

SSPR & PASSWORD WRITEBACK CONFIGURATION GUIDE



Professional Introduction

The cover page introduces the guide with a clear title and subtitle outlining secure password management.

Hybrid Identity Diagram

Visual diagram illustrates user devices interacting with cloud and on-premises directories for password reset and writeback.

Core Network Components

The layout includes key components like Entra Sync Server, Active Directory Domain Controller, and DHCP-configured user PCs.

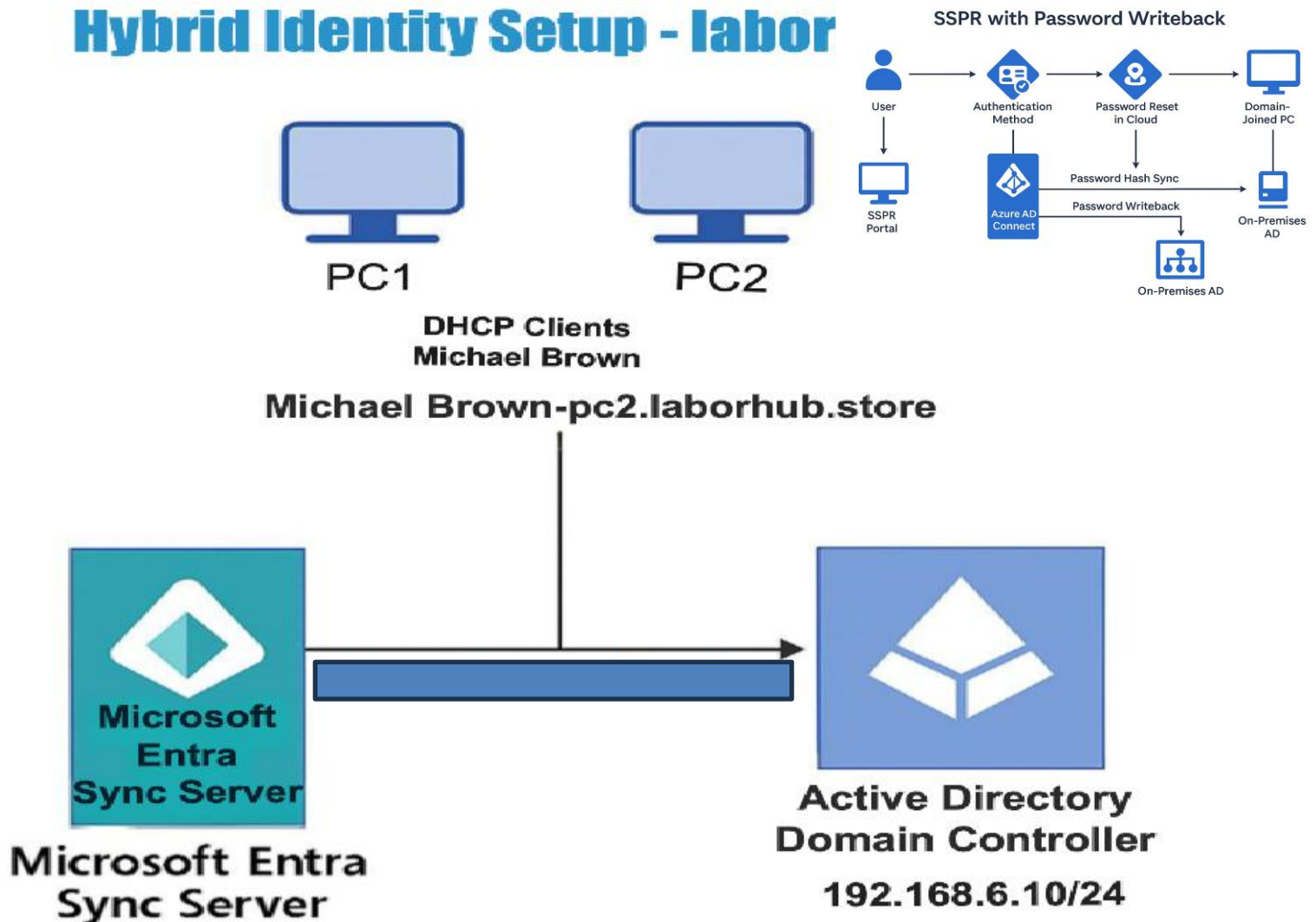
Synchronization Process

Synchronization between Entra Sync Server and Active Directory enables password writeback and secure user authentication.

User Integration Example

PC2, used by a real user, demonstrates practical application of the hybrid identity network setup.

Hybrid Identity Setup - labor



❑ Project Overview

This project demonstrates the configuration of Self-Service Password Reset (SSPR) using Microsoft Entra ID with password writeback to on-premises Active Directory. It enables users to securely reset their own passwords while ensuring changes are synchronized across cloud and on-prem environments, reducing helpdesk workload and improving user experience.

SSPR Feature Overview

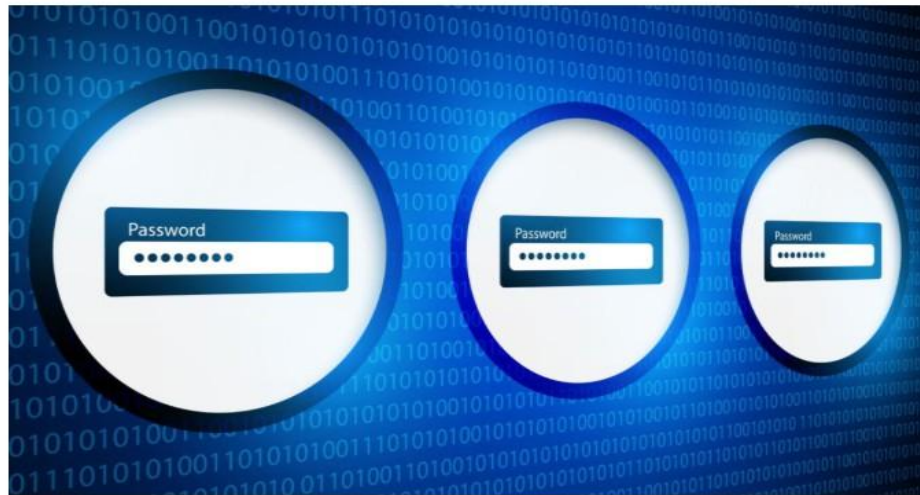
SSPR enables users to reset passwords independently, reducing IT support workload and improving user experience.

Hybrid Identity Integration

Configuring password writeback integrates cloud SSPR with on-premises Active Directory for hybrid identity management.

Security and Testing

The project focuses on enhancing security by setting authentication methods and validating configurations through testing.



❑ Technologies Used



Cloud Identity Management

Microsoft Entra ID enables cloud-based identity management for secure user authentication and access control.

Directory Synchronization

Microsoft Entra Connect synchronizes identity data between cloud and on-premises Active Directory environments.

Authentication Methods

Authentication methods like Microsoft Authenticator and SMS verification enhance security during password resets.

Hybrid Identity Features

Features such as password hash synchronization and password writeback ensure secure and seamless password management.

❑ Enabling SSPR and Authentication Methods

Enable SSPR Settings

Administrators enable SSPR by accessing password reset settings in the admin center for users or groups.

Configure Authentication Methods

Select authentication options like authenticator app, SMS, or email for secure identity verification.

Define Method Requirements

Set the number of required verification methods, typically one or two, based on security needs.

Apply Configuration Changes

Save settings to apply SSPR and authentication policies across the organization effectively.



❖ Sign in to Microsoft Entra Admin Center

- Go to: <https://entra.microsoft.com>
- Log in with your admin credentials.
- Navigate to Microsoft **Entra ID**
- On the left-hand menu, click Entra ID (under Favorites or main navigation).
- Go to Password Reset Settings
- Scroll down the left menu and click **Password reset**.
- Open **Properties**
- Under Manage, select Properties.
- **Enable SSPR for All Users**
- **Save Changes**

The screenshot displays the Microsoft Entra Admin Center web interface. The browser address bar shows the URL: https://entra.microsoft.com/#view/Microsoft_AAD_IAM/PasswordResetMenuBlade/~/_/Properties?Microsoft_AAD_IAM_legacyAADRedirect.... The left-hand navigation pane is visible, with the 'Microsoft Entra admin center' header. Under the 'Favorites' section, 'Entra ID' is highlighted. In the main navigation list, 'Password reset' is selected. The main content area is titled 'Password reset | Properties' and shows the 'Self service password reset enabled' toggle set to 'All'. A red circle highlights the 'Save' button at the top of the settings card. A red arrow points from the 'Save' button to the 'All' radio button. A blue information box at the bottom of the settings card states: 'These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.'

❖ Navigation Path

From the left menu:

➤ Password reset → Authentication methods

This section controls how users verify their identity when resetting passwords.

➤ Number of Methods Required to Reset

This means users need only one authentication method to reset their password.

If you select 2, users must complete two verification steps (more secure).

➤ Methods Available to Users

Currently, Security questions is shown but not checked.

You can enable this if you want users to answer security questions as a verification method.

➤ Auth Methods Policy Link

The blue link auth methods policy lets you manage other authentication methods (like phone, email, Microsoft Authenticator).

➤ Save Changes

After making changes, click Save at the top.

The screenshot shows the Microsoft Entra admin center interface. The top navigation bar includes the Microsoft Entra admin center logo, a search bar, and the Copilot logo. The left sidebar contains a navigation menu with options like Home, Password reset, Diagnose and solve problems, Manage, Properties, Authentication methods (highlighted with a red box), Registration, Notifications, Customization, On-premises integration, Administrator Policy, Activity, Audit logs, and Usage & insights. The main content area is titled 'Password reset | Authentication methods' and includes a 'Save' button (highlighted with a red arrow) and a 'Discard' button. Below the title, there is a message about Authentication Methods for SSPR and Signin. The 'Number of methods required to reset' is set to 1. The 'Methods available to users' section shows 'Security questions' as an option. A red arrow points to the 'auth methods policy' link in the text 'Use the auth methods policy to manage other authentication methods.' At the bottom, there is a note about the settings applying to end users and a link to learn more about administrator password policies.

- ❖ Enabling methods like **Microsoft Authenticator** and **SMS** ensures users have secure options for verification during password reset or sign-in.

The screenshot shows the Microsoft Entra admin center interface. The 'Auth Methods' page is active, displaying a list of authentication methods. The 'Auth Methods' title is highlighted with a red box. Below it, the 'Authentication method policies' section is visible, with a description: 'Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). [Learn more](#)'. A table lists various authentication methods, with 'SMS' highlighted by a red box and a red arrow pointing to it from the left sidebar.

Method	Target	Enabled
Built-In		
Passkey (FIDO2)		No
Microsoft Authenticator	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens	All users	Yes

- ❖ It enables SMS as an authentication method for all users and saves the configuration so they can receive one-time codes for sign-in or password reset.

Microsoft Entra admin center

Home > Auth Methods > SMS settings

This authentication method delivers a one-time code via SMS to a user's phone, and the user then inputs that code to sign-in. [Learn more.](#) SMS is usable for multi-factor authentication and Self-Service Password Reset; it can also be configured to be used as a first factor.

Enable and Target

Enable ☒

Include Exclude

Target ☒ All users ☐ Select groups

Name	Type	Use for sign-in	Registration
All users	Group	<input checked="" type="checkbox"/>	Optional

Save Discard

- ❖ Users are required to register for password reset when signing in (set to Yes), and they must re-confirm their authentication information every 180 days.

Microsoft Entra admin center

Home > Auth Methods > Password reset

Everestitt

Manage

Require users to register when signing in? ☒ Yes ☐ No

Number of days before users are asked to re-confirm their authentication information *

These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. [Click here to learn more about administrator password policies.](#)

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Domain services

Conditional Access

Multifactor authentication

Identity Secure Score

Authentication methods

Account recovery (Preview)

Password reset

Custom security attributes

Certificate authorities

External Identities

Properties

Authentication methods

Registration

Notifications

Customization

On-premises integration

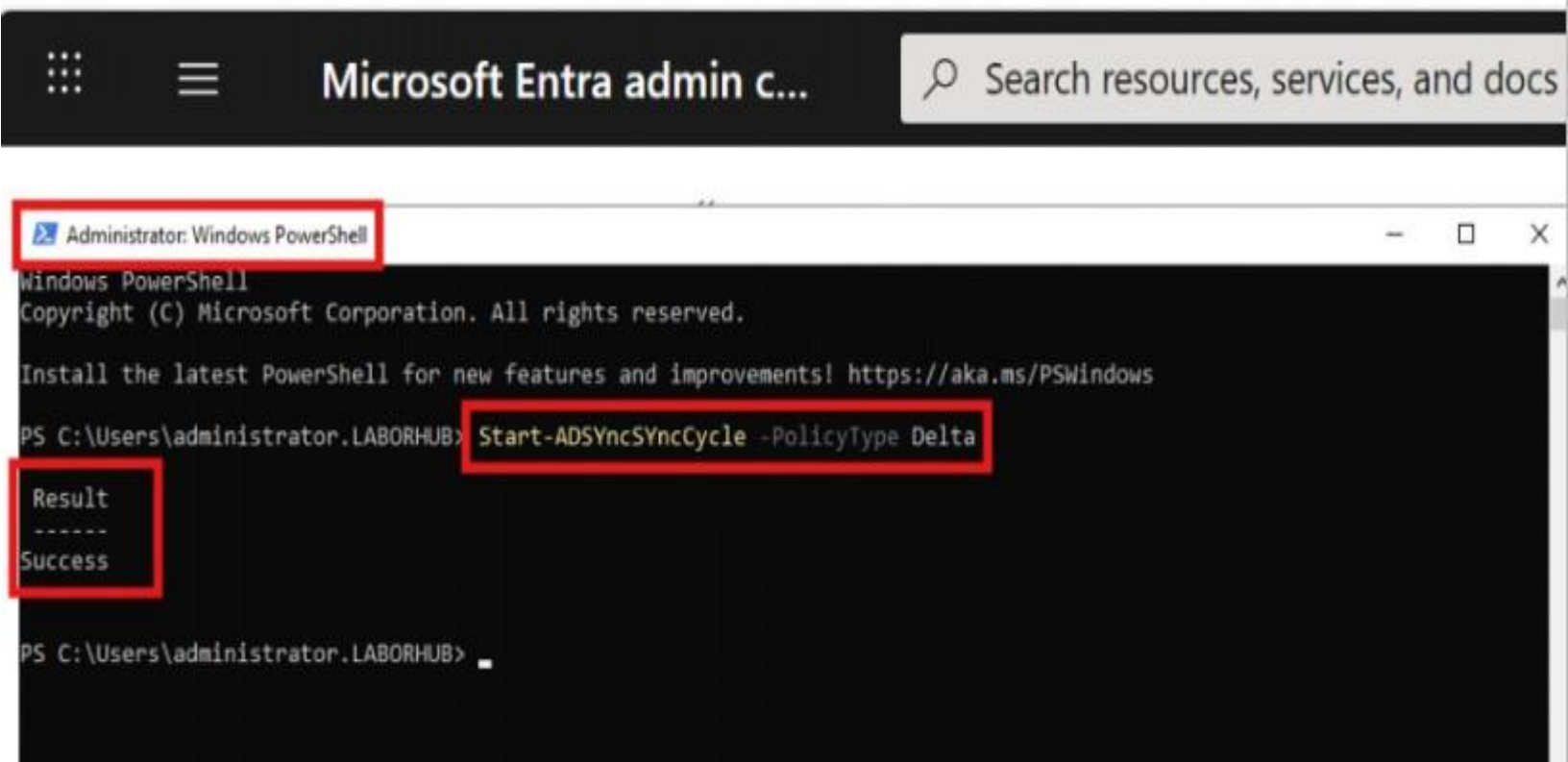
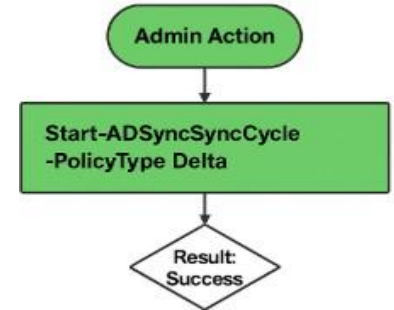
Administrator Policy

Audit logs

Usage & insights

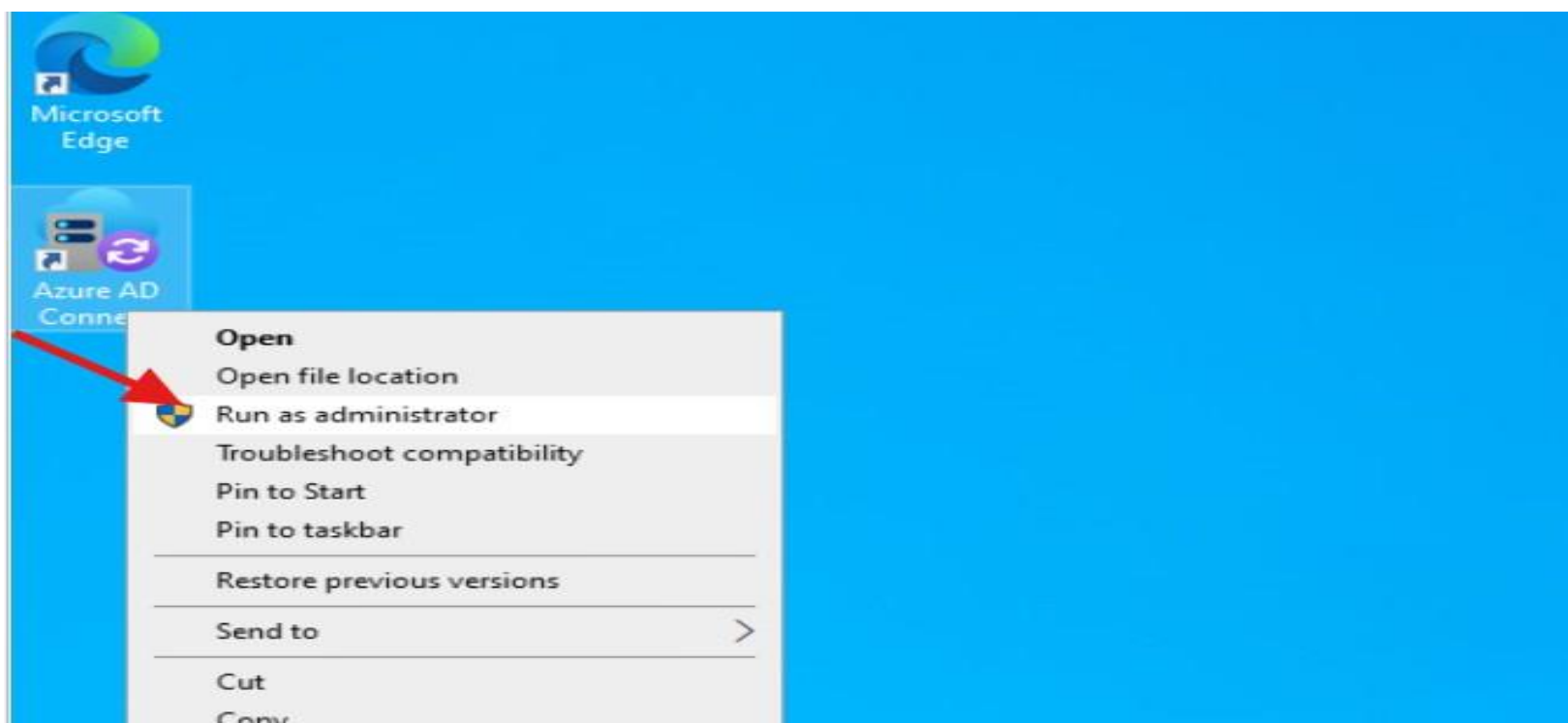
Troubleshooting + Support

- ❖ SYNC between on-prem Active Directory and Microsoft Entra ID, the result “Success” confirms it worked.

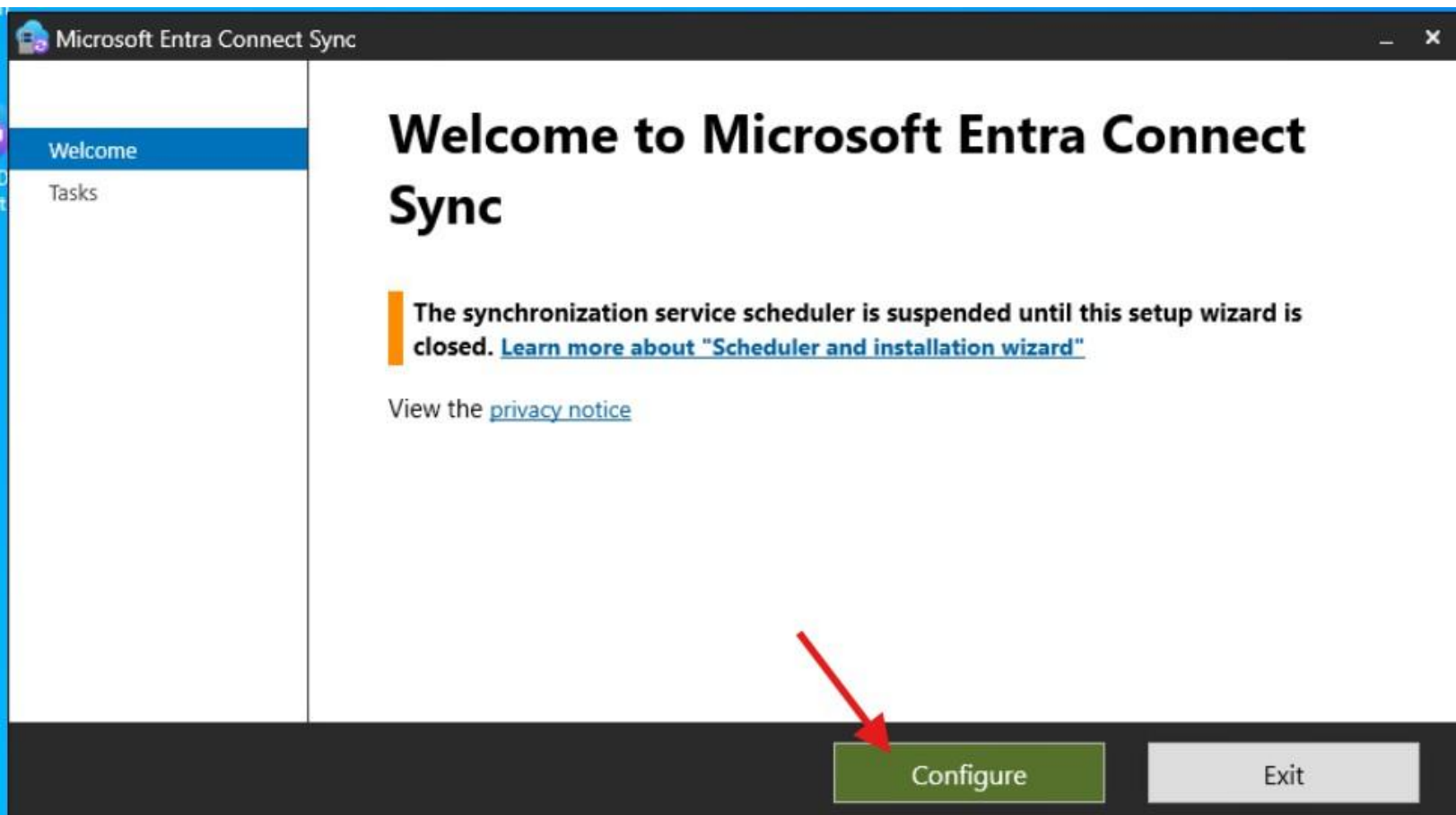


❖ “Run as administrator”

- This means you need to launch the Azure AD Connect tool with administrative privileges to configure or manage synchronization settings between on-prem Active Directory and Microsoft Entra ID.

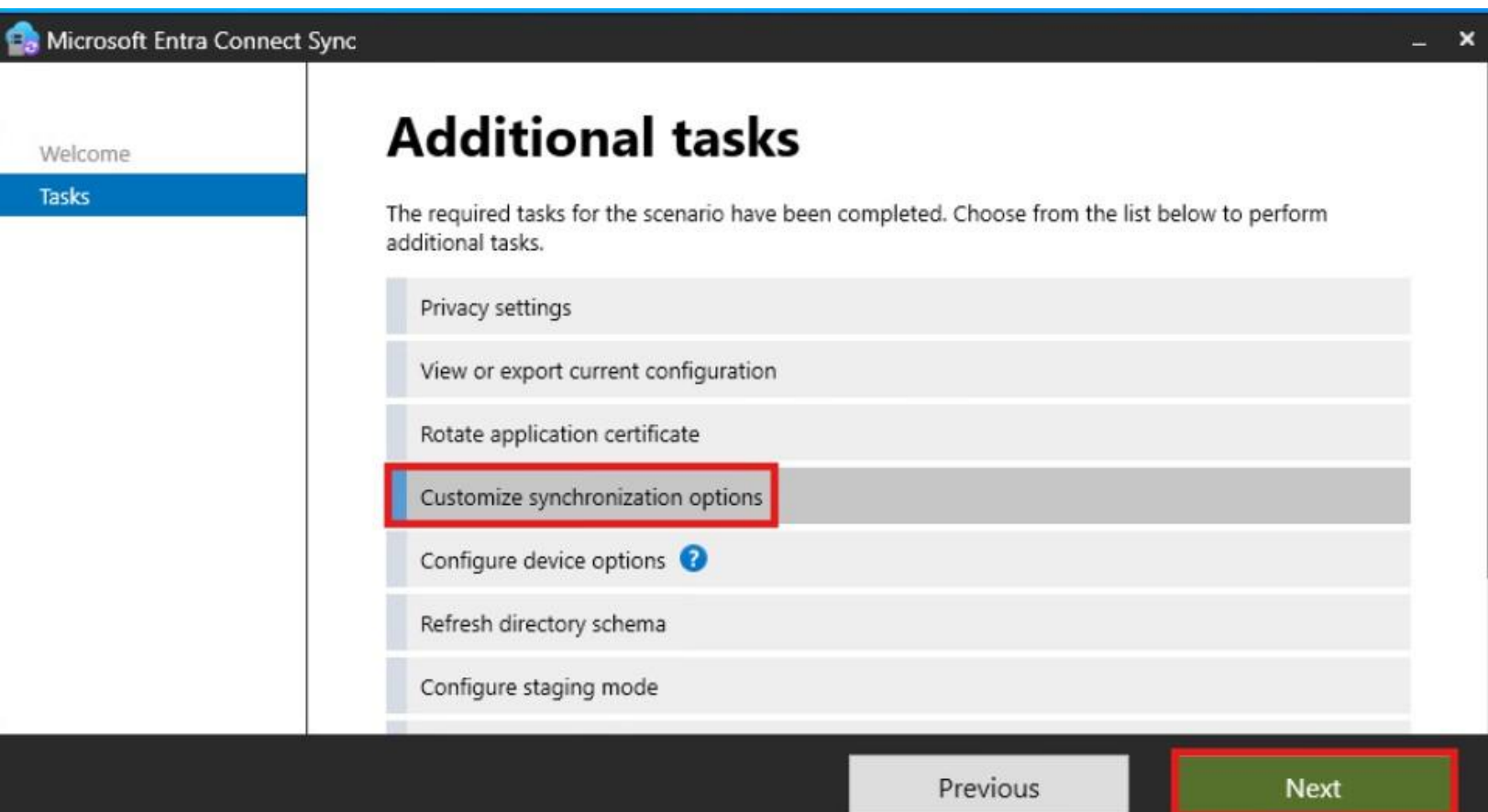


- ❖ Click **Configure** to start setting up Microsoft Entra Connect Sync.



“Customize synchronization options”

- ❖ This means you need to select this option to modify sync settings (such as enabling password writeback), and then click **Next** to proceed with the configuration.



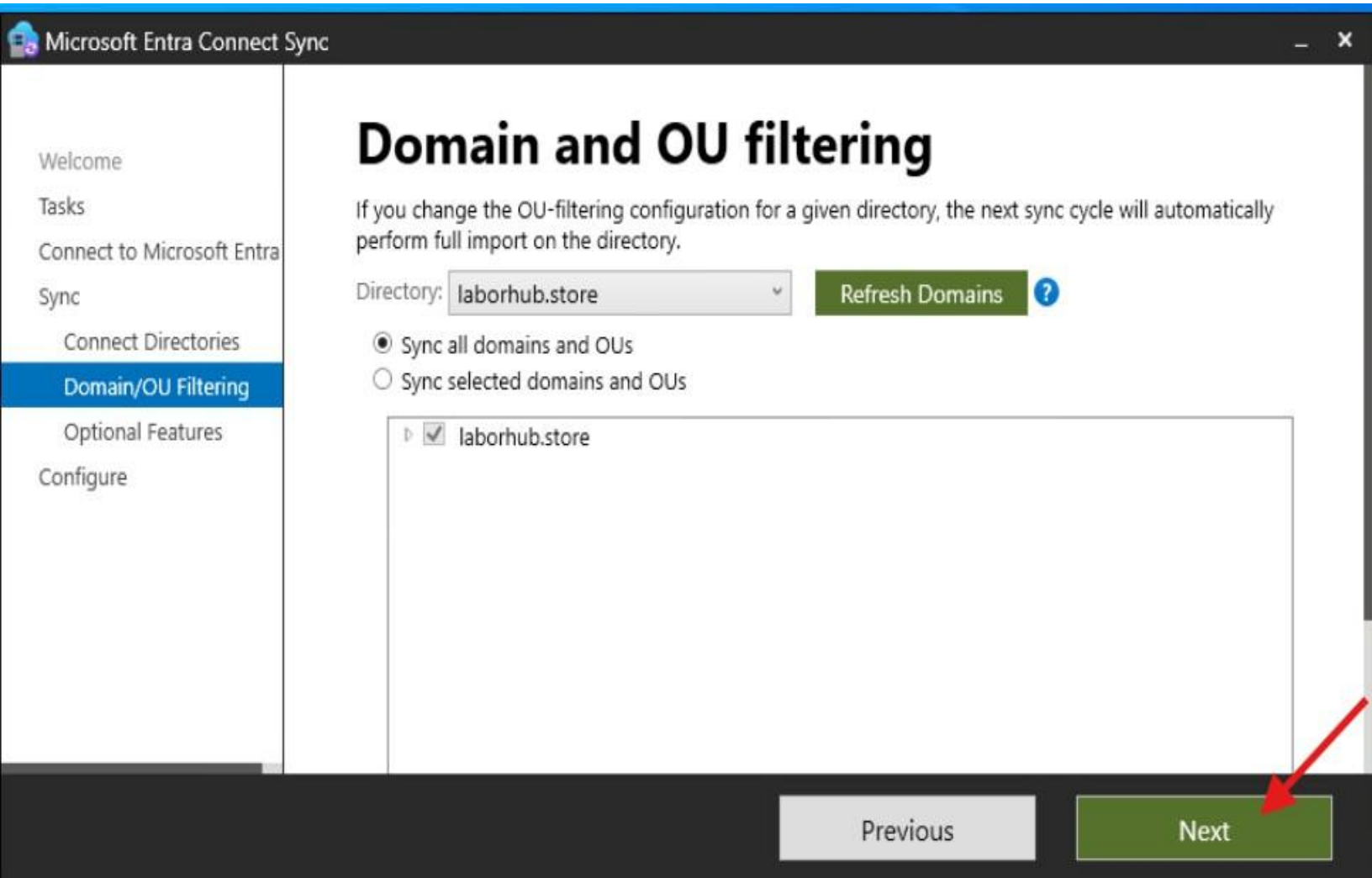
- ❖ Enter your Microsoft Entra admin credentials and click **Sign in** to connect Azure AD Connect to Microsoft Entra ID for synchronization setup.

The screenshot shows the 'Microsoft Entra Connect Sync' application window. On the left is a navigation pane with 'Connect to Microsoft Entra' selected. The main area is titled 'Connect to Microsoft' and contains a sign-in form. The form has a 'USERNAME*' field and a password field with the text 'Enter password' and masked dots. A red rectangle highlights the password field. Below the password field is a 'Forgot my password' link. At the bottom right is a blue 'Sign in' button, which is pointed to by a red arrow. A progress bar at the bottom indicates 'Connecting to Microsoft Online to verify credential'.

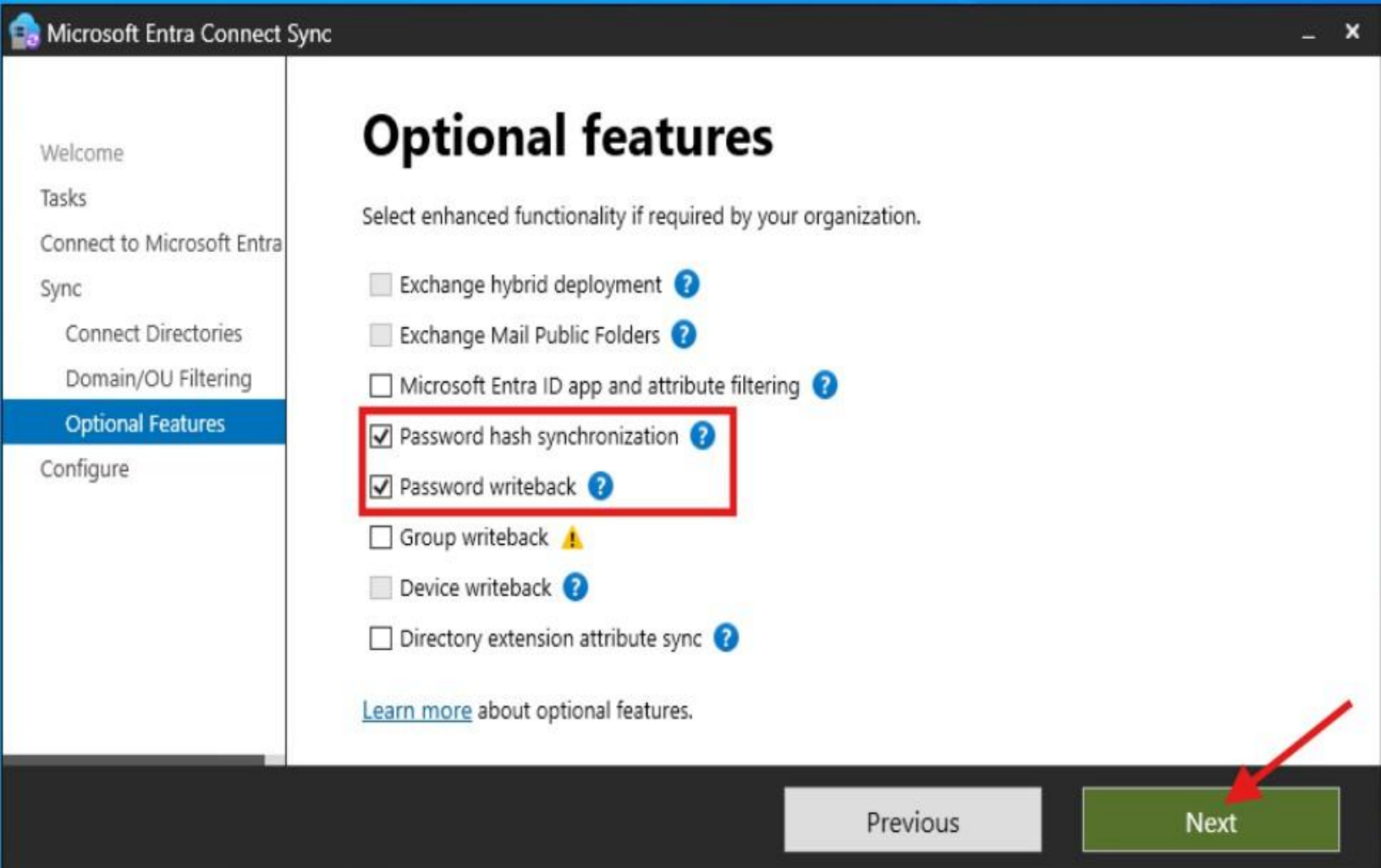
- ❖ Microsoft Entra Connect Sync is used to link your on-premises Active Directory to Microsoft Entra ID. It shows that the directory type selected is **Active Directory**, and the forest name entered is **laborhub.store**, which has been successfully added and verified (indicated by the green check mark). This step ensures that your local Active Directory environment is connected for synchronization with Microsoft Entra. Once the configuration is confirmed, you click **Next** to proceed to the next stage of the setup.

The screenshot shows the 'Microsoft Entra Connect Sync' application window at the 'Connect your directories' step. The left navigation pane has 'Connect Directories' selected. The main area is titled 'Connect your directories' and contains a form for adding directories. It has a 'DIRECTORY TYPE' dropdown set to 'Active Directory' and a 'FOREST' dropdown set to 'laborhub.store'. A green 'Add Directory' button is next to the forest field. Below these fields, a section titled 'CONFIGURED DIRECTORIES' shows 'laborhub.store (Active Directory)' with a green checkmark. At the bottom right, there are 'Previous' and 'Next' buttons. The 'Next' button is green and pointed to by a red arrow.

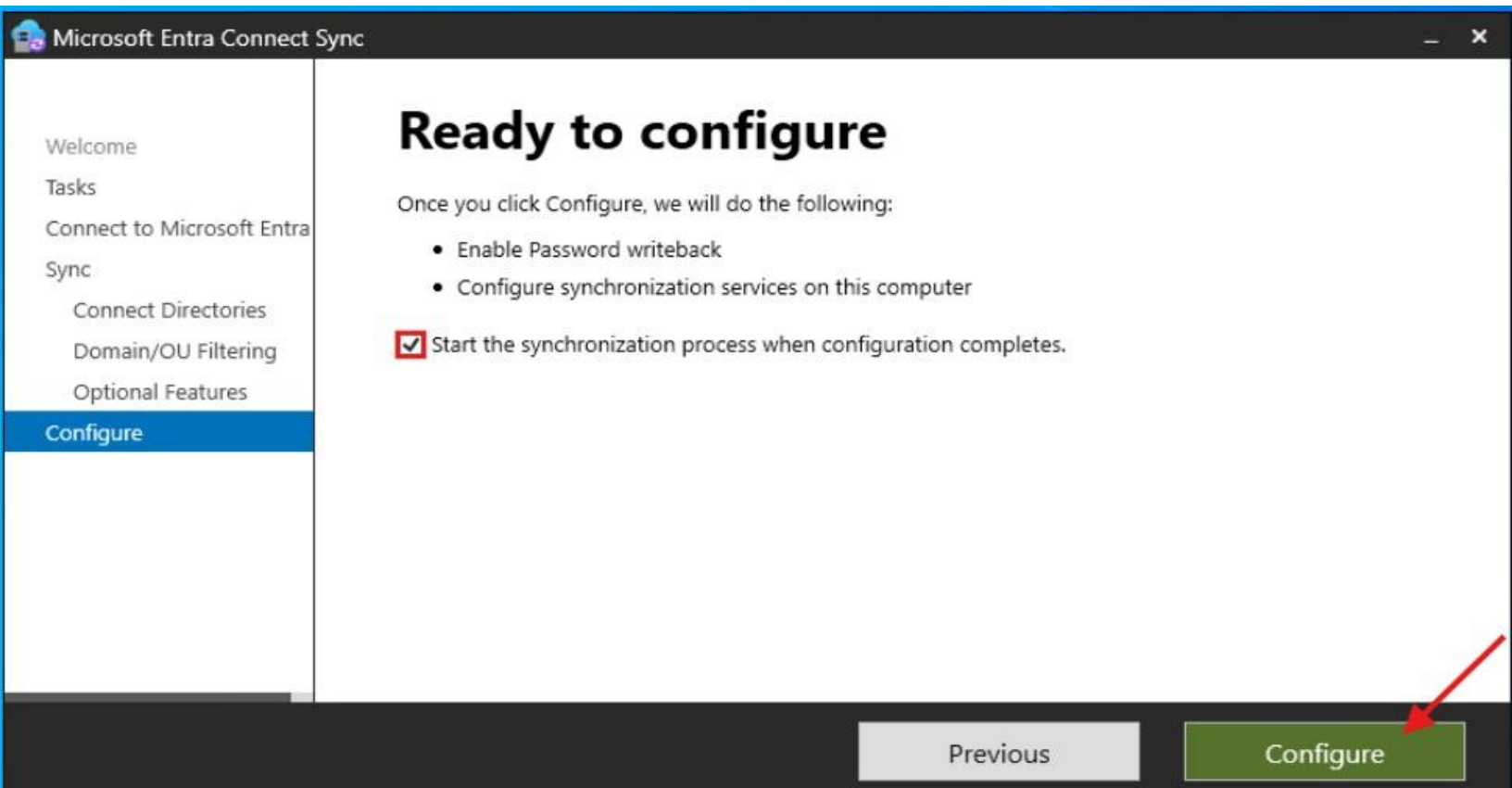
- ❖ This step decides whether to sync all OUs or only selected ones from your Active Directory to Microsoft Entra.



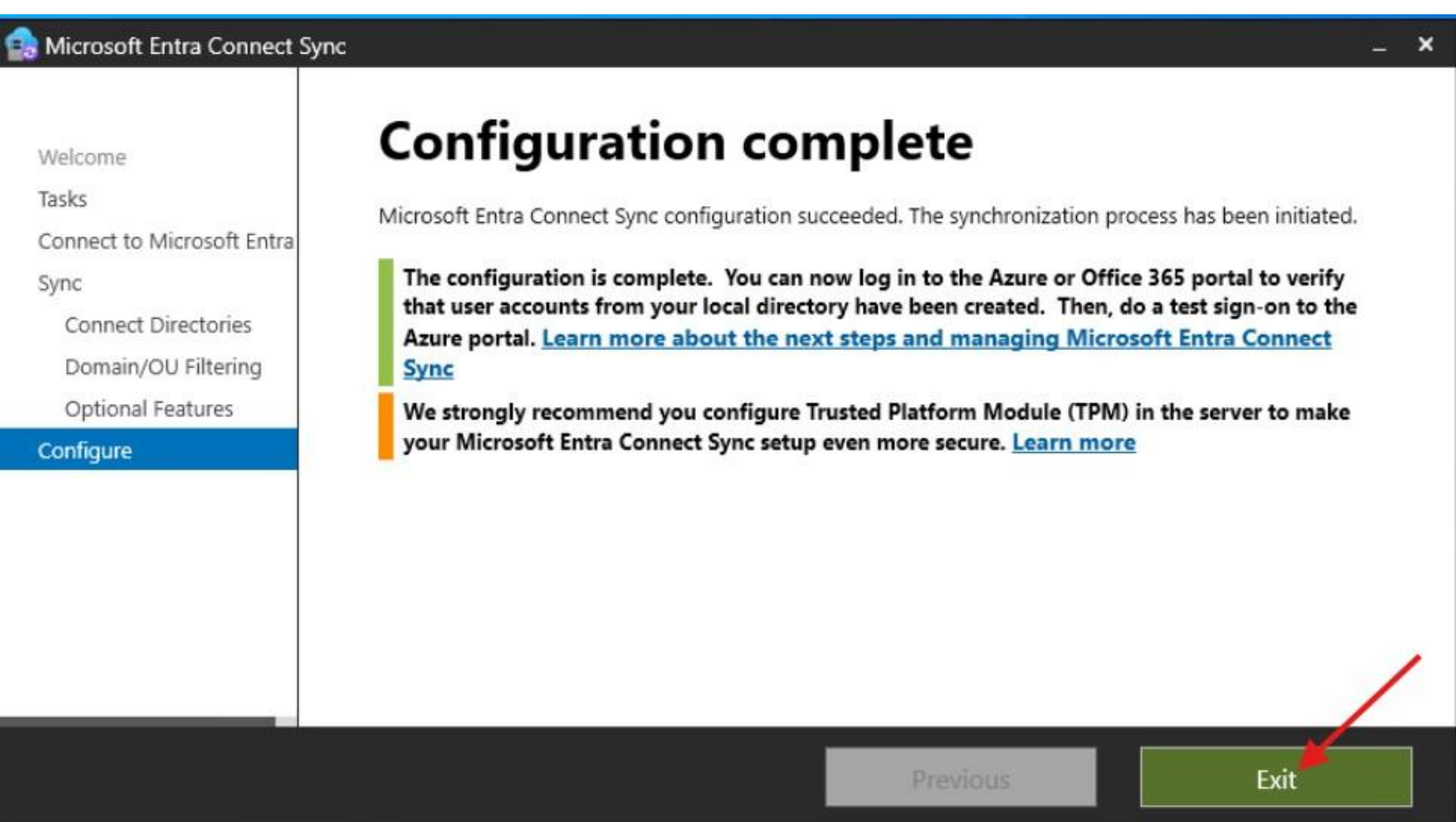
- ❖ This is the **Optional Features** step in Microsoft Entra Connect Sync. It lets you enable additional functionalities during synchronization.
- **Password hash synchronization** is checked, which means user password hashes from on-prem Active Directory will sync to Microsoft Entra ID for cloud authentication.
- **Password writeback** is also checked, allowing users to reset their passwords in the cloud (via SSPR) and have those changes written back to the on-prem Active Directory.
- ❖ After choosing the required features, you click **Next** to continue the configuration.



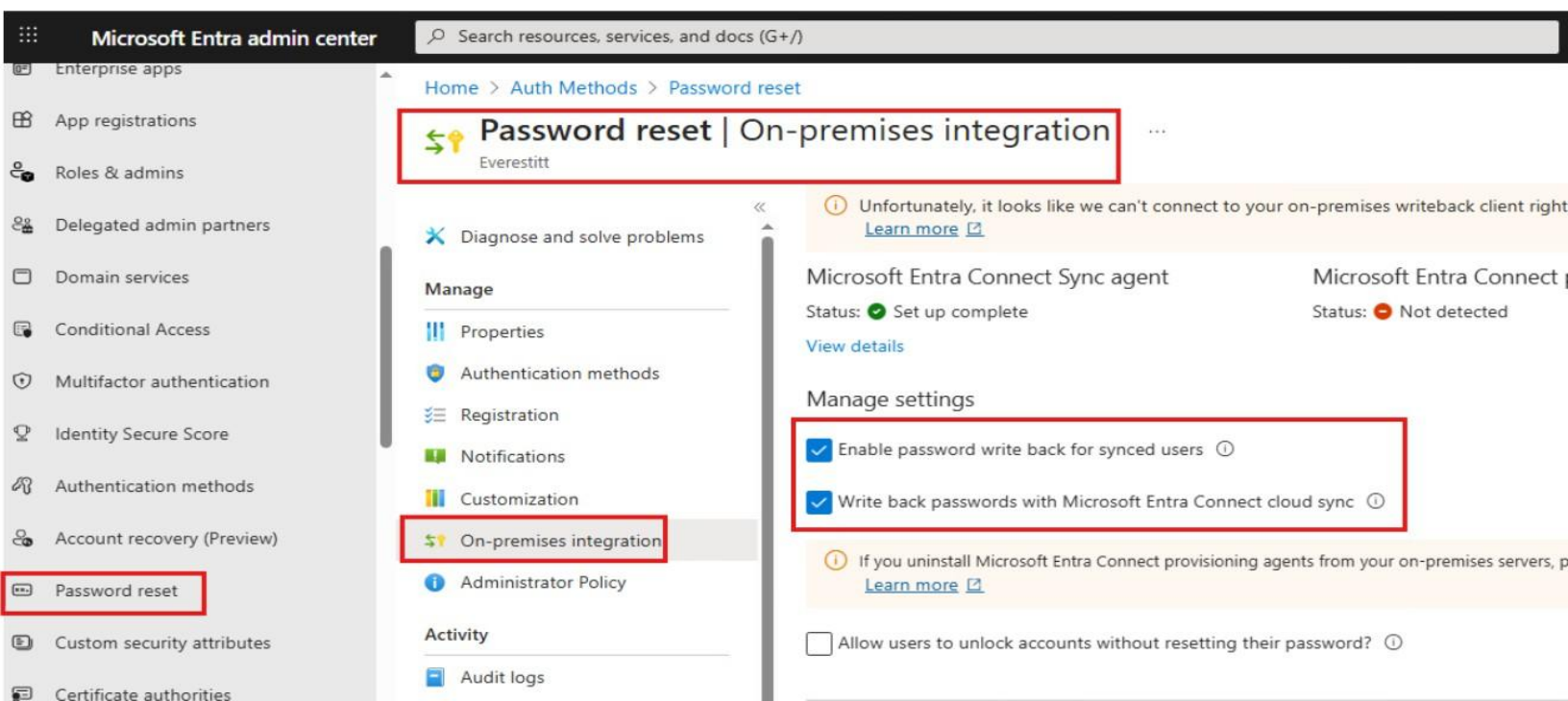
- ❖ It enables **Password hash synchronization** and **Password writeback**, sets up sync services on the computer, and begins the initial sync after clicking **Configure**.



- ❖ This confirms the sync setup is complete and advises verifying accounts and enhancing security.



- ❖ Microsoft Entra admin center shows the On-premises integration settings for password reset. It enables two key options: password writeback for synced users and write back passwords with Microsoft Entra Connect cloud sync, allowing password changes made in the cloud to update the on-premises Active Directory. This ensures seamless synchronization between cloud and local environments.



❖ Change Password While Signed In

- Go to myaccount.microsoft.com.
- Sign in with your current credentials.
- Select **Change Password**.
- Enter your old password, then set a new password.
- Submit and confirm the change.

The image shows a two-part screenshot of a web browser. The top part shows the Microsoft sign-in page at https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=8c59ea.... It features the Microsoft logo, a back arrow, the email michael.brown@laborhub.store, a red-bordered box around the "Enter password" field with masked dots, a "Forgot my password" link, and a blue "Sign in" button with a red arrow pointing to it. The bottom part shows the "My Account" page at <https://myaccount.microsoft.com>. The browser's address bar and the "My Account" header are visible. On the left is a navigation menu with "My Account" selected. The main content area has a blue banner with a new homepage notification. Below this are three tiles: "Michael Brown" (with a red box around the profile card), "Security info", and "Change password" (with a red box around the tile). The "Change password" tile includes a key icon, a description, and a red arrow pointing to the "CHANGE PASSWORD" link.

Sign in to your account

https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client_id=8c59ea... InPrivate

Microsoft

← michael.brown@laborhub.store

Enter password

.....

[Forgot my password](#)

Sign in

<https://myaccount.microsoft.com>

My Account

MB Michael Brown
michael.brown@laborhub.store

There's a new version of this homepage

My Account

Overview

Security info

Devices

Change password

Organizations

Settings & Privacy

Recent activity

MB

Michael Brown

michael.brown@laborhub.store

Security info

Keep your verification methods and security info up to date.

[UPDATE INFO >](#)

Change password

Make your password stronger, or change it if someone else knows it.

[CHANGE PASSWORD >](#)

- ❖ Your password has been successfully changed, and you can now use the new password to sign in.

My Sign-Ins ▾

MB Michael Brown
michael.brown@laborhub....

My Account ▾

- Overview
- Security info
- Devices
- Change Password
- Organizations
- Settings & Privacy
- Recent activity

My Apps

My Groups ▾

Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification [Change](#)

+ Add sign-in method

Password	Last updated: a few seconds ago	Change
Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 15 Pro Max	Delete

Lost device? [Sign out everywhere](#)

Success, password changed ✕
You can now use your new password when you next sign in.
[Done](#)

❖ Verify Password Writeback

On a domain-joined PC, sign out and log in with the **new password**.
If login succeeds, SSPR and Password Writeback are working correctly.

Student012-PC2

Enforce US Keyboard Layout

Other user

michael.brown

Sign in to: LABORHUB

Admin

Other user

SSPR – Common Troubleshooting

Issue: User can't reset password



Common Issues and Quick Checks

Common SSPR Issues

Users may face issues like inability to reset passwords or missing authentication methods during SSPR.

Configuration Checks

Verify SSPR is enabled and authentication methods are correctly configured in password reset properties.

Password Writeback and Sync

Ensure password writeback is active and Microsoft Entra Connect synchronization is successful for on-prem integration.

End-to-End Testing

Test by resetting password online and logging into a domain-joined PC to confirm functionality.

Troubleshooting Paths

Verify Licensing

Ensure Microsoft Entra ID P1 or higher license is active to enable SSPR functionality.

Check User Registration

Confirm users have registered authentication methods required for self-service password reset.

Audit Log Review

Analyze audit logs in the admin center to identify failed attempts or synchronization errors.

Network Connectivity Validation

Verify network connections between sync servers and on-premises Active Directory are stable.

1 Check SSPR Status

Path: Microsoft Entra admin center → Password reset → Properties

✓ Ensure SSPR is enabled for All users or the correct group



2 Verify Authentication Methods

Path: Password reset → Authentication methods

✓ Confirm methods like Microsoft Authenticator or SMS



3 Confirm Password Writeback

Path: Password reset → On-premises integration

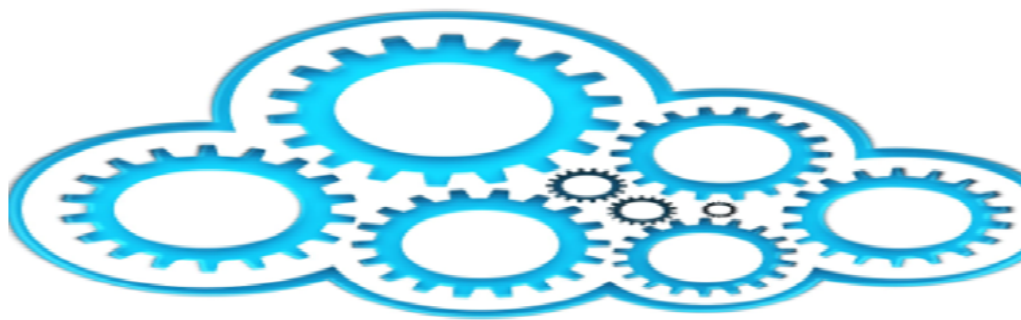
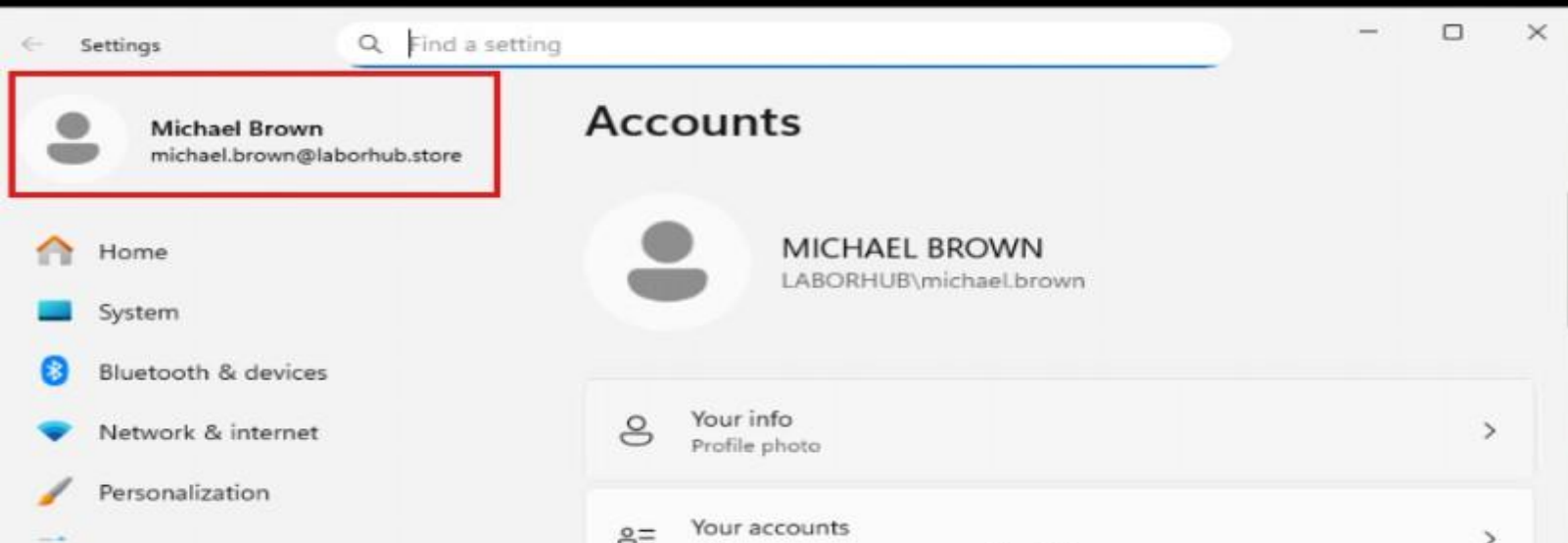
✓ Password writeback enabled ✓ Microsoft Entra Connect status = Success



4 Test End-to-End

- ❖ This step confirms that the user has successfully logged in to a **domain-joined PC** using the **new password** that was reset through SSPR, proving that **Password Writeback to on-prem Active Directory is working**.

Student012-PC2



❑ Conclusion

This project shows how SelfService Password Reset (SSPR) can be configured using Microsoft Entra ID with password writeback to on-premises Active Directory to solve a common IT support problem. By enabling SSPR, users can securely reset their own passwords while ensuring changes are synced across cloud and local systems, which helps reduce helpdesk tickets and saves time. The project also includes practical troubleshooting steps, such as checking SSPR settings, authentication methods, password writeback status, and testing end-to-end user login, to quickly identify and fix issues. Overall, this project demonstrates real-world IT support skills, focusing on security, user experience, and reliable problem resolution in a hybrid environment.

Hybrid Identity Configuration

This project showcases configuring hybrid identity using Microsoft Entra ID and Active Directory for seamless integration.

Self-Service Password Reset

Implementing SSPR with password writeback enhances password management security and user convenience.

Troubleshooting and Support

Documented troubleshooting steps demonstrate diagnosing and resolving common hybrid identity issues effectively.

Thank You!

I hope this guide helps you implement secure password management and hybrid identity solutions with confidence.