

# Student Lab Manual

## MS101.1x: Microsoft 365 Security 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 edit an ATP Safe Links policy, create a Safe Attachment policy, and enable and install the ATA Center.

There are three lab exercises in this course. For a successful outcome to each lab, the exercises and their corresponding tasks must be completed in order. The three exercises include:

- Exercise 1: Setting up your lab environment
  - Task 1 – Obtain your Office 365 credentials
  - Task 2 - Create a Microsoft 365 tenant account
  - Task 3 – Create a user account
  
- Exercise 2: Editing an ATP Safe Links policy and create a Safe Attachment policy
  - Task 1 – Edit an ATP Safe Links policy
  - Task 2 - Create a Safe Attachment policy and turn on ATP for SharePoint, OneDrive, and Microsoft Teams
  
- Exercise 3: Enabling and installing the ATA Center
  - Task 1 – Enable trial subscriptions for the ATA Center
  - Task 2 – Install an ATA Center on your Domain Controller

### Lab Design

#### Getting a lab for the lab exercises

The lab exercises in this course require you to log on to the Microsoft Labs Online environment to do the lab steps in a virtual environment.

## 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 manual.

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.**

## Exercise 1: Setting up your lab environment

This lab deploys several desktops; therefore, you must create a tenant account in Microsoft 365 to set up your Microsoft 365 clients.

### 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 - Create the tenant account

1. At the top of the screen, click the **Virtual machine** drop-down field and select **LON-DC1**.
2. On the VM titled **LON-DC1**, you are already logged on as the **adatum\administrator** account.
3. Open **Internet Explorer**. Navigate to **Tools > Internet Options > Security** tab.
4. In the **Internet** zone, click **Custom Level**. Scroll down and under the **Downloads** section, you must enable the **File download** setting.
5. Then in the **Trusted Sites** zone, you need to add the following sites:
  - <https://outlook.office365.com/>
  - <https://outlook.office.com/>
  - <https://portal.office.com/>
6. In Internet Explorer, sign in to Office 365 by navigating to **https://portal.office.com** and logging in with the O365 Credentials (username and password) that you retrieved in the prior task.
7. On the **Stay signed in?** page, click **Yes** to stay signed in.
8. Select **Admin**.
9. Under **Active users**, you should add a user account for **Jenna Glover** with the following attributes:
  - **Username:** jenna
  - **Domain:** leave as is
  - **Location:** United States
  - **Password:** Pa\$\$w0rd (uncheck the **Make user change their password when they first sign in** option)
  - **Role:** Global Administrator
  - **Product licenses:** Office 365 Enterprise E5
10. After adding the user, in the **User was added** window, review the information for correctness. Unselect the **Send password in email** check box.

11. Close the window and sign out.

## Task 3 – Create a user account

1. On the Admin center, navigate to **Active users** and then add the following user account:
  - First name: **Holly**
  - Last name: **Dickson**
  - Username: **holly2**
  - Domain: Leave the **.onmicrosoft.com** domain as the default domain
  - Role: **Global Administrator**
  - Product licenses: **Office 365 Enterprise E5** enabled
  - Password: select **Let me create the password**. Use this password: **Pa\$\$w0rd**. Uncheck the box that says **Make user change password when they first sign in**.
2. Review information and password for correctness and **uncheck Send Password in email**.

## Exercise 2: Editing an ATP Safe Links policy and creating a Safe Attachment policy

You now have a Global Admin account set up and are ready to edit a Safe Links policy.

### Task 1 – Edit an ATP Safe Links Policy

1. At the top of the screen, click the **Virtual machine** drop-down field and select **LON-WIN10**.
2. On **LON-WIN10**, open **Internet Explorer** and navigate to **https://protection.office.com**.
3. Sign in with the O365 Admin (.onmicrosoft.com domain) global admin account.
4. In the **Threat Management** menu, select **Policy**.
5. Select the **ATP Safe Links** tile.
6. Once you have been redirected to the safe links interface select the pencil next to the **refresh** button on the left-hand side.
7. Create a Safe Links policy for the following URL: **CLD274test.com**.

### Task 2 – Create a Safe Attachment policy and turn on ATP for SharePoint, OneDrive, and Microsoft Teams

1. In the **Threat Management** menu, select **Policy**.
2. Select the **ATP Safe Attachments** tile.
3. On the user interface page, select the **Turn on ATP for SharePoint, OneDrive and Microsoft Teams** checkbox.
4. Click on the plus symbol located at the bottom of the UI. A new UI will pop up.
5. In the **Name** field type **NewAttachmentPolicy1**.
6. Then select **dynamic delivery** (this option will still send the email but will hold the attachment till it has been scanned and marked acceptable.)
7. Under the **Applied To** option, under **If**, click the drop-down and select **The recipient domain is...**
8. A UI will pop up; select your **onmicrosoft** domain and then save the policy.
9. Two pop up warning boxes will appear. Accept them both.
10. On the third pop up wait for the loading process to complete and then click **OK**.
11. Close the **new safe attachment policy** window.
12. Go to the top right corner of the internet browser and select your username and sign out.

## Exercise 3: Enabling and installing the ATA Center

**Note:** In this exercise we will not be pulling live client or server machines. We will be running though the setup for familiarization.

### Task 1 – Enable trial subscriptions for the ATA Center

1. Switch to **LON-DC1**.
2. Run **Internet Explorer**; if required, sign in to the Microsoft 365 admin center as **holly@AdatumXXYYZZ.onmicrosoft.com** with the password of **Pa\$\$w0rd**.
3. Open another tab on your browser and go to: **https://www.microsoft.com/en-us/evalcenter/evaluate-microsoft-advanced-threat-analytics**.
4. Fill out the **Start your evaluation** section by using the **Holly** account.
  - Company: use your custom **Adatum** name as directed in the start of this lab
  - Work email: use the **holly onmicrosoft** account
  - Phone number: **111 111 1111**
  - Country: **United Kingdom**
5. Save the application that will be downloaded on the bottom of your page.
6. Click the open folder.
7. Double-click on **ATA1.9.iso**.
8. Right click on the **Microsoft ATA Center Setup.exe** file and select **run as Administrator**.

### Task 2 – Install an ATA center on your Domain Controller

1. In the main UI of the **Microsoft Advanced Threat Analytics**, select **English** as the **language**, and then click **Next**.

2. Select the **I accept Microsoft Software License Terms agreement** checkbox, and then click **Next**.
3. On the **Use Microsoft update to help keep your computer secure** screen, ignore the warning and click **Next**.
4. On the **Configure the Center splash** screen confirm that the **self-signed certificate** option is checked.
5. Click **Install**.
6. Once the ATA center is installed, click **Launch**. A web browser will appear and **directory services** will display on the main page.  
**Note:** If you get a certificate error, click **continue to the website**.
7. Fill in the following field values:
  - Username: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **LON-DC1.Adatum.com**
8. Click **Save**.
9. On the left-hand pane select **Gateways**.
10. Click **Gateway Setup**.
11. On the download menu click **Save**.
12. Select **open folder**.
13. In the folder, right-click on the **Microsoft ATA Gateway Setup.zip** file and select **extract all**.
14. Leave the folder destination and click **extract**.
15. In the folder right click on **Microsoft ATA Gateway Setup.exe** and select **run as Administrator**.
16. The gateway UI will appear. Click **Next**.
17. Select **English** and then click **Next**.
18. Ignore the minimum requirements warning and click **Next**, and then click **Install**.
19. After the installation completes click **Finish**. You have now successfully installed the ATA Center on your domain controller.

End of lab