**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:**

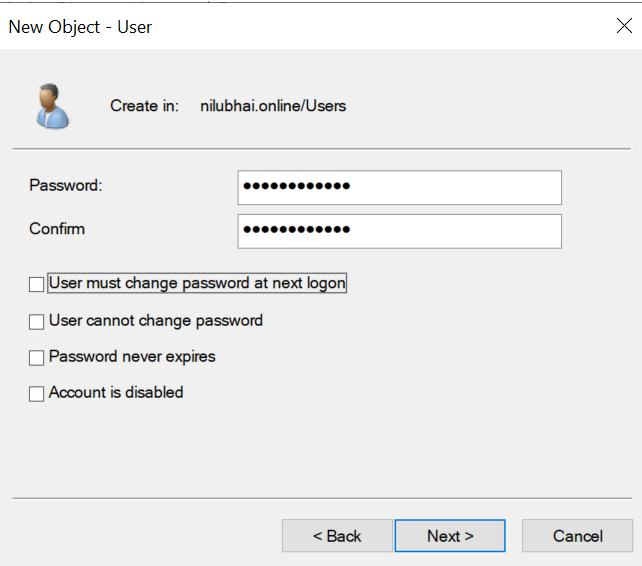
A working Azure AD tenant with at least an Azure AD Premium P1 or trial license enabled.

Azure AD configured for self-service password reset.

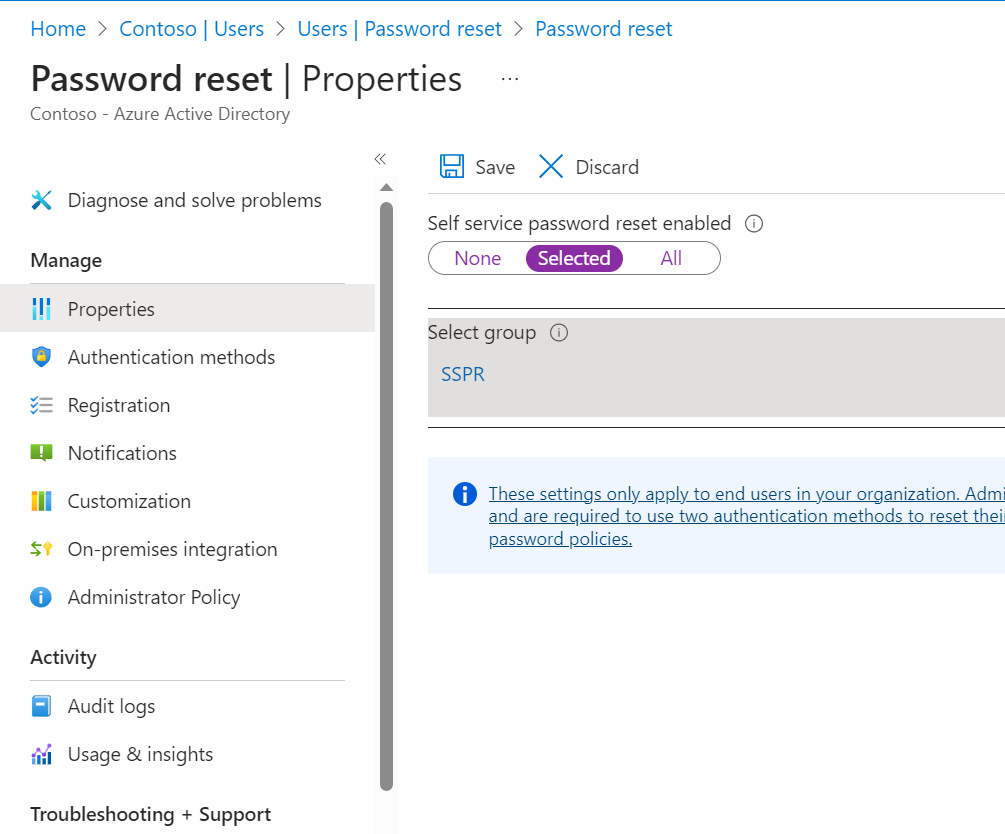
An existing on-premises AD DS environment configured with a current version of Azure AD Connect.

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.



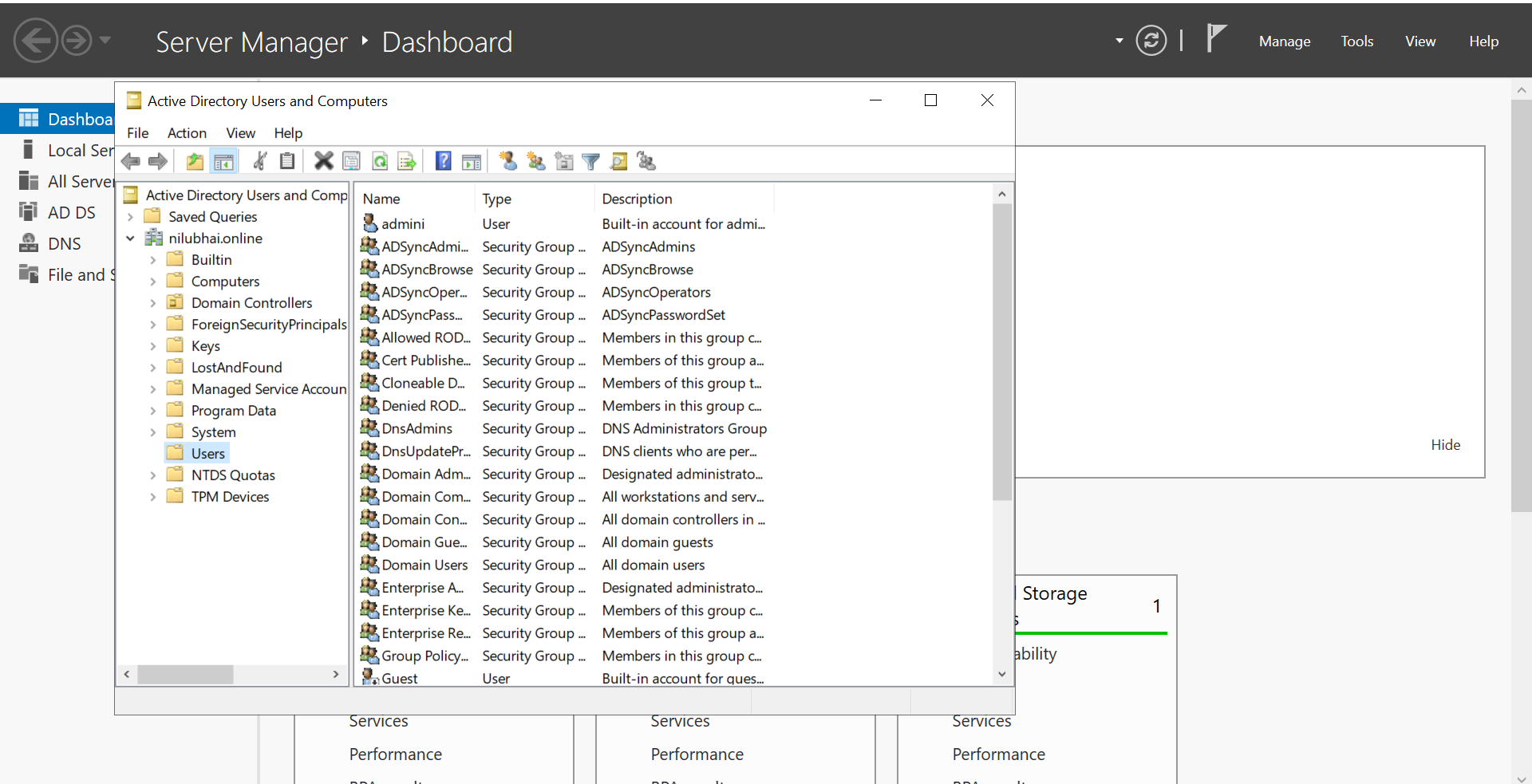
**Step 2:** Enable Self Service Password Reset for the Users that are Sync in Azure AD. For enabling SSPR go to Users🡪Password Reset🡪Properties.



**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 create 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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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:

A screenshot of a computer

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

**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.

A screenshot of a computer

Description automatically generated

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