**Module 6: Implementing Azure Active Directory**

**Lab: Implementing Azure Active Directory**

**Exercise 1: Administering Azure AD**

**Task 1: Create an Azure Active Directory tenant**

1. Ensure that you are signed in to Wintellect10 as **Administrator** with the password **@Pa55w.rd**.
2. Start the browser and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com/), and then sign in using the Microsoft account that is the Azure Cloud Slice account for listed in the LODs Resources tab.
3. In the Azure portal, in the hub menu, click **+ Create a resource**, click **Identity** and then, click **Azure Active Directory**.
4. On the **Create directory** blade, specify the following and click **Create**:

* Organization name: **Wintellect**
* Initial domain name: **WintellectLocalXX** (Where XX is your student number)
* Country or region: **United States**

1. Leave Microsoft Edge open and wait until the Azure Active Directory tenant is provisioned. Note the unique name you specified, since you will need it later in this task.

**Task 2: Activate Azure AD Premium trial**

1. Refresh the Microsoft Edge window displaying the Azure portal. Next, click the **Directory + subscription** filter icon appearing directly to the left of your name in the upper right corner of the Azure portal and, in the **Directory + Subscription** pane, click the name of the Azure Active Directory tenant you created in the previous task.
2. In the hub menu of the Azure portal, click **Azure Active Directory**. This will display the **WintellectLocal** Azure Active Directory tenant blade.
3. Click **Start a free trial**.
4. In the **Azure AD and Office 365** section, click **Get a free trial for Azure AD Premium**.
5. On the **Activate** blade, in the **AZURE AD PREMIUM P2** section, click **Free trial**.
6. On the **Activate Azure AD Premium P2 trial**, click **Activate**.
7. Wait until the Azure AD Premium trial is successfully activated.

**Task 3: Manage users by using the Azure portal**

1. Navigate back to the **WintellectLocalXX** Azure Active Directory tenant blade.
2. On the WintellectLocalXX blade, click **Users**.
3. Click **+ New user**
4. On the **User** blade, specify the following settings (where ***domain-name*** is the name you assigned to the Azure Active Directory tenant in the first task of this exercise):

* Name: **Jeff Prosise**
* User name: **jeff@*WintellectLocal*.onmicrosoft.com**

1. Click **Profile** and, on the **Profile** blade, specify the following settings and click **OK**:

* First Name: **Jeff**
* Last Name: **Prosise**

1. Accept the default **Properties**, **Groups** and **Directory role** settings, click the **Show Password** checkbox and note the temporary password.
2. Click **Create**.
3. Click **+ New user**
4. On the **User** blade, specify the following settings (where ***domain-name*** is the name you assigned to the Azure Active Directory tenant in the first task of this exercise):

* Name: **Kimberly Pruitt**
* User name: **kim@*WintellectLocal*.onmicrosoft.com**

1. Click **Profile** and, on the **Profile** blade, specify the following settings and click **OK**:

* First Name: **Kimberly**
* Last Name: **Pruitt**

1. Accept the default **Properties** and **Groups** settings and click **Directory role**.
2. On the **Directory role** blade, click **Global administrator** and click **OK**.
3. Click the **Show Password** checkbox and note the temporary password.
4. Click **Create**.
5. Start an InPrivate browser session and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com/).
6. When prompted to sign in, specify the full user name (including the @*domain-name*.onmicrosoft.com suffix) of the Kimberly Pruitt account and the corresponding temporary password.
7. On the **Update your password** page, in the **Current password** box, type again the temporary password. In the **New password** and **Confirm password** text boxes, type a **@Pa55w.rd**, and click **Update password and sign in**.

**Note:** If you receive the message **We've seen that password too many times before. Choose something harder to guess**, you'll need to modify the password until it is unique enough to be accepted.

1. If prompted to stay signed in, click **No**. Next, if prompted to start Microsoft Azure tour, click **Maybe later**. Next, click the user name in the upper-right corner and, in the drop-down menu, click **Sign out**
2. Close the InPrivate browser session.
3. Start an InPrivate browser window and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com/).
4. When prompted to sign in, specify the full user name (including the @*domain name*.onmicrosoft.com suffix) of Kimberly Pruitt’s account and the corresponding temporary password.
5. On the **Update your password** page, in the **Current password** box, type the temporary password. In the **New password** and **Confirm password** boxes, type **@Pa55w.rd**, and click **Update password and sign in**.

**Note:** If you receive the message **We've seen that password too many times before. Choose something harder to guess**, you'll need to modify the password until it is unique enough to be accepted.

1. If prompted to stay signed in, click **No**. Next, if prompted to start Microsoft Azure tour, click **Maybe later**. Next, click the user name in the upper-right corner and, in the drop-down menu, click **Sign out**

**Task 4: Manage groups by using the Azure portal**

1. Switch to the browser window displaying the Azure portal and ensure that you are viewing the **Users - All users** page of the **WintellectLocal** Azure Active Directory tenant blade.
2. Click your user account that is the Service Administrator of your subscription.
3. Click **Profile**.
4. In the details pane of the blade, click the **edit** hyperlink by **Settings**.
5. In the **Usage location** drop down list, select your country and click **Save**.
6. Click **Licenses**.
7. Click **+ Assign**.
8. On the **Assign license** blade, click **Products (>)**.
9. On the **Products** blade, select the checkbox next to the **Azure Active Directory Premium P2** entry and click **Select**.
10. Click **Assignment options (>)**.
11. On the **License options** blade, verify that **Azure Active Directory Premium P2**, **Azure Active Directory Premium Plan 1**, **Azure Multi-Factor Authentication**, and **Cloud App Security Discovery** are set to **On** and click **OK**.
12. Click **Assign**.
13. Verify that the assignment completed successfully.
14. Navigate back to the **WintellectLocal** blade and click **Groups**.
15. Click **General** (Note: if the options listed below are grayed out, refresh the Edge browser window).
16. On the **General** blade, specify the following settings and click **Save**:

* Owners can manage group membership requests in the Access Panel: **Yes**.
* Users can create security groups in Azure portals: **Yes**

1. Click **All groups**.
2. Click **+ New group**.
3. On the **Group** blade, specify the following settings:

* Group Type: **Security**
* Group name: **Executives**
* Group description: **WintellectLocalXX Executives**
* Membership type: **Assigned**

1. Click **Members**.
2. On the **Members** blade, select the checkbox next to the entry **Jeff Prosise** and click **Select**.
3. Click **Create** and close the **Group** blade.
4. Switch back to the **Groups - All groups** blade and click **+ New group**.
5. On the **Group** blade, specify the following settings:

* Group Type: **Security**
* Group name: **Training**
* Group description: **Training employees**
* Membership type: **Assigned**

1. Click **Members**.
2. On the **Members** blade, select the checkbox next to the entry **Kimberly Pruitt** and click **Select**.
3. Click **Create** and close the **Group** blade.
4. Switch back to the **Groups - All groups** blade and click **+ New group**.
5. On the **Group** blade, specify the following settings:

* Group type: **Security**
* Group name: **Executives and Training**
* Group description: **Executives and Training employees**
* Membership type: **Assigned**

1. Click **Members**.
2. On the **Members** blade, select the checkbox next to the **Executives** and **Training** entries and click **Select**.
3. Click **Create** and close the **Group** blade.

**Task 5: Manage users and groups by using Azure PowerShell**

**Note:** [**https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-msonlinev1?view=azureadps-1.0**](https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-msonlinev1?view=azureadps-1.0)

Install-Module MSOnline

1. On **WintellectSvr**, click **Start**, in the Start menu, expand the **Windows PowerShell** folder, right-click **Windows PowerShell ISE**, click **More**, and then click **Run as administrator**. If prompted by User Account Control for confirmation, click **Yes**.
2. In the PowerShell ISE, click **File**, and then click **Open**.
3. In the **Open** dialog box, browse to **C:\Labfiles\Lab06\**.
4. Click **addAADUserLab06.ps1**, and then click **Open**.
5. In the PowerShell ISE window, in the console pane, enter the following command and press Enter:

Connect-MsolService

1. In the **Enter Credentials** dialog box, enter the full name (including the @*domain name*.onmicrosoft.com suffix) of Kim Pruitt's user account and its password, and then click **OK**.
2. In the PowerShell ISE, in the script pane, locate the following code:

New-MsolUser -UserPrincipalName john@<#Copy your Azure Directory domain name here#>.onmicrosoft.com -DisplayName 'John Garland' -FirstName 'John' -LastName 'Garland' -Password '@Pa55w.rd' -ForceChangePassword $false -UsageLocation 'US'

1. Replace ***<#Copy your Azure Directory domain name here#>*** with the unique name you used to specify the DNS domain name of the WintellectLocal Azure AD tenant in the first exercise of this lab.
2. In the PowerShell ISE window, in the script pane, select the code that you just edited.
3. On the toolbar, click the **Run Selection** button and wait for the script to complete.
4. In the PowerShell ISE window, in the console pane, enter the following command, press Enter, and verify that the new user appears in the list of users:

Get-MsolUser

1. In the PowerShell ISE window, in the script pane, locate the following code and select it:

New-MsolGroup -DisplayName 'Azure team' -Description 'WintellectLocal Azure team users'

1. On the toolbar, click the **Run Selection** button and wait for the script to complete.
2. In the PowerShell ISE window, in the console pane, enter the following command, press Enter, and verify that the new group appears in the list of groups:

Get-MsolGroup

1. In the PowerShell ISE window, in the script pane, locate the following code and select it:

$group = Get-MsolGroup | Where-Object DisplayName -eq 'Azure team'

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. In the PowerShell ISE window, in the script pane, locate the following code and select it:

$user = Get-MsolUser | Where-Object DisplayName -eq 'John Garland'

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. In the PowerShell ISE window, in the script pane, locate the following code and select it:

Add-MsolGroupMember -GroupObjectId $group.ObjectId -GroupMemberType 'User' -GroupMemberObjectId $user.ObjectId

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. In the PowerShell ISE window, in the script pane, locate the following code and select it:

Get-MsolGroupMember -GroupObjectId $group.ObjectId

1. On the toolbar, click the **Run Selection** button, and wait for the script to complete.
2. Return to **Wintellect10**.
3. Switch to the **WintellectLocal** blade of the Azure portal in Microsoft Edge.
4. Click **Users**, **All users**, and verify that **John Garland** appears in the list of users.
5. Switch back to the **WintellectLocal** blade of the Azure portal in Microsoft Edge.
6. Click **Groups**, **All groups**, and verify that **Azure team** appears in the list of groups.

**Result**: After completing this exercise, you should have created Azure AD users and groups by using the Azure portal and Microsoft Azure Active Directory Module for Windows PowerShell. You also should have enabled the delegated group management Azure AD Premium functionality.

**Exercise 2: Configuring Application SSO**

**Task 1: Add directory applications and configure SSO**

1. Navigate to the **WintellectLocal** Azure Active Directory tenant blade in the Azure portal and click **Enterprise applications**.
2. Click **+ New application**.
3. On the **Add an application** blade, in the **Enter a name** text box above the **Add from the gallery** section, type **Microsoft Account (Windows Live)**
4. In the list of results, click **Microsoft Account (Windows Live)**
5. On the **Microsoft Account (Windows Live)** blade, click **Add**. Wait till the application gets added.
6. On the **Microsoft Account (Windows Live) - Getting started** blade, click **Configure single sign-on (required)**.
7. On the **Single sign-on** blade, in the **Single Sign-on Mode** drop-down list, select **Password-based Sign-on** and click **Save**.
8. Go back to the **Microsoft Account (Windows Live) - Getting started** blade, and then click **Assign a user for testing (required)**.
9. On the **Users and groups** blade, click **+ Add user**.
10. On the **Add assignment** blade, click **Users and groups**.
11. On the **Users and groups** blade, in the **Select** text box, type **John Garland**.
12. Select the entry representing the John Garland user account and click **Select**.
13. Click **Assign Credentials**.
14. On the **Assign Credentials** blade, next to the **Assign credentials on behalf of the user?** label, click **Yes**.
15. On the **Assign Credentials** blade, in the **Email Address** text box, type the email address of your Microsoft Account that is the Service Administrator of the Azure subscription you are using for this lab, in the **Password** text box, type the password of that account, and click **OK**.
16. Click **Assign**.
17. Navigate back to the **Add an application** blade, click + Add Application, and in the search box, type **Skype**.
18. In the list of search results, click **Skype** and, then on the **Skype** blade, click **Add**. Wait till the application gets added.
19. On the **Skype - Getting started** blade, click **Configure single sign-on (required)**.
20. On the **Single sign-on** blade, in the **Single Sign-on Mode** drop-down list, select **Password-based Sign-on** and click **Save**.
21. Go back by clicking the **Skype - Getting started** node, and then click **Assign a user for testing (required)**.
22. On the **Users and groups** blade, click **+ Add user**.
23. On the **Add assignment** blade, click **Users and groups**.
24. On the **Users and groups** blade, in the **Select** text box, type **john Garland**.
25. Select the entry representing the John Garland user account and click **Select**.
26. Click **Assign**.
27. On the top right side of the page, click your Azure account name, and then click **Sign out**.

**Task 2: Configure SSO on a client computer**

1. From the browser, browse to [**https://myapps.microsoft.com**](https://myapps.microsoft.com/).
2. On the **Microsoft Azure** page, click **Use another account**.
3. When prompted to sign in, specify the full user name (including the @*domain name*.onmicrosoft.com suffix) of the John Garland’s account you created in the previous exercise and @**Pa55w.rd** as the corresponding password.
4. On the Apps page, click the ellipsis next to the **Skype** icon (mouse-over will cause ellipses to appear). Note the option to update the credentials.
5. On the Apps page, click the ellipsis next to the **Microsoft Account (Windows Live)** icon. Note that there is no option to update the credentials.
6. Switch to the PowerShell ISE window, the console pane, enter the following command, and press Enter:

Set-Service -Name 'wuauserv' -StartupType Manual

1. Switch to the browser window and, on the Apps page, click **Skype**.
2. In the **Skype** dialog box, click **Install Now**.
3. In the **Sign me up** pop-up window, click the **X** to close.
4. In the **Store** window, under the **My Apps Secure Sign-in Extension** header, click **Get**. You may have to do this twice. Click **No, thanks** to the **Use across your devices** pop-up window.
5. Wait for the extension to be downloaded and then switch back to the browser window. Refresh the page.
6. When prompted, in the **You have a new extension** dialog box in the browser window, click **Turn it on**.
7. In the upper right corner of the browser window, click the ellipsis and, in the drop-down menu, click **Extensions**.
8. Verify that My Apps Secure Sign-in Extension is turned on. If not, click **My Apps Secure Sign-in Extension** and move the slider to the **On** position.
9. Restart the browser and browse back to [**https://myapps.microsoft.com**](https://myapps.microsoft.com/). If prompted to sign in, specify the full user name (including the @*domain name*.onmicrosoft.com suffix) of the John Garland's account you created in the previous exercise and **@Pa55w.rd** as the corresponding password.
10. On the Apps page, click **Skype**. Note that you are prompted for credentials, because you did not enter any credentials on behalf of the user when configuring the application single sign-on settings.
11. Click **Cancel** in the **Skype** dialog box.
12. Click the user name in the upper right corner of the browser page and click **Sign out**.
13. Close Microsoft Edge.
14. Switch to the PowerShell ISE window,the console pane, enter the following command, and press Enter:

Set-Service -Name 'wuauserv' -StartupType Disabled

**Result**: After completing this exercise, you should have configured test applications and validated the SSO experience.

**Exercise 3: Configuring Multi-Factor Authentication**

**Task 1: Configure Multi-Factor Authentication**

1. Start the browser and browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com/), and then sign in using the Microsoft account that is the Service Administrator of your subscription.
2. In the hub menu, click **Azure Active Directory**.
3. On the **WintellectLocal** blade, click **Users**.
4. Click **All users**.
5. In the toolbar of the **Users and groups - All users** blade, click **Multi-Factor Authentication**. This will open another Microsoft Edge tab. If prompted, sign in using the Microsoft account that is the Service Administrator of your subscription.
6. On the **multi-factor authentication** page, ensure that the **users** tab is displayed. In the **users** list, select the check box next to **Kimberly Pruitt** and, in the **quick steps** section, click **Enable**.
7. On the **About enabling multi-factor auth** page, click **enable multi-factor auth**.
8. On the **Updates successful** page, click **close**.
9. Click the user name entry in the upper right corner of the browser window and, in the drop down menu, click **Sign out**.
10. Close the browser window, including both tabs.

**Task 2: Test Multi-Factor Authentication**

1. Start the browser and browse to [**https://myapps.microsoft.com**](https://myapps.microsoft.com/).
2. On the **Microsoft Azure** page, click **Use another account**.
3. When prompted to sign in, specify the full user name (including the @*domain name*.onmicrosoft.com suffix) of the Kim Pruitt's account and the corresponding password. You will be presented with the message stating ***Your admin has required that you set up this account for additional security verification***.
4. Click **Set it up now**.
5. On the **Additional security verification** page, in the first drop-down list, select **Authentication phone**.
6. In the **Select your country or region** drop down list, click the entry representing your country or region.
7. In the adjacent text box, type your mobile phone number, under **Method** select **Send me a code by text message**, and click **Next**.
8. Retrieve the message on your mobile phone, type it in the text box on the page, and click **Verify**.
9. On the page **Step 3: Keep using your existing applications**, note the **Get started with this app password** entry, and click **Done**.
10. Click the user name in the upper right corner of the **Apps** page and, in the drop-down menu, click **Sign out**.
11. Close the browser.

**Result**: After completing this exercise, you should have configured Multi-Factor Authentication for a Global Admin account.

**Exercise 4: Configuring SSO from a Windows 10-based computer that is joined to Azure AD**

**Task 1: Join a Windows 10-based computer to Azure AD**

1. Start the browser, and then browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com/), and then sign in using the Microsoft account that is the Service Administrator of your subscription.
2. In the hub menu, click **Azure Active Directory**.
3. On the **WintellectLocal** blade, click **Devices**.
4. On the **Devices - All devices** blade, click **Device settings**.
5. Verify that the **Users may join devices to Azure AD** setting is set to **All**.
6. On Wintellect10, click Start and then click **Settings**.
7. In the Settings app, click **Accounts**, and then click **Access work or school**.
8. On the **Access work or school** page, click **Connect**. This will open the **Set up a work or school account** window.
9. Click **Join this device to Azure Active Directory**.
10. On the **Let's get you signed in** page, in the **Work or school account** text box, type the full user name (including the @*domain name*.onmicrosoft.com suffix) of the Kim Pruitt's account and click **Next**.
11. On the **Enter password** page, type the password you assigned to the Kim Pruitt's account in exercise 1 of this lab and click **Sign in**.
12. Since you set up Kim Pruitt's account with MFA in the previous exercise, you should receive at this point a text message containing a verification code. Retrieve the verification code from your mobile phone, type it in the text box on the **Help us protect your account** page, and click **Next**.
13. On the **Make sure this is your organization** page, click **Join**.
14. On the **You're all set** page, click **Done**.
15. Switch back to Microsoft Edge.
16. Navigate back to the **WintellectLocal** page, click **Users and Groups**, click **All Users**, and then click **Kim Pruitt**
17. On the **Kim Pruitt** blade, click **Devices**.
18. Verify that **Wintellect10** appears in the list of devices.
19. Restart **Wintellect10**.

**Task 2: Authenticate to Azure from a Windows 10 Azure-joined computer**

1. Sign in to Wintellect10 by using the full user name (including the @*domain name*.onmicrosoft.com suffix) of the Kim Pruitt's WintellectLocal Azure AD account and its password.
2. Start Microsoft Edge, and then go to [**https://portal.azure.com**](https://portal.azure.com/).
3. Verify that you are automatically signed in as Kim Pruitt by using single sign-on.
4. Sign out from the Azure portal
5. In Wintellect10, click Start and then Settings. Then click Yes.
6. In the Settings app, click **Accounts**, and then click the [kim@wintellectLocalXX.onmicrosoft.com](mailto:kim@wintellectLocalXX.onmicrosoft.com) account, and then click **Manage**.

Sign in as [kim@wintellectLocalXX.onmicrosoft.com](mailto:kim@wintellectLocalXX.onmicrosoft.com).

**Task 3: Remove the lab environment**

1. In the Access Panel Profile, by the Device name you just added in Task 1, click **Disable device**. Now click **Yes** in the Disable device pop-up window.
2. On the Profile page, click the **Sign out everywhere** hyperlink, and click **Yes** on the **Sign out everywhere** pop-up window. Close the browser.
3. Restart Wintellect10.
4. Sign into Wintellect10 as the original user, **Wintellect Student**, with a password of **@Pa55w.rd**.
5. In Wintellect10, click **Start** and then **Settings**.
6. In the Settings app, click **Accounts**, and then in **Account** settings, click **Other people**.
7. Click the **AzureAD\KimberlyPruitt** account and then click **Remove**.
8. In the **Remove account** pop-up window, click **Remove**.
9. On the Wintellect10, start Microsoft Edge.
10. In the browser, browse to the Azure portal at <http://portal.azure.com>
11. If prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
12. In the hub menu, click **Azure Active directory**.
13. On the **WintellectLocal** blade, in the **Overview** details pane, click **Delete directory**.
14. In the **Delete directory** blade, note the requirements to delete have not been met. Click the Properties link.
15. In the properties link, note the line stating **Global admin can manage Azure Subscriptions and Management groups**. Click the **Yes** button, and then click **Save** (above). Close properties.
16. Repeat steps 12 and 13.
17. In the **Delete directory** blade, note the requirements to delete have changed to a list of actions. Click each the Delete hyperlink, starting with the bottom link, Subscriptions, and finishing with Users.
18. Close all open windows.

**Result**: After completing this exercise, you should have joined the Wintellect10 computer to Azure AD and tested the SSO access to the resources in the cloud.