

EasyEntra



Installation and Configuration

Contents

1.	Introduction	3
2.	Preparing the Installation	5
2.1	Operating System	5
2.2	Network Communication	5
2.3	Active Directory Schema Version	6
2.4	Delegation of Administrative Rights	7
2.4.1	Active Directory	7
2.4.2	Entra ID	7
2.4.3	Exchange Online.....	8
2.4.4	SharePoint Online	9
2.4.5	Microsoft Entra Connect	9
3.	Performing the Installation	11
3.1	Unattended Installation	11
4.	Post-Installation Configuration.....	12
4.1	Configuring the AD Connection(s)	12
4.2	Configuring the Entra ID Connection(s)	14
4.3	Microsoft 365 Authentication	14
4.4	Microsoft Entra Connect Server.....	15
5.	Operational Notes	16
5.1	Domain Controller Selection.....	16
5.2	Software Updates.....	16
5.3	License Renewal	17
6.	Troubleshooting	18

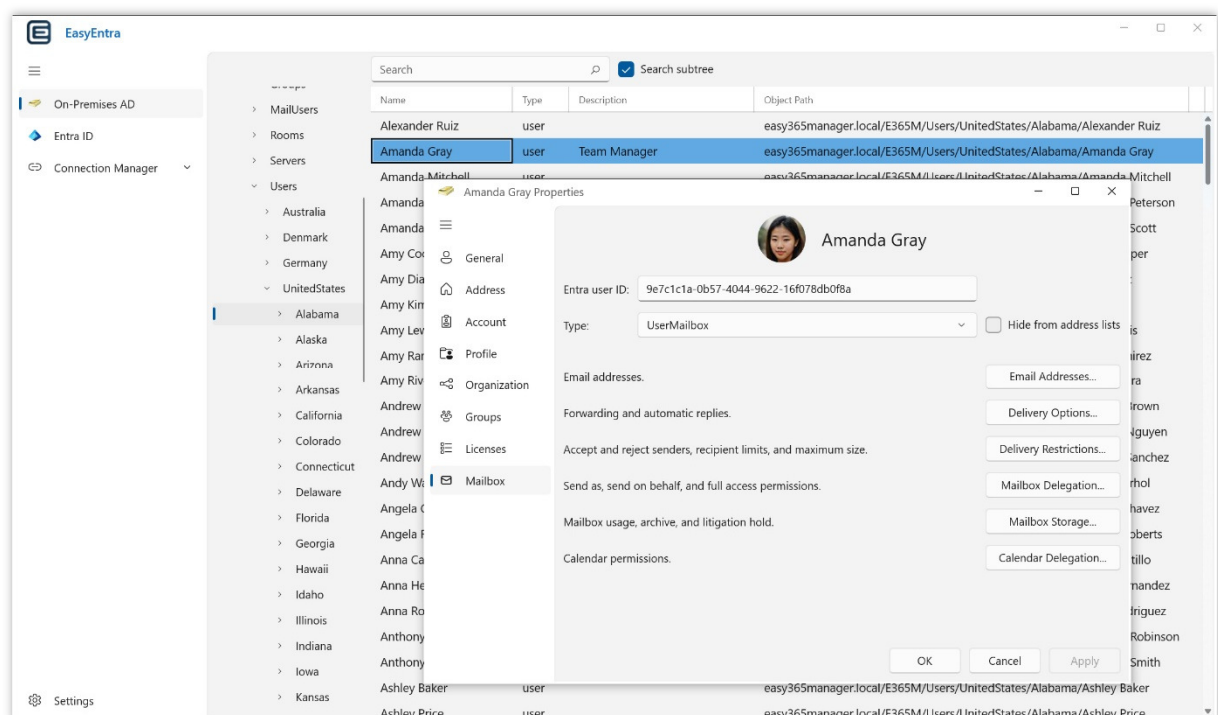
1. Introduction

EasyEntra embodies our vision to transform hybrid and cloud-only Entra ID management into a cost-effective and genuinely pleasant experience for companies worldwide.

EasyEntra offers a single pane of glass to manage one or more Active Directories and one or more Entra ID tenants in a simple, intuitive, and highly responsive UI.

EasyEntra's primary target audience is the first-level support teams of organizations using Active Directory, Entra ID, or both.

The visual design of EasyEntra is intentionally familiar, closely mimicking the design of AD Users & Computers (ADUC). This familiarity practically eliminates the need for training, making the transition from standard tools to EasyEntra a breeze.



With EasyEntra, first-line support teams no longer need to worry about attribute authority, using PowerShell, or slow-performing web consoles. All daily operations are available in a consolidate, intuitive and highly responsive GUI.

The security design of EasyEntra does not include a proprietary security subsystem. All access permissions to Active Directory, Microsoft Graph, and Exchange Online are evaluated exactly as they are with the native tools. Similarly, all logging of activities remains possible using the highly trusted and certified native logging mechanisms in Active Directory (Security Access Control Lists/SACLs) and Entra ID (Unified Audit Log).

Compared to other similar solutions, this design eliminates the need for a central server or database, and provides easier troubleshooting of permissions issues (only native security), easy fallback to standard tools (same permissions apply), and zero vendor lock-in.

Additionally, EasyEntra enables you to remove your on-premises Exchange Server without resorting to PowerShell for daily user management. And without compromising security.

This guide shows you how to install and configure EasyEntra.

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

[EasyEntra.com](https://www.easyentra.com)

2. Preparing the Installation

This section describes how you prepare for a successful deployment of EasyEntra.

EasyEntra comes as a .msi installer, and can be easily installed on or removed from your system.

EasyEntra is a simple executable and requires no services or changes to your Active Directory.

EasyEntra 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 EasyEntra. Similarly, all logging of activities remains possible using the highly trusted and certified native logging tools in Active Directory (Security Access Control Lists/SACLs) and Entra ID (Unified Audit Log).

The security design of EasyEntra eliminates the need for a central server or database, easier troubleshooting of permissions issues (only native security), easy fallback to standard tools (same permissions apply), and zero vendor lock-in.

2.1 Operating System

Supported operating systems are Windows 10 or later and Windows Server 2019 or later.

You can install EasyEntra on your domain-joined Windows client, shared management server, Domain Controller, and even Entra ID-joined or standalone Windows clients.

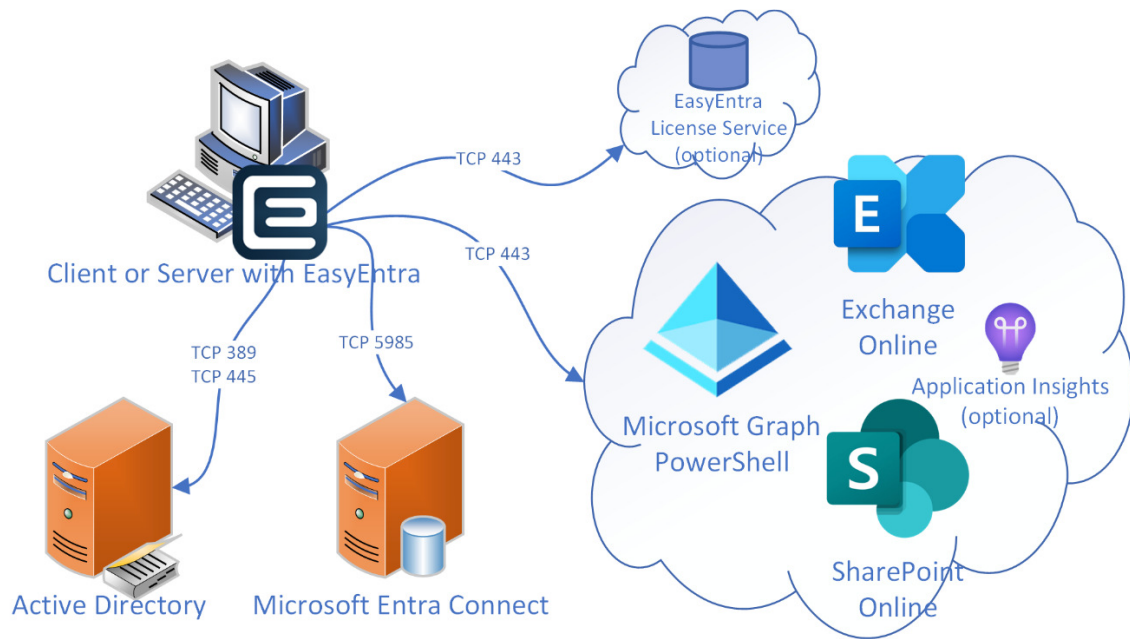
2.2 Network Communication

EasyEntra 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/Microsoft 365 environment.

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

- Active Directory (AD user, group, contact, and computer management).
- Microsoft Entra Connect (AD-to-Entra ID synchronization).
- Microsoft Graph PowerShell (Entra ID user, group, and license management).
- Exchange Online (Exchange Online mailbox management).
- SharePoint Tenant Administration API.
- Application Insights (optional).
- EasyEntra 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.

Microsoft Entra Connect uses WinRM, which by default is TCP 5985.

Microsoft Graph, Exchange Online, Application Insights, and the EasyEntra License Service use HTTP 443.

The EasyEntra license validation only communicates your tenant and company name, user count, and EasyEntra version number. The license service is hosted on license.easyentra.com (currently 104.43.246.71 - subject to change) and e365mweb.azurewebsites.net (currently 104.43.246.71 - subject to change). If your firewall performs application filtering, you must allow HTTP POST.

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

Application Insights only reports a minimal anonymous stack trace in case of application failures. No client data is included. Error reporting is optional (opt-in) and is enabled in EasyEntra settings.

Please refer to Microsoft documentation to troubleshoot network communication with AD, Entra Connect, Entra ID, and Exchange Online.

2.3 Active Directory Schema Version

If you're using EasyEntra for hybrid management, your Active Directory must include the Exchange schema attributes for proper integration with Microsoft 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 Microsoft 365.

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

Please refer to the EasyEntra knowledge base and official Microsoft documentation for instructions on identifying your Active Directory schema version and extending it with the Exchange schema attributes.

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

You can ignore the AD schema version if you intend to use EasyEntra for cloud-only management.

2.4 Delegation of Administrative Rights

This section details the permissions needed to manage users, groups, contacts, and computers in a hybrid AD/Microsoft 365 environment.

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

Delegate these rights in advance to any administrator who will use EasyEntra.

2.4.1 Active Directory

To fully manage Active Directory users, groups, contacts, and computers, you need 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
- Create/delete Computer objects
- Full control of Computer objects

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

Refer to Microsoft documentation for further information.

2.4.2 Entra ID

To manage Entra ID user accounts, mailboxes, and licenses, you need the following roles:

- *User Administrator*
- *Exchange Recipient Administrator*
- *Authentication Administrator (optional, for MFA management)*
- *Reports Reader (optional, for report generation)*
- *Cloud Device Administrator (optional, for LAPS and BitLocker management)*
- *SharePoint Administrator (optional, for OneDrive management)*

These roles can be assigned via the Entra ID Portal or PowerShell, with or without PIM.

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

Refer to Microsoft documentation for further information.

2.4.2.1 Microsoft Graph Command Line Tools

All requests to Entra ID are performed using the Microsoft Graph PowerShell API (app ID: **14d82eec-204b-4c2f-b7e8-296a70dab67e**). You must configure the API with consent to allow impersonation. Users need consent to the following actions:

- User.ReadWrite.All
- Group.ReadWrite.All
- Device.ReadWrite.All
- UserAuthenticationMethod.ReadWrite.All
- Domain.Read.All
- Sites.Read.All
- Reports.Read.All
- AuditLog.Read.All
- Directory.AccessAsUser.All
- DeviceLocalCredential.Read.All
- BitLockerKey.Read.All
- Mail.ReadWrite.Shared
- Calendars.Read.Shared
- Contacts.Read.Shared
- RoleEligibilitySchedule.Read.Directory
- RoleAssignmentSchedule.ReadWrite.Directory
- offline_access

For most organizations, configuring an Admin Consent will be acceptable, as it doesn't grant any new permission - it only allows the API to impersonate user credentials. However, some organizations may require individual consent.

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

<https://EasyEntra.com/configure-microsoft-graph-powershell-for-easyentra-delegation/>

2.4.3 Exchange Online

To manage Exchange Online mailboxes, you need the Entra ID role *Exchange Recipient Administrator* (see section 2.4.2).

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

You don't need any explicit Exchange Admin Roles. The Entra ID role *Exchange Recipient Administrator* role corresponds to the Exchange Admin role *Recipient Management*.

Notice: To create MailEnabledSecurity groups and modify their membership, you must have the Exchange Permission *Security Group Creation and Membership* or equivalent. For least privilege access, assign it via a custom Exchange Admin Role.

Refer to Microsoft documentation for further information.

2.4.3.1 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**). This API does not require any consent.

2.4.4 SharePoint Online

To manage users' OneDrive settings and delegation in EasyEntra, you need the Entra ID role *SharePoint Administrator* (see section 2.4.2).

Refer to Microsoft documentation for further information.

2.4.4.1 Microsoft SharePoint REST API-Based PowerShell

All requests to SharePoint Online are performed using the SharePoint Online REST API (app ID: 9bc3ab49-b65d-410a-85ad-de819febddc). This API does not require any consent.

2.4.5 Microsoft Entra Connect

To perform a successful replication of Microsoft Entra Connect, you need the following:

- *Permission to create a remote PowerShell session to the Microsoft Entra Connect server.*
- *Permission to synchronize Microsoft Entra Connect.*

To verify these permissions, log on to the system where you run EasyEntra and start a PowerShell prompt using the same credentials as when running EasyEntra. Execute the two following commands:

```
Enter-PSSession [Microsoft Entra 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.

2.4.5.1 Microsoft Entra Connect Server Remote PowerShell Permissions

To establish a remote PowerShell session, the WinRM service must be running on the Microsoft Entra Connect Server, and you need permission to execute PowerShell commands.

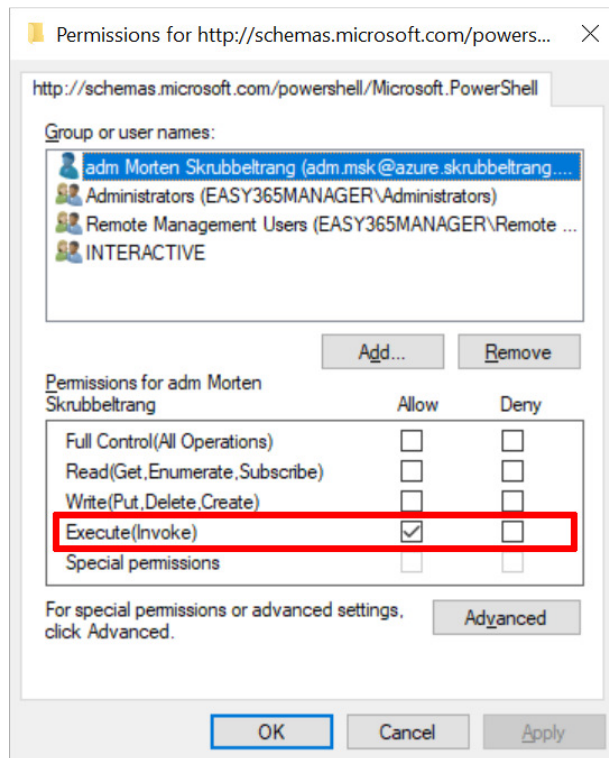
Use the following command on the Microsoft Entra Connect Server to see if the WinRM service is running:

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

Use the following command on the Microsoft Entra 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 in the ACL:



You need remote PowerShell permissions even if EasyEntra is installed directly on your Microsoft Entra Connect Server.

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

2.4.5.2 Entra ID Connect Synchronization Permissions

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

If Microsoft Entra Connect is installed on a member server, this group is a local computer group.

If Microsoft Entra Connect is installed on a domain controller, this is a domain local group.

2.4.5.3 How to Run EasyEntra From an Entra ID Domain-Joined PC

You need to take additional configuration steps to run EasyEntra from an Entra ID 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 Microsoft Entra Connect Server.
- Configure the WSMAN TrustedHosts list on your local client to enable remote PowerShell connection to your Microsoft Entra Connect Server
- Configure AD Users & Computers for first use.

Refer to the following article for more details on how to set up EasyEntra to run on an Entra ID domain-joined PC:

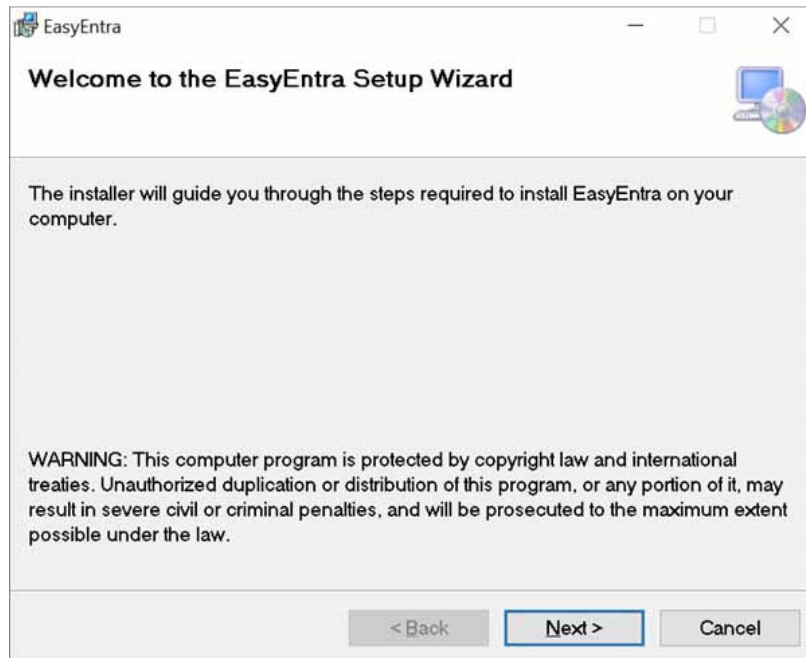
<https://easyentra.com/knowledge-base/how-to/how-to-run-easy-entra-from-an-entra-id-domain-joined-pc/>

If you use EasyEntra for cloud-only management, you don't need additional configuration steps.

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

EasyEntra supports unattended installation and removal.

Use the following command to perform an unattended installation:

```
msiexec /package EasyEntra-v0.0.37-x64.msi /quiet
```

Use the following command to perform an unattended removal:

```
msiexec /uninstall EasyEntra-v0.0.37-x64.msi /quiet
```

(Replace the .msi file name with the actual version being installed/removed.)

4. Post-Installation Configuration

You can use EasyEntra to manage pure Active Directory, cloud-only Entra ID, and hybrid environments (Active Directory synchronized with Entra ID).

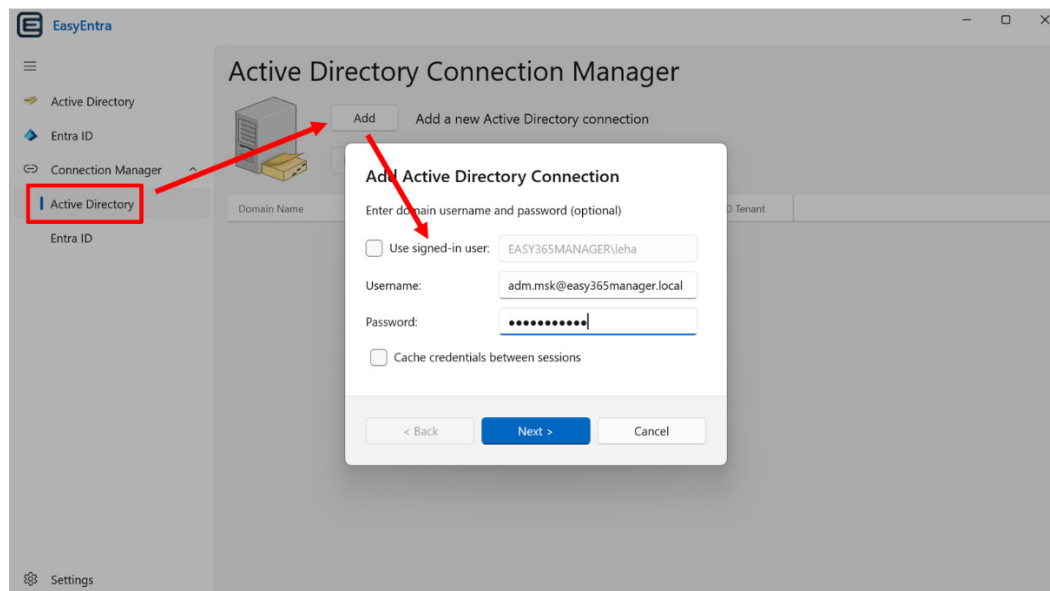
- Use the *Active Directory Connection Manager* to connect with an Active Directory.
- Use the *Entra ID Connection Manager* to connect with an Entra ID.
- Use *both Connection Managers* to connect with a hybrid environment.

You can manage any number of Active Directories and Entra ID tenants side-by-side.

4.1 Configuring the AD Connection(s)

By default, EasyEntra will interact with Active Directory (domain controllers) and Microsoft Entra Connect using the security context of the application process token, just like AD Users & Computers. Therefore, you must start EasyEntra using a privileged account.

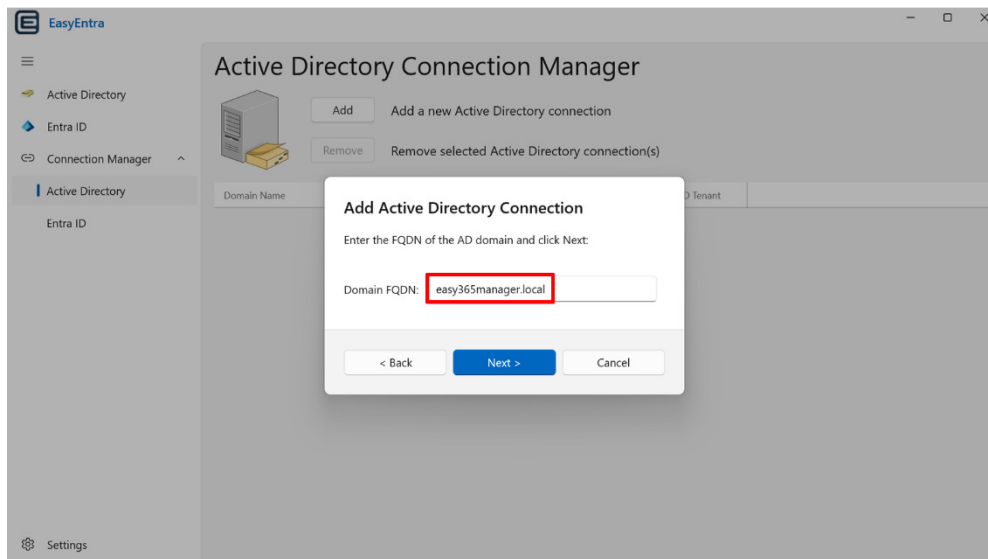
Apart from using the identity of the process token, EasyEntra offers an additional method of authentication: In-app authentication.



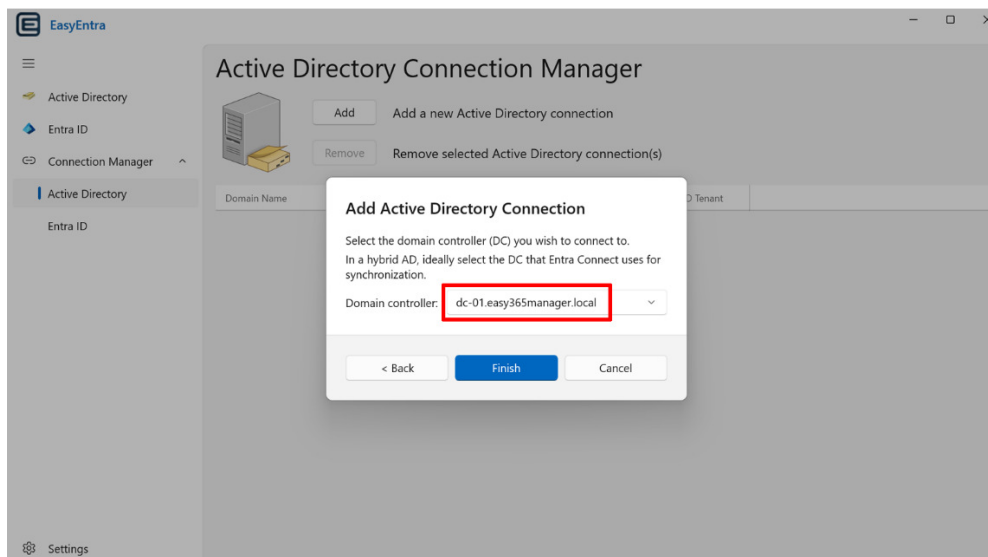
In-app authentication has two benefits:

1. You can easily connect to your AD from non-domain PCs (e.g., Entra joined workstations).
2. Your process will not expose admin credentials, providing full protection from token theft.

After you select your authentication method and click Next, you must enter the FQDN of the AD domain you wish to connect:



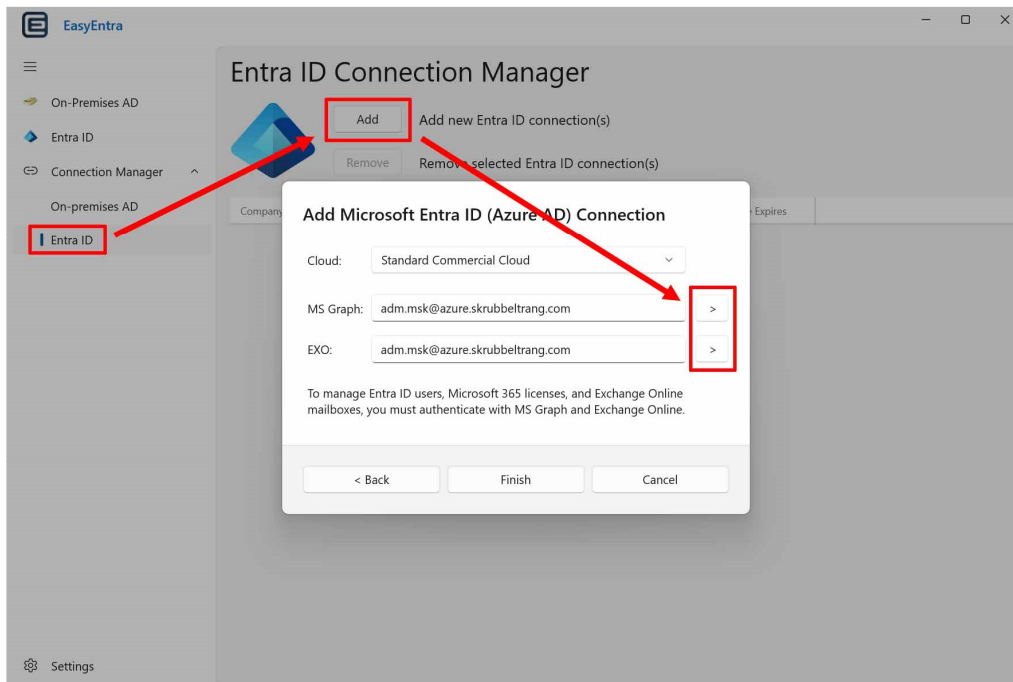
Click Next and select the domain controller you wish to connect with. Optimally, choose the domain controller from which Entra Connect is synchronizing for minimal latency:



In a hybrid environment, you must also connect with your Entra ID tenant (see next section).

4.2 Configuring the Entra ID Connection(s)

To connect to one or more Entra ID tenants, go to Connection Manager -> Entra ID -> Click Add -> Select Primary Tenant and click Next. Log in to MS Graph and EXO and click Finish:



Your tenant will auto-associate with your AD in EasyEntra if you have a standard single-AD single-tenant environment.

You must explicitly configure your AD connection to associate with the desired tenant if you have multiple tenants or multiple AD domains.

4.3 Microsoft 365 Authentication

Click the MS Graph login button to authenticate with Microsoft Graph PowerShell.

Click the EXO login button to authenticate with Exchange Online.

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

- EasyEntra will never know your credentials.
- EasyEntra supports multi-factor authentication (MFA), FIDO2, and Conditional Access Policies.

If authentication is successful, EasyEntra 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 EasyEntra is running.

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

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

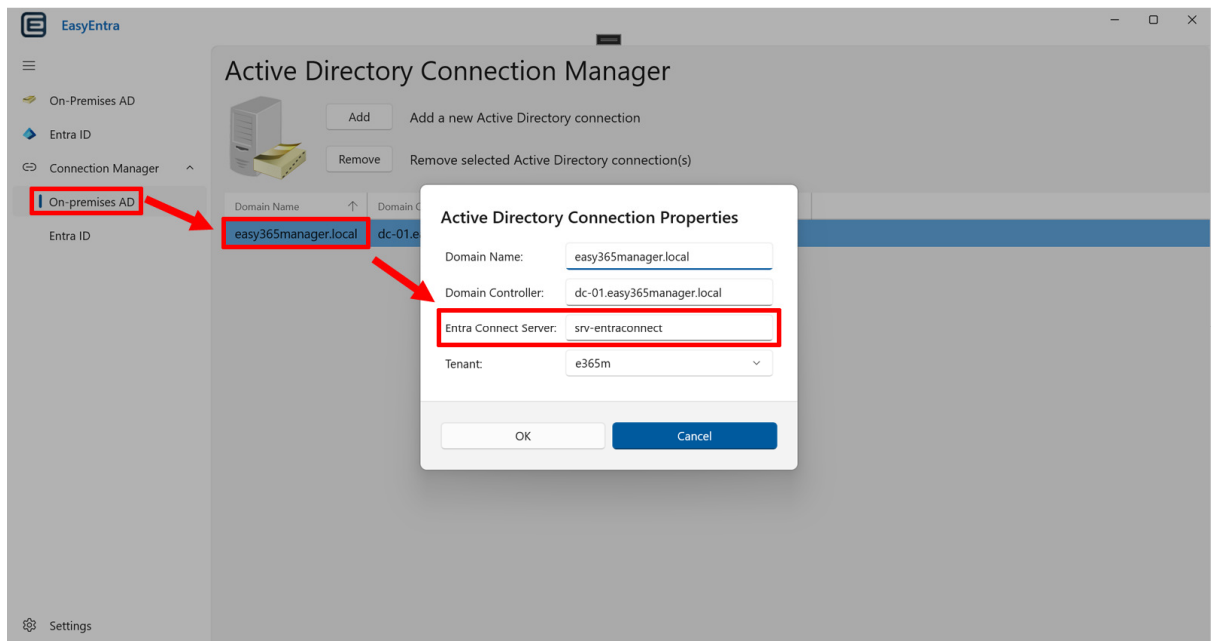
`C:\Users\[username]\AppData\Local\EasyEntra\EasyEntra_Config.json`

Alternatively, you can start PowerShell 7 and run the following CmdLet:

Reset-EEConfiguration

4.4 Microsoft Entra Connect Server

Go to Connection Manager -> On-Premises AD -> Double click your AD Connection -> Enter the name of your Microsoft Entra Connect Server and click OK:



You must use the hostname or FQDN (fully qualified domain name). Specifying the Microsoft Entra 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 EasyEntra.

5.1 Domain Controller Selection

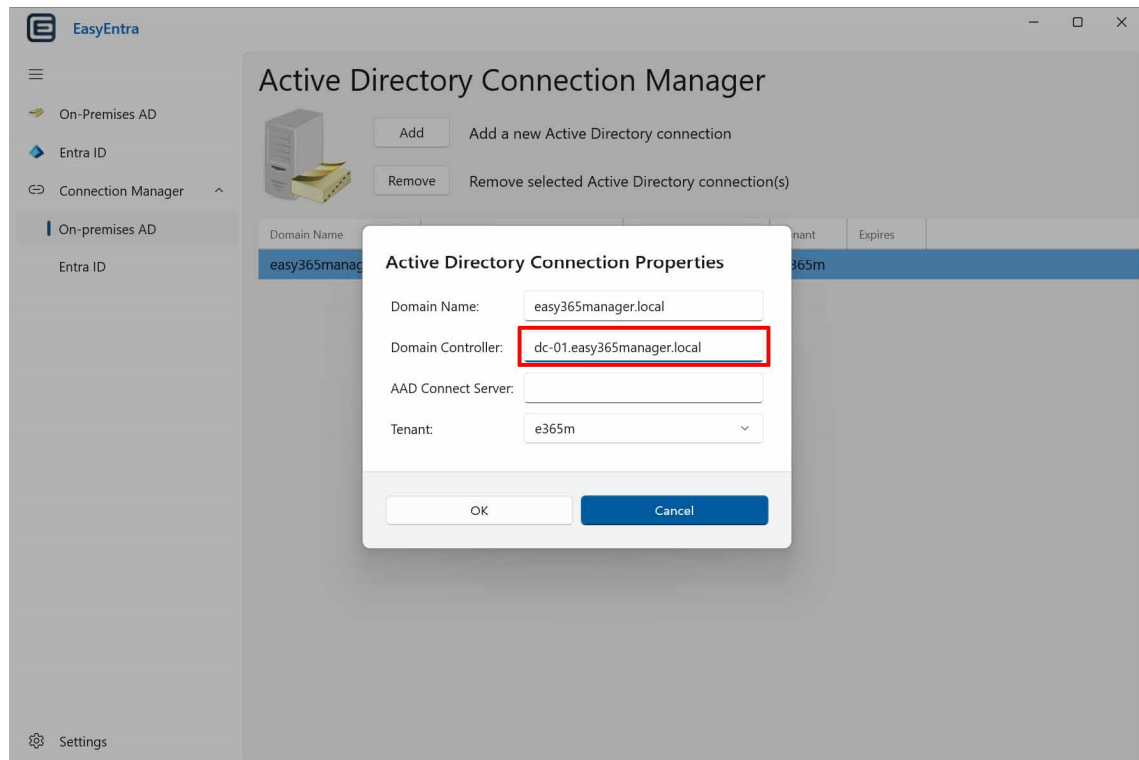
To ensure your Active Directory changes are replicated as quickly as possible to Entra ID, you must make your AD changes on the Domain Controller preferred by Microsoft Entra Connect.

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

Use the following command on your Microsoft Entra 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 your On-Premises AD Connection is configured to use this Domain Controller:



5.2 Software Updates

EasyEntra 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 EasyEntra (e.g., on a shared management server) can disable software update notifications by selecting "Disabled (for any update)" in the notification.

5.3 License Renewal

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

Renewing your EasyEntra 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 EasyEntra, please refer to the online knowledge base:

<https://EasyEntra.com/knowledge-base>

For further assistance, contact EasyEntra support.

You'll find contact information for EasyEntra here:

<https://EasyEntra.com/contact-support/>