AZURE AD CONNECT

1. Log on your Server with Pa55w.rd
2. Click on the internet explorer icon on the taskbar
3. Type "portal.office.com) Enter the the text where the cursor is blinking", press Enter.
4. Click in the Sign in box and sign in using admin@m365x010806.onmicrosoft.com. Password Xtr3msL@bs. Click Yes to stay signed in.
5. Click Yes to the message above the task bar.
6. Close the Microsoft Message box.
7. Click on "Got it" and double click on the Admin icon.
8. Click on show all to expand the items in the left margin.
9. Select Azure Active directory
10. In the Right pane scroll down until you see click on AzureAD Connect.
11. Select on Azure AD Connect
12. Scroll down and click on Download Azure AD connect
13. When the file downloads you will see that the file has already been dowloaded and you are ready to navigate through the wizard.
14. On the Welcome to Azure AD Connect page select the check box next to I agree and click on continue.
15. Select Use Express settings.
16. Login with Adatum.com\Administrator, password Pa55w.rd
17. Click on Next
18. For our lab purposes Click on "continue without matching all UPN suffixes to verified domains"
19. Click on Next to Continue, Review your options then click on Install
20. Your configuration should be complete. Click on Exit.
21. Close the Download page.
22. Scroll down the page and click on Enabled State rollout
23. Observe the Authentication Methods
24. Select passthrough Authentication
25. Click on Ok
26. Close the message at the top left of the screen and click on password has sync. Select ok.
27. Close the window.
28. Azure AD connect password hash vs Pass Through
29. Similar to **Password Hash** Synchronization, **Azure AD Pass-through** Authentication allows users to sign in to on-prem apps as well as cloud-based apps, **using** the same **password**. However, **pass-through** authentication validates user **passwords** directly against the on-premises **Active Directory**.

Password hash synchronization

With password hash synchronization, hashes of user passwords are synchronized from on-premises Active Directory to Azure AD. When passwords are changed or reset on-premises, the new password hashes are synchronized to Azure AD immediately so that your users can always use the same password for cloud resources and on-premises resources. The passwords are never sent to Azure AD or stored in Azure AD in clear text. You can use password hash synchronization together with password write-back to enable self-service password reset in Azure AD.

In addition, you can enable Seamless SSO for users on domain-joined machines that are on the corporate network. With single sign-on, enabled users only need to enter a username to help them securely access cloud resources.

Pass-through authentication

With pass-through authentication, the user’s password is validated against the on-premises Active Directory controller. The password doesn't need to be present in Azure AD in any form. This allows for on-premises policies, such as sign-in hour restrictions, to be evaluated during authentication to cloud services.

Pass-through authentication uses a simple agent on a Windows Server 2012 R2 domain-joined machine in the on-premises environment. This agent listens for password validation requests. It doesn't require any inbound ports to be open to the Internet.

In addition, you can also enable single sign-on for users on domain-joined machines that are on the corporate network. With single sign-on, enabled users only need to enter a username to help them securely access cloud resources.