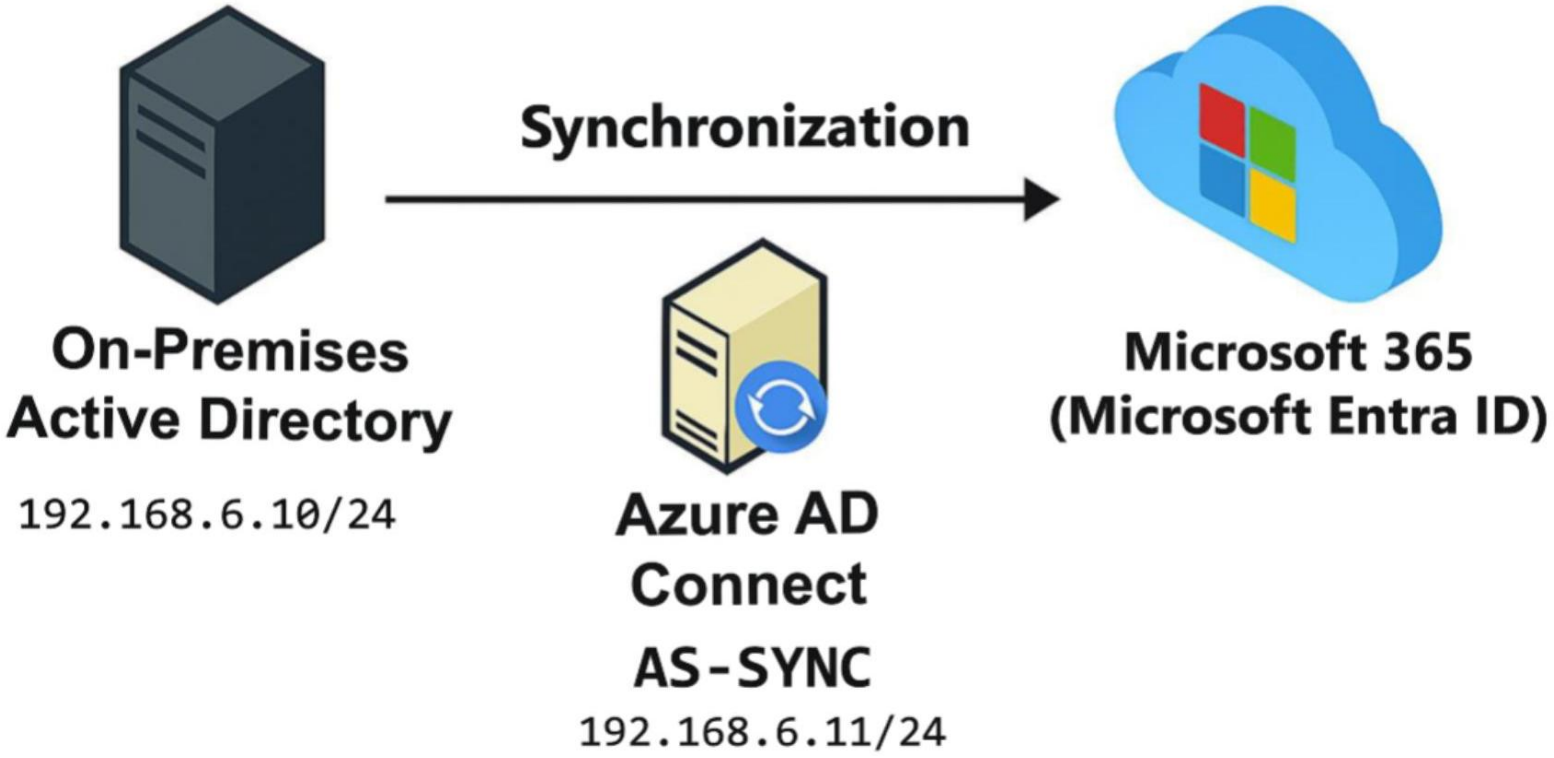
Active Directory Sync With Microsoft 365

Using Azure AD Connect (Hybrid Identity Project)



❑ Overview

This project demonstrates the implementation of a hybrid identity environment by integrating an on-premises Active Directory domain with Microsoft 365 (Microsoft Entra ID). Azure AD Connect was installed on a dedicated sync server (AS-SYNC) to enable directory synchronization and password hash synchronization.

❑ Objective

To provide seamless identity access for users across on-prem systems and Microsoft 365 services, enabling Single Sign-On (SSO), centralized identity management, and secure cloud access.

❑ Outcome

User accounts from the on-prem AD were successfully synchronized to Microsoft 365, allowing consistent authentication across local and cloud environments.

WHAT IS AD SYNC?

ACTIVE DIRECTORY SYNC (AZURE AD CONNECT)

- Connects your local Active Directory to Microsoft 365 (Azure AD)
- Syncs users, groups, and passwords from on-prem AD to cloud
- Keeps both directories updated automatically tv
- Lets users sign in to Outlook, Teams, OneDrive with same username and password they use on their office computer
- Improvees identity management and gives users a smoother login experience

WHY WE DO AD SYNC?

We do AD Sync to make user management easier and more secure.

- Without sync, admins would need to manage users separately in local AD and Microsoft 365
- AD Sync keeps data consistent in both places
- When a password or user detail changes in on-prem AD, it updates in Microsoft 365 automatically
- Users only need one username and password for their computer, Outlook, Teams, and OneDrive
- Makes IT admin work much faster and reduces mistakes

MAIN PURPOSE OF AD SYNC

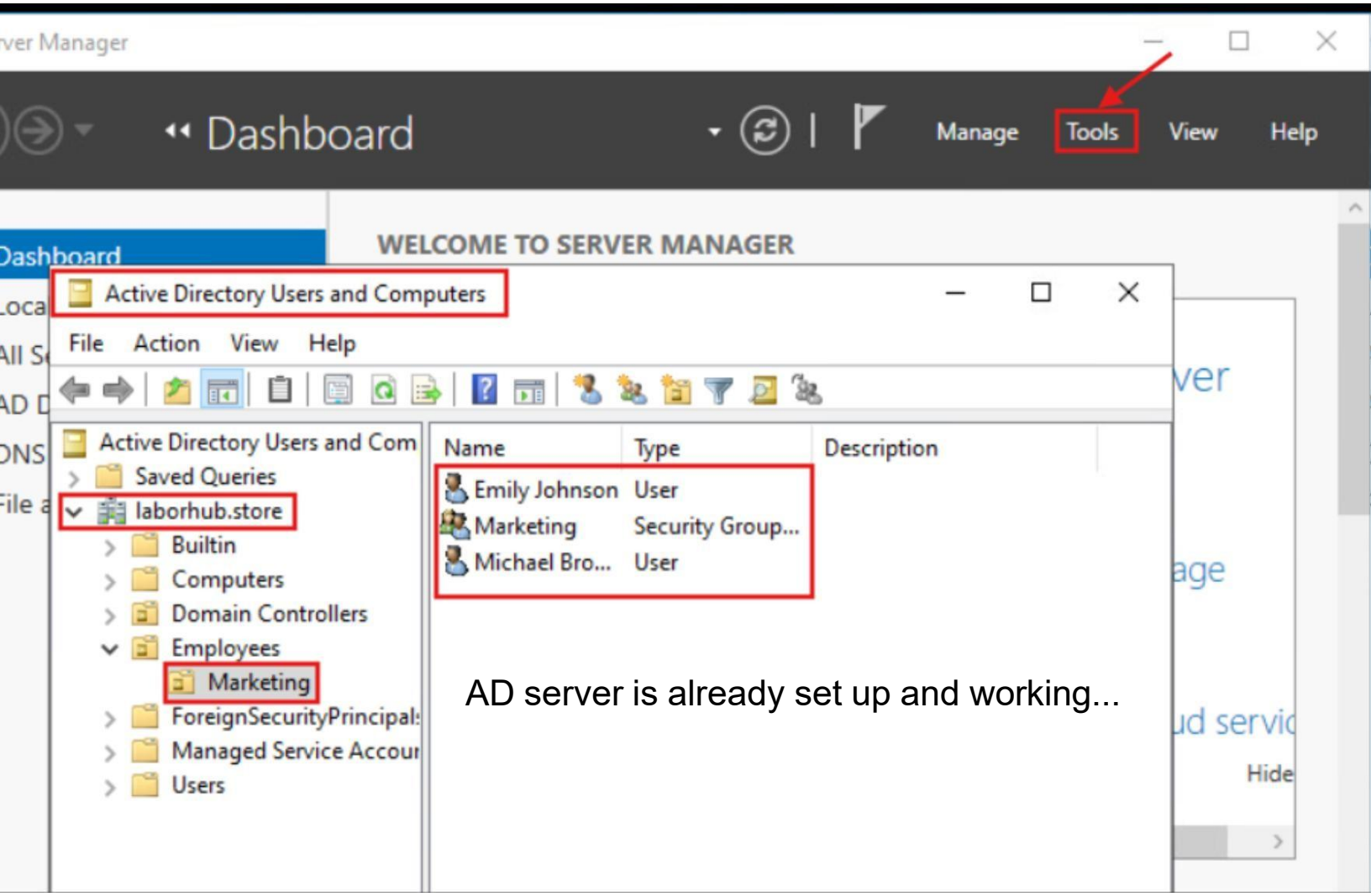
The main purpose of AD Sync is to give users one identity that works everywhere.

- Maintains same users, groups, and passwords in both on-prem AD and Microsoft 365
- Provides single sign-on (SSO) for cloud and local services
- Makes login easier for users with one set of credentials
- Centralizes user management in one place
- Improves security by ensuring all identity changes sync to the cloud
- Saves admin time and gives a smooth login experience for everyone

AD server is already set up and working:

It has Active Directory installed.
It uses a static IP address: 192.168.6.10/24.
It is domain joined with the domain name laborhub.store.
Inside Active Directory, you already have users and groups (for example, Emily Johnson and Michael Brown under the Marketing OU).

So now, you don't need to create new users. The next step is just to sync these existing on-premises users to Microsoft 365 (Azure AD) using Azure AD Connect. This will allow the same accounts to work in the cloud for services like Outlook, Teams, and OneDrive.



Sync Server Configuration (AS-SYNC)

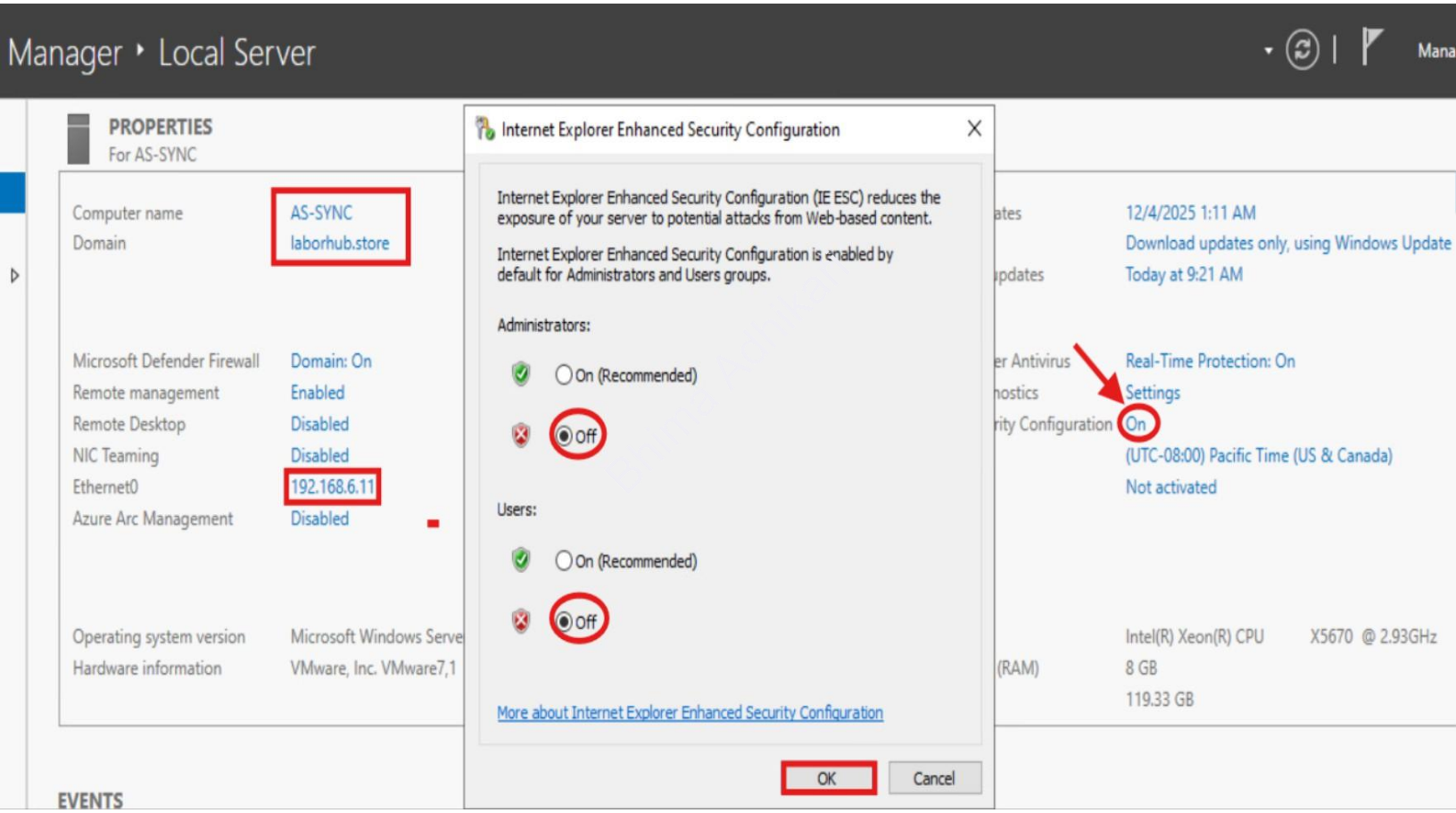
Computer Name: AS-SYNC
Domain: laborhub.store
Static IP: 192.168.6.11
Purpose: This server is prepared for installing Azure AD Connect to sync on-premises AD users to Microsoft 365.

Additional Configuration

IE Enhanced Security Configuration: Turned Off for both Administrators and Users.

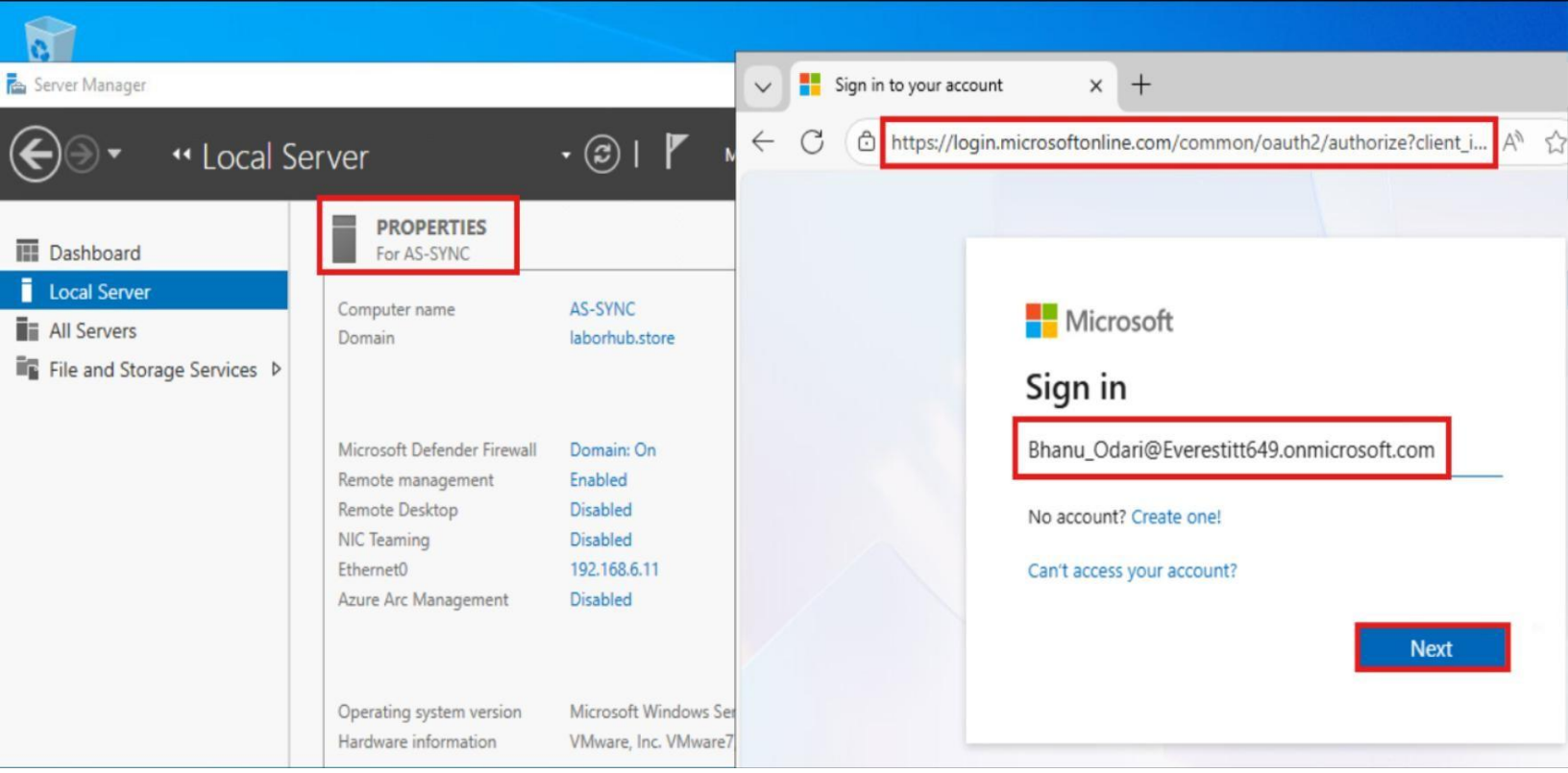
This is done to make it easier to access Microsoft websites and download tools during setup. To turn it off:

Open Server Manager → Local Server.
Click IE Enhanced Security Configuration.
Set both Administrators and Users to Off.
Click OK.

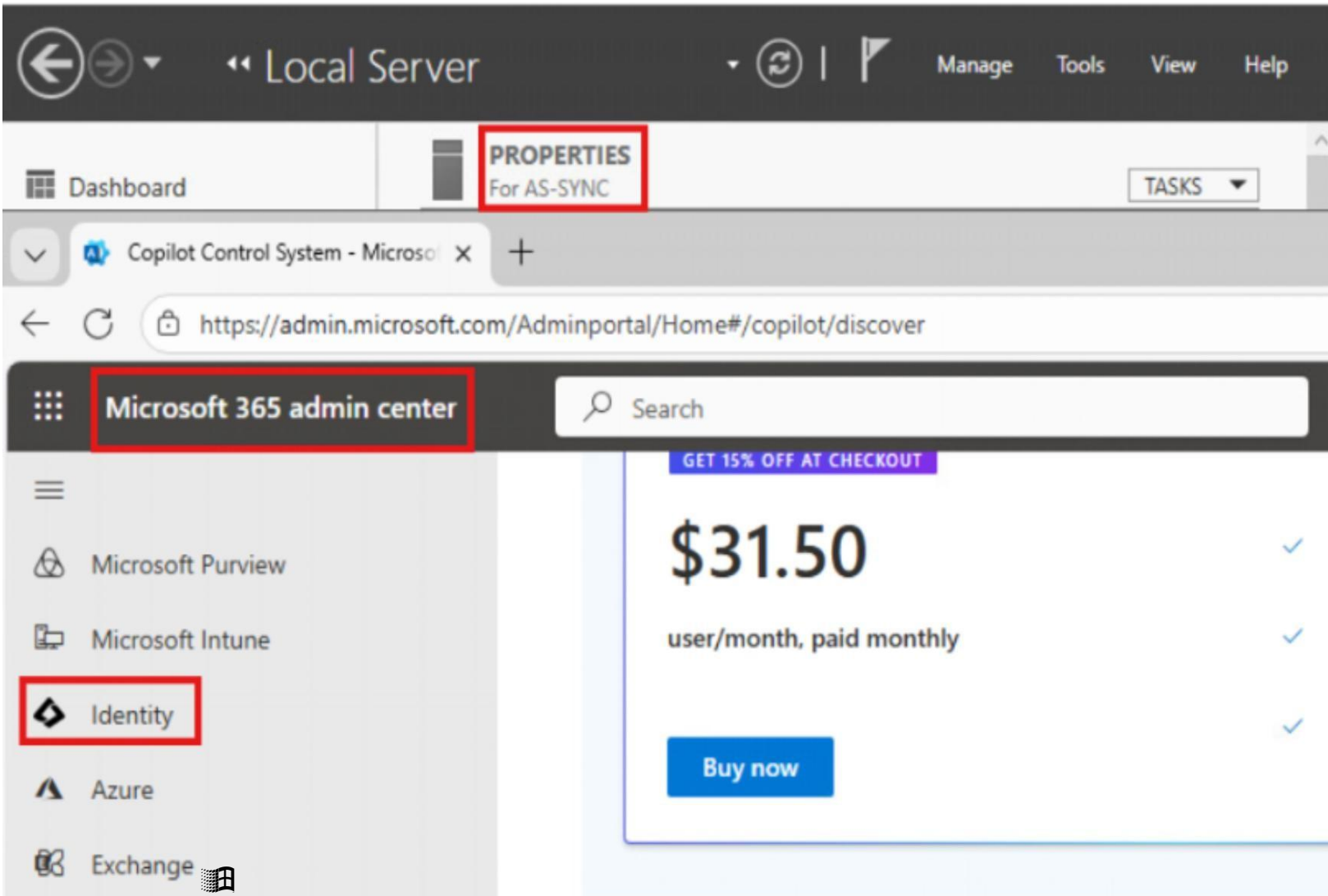


Additional Configuration: IE Enhanced Security.

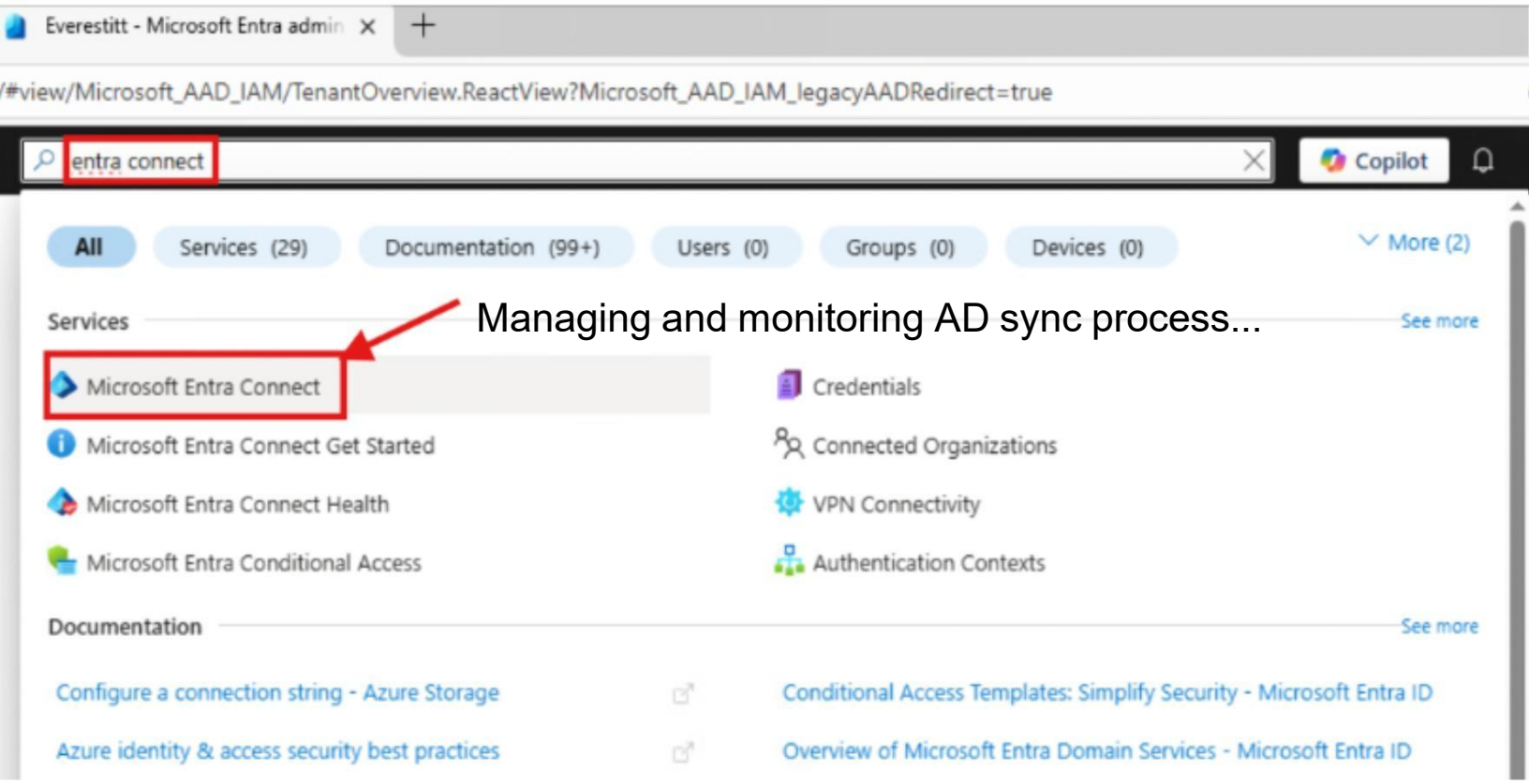
This shows the sync server is ready and you are signing in to Microsoft 365 with a global admin account to link your on-premises AD to the cloud. This is required during Azure AD Connect configuration.



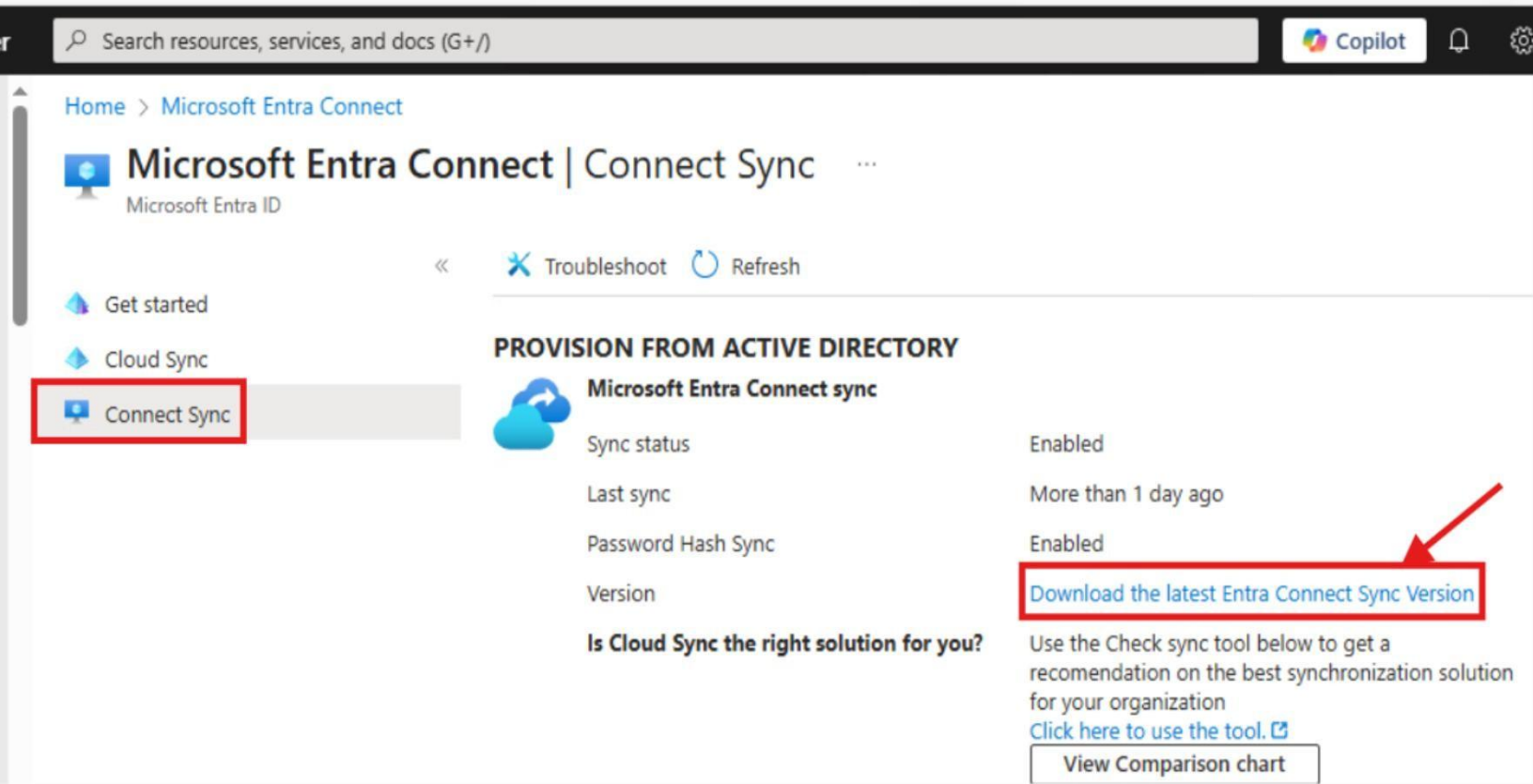
This shows that the sync server is ready, and you have successfully accessed the Microsoft 365 Admin Center to manage identities. This is part of preparing for or verifying Azure AD Connect synchronization.



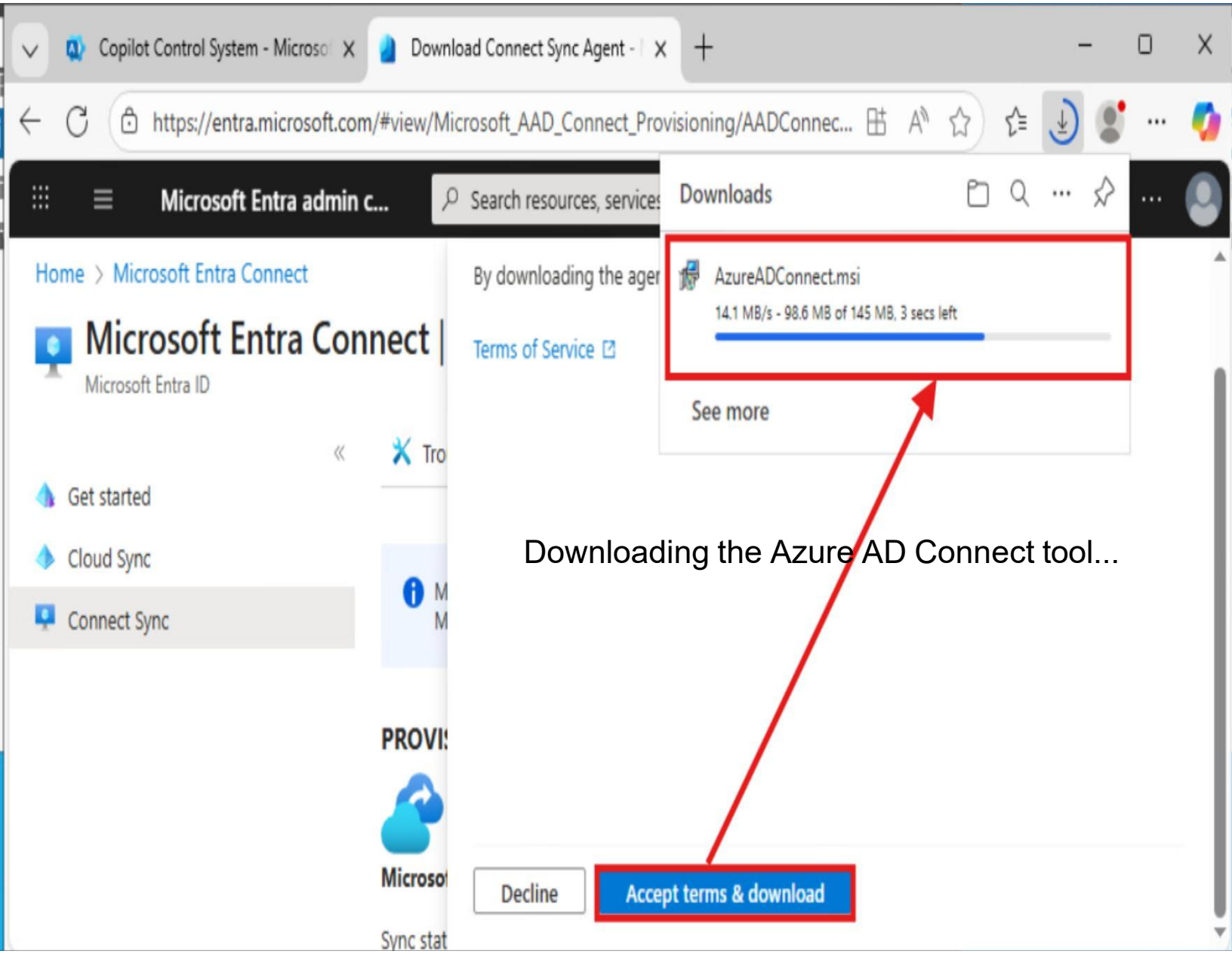
This is where you manage and monitor the AD sync process in the cloud. Microsoft Entra Connect is the cloud-side component that works with Azure AD Connect installed on your sync server to keep users and groups synchronized.



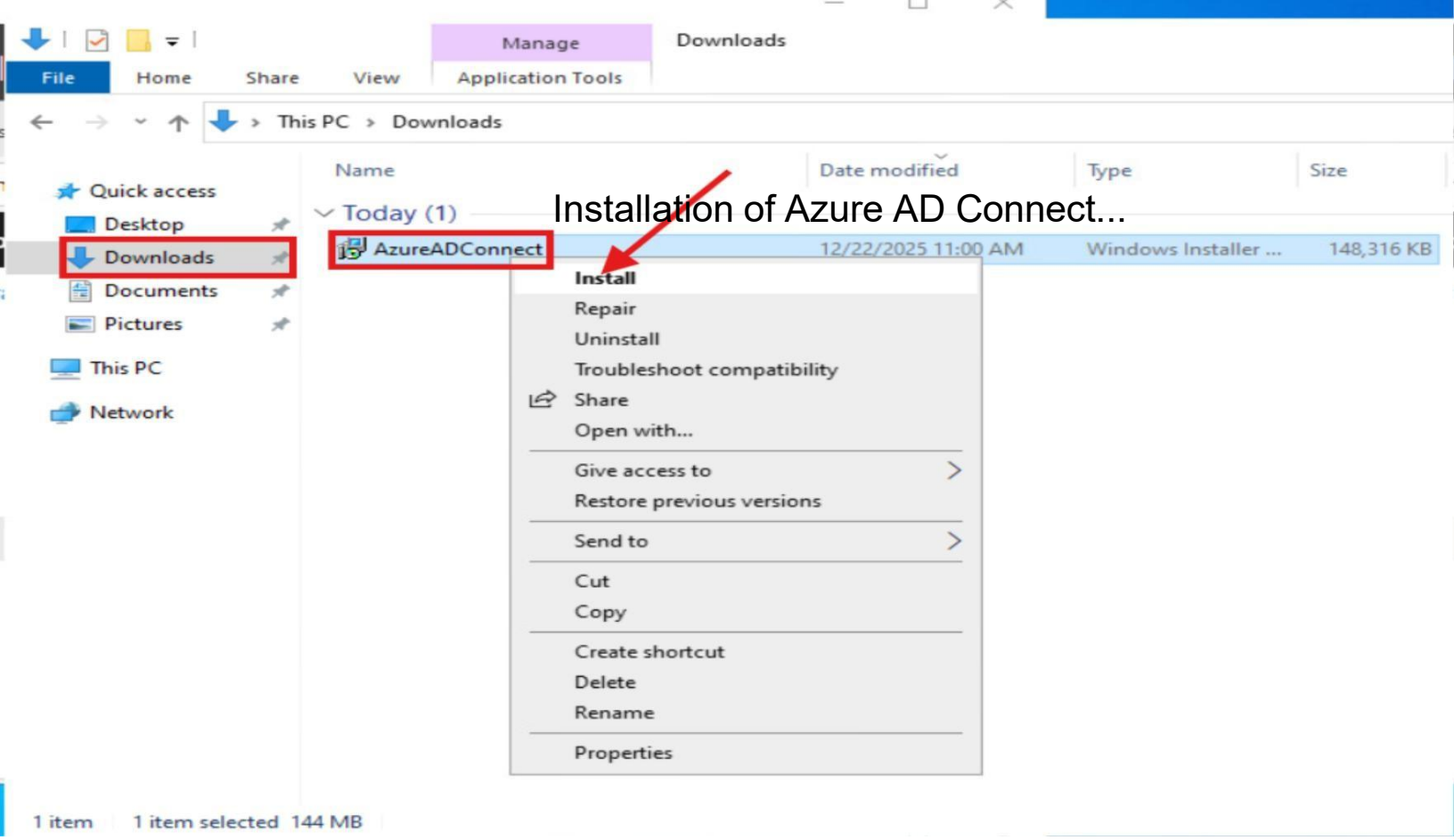
This page confirms that AD sync is active and working, but it hasn't synced in over a day. It also provides an option to download the latest version of Microsoft Entra Connect to keep your sync tool updated.



This step is downloading the Azure AD Connect tool, which is required to set up and manage the sync between your local AD and Microsoft Entra ID (Microsoft 365). After this, you will install and configure it on the sync server.

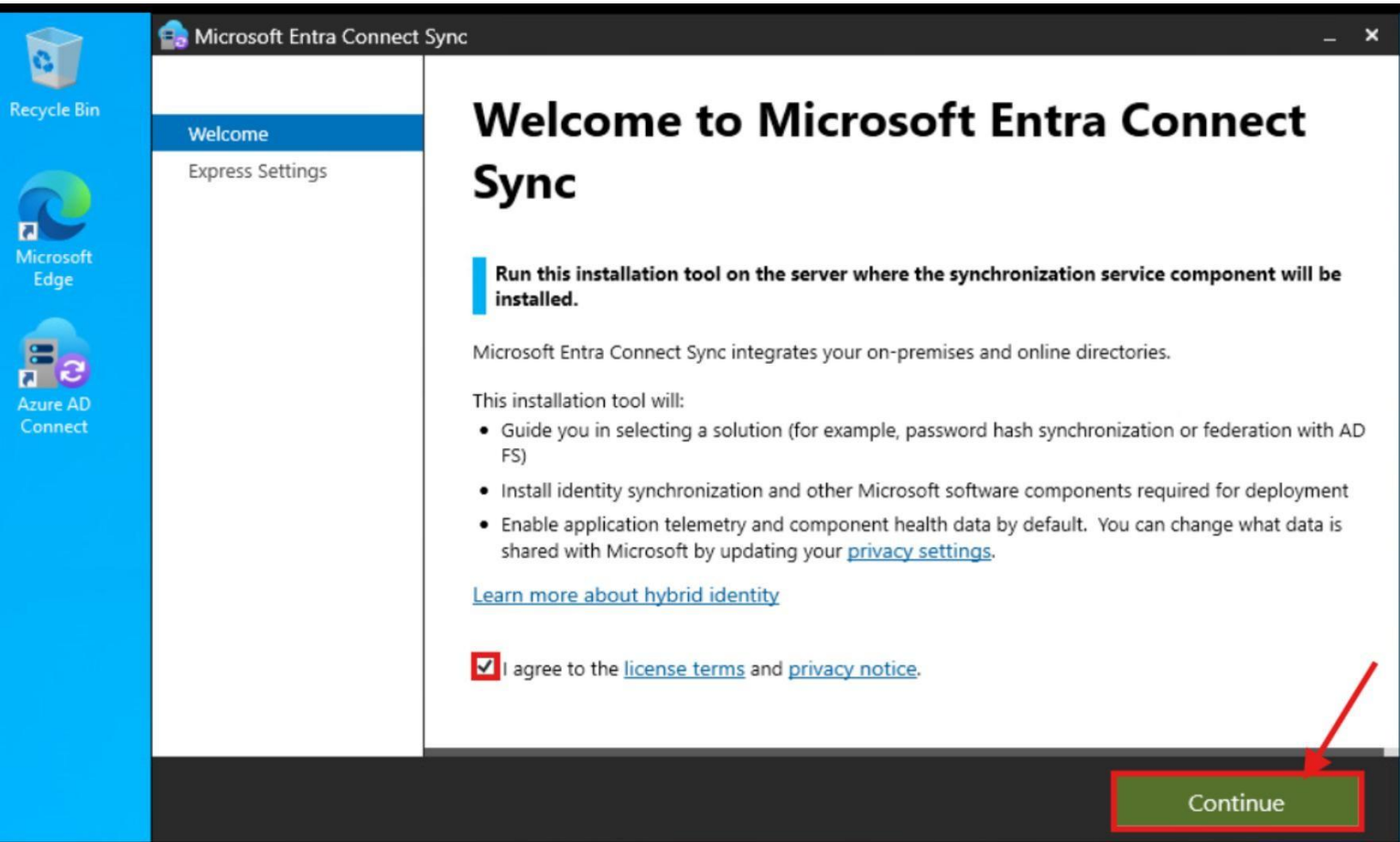


You are in the Downloads folder on your sync server.
The file AzureADConnect.msi (about 148 MB) has finished downloading.
You right-clicked the file and selected Install from the context menu.
This step begins the installation of Azure AD Connect, which is the tool that will synchronize your on-premises Active Directory with Microsoft 365 (Microsoft Entra ID).



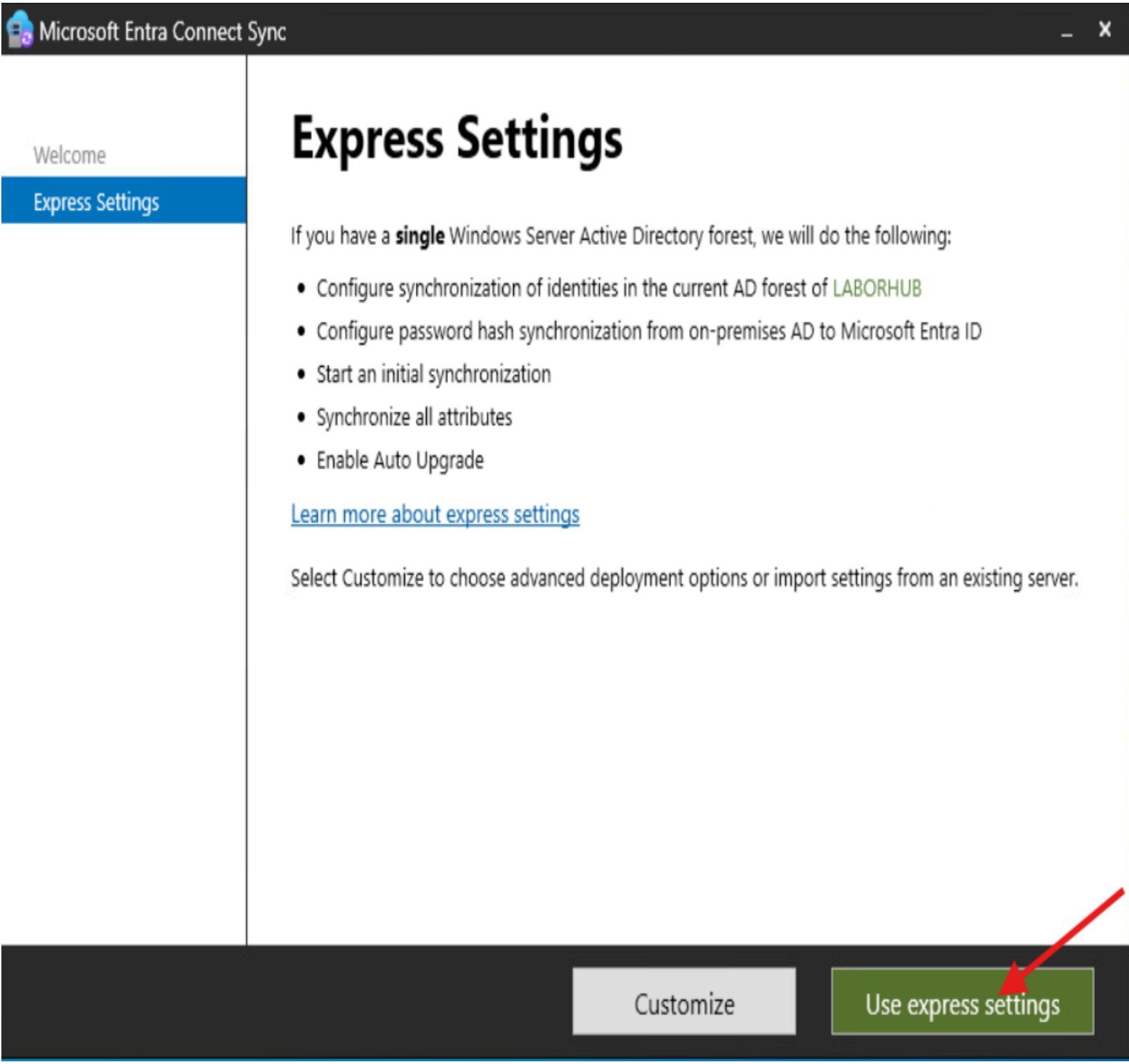
Installation of Azure AD Connect...

This step is the actual installation of Azure AD Connect, which is the key tool for syncing your on-premises AD with Microsoft 365. After installation, you will configure sync settings and start synchronization.

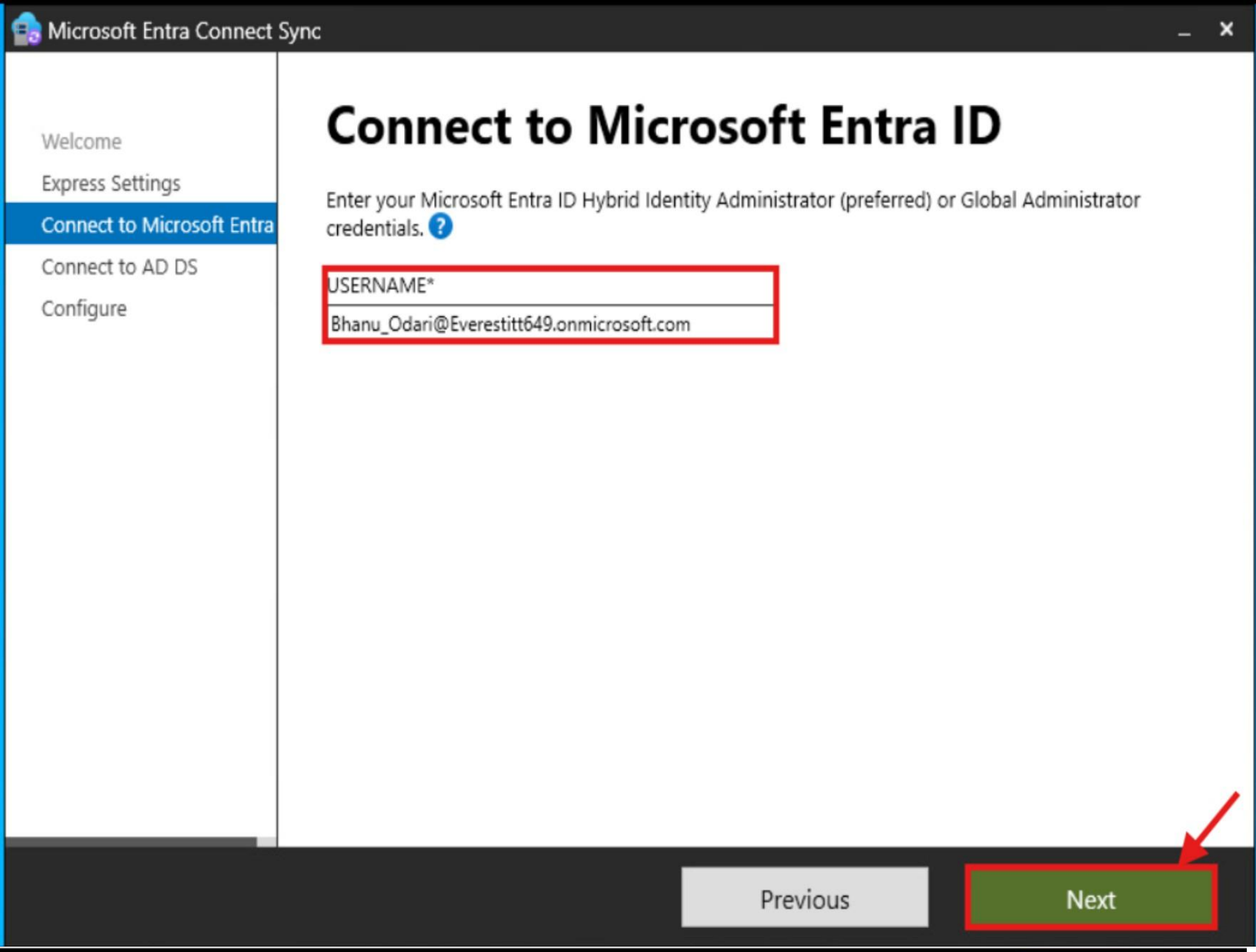


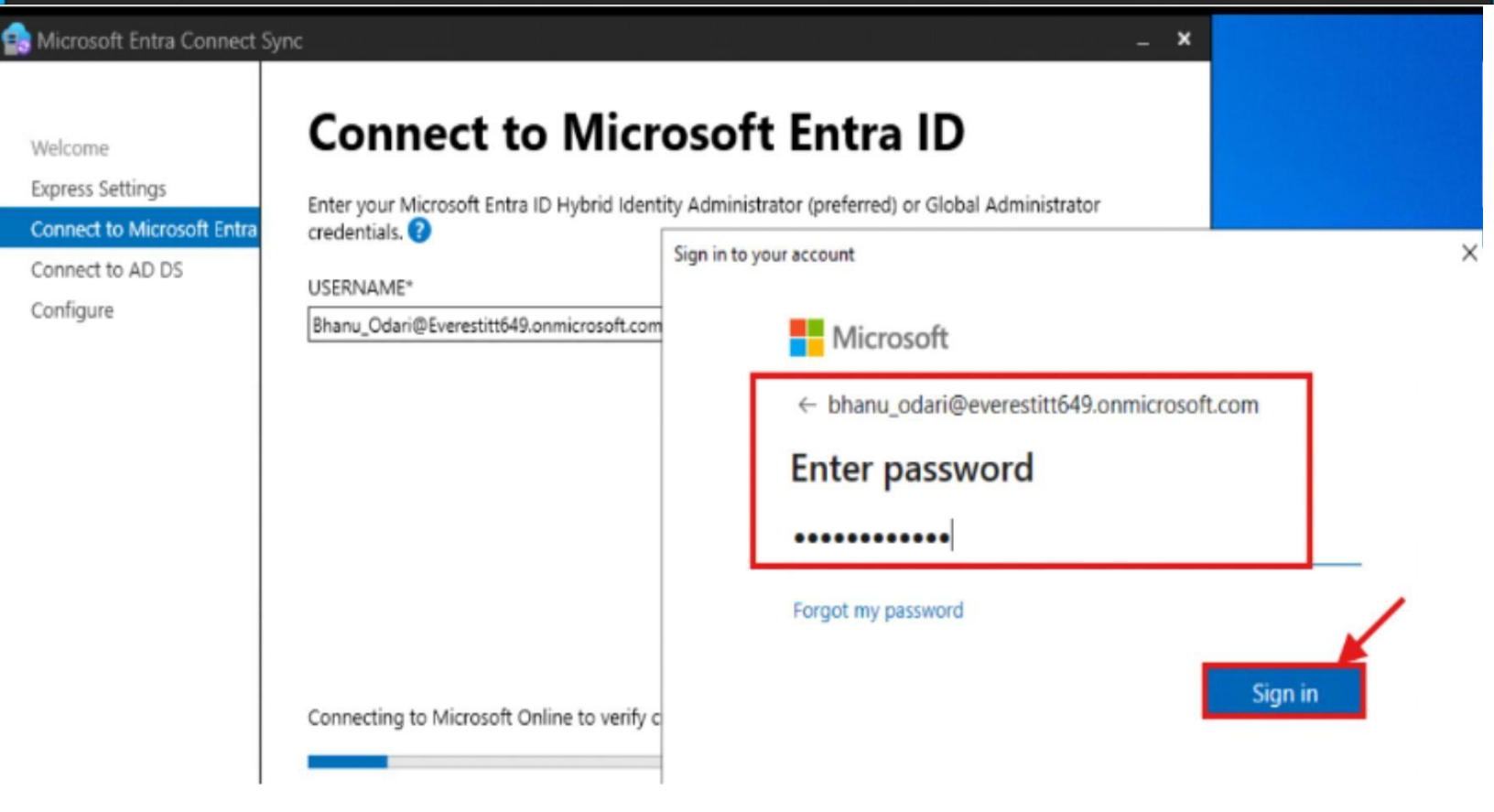
If you choose Use express settings, the wizard will:

This step is where you decide how to configure Azure AD Connect. Using Express Settings is recommended for a single AD forest because it's quick and includes all basic sync features.

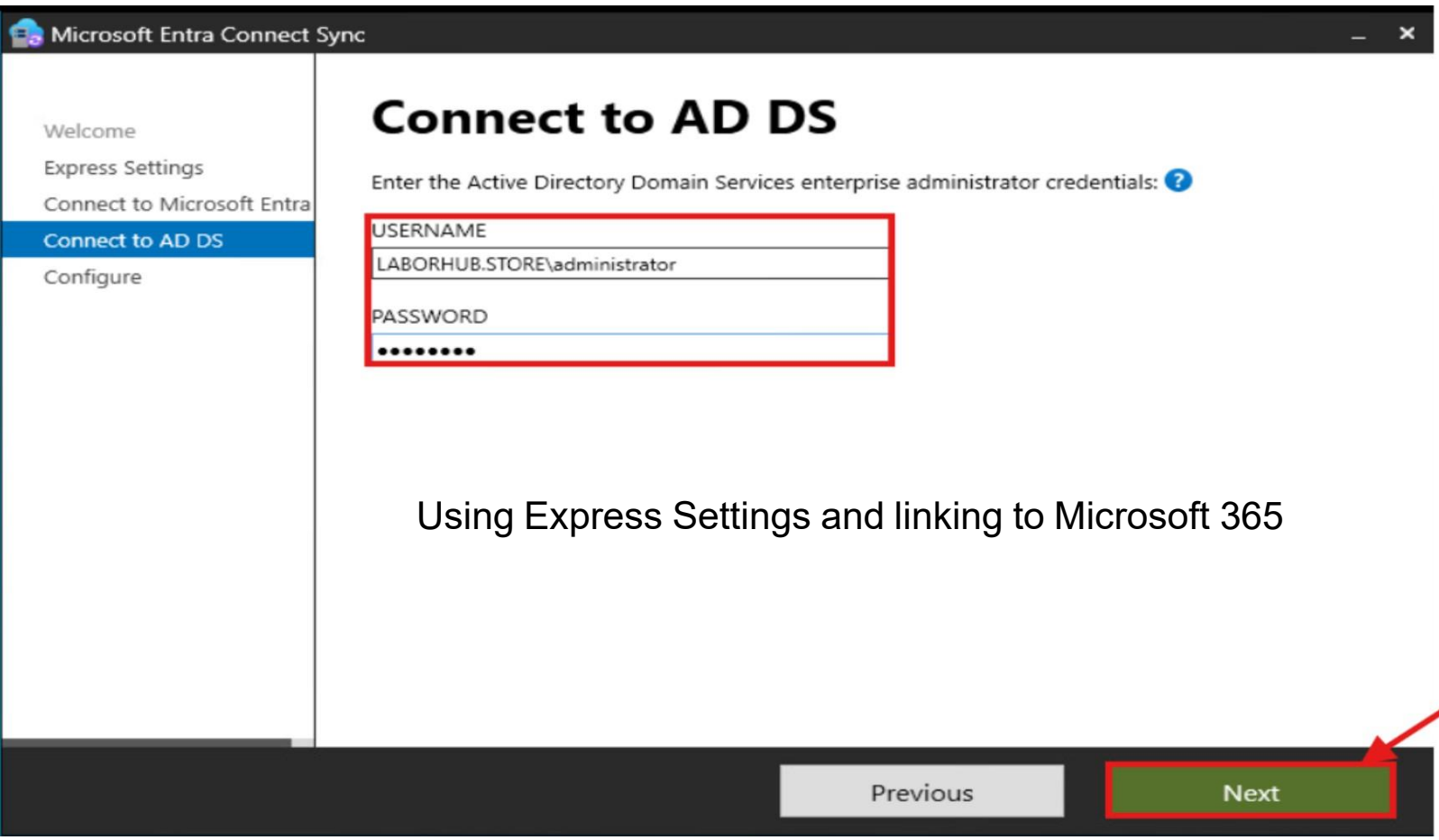


This step links your sync tool to Microsoft 365 by authenticating with an admin account. Without this, Azure AD Connect cannot synchronize your users to the cloud.


Microsoft Entra Connect Sync
Welcome
Express Settings
Connect to Microsoft Entra
Connect to AD DS
Configure
Connect to Microsoft Entra ID
Enter your Microsoft Entra ID Hybrid Identity Administrator (preferred) or Global Administrator credentials.
USERNAME*
Bhanu_Odari@Everestitt649.onmicrosoft.com
Previous
Next

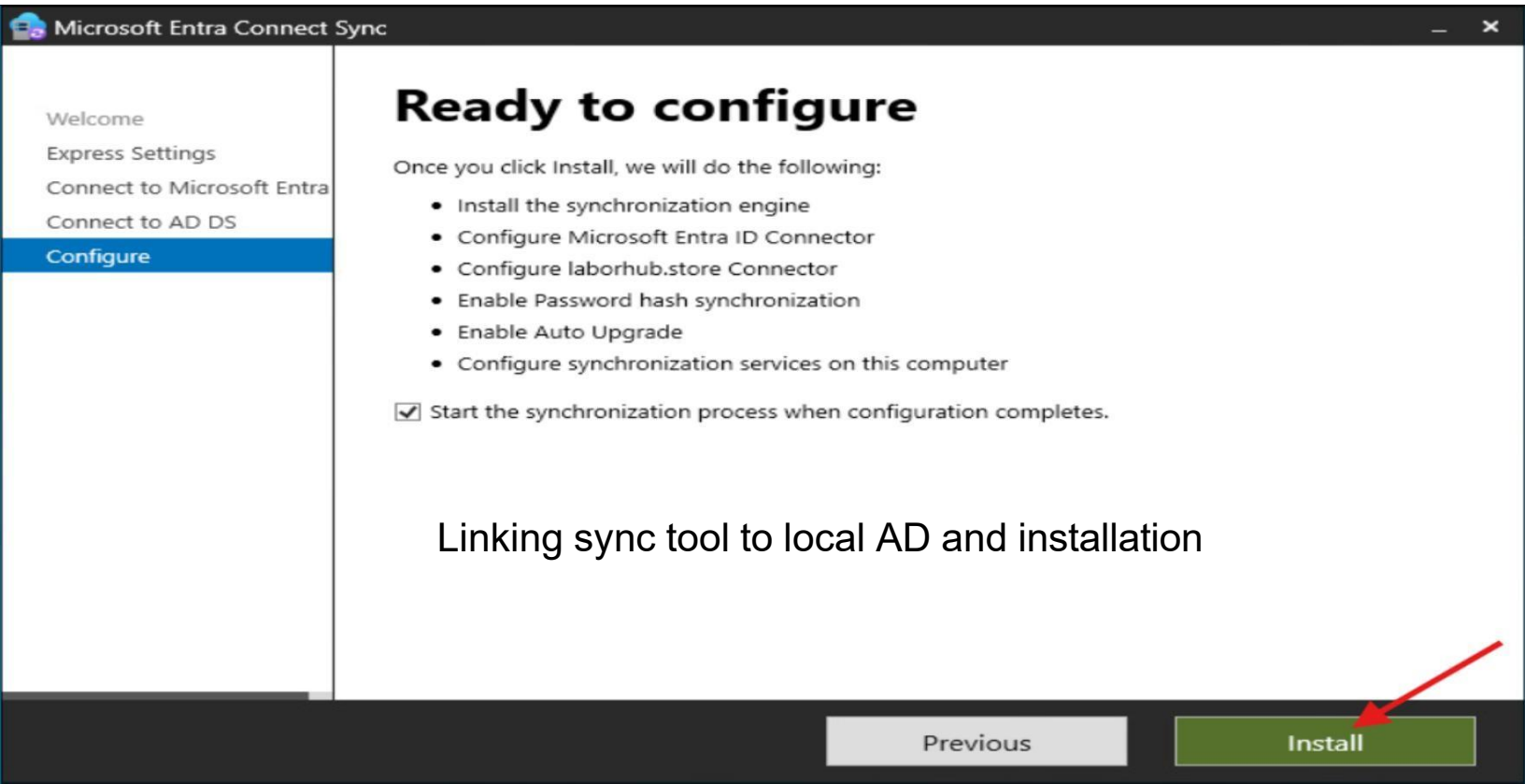

Microsoft Entra Connect Sync
Welcome
Express Settings
Connect to Microsoft Entra
Connect to AD DS
Configure
Connect to Microsoft Entra ID
Enter your Microsoft Entra ID Hybrid Identity Administrator (preferred) or Global Administrator credentials.
USERNAME*
Bhanu_Odari@Everestitt649.onmicrosoft.com
Connecting to Microsoft Online to verify c
Sign in to your account
Microsoft
bhanu_odari@everestitt649.onmicrosoft.com
Enter password
Forgot my password
Sign in

This step links the sync tool to your local AD by authenticating with a domain administrator account. Without this, Azure AD Connect cannot access and sync your users and groups to Microsoft 365.



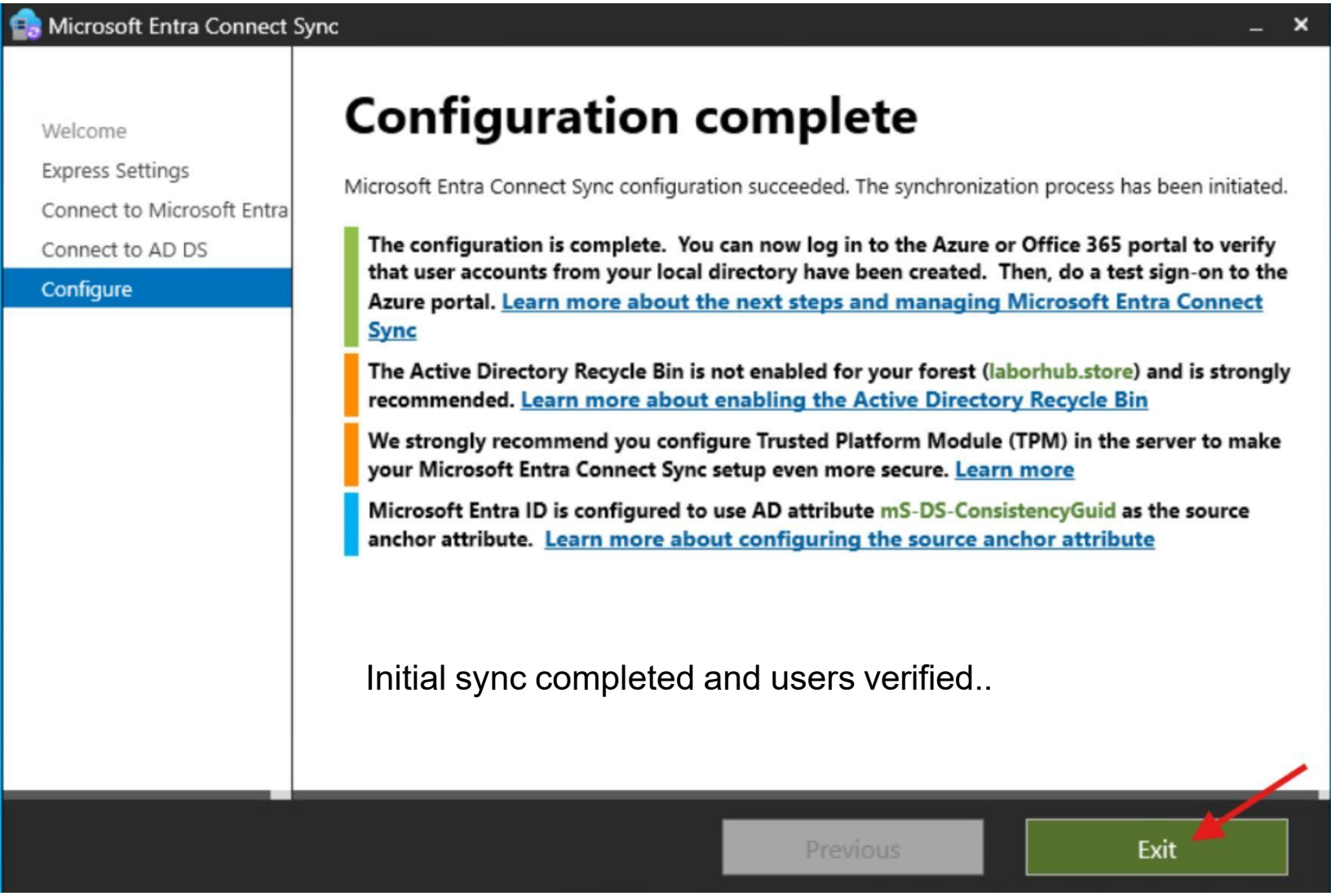
Using Express Settings and linking to Microsoft 365

This is the final confirmation step before Azure AD Connect starts syncing your on-premises AD users to Microsoft 365. After clicking Install, the sync engine will be installed and the first synchronization will run automatically.



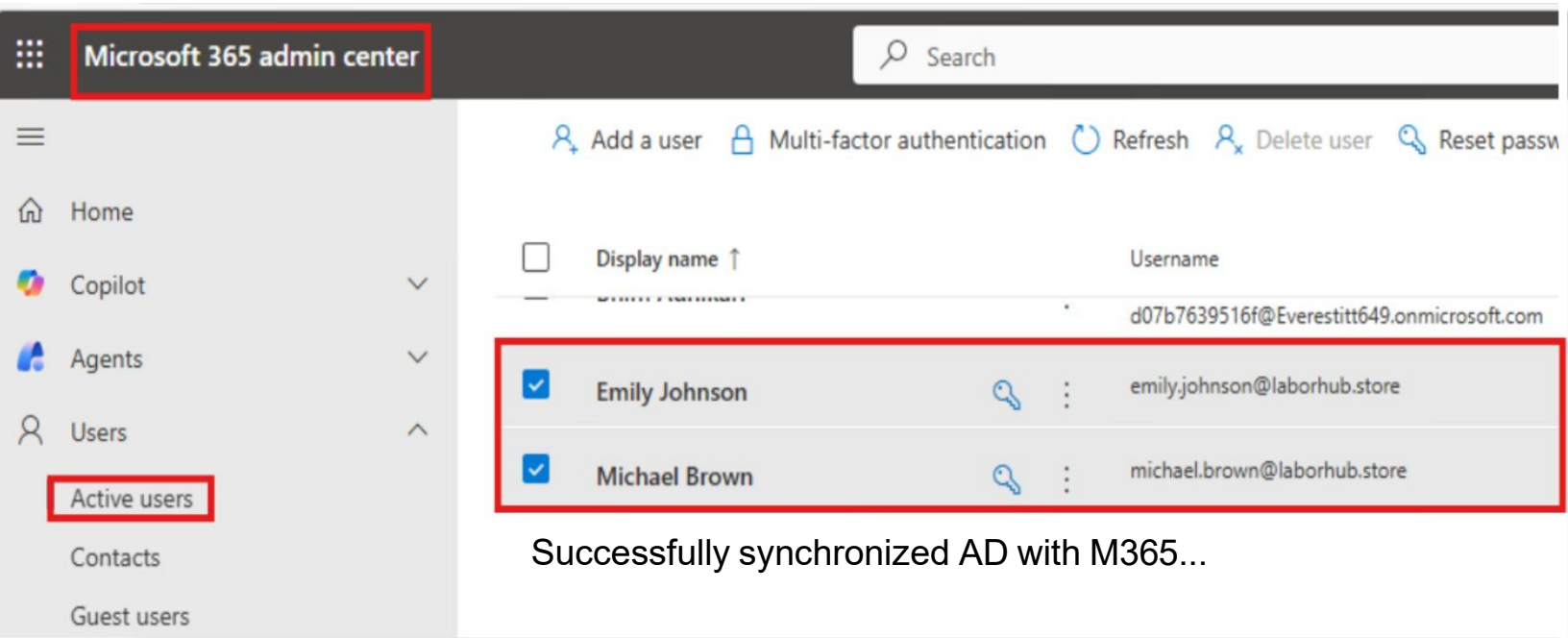
Linking sync tool to local AD and installation

Your Azure AD Connect setup is complete, and the initial sync has started. Next, you should verify synced users in Microsoft 365.

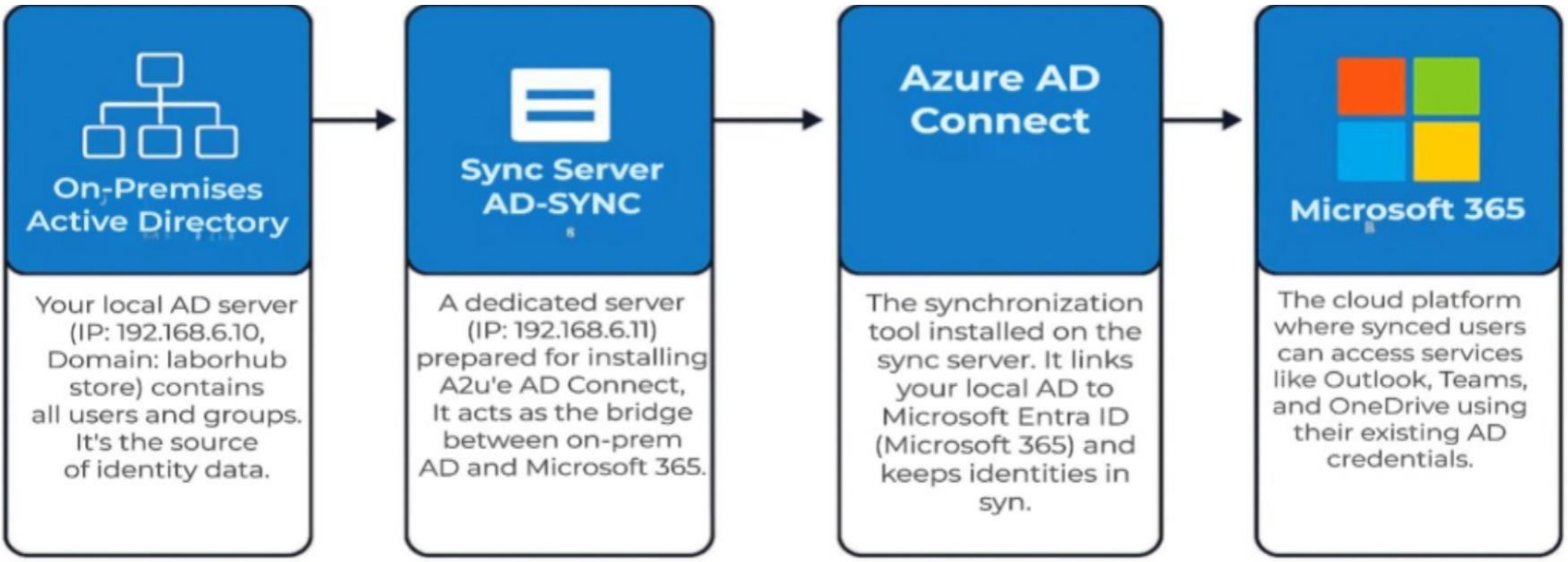


Initial sync completed and users verified..

This verifies that your on-premises AD users are now active in Microsoft 365. They can use their existing credentials to access cloud services like Outlook, Teams, and OneDrive.



Successfully synchronized AD with M365...



**Feature	On-Premises Active Directory	Microsoft 365 / Azure AD**
Location	Installed on local servers within your organization	Cloud-based, managed by Microsoft
Purpose	Manages internal network resources (PCs, printers, apps)	Manages cloud identities and SaaS apps
Infrastructure	Requires physical hardware and maintenance	No physical infrastructure; updates handled by Microsoft
Authentication	Kerberos, NTLM	OAuth 2.0, SAML, OpenID Connect
Scope	On-premises resources only	Cloud services like Outlook, Teams, OneDrive
Features	Group Policy, OU structure, full customization	MFA, Conditional Access, Single Sign-On (SSO)
Management	Manual updates, backups, and security patches	Automatic updates and built-in security

AD Sync Troubleshooting

Sync Not Running
Path: PowerShell: StartADSyncCycle –PolicyType Delta

Global Admin Login Fails
Path: M365 Admin Center → Users → Active Users → Roles

Domain Admin Credentials Fail
Path: Server Manager → Local Server → Domain

Last Sync Over 24 Hours
Path: Services msç → AD Conneect'th Health Sync Monitor → Restart

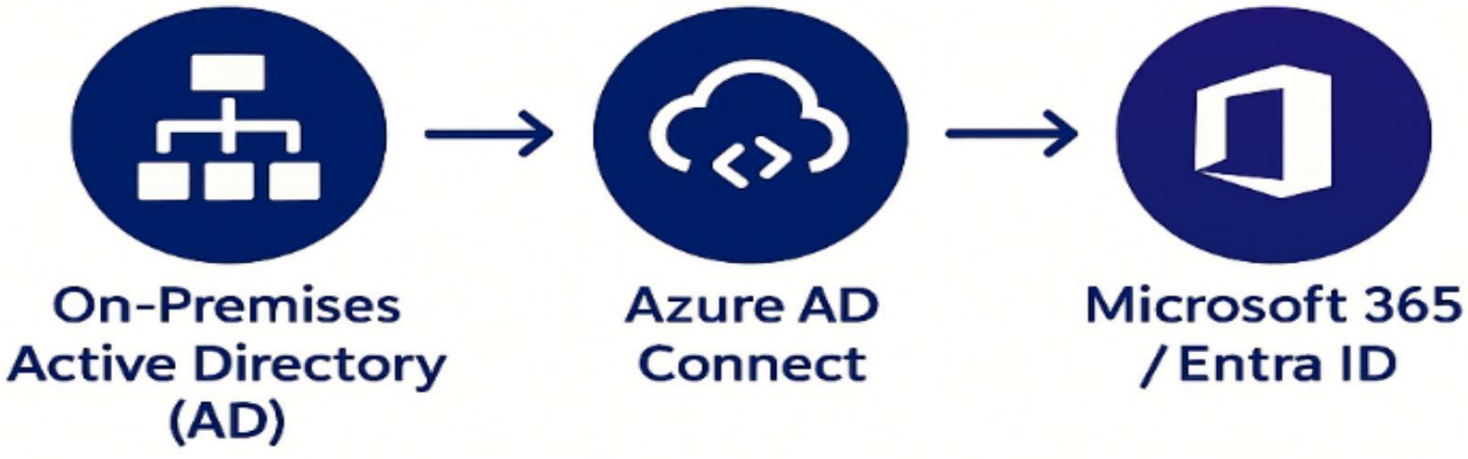
Password Not Syncing
Path: Azure AD Connect → Configure → Sync Options → Password Sync

Cannot Download Installer (IE Security)
Path: Server Manager → Local Server → IE ESC → Off

Duplicate UPN / Attribute Error
Path: ADUC → User Properties → Account → UPN

Version Out of Date
Path: Entra Admin → Identity → Hybrid Mgmt → Connect

Windows Server (On-Premises Active Directory)
Azure AD Connect (Express Settings)
Microsoft 365 Admin Center



Project Summary – AD Sync with Microsoft 365

- Configured Azure AD Connect to sync on-premises Active Directory users with Microsoft 365
- Verified successful hybrid identity synchronization in Microsoft Entra ID
- Enabled users to access Outlook, Teams, and OneDrive using on-prem Active Directory credentials
- Gained hands-on experience with hybrid identity, directory synchronization, and Microsoft 365 administration

This project successfully synchronized the on-premises Active Directory (AD) with Microsoft 365 Entra ID using Azure AD Connect. The entire process involved preparing the AD environment, configuring the synchronization server, installing Azure AD Connect, and verifying cloud identities to ensure that all users can now sign in to Microsoft 365 using their AD credentials.

This integration improves identity management, reduces password-related issues, and provides seamless experience across cloud services such as Outlook, SharePoint, Teams, and OneDrive. By enabling hybrid identity, the organization can now benefit from centralized user management, stronger security, and streamlined onboarding for future cloud services.