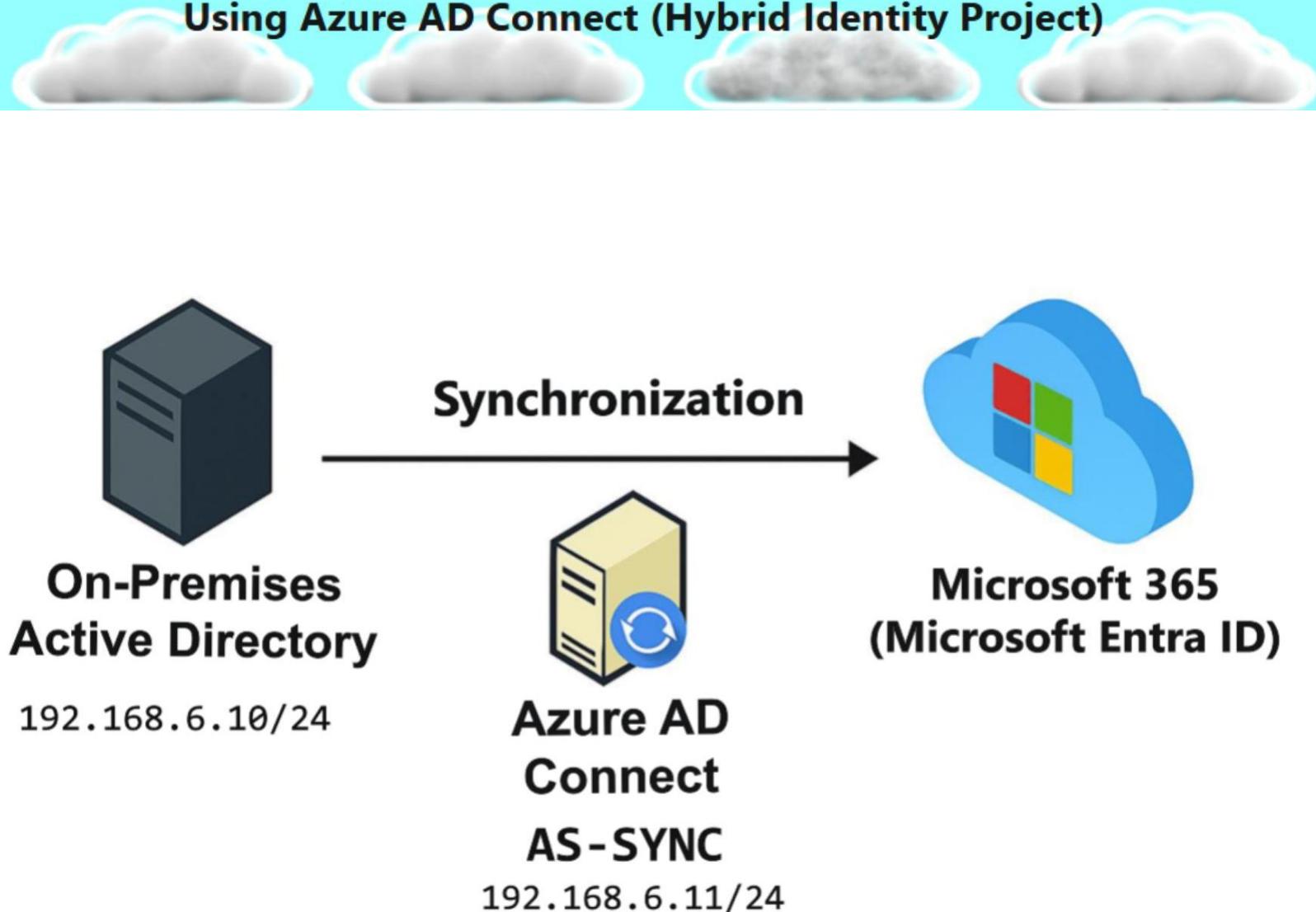


Active Directory Sync With Microsoft 365

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
- Lets users sign in to Outlook, Teams, OneDrive with same username and password they use on their office computer
- Improves 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:

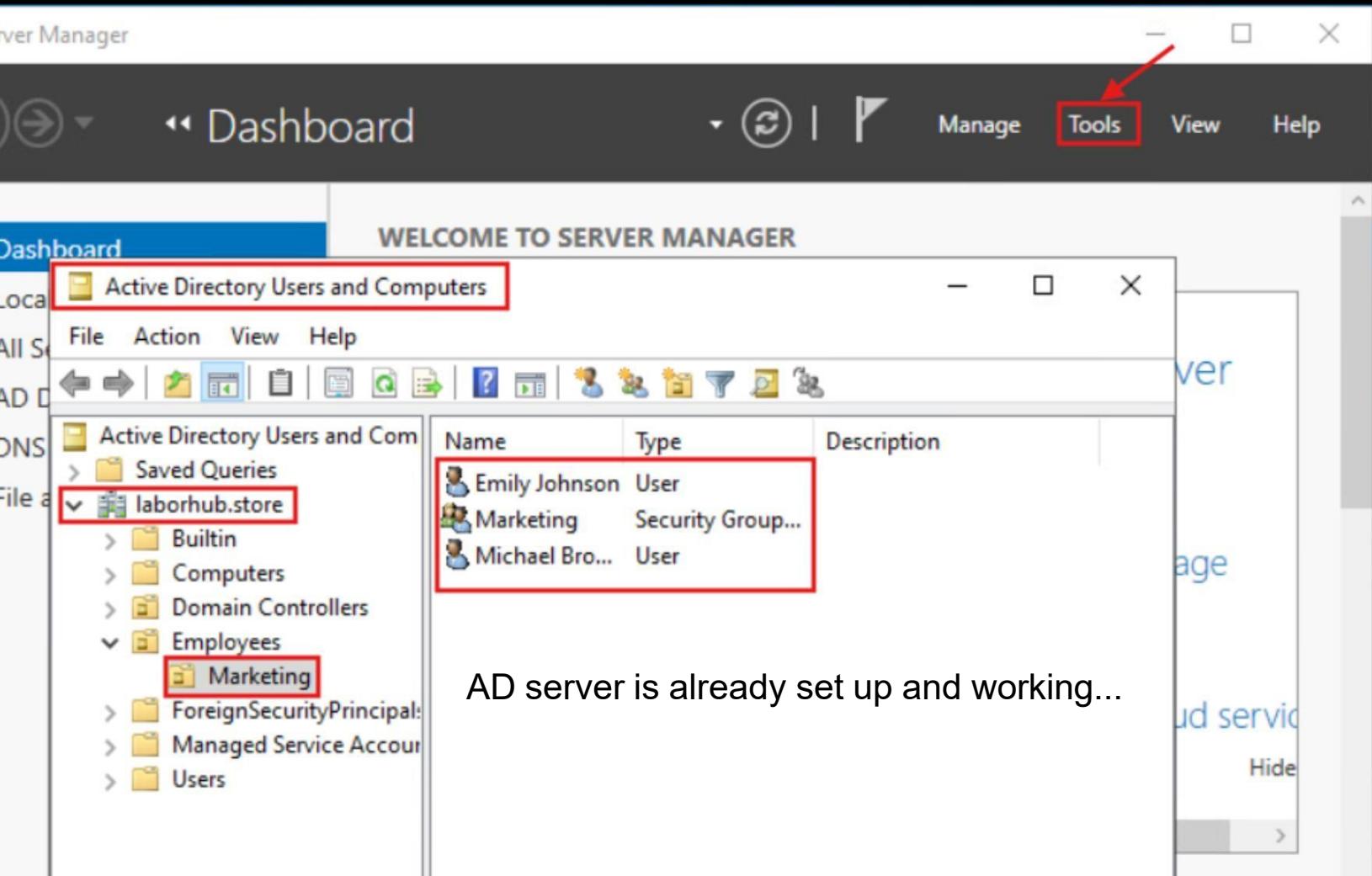
It has Active Directory installed.

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.

The screenshot shows the Windows Server Manager interface with the Local Server selected. On the left, there's a properties pane for 'AS-SYNC' with sections for Computer name, Domain, Microsoft Defender Firewall, Remote management, Remote Desktop, NIC Teaming, Ethernet0, Azure Arc Management, Operating system version, and Hardware information. The 'Domain' section is highlighted with a red box. In the center, a modal dialog titled 'Internet Explorer Enhanced Security Configuration' is open. It contains a message about IE ESC reducing exposure to attacks. Under the 'Administrators:' section, the 'On (Recommended)' radio button is checked, while the 'Off' radio button is selected and circled in red. Under the 'Users:' section, the same pattern is shown: 'On (Recommended)' is checked, and 'Off' is selected and circled in red. At the bottom right of the dialog, there are 'OK' and 'Cancel' buttons, with 'OK' also circled in red. To the right of the dialog, there's a sidebar with system status information like updates, antivirus, and hardware details.

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.

The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server' (which is selected and highlighted in blue), 'All Servers', and 'File and Storage Services'. The main content area displays the 'PROPERTIES For AS-SYNC' page for the local server. It lists various system details such as Computer name (AS-SYNC), Domain (laborhub.store), Microsoft Defender Firewall (Domain: On), Remote management (Enabled), Remote Desktop (Disabled), NIC Teaming (Disabled), Ethernet0 (IP 192.168.6.11), Azure Arc Management (Disabled), Operating system version (Microsoft Windows Server 2022 Datacenter), and Hardware information (VMware, Inc. VMware7). To the right, a Microsoft sign-in window is open, showing the URL https://login.microsoftonline.com/common/oauth2/authorize?client_i... and the email address Bhanu_Odari@Everestitt649.onmicrosoft.com.

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.

The screenshot shows the Microsoft 365 Admin Center interface. The top navigation bar includes 'Manage', 'Tools', 'View', and 'Help'. Below it, the main menu has items like 'Dashboard', 'Copilot Control System - Microsoft', and 'Microsoft 365 admin center' (which is selected and highlighted in red). A search bar is also present. The left sidebar features categories: 'Identity' (selected and highlighted in red), 'Microsoft Purview', 'Microsoft Intune', 'Azure', and 'Exchange'. The main content area displays a promotional offer for \$31.50 per user/month, paid monthly, with a 'Buy now' button. The URL https://admin.microsoft.com/Adminportal/Home#/copilot/discover is visible in the browser's address bar.

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.

Everestt - Microsoft Entra admin

entra connect

All Services (29) Documentation (99+) Users (0) Groups (0) Devices (0) More (2)

Services See more

Managing and monitoring AD sync process...

Microsoft Entra Connect

Microsoft Entra Connect Get Started

Microsoft Entra Connect Health

Microsoft Entra Conditional Access

Credentials

Connected Organizations

VPN Connectivity

Authentication Contexts

Documentation See more

Configure a connection string - Azure Storage

Conditional Access Templates: Simplify Security - Microsoft Entra ID

Azure identity & access security best practices

Overview of Microsoft Entra Domain Services - Microsoft Entra ID

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.

Search resources, services, and docs (G+/-)

Copilot

Home > Microsoft Entra Connect

Microsoft Entra Connect | Connect Sync

Microsoft Entra ID

Get started

Cloud Sync

Connect Sync

Troubleshoot Refresh

PROVISION FROM ACTIVE DIRECTORY

Microsoft Entra Connect sync

Sync status	Enabled
Last sync	More than 1 day ago
Password Hash Sync	Enabled
Version	Download the latest Entra Connect Sync Version

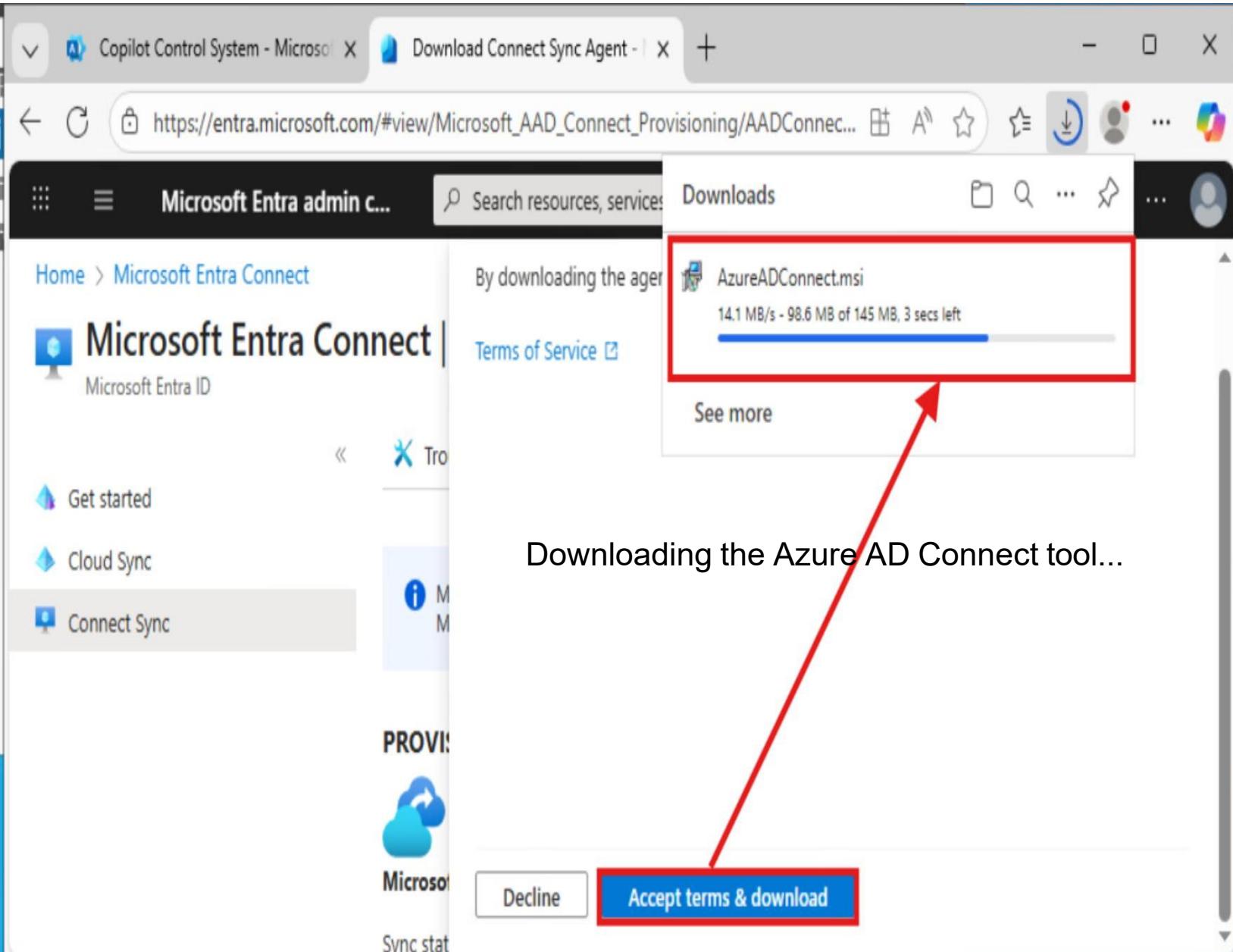
Is Cloud Sync the right solution for you?

Use the Check sync tool below to get a recommendation on the best synchronization solution for your organization

[Click here to use the tool.](#)

[View Comparison chart](#)

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.



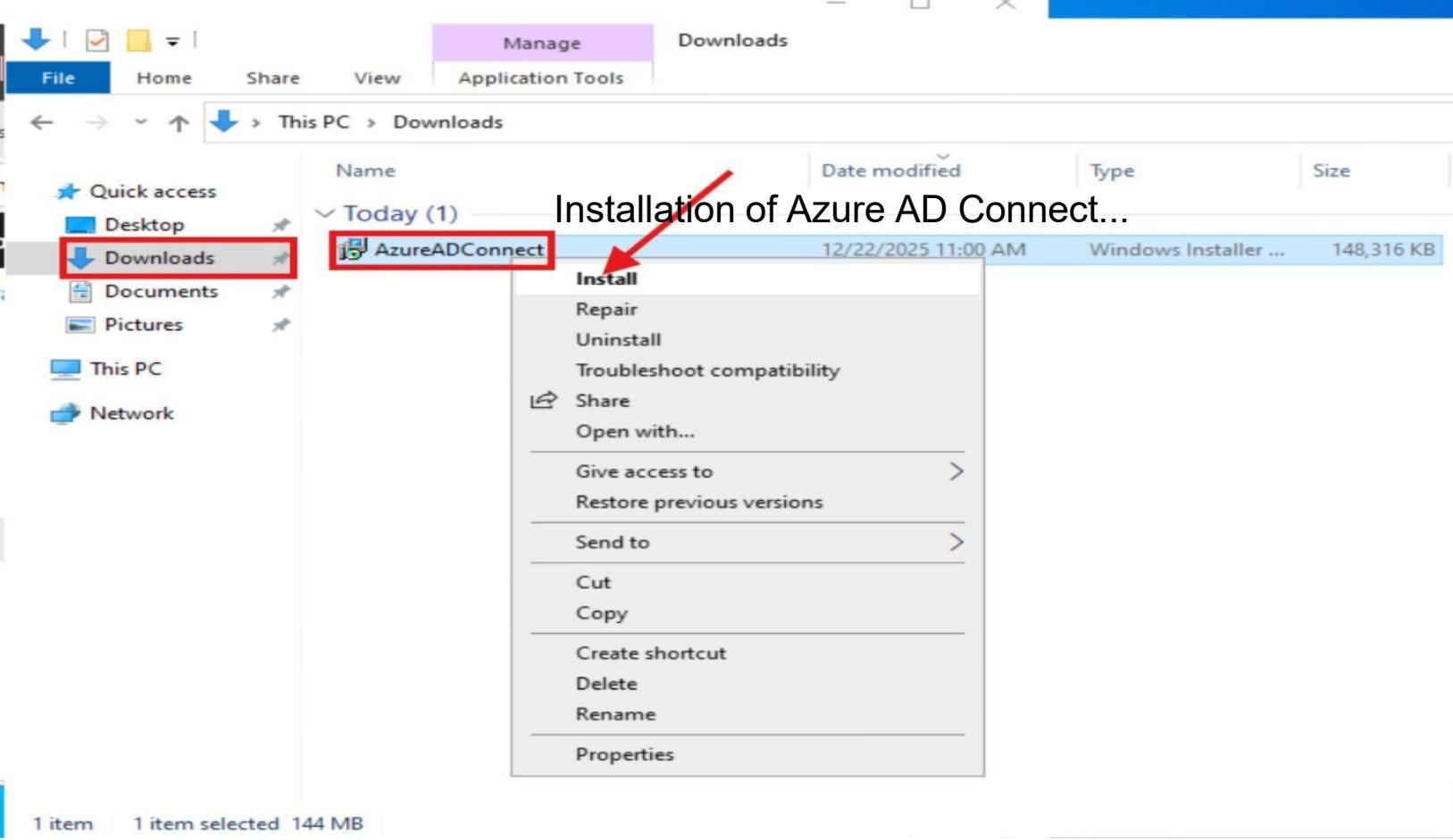
Downloading the Azure AD Connect tool...

You are in the **Downloads folder** on your sync server.

The file **AzureADConnect.msi** (about 148 MB) has finished downloading.

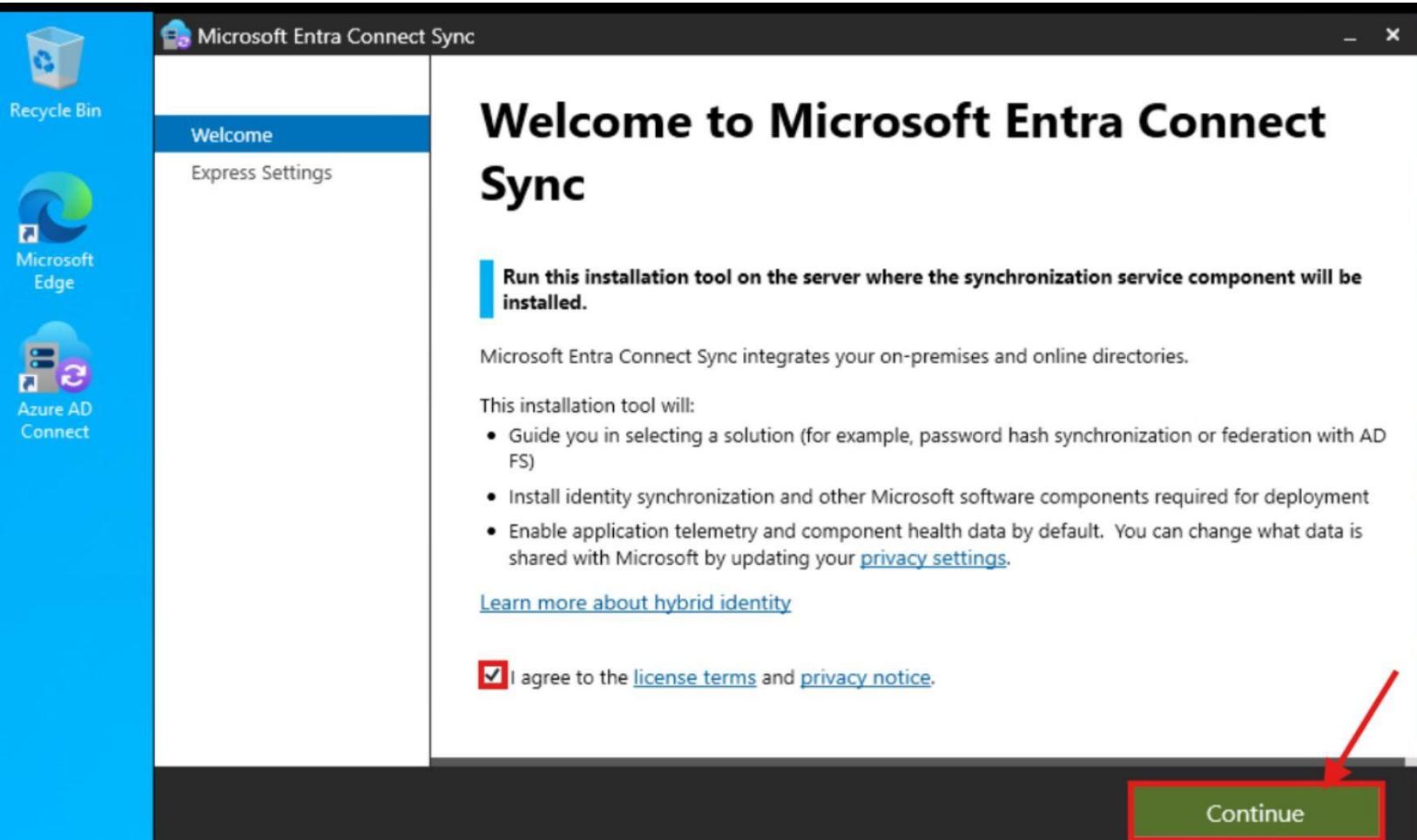
You right-clicked the file and selected **Install** from the context menu.

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).



1 item 1 item selected 144 MB

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.

The screenshot shows the Microsoft Entra Connect Sync Express Settings wizard window. The title bar says "Microsoft Entra Connect Sync". The left sidebar has two options: "Welcome" and "Express Settings", with "Express Settings" being the active tab. The main content area has a large heading "Express Settings". Below it, text states: "If you have a **single** Windows Server Active Directory forest, we will do the following:" followed by a bulleted list of six items. At the bottom, there are two buttons: "Customize" and "Use express settings". A red arrow points to the "Use express settings" button.

Microsoft Entra Connect Sync

Welcome

Express Settings

Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of LABORHUB
- Configure password hash synchronization from on-premises AD to Microsoft Entra ID
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

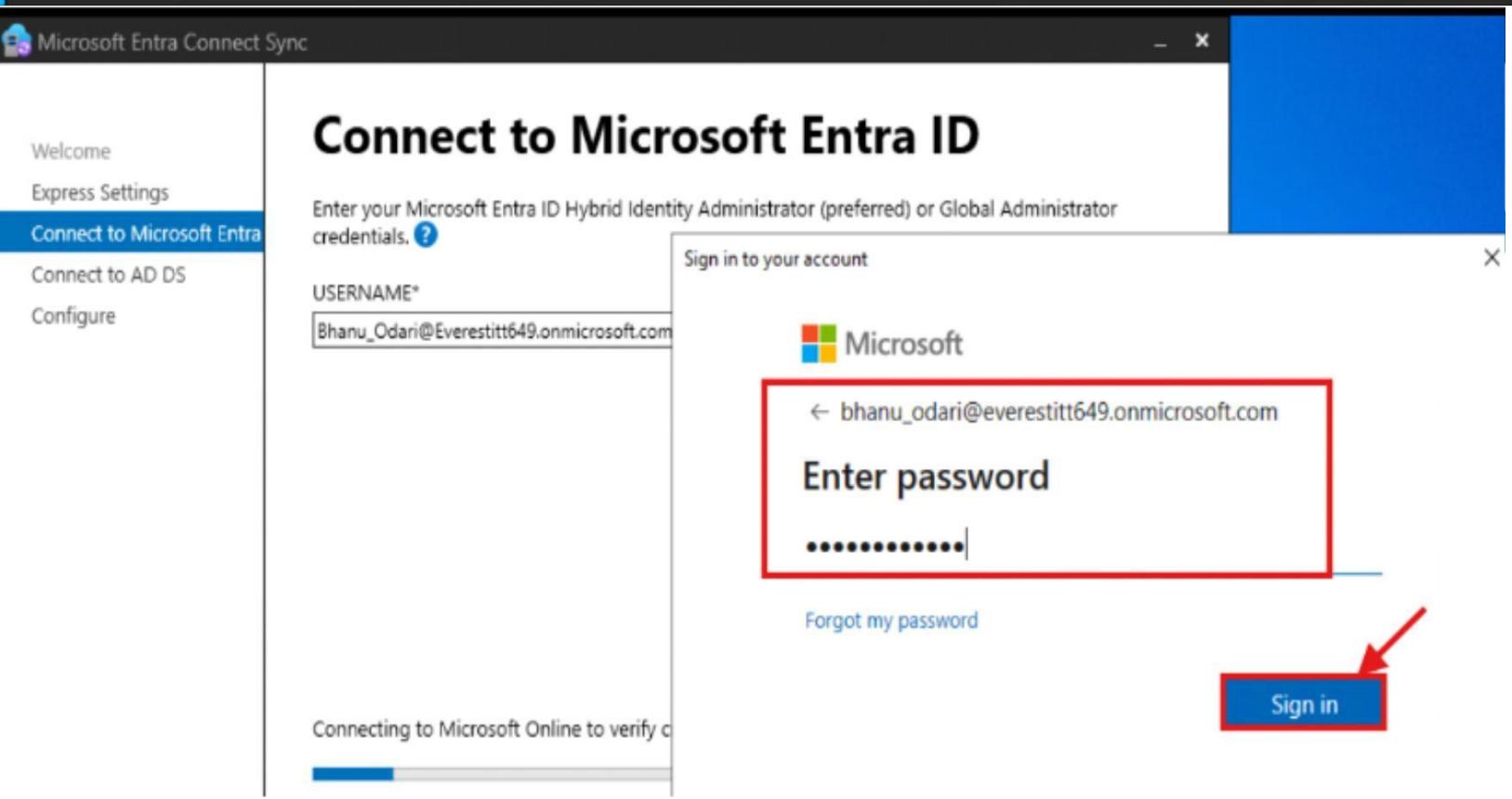
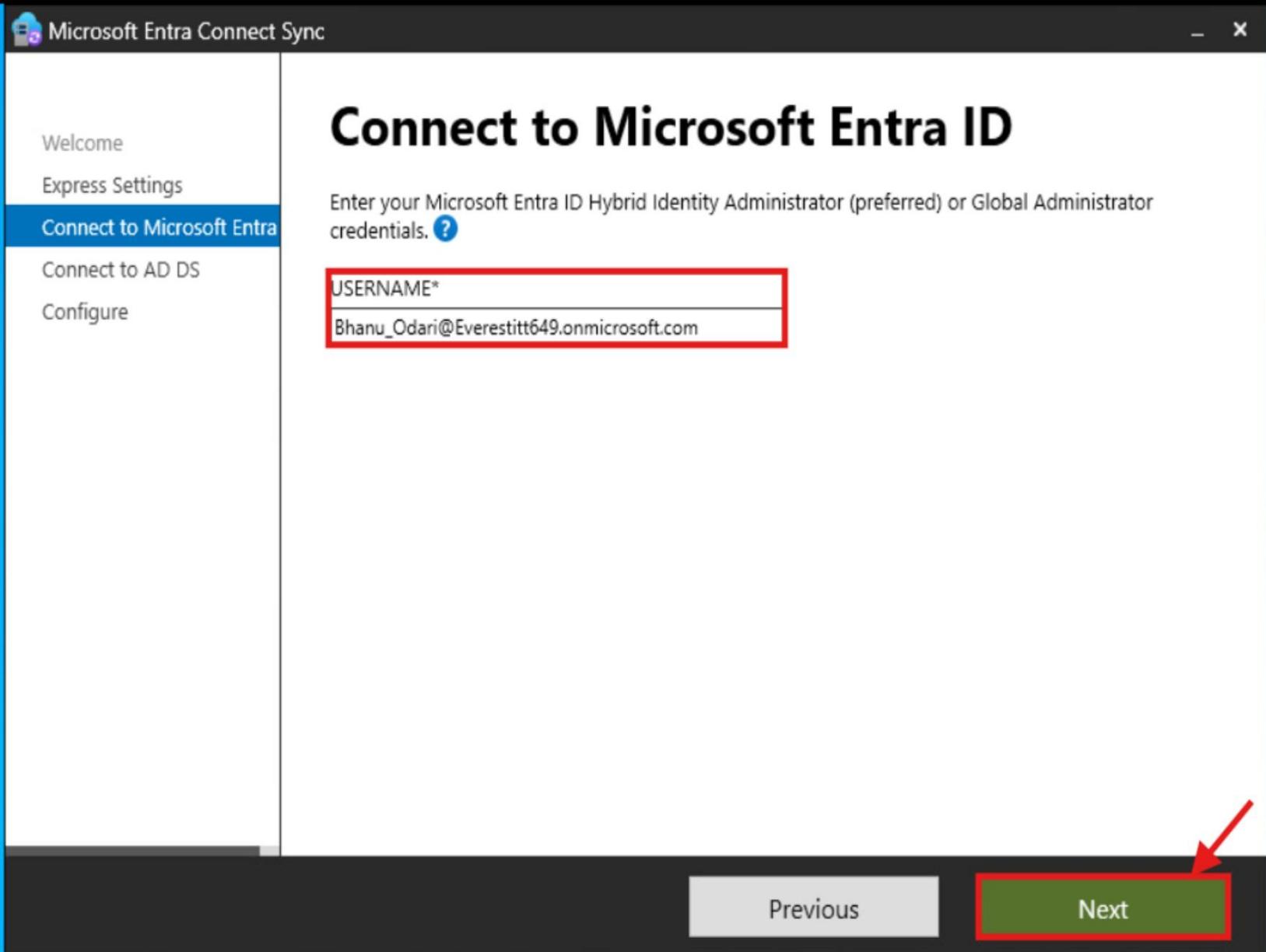
[Learn more about express settings](#)

Select Customize to choose advanced deployment options or import settings from an existing server.

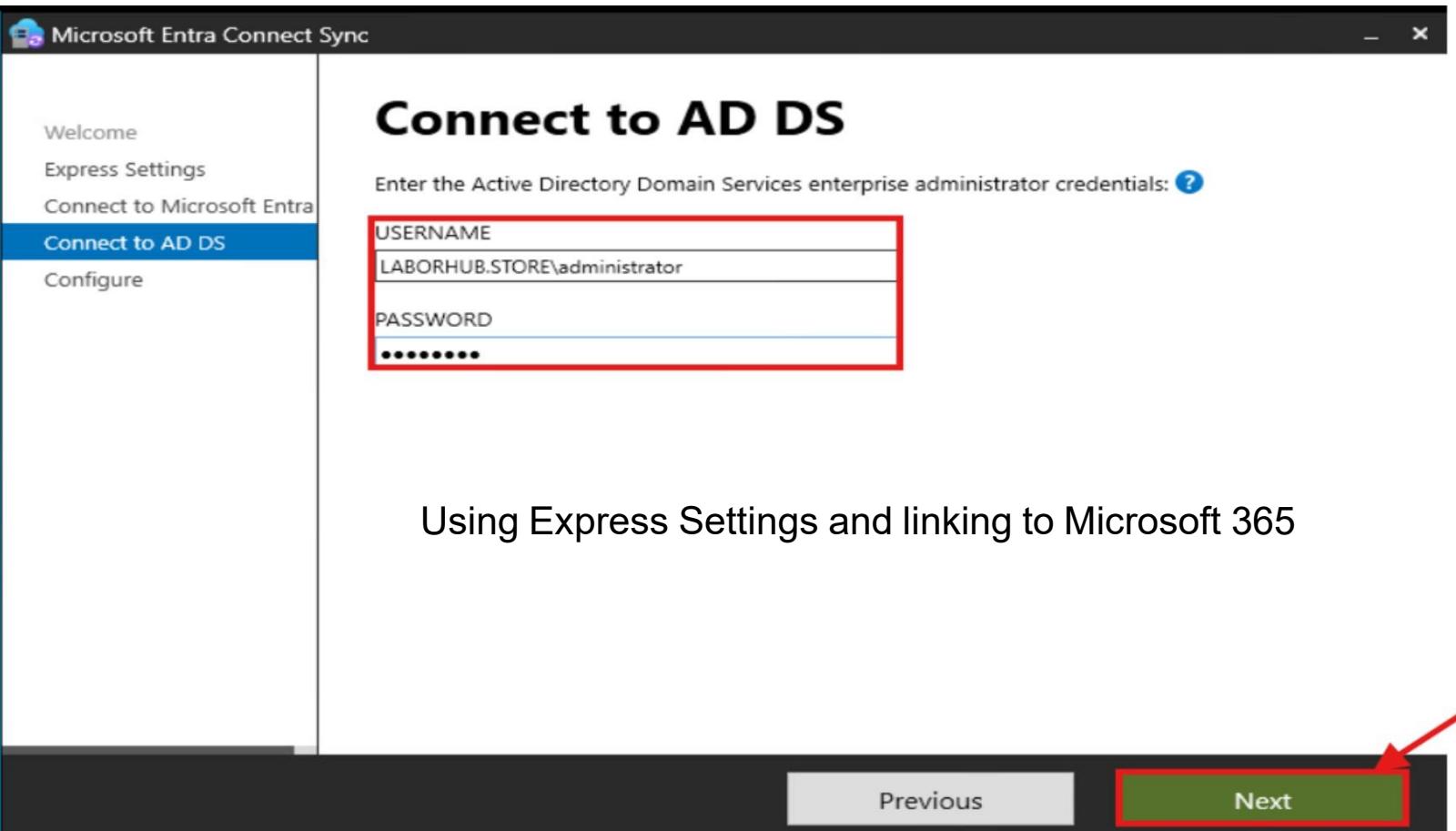
Customize

Use express settings

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.

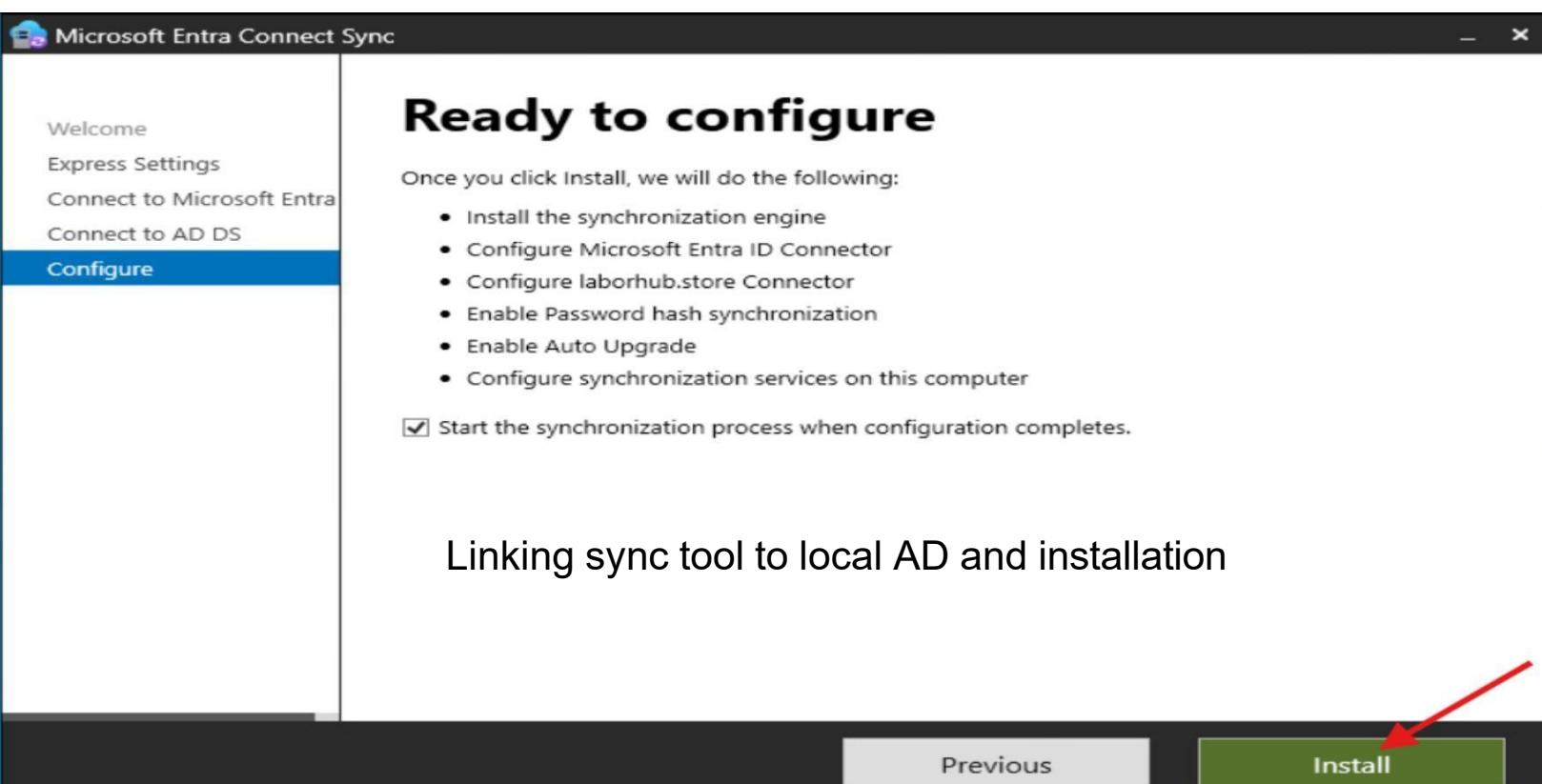


This step links the sync tool to your local AD by authenticating with a domain administrator account. Without this, Azure AD Connect cannot access and sync your users and groups to Microsoft 365.



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.

Microsoft Entra Connect Sync

Configuration complete

Microsoft Entra Connect Sync configuration succeeded. The synchronization process has been initiated.

The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. [Learn more about the next steps and managing Microsoft Entra Connect Sync](#)

The Active Directory Recycle Bin is not enabled for your forest (`laborhub.store`) and is strongly recommended. [Learn more about enabling the Active Directory Recycle Bin](#)

We strongly recommend you configure Trusted Platform Module (TPM) in the server to make your Microsoft Entra Connect Sync setup even more secure. [Learn more](#)

Microsoft Entra ID is configured to use AD attribute `mS-DS-ConsistencyGuid` as the source anchor attribute. [Learn more about configuring the source anchor attribute](#)

Initial sync completed and users verified..

Previous

Exit



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.

Microsoft 365 admin center

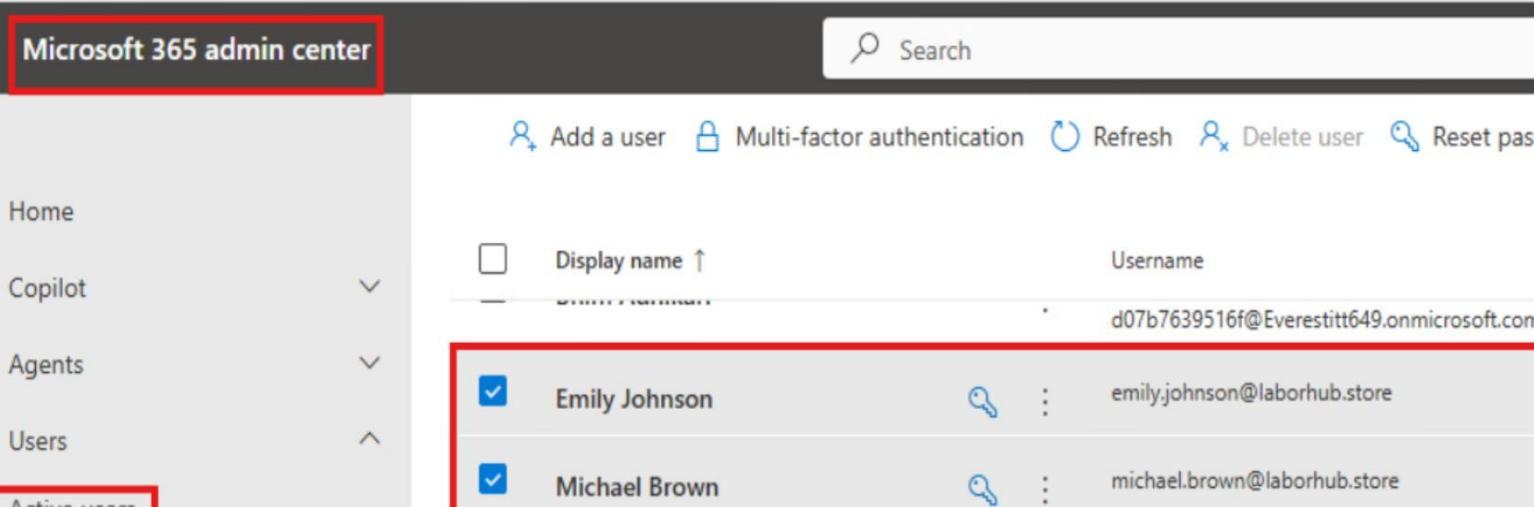
Search

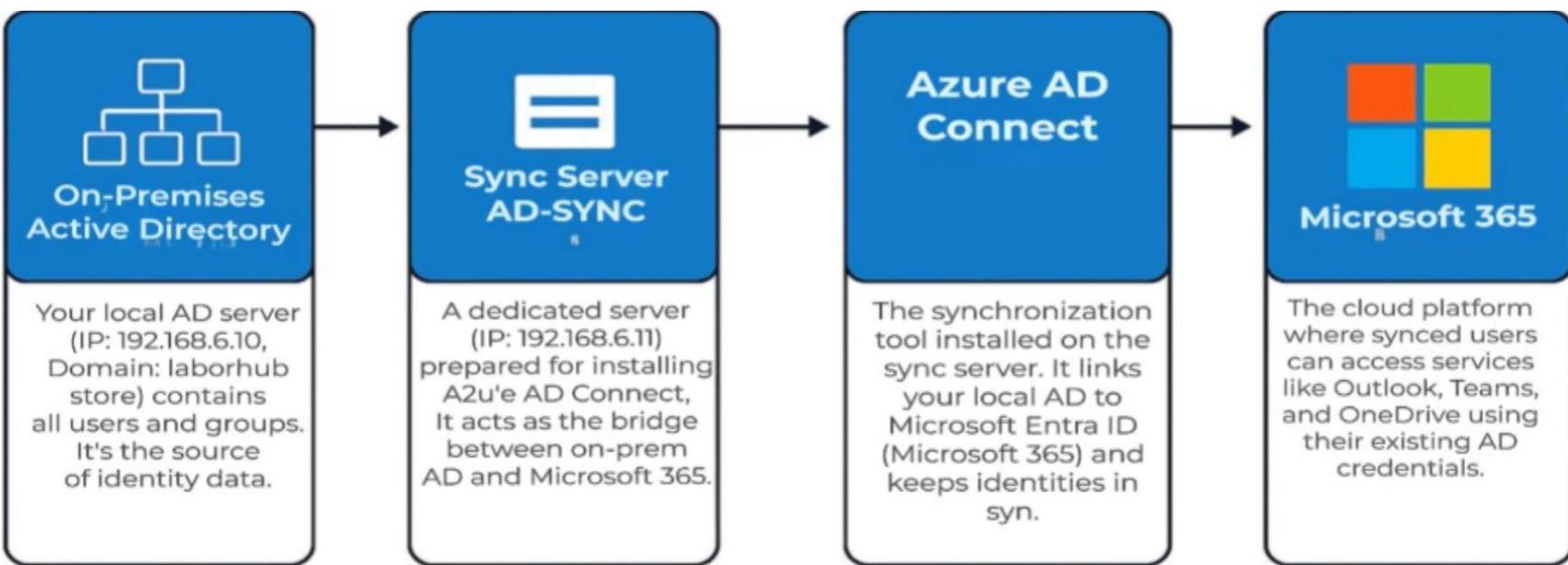
Add a user Multi-factor authentication Refresh Delete user Reset password

Home Copilot Agents Users Active users Contacts Guest users

Display name ↑	Username
Emily Johnson	d07b7639516f@Everestitt649.onmicrosoft.com
Michael Brown	michael.brown@laborhub.store

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 Connection 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



**On-Premises
Active Directory
(AD)**



**Azure AD
Connect**



**Microsoft 365
/ Entra ID**

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.