

Password Writeback

Password writeback can be used to synchronize password changes in Azure AD back to your on-premises AD DS environment. Azure AD Connect provides a secure mechanism to send these password changes back to an existing on-premises directory from Azure AD.

Prerequisites:

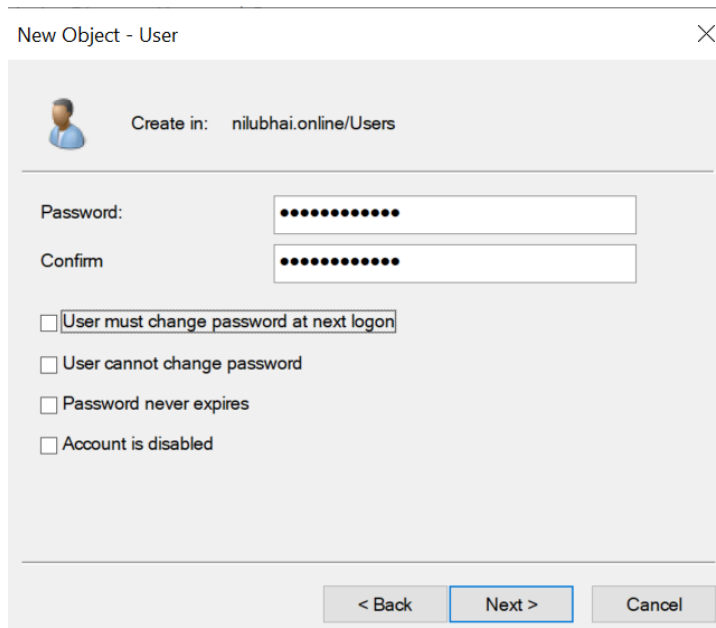
A working Azure AD tenant with at least an Azure AD Premium P1 or trial license enabled.

Azure AD configured for self-service password reset.

An existing on-premises AD DS environment configured with a current version of Azure AD Connect.

Azure AD Connect lets you synchronize users, groups, and credential between an on-premises AD DS environment and Azure AD. You typically install Azure AD Connect on a Windows Server 2016 or later computer that's joined to the on-premises AD DS domain.

Step 1: Create on Prem Users and Sync that users to Azure Ad and Assign Azure P1 or P2 Licenses to the users make sure while creating users on-prem you should not assign any password policy to a user.



New Object - User

Create in: nilubhai.online/Users

Password:

Confirm:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

Step 2: Enable Self Service Password Reset for the Users that are Sync in Azure AD. For enabling SSPR go to Users→Password Reset→Properties.

The screenshot shows the Azure Active Directory (Azure AD) interface for configuring Password Reset properties. The breadcrumb navigation at the top reads: Home > Contoso | Users > Users | Password reset > Password reset. The main heading is "Password reset | Properties" with a three-dot menu icon. Below the heading, it says "Contoso - Azure Active Directory".

On the left is a navigation pane with sections: "Diagnose and solve problems" (with a wrench icon), "Manage" (with a list icon), "Activity" (with a clock icon), and "Troubleshooting + Support" (with a question mark icon). Under "Manage", the following items are listed: "Properties" (highlighted with a blue bar), "Authentication methods", "Registration", "Notifications", "Customization", "On-premises integration", and "Administrator Policy".

The main content area has a top bar with a back arrow, "Save" (with a floppy disk icon), and "Discard" (with an 'X' icon). Below this, it says "Self service password reset enabled" with an information icon. There are three radio buttons: "None", "Selected" (which is selected and highlighted in blue), and "All".

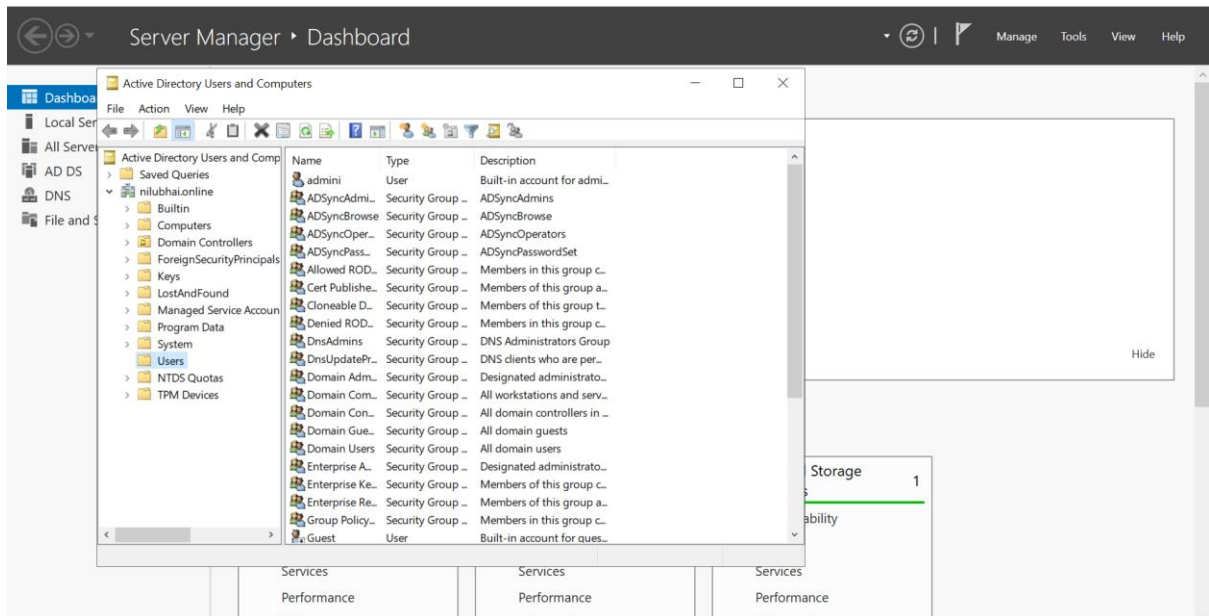
Below the radio buttons is a section titled "Select group" with an information icon. It contains a single entry, "SSPR", which is highlighted in blue.

At the bottom of the main content area is a light blue information box with an 'i' icon. The text inside reads: "These settings only apply to end users in your organization. Administrators and are required to use two authentication methods to reset their password policies."

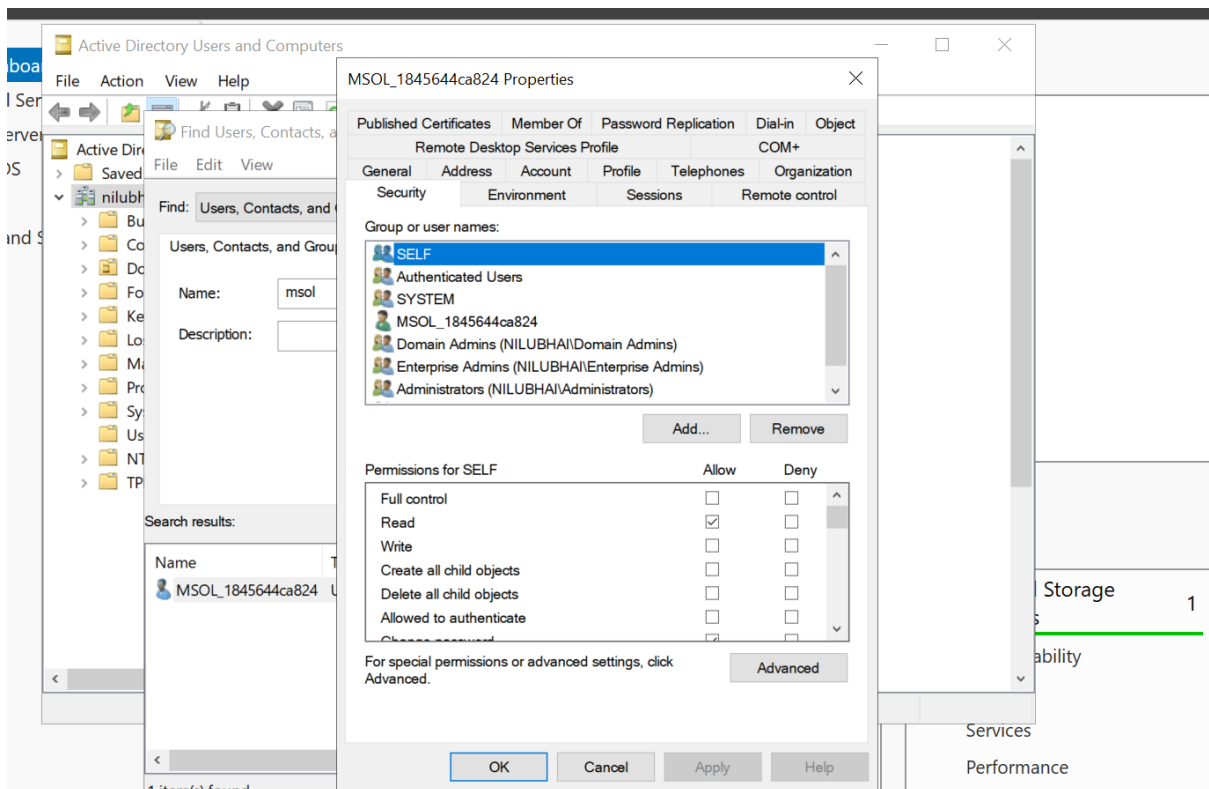
Step 3: Assign certain permissions on the service account of Azure Ad Connect

When we install Azure Ad Connect one service account is created on On-prem and one is created on Azure Active Directory.

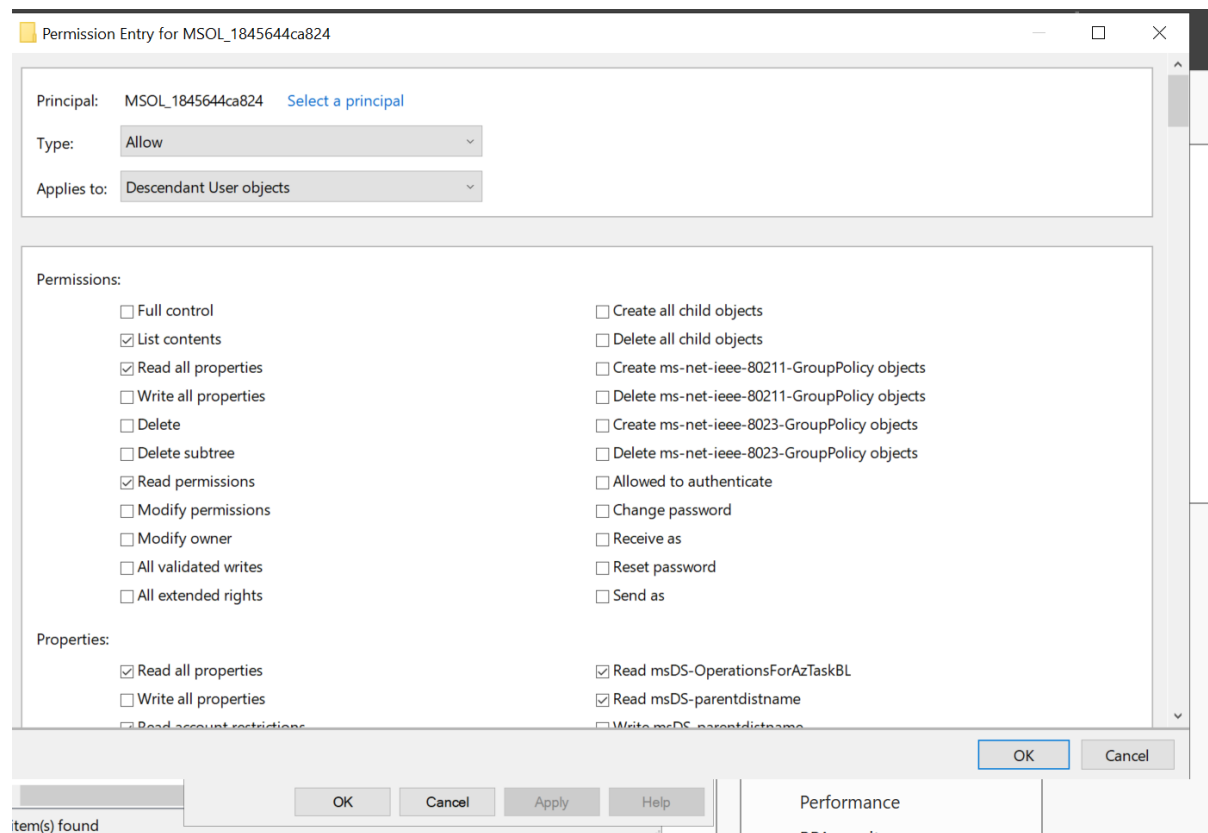
Go to Active Directory users and Computer right click on Domain name and Find for service account Msol.



Click on MSOL service account and Go to security and click on Advance Options



After clicking on Advanced Go to add options and select user principal as MSOL Service account and Applies to: Descendant User Objects. And Type: Allow



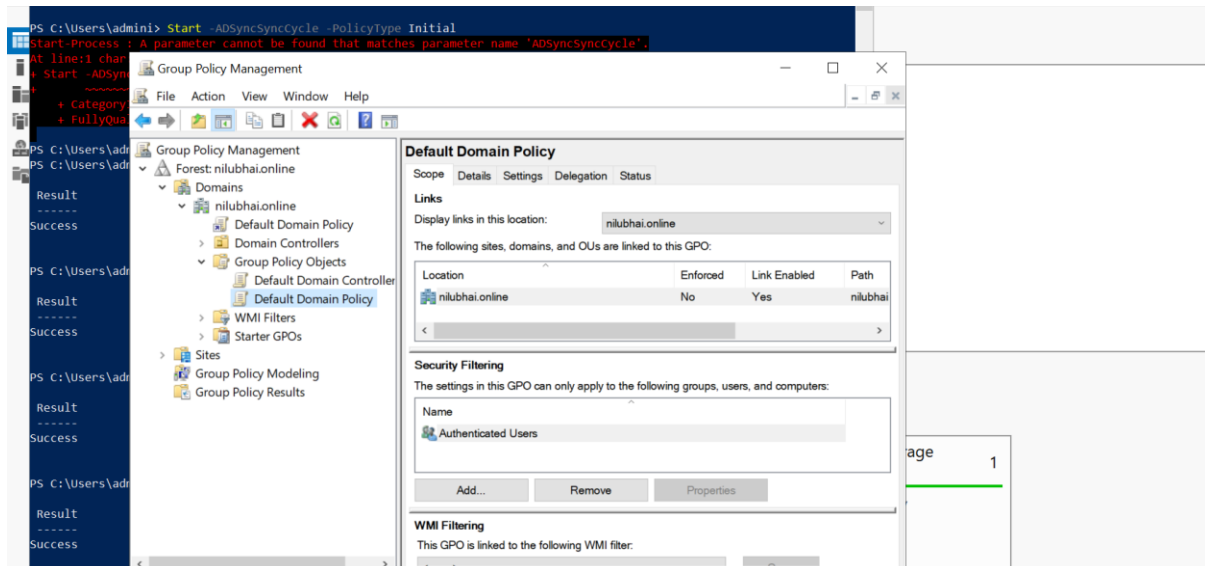
Now Select the Following Permissions:

- Reset Password
- Change Password
- Write lockout time
- Write pwdlastset

Now click on Apply and Ok.

Step 4: Now we have to make certain changes in Group Policy Management

Right Click on Default Domain Policy and Click on Edit:




Under Computer Configuration expand Policy → Windows Settings → Security Settings → Account Policies → Password Policy this is the password policy for On-prem Active Directory set minimum password age = 0.

This password policy will be applicable to Azure AD when the users are sync.

Step 5: Now open Azure AD Connect and click on configure and customize synchronization options click on next type password for Azure AD in optional features check for Password Writeback feature.

Step 6: Go to Azure Portal Users → Click on Password Reset → Go to on-premises Integration and make some changes and click on save.

✔ Your on-premises writeback client is up and running.
[Learn more](#) 

Azure AD Connect sync agent




Status: ✔ Set up complete

[View details](#)

Azure AD Connect provisioning agent (cloud sync)

Status: ❌ Not detected

Manage settings

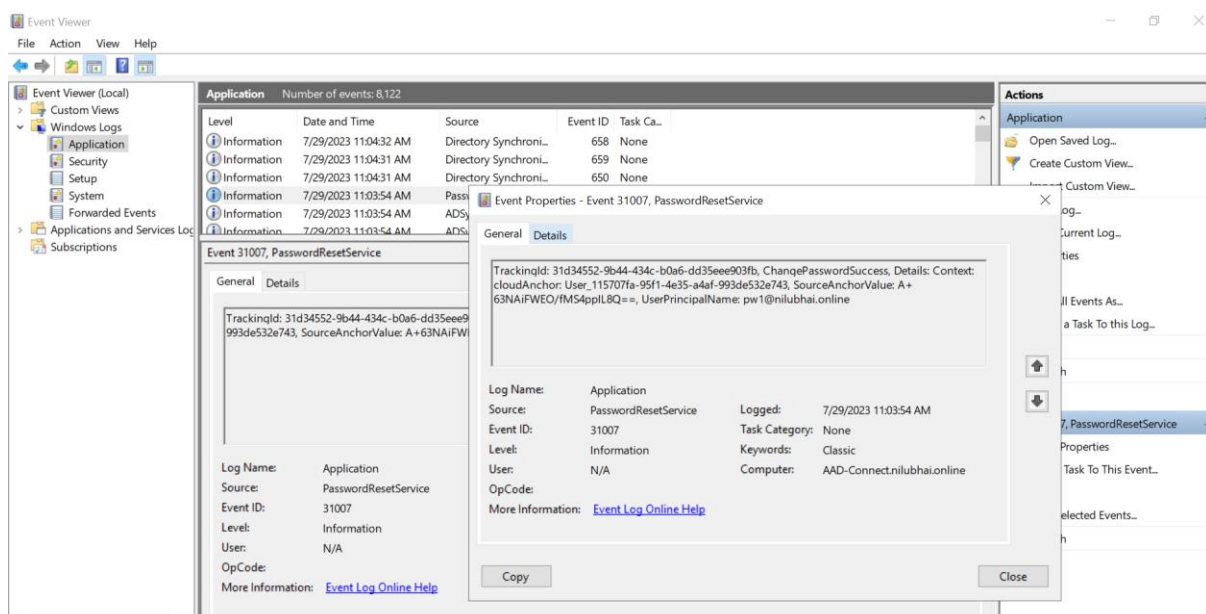
- ☒ Enable password write back for synced users 
- ☐ Write back passwords with Azure AD Connect cloud sync 
- ☒ Allow users to unlock accounts without resetting their password? 

Save

Discard

Step 7: Login to portal.office.com with the created user and try to change password for the following account.

Step 8: Go the Event viewer logs in Windows Logs → Application → Password Reset Service.



Here you can see password has also been changed for On-prem active directory.