Student Lab Manual
MS101.3x: Microsoft 365 Device Management

Lab Scenario

You are the system administrator for Adatum Corporation, and you have Microsoft 365 deployed in a virtualized lab environment. In this lab, you will work with Microsoft Store for Business, and you will manage devices using Intune.

There are two labs in this course, each of which contains one or more exercises, and within each exercise is one or more tasks. For a successful outcome to the lab, the exercises and their corresponding tasks must be completed in order. These include:

Lab A: Working with the Microsoft Store for Business

- Exercise 1: Provisioning and managing the Microsoft Store for Business
  - Task 1: Obtain your Office 365 credentials
  - Task 2: Sign up for Microsoft Store for Business and perform initial configuration
  - Task 3: Work with roles in Microsoft Store for Business

- Exercise 2: Using the Microsoft Store for Business
  - Task 1: Add apps to private store
  - Task 2: View Microsoft Store for Business as a company employee

Lab B: Managing Devices by using Intune

- Exercise 1: Obtain Intune and enable device management
  - Task 1: Activate Enterprise Mobility + Security trial
  - Task 2: Assign Intune license
  - Task 3: Enable device management

- Exercise 2: Configure Azure AD for Intune
  - Task 1: Integrate Azure AD with Intune
  - Task 2: Configure Azure AD join
  - Task 3: Create dynamic Azure AD device group

- Exercise 3: Create Intune policies
  - Task 1: Create and apply compliance policy
  - Task 2: Configure enrollment restrictions
  - Task 3: Review device configuration profiles

- Exercise 4: Enroll Windows 10 device

    - Task 1: Verify that device is not enrolled
    - Task 2: Enroll device to Azure AD and Intune
    - Task 3: Verify that device is enrolled to Azure AD and Intune

- Exercise 5: Manage and monitor a device in Intune
    - Task 1: Create device categories
    - Task 2: Manage device and assign it to a category
    - Task 3: Create dynamic group for device category
    - Task 4: Create conditional access policy

WARNING – Be prepared for UI changes

Given the dynamic nature of Microsoft cloud tools, you may experience user interface (UI) changes that were made following the development of this training content that do not match up with lab instructions presented in this lab.

The Microsoft Learning team will update this training course as soon as any such changes are brought to our attention. However, given the dynamic nature of cloud updates, you may run into UI changes before this training content is updated. **If this occurs, you will have to adapt to the changes and work through them in the labs as needed.**

Lab A: Working with the Microsoft Store for Business

Exercise 1: Provisioning and Managing Microsoft Store for Business

▶ Task 1: Obtain your Office 365 credentials

Once you launch the lab, a free trial tenant will be automatically created for you to access Azure in the Microsoft Virtual Lab environment. This tenant will be automatically assigned a unique user name and password. You must retrieve this user name and password so that you can sign into Azure within the Microsoft Virtual Lab environment.

1. On the **XtremeLabs Online** menu bar at the top of the screen, click on the **Files** drop-down arrow.
2. Click on **O365 Credentials**. A window will open with your credentials.
3. This is the user name and password you will need to sign in to Azure. Keep this page open as you will need the information later.
4. When the lab directs you to sign in to the Azure portal at **https://portal.azure.com,** you will sign in using the credentials you obtained in this task.

▶ Task 2: Sign up for Microsoft Store for Business and perform initial configuration

1. On **LON-CL1**, on the taskbar, click **Microsoft Edge**.
2. In Microsoft Edge, type **https://www.microsoft.com/business-store** in the address bar, and then press Enter.
3. In the top-right corner of Microsoft Edge, click the **Sign in** link.

   Note: The page localizes based on your location.
4. In the **Sign in to Microsoft Store** dialog box, in the **someone@example.com** text box, type **Admin@*XXYYZZ*.onmicrosoft.com** (replace ***XXYYZZ*** with the corresponding attribute from your O365 Credentials), use the Admin password and then select **Sign in**. On **Stay signed in?** dialog, click **No**.
5. On the **Microsoft Store for Business** page, click **Manage**.
6. In the **Microsoft Store for Business and your data** dialog box, select the check box and click **Accept**.
7. On the **Microsoft Store for Business** page, click **Shop for my group**.

8. Scroll down to the **Made by Microsoft** section, click **Show all**, click **Microsoft Remote Desktop** and click **Get the app**.
9. At the bottom of the **Microsoft Store for Business and Education Services Agreement** page, select both check boxes, click **Accept** and then click **Close**.
10. On the **Microsoft Store for Business** page, on the taskbar, click **Manage**.
11. In the navigation pane, click **Products & services**. In the details pane, verify that the Sway, OneNote, PowerPoint Mobile, Excel Mobile, Microsoft Remote Desktop and Word Mobile apps are listed.

    Note: When you sign up for the Microsoft Store for Business and accept the agreement, the portal automatically adds those apps to your private store.
12. In the navigation pane, click **Settings**. In the details pane, on the **Shop** tab, in the **Shopping experience** section, turn the **Show offline apps** switch to **On**.
13. Verify that under Microsoft Store for Business, the second option from the left on the toolbar is **Private Store**.
14. In the details pane, click the **Distribute** tab. In the **Private store** section, click **Change**, in the **Display name** text box, type **Adatum Store**, and then click **Save**.
15. Verify that the second option from the left on the toolbar below Microsoft Store for Business is now the **Adatum Store**. This is your private store.
16. In the **Settings** details pane, click the **Devices** tab, and then review where you can configure **Device Guard signer** policies by downloading the default policy and upload your custom device guard signer policies. Don't confuse this option with the Devices option in the navigation pane!

    Note: When configured, these policies allow apps from the Microsoft Store for Business to run on a device that Windows Defender Device Guard is protecting.

▶ Task 3: Work with roles in Microsoft Store for Business

1. On **LON-CL1**, open a new tab in Microsoft Edge, and browse to **https://portal.office.com**/.
2. Sign in as **Admin@*XXYYZZ*.onmicrosoft.com,** (replace ***XXYYZZ*** with the corresponding attribute from your O365 Credentials), use the tenant Admin password.
3. In the Office 365 admin center, click **Admin**.
4. In the Office 365 admin center, on the left rail, click **Users**, then click **Active Users**.
5. Click the Add a user to open the New user panel and enter in the following:
   - First name: **Ada**
   - Last name: **Russell**
   - Username: **ada** (leave the domain the default .onmicrosoft.com domain)
   - Location: **United Kingdom**
6. Click **Password** and select **Let me create the password**. Enter the password **Pa$$w0rd**. Uncheck the **Make this user change their password when the first**

sign in.

7. Click **Product Licenses** and verify **Office 365 Enterprise E5** is set to On.
8. Click **Add**, and then click **Send email and Close**.
9. Using the previous steps, create another new user:
   - First name: **Holly**
   - Last name: **Dickson**
   - Username: **hdickson** (leave the domain the default.onmicrosoft.com domain)
   - Location: **United Kingdom**
10. Set the password to **Pa$$w0rd** and enable **Office 365 Enterprise E5**.
11. On **LON-CL1**, in Microsoft Edge, on the **Microsoft Store for Business** page, in the navigation pane, click **Permissions**.
12. In the details pane, on the **Roles** tab, click **Assign roles**.
13. In the **Assign roles to people** dialog box, in the text box, type **Ada**, then click **Ada Russell**, select the **Admin** check box, and then click **Save**.
14. Click **Assign roles**, in the text box, type **Holly**, click **Holly Dickson**, select the **Purchaser** check box, and then click **Save**.
15. In the details pane, verify that the Admin user has the Global Admin role, Ada Russell has the Admin role, and Holly Dickson has the Purchaser role.

Exercise 2: Using the Microsoft Store for Business

▶ Task 1: Add apps to private store

1. On **LON-CL1**, in Microsoft Edge, on the **Microsoft Store for Business** page, on the taskbar, click **Shop for my group**.
2. Scroll down to the **Made by Microsoft** section, click **Translator**, click **Get the app**, and then click **Close**. Notice the ellipsis (…) near the Install button.
3. Click the ellipsis (**…**), and then notice that only the **Manage** option is available. Additionally, notice that **License type** is set to **Online,** but the **Offline licensing** type also is available.
4. Click **Shop for my group**, scroll down to the **Made by Microsoft** section, click **Show all**, click **Fresh Paint**, click **Get the app**, and then click **Close**.
5. Click **Shop for my group**, scroll down to the **Made by Microsoft** section, click **Show all**, and then click **Reader**.
6. On the **Reader** page, in the **License type: Online** drop-down list, select **Offline**. Click **Get the app**, click **Close**, click **Manage**, scroll down the page, and then verify that you can view **Download** button to download the Reader package for offline use.
7. In the **Microsoft Store for Business**, on the taskbar, click **Adatum Store.**
8. Click **+Add collection**, in the **Enter a collection name** text box type **Collection1**.
9. Click **Add** below Fresh Paint, Microsoft Remote Desktop, and Translator, and then

at the bottom of the page click **Done**.

10. Close Microsoft Edge.

▶ Task 2: View Microsoft Store for Business as a company employee

1. On **LON-CL1**, on the taskbar, right-click **Microsoft Edge** and select **New InPrivate window**.
2. In Microsoft Edge, type **https://www.microsoft.com/business-store** in the address bar, and then press Enter.
3. In the top-right corner of Microsoft Edge, click the **Sign in** link.
4. Sign in to **Microsoft Store** as **Holly@*XXYYZZ*.onmicrosoft.com,** (replace ***XXYYZZ*** with the corresponding attribute from your O365 Credentials), with the **Pa$$w0rd** password.
5. In Microsoft Edge, click on **Adatum Store** and verify that you can see the following:
    - The five apps that were automatically added to the private store (Sway, OneNote, PowerPoint Mobile, Excel Mobile, and Word Mobile)
    - The Collection1 app that you created, which includes Fresh Paint, Microsoft Remote Desktop, and Translator

    Note: Company employees can also use the Microsoft Store app for accessing Microsoft Store for Business. However, because it can take up to 36 hours for newly added apps to propagate to the private store and be visible in the Microsoft Store app, this lab used a web browser to access the Microsoft Store for Business.
6. Close Microsoft Edge.

Lab B: Managing Devices by using Intune

Exercise 1: Obtain Intune and enable device management

▶ Task 1: Activate Enterprise Mobility + Security trial

1. On **LON-CL1**, on the taskbar, click **Microsoft Edge**.
2. In Microsoft Edge, type **https://portal.azure.com** in the address bar, and then press Enter.
3. Sign in as user **Admin@XXYYZZ.onmicrosoft.com**, (replace XXYYZZ with the corresponding attribute from your O365 Credentials), use the tenant Admin password.
4. In the Azure portal, in the navigation pane, click **Azure Active Directory**.
5. On the **Azure Active Directory** blade, click **Company branding** and then click **Get a free Premium trial to use this feature**.
6. On the **Activate** blade, in the **ENTERPRISE MOBILITY + SECURITY E5** section, click **Free trial** and then click **Activate**.

▶ Task 2: Assign Intune license

1. In **LON-CL1**, in the Edge browser, in the Azure portal, and in the navigation pane, click **Azure Active Directory**.
2. On the **Azure Active Directory** blade, click **Users**, click **Ada**, click **Edit.** In the **Settings** section, click **Edit**, and in the **Usage location** dropdown list select **United States** and click **Save**.
3. Scroll the page to the left on the page, click **Admin**, click **Edit**, and then in the **Settings** section, in the **Usage location** dropdown list select **United States** and click **Save**.
4. Scroll the page to the left on the page. On the **Azure Active Directory** blade click **Licenses** and then in the details pane click **2 products**.
5. On the **Products** blade, click **Enterprise Mobility + Security E5** and then in details pane click **+ Assign**.
6. On the **Assign license** blade, click **Users**. In the **Users** pane click **Ada** and **Admin**, click **Select,** and then click **Assign.**

▶ Task 3: Enable device management

1. In **LON-CL1**, in the Edge browser, in the Azure portal, click **All services**, type **intune** in the search box and then click **Intune**.
2. On the **Microsoft Intune** blade, click **Quick start**. In the **Account details** section,

verify that **MDM authority** is **unknown**.

3. Scroll to the right. On the **Choose MDM Authority** blade, select the **Intune MDM Authority** radio button and then click **Choose**.
4. In upper right part of the details pane, verify that **MDM authority** is now set to **Intune**.
5. Scroll the page left. On the **Microsoft Intune** blade, select different options and review their settings. You can return to the Microsoft Intune blade by clicking **Microsoft Intune** in the navigation row on top of blade name, after **Home > string**.

Exercise 2: Configure Azure AD for Intune

▶ Task 1: Integrate Azure AD with Intune

1. In **LON-CL1**, in the Azure portal, in the navigation pane, click **Azure Active Directory**.
2. On the Azure Active Directory blade, click **Mobility (MDM and MAM)** and then in the details pane, click **Microsoft Intune**.

   Note: If you see a notification that automatic enrollment is available only for Azure AD Premium, press F5 to refresh the page in your web browser and then click **Microsoft Intune** again.
3. On the **Configure** blade, in the **MDM user scope** row, click **All** and then click **Save**.

   Note: By performing this step you allowed all users who join their device to Azure AD to automatically enroll it to Intune as well.

▶ Task 2: Configure Azure AD join

1. In **LON-CL1**, in the Azure portal, scroll the page to the left on the page and then in the **Azure Active Directory** blade click **Devices**.
2. In the details pane, verify that no device is listed. This is because no device has been joined to Azure Active Directory yet.
3. On the **Devices** pane, click **Device settings**.
4. In the details pane, in the **Users may join devices to Azure AD** row, verify that **All** is selected. This means that all Azure AD users can join their devices to Azure Active Directory.
5. In the **Additional local administrator on Azure AD joined devices** row click **Selected**, click **Selected** in No member selected area, click **+Add members**, select **Ada**, click **Select** and then click **OK**.
6. Verify that **Require Multi-Factor Auth to join devices** is set to **No** and that the **Maximum number of devices per user** is set to **50**, and then click **Save**

Task 3: Create dynamic Azure AD device group

1. In **LON-CL1**, in the Azure portal, scroll the page to the left and then in the **Azure Active Directory** blade click **Groups**.
2. On the **Group** blade, on the details pane, click **+New group**.
3. On the **Group** blade, provide the following values:
    - Group type: **Security**
    - Group name: **Enrolled Devices**
    - Membership type: **Dynamic Device**
4. On the **Group** blade, click **Dynamic device members.**
5. On the **Dynamic membership rules** blade, provide the following Simple membership rule to add devices where (select first two options from drop down lists and type MDM in third text box):

    managementType Equals MDM
6. On the **Dynamic membership rules** blade, click **Add query** and then click **Create**.

Exercise 3: Create Intune policies

▶ Task 1: Create and apply compliance policy

1. In **LON-CL1**, in the Azure portal, click **All services**, type **intune,** and then click **Intune**.
2. On the **Microsoft Intune** blade, click **Device compliance**.
3. On the **Device compliance** blade, click **Policies** and then in the details pane click **+Create Policy**.
4. On the **Create Policy** blade, provide the following values:
    - Name: **Compliance1**
    - Platform: **Windows 10 and later**
5. On the **Windows 10 compliance policy** blade, click **Device Health** and review the available settings.
6. On the **Windows 10 compliance policy** blade, click **Device Properties**.
7. On the **Device Properties** blade, in the **Minimum OS version** row, type **10.0.16299.15** and then click **OK**.
8. On the **Windows 10 compliance policy** blade review the other available options and then click **OK**.
9. On the **Create Policy** blade, click **Actions for noncompliance** and then on the details pane, click **+Add**.
10. On the **Action parameters** blade review the available options and then close the

blade.

11. In the Actions blade click **Mark device noncompliant**. Review how you can configure the number of days after which the device is marked as noncompliant, then click **OK** twice and then click **Create**.
12. On the **Compliance1** blade, click **Assignments**, click **Select groups to include**, click **Enrolled Devices**, click **Select,** and then click **Save**.

▶ Task 2: Configure enrollment restrictions

1. In **LON-CL1**, in the Azure portal, scroll the page to the left and then on the **Microsoft Intune** blade, click **Device enrollment**.
2. Review the available options on the **Device enrollment** blade.
3. On the **Device enrollment** blade, click **Enrollment restrictions**.
4. On the details pane, in the **Device Type Restrictions** section, click **Default,** click **Properties,** and then click **Select platforms**.
5. On the **Select platforms** blade, in the **iOS** and **macOS** rows click **Block**, click **OK,** and then click **Save**.
6. On the left pane, in the **Device Limit Restrictions** section, click **Default** and then click **Properties**.
7. In the **Device Limit** dropdown list, select **3** and then click **Save**.

Task 3: Review device configuration profiles

1. In **LON-CL1**, in the Azure portal, scroll the page to the left and then on the **Microsoft Intune** blade click **Device configuration**.
2. On the **Device configuration** blade, click **Profiles** and then click **+Create profile**.
3. On the **Create profile** blade, select different platforms and profile types and then review available options.
4. Do not configure any option. Close the **Create profile** blade and click **OK**.

Exercise 4: Enroll Windows 10 device

▶ Task 1: Verify that device is not enrolled

1. In **LON-CL1**, in the Azure portal, scroll the page to the left and then on the **Microsoft Intune** blade, click **Devices**.
2. On the **Devices** pane, verify that no device is currently enrolled to Intune.
3. Click **All Devices** and verify that no device is listed in the details pane.
4. Switch to **LON-CL2**. On the **LON-CL2** taskbar, click **Start**, type **certlm.msc**, press Enter and then click **Yes**.

5. In the **Certificates** console, in the navigation pane, click **Personal** and verify that no certificate is listed in the details pane.

▶ Task 2: Enroll device to Azure AD and Intune

1. In **LON-CL2**, on the taskbar, click **Start**, type **connect to work** and then click **Connect to work or school**.
2. In the **Settings** app, in the **Access work or school** section, click **+Connect**.
3. In the **Microsoft account** window, on the **Set up a work or school account** page, click **Join this device to Azure Active Directory**.
4. On the **Let's get you signed in** page, in the **Work or school account** text box, type **Admin@*YourInitialsMMDDYY*.onmicrosoft.com** and then click **Next**.
5. On Enter password page, type **Pa55w.rd** in the text box and then click **Sign in**.
6. Wait a few seconds and then on the **Make sure this is your organization** dialog, click **Join**.
7. On the **You're all set!** page, click **Done**.
8. In the **Settings** app, in the **Access work or school** section, verify that the device is connected to Azure AD and then close the **Settings** app.

▶ Task 3: Verify that device is enrolled to Azure AD and Intune

1. In **LON-CL2**, in the **Certificates** console, in the navigation pane, right click **Personal** and click **Refresh**.
2. In the navigation pane, under the **Personal** node, click **Certificates**. In the details pane, verify that several certificates are listed.

   Note: Those certificates were added when you joined the device to Azure AD and enrolled it to Intune.
3. Close the **Certificates** console.
4. In **LON-CL1**, in the Azure portal, scroll the page to the left and then on the **Microsoft Intune** blade, click **Devices**.
5. Maximize your Edge browser and verify that the **All devices** option is selected. No devices are listed because this view was generated before your device was enrolled.
6. In the details pane click **Refresh** and verify that one device is now listed. This is the device that you joined to Azure AD!

   Note: This view lists devices that are enrolled to Intune. Review the values in the device properties.
7. On the **Devices** blade, click **Azure AD devices** and verify that in the details pane the same device is listed.

   Note: This view lists devices that are joined to Azure AD. Remember that you configured integration between Azure AD and Intune, and because of that, any

device that is joined to Azure AD is automatically enrolled to Intune.

Exercise 5: Manage and monitor device in Intune

▶ Task 1: Create device categories

1. In **LON-CL1**, in the Azure portal, scroll the page to the left and then on the **Microsoft Intune** blade, click **Device enrollment**.
2. On the **Device enrollment** pane, click **Device categories** and then click **+Create device category**.
3. On the **Create device category** blade, in the **Category** text box, type **Mobile Device** and click **Create**.
4. Click **+Create device category**, in the **Category** text box, type **Desktops** and then click **Create**.

▶ Task 2: Manage device and assign it to a category

1. In the Azure portal, on the **Microsoft Intune** blade, click **Devices** and then click **All devices**.
2. In the details pane, click device that you joined to Azure AD (and which was automatically enrolled to Intune).
3. On the **device** pane, review the device details. Also review the actions that you can start against the device (available on the taskbar). Click **...More** and review the additional tasks.
4. On the device pane, click **Properties**. In the **Device category** list box select **Mobile device** and then click **Save**.

Note: For Android or iOS devices, you must select **device category** during enrollment.

5. On the **device** pane, click **Hardware** and review the hardware information that synced from the device. Also review the **Conditional access** section at the end of the page!
6. On the **device** pane, click **Discovered apps** and review the list of apps that were discovered on the device.

▶ Task 3: Create dynamic group for device category

1. In the Azure portal, scroll the page to the left and then on the **Microsoft Intune** blade, click **Groups**.
2. In the **details** pane, click **+New group**.
3. On the **Group** blade, provide following values:

- Group type: **Security**
- Group name: **Mobile Devices**
- Membership type: **Dynamic Device**

4. On the **Group** blade, click **Dynamic device members.**
5. On the **Dynamic membership rules** blade, provide the following membership Simple rule:

   deviceCategory Equals Mobile Device
6. On the **Dynamic membership** rules blade, click **Add query** and then click **Create**.

▶ Task 4: Create conditional access policy

1. In the Azure portal, on the **Microsoft Intune** blade, click **Conditional access**.
2. In the **details** pane, click **+New policy**.
3. On the **New** blade, in the **Name** text box, type **Conditional1** and then click **Users and groups**.
4. On the **Users and groups** blade, select the **All users** radio button and then click **Done**.
5. On the **New** blade, click **Cloud apps**, select the **Select apps** radio button, click **Select**, click **Office 365 Exchange Online**, click **Select,** and then click **Done**.
6. On the **New** blade, click **Conditions**, click **Device platforms**, in the **Configure** section click **Yes**, select the **Select device platforms** radio button, select the **Windows** check box, and then click **Done** twice.
7. On the **New** blade, click **Grant**, select the **Require device to be marked as compliant** check box, and then click **Select**.
8. On the **New** blade, click **Session**, review the explanation and then on the **New** blade click **Create**.

Note: You created a conditional access policy to get familiar with the available options; however, the policy is not effective because you didn't enable it.

End of lab