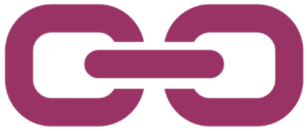
EASY365MANAGER



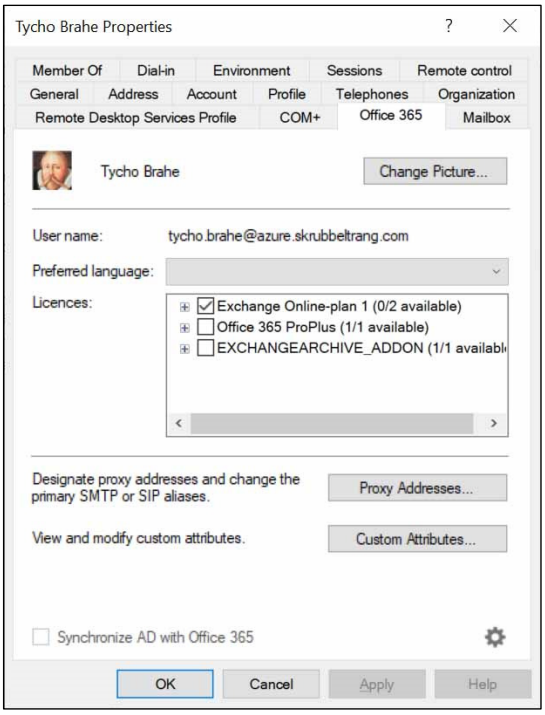
Installation and Configuration

Contents

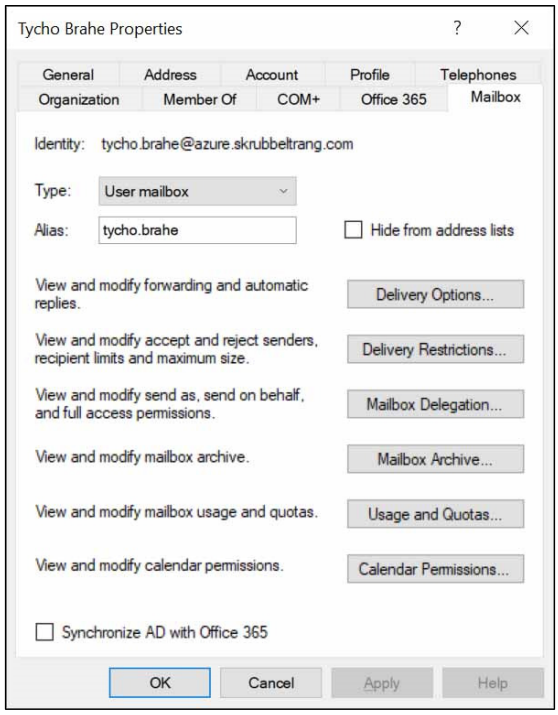
1. Introduction

Easy365Manager is a snap-in to Active Directory Users & Computers. Easy365Manager ads two new tabs to user properties, one new tab to group properties, and one new tab to contact properties.

The settings in the new tabs allow you to perform management of email attributes, Office 365 licenses, and Office 365 mailboxes without leaving AD Users & Computers.



User properties, Office 365 tab



User properties, Mailbox tab

Additionally, Easy365Manager allows you to remove your on-premises Exchange Server.

Easy365Manager is designed with the intent to make Active Directory and Office 365 mailbox and license administration as easy as possible without compromising security.

The installation, as well as the configuration, reflect this intent.

This guide shows you how to install and configure Easy365Manager.

To find the latest information and to download the most recent version of Easy365Manager, please visit:

Easy365Manager.com

2. Preparing the Installation

This section describes how you prepare for a successful installation of Easy365Manager.

Easy365Manager comes as a .msi installer and can easily be installed to or removed from your system.

Easy365Manager is a simple dll and requires no changes to your Active Directory.

Easy365Manager does not use a proprietary security subsystem. As a result, all accesses to Active Directory, Microsoft Graph, and Exchange Online work precisely as they would without Easy365Manager. Similarly, all logging of activities remains possible using the standard logging tools in Active Directory (Security Access Control Lists/SACLs) and Azure (Unified Audit Log).

2.1 Operating System

You can install Easy365Manager on any system where you use Active Directory Users & Computers. This includes your domain controller, a shared RDP management server, your domain-joined Windows client, and even your Azure AD-joined Windows client.

Supported operating systems are Windows 2012 R2 or later and Windows 8.1 or later.

Easy365Manager uses the TLS settings of your operating system and .Net Framework. If your tenant requires TLS 1.2, you must ensure your OS and .Net Framework are configured accordingly. Refer to the following article for more information:

https://www.easy365manager.com/enable-tls-1-2/

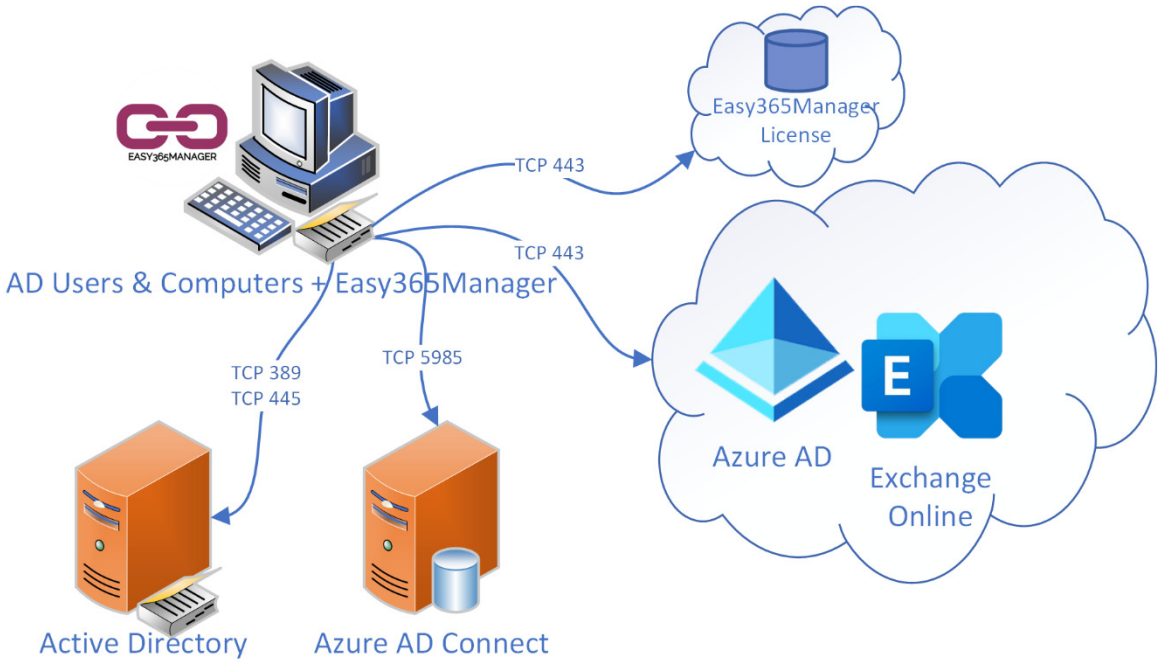
2.2 Network Communication

Easy365Manager saves you the trouble of using multiple tools, web consoles, and PowerShell for daily user management.

It does so by remotely connecting to the many systems involved in managing a hybrid AD/Office 365 environment.

As part of daily operations, Easy365Manager communicates with the following systems:

- Active Directory (AD user, group, and contact management).
- Azure AD Connect (AD-to-O365 synchronization).
- Microsoft Graph PowerShell (O365 user, group, and license management).
- Exchange Online (O365 mailbox configuration).
- Easy365Manager web service (license validation).



Active Directory communication uses LDAP, which by default is TCP 389. For secure password changes Active Directory requires secure RPC over SMB which by default is TCP 445.

Azure AD Connect uses WinRM, which by default is TCP 5985.

Microsoft Graph, Exchange Online, and Easy365Manager License service use HTTP 443.

Only your tenant name and the Easy365Manager version number are communicated to the Easy365Manager license validation service.

The Easy365Manager license validation only communicates your tenant, company name, and Easy365Manager version number. The license service is hosted on e365mwebsvc.azurewebsites.net. This currently resolves to 104.43.246.71 but may change in the future. If your firewall performs application filtering, you must allow HTTP POST.

If, due to security concerns, you don't want Easy365Manager to communicate with the Easy365Manager license service, you can use a local license key instead. Using a local license key involves some additional licensing steps and limitations: Easy365Manager cannot provide notifications regarding new versions or license expiration. Contact support@easy365manager.com for more information on how to achieve this.

Please refer to Microsoft documentation to troubleshoot network communication with the various systems.

2.3 PowerShell Version

You need to have PowerShell version 5.1 installed on your system before installing Easy365Manager.

PowerShell 5.1 is installed by default on:

- Windows Server 2016 and later.
- Windows 10 version 1607 and later.

You can check the version of PowerShell using the following command:

```
$PSVersionTable.PSVersion
```

If you don't have PowerShell version 5.1 on your system, refer to Microsoft documentation on installing it.

2.4 Active Directory Schema Version

Your Active Directory must include the Exchange schema attributes for proper integration with Office 365.

If you previously had Exchange (2010 SP2 or later) installed on-premises, your AD schema already has the attributes needed for successful integration with Office 365.

If you never had Exchange on-premises, your schema may be missing essential Exchange attributes.

Refer to the Easy365Manager knowledge base and official Microsoft documentation on identifying your Active Directory schema version and extending it with the Exchange schema attributes.

https://www.easy365manager.com/knowledgebase/the-exchange-schema-updates-are-missing-from-active-directory/

2.5 Active Directory Users & Computers

You must have AD Users & Computers installed before installing Easy365Manager.

You can check if AD Users & Computers is installed by running the following command:

```
DSA.msc
```

Refer to the following article for information on how to install AD Users & Computers:

https://www.easy365manager.com/how-to-install-rsat-remote-server-administration-tools/

2.6 Delegation of Administrative Rights

This section details the permissions needed to successfully perform user and group management in a hybrid AD/Office 365 environment.

The permissions are general and not specific to Easy365Manager, but they are listed here for your convenience.

You need to delegate the rights in advance to any administrator who will be using Easy365Manager.

2.6.1 Active Directory

To fully manage Active Directory users and groups, you need, as a minimum, the following rights:

- Create/delete User objects
- Full control of User objects
- Create/delete Group objects
- Full control of Group objects
- Create/delete Contact objects
- Full control of Contact objects

The permissions can be delegated to specific OUs via AD Users & Computers.

Refer to Microsoft documentation for further information.

2.6.2 Azure AD

To manage Azure AD user accounts and licenses, you need the following role:

- *User Administrator*

This role can be assigned via the Azure AD Portal or PowerShell.

You can limit what users are available to certain admins by using *Administrative Units*.

Refer to Microsoft documentation for further information.

2.6.2.1 Microsoft Graph Command Line Tools

All requests to Azure AD are performed using the Microsoft Graph PowerShell API (app ID: 14d82eec-204b-4c2f-b7e8-296a70dab67e). The API must be configured with consent to allow impersonation. Users need consent for the following actions:

- User.ReadWrite.All
- Group.ReadWrite.All
- Domain.Read.All
- Directory.ReadWrite.All
- offline_access

For most organizations, configuring an admin consent will be acceptable, as consent doesn't grant any new permission - it only allows the Graph API to impersonate your existing permissions. However, some organizations may require the use of individual consent.

You'll find more extensive information on API consent here, as well as a script to manage admin or user consent:

https://www.easy365manager.com/configure-microsoft-graph-powershell-for-easy365manager-delegation/

2.6.3 Exchange Online

To manage Exchange Online mailboxes, you need the following role:

- *Exchange Recipient Administrator*

This role can be assigned via the Azure AD Portal or PowerShell.

You can limit what mailboxes are available to certain admins by using *Management Role Scopes*.

Refer to Microsoft documentation for further information.

2.6.3.1 Microsoft Exchange REST API-Based PowerShell

All requests to Exchange Online are performed using the Exchange Online REST API (app ID: fb78d390-0c51-40cd-8e17-fdbfab77341b). The API does not require any consent.

2.6.4 Azure AD Connect

To perform a successful replication of Azure AD Connect, you need the following:

- *Permission to create a remote PowerShell session to the Azure AD Connect server.*
- *Permission to synchronize Azure AD Connect.*

To verify these permissions, log in to the system where you run Easy365Manager and execute the two following commands:

```
Enter-PSSession [Azure AD Connect Server]
```

```
Start-ADSyncSyncCycle -PolicyType Delta
```

If you experience any errors, read the following two sections for additional details on troubleshooting and configuring the necessary rights.

2.6.4.1 Azure AD Connect Server Remote PowerShell Permissions

To establish a remote PowerShell session, the WinRM service must be running on the Azure AD Connect server, and you need permission to execute PowerShell commands.

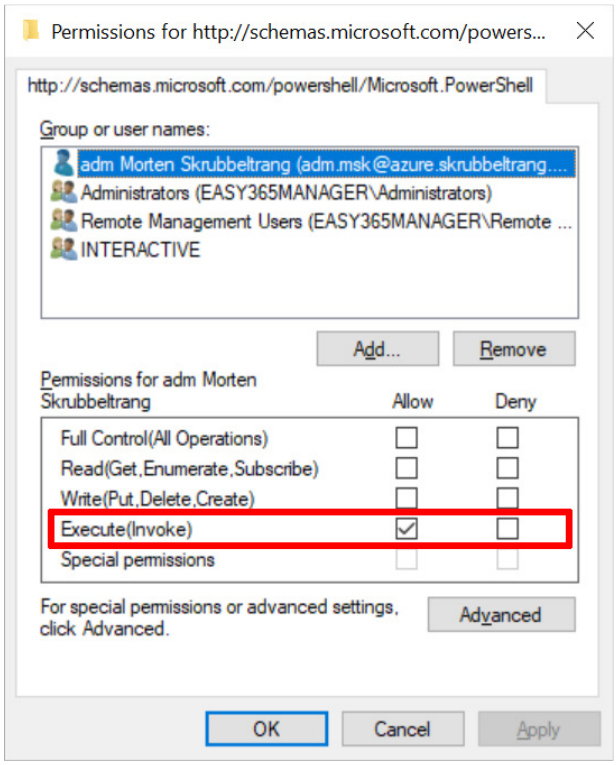
Use the following command on the Azure AD Connect server to see if the WinRM service is running:

```
(Get-Service -Name WinRM).Status
```

Use the following command on the Azure AD Connect server to see if you have Execute permissions on PowerShell:

```
Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name
Microsoft.PowerShell
```

The command opens up the PowerShell security descriptor UI. You must have Execute or Full Control permissions:



You need remote PowerShell permissions even if Easy365Manager is installed directly on your Azure AD Connect Server.

Refer to Microsoft documentation for further information on how to allow Azure AD Connect synchronization and how to allow remote PowerShell sessions.

2.6.4.2 Azure AD Connect Synchronization Permissions

To synchronize Azure AD Connect, you must be a member of the ADSyncOperators group at a minimum.

If Azure AD Connect is installed on a member server, this group is a local computer group.

If Azure AD Connect is installed on a domain controller, this is a domain local group.

2.7 How to Run Easy365Manager From an Azure AD Domain Joined PC

You need to take additional configuration steps to run Easy365Manager from an Azure AD domain joined PC:

- Ensure proper client DNS integration with your on-premises Active Directory.
- Configure Windows Credential Manager with credentials to access your preferred domain controller and your Azure AD Connect Server.
- Configure the WSMAN TrustedHosts list on your local client to enable remote PowerShell connection to your Azure AD Connect Server
- Configure AD Users & Computers for first use.

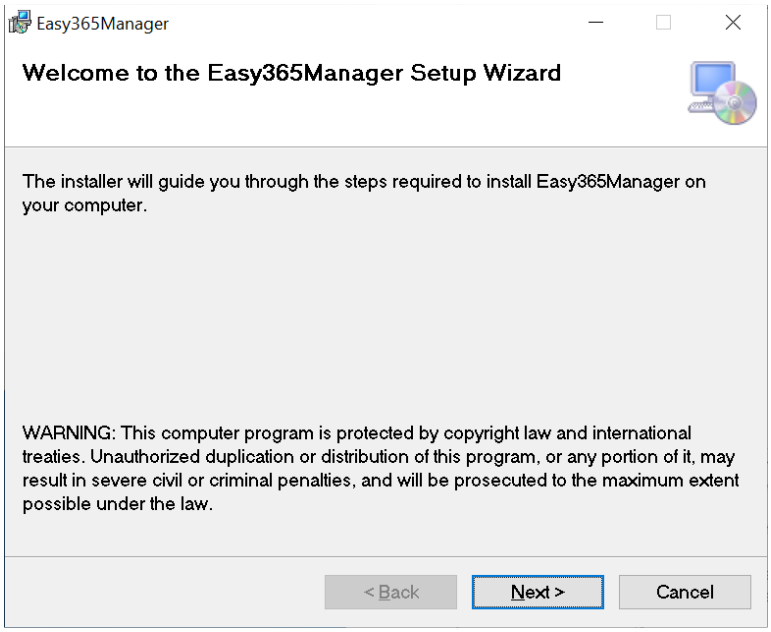
Refer to the following article for more details on how to set up Easy365Manager to run on an Azure AD domain-joined PC:

https://www.easy365manager.com/knowledgebase/how-to-run-easy365manager-from-an-azure-ad-domain-joined-pc/

3. Performing the Installation

Once all prerequisites are met, you can run the .msi installation file on your system.

Unless you want to change the default installation folder, there is nothing to customize.



3.1 Unattended Installation

Easy365Manager supports unattended installation and removal.

Use the following command to perform an unattended installation:

```
msiexec /package Easy365Manager-v1.8.3-x64.msi /quiet
```

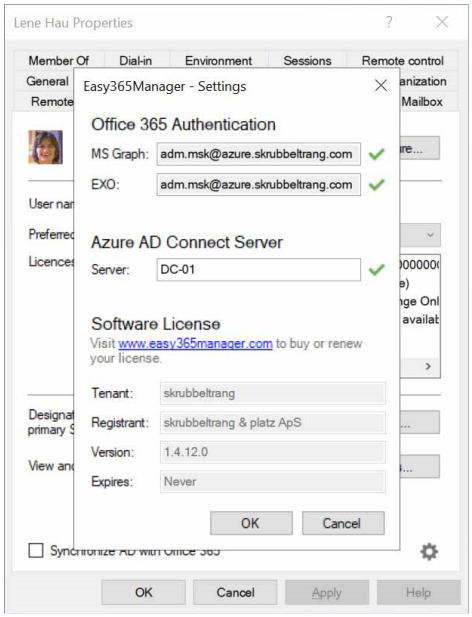
Use the following command to perform an unattended removal:

```
msiexec /uninstall Easy365Manager-v1.8.3-x64.msi /quiet
```

4. Post-Installation Configuration

On the first run, after installing Easy365Manager, you must authenticate with Microsoft Graph PowerShell and Exchange Online. Additionally, you must specify your Azure AD Connect Server.

This is done via the Easy365Manager Settings form, which opens automatically the first time you access (any) user properties and select the “Office 365” or “Mailbox” tab:



After successful authentication, the form will show your license expiration date. You can always access the settings form via the configuration cog in the bottom right corner of the Office 365 tab.

4.1 Office 365 Authentication

Click the MS Graph textbox to authenticate with Microsoft Graph PowerShell.

Click the EXO textbox to authenticate with Exchange Online.

Both MS Graph and Exchange Online authentication use OAuth2 authentication, which includes the following advantages:

- Easy365Manager will never know your credentials.
- Easy365Manager supports multi-factor authentication (MFA).

If authentication is successful, Easy365Manager receives an access token which is encrypted and cached to disk. The token is protected by the user and machine passwords of the system where Easy365Manager is running.

The caching of the token ensures that you don’t need to authenticate every time you use Easy365Manager.

You can remove the cached token and Azure AD Connect information from your system by deleting the user.config file found in your user profile:

```
C:\Users\[username]\AppData\Local\Microsoft_Corporation\
_Easy365Manager,_Version=_Path_[string]\[id]
```

4.2 Azure AD Connect Server

Insert the name of your Azure AD Connect Server. You must use the hostname or FQDN (fully qualified domain name). Specifying the Azure AD Connect server by IP address is not allowed.

5. Operational Notes

This section covers a few things to be aware of to get the best experience running Easy365Manager.

5.1 AD Search Results With Easy365Manager Tabs

When you do a regular search in AD Users & Computers and open up properties of users, groups, or contacts, a minimal set of tabs are displayed. This is expected behavior as AD Users & Computers search results disregard some tabs like the Attributes tab and tab extensions.

To get access to Easy365Manager in search results performed in AD Users & Computers, follow these instructions:

https://www.easy365manager.com/knowledgebase/how-to-search-for-a-user-and-show-the-easy365manager-tabs/

5.2 Domain Controller Selection

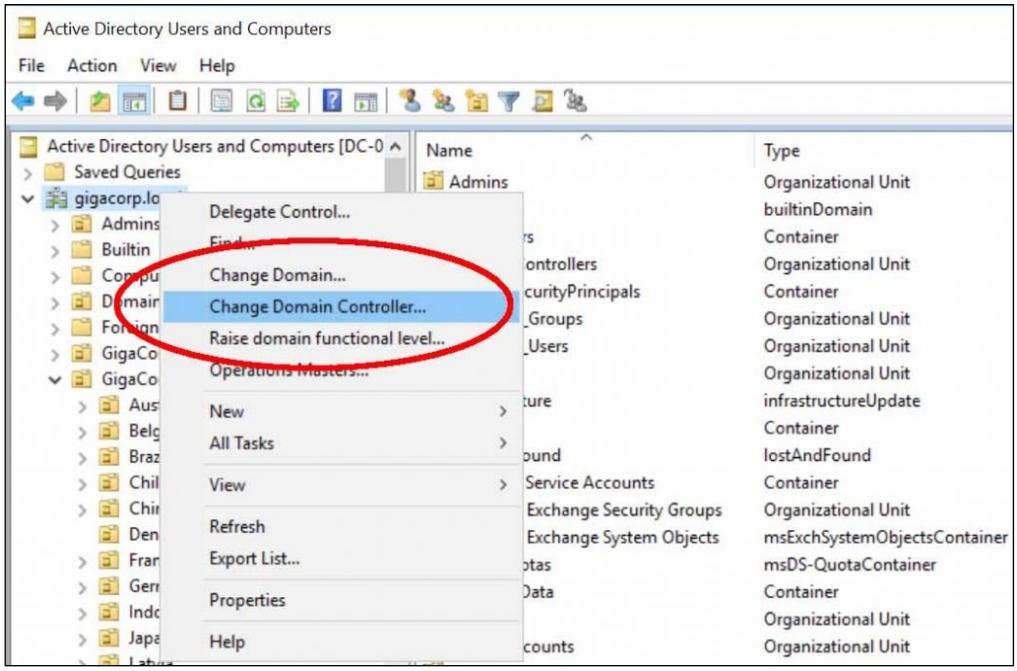
To ensure your Active Directory changes are replicated as quickly as possible to Azure AD, you must make your AD changes on the Domain Controller preferred by Azure AD Connect.

This is a general guideline that is not specific to Easy365Manager.

Use the following command on your Azure AD Connect server to identify the preferred Domain Controller:

```
((Get-ADSyncConnector).Partitions.Parameters | ? {$_.Name -eq 'last-dc'}).value
```

Once the Domain Controller is identified, make sure AD Users & Computers is connected to this Domain Controller:



5.3 Software Updates

Easy365Manager will notify you whenever new updates are available. Notifications will occur no later than 14 days after the new update is available.

First-level supporters who don't have permission to update Easy365Manager (e.g., on a shared management server) can disable software update notifications by selecting "Disabled (for any update)" in the notification.

5.4 License Renewal

Easy365Manager will notify you when your license is 30 days away from expiration. Click on the link in the notification to renew your Easy365Manager license.

Renewing your Easy365Manager license will add another year to your current expiration date, so you should renew the license as soon as possible to avoid downtime.

You can disable license renewal notifications by selecting "Disabled" in the notification.

6. Troubleshooting

If you are having trouble installing or configuring Easy365Manager, please refer to the online knowledgebase:

https://easy365manager.com/knowledgebase

For further assistance, contact your software vendor (if you bought Easy365Manager from a partner) or contact Easy365Manager support (if you purchased Easy365Manager directly from us).

You'll find contact information for Easy365Manager here:

https://easy365manager.com/contact