowerShell132" is not found. Running command "Register-PSessionConfiguration Microsoft.PowerShell132 -processorarchitecture x86 -force" to create "Microsoft.PowerShell132" session configuration. This will restart WinRM service.".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

```

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
```

```

Machine: E2F-Fx10.e2e.dom
PS1 C:\Windows\system32> Set-PowerShellVirtualDirectory "E2E-Ex10\PowerShell (Default Web Site)" -BasicAuthentication $true

```

i **NOTE:** 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 *Migrator Pro for Exchange Default Installation* option will suit most organizations. The *Migrator Pro for Exchange Advanced Installation or Upgrade* option is appropriate if you want to specify particular components other than those the wizard would find and use by default.

Migrator Pro for Exchange *Default Installation*

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

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 **Run as Administrator**.

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



The wizard prompts you to review and accept the Migrator Pro for Exchange license and software transaction agreement. To accept the agreement, select the **I read, understand, and accept...** radio button and click **Next**.



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

i NOTE: 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
```

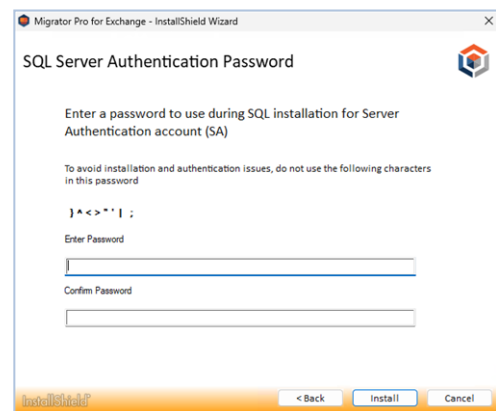
If you have uninstalled a prior Migrator Pro for Exchange version and now want to run the *Default Installation* option for the new version, you must first remove that entry from the registry.

The wizard then prompts you for the *SQL Server Authentication Password*. Enter a password for use during SQL installation for the Server Authentication (SA) account.

When ready, choose **Install**.

! **NOTE:** To avoid installation and authentication issues, do not use the following characters in this password:

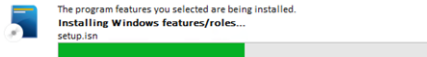
```
} ^ < > " ' | ;
```



The wizard then scans your environment to gather the information it needs, and to determine whether you need to install any of several required prerequisite applications. They will be installed automatically if they are not present.

- Windows features IIS and .NET Framework 4.8 full
- SQL Server 2022 Express
 - [local]\SQLEXPRESS installs as a named instance using the format *servername\SQLExpress*
 - Installs in Mixed mode with install account as SA (System Administrator). The *SQL Server Authentication Password* you entered on the previous panel will be used for the SA account.

A progress meter shows the wizard's progress:



On the *Enter a Passphrase...* screen, enter a passphrase to secure secrets stored in the SQL database. Then choose **Next**.

Store this phrase in a secure place for future reference. This phrase will be needed for all installations that access the SQL database.

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 choose **Next**.

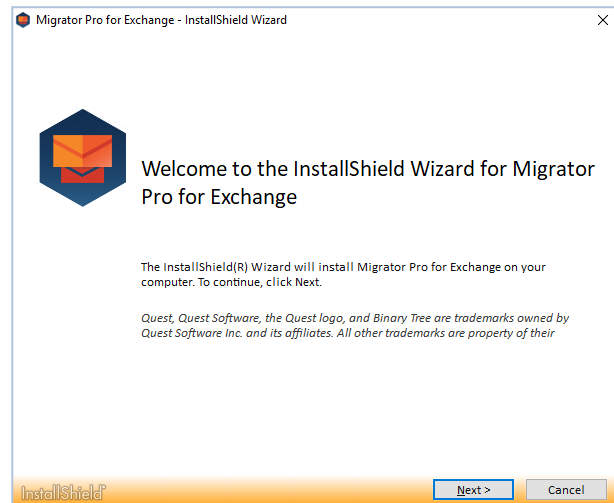
The installation resumes when you choose **Next**. A progress meter shows the progress, and notifies you when the installation is complete. Choose the **Finish** button to close this portion of the wizard. Another progress meter shows the process progress through this last phase of the installation, and the wizard then notifies you when the process is complete. Choose this **Finish** button to close the Migrator Pro for Exchange Installer.

Now that the physical installation is complete, see [Configuring Migrator Pro for Exchange](#) to configure Migrator Pro for Exchange for your environment and purposes. The first time you run the Migrator Pro for Exchange Admin Console after this installation, Migrator Pro for Exchange will prompt you to define your target forest.

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): 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 **Run as Administrator**.

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



The wizard then prompts you to review and accept the Migrator Pro for Exchange license and software transaction agreement. To accept the agreement, select the **I read, understand, and accept...** radio button and click **Next**.



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.

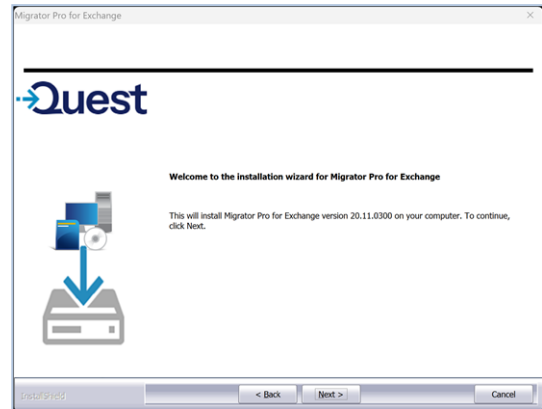
i **NOTE:** If the Migrator Pro for Exchange Installer detects a previous version of Migrator Pro for Exchange, it will skip this screen that offers the *Default Installation* option, and will perform an upgrade using the *Advanced Installation* process.

The wizard then scans your environment to gather the information it needs, and to determine whether you need to install IIS and .NET Framework 4.8 full

A progress meter shows the wizard's progress:

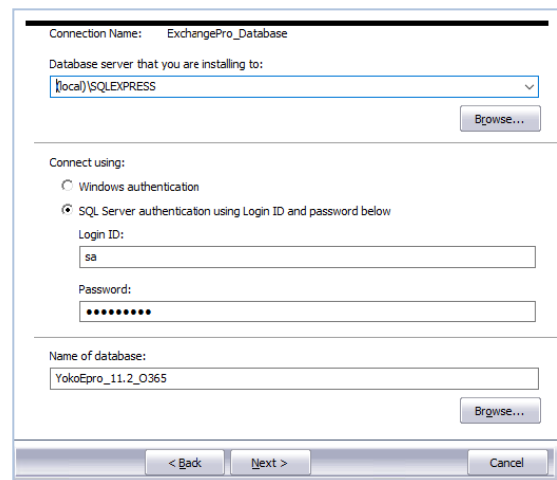


On the installation wizard *Welcome* screen, click **Next**.

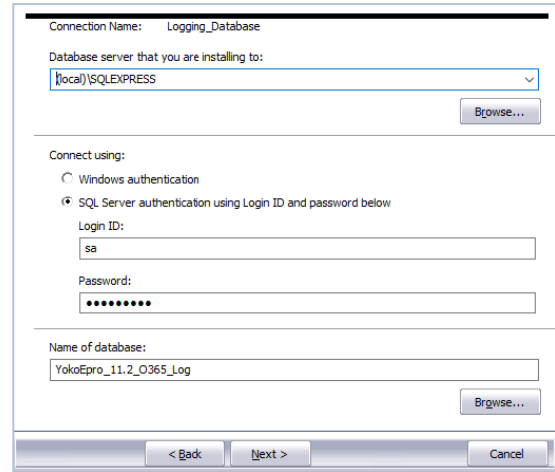


On the *Destination Location* screen, select the destination folder for the installation and then click **Next**.

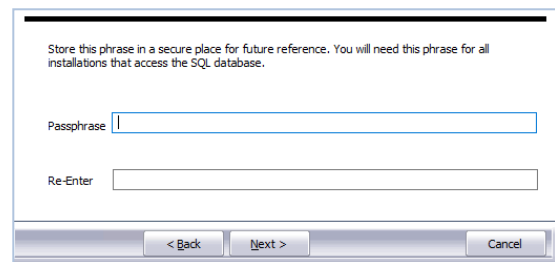
On the *Database Server Login* screen, select or browse to the Migrator Pro for Exchange database server you are installing to, select the connection authentication method, and enter the **Name of database** (or **Browse** to it and select it). Then click **Next**.



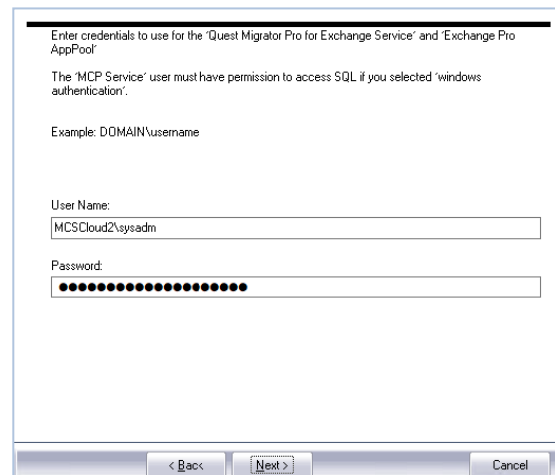
The *Database Server Login* screen appears again, this time for the Migrator Pro for Exchange Logging Database. Select or browse to the logging database server you are installing to, select the connection authentication method, and enter the **Name of database** (or **Browse** to it and select it). Then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



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.



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



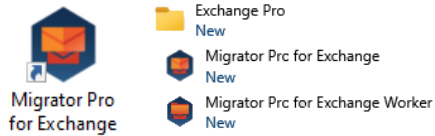
On the *Ready to Install the Program* screen, click **Install**. The installation process may take a few minutes, and the window shows a progress meter while you wait.

Choose **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.

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

Choose **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 [Configuring Migrator Pro for Exchange](#) to configure Migrator Pro for Exchange for your environment and purposes. The first time you run the Migrator Pro for Exchange Admin Console after this installation, Migrator Pro for Exchange will prompt you to define your target forest.

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.

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

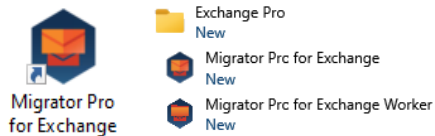
4. Click **Yes**.
5. Click **Finish**.

Configuring Migrator Pro for Exchange

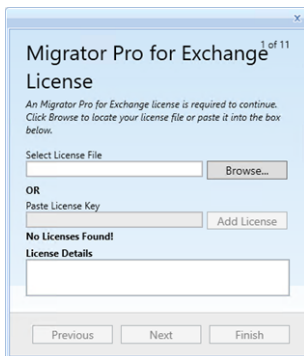
The first time you run the Migrator Pro for Exchange Admin Console after installing the software Migrator Pro for Exchange will prompt you to define your target forest. Your target forest can reside in a local Exchange environment, or may be a tenant forest in Microsoft 365.

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.



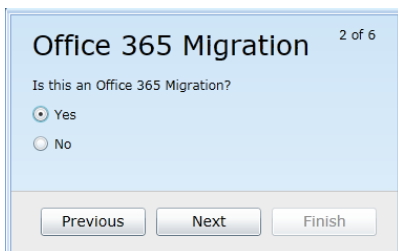
The Admin Console opens, and Migrator Pro for Exchange starts its New Forest wizard with the *Migrator Pro for Exchange License* screen:



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**.

NOTE: It will be necessary to exit and restart the external Public Folder worker for it to recognize the license.

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 [Configuring Migrator Pro for Exchange for Microsoft 365](#).

If you are migrating to an on-premises Exchange forest: Click the **No** option, then click **Next**, and continue this procedure in [Defining a Local Exchange Target Forest](#).

NOTE: If you are migrating to Microsoft 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.

Defining a Microsoft 365 (Tenant) Target Forest

If your target forest is in a local Exchange environment (not in Microsoft 365), see [Defining a Local Exchange Target Forest](#).

Entra ID App Registration

For migration to Microsoft 365, you must register an application with the Microsoft Entra admin center to support Multi-Factor Authentication for PowerShell and Graph calls from Migrator Pro for Exchange. Follow the directions from Microsoft Learn at [App-only authentication for unattended scripts in Exchange Online PowerShell and Security & Compliance PowerShell](#).

After App registration is complete, note the following information from the Microsoft Entra admin center. You will need to enter this information later in this configuration process.

- **Tenant Domain Name:** Your tenant's *primary domain name* on the Microsoft Entra admin center. For example, `sitraka.onmicrosoft.com`.
- **Tenant ID:** Your tenant's ID, found on the Home page of the Microsoft Entra admin center.
- **Registered App Client ID:** The Application ID created with application permissions after the application is registered in the Microsoft Entra admin center.
- **Registered App Client Secret:** The Application Secret created after the application is registered in the Microsoft Entra admin center.

i Show App Client Secret: When the check box is selected, the App Client Secret value is displayed unmasked, so that you can make note of the client secret value.

Manually registering the Migrator Pro for Exchange application with the Microsoft Azure portal


To find your Microsoft 365 tenant's primary domain name, log in into Microsoft 365 Admin Center as an administrator. Under Settings, click Domains and find a domain which ends in `.onmicrosoft.com`. This is your Microsoft 365 tenant domain name, for example `sitraka.onmicrosoft.com`.

The process of registering an application with the Microsoft Azure portal is also described in the Microsoft Learn topic [Register an application with the Microsoft identity platform](#).

i If you are connecting to Microsoft Azure China portal, you can use the same manual procedure to register an application with Azure China. You can find the Azure China portal at: <https://portal.azure.cn>

Depending on the region from which you are accessing the Microsoft portal site, the user interface can differ.

To manually register the Migrator Pro for Exchange application:

1. Sign in to the Microsoft Entra admin center. (<https://entra.microsoft.com/>)
 -  **IMPORTANT:** You must have global admin rights to register this application.
2. Search for App registrations in the search box at the top.
 - OR -
 - In the left navigation pane, choose **Applications**, choose **App registrations**. From the Navigation bar, choose **New registration**.
3. On the Register an application page, enter the application registration information.
 - **Name:** For example, Quest Migrator Pro for Exchange
 - **Supported account types:** Select *Accounts in this Organization Only (Tenant name – Single tenant)*
 - **Redirect URI:**
 - Select Public client/native (mobile & desktop)
 - Enter a URI: ms-appx-web://microsoft.aad.brokerplugin/ef8638f2-41c2-48ae-98b7-e87fac30b8ee
4. Click **Register**:

The newly registered application is displayed and the following application details become available.

 - **Application (client) ID:** The Application ID created after the application is registered in the Microsoft Entra admin center. You must copy this ID and use it later to complete the App Registration.
5. Enable additional redirect URLs
 - While on the **Overview** page, under **Essentials**, click the link next to “**Redirect URIs**”
 - Under **Mobile and Desktop Applications**, enable the checkboxes next to the 3 default URLs.
 - Choose **Save**.
6. Return to the *Overview*. Under **Manage** in the left side menu, choose **API permissions**.
7. Under *Configured permissions* choose **Add a permission**. The *Request API permissions* panel opens on the right.
8. Under *Microsoft APIs*, choose **Microsoft Graph**.
9. Select **Application permissions**. From the **Select permissions** list:
 - Filter on **Sites**, then expand **Sites** and select **Sites.FullControl.All**,
 - Filter on **User**, then Expand **User**, select **User.Read.All** and click **Add permissions** to grant application permission. The *Request API permissions* panel will close.
 - Verify that the new permissions appear in the *Configured permissions* table.

- Verify that the default **User.Read** Delegated permission also appears. If not, follow the same process to add this Microsoft.Graph Delegated permission.
10. Under *Configured permissions* choose **Add a permission**. The *Request API permissions* panel opens on the right.
 11. Under *APIs my organization uses*, choose **Office 365 Exchange Online**.
 12. Select **Application permissions**. From the **Select permissions** list, select **Exchange.ManageAsApp** under *Exchange*. Choose **Add permissions** to grant this application permission.
 13. Choose **Grant admin consent for (your company name)**.
A confirmation message appears on the top. Click **Yes**.
 14. Under *App registrations*, on the left side menu for your application, under *Manage*, choose **Certificates & secrets**.
 - a. Under **Client secrets**, choose **New client secret**.
 - b. Enter a description and specify an expiration for the client secret (for example, In 2 years).
 - c. Choose **Add** to generate the client secret.
 - d. Copy the new client secret **value** and keep it safe as you need it to complete the application registration in Migrator Pro for Exchange. You cannot retrieve a client secret after you perform another operation or leave this resource management view (blade).
 15. Optionally, create a Certificate. Using “Certificate based authentication (CBA)” a self signed certificate can be created and uploaded to secure the connection. Please refer to this [Microsoft Learn document](#) for additional information.
 16. On the left side menu for your application, under *Manage*, choose **API permissions**.
 17. Under *App registrations*, on the left side menu for your application, under *Manage*, choose **Authentication**.
 18. Under *Advanced settings*, click **Yes** next to **Treat application as a public client** and click **Save**.
 19. In the Microsoft Entra admin center’s left side pane, select **Roles & admins**. On the **Roles and administrators | All roles** page,
 - a. Enter *Exchange Administrator* in the search box. Click anywhere (except the check box) in the resulting *Exchange Administrator* row to select it. The **Exchange Administrator | Assignments** page opens.
 - b. Choose **Add Assignments**. Once the page fully loads, a clickable link (“x Member(s) selected”) appears under *Select Members*. Select this link.
 - c. A *Select a member* page opens. In the Search box, enter either the name you chose for your Migrator Pro for Exchange application or the Application (client) ID. Select the corresponding row on the table, then choose **Select**.
 - d. Select **Next**. Enter a justification, such as “Quest Migrator Pro for Exchange requires this permission.” and choose **Assign**.
 20. Close the **Exchange Administrator | Assignments** page.

21. Repeat this process for the *License Administrator* role.
22. Your Migrator Pro for Exchange app registration is complete.

Configuring Migrator Pro for Exchange for Microsoft 365

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

Enter the domain name of the tenant target forest. Use your tenant's *primary domain name* as shown on the Microsoft Entra admin center, for example, `sitraka.onmicrosoft.com`. Do not use a vanity or brand top-level domain.

Click **Next**.

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

Enter the **User Name** and **Password** for the account Migrator Pro for Exchange should use to access Microsoft 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 Microsoft Learn [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**.

Enter the information you recorded during the [Entra ID App Registration](#) step.

Enter the Client ID, Tenant ID, and either the Certificate Thumbprint or the Client Secret from your App Registration. (If you like, you may enter both a Thumbprint and Secret.)

The *Exchange (MAPI)* settings are required if you selected MAPI public folder migration.

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

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

CAUTION: Unlike older versions of Migrator Pro for Exchange, you *must* use an Outlook Profile for MAPI public folder migration.

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. Key properties and connectivity to the Microsoft 365 tenant will be validated before the configuration is saved, and any errors will be displayed.

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

Defining a Local Exchange Target Forest

This section applies if your target forest is in a local Exchange environment (not in Microsoft 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).

The screenshot shows the 'Office 365 Migration' dialog box, step 2 of 11. It asks 'Is this an Office 365 Migration?' with two radio buttons: 'Yes' and 'No'. The 'No' option is selected. At the bottom, there are three buttons: 'Previous', 'Next', and 'Finish'.

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 screenshot shows the 'Target Forest' dialog box, step 3 of 11. It asks 'Please enter the name of the Forest you would like to add to Migrator Pro for Exchange. This should be the name of the top-level domain.' There is a text input field for 'Target Forest' and a checkbox for 'Resource Forest'.

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**.

The screenshot shows the 'Active Directory' dialog box, step 4 of 11. It asks 'Please enter the account you would like to make Active Directory calls. This account should have Read access to all Exchange objects in the Forest.' It has fields for 'User Name' (containing 'HVH\administrator') and 'Password' (masked with dots). There is a checked checkbox for 'Auto-detect a Global Catalog for this Forest' and a 'Global Catalog' field. At the bottom, there are three buttons: 'Previous', 'Next', and 'Finish'.

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**.

PowerShell 5 of 11

Please enter the account you would like to make PowerShell calls. This account should have PowerShell Remoting access within the Exchange organization. By default the AD account specified previously is used.

User Name

Domain\User Name or Username@Domain

Password

Auto-detect PowerShell Hosts

Exchange 2010 Host

Exchange 2013 Host

Exchange 2016 Host

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**, **Exchange 2016 Host**, and **Exchange 2019 Host**. If specifying the hosts manually, click the **Verify PowerShell Host(s)** button to validate connectivity to the PowerShell host servers.

Click **Next**.

i **NOTE:** 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.

Exchange (MAPI) 6 of 11

Please enter the account you would like to make Exchange (MAPI) calls. This account is used to collect mailbox statistics and public folders as well as to copy & sync public folder contents.

User Name

Domain\User Name or Username@Domain

Password

Email Address

Outlook Profile

 No Profile
 Blue
 HVH

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**.

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

SMTP 7 of 11

Please enter the account you would like to make SMTP calls. This account should have SMTP relay rights. We don't recommend using the 'administrator' account.

User Principal Name

Password

Reply Email Address

SMTP Server

SMTP Port

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**.

i 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 specified SMTP servers.

Staged Migrations 8 of 11

If you plan on migrating from Exchange 2003 to Exchange 2013 or Exchange 2016, you will need to stage these migrations through an Exchange 2010 server. If you plan on migrating from Exchange 2007 to Exchange 2016, you will need to stage these migrations through an Exchange 2010 server or an Exchange 2013 server. If needed, please specify this information below.

Enable staged migrations on this forest.

Exchange Staging Server

Exchange Staging Database

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**.

i NOTE: Staged migrations are no longer enabled by default. This feature will be removed in a future update of Migrator Pro for Exchange.

Mailboxes 9 of 11

Select the sites, servers and databases to search for Mailboxes. By default all content is included.

- Default-First-Site-Name
 - HVHEX13
 - Mailbox Database 0496228736

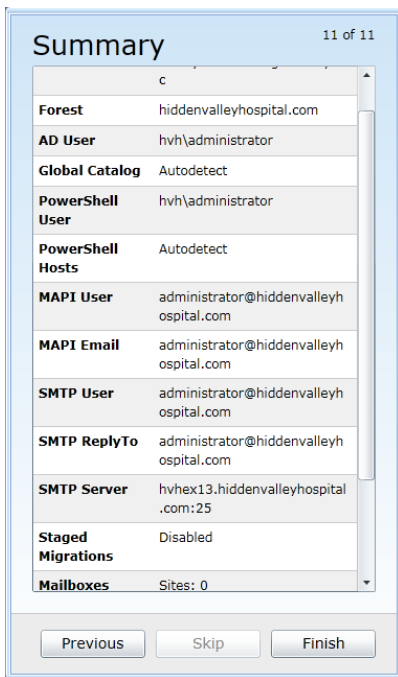
On this *Mailboxes* screen: Select the sites, servers, and databases to search for mailboxes. All content is selected by default. Right-click in the list area to select options to expand/collapse the list or select/deselect all items.

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.

i **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 Console.

Installing Migrator Pro for Exchange Public Folder Workers

Migrator Pro for Exchange Public Folder Workers can be used to distribute 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:

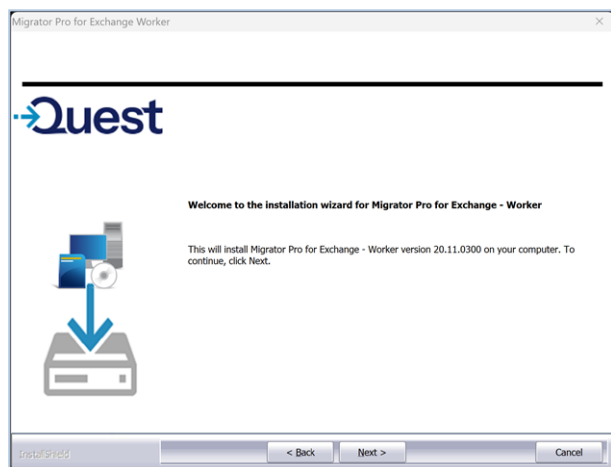
Download or copy the Migrator Pro for Exchange Public Folder Worker installation executable (*Migrator Pro for Exchange Worker Installer*) to the computer that will be used as a Public Folder Worker.

Right-click on the *Migrator Pro for Exchange Worker Installer* file and select to **Run as Administrator**. Click **Run** on the security warning.

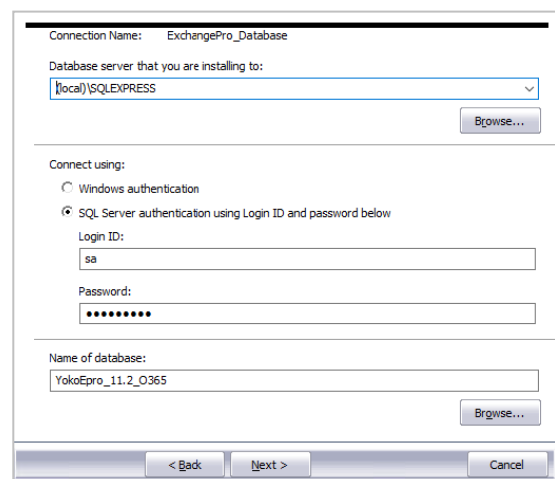
The wizard then scans your environment to gather the information it needs, and to determine whether you need to install any required prerequisite applications. They will be installed automatically if they are not present.

When the prerequisites are installed, the Migrator Pro for Exchange Worker installer *Welcome* screen appears. Click **Next**.

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



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**.



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**.

Connection Name: Logging_Database

Database server that you are installing to: [local]\SQLEXPRESS

Connect using:

Windows authentication

SQL Server authentication using Login ID and password below

Login ID: sa

Password:

Name of database: YokoEpro_11.2_O365_Log

< Back Next > Cancel

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

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.

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.

i | **NOTE:** You **must** create Outlook Profiles on the worker machines where the profile names *exactly* match the profile names configured on the main workstation.

Components of Migrator Pro for Exchange

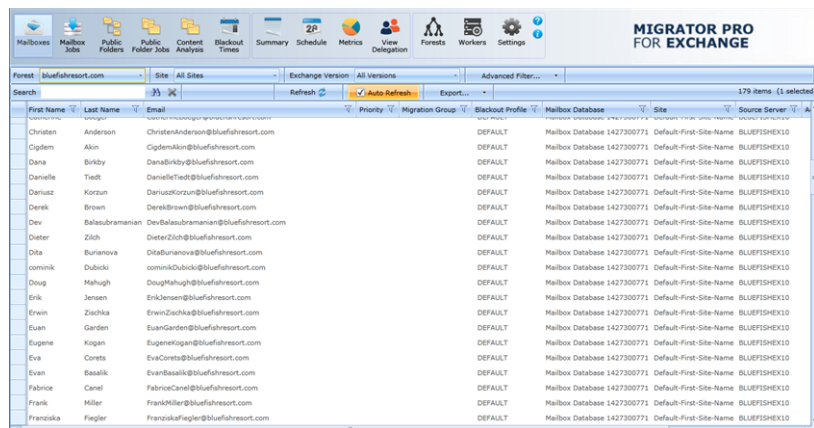
MCP Windows Service

The MCP Windows Service (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 Migrator Pro for Exchange MCP Service is started in Windows Services.

Admin Console

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

To launch the Admin Console, 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 Console opens.



The screenshot shows the Migrator Pro for Exchange Admin Console interface. The top navigation bar includes icons for Mailboxes, Mailbox Jobs, Public Folders, Public Folder Jobs, Content Analysis, Blackout Times, Summary, Schedule, Metrics, View Delegation, Forests, Workers, and Settings. The main area displays a table with columns for First Name, Last Name, Email, Exchange Version, All Versions, Advanced Filter, Priority, Migration Group, Blackout Profile, Mailbox Database, Site, and Source Server. The table contains 179 items, with 1 selected.

First Name	Last Name	Email	Exchange Version	All Versions	Advanced Filter	Priority	Migration Group	Blackout Profile	Mailbox Database	Site	Source Server
Christen	Anderson	ChristenAnderson@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Cigdem	Akin	CigdemAkin@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Dana	Erikby	DanaErikby@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Danielle	Tiedt	DanielleTiedt@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Dariusz	Kurzyn	DariuszKurzyn@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Danek	Brown	DanekBrown@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Dev	Balasubramanian	DevBalasubramanian@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Dieter	Zlich	DieterZlich@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Dita	Bulanova	DitaBulanova@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
dominik	Dubicki	dominikDubicki@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Doug	Mahugh	DougMahugh@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Erik	Jensen	ErikJensen@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Erwin	Zischka	ErwinZischka@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Euan	Garden	EuanGarden@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Eugene	Kogan	EugeneKogan@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Eva	Corsets	EvaCorsets@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Evan	Basalik	EvanBasalik@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Fabrice	Canal	FabriceCanal@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Frank	Miller	FrankMiller@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10
Franziska	Faegler	FranziskaFaegler@bluefishresort.com	14.0.0.71	14.0.0.71	Default	Default	Default	Default	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHHEX10

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.

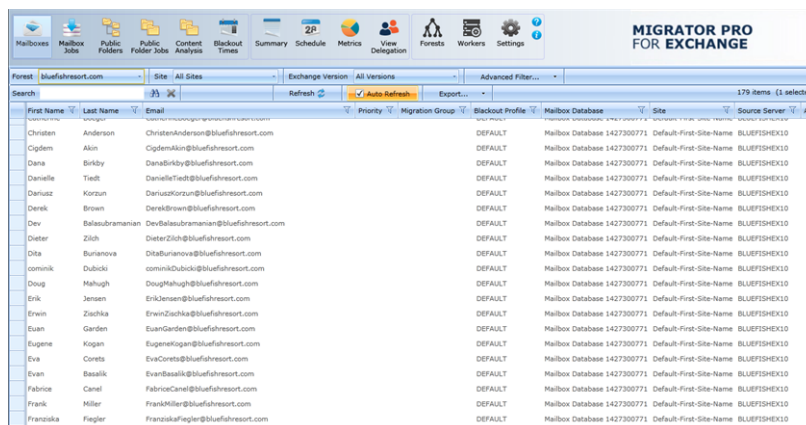
Introduction to the Admin Console

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

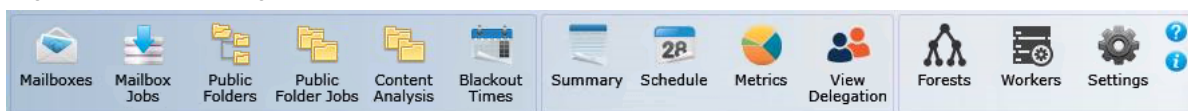
The first time you run the Admin Console after installing Migrator Pro for Exchange, the program leads you through a series of screens for you to enter your Migrator Pro for Exchange license key and configure Migrator Pro for Exchange communications with other programs and hardware. After that initial configuration, the Admin Console 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 launch the Admin Console, 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 Console opens.





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

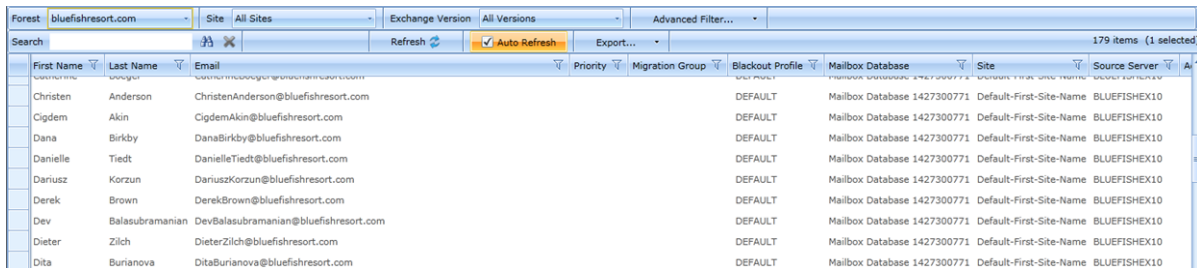


The toolbar buttons let you change the view of the Admin Console, to show different types of information and different groups of available features below the Main Toolbar:

- **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 Console also contains a Data Panel that displays data depending on the button that is currently selected.



First Name	Last Name	Email	Priority	Migration Group	Blackout Profile	Mailbox Database	Site	Source Server
Christen	Anderson	ChristenAnderson@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Cigdem	Akin	CigdemAkin@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Dana	Birkby	DanaBirkby@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Danielle	Tiedt	DanielleTiedt@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Dariusz	Korzun	DariuszKorzun@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Derek	Brown	DerekBrown@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Dev	Balasubramanian	DevBalasubramanian@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Dieter	Zilch	DieterZilch@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10
Dita	Burianova	DitaBurianova@bluefishresort.com			DEFAULT	Mailbox Database 1427300771	Default-First-Site-Name	BLUEFISHEX10

Detailed information about the Admin Console 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

See [Security Technical Implementation Guides \(STIGs\)](#) for more information.

Appendix B. Deployment in FIPS Environment

Migrator Pro for Exchange 20.11.4 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 2016 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.
 - a. Ensure this policy is enabled.
 - b. Network Security: Configure encryption types allowed for Kerberos.
 - a. Ensure the "AES128_HMAC_SHA1" and "AES256_HMAC_SHA1" values are selected.
 - b. 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..."
 - a. 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 that the website can be accessed and the browser indicates that 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](#)

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product