20347A-V2 – Enabling and Managing Office 365

Lab Steps for XTREMELABS

This document supersedes the Lab Step documentation provided in the standard 20347A Digital MOC distribution when the class is using Microsoft Labs Online for student lab access.

When XTREMELABS is being used to teach this class, students should refer to the Skillpipe reader only for general course material in each module. When performing the required lab steps students should use this document and not the steps described in the Skillpipe module documentation.

The XTREMELABS implementation of labs for this course uses pre-created Lab VMs which are hosted on the XTREMELABS platform. Doing so ensures a much more efficient lab experience during the course and allows students to focus on the core content without learning about Azure internals.

Note that this XTREMELABS hosted Lab implementation differs from the standard XTREMELABS Lab environment, in that the lab sessions runs for 5 contiguous days and each lab section is cumulative, building on the previous steps. Students and instructors should review the "**Notes about XTREMELABS Hosted 20347A Labs**" section before starting the lab environment.

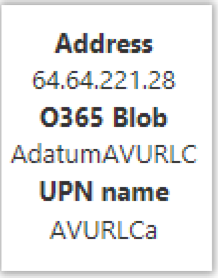
Notes about XTREMELABS Hosted 20347A Labs

The Microsoft Labs Online (XTREMELABS) implementation for course 20347A differs from the standard XTREMELABS experience. The Virtual Machines which each student and instructor uses are hosted on the XTREMELABS platform with a unique pre-built environment created specifically for that user. Before using the lab environment to complete the steps in this manual, all users should review the following notes which describe the difference between this and other XTREMELABS environments.

General Differences with 20347A XTREMELABS

- **User attachment to Lab Instance** - once a user has launched their 20347A lab instance they are automatically attached to it for 5 days.
  - For the duration of the class (5 days) the user may not launch any other courses under that user ID.
  - Once attached, when logging into the XTREMELABS platform the user will be taken directly to their running 20347A instance.
  - At the conclusion of the class 5 days after class start the 20347A lab instance will be closed and the user may launch any other course labs to which they have access, but not the 20347A class.
- **No "End Lab" Option** - There is no "End Lab" option for the 20347A XTREMELABS user interface.
  - To prevent users from accidentally tearing down their working and partially configured 20347A environments the web UI does not contain the "End Lab" option.
  - All student tenants will normally be torn down automatically 5 days after the lab is launched.
  - Each student's environment will continue to run during the 5 days to ensure that VMs are always available and connectivity with O365 is maintained.
- **Use this Manual for all Lab Steps** - This is a specific version of the student Lab Steps which must be used with this XTREMELABS hosted implementation.
  - Users should not follow the lab steps in the standard DMOC course content as they do not match this lab environment.
  - This specific version can be downloaded from the Lab View page of the XTREMELABS 20347A.
  - This manual is based on the standard 20347A lab manual set, but many steps have been removed or modified as they are no longer required in this implementation.
- **Firefox Browser Not Recommended** - We do not recommend using Firefox browser to access this course XTREMELABS lab environment.
  - A bug in the Firefox HTML5 implementation causes some keyboard characters to be dropped.
  - Specifically, such important characters such as hyphen and colon (- and :) may not be accessible.
  - We therefore recommend students and instructors using Internet Explorer, Chrome or Safari as these are fully tested and known to be working.
- **Network Troubleshooting Guide –** Students may occasionally have trouble with the networking portions of the lab steps. To rule out mistakes, a Network Troubleshooting Guide is available in the Lab Notes, located in the File Menu in the upper-right of the Lab Environment.

- **Unique User Session Numbers**
  - Once a user has connected to their 20347A XTREMELABS Lab Instance, they are presented with the Lab View web page.
  - On that page each lab user is provided with a unique IP address and two globally unique names used during the labs.
  - These are presented in the 'Lab Network Info', located in the 'Files' menu in the top right of the Lab View UI.
  - The names and IP addresses are unique to each lab user and are used to publish specific endpoints on the Internet. They must be typed exactly as written.
  - These names are used at many points throughout all modules of the course. The IP address is used in only two modules.



Address
64.64.221.28
O365 Blob
AdatumAVURLC
UPN name
AVURLCa

- **Domain Name Formats**
  - The steps use two different unique domain names during the Lab Steps, as follows (using the example unique names based on AVURLC from the graphic above):

Names	Typical Format as typed	Used in Modules
O365 Domain	**AdatumAVURLC.onmicrosoft.com**	All
UPN	**AVURLCa.xtremelabs.us**	All

Lab environment virtual machines:

- LON-CL1
- LON-CL2
- LON-CL3
- LON-DC1
- LON-DS1
- LON-WAP1

Domain names:

- Adatum.com is the Adatum Corporation 's internal private domain name.
- AdatumAVXXXX.onmicrosoft.com is the temporary Office 365 domain assigned to Adatum Corporation at the start of the pilot project. This identifier is unique to your session and is displayed in your Lab View web page.

Module 1: Planning and provisioning Office 365

Lab: Provisioning Office 365

Exercise 1: Configuring an Office 365 tenant

▶ Task 1: Create the tenant account

1. On **LON-CL1**, log on as **Adatum\Holly** using the password **Pa55w.rd**, on the Task bar, click **Microsoft Edge**.
2. In the address bar, type **https://products.office.com/en-us/business/office-365-enterprise-e5-business-software**, and then press Enter.
3. Click **Free trial**.
4. For Step 1, in the **Welcome, let's get to know you** page, complete the following fields. Regardless of your location, use the following information:
    - Country: **United Kingdom**
    - First name: **Holly**
    - Last name: **Spencer**
    - Business email address: **(use your new Microsoft account that you created for this course)**
    - Business phone number: **Your mobile phone number, including international code for your current country**
    - Company name: **A. Datum**
    - Organization size: **50-249 people**
5. Click **Next**.
6. For Step 2, in the **Create your user ID** page, you have to create a unique domain for the Company name to use in the course. Use the **AdatumAVXXXX** name provided by **XtremeLabs** (Located in the **Lab Network Info** found in the **Files** menu of the lab environment). For the rest of the fields, use the following information:
    - User name: **Holly**
    - Company name: **AdatumAVXXXX** (where **AVXXXX** is your unique Adatum number)
    - Password: **Pa55w.rd1**
    - Confirm password: **Pa55w.rd1**
7. Click **Create my account.**
8. For Step 3, on the **Prove. You're. Not. A. Robot.** page, you have to confirm your identity using your mobile phone. Under **Text me** from the drop-down box, select the code for the country that you are now in.
9. In the **Phone number** box, enter your correct mobile phone number.
10. Ensure that the **Text me** option is selected, and then click **Text me**.
11. When you receive the confirmation text on your mobile phone, enter the code provided in the **Enter your verification code** box.

12. Click **Next**.
13. Wait until the Office 365 tenant is provisioned, note your sign in data, and then click **You're ready to go…**

Note: If **You're ready to go** doesn't appear within 1 minute, navigate to **portal.office.com** and sign in as **Holly@AdatumAVXXXX.onmicrosoft.com** with the password **Pa55w.rd1,** then proceed with step 14. If it does appear and your trial is provisioned, proceed with Task 2.

14. Click the **Admin** tile to go to the Office 365 admin center. If a confirm your current password page appears, click **re-enter my password**, and type **Pa55w.rd1**
15. If the **Welcome to the new Office365 admin center** window appears, close it.
16. Click **Billing** on the left-hand menu, then click **Purchase Services**
17. Scroll down to **Office 365 Enterprise E5** and click on **Start Free Trial**
18. On the **Check Out** page, click **Try Now**, then click **Continue**
19. On the left-hand menu, click **Users**, then click **Active Users**, and select **Holly Spencer**
20. Click **Edit** next to Product licenses, and enable the **Office 365 Enterprise E5** license
21. Sign out of the office portal, and sign in as **Holly@AdatumAVXXXX.onmicrosoft.com** with the password **Pa55w.rd1**. Your trial tenant will now begin to provision. You may proceed to the next task while this takes place.

▶ Task 2: Verify Office 365 service health

1. Click **Health** on the left-hand menu, then click **Service health** to display the Service health dashboard.
2. In the left pane, view the status of the Office 365 services. If any services are showing a status other than **healthy**, click the service.
3. Review any service interruption records or additional information in the status page.

Note: During Microsoft testing, on rare occasions Office 365 did not create the trial tenant properly; as a result, the tenant did not have all the services available to it. If this happens to you, you should create a new trial tenant using a different business email (Microsoft account).

4. Close Microsoft Edge.
5. If prompted, click **Close all tabs**.

Results: After completing this exercise, you should have successfully provisioned the Office 365 tenant account for A. Datum Corporation.

Exercise 2: Configuring a custom domain

▶ Task 1: Add the custom domain

1. On **LON-CL1**, start **Microsoft Edge**, and then browse to **portal.office.com**.
2. Sign in as **Holly@AdatumAVXXXX.onmicrosoft.com** with the password **Pa55w.rd1**

3. Click **Admin**.
4. In the left-hand menu, click **Setup** and then click **Domains**.
5. Click **Add domain**.
6. In the New Domain window, in the text box enter your domain name in the form of **AVXXXXa.xtremelabs.us**
7. Click **Next**.
8. On the **Verify domain** page, click **TXT record**.
9. Write down the **TXT** record shown in the **TXT value** column. This entry will be similar to MS=msXXXXXXXX. Record this value below:

   MS=_____________________
10. Switch to **LON-DC1**.
11. Click **Start**, and then click **Server Manager**
12. Click **Tools**, and then click **DNS**.
13. Expand **LON-DC1**, and click **Forward Lookup Zones**.
14. Right-click **Forward Lookup Zones** and click **New Zone**.
15. On the **New Zone Wizard** page, click **Next**.
16. On the **Zone Type** page, verify that **Primary zone** is selected.
17. Clear the **Store the zone in Active Directory** check box, and click **Next**.
18. On the **Zone Name** page, type **AVXXXXa.xtremelabs.us** and click **Next**.
19. On the **Zone File** page, click **Next**.
20. On the **Dynamic Update** page, click **Next**, and then click **Finish**.
21. Expand **Forward Lookup Zones**, click and then right-click **AVXXXXa.xtremelabs.us**, and then click **Other New Records**.
22. Under **Select a resource record type**, scroll down to **Text (TXT)**, and then click **Create Record**.
23. In the **New Resource Record** box, leave the **Record name** field blank.
24. In the **Text** field, enter **MS=msXXXXXXXX** that you recorded in Step 9.
25. Click **OK** to create the record.
26. In the **Resource Record type** dialog box, click **Done**.
27. Right-click **AVXXXXa.xtremelabs.us**, and click **New Host (A or AAAA)**.
28. In the **New Host** box, Under **Name**, type **NLS01**
29. Under **IP address**, provide the IP address of the external name server as provided by **XtremeLabs**. (Located in the **Lab Network Info** found in the **Files** menu of the lab environment UI)
30. Click **Add Host**, click **OK,** and then click **Done**.
31. Double-click the **Start of Authority (SOA)** record and replace the **Primary Server** reference with **NLS01.AVXXXXa.xtremelabs.us** then click **OK**.

32. Double-click the **Name Server (NS)** record, and click **Edit**. Replace the **Server fully qualified domain name (FQDN)** name with **NLS01.AVXXXXa.xtremelabs.us**. Click **Resolve**, and then click **OK** twice.

33. Switch back to **LON-CL1** and in the Office 365 Admin center, click **Verify**.

Note: If you are having difficulty verifying the custom domain, please review the network troubleshooting guide located in the Lab Notes in the File Menu in the upper-right of the lab environment.

▶ Task 2: Completing the custom domain setup

1. On the **Set up your online services** page, if it appears, accept the default setting of **I'll manage my own DNS records**, and then click **Next**.

2. On the **Update DNS settings** page, review the DNS records that you should add to the domain, select the **Skip this step** check box, and click **Skip**.

3. Click **Finish**. The domain shows a warning icon because you did not verify the DNS records. You can ignore this warning for now.

Results: After completing this exercise, you should have:

- Added a custom domain.
- Verified domain ownership.

Exercise 3: Exploring the Office 365 administrator interfaces

▶ Task 1: Explore the Office 365 admin center

1. On **LON-CL1**, in the Admin center, click **Home**.

2. On the left navigation menu, scroll down to explore all available items. Expand items such as Users, Groups, Settings, etc.

3. On the left navigation menu, expand **Users**, and then click **Active users**.

4. Review the users list.

5. On the left navigation menu, expand **Health**, and then click **Message center**, and then in the right pane, review the messages.

6. Do not close the browser window.

▶ Task 2: Explore the Exchange admin center

1. On the left navigation menu, expand **Admin centers**, and then click **Exchange**.

2. A new tab will open displaying **Exchange admin center**.

3. On the left navigation menu, click each of the items, and review the results displayed on the right pane.

▶ Task 3: Explore the Skype for Business admin center

1. Click the **portal.office.com** tab.

2. On the left navigation menu, under **Admin centers**, click **Skype for Business**.

3. A new tab will open displaying **Skype for Business admin center**.
4. On the left navigation menu, click each of the items, and review the results displayed on the right pane.

▶ Task 4: Explore the SharePoint admin center

1. Click the **portal.office.com** tab.
2. On the left navigation menu, click **Admin centers**, and then click **SharePoint**.
3. A new tab will open displaying **SharePoint admin center**.
4. On the left navigation menu, click each of the items, and review the results displayed on the right pane.
5. Close Microsoft Edge.

▶ Task 5: Explore the Office 365 Security & Compliance Center

1. Click the **portal.office.com** tab.
2. On the left navigation menu, click **Admin centers**, and then click **Security & Compliance**.
3. A new tab will open displaying **Security & Compliance admin center**.
4. On the left navigation menu, click each of the items, and then review the results displayed in the right pane.
5. Close Microsoft Edge.

▶ Task 6: To prepare for the next module

Keep the virtual machines running for the lab in the next module.

Results: After completing this exercise, you should have provided a high-level overview of administrative portals of Office 365.

Module 2: Managing Office 365 users and groups

Lab A: Managing Office 365 users and passwords

Exercise 1: Managing Office 365 users and licenses by using the Office 365 admin center

▶ Task 1: Create Office 365 users

1. On **LON-CL1**, verify that you signed in as **Adatum\Holly**.
2. Open **Microsoft Edge**, and then browse to **https://portal.office.com/**
3. Sign in as **Holly@AdatumAVXXXX.onmicrosoft.com**, where **AVXXXX** is your unique Adatum number, with the password **Pa55w.rd1**
4. On the Microsoft Office 365 portal, click **Admin**.
5. On the menu on the left side, click **Users**, and then click **Active Users**.
6. Click **Add a user**.
7. On the **New User** page, in the **First name** text box, type **Lindsey**.
8. In the **Last name** text box, type **Gates**.
9. Notice the **Display name** text box is automatically filled in as **Lindsey Gates**.
10. In the **User name** text box, type **Lindsey**.
11. Verify that **AVXXXXa.xtremelabs.us** is listed in the text box after the at sign (@), where **AVXXXXa** is your unique domain name
12. Click **Password,** select **Let me create the password** and enter **Pa55w.rd.** Clear the **make this user change their password when they first sign in** checkbox
13. Click **Send email and close**.
14. Repeat steps 6 to 13 to create the following users (for the **User name**, use the **First name**):
    - **Christie Thomas**
    - **Amy Santiago**
    - **Sallie McIntosh**
    - **Francisco Chaves**

▶ Task 2: Edit Office 365 users

1. In the Office 365 admin center, in the **Active Users** list, click the **Francisco Chaves** user object.
2. On the right side, beside **Display name**, click **Edit**.
3. On the **Edit contact information** page, expand **Contact information**, and in the **Department** text box, type **Accounts**, click **Save**, and then click **Close**.
4. On the right side menu, in the **Sign in status** section, click **Edit**.
5. Click **Sign-in blocked**, click **Save**, and then click **Close**.

6. Close the **Francisco Chaves** page.
7. In the **Active Users** list, under **Display name**, click **Francisco Chaves**.
8. On the right side, beside **Display name**, click **Edit**.
9. Verify that the **Department** box displays **Accounts**, and then close the page.
10. Verify that **Sign-in status** is set to **Sign-in blocked**, and then close the **Francisco Chaves** page.
11. In the **Active Users** list, click the **Lindsey Gates** user object.
12. On the top menu, click **Delete user**.
13. On the **Delete user** page, click **Delete**, and then click **Close**.
14. In the left navigation pane, click **Users**, and click **Deleted users**.
15. Verify that **Lindsey Gates** is in this list.
16. In the **Deleted users** list, select **Lindsey Gates**.
17. On the toolbar, click **Restore**, and then on the **Restore** page, click **Restore**.
18. Note the new temporary password, and then click **Send email and close**.
19. On the left navigation pane, click **Users**, and click **Active Users**.
20. Verify that **Lindsey Gates** is in this list.
21. Close **Microsoft Edge**.

▶ Task 3: Verifying user settings

1. On **LON-CL1**, open **Microsoft Edge**, and then browse to **https://portal.office.com/**
2. Sign in as **Lindsey@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
3. Verify that you can access the Office 365 portal home page.
4. Close **Microsoft Edge**.
5. Open **Microsoft Edge**, and then browse to **https://portal.office.com/**
6. Sign in as **Francisco@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
7. Verify that you cannot sign in and that the message states that your account has been locked.
8. Close **Microsoft Edge**.
9. Open **Microsoft Edge**, and then browse to **https://portal.office.com/**
10. Sign in as **Holly@AdatumAVXXXX.onmicrosoft.com** with the password **Pa55w.rd1**
11. On the Office 365 portal, click **Admin**.
12. On the left menu, click **Users**, and then click **Active Users**.
13. In the **Active Users** list, click **Francisco Chaves**.
14. On the right side, in the **Sign-in status** section, click **Edit**.
15. On the **Sign in status** page, select **Sign-in allowed**, click **Save**, and then click **Close**.
16. Close **Microsoft Edge**.
17. Open **Microsoft Edge**, and then browse to **https://portal.office.com/**

18. Sign in as **Francisco@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
19. Verify that you can access the **Office 365 portal**.
20. Close **Microsoft Edge**.

Results: After completing this exercise, you should have created and managed user accounts and licenses according to business needs.

Exercise 2: Managing Office 365 password policies

▶ Task 1: Configure the Office 365 password policy

1. Open **Microsoft Edge**, and then browse to **https://portal.office.com/**
2. Sign in as **Holly@AdatumAVXXXX.onmicrosoft.com** with the password **Pa55w.rd1**
3. On the Office 365 portal, click **Admin**.
4. On the left side menu, click **Settings**, and then click **Security & privacy**.
5. In the **Password policy** area, click **Edit**.
6. In the **Password policy** page, in the **Days before passwords expire** text box, type **14**.

Note: This setting does not correspond with a real-world scenario. Use it as a sample scenario to verify the policy applied in the next exercise task.

7. In the **Days before a user is notified about expiration** box, leave the default value of **14**, and then click **Save**.
8. Verify that the **"Password policy has been updated"** message appears at the top of the page and then click **Close**.
9. Close **Microsoft Edge**.

▶ Task 2: Validate the password policy

1. Open **Microsoft Edge**, and then browse to **https://portal.office.com**
2. Sign in as **Lindsey@AVXXXXa.xtremelabs.us**, where **AVXXXXa** is your unique domain name, with the password **Pa55w.rd**
3. On the upper-right side of the window, verify that the notification appears with the following information: **"Time to change your password. Your password will expire in 13 days."**

Note: It might take a few minutes before the password change notification appears.

Note: You have now verified that your password policy is applied. In a real-world scenario, after you verify that the password policy is applied, you would need to increase the number of days before the password expires, according to your organizational policy.

4. Close **Microsoft Edge**.

▶ Task 3: Enable multi-factor authentication

1. Open **Microsoft Edge**, and then browse to **https://portal.office.com**
2. Sign in as **Holly@AdatumAVXXXX.onmicrosoft.com**, where **AVXXXX** is your unique Adatum number, with the password **Pa55w.rd1**
3. In the Microsoft Office 365 portal, click **Admin**.
4. On the **Home** page, on the left menu, click **Settings**, and then click **Services & add-ins**.
5. On the **Services & add-ins** page, click **Azure multi-factor authentication**.
6. On the **Azure multi-factor authentication** page, click **Manage multi-factor authentication**.
7. On the **multi-factor authentication** page, select the **Amy Santiago** check box, and then click **Enable**.
8. In the **About enabling multi-factor auth** pop-up, click **enable multi-factor auth**, and then click **Close**.
9. On the **multi-factor authentication** page, click **service settings**.
10. Under **verification options**, clear the **Call to phone** check box, click **save**, and then click **Close**.
11. Close **Microsoft Edge**.

Results: After completing this exercise, you should have configured and validated an Office 365 password policy.

▶ Task: To prepare for the next lab

Keep the virtual machines running for the next lab in this module.

Lab B: Managing Office 365 groups and administration

Exercise 1: Managing Office 365 groups

▶ Task 1: Creating Office 365 security groups

1. On **LON-CL1**, open **Microsoft Edge**, and then browse to **https://portal.office.com/**
2. Sign in as **Holly@AdatumAVXXXX.onmicrosoft.com**, where **AVXXXX** is your unique Adatum number, with the password **Pa55w.rd1**
3. In the Office 365 admin center, click **Admin**.
4. On the left side menu, click **Groups**, click **Groups**, and then click **Add a group**.
5. On the **New Group** page, in the **Type** drop-down box, click **Security group**, and in the **Name** text box, type **Sales**.
6. In the **Description** text box, type **Sales department users**, click **Add**, and then click **Close**.
7. Select the **Sales** group, and then on the **Sales** page, next to **Members**, click **Edit**.
8. Click **Add members**, click **Lindsey Gates**, click **Christie Thomas**, click **Save**, and then click **Close** three times.
9. Click **Add a group**.
10. On the **New Group** page, in the **Type** drop-down box, click **Security group**, and then in the **Name** text box, type **Accounts**.
11. In the **Description** text box, type **Accounts department users**, click **Add**, and then click **Close**.
12. Select the **Accounts** group, and then on the **Accounts** page, next to **Members**, click **Edit**.
13. Click **Add members**, click **Francisco Chaves**, click **Sallie McIntosh**, click **Save**, and then click **Close** three times.

▶ Task 2: Manage security groups

1. In the **Office 365 admin center**, verify that you can see the following groups:
    - **Sales**
    - **Accounts**
2. In the **Groups** list, select the **Sales** group, and then on the **Sales** page, next to **Members**, click **Edit**.
3. Click **Add members**, click **Amy Santiago**, click **Save**, and then click **Close** three times.
4. Open **Sales** details page, and ensure that **Amy Santiago** now lists under the **Members** list.
5. Click **Delete group**.
6. On the **Delete group** page, click **Delete**, and then click **Close**.
7. On the left side menu, click **Users**, and then click **Active users**.
8. Confirm that **Amy Santiago's** account still exists in the list of users.
9. Close **Microsoft Edge**.

Results: After completing this exercise, you should have created and managed security groups.

Exercise 2: Managing Office 365 users and groups by using Windows PowerShell

▶ Task 1: Installing Microsoft Azure Active Directory module for Windows PowerShell

1. On **LON-CL1**, open **Microsoft Edge**, and browse to **http://aka.ms/t01i1o**
2. Under **Microsoft Online Services Sign-In Assistant for IT Professionals RTW**, click **Download**.
3. Select the **en\msoidcl_64.msi** check box, and then click **Next**.
4. When prompted, click **Save**.
5. When the download finishes, click **Run**.
6. In the **Microsoft Online Services Sign-in Assistant Setup wizard**, click **I accept the terms in the License Agreement and Privacy Statement**, and then click **Install**.
7. In the **User Account Control** dialog box, click **Yes**.
8. On the **Completed the Microsoft Online Services Sign-in Assistant Setup Wizard** page, click **Finish**.
9. In **Microsoft Edge**, browse to **http://aka.ms/siqtee**, and then next to **AdministrationConfig-V1.1.166.0-GA.msi**, click **Download**.
10. Click **Save**. After **AdministrationConfig_3.msi** finishes downloading, click **Run**.
11. In the **Microsoft Azure Active Directory Module for Windows PowerShell Setup wizard**, click **Next**.
12. On the **License Terms** page, click **I accept the terms in the License Terms**, and click **Next**.
13. On the **Install Location** page, click **Next**.
14. On the **Ready to Install** page, click **Install**.
15. In the **User Account Control** dialog box, click **Yes**.
16. On the **Completing the Microsoft Azure Active Directory Module for Windows PowerShell Setup** page, click **Finish**.
17. Close **Microsoft Edge**.

▶ Task 2: Create new users and assign licenses by using Windows PowerShell

1. On **LON-CL1**, on the desktop, right-click the **Windows Azure Active Directory Module for Windows PowerShell** shortcut, and then click **Run as administrator**.
2. If a **User Account Control** dialog box appears, click **Yes**.
3. At the command prompt, type the following command, and then press Enter:

   ```
   Connect-MsolService
   ```

4. In the **Enter Credentials** dialog box, sign in as **Holly@AdatumAVXXXX.onmicrosoft.com**, where **AVXXXX** is your unique Adatum number, with the password **Pa55w.rd1**
5. At the command prompt, type the following command, and then press Enter; **AVXXXXa** is your unique domain name:

```
New-MsolUser –UserPrincipalName Catherine@AVXXXXa.xtremelabs.us –DisplayName “Catherine
Richard” –FirstName “Catherine” –LastName “Richard” –Password ‘Pa55w.rd’ –
ForceChangePassword $false –UsageLocation “CH”
```

6. At the command prompt, type the following command, and then press Enter; **AVXXXXa** is your unique domain name:

```
 New-MsolUser –UserPrincipalName tameka@AVXXXXa.xtremelabs.us –DisplayName “Tameka
Reed” –FirstName “Tameka” –LastName “Reed” –Password ‘Pa55w.rd’ –ForceChangePassword
$false –UsageLocation “CH”
```

7. To determine which users are unlicensed, at the command prompt, type the following command, and then press Enter:

```
Get-MsolUser –UnlicensedUsersOnly
```

8. To view the available licenses, at the command prompt, type the following command, and then press Enter:

```
Get-MsolAccountSku
```

9. To license **Catherine Richard**, at the command prompt, type the following command, and then press Enter; replace **AdatumAVXXXX** in the **–AddLicenses** attribute with the Adatum domain name provided by XtremeLabs:

```
Set-MsolUserLicense -UserPrincipalName Catherine@AVXXXXa.xtremelabs.us –AddLicenses
“AdatumAVXXXX:ENTERPRISEPREMIUM”
```

10. To license **Tameka Reed**, at the command prompt, type the following command, and then press Enter; replace **AdatumAVXXXX** in the **–AddLicenses** attribute with the Adatum domain name provided by XtremeLabs:

```
Set-MsolUserLicense -UserPrincipalName Tameka@AVXXXXa.xtremelabs.us –AddLicenses
“AdatumAVXXXX:ENTERPRISEPREMIUM”
```

11. To prevent a user from signing in, at the command prompt, type the following command, and then press Enter; **AVXXXXa** is your unique domain name:

```
Set-MsolUser -UserPrincipalName Catherine@AVXXXXa.xtremelabs.us -BlockCredential $true
```

12. To delete a user, at the command prompt, type the following command, and then press Enter; **AVXXXXa** is your unique domain name:

```
Remove-MsolUser -UserPrincipalName Catherine@AVXXXXa.xtremelabs.us –Force
```

13. To view the **Deleted Users** list, at the command prompt, type the following command, and then press Enter:

```
Get-MsolUser –ReturnDeletedUsers
```

14. Verify that **Catherine Richard** is in the list of deleted users. Note that it specifies that she is still licensed.

15. To restore a deleted user, at the command prompt, type the following command, and then press Enter; **AVXXXXa** is your unique domain name:

```
Restore-MsolUser –UserPrincipalName Catherine@AVXXXXa.xtremelabs.us
```

16. To view the deleted users list, at the command prompt, type the following command, and then press Enter:

```
Get-MsolUser –ReturnDeletedUsers
```

17. Verify that **Catherine Richard** is no longer in the list of deleted users.

18. To view the active users list, at the command prompt, type the following command, and then press Enter:

```
Get-MsolUser
```

19. Verify that **Catherine Richard** is in the active users list.

20. To allow a user to sign in, at the command prompt, type the following command, and then press Enter; **AVXXXXa** is your unique domain name:

```
Set-MsolUser -UserPrincipalName Catherine@AVXXXXa.xtremelabs.us -BlockCredential $false
```

▶ Task 3: Modify existing users by using Windows PowerShell

1. On **LON-CL1**, on the taskbar, click **File Explorer**.

2. Navigate to **C:\labfiles**, right-click **O365users.csv**, point to **Open with**, and then click **Notepad**.

3. In Notepad, click **Edit**, and then click **Replace**.

4. In the **Find what** text box, type **yourdomain.hostdomain.com**

5. In the **Replace with** text box, type **AVXXXXa.xtremelabs.us**, where **AVXXXXa** is your unique domain name provided by XtremeLabs, and then click **Replace All**.

6. In the **Find what** text box, type **Adatumyyxxxx:ENTERPRISEPACK**

7. In the **Replace with** text box, type your unique **AdatumAVXXXX** value followed by **:ENTERPRISEPREMIUM**, and then click **Replace All**.

Note: AdatumAVXXXX in this step must be the onmicrosoft.com domain name.

8. Close O365users.csv, and then in the **Notepad** message box, click **Save**.

9. To bulk import several users from a comma-separated value (CSV) file, copy and paste this code into the **Administrator: Windows Azure Active Directory Module for Windows PowerShell** window on **LON-CL1**, and then press Enter:

```
Import-Csv -Path C:\labfiles\O365Users.csv | ForEach-Object { New-MsolUser -
UserPrincipalName $_."UPN" -AlternateEmailAddresses $_."AltEmail" -FirstName
$_."FirstName" -LastName $_."LastName" -DisplayName $_."DisplayName" -BlockCredential
$False -ForceChangePassword $False -LicenseAssignment $_."LicenseAssignment" -Password
$_."Password" -PasswordNeverExpires $True -Title $_."Title" -Department $_."Department"
-Office $_."Office" -PhoneNumber $_."PhoneNumber" -MobilePhone $_."MobilePhone" -Fax
$_."Fax" -StreetAddress $_."StreetAddress" -City $_."City" -State $_."State" -
PostalCode $_."PostalCode" -Country $_."Country" -UsageLocation $_."UsageLocation" }
```

10. To view the **Active Users** list, at the command prompt, type the following command, and then press Enter:

```
Get-MsolUser
```

11. Switch back to Microsoft Edge, click **Admin**.

12. On the Home page, click **Users**.

13. Review the active users that you just imported.

14. On the Admin center menu, click **Exchange**.

15. Under recipients, click **mailboxes** and review the mailboxes and associated email addresses that were created.

▶ Task 4: Configure groups and group membership by using Windows PowerShell

1. To create a Marketing group, at the command prompt, type the following command, and then press Enter:

```
New-MsolGroup –DisplayName “Marketing” –Description “Marketing department users”
```

2. To configure a variable for the group, at the command prompt, type the following command, and then press Enter:

```
$MktGrp = Get-MsolGroup | Where-Object {$_.DisplayName -eq "Marketing"}
```

3. To configure a variable for the first user account, at the command prompt, type the following command, and then press Enter:

```
$Catherine = Get-MsolUser | Where-Object {$_.DisplayName -eq "Catherine Richard"}
```

4. To configure a variable for the second user account, at the command prompt, type the following command, and then press Enter:

```
$Tameka = Get-MsolUser | Where-Object {$_.DisplayName -eq "Tameka Reed"}
```

5. To add **Catherine Richard** to the Marketing group, at the command prompt, type the following command, and then press Enter:

```
Add-MsolGroupMember -GroupObjectId $MktGrp.ObjectId -GroupMemberType "User" -
GroupMemberObjectId $Catherine.ObjectId
```

6. To add **Tameka Reed** to the Marketing group, at the command prompt, type the following command, and then press Enter:

```
Add-MsolGroupMember -GroupObjectId $MktGrp.ObjectId -GroupMemberType "User" -
GroupMemberObjectId $Tameka.ObjectId
```

7. To verify the members of the Marketing group, at the command prompt, type the following command, and then press Enter:

```
Get-MsolGroupMember -GroupObjectId $MktGrp.ObjectId
```

▶ Task 5: Configure user passwords by using Windows PowerShell

1. At the command prompt, type the following command, and then press Enter; **AVXXXX** is your unique Adatum number:

```
Set-MsolPasswordPolicy -DomainName “AdatumAVXXXX.onmicrosoft.com” –ValidityPeriod “90”
-NotificationDays “14”
```

2. At the command prompt, type the following command, and then press Enter; **AVXXXXa.xtremelabs.us** is your unique domain name:

```
Set-MsolUserPassword –UserPrincipalName “Tameka@AVXXXXa.xtremelabs.us” –NewPassword
‘Pa55w.rd123’
```

3. At the command prompt, type the following command, and then press Enter:

```
Get-MsolUser | Set-MsolUser –PasswordNeverExpires $false
```

Results: After completing this exercise, you should have created new users, assigned licenses, modified existing users, and configured groups and user passwords by using the Windows PowerShell command-line interface.

Exercise 3: Configuring service administrators

▶ Task 1: Assign service administrators in the Office 365 admin center

1. On **LON-CL1**, open **Microsoft Edge**, and then browse to **https://portal.office.com**
2. Sign in as **Holly@AdatumAVXXXX.onmicrosoft.com**, where **AVXXXX** is your unique Adatum number, with the password **Pa55w.rd1**
3. In the Office 365 admin center, click **Admin**.
4. On the left-hand side, click **Users**, click **Active users**, and then click **Francisco Chaves**.
5. On the **Francisco Chaves** page, in the Roles section, click **Edit.**
6. Under Edit user role, click **Customized administrator**, select **Billing administrator** from the list, click **Save**, and then click **Close** twice.
7. In the list view, click **Tameka Reed**.
8. On the **Tameka Reed** page, in the Roles section, click **Edit**.
9. Under Edit user role, click **Customized administrator**, and then select **Password administrator** from the list.
10. Click **Save**, and then click **Close** twice.
11. In the list view, click **Christie Thomas**.
12. On the **Christie Thomas** page, in the Roles section, click **Edit**.
13. Under Assign role, click **Customized administrator**, and then select **User management administrator** from the list.
14. Above the **Alternative email address** text box, click **Edit**, in the text box type **user@alt.none**, click **Save**, and then click **Close** twice.
15. Close **Microsoft Edge**.

▶ Task 2: Manage service administration with Windows PowerShell

1. In the Windows PowerShell window, at the command prompt, type the following command, and then press Enter:

```
Add-MsolRoleMember –RoleName “Service Support Administrator” –RoleMemberEmailAddress
“Sallie@AVXXXXa.xtremelabs.us”
```

2. At the command prompt, type the following command, and then press Enter:

   ```
   Add-MsolRoleMember –RoleName “Company Administrator” –RoleMemberEmailAddress
   “Amy@AVXXXXa.xtremelabs.us”
   ```

3. At the command prompt, type the following command, and then press Enter:

   ```
   $role = Get-MsolRole –RoleName “Service Support Administrator”
   ```

4. At the command prompt, type the following command, and then press Enter:

   ```
   Get-MsolRoleMember –RoleObjectId $role.ObjectId
   ```

5. Verify that **Sallie McIntosh** is in the list of users who have the Service Support Administrator role.

6. At the command prompt, type the following command, and then press Enter:

   ```
   $role = Get-MsolRole –RoleName “Billing Administrator”
   ```

7. At the command prompt, type the following command, and then press Enter:

   ```
   Get-MsolRoleMember –RoleObjectId $role.ObjectId
   ```

8. Verify that **Francisco Chaves** is in the list of users who have the billing administrator role.

9. At the command prompt, type the following command, and then press Enter:

   ```
   $role = Get-MsolRole –RoleName “Company Administrator”
   ```

10. At the command prompt, type the following command, and then press Enter:

    ```
    Get-MsolRoleMember –RoleObjectId $role.ObjectId
    ```

11. Verify that **Amy Santiago** is in the list of users who have the Company Administrator role. You should also see **Holly Spencer** on the list.

12. Close the Windows PowerShell window.

▶ Task 3: Verify service administration

1. On **LON-CL1**, open **Microsoft Edge**, and then browse to **https://portal.office.com**
2. Sign in as **Tameka@AVXXXXa.xtremelabs.us**, where **AVXXXXa** is your unique domain name, with the password **Pa55w.rd123**
3. On the **Update your password** page, in the **Current password** text box, type **Pa55w.rd123**
4. In the **New password** and **Confirm password** text boxes, type **Pa55w.rd1**, and then click **Update password and sign in**.
5. On the Office 365 portal, click **Admin**.
6. If prompted, sign in again as **Tameka@AVXXXXa.xtremelabs.us** using the password **Pa55w.rd1**
7. On the Home page, click **Users**.
8. Click **Jessica Jennings**. Note that you cannot perform any administrative tasks.
9. Click **Reset password**.

10. On the **Reset password** page, click **Reset**.
11. Write down the temporary password here for future reference, and then click **Send email and close**:
    ____
12. Close and reopen **Microsoft Edge**, and then browse to **https://portal.office.com**
13. Sign in as **Christie@AVXXXXa.xtremelabs.us**, where **AVXXXXa** is your unique domain name, with the password **Pa55w.rd**
14. In the Office 365 portal, click **Admin**.
15. If prompted, sign in again as **Christie@AVXXXXa.xtremelabs.us** using the password **Pa55w.rd**
16. In the Office 365 admin center, on the Home page, click **Users**, and then click **Jessica Jennings**.
17. On the **Jessica Jennings** page, in the **Display name** section, click **Edit**.
18. On the **Edit contact information** page, expand **Contact** information.
19. In the **Office Phone** text box, type **555-1234**, click **Save**, and then click **Close**.
20. In the **Sign-in status** section, click **Edit**, click **Sign-in blocked**, click **Save**, and then click **Close** twice.
21. In the **Office 365 admin center**, click **Add a user**.
22. In the **First name** text box, type **Chris**.
23. In the **Last name** text box, type **Breland**.
24. In the **User name** text box, type **Chris**, click **Add**, in Product licenses section, enable **Office365 E5 license**, click **Add**, and then click **Send email and close**.
25. In the Active users list, click **Chris Breland**.
26. On **Chris Breland** page, click the **Delete user**.
27. On the **Delete user** page, click **Delete**, and then click **Close**.
28. Close **Microsoft Edge**.

Results: After completing this exercise, you should have assigned service administrators in the Office 365 admin center, managed service administration with Windows PowerShell, and verified service administration.

Module 3: Configuring client connectivity to Microsoft Office 365

Lab: Configuring client connectivity to Office 365

Exercise 1: Configuring DNS records for Office 365 clients

▶ Task 1: Review the recommended DNS records in the Office 365 admin center

1. On **LON-CL1**, open **Microsoft Edge**.
2. Connect to **http://portal.office.com**, and then sign in as **Holly@AdatumAVXXXX.onmicrosoft.com**, replacing **AdatumAVXXXX** with your unique Adatum number, and with the password **Pa55w.rd1**
3. In the Office 365 portal, click **Admin.**
4. In the Office 365 admin center, in the menu to the left, go to **Setup**, click **Domains**, and then review the domain names assigned to the **Adatum** tenant.
5. In the Domains window, click **AVXXXXa.xtremelabs.us**.
6. On the **DNS errors** page, review the records that need to be configured for your domain.
7. Leave the Microsoft Edge window open.

▶ Task 2: Configure the DNS records for external clients

Configure DNS settings for Exchange Online

1. On **LON-DC1**, open Server Manager.
2. In Server Manager, click the **Tools** menu, and then click **DNS**.
3. In DNS Manager, expand **LON-DC1**, and then expand **Forward Lookup Zones**.
4. Click, and then right-click **AVXXXXa.xtremelabs.us**, and then click **New Alias (CNAME)**.
5. In the **Alias name** text box, type **autodiscover** as the alias name.
6. In the **Fully qualified domain name (FQDN) for target host** text box, type **autodiscover.outlook.com**.
7. Click **OK**.
8. Right-click **AVXXXXa.xtremelabs.us**, and then click **New Mail Exchanger (MX)**.
9. In the Mail Exchanger (MX) dialog box, in the **Fully qualified domain name (FQDN) of mail server** text box, type **AVXXXXa-xtremelabs-us.mail.protection.outlook.com**
10. Click **OK**.

Configure DNS settings for Skype for Business Online

11. On **LON-DC1**, right-click the **AVXXXXa.xtremelabs.us** zone, and then select **Other New Records**.
12. In the **Resource Record Type** dialog box, scroll down the list, click **Service Location (SRV)**, and then click **Create Record**.

13. On the **Service Location (SRV)** tab, enter the following information, and then click **OK**:
    - Service: **_sip**
    - Protocol: **_tls**
    - Priority: **100**
    - Weight: **1**
    - Port number: **443**
    - Host offering this service: **sipdir.online.lync.com**
    - Time to live: **1 hour (default)**
14. In the **Resource Record Type** dialog box, click **Create Record**.
15. On the **Service Location (SRV)** tab, enter the following information, and then click **OK**:
    - Service: **_sipfederationtls**
    - Protocol: **_tcp**
    - Priority: **100**
    - Weight: **1**
    - Port number: **5061**
    - Host offering this service: **sipfed.online.lync.com**
    - Time to live: **1 hour (default)**
16. In the **Resource Record Type** dialog box, scroll back up the list, click **Alias (CNAME)**, and then click **Create Record**.
17. On the **Alias (CNAME)** tab, enter the following information, and then click **OK**:
    - Alias name: **sip**
    - Fully qualified domain name: **sip.AVXXXXa.xtremelabs.us**
    - Fully qualified domain name (FQDN) for target host: **sipdir.online.lync.com**
    - Time to live: **1 hour (default)**
18. In the **Resource Record Type** dialog box, click **Create Record**.
19. On the **Alias (CNAME)** tab, enter the following information, and then click **OK**:
    - Alias name: **lyncdiscover**
    - Fully qualified domain name: **lyncdiscover.AVXXXXa.xtremelabs.us**
    - Fully qualified domain name (FQDN) for target host: **webdir.online.lync.com**
    - Time to live: **1 hour (default)**
20. In the **Resource Record Type** dialog box, click **Done**.
21. Switch back to **LON-CL1**, and then in the Office 365 admin console, click **Check DNS**.
22. You should now see that most records are not listed anymore (you should see msoid, enterpriseregistration, enterpriseenrollment and SPF records). Close the page.

23. In the top bar, click **Office 365** apps icon.
24. Click **Mail**.
25. On the Outlook page, select your time zone and click **Save**.
26. In the upper right corner, click your user icon and select **Sign in to IM**.
27. On **LON-CL2**, verify that you are signed in as **Francisco**.
28. Open **Microsoft Edge**, and then connect to **https://portal.office.com**
29. Sign in as **Francisco@AVXXXXa.xtremelabs.us** by using the password **Pa55w.rd**
30. In the Office 365 portal, click **Mail**.
31. On the Outlook page, select your time zone, and then click **Save**.
32. In the upper right corner, click your user icon and select **Sign in to IM**.
33. In the upper-left corner, click the **New** button.
34. In the **To** text box, type **Holly Spencer**.
35. When the name resolves, note her instant message (IM) status. It might take a couple of minutes for her status to update.
36. Click **Holly Spencer** in the **To** text box.
37. In the pop-up dialog box, click the **IM** icon on the right (icon below email address, with same UPN as email).
38. In the IM pop-up window, type a message, and then press Enter.
39. On **LON-CL1**, click the **IM** dialog box.
40. Reply to the IM. Note that you now can send IMs between the two users.
41. Close both the IM windows, and then close the **Microsoft Edge** windows on both virtual machines.

Results: After completing this exercise, you should have:

- Reviewed the recommended DNS records in the Office 365 admin center.
- Configured the DNS records for external clients.
- Configured the DNS records for internal clients.

Exercise 2: Running the Office 365 connectivity analyzer tools

▶ Task 1: Run the Microsoft Connectivity Analyzer tool

1. On **LON-CL1**, open **Microsoft Edge**.
2. In the address bar, type **https://testconnectivity.microsoft.com/**
3. On the **Microsoft Remote Connectivity Analyzer** page, click the **Office 365** tab.
4. On the Office 365 tab, click **Office 365 Exchange Domain Name Server (DNS) Connectivity Test**, and then click **Next**.
5. Under **Domain Name**, type **AVXXXXa.xtremelabs.us**

6. Under **Verification**, type the characters that you can see in the verification field, and then click **Verify**.

   Note: The verification code is not case-sensitive.

7. Click **Perform Test**.

   Note: If you receive a message about having performed too many tests in 60 seconds, wait for a minute and then repeat the test.

8. When you see **Connectivity Test Successful**, under **Test Details**, expand **Test Steps**, and then review the checks that were made against the Exchange Online domain.
9. Click **Start Over**.
10. On the **Office 365** tab, click **Office 365 Lync Domain Name Server (DNS) Connectivity Test**, and then click **Next**.
11. In the **Sign-in address** text box, type **Francisco@AVXXXXa.xtremelabs.us**, and then click **Perform Test**.

    Note: If you receive a message about having performed too many tests in 60 seconds, wait for a minute and then repeat the test.

12. When you see **Connectivity Test Successful**, under **Test Details**, expand **Test Steps**, and then review the checks that were made against the Skype for Business Online domain.
13. Click **Start Over**.
14. Under **Microsoft Office Outlook Connectivity Tests**, click **Outlook Connectivity**, and then click **Next**.
15. On the Outlook Connectivity page, in **Email Address** and **Microsoft Account**, type **Francisco@AVXXXXa.xtremelabs.us**
16. In the **Password** and **Confirm password** text boxes, type **Pa55w.rd**
17. Select **Use Autodiscover to detect server settings**.
18. Select **I understand that I must use the credentials of a working account from my Exchange domain to be able to test connectivity to it remotely. I also acknowledge that I am responsible for the management and security of this account**.
19. Click **Perform Test**.
20. When you see **Connectivity Test Successful with Warnings**, under **Test Details**, expand **Test Steps**, and then review the checks that were made against **Outlook Anywhere**. Note in particular the message that contains information about the **Autodiscover** steps that fail.
21. Under **Run Test Again** at the top-right corner of the window, note that you can copy this test to the clipboard, or save it as an XML or HTML file.

▶ Task 2: Run the Office 365 Support and Recovery Assistant

1. In the Microsoft Connectivity Analyzer window, on the Client tab, in the Microsoft Support and Recovery Assistant for Office 365 section, click **Support and Recovery Assistant download**.
2. On the new web page that opens, click **Download now** and then click **Save**.
3. Wait for the download to finish, and then click **Run**.
4. In the Application Install – Security Warning window, click **Install**.
5. In the Microsoft Support and Recovery Assistant for Office 365 window, click **I agree**, then click **Advanced diagnostics**, and then click **Next**.
6. On the next page, click **Exchange Online** and click **Next**.
7. On the Select the diagnostic you'd like to run page, click **Perform authentication checks** and click **Next** and then select **Yes** and click **Next** again.
8. On the next page, type **Holly@AdatumAVXXXX.onmicrosoft.com**, type **Pa55w.rd1** as password, select **Keep me signed in** and then click **Next**.
9. Wait until Office 365 Support and Recovery assistant generates the results.
10. Review the details, and then close the window.

Results: After completing this exercise, you should have:

- Run the Microsoft Connectivity Analyzer tool.
- Run the Office 365 Client Performance Analyzer tool.

Exercise 3: Connecting Office 2016 clients

▶ Task 1: Verify that Outlook 2016 can connect to Office 365

1. On **LON-CL1**, start **Outlook 2016**.
2. On the Welcome to **Outlook 2016** page, click Next.
3. On the Add an Email Account page, click Next.
4. On the **Auto Account Setup** page, type the following information, and then click **Next**:
    - Your Name: **Holly Spencer**
    - E-mail Address: **Holly@AdatumAVXXXX.onmicrosoft.com**
    - Password: **Pa55w.rd1**
    - Retype Password: **Pa55w.rd1**
5. In the **Windows Security** dialog box, type **Pa55w.rd1** as the password, select **Remember my credentials**, and then click **OK**.
6. Verify that you are connected to Exchange Online, and then click **Finish**.
7. In the First things first dialog box, click **Ask me later**, and then click **Accept**.
8. On **LON-CL2**, repeat steps 1 through 4 by using the following information:
    - Your Name: **Francisco Chaves**

  - E-mail Address: **Francisco@AdatumAVXXXX.onmicrosoft.com**
  - Password: **Pa55w.rd**
  - Retype Password: **Pa55w.rd**

9. In the **Windows Security** dialog box, change the username to **Francisco@AVXXXXa.xtremelabs.us**, type **Pa55w.rd** as the password, select **Remember my credentials**, and then click **OK**.
10. Verify that you are connected to Exchange Online, and then click **Finish**.
11. In the First things first dialog box, click **Ask me later**, and then click **Accept**.

▶ Task 2: Verify that Skype for Business can connect to Office 365

1. On **LON-CL1**, start Skype for Business by clicking on **Start** button and typing **Skype**. In the Apps list click **Skype for Business 2016**.
2. Close the Welcome - Skype for Business dialog box.
3. On the **Skype for Business sign in** page, type **Holly@AdatumAVXXXX.onmicrosoft.com** as the **Sign-in address**, and then click **Sign in**.
4. On the **second Sign in** page, type **Pa55w.rd1** as the password, select **Save my password**, and click **Sign In**.
5. Click **Yes**. In the Help Make Skype for Business Better! dialog box, if it appears, click **No**. Verify that you are connected to Skype for Business Online.
6. On **LON-CL2**, repeat steps 1 through 5 by using the following information:
   - Sign-in address: **Francisco@AVXXXXa.xtremelabs.us**
   - Password: **Pa55w.rd**
7. Keep the virtual machines running for the next module.

Results: After completing this exercise, you should have verified:

- That Outlook 2016 can connect to Office 365.
- That Skype for Business can connect to Office 365.
- OneDrive for Business connectivity to Office 365

Module 4: Planning and configuring directory synchronization

Lab: Configuring directory synchronization

Exercise 1: Preparing for directory synchronization

▶ Task 1: Configure UPN

1. Sign in to the **LON-DC1** virtual machine as **ADATUM\Administrator** with a password of **Pa55w.rd**
2. On the Start screen, click **Administrative Tools**, and then double-click **Active Directory Domains and Trusts**.
3. In the **Active Directory Domains and Trusts** window, right-click **Active Directory Domains and Trusts**, and then click **Properties**.
4. Select the **UPN Suffixes** tab, in the **Alternative UPN suffixes:** box, type **AVXXXXa.xtremelabs.us**, and then click **Add**.
5. Click **OK**.
6. On the Start screen, right-click **Windows PowerShell**, and then click **Run as administrator**.
7. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-ADUser –Filter * -Properties SamAccountName | foreach { Set-ADUser $_ -
UserPrincipalName ($_.SamAccountName + “@AVXXXXa.xtremelabs.us” )}
```

▶ Task 2: Prepare problem user accounts

1. On the **LON-DC1**, in the Windows PowerShell prompt, type the following command, and then press Enter:

```
CD C:\labfiles\
```

2. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Set-ExecutionPolicy Unrestricted
```

3. To confirm the execution policy change, type **Y** and press Enter**.**
4. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
.\CreateProblemUsers.ps1
```

Note: Wait until the script has completed before proceeding to the next step.

5. This Windows PowerShell script will make the following changes in AD DS:
   - **Klemen Sic**. Add the "@" character to the beginning of "adatum" for the **UserPrincipalName** attribute.
   - **Lara Raisic**. Replace the existing string with "lara@adatum.com" for the **emailAddress** attribute.
   - **Logan Boyle**. Replace the existing string with “lara@adatum.com” for the **emailAddress** attribute.
   - **Holly Spencer**. Replace the existing string with “holly @adatum.com” for the **EmailAddress** attribute.

- **Maj Hojski**. Replace the existing string with " " for the **emailAddress** attribute.

▶ Task 3: Run the IdFix tool and fix identified issues

1. On **LON-CL1**, open **Microsoft Edge**, and then connect to **https://www.microsoft.com/en-us/download/details.aspx?id=36832**
2. On the **IdFix DirSync Error Remediation Tool** page, click **Download**, then click **Save**.
3. Wait for the download to complete, and then click **Open**.
4. In the File Explorer windows, browse to the **Downloads** folder, right-click **IdFix.zip**, and then click **Extract All...**
5. In the **Extract Compressed (Zipped) Folders** dialog box, in the destination box, type **C:\Deployment Tools\IdFix**, and then click **Extract**.
6. In File Explorer, in the **C:\Deployment Tools\IdFix** folder, right-click **IdFix**, and then click **Run as administrator**.
7. In the User Account Control dialog box, click **Yes**.
8. In the **IdFix Privacy Statement** message box, click **OK**.
9. Click **Query**. You should see several errors.
10. Click the **ERROR** column to sort the character errors to the top of the list.

Note: Ignore topleveldomain errors, which cannot be fixed by the IdFix tool.

11. In the **Klemen Sic** row, in the **ACTION** column, select **EDIT**.
12. In the **Holly Spencer** row, in the **ACTION** column, select **EDIT.**
13. In the **Maj Hojski** row, in the **ACTION** column, select **EDIT**
14. On the toolbar, click **Apply**.
15. In the **Apply Pending** dialog box, click **Yes**; note the **COMPLETE** status in the **ACTION** column indicating successful writes.
16. Switch to **File Explorer**, and in the **C:\Deployment Tools\IdFix** folder, double-click **Verbose <date> <time>.txt** to view the updated transactions in the transaction log.
17. Switch back to the IdFix tool.
18. On the toolbar, click **Query**.
19. Click in the **UPDATE** column to locate the **Logan Boyle** error, and replace the string with **logan@adatum.com**, and then in the **ACTION** column, select **EDIT**.
20. Click in the **UPDATE** column to locate the **Maj Hojski** error, and replace the string with **maj@adatum.com**, and then in the **ACTION** column, select **EDIT**.
21. On the toolbar, click **Apply**.
22. In the **Apply Pending** box, click **Yes**.
23. On the toolbar, click **Query** and verify that errors are corrected.

Note: Where there are format and duplicate errors for distinguished names, the UPDATE column either contains the same string as the VALUE column, or the UPDATE column entry is blank; in either case, this means that IdFix cannot suggest a remediation for the error.

You can either fix these errors outside IdFix, or manually remediate them within IdFix. You can also export the results and use Windows PowerShell to remediate a large number of errors.

▶ Task 4: Configure the Office 365 tenant for directory synchronization

1. On **LON-CL1**, on the desktop, double-click **Windows Azure Active Directory Module for Windows PowerShell**.
2. At the **Windows PowerShell** prompt, type the following command, and press Enter after each:

```
$msolcred = Get-Credential
```

3. In the **Windows PowerShell Credential** dialog box, enter **Holly@AdatumAVXXXX.onmicrosoft.com** in the **User name** box, enter **Pa55w.rd1** in the **Password** box, and then click **OK**.
4. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

```
Connect-MsolService -Credential $msolcred
```

5. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

```
Set-MsolDirSyncEnabled -EnableDirSync $true -Force
```

Note: The **-Force** switch disables the confirmation dialog box.

6. Although you might have to wait up to 24 hours for activation to complete, you should be able to continue.
7. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

```
(Get-MsolCompanyInformation).DirectorySynchronizationEnabled
```

8. The output returns “**True**” if sync is enabled.

Note: It might take a few minutes to return “True.” Rerun the command until you see “True” showing.

9. Switch to **Microsoft Edge**, and in the address box, type **https://portal.office.com**, and then press Enter.
10. On the **Sign-in** page, in the **Name** box, select **Holly@AdatumAVXXXX.onmicrosoft.com**. In the **Password** box, type **Pa55w.rd1**, and then click **Sign in**.
11. Navigate to the **Office 365 admin center**.
12. Click **Users**, then click **Active Users**. To the right of **Add a user**, click **More** (or if Active Directory synchronization has not yet completed, click **Set up**).
13. Click Directory synchronization, then click Go to the DirSync management link. verify that under **Integration with local Active Directory** the **Directory sync enabled** is **true**.

Results: After completing this exercise, you will have resolved issues in AD DS identified by the IdFix tool and you will have enabled Active Directory synchronization in Office 365.

Exercise 2: Configuring directory synchronization

▶ Task 1: Download and install Azure AD Connect

1. Sign in to the **LON-DS1** as **ADATUM\Administrator** with a password of **Pa55w.rd**. If the Networks pane appears, click **Yes**.
2. Start **Internet Explorer** from the taskbar.
3. If a **Windows Internet Explorer 10** dialog box appears, select **Use recommended security and compatibility settings**, and then click **OK**.
4. In the **Address** box, type **https://portal.office.com**, and then press Enter.
5. On the **Sign in** page, in the **Name** box, type **Holly@AdatumAVXXXX.onmicrosoft.com**.
6. In the **Password** box, type **Pa55w.rd1**, and then click **Sign in**.
7. Navigate to the Office 365 admin center**.**
8. In the left side menu, click **Users**, and then click **Active Users**.

Note: If you see the Active Directory synchronization is being activated warning, you can ignore it at this time, but you will not be able to run directory synchronization later in this exercise. You must wait until directory synchronization is activated. However, you can complete the following steps, even if you do see the warning message.

9. Click **Holly Spencer**.
10. On the **Holly Spencer** page, click **Edit** in the **User name / Email** section.
11. In the Aliases section, type **Holly** in the **Alias** textbox and ensure that **AVXXXXa.xtremelabs.us** domain is selected. Click **Add**.
12. Click **Set as primary** and then read the warning and click **Save**.
13. Click **Sign Out**.
14. Close Internet Explorer.
15. Open **Internet Explorer**.
16. If a **Windows Internet Explorer 10** dialog box appears, select **Use recommended security and compatibility settings**, and then click **OK**.
17. In the **Address** box, type **https://portal.office.com**, and then press Enter.
18. Sign in as **Holly@AVXXXXa.xtremelabs.us**, using the password **Pa55w.rd1**
19. In the Office365 admin center, in the left side menu, click **USERS**, and then click **Active Users**.
20. To the right of **Add a user**, click **More** (or if Active Directory synchronization has not yet completed, click **Set up**). Click **Directory synchronization**, then click **Go to the DirSync management** link
21. Next to **Directory Sync client version**, click **Upgrade to the latest version of Azure AD Connect**.

Note: You will automatically be redirected to the Microsoft Azure Active Directory Connect download page.

22. On the **Microsoft Azure Active Directory Connect** download page in Internet Explorer, click **Download**. If you get the message that your current security settings do not allow you to download file, open Internet options in the Internet Explorer and on **Security** tab click **Internet**, click **Custom level** and enable **File download** option.
23. In the Internet Explorer notification bar, click **Save as**, browse to **C:\Labfiles**, and then click **Save**. If the LabFiles folder does not exist, create it.
24. When the download has completed, in the Internet Explorer notification bar, click **Open folder**.
25. In **File Explorer**, right-click **AzureADConnect.msi**, and then click **Install**. Click **Run**.
26. In the **Microsoft Azure Active Directory Connect** wizard, on the **Welcome** page, click **I agree to the license terms and privacy notice**, and then click **Continue**.
27. On the **Express Settings** page, click **Customize**.
28. Leave the Microsoft Azure Active Directory Connect wizard open for the next task.

▶ Task 2: Run the Azure AD Connect tool with custom settings

1. On the **Install required components** page, leave all the checkboxes unchecked and click **Install**.
2. On the **User Sign-in** page, click **Password Synchronization**, and then click **Next**.
3. On the **Connect to Azure AD** page, enter the following credentials, and then click **Next**:
   - User name: **Holly@AVXXXXa.xtremelabs.us**
   - Password: **Pa55w.rd1**
4. On the **Connect your directories** page, click **Add Directory**, enter the following credentials, click **OK,** and then click **Next**:
   - User name: **ADATUM\Administrator**
   - Password: **Pa55w.rd**
5. On the **Azure AD sign-in configuration** page click **Next**.
6. On the **Domain and OU filtering** page, click **Sync selected domains and OUs**, expand **Adatum.com**, clear all check boxes for the child containers except for the **IT** checkbox, and then click **Next.**
7. On the **Uniquely identifying your users** page, click **Next**.
8. On the **Filter users and devices** page, verify that **Synchronize all users and devices** is selected, and then click **Next**.
9. On the **Optional Features** page, leave the default options, and then click **Next**.
10. On the **Ready to configure** page, review the features that will be installed. Ensure that **Start the synchronization process when configuration completes** is selected, and then click **Install.**

Note: The installation process will take approximately 10 minutes to complete.

11. Once the installation completes, on the **Configuration complete** page, click **Exit**.

12. On the Start screen, sign out of **LON-DS1**, and then sign back in as **Adatum\Administrator** with password **Pa55w.rd**

Note: Because Adatum\administrator was used to install Azure AD Connect, it will be automatically added to the ADSyncAdmins group, and you need to sign out for the Kerberos token to be updated. Otherwise, if you use a different user account to install Azure AD Connect, you will need to manually add the Azure AD Connect admin to the local ADSyncAdmins group on LON-DS1.

▶ Task 3: Configure synchronization service filtering for organizational units

1. On **LON-DS1**, click **Start**, open **Azure AD Connect** folder, and then click on **Synchronization Service.**
2. In **Synchronization Service Manager**, click the **Connectors** tab.
3. In the **Connectors** tab, double-click **Adatum.com**.
4. In the **Properties** dialog box, click **Configure Directory Partitions**.
5. Click **Containers**.
6. In the **Credentials** dialog box, enter the following credentials, and then click **OK**:
   - User name: **Administrator**
   - Password: **Pa55w.rd**
   - Domain: **Adatum.com**

Note: While this account is not the one used for directory synchronization, you use the account credentials temporarily to access AD DS for configuring filtering.

7. In the **Select Containers** dialog box, select the **Research** checkbox, verify that **IT** is selected, and then click **OK**.
8. Click **OK** to close the Properties dialog window.

▶ Task 4: Configure synchronization service filtering for object attribute

1. On **LON-DS1**, open the Start screen, open **Azure AD Connect** folder, and then click **Synchronization Rules Editor**.
2. In **Synchronization Rules Editor**, click **Add new rule**.
3. On the **Create inbound synchronization rule** dialog window, in the **Name** box, type **In from AD – User DoNotSyncFilter**
4. For **Connected System**, select **Adatum.com**.
5. For **Connected System Object Type**, select **user**.
6. For **Metaverse Object Type**, select **person**.
7. For **Link Type**, select **Join**.
8. For **Precedence**, type **50**.
9. Click **Next**.

10. In the **Create inbound synchronization rule** dialog box, on the **Scoping filter** tab, click **Add group**, and then click **Add clause**.
11. In **Add scoping filters**:
    - For **Attribute**, select **msDS-cloudExtensionAttribute15**.
    - For **Operator**, select **EQUAL**.
    - For **Value**, type **NoSync**,
12. Click **Next**.
13. On the **Add join rules**, click **Next**.
14. On the **Add transformations** page, click **Add transformation**.
15. For **FlowType**, select **Constant**.
16. For **Target Attribute**, select **cloudFiltered**.
17. In the **Source** text box, type **True**.
18. To save the rule, click **Add**, and then close Synchronization Rules Editor window.
19. Open Windows PowerShell from the Start menu. In Windows PowerShell, type the following command, and then press Enter. The initial synchronization can take several minutes to complete. Leave the Windows PowerShell window open.

    ```
    Start-ADSyncSyncCycle –PolicyType Initial
    ```

▶ Task 5: Verify that synchronization was successful

1. Ensure that you are signed in to the **LON-DS1** as **ADATUM\Administrator** with a password of **Pa55w.rd**
2. Open Internet Explorer, and then browse to **http://aka.ms/siqtee**
3. After **AdministrationConfig-en.msi** finishes downloading, click **Run**.
4. In the **Microsoft Azure Active Directory Module for Windows PowerShell Setup Wizard**, on the **Welcome** page, click **Next**.
5. On the **License Terms** page, click **I accept the terms in the License Terms**, and then click **Next**.
6. On the **Install Location** page, click **Next**.
7. On the **Ready to Install** page, click **Install**.
8. On the **Completing the Microsoft Azure Active Directory Module for Windows PowerShell Setup** page, click **Finish**.
9. On the Start screen, open **Azure AD Connect folder**, and then click **Synchronization Service**.
10. In **Synchronization Service Manager** on **LON-DS1**, click **Operations**.
11. In the **Connector Operations** list, click the line at the top of the list, and then review the **Start Time**, **End Time**, and the **Status**.
12. Verify the connector has a **Start Time** and **End Time** that aligns with the last time synchronization was initiated in the previous task.
13. On the taskbar, right-click **Windows PowerShell**, and then select **Run as Administrator**.

14. At the Windows PowerShell prompt, type the following commands, and then press Enter after each one:

```
Import-Module MSOnline
Connect-MsolService
```

15. In the **Enter Credentials** dialog box, enter the following credentials, and then click **OK**:

    - User name: **Holly@AVXXXXa.xtremelabs.us**
    - Password: **Pa55w.rd1**

16. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-MsolCompanyInformation | fl LastDirSyncTime
```

17. Verify the **LastDirSyncTime** aligns with the last time synchronization was initiated in the previous task.
18. On the Start screen, open **Internet Explorer**, and then type **https://portal.office.com/admin/default.aspx** in the address bar.
19. On the **Sign-in** page, sign in by using the following credentials:
20. User name: **Holly@AVXXXXa.xtremelabs.us**
21. Password: **Pa55w.rd1**
22. In the admin center, in left navigation, click **USERS**, and then click **Active Users**.
23. Verify that the **Last synced less than an hour ago** message appears.
24. In the Active users list, note that your on-premises accounts from the selected OUs now have a status of Synced with Active Directory.

Results: After completing this exercise, you will have installed Azure AD Connect with customized settings. Upon completion of the installation, you will start directory synchronization to Office 365 and have verified that synchronization was successful.

Exercise 3: Managing Active Directory users and groups

▶ Task 1: Create a new user and group account

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, expand **Adatum.com**, right-click **Research**, click **New**, and then click **User**.
3. In the **First name** box, type **Perry**.
4. In the **Last name** box, type **Brill**.
5. In the **User logon name** box, type **Perry**, select your lab domain **UPN** (not **Adatum.com**), and then click **Next**.
6. In the **Password** and **Confirm password** boxes, type **Pa55w.rd**, clear the **User must change password at next logon** checkbox, select the **Password never expires** checkbox, click **Next**, and then click **Finish**.
7. In the **Research** OU user list, double-click the **Perry Brill** user.
8. In the **Properties** dialog box, in the **E-mail** box, type **Perry@AVXXXXa.xtremelabs.us**, and then click **OK**.

9. In the console tree, right-click the **Research** OU, click **New**, and then click **Group**.
10. In the New Object – Group window, in the **Group name:** box, type **Project Team**, click **Universal**, click **Distribution**, and then click **OK**.
11. In the **Research** OU, double-click the **Project Team** group.
12. In the **Properties** dialog window, in the **E-mail** box, type **projectteam@AVXXXXa.xtremelabs.us**.
13. On the **Members** tab, click **Add**.
14. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter the object names to select**, type the following names, and then click **Check Names**:
    - **Arturs Priede**
    - **August Towle**
    - **Cai Chu**
15. Click **OK** twice.

▶ Task 2: Move a user out of the scope of synchronization

1. On **LON-DS1**, at the **Windows PowerShell** prompt, type the following command, and then press Enter:

```
Get-MsolUser -Search Vera
```

2. Verify that the user **Vera Pace** is listed in Office 365.
3. On **LON-DC1**, in Active Directory Users and Computers, move **Vera Pace** from the **Research** OU to the **Sales** OU, by right-clicking **Vera Pace** in the **Research** OU user list, and then clicking **Move** and selecting **Sales** OU. Click **OK.**

▶ Task 3: Move a user into the scope of synchronization

1. On **LON-DC1**, ensure that the **Active Directory Users and Computers** is opened.
2. In the console tree, if needed expand **Adatum.com**, and then click **Marketing**.
3. Right-click **Ada Russell**, and click **Move**.
4. In the **Move** dialog box, expand **Adatum.com**, click **Research**, and then click **OK**.

▶ Task 4: Change group membership

1. In the console tree of **Active Directory Users and Computers**, click **Research**.
2. In the right pane, double-click **Research**.
3. In the **Research Properties** dialog box, click the **Members** tab.
4. Select the following three users, and then click **Remove**. In the confirmation dialog box, click **Yes**.
    - **Claire Roberson**
    - **Connie Vaughn**
    - **Esther Wiggins**
5. Click **OK**.

▶ Task 5: Force synchronization

1. On **LON-DS1**, from the taskbar, right-click the **Windows PowerShell** shortcut, and then click **Run as administrator**.

Note: If a **User Account Control** dialog box appears, click **Yes**.

2. At the Windows PowerShell prompt, type the following, and then press Enter:

```
Start-ADSyncSyncCycle –PolicyType Delta
```

Note: The **Delta** switch is used here so that only the updates are synchronized.

3. Wait until synchronization has completed before proceeding to the next task.

▶ Task 6: Validate the results of directory synchronization

1. To verify the new user you created, on **LON-CL1**, open the **Office 365 Admin Center** in **Microsoft Edge** by typing **https://portal.office.com/admin/default.aspx** in the address bar.
2. Sign in using the following credentials:
3. User name: **Holly@AVXXXXa.xtremelabs.us**
4. Password: **Pa55w.rd1**
5. If you are connected to the previous Office 365 admin center, click that banner at the top of the page to connect to the new Office 365 admin center.
6. In the **Office 365 Admin Center**, in the left navigation, click **Users**, and then click **Active Users**.
7. In the Active Users list, verify that **Perry Brill** has a value of **Synced with Active Directory** in the Sync Type column.

Note: You might need to wait up to 10 minutes before the account appears. Refresh the list until you see Perry Brill's account.

8. In the **Active Users** list, click the **Perry Brill**.
9. Under Product licenses section, click **Edit**.
10. On the **Product licenses** page, in the **Location** drop-down menu, select **United Kingdom**, and then click on the icon next to **Office 365 Enterprise E5**.
11. Click **Save**, and then click **Close** twice.
12. Repeat the steps 8-11 to assign Office 365 license for user **Ada Russell**.
13. To verify that you have created the new group, in **Office 365 admin center**, in the left navigation, click **Groups**, and then click **Groups**.
14. In the **Groups** list, verify that the **Project Team** appears.

Note: You might need to wait up to 10 minutes before the group appears. Refresh the list until you see the object.

15. In the **Groups** list, select the **Project Team** group.

Note: In the right pane, notice that **Edit Members** is unavailable. This is because group membership is maintained by Active Directory. To view the membership, you need to use Windows PowerShell.

16. On **LON-DS1**, in Windows PowerShell, type the following command, and then press Enter:

    ```
    Get-MsolGroup
    ```

17. Verify that you see **Research** and **Project Team** groups. Copy the ObjectID value for these two groups.
18. To verify that you updated the group membership in AD DS, type the following command at the Windows PowerShell prompt, and then press Enter:

    ```
    Get-MsolGroupMember –GroupObjectId <ObjectID for Research group>
    ```

19. Verify the membership of the group does not contain the users removed in AD DS. The users who were removed from the group are:
    - **Claire Roberson**
    - **Connie Vaughn**
    - **Esther Wiggins**
20. To verify that you have moved the user, **Vera Pace**, out of the scope of synchronization, type the following command at the Windows PowerShell prompt, and then press Enter:

    ```
    Get-MsolUser –Search Vera
    ```

21. At the Windows PowerShell prompt, type the following command, and then press Enter:

    ```
    Get-MsolAccountSku
    ```

Note: The number of **ConsumedUnits** is now less than before.

22. Leave the virtual machines running for the next lab.

Results: After completing this exercise, you will have identified how managing user and group accounts has changed with directory synchronization.

Module 5: Planning and deploying Office 365 ProPlus

Lab: Managing Office 365 ProPlus installations

Exercise 1: Preparing an Office 365 ProPlus managed installation

▶ Task 1: Download the Office 365 deployment tool

1. On **LON-CL1**, on the taskbar, click **File Explorer**.
2. In **File Explorer**, click **Local Disk (C:)** in the left navigation pane
3. In **File Explorer**, click the **Home** tab, and then click **New Folder**.
4. Type **Office16**, and then press Enter.
5. In **File Explorer**, right-click **Office16**, click **Share with**, and then click **Specific people**.
6. In the **File Sharing** dialog box, click the drop-down list box, select **Everyone** from the list, click **Add**, and then click **Share**.
7. In the **File Sharing** dialog box, click **Done**.
8. From the taskbar, open the **Microsoft Edge** browser.
9. In the address bar, type **https://portal.office.com**, and then press Enter.
10. Sign in as **Holly@AVXXXXa.xtremelabs.us**, with the password **Pa55w.rd1**
11. On the **Office 365** home page, click **Admin**.
12. In the **Office 365 admin center**, under **Office Software**, click **Software download settings**, and then click **Manually deploy user software**.
13. Under the Manually deploy user software area, click **Learn how to download and deploy software**.
14. In the Manually download and install the Office apps by using the Office Deployment Tool section, click the **Microsoft Download Center** link to open the Office Deployment Tool download page.
15. On the download page, expand Details, System Requirements, and Install Instructions.
16. Read and familiarize yourself with each section. You can mark this page as a favorite to refer to later.
17. Click **Download** and notice the information bar at the bottom of the browser.
18. Click **Save,** then once the download is completed, click **Run**.
19. In the User Account Control dialog box, click **Yes**.
20. Accept the license agreement and click **Continue**.
21. Browse to the **Office16** folder on This PC’s C: drive.
22. Click **OK**. You should see that the files were extracted successfully. Click **OK**.
23. Navigate to the **Office16** folder with File Explorer. You should see two files in the newly created Office Deployment Tool folder named **configuration** and **setup.**

▶ Task 2: Modify an Office 365 ProPlus installation

1. In this step, you will back up the Office 16 **configuration.xml** file and then open it so that you can edit it in the next step. To do this, perform the following steps:

a. In File Explorer, double-click **C:\Office16**.

b. Right-click **configuration.xml**, and click **Copy**. Right click again and click **Paste**.

c. Right-click the **configuration.xml** file, click **Open with**, and then click **Notepad**.

2. In Notepad, edit the first Add line after **<Configuration>** to read **<Add SourcePath=”\\LON-CL1\Office16\” OfficeClientEdition=”32” Branch=”Current”>**.

3. In **Notepad**, remove all the remaining comment codes (lines that start with **<!--** and end with **-->**).

4. Comment out Microsoft Visio with the **<!-- -->** code to make the download quicker, by replacing this code:

```
</Product>
<Product ID="VisioProRetail">
<Language ID="en-us" />
</Product>
```

   with this code:

```
</Product>

<!--
<Product ID="VisioProRetail">
<Language ID="en-us" />
</Product>

-->
```

5. Save the file as **AdatumConfiguration.xml**.

6. Switch to File Explorer (you should still be in the Office16 folder), press Shift, right-click any white space below the file list, and then click **Open command window here**.

7. At the command prompt, type the following command, and then press Enter:

```
Setup /?
```

8. Note the Office Deployment Tool command-line options.

9. At the command prompt, type the following command, and then press Enter:

```
setup.exe /download \\LON-CL1\Office16\AdatumConfiguration.xml
```

10. In the **User Account Control** window, click **Yes**.

11. The download will take several minutes to complete.

12. Switch to **File Explorer**, and verify that the download has started in the Office16 folder. You can continue with the next task and leave the download in the background.

Results: You will have downloaded a copy of the Microsoft Office 365 ProPlus install for managed deployment to a shared folder. You will also download and install the Office Deployment Tool on the same machine.

Exercise 2: Managing user-driven Office 365 ProPlus installations

▶ Task 1: Managing user rights to install Office 365 ProPlus

1. On **LON-CL1**, if required, sign in to Office365 admin center as **Holly@AVXXXXa.xtremelabs.us** with the password of **Pa55w.rd1**
2. Connect to the new **Office 365 admin center**.
3. On the **Office 365** home page, click **Admin**.
4. In the Office 365 admin center, click **Users**.
5. Select **Abbi Skinner**, and then next to **Product licenses**, click **Edit**.
6. Under Set user location, select **United Kingdom**, and then enable **Office 365 Enterprise E5**.
7. Set the **Office 365 ProPlus** option to **Off**, click **Save**, and then click **Close** twice.
8. In the **Office 365 admin center**, under Active users, click **Beth Burke**.
9. Beside Product licenses, click **Edit**.
10. Under Location, select **United Kingdom**, and then enable **Office 365 Enterprise E5**.
11. Verify that **Beth** has permission to use all features.
12. Click **Save**, and then click **Close** twice.
13. Repeat steps 8 through 12 for **Cai Chu**.
14. In the **Office 365 admin center**, click the **Home** icon.
15. Click **Software download settings**.
16. In the **Software for PC** section, under **2016 version**, turn off all options.
17. Click **Save**, and then **Close**.
18. On the **Admin** page, click **Holly Spencer**'s profile photo icon in the top right of the screen, and then click **Sign Out**.
19. On the Sign in page, at **https://portal.office.com**, sign in as **Abbi@AVXXXXa.xtremelabs.us**, using the password **Pa55w.rd**
20. On the **Default Landing** page, click the small Gear icon in the top- right corner, and then click the **Office 365** option.
21. On the **Office 365 settings** page, click **Software**.

Note: Because this user is not licensed for Office 365 ProPlus, Office 2016 is not available for download.

22. Close and reopen **Microsoft Edge** and connect to **https://portal.office.com**
23. On the Sign in page, in the Name box, type **Beth@AVXXXXa.xtremelabs.us**.
24. In the **Password** box, type **Pa55w.rd**, and then click **Sign in**.
25. On the default landing page, click the small Gear icon in the top-right corner, and then click **Office 365**.
26. On the **Settings** page, click **Software.**

Note: This user has a license, but Skype for Business 2016 and Office 2016 are not available for download because Holly disabled Office download. Skype for Business 2015 is available since it has not been disabled.

27. Click **Phone & tablet**. Verify that **Phone and tablet** apps are available.
28. Close **Microsoft Edge**.
29. Open **Microsoft Edge**.
30. In the address bar, type **https://portal.office.com**, and then press Enter.
31. Sign in as **Holly@AVXXXXa.xtremelabs.us**.
32. Click **Admin** on the **Office 365** home page.
33. In the **Office 365 admin center**, click **Home**.
34. Click **Software download settings**.
35. Next to the 2016 version, set the value to **On**. Verify that Office and Skype for Business are both set to on, and click **Save**.
36. Click **Close**.
37. In **Microsoft Edge**, on the **User Software** page, click **Holly Spencer's** profile photo icon, and then click **Sign out**.

Note: Instead of signing out your admin user every time, you can click the Microsoft Edge browser ellipse menu (…) at the top right of the browser and open a New InPrivate window. This will allow you to have two sessions at a time open

38. Switch to **LON-CL3**. Verify that you are signed in as **Beth**.
39. Open **Microsoft Edge**.
40. In the **address bar**, type **https://portal.office.com**, and then press Enter.
41. On the Sign in page, in the Name box, type **Beth@AVXXXXa.xtremelabs.us**.
42. In the **Password** box, type **Pa55w.rd**, and then click **Sign in**.
43. On the **Office 365** home page, click the small Gear icon in the top-right corner, and then click **Office 365**.
44. On the **Settings** page, click **Software**.

Note: This user has a license, and Office 2016 is now available for download.

45. Verify that **Office** and **Skype for Business** desktop software are available to install.
46. Do not install, but notice that this user can now install the 32-bit version of Office 365 ProPlus and select which language they want to install. They must click **Advanced** to turn on the 64-bit version option.
47. Note also that **Phone and tablet** apps are available from the left menu.
48. Leave this page open and continue to the next lab to perform the user-driven installation.

▶ Task 2: Installing Office 365 ProPlus from the Office 365 portal

1. On **LON-CL3**, if needed, open **Microsoft Edge** and sign into **Office 365** portal at **portal.office.com**, with the username **Beth@AVXXXXa.xtremelabs.us**, click **Office365 Settings** in upper right corner and then click **Software**.
2. In the Language section, select the language to install from the drop-down menu.
3. Leave 32-bit (recommended) selected.
4. Click **Install**.
5. In the **Microsoft Edge** notification bar, click **Save**, and then click **Run**.
6. If the **User Account Control** dialog box appears, type **Adatum\Holly** in the user name box, in the **Password** box, type **Pa55w.rd**, and then click **Yes**.
7. On the taskbar, click the **Office** icon, and note the status of the download.

Note: It will take several minutes to complete, but applications are now available.

8. Click **Close** when the wizard finishes.
9. Go to the **Start** screen.
10. On the **Start** screen, click **Word 2016**. On the first things first window click **Accept**.
11. In the top-right corner, if no one is signed in, sign in as **Beth@AVXXXXa.xtremelabs.us**, with the password **Pa55w.rd**, by clicking the link **Sign in to get most out of office**.
12. Once signed in, your subscription license is activated. At the top right, under **Beth Burke**, click **Switch account**.
13. Click **SIGN OUT**, and then click **Sign out** next to **Beth's** name.
14. Click **Yes** in the **Remove Account** dialog box.
15. At the top right, click **Sign in to get the most out of Office**.
16. On the Sign in page, in the E-mail address box, type **Holly@AVXXXXa.xtremelabs.us**, and then click Next.
17. On the **Sign in** page, in the **Password** box, type **Pa55w.rd1**, and then click **Sign in**.
18. Click **Blank document**.
19. Type some text.
20. Click **File**, then click **Save**.
21. Click **Sites – A. Datum** and click **A. Datum** in the right pane.
22. Double-click the **Documents** folder and then save the file with the name **Meeting Agenda**.
23. Click **Save**. You might see a **streaming features** message.
24. Close **Word**.
25. Switch back to **Beth Burke's** Office 365 session in Microsoft Edge.
26. In the top-right corner, click the **Settings** icon, and then click **Office 365 settings**.
27. On the Office 365 settings page, click Software.

28. Note that you now have a new section at the top of the page where you can manage Office 365 installs.
29. Click **Tools & Add-ins**.

▶ Task 3: Managing office licenses

1. On **LON-CL3**, sign out of **Beth's** account on the **Office 365** page.
2. Sign back in as **Holly Spencer** with the username **Holly@AVXXXXa.xtremelabs.us**.
3. In the **Password** box, type **Pa55w.rd1**, and then click **Sign in**.
4. On the **Office 365** home page, click **Admin**.
5. In the Office 365 admin center, click Users, and then click **Beth Burke**.
6. In the right pane, under **Product licenses**, click **Edit**.
7. Under **Office 365 Enterprise E5**, set the **Office 365 ProPlus** option to **Off** to remove the license from **Beth's** account, click **Save**, and then click **Close** twice.
8. In **Microsoft Edge**, at the top right, click the Profile photo icon for **Holly Spencer**, and then click **Sign out**.
9. On the Sign in page, type **Beth@AVXXXXa.xtremelabs.us**.
10. In the **Password** box, type **Pa55w.rd**, and then click **Sign in**.
11. In the top-right corner, click the **Settings** icon, and then click **Office 365**.
12. On the **Settings** page, click **Software**.
13. Note that the Office installation is no longer listed, as this user no longer has an active license (although software is available).

Note: The Office 365 ProPlus applications will still be available to Beth on any machine on which she already installed them, but within 30 days, they will drop into low-functionality mode. This means she will only be able to read and print documents.

▶ Task 4: Reactivating Office 365 ProPlus

1. Sign out of the **Office 365** page, and sign back in as **Holly@AVXXXXa.xtremelabs.us**.
2. In the **Password** box, type **Pa55w.rd1**, and then click **Sign in**.
3. On the **Office 365 home page**, click the **Admin** tile.
4. In the **Office 365 admin center**, click Users, and then click **Beth Burke**.
5. In the right pane, under **Product licenses**, click **Edit**.
6. Under **Office 365 Enterprise E5**, set the **Office 365 ProPlus** option to **On**, click **Save**, and then click **Close** twice.
7. Close **Microsoft Edge**.

Results: When completed, you should be able to activate Office 365 ProPlus for self-service installations. You should also be able to set licensing options correctly for end users so that deployment and installation is possible.

Exercise 3: Managing centralized Office 365 ProPlus installations

▶ Task 1: Configure a Group Policy Object (GPO) to distribute the custom installation

1. Switch to **LON-DC1** and connect as **Adatum\administrator**, with the password **Pa55w.rd**
2. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, right-click **Adatum.com**, point to **New**, and then click **Organizational Unit**.
4. Type **Adatum_Computers**, and then click **OK**.
5. In the console tree, under **Adatum.com**, click **Computers**.
6. Right-click **LON-CL4**, click **Move**, click **Adatum_Computers**, and then click **OK**.
7. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
8. In the Group Policy Management window, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Adatum_Computers**.
9. Right-click **Adatum_Computers**, and then click **Create a GPO in this domain, and Link it here**.
10. In the **New GPO** dialog box, in the **Name** box, type **DeployO365**, and then click **OK**.
11. In **Group Policy Management**, click **Adatum_Computers**, and in the right pane, right-click **DeployO365**, and then click **Edit**. If you see a Group Policy Management Console window, click **OK**.
12. In Group Policy Management Editor, expand **Computer Configuration, Policies, Windows Settings**, and then double-click **Scripts (Startup/Shutdown)**.
13. Double-click **Startup**, and then click **Show Files**.
14. In **File Explorer**, click **Home**, click **New item**, click **Text Document**, and then press Enter to accept the default name.
15. Double-click **New Text Document.txt**.
16. In **Notepad**, add the following line:

    ```
    \\LON-CL1\Office16\setup.exe /configure \\LON-CL1\Office16\AdatumConfiguration.xml
    ```

17. Save the file as **DeployO365.cmd**. Ensure that in **Save as type**, you select **All Files** and that the file extension is **.CMD**.
18. Click **Save**.
19. Close **Notepad**.
20. Delete New Text Document.
21. Switch back to the Group Policy Management Editor, Startup Properties dialog box.
22. Click **Add**.
23. In the **Add a Script** dialog box, click **Browse**.
24. In the **Browse** dialog box, select **DeployO365.cmd**, and then click **Open**.
25. In the **Add a Script** dialog box, click **OK**.
26. In the **Startup Properties** dialog box, click **OK**.
27. Close **Group Policy Management Editor**.

Note: You could also deploy this script by using Microsoft Intune, Microsoft System Center Configuration Manager, or other electronic software distribution.

▶ Task 2: Verifying the installation

1. Switch to **LON-CL4**, and if necessary, sign in as **Adatum\Beth**, with the password, **Pa55w.rd**
2. Right-click the **Start** button, and click **Command Prompt (Admin)**.
3. In the **User Account Control** dialog box, type **Adatum\Holly** as the user name and **Pa55w.rd** as the password, and click **Yes**.
4. Type **gpupdate /force** and press Enter.
5. Wait for the Group Policy to update for both the computer and user and then close the command prompt.
6. Restart the computer.

Note: If any updates have downloaded, click **Update**, and then restart.

7. Wait five minutes after **LON-CL4** has restarted before continuing. This is to allow the **Group Policy** settings to take effect on **LON-CL4**.
8. Sign in as **ADATUM\Beth** with the password **Pa55w.rd**. You may have to wait for Office to finish installing.
9. Navigate to the **Start** screen, and note that **Office 2016** is installed. You might have to wait up to 15 minutes before you see any available Office applications.
10. Click **Word 2016**. If you do not see it on the **Start** screen, type **Word** to bring up the icon.
11. On the **Activate Office** page, in the **E-mail address** box, type **Beth@AVXXXXa.xtremelabs.us**, and then click **Next**.
12. On the **Sign in** page, in the **Password** box, type **Pa55w.rd**, and then click **Sign in**. Click **OK** on the notification window.
13. In the **First things first** dialog box, click **Accept**.
14. Close the **Welcome to your new Office** dialog box.
15. In the templates list, click **Blank document**.
16. Type some text.
17. Click **File**, and then click **Save**.
18. Click **Browse** in **This PC – Documents**.
19. In **File name**, enter **Meeting Report**, and then click **Save**.
20. Right-click the taskbar and then click **Task Manager**.
21. In Task Manager, click **More details**.
22. On the **Processes** tab, under **Background processes**, notice that **Microsoft Office Click-to-Run** appears.
23. Click the **Details** tab, and notice **officeclicktorun.exe** in the task list.
24. Click the **Services** tab, and notice that the **ClickToRunSvc** service is running.

Note: Check **Task Manager** for your deployment. These items will all be present in a successful install.

25. Close Task Manager.

26. Close **Word 2016**.

Results: You will have enabled centralized managed deployment of Office 365 ProPlus and implemented a standardized Microsoft Office configuration by using one version of Office.

Module 6: Planning and managing Exchange Online recipients and permissions

Lab: Managing Exchange Online recipients and permissions

Exercise 1: Configuring Exchange Online recipients

▶ Task 1: Create user mailboxes

1. On **LON-CL1**, open **Microsoft Edge**.
2. In the address bar, type **https://portal.office.com/**, and then press Enter.
3. Sign in as **Holly@AVXXXXa.xtremelabs.us** , with the password **Pa55w.rd1**
4. On the Office 365 home page, click **Admin**.
5. In the **Office 365 admin center**, click **Users** and then click **Active Users**.
6. Above the list of users, click **Add a user**.
7. On the **New user** page, enter the following information:
   - First name: **Martina**
   - Last name: **Blair**
   - Display name: **Martina Blair**
   - User name: **Martina**
   - Domain: **AVXXXXa.xtremelabs.us**
   - Location: **United Kingdom**
8. Expand the **Password** area, select the following options, and then click **Add**:
   - Select **Let me create the password** , and then type the following password: **Pa55w.rd**
   - Make this user change their password when they first sign in: **Not selected**
   - Roles: **User (no administrator access)**
   - Product licenses: **Office 365 Enterprise E5**
9. On the **User was added** page, click **Send email and close**.
10. Repeat steps 6 to 9 to add the following additional users:
    - **Matt Villagomez** (since **Matt@AVXXXXa.xtremelabs.us** is in use, use the username **MattV**)
    - **Olivia Emerson**
    - **Kendra Sexton**
11. In the Office 365 admin center, on the **Admin centers** menu, click **Exchange**.
12. In the Exchange admin center, click **recipients**.

Note: It might take a few minutes for the mailboxes to appear. Click the refresh icon periodically until they do.

▶ Task 2: Connect to Exchange Online with Windows PowerShell

1. On the desktop, right-click **Windows Azure Active Directory Module for Windows PowerShell**, and then click **Run as administrator**.
2. At the **User Account Control** prompt, click **Yes**.

Note: You can copy and paste these commands into the virtual machine.

3. In the Windows PowerShell window, type the following command, and then press Enter:

```
$credential = Get-Credential
```

4. In the **Enter Credentials** dialog box, in the **User name** box, type **Holly@AVXXXXa.xtremelabs.us**
5. In the **Password** box, type **Pa55w.rd1**, and then click **OK**.
6. In the Windows PowerShell window, type the following command, and then press Enter:

```
Connect-MsolService –Credential $credential
```

7. In the Windows PowerShell window, type the following command, and then press Enter:

```
$exchangeSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
"https://outlook.office365.com/powershell-liveid/" -Credential $credential -
Authentication "Basic" -AllowRedirection
```

8. In the Windows PowerShell window, type the following command, and then press Enter:

```
Import-PSSession $exchangeSession -DisableNameChecking
```

9. In the Windows PowerShell window, type the following command, and then press Enter:

```
Get-AcceptedDomain
```

Note: This command returns the list of accepted domains and verifies that you can connect to your Office 365 subscription.

▶ Task 3: Create groups and assign members

1. In the Windows PowerShell window, type the following command, and then press Enter to create the **IT** distribution group with **Olivia** as a member:

```
New-DistributionGroup -Name IT -Members Olivia
```

2. Repeat step 1 to add the following additional groups and members:
   - **Managers**
     - Members: **Martina**

  - **Development**
    - Members: **MattV**
  - **Sales**
    - Members: **Kendra**

▶ Task 4: Create resource mailboxes

1. In **Microsoft Edge**, in the **Exchange Admin center**, in **recipients**, click **resources**.
2. In the Windows PowerShell window, type the following command, and then press Enter:

```
New-Mailbox -Name "Conference Room" -Room
```

3. In the Windows PowerShell window, type the following command, and then press Enter:

```
Set-CalendarProcessing "Conference Room" -AutomateProcessing AutoAccept
```

4. In the Windows PowerShell window, type the following command, and then press Enter:

```
New-Mailbox -Name "Demonstration Laptop” –Equipment
```

5. In the Windows PowerShell window, type the following command, and then press Enter:

```
Set-CalendarProcessing "Demonstration Laptop” -AutomateProcessing AutoAccept
```

Note: If you receive an error running the **Set-CalendarProcessing** cmdlet for either of these objects, wait a few moments and repeat.

6. Switch to **Microsoft Edge**, and in the **Exchange Admin center**, click **Refresh**. You should be able to see both resources.
7. In the Windows PowerShell window, type the following command, and then press Enter:

```
Set-Mailbox “Conference Room” –ResourceCapacity “25”
```

8. Switch to **Microsoft Edge**, and in the **Exchange Admin center**, click **Conference Room**. You should be able to see the Capacity you configured in the details pane on the right. If not, click **Refresh**.

▶ Task 5: Configure additional Exchange Online recipients

1. On **LON-CL1**, browse to **C:\Labfiles**, and the open **ExternalContacts.csv**.
2. Review the file contents, and then close **Excel**.
3. In **Microsoft Edge**, in the **Exchange admin center**, click **contacts**.
4. Switch to **Windows PowerShell**.
5. In the Windows PowerShell window, type the following command, and then press Enter:

```
CD C:\Labfiles
```

Note: You can copy and paste these commands into the virtual machine.

6. In the Windows PowerShell window, type the following command, and then press Enter:

```
Import-Csv .\ExternalContacts.csv | ForEach-Object {New-MailContact -Name $_.Name -
DisplayName $_.Name -ExternalEmailAddress $_.ExternalEmailAddress -FirstName
$_.FirstName -LastName $_.LastName}
```

7. In the Windows PowerShell window, type the following command, and then press Enter:

```
$contacts = Import-CSV .\ExternalContacts.csv
```

8. In the Windows PowerShell window, type the following command, and then press Enter:

```
$contacts | ForEach {Set-Contact $_.Name -StreetAddress $_.StreetAddress -City $_.City
-StateorProvince $_.StateorProvince -PostalCode $_.PostalCode -Phone $_.Phone -
MobilePhone $_.MobilePhone -Pager $_.Pager -HomePhone $_.HomePhone -Company $_.Company
-Title $_.Title -OtherTelephone $_.OtherTelephone -Department $_.Department -Fax $_.Fax
-Initials $_.Initials -Notes $_.Notes -Office $_.Office -Manager $_.Manager}
```

9. In **Microsoft Edge**, in the **Exchange Admin center**, in **contacts**, click **Refresh**. You can see the newly created objects.

Results: After completing this exercise, you will have created and configured Microsoft Exchange Online recipients.

Exercise 2: Configuring role-based access control

▶ Task 1: Assign users to built-in role groups

1. In the **Exchange admin center**, click **permissions**.
2. On the **admin roles** tab, click **Organization Management**, and then click **Edit**.
3. In the Role Group window, under **Members**, click the **+** icon.
4. In the Select Members window, click **Olivia**, click **add**, and then click **OK**.
5. In the Role Group window, click **Save**.

▶ Task 2: Create a new admin role and assign a user to it

1. Switch to **Windows PowerShell**.

Note:
If possible, use the paste functionality provided by XtremeLabs to copy and paste these commands
into the virtual machine.

2. In the Windows PowerShell window, type the following commands, and then press Enter after each command:

```
Enable-OrganizationCustomization

New-RoleGroup -Name BranchOfficeAdmins -roles “Mail Recipients”, “Distribution Groups”,
“Move Mailboxes”, “Mail Recipient Creation”
```

3. In the Windows PowerShell window, type the following command, and then press Enter:

```
Add-RoleGroupMember "BranchOfficeAdmins" -Member Martina
```

4. In the Windows PowerShell window, type the following command, and then press Enter:

```
Get-RoleGroupMember "BranchOfficeAdmins"
```

5. Switch to **Microsoft Edge**, and then in the **Exchange admin center**, click **Refresh**. Ensure that you can see the new BranchOffice Admins role group.

▶ Task 3: Create a new role assignment policy

1. In **Microsoft Edge**, in the **Exchange Admin center**, click **user roles**.
2. Switch to **Windows PowerShell**.

Note: If possible, use the paste functionality provided by the hosting server to copy and paste these commands into the virtual machine.

3. In the Windows PowerShell window, type the following command, and then press Enter:

```
New-RoleAssignmentPolicy "Limited Mailbox Configuration" -Roles
MyBaseOptions,MyAddressInformation,MyDisplayName
```

4. To change the default role assignment policy for new mailboxes, in the Windows PowerShell window, type the following command, and then press Enter:

```
Set-RoleAssignmentPolicy "Limited Mailbox Configuration" -IsDefault
```

5. When prompted, type **Y**, and then press Enter.
6. In the **Exchange admin center**, click **Refresh**. You can see the new role assignment policy.

▶ Task 4: Prepare for the next module

- When you have finished the lab, leave all of the virtual machines running.

Results: After completing this exercise, you will have configured delegated administration of your Exchange Online organization.

Module 7: Planning and configuring Exchange Online services

Lab A: Configuring message transport in Exchange Online

Exercise 1: Configuring message-transport settings

▶ Task 1: Connect to Exchange Online in Windows PowerShell

1. On **LON-CL1**, on the desktop, double-click **Windows Azure Active Directory Module for Windows PowerShell**.

Note: You might have a Windows PowerShell connection to Office 365 open from a previous lab. If so, you can use the existing connection and skip this task.

2. In **Windows PowerShell**, type **$cred=Get-Credential**, and then press Enter.
3. In the Windows PowerShell credential request window, in the **User name** box, type **Holly@AVXXXXa.xtremelabs.us**
4. In the **Password** box, type **Pa55w.rd1**, and then click **OK**
5. In Windows PowerShell, type the following command, and then press Enter:

```
$Session=New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $cred -Authentication
Basic –AllowRedirection
```

6. Type the following command, and then press Enter:

```
Import-PSSession $Session
```

▶ Task 2: Create a custom send and receive connector to enforce TLS

1. On the taskbar, click **Microsoft Edge**.
2. In **Microsoft Edge**, in the **search** box, type **https://login.microsoftonline.com**, and press Enter.
3. At the login page, sign in as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**.
4. To open the **Office 365 admin center**, click **Admin**.
5. In the **Office 365 admin center**, on menu on the left, in **Admin centers**, click **Exchange**.
6. In the **Exchange admin center**, click **mail flow**, and then click **connectors**.
7. Click **New**.
8. On the **Select your mail flow scenario** page, in the **From** box, select **Office 365**.
9. In the **To** box, select **Partner organization**, and then click **Next**.
10. On the **New connector** page, in the **Name** box, type **Humongous Insurance Outgoing**, and then click **Next**.
11. Click **Only when email messages are sent to these domains**, and then click **Add**.

12. On the **add domain** page, type **humongousinsurance.com**, click **OK**, and then click **Next**.
13. Click **Use the MX record associated with the partner's domain**, and then click **Next**.
14. Select the **Always use Transport Layer Security (TLS) to secure the connection** check box, click **Issued by a trusted certificate authority (CA)**, and then click **Next.**
15. On the **Confirm your settings** page, click **Next**.
16. On the **Validate this connector** page, click **Add**.
17. In the **Send the test email to the address** box, type **postmaster@humongousinsurance.com**, click **OK**, and then click **Validate**.
18. Wait while validation completes, and then click **Close**.
19. On the **Validation Result** page, click **Save**.
20. In the Warning window, click **Yes**.

Note: Validation of mail flow will fail because the connector is to a fictitious organization. This is expected behavior for this lab.

21. In the **Exchange admin center**, on the **connectors** tab, click **New**.
22. On the **Select your mail flow scenario** page, in the **From** box, select **Partner organization**.
23. In the **To** box, select **Office 365**, and then click **Next**.
24. On the **New connector** page, in the **Name** box, type **Humongous Insurance Incoming**, and then click **Next**.
25. Click **Use the sender's domain**, and then click **Next**.
26. Click **Add**, type **humongousinsurance.com**, click **OK**, and then click **Next.**
27. Select the **Reject email messages if they aren't sent over TLS** check box, and then click **Next**.
28. On the **Confirm your settings** page, click **Save**.

▶ Task 3: Create transport rules

1. On **LON-CL1**, in the Exchange admin center page, click **rules**.
2. Click **New**, and then click **Apply disclaimers**.
3. In the new rule window, in the **Name** box, type **A. Datum Disclaimer**.
4. In the **Apply this rule if** box, select **The recipient is located**, click **Outside the organization**, and then click **OK**.
5. Click **Enter text**.
6. In the specify disclaimer text window, type **<HR> If you are not the intended recipient of this message, you must delete it**, and then click **OK**.
7. Click **Select one**.
8. In the specify fallback action window, select **Wrap**, and then click **OK**.
9. In the new rule window, click **Save**.

10. If the Warning window appears, click **Yes**.
11. In **Exchange admin center**, click **New**, and then click **Send messages to a moderator**.
12. In the new rule window, in the **Name** box, type **Moderate Managers**.
13. In the **Apply the rule if** box, select **The recipient is a member of**, in the Select Members window, click **Managers**, click **add**, and then click **OK**.
14. In the **Do the following** box, select **Forward the message for approval to**, click **Holly Spencer**, click **add**, and then click **OK**.
15. In the new rule window, click **Save**.
16. On **LON-CL2**, on the taskbar, click **Microsoft Edge**.
17. In **Microsoft Edge**, in the **search** box, type **https://login.microsoftonline.com**, and then press Enter.
18. Sign in as **Francisco@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
19. In Office 365, click **Mail**.
20. In the Mail window, click **New**.
21. In the **To** field, type **alias@outlook.com**, where **alias@outlook.com** is the Microsoft account that you configured at the beginning of this course.
22. In the **Subject** field, type **Disclaimer Test**.
23. In the message body, type **This message will have a disclaimer**, and then click **Send**.
24. Sign in to **Outlook.com**, and then verify that the message has the disclaimer **If you are not the intended recipient of this message, you must delete it** added at the end of the message body. If the message is not in the Inbox, check the Junk folder.
25. In the Mail window in which you are signed is as **Francisco**, click **New**.
26. In the **To** field, type **Martina**.
27. In the **Subject** field, type **Moderation Test**.
28. In the message body, type **This message requires approval by Holly**, and then click **Send**.
29. On **LON-CL1**, click **Start**, type **Outlook**, and then click **Outlook 2016**.
30. Type **Holly@AVXXXXa.xtremelabs.us** and **Pa55w.rd1** in the Windows Security dialog box.
31. In **Outlook**, read the approval request, and then click **Approve**.
32. Close **Outlook 2016**.

▶ Task 4: Create a journal rule for members of the research department

1. On **LON-CL1**, in the **Exchange admin center**, click **compliance management**, click **journal rules**, and then click **Select address**.
2. In the non-delivery reports window, click **Browse**, click **Holly Spencer**, click **OK**, and then click **Save**.
3. In the Warning window, click **OK**.
4. Click **New**.
5. In the new journal rule window, in the **Send journal reports to** box, type **journal@humongousinsurance.com**.

6. In the **Name** box, type **Development Messages**.
7. In the **If the message is sent to or received from** box, select **A specific user or group**, click **Development**, click **add**, and then click **OK**.
8. In the **Journal the following messages** box, select **All messages**, and then click **Save**.

▶ Task 5: Track internal and external message delivery

1. On **LON-CL1**, in the **Exchange admin center**, click **mail flow**, and then click **message trace**.
2. Review the available search options, and then click **search**.
3. In the Message Trace results window, double-click the message sent to **alias@outlook.com**.
4. Review the information in the message, including the message events that show that the disclaimer was applied.
5. Click **Close**.
6. Double-click the message sent from **Francisco** to **Martina**.
7. Review the information in the message, including that the message was sent for moderation.
8. Click **Close**.
9. In the Message Trace Results window, click **Close**.

Results: After completing the exercise, you will have configured message-transport settings.

Lab B: Configuring email protection and client policies

Exercise 1: Configuring email protection

▶ Task 1: Configure the malware filter

1. On **LON-CL1**, in the **Exchange admin center**, click **protection**, and then click **malware filter**.
2. Click **Default**, and then click **Edit**.
3. In the Default window, click **settings**.
4. Under Notifications, select the **Notify internal senders** check box.
5. Select the **Notify administrator about undelivered messages from internal senders** check box.
6. In the **Administrator email address** box, type **Holly@AVXXXXa.xtremelabs.us**
7. Select the **Notify administrator about undelivered messages from external senders** check box.
8. In the **Administrator email address** box, type **Holly@AVXXXXa.xtremelabs.us**, and then click **Save**.

▶ Task 2: Configure the connection filter

1. On **LON-CL1**, in the **Exchange admin center**, click **connection filter**.
2. Click **Default**, and then click **Edit**.
3. In the Default window, click **connection filtering**.

4. Under **IP Block list**, click **Add**.
5. In the add blocked IP address window, type **192.168.0.0/24**, and then click **OK**.
6. Select the **Enable safe list** check box, and then click **Save**.

▶ Task 3: Configure the spam filter

1. On **LON-CL1**, in the **Exchange admin center**, click **spam filter**.
2. Click **Default**, and then click **Edit**.
3. In the Default window, click **spam and bulk actions**.
4. In the **High confidence spam** box, select **Quarantine message**, and then click **Save**.
5. Click **Add**.
6. In the new spam filter policy window, in the **Name** box, type **Sales spam policy**.
7. In the **Spam** box, select **Prepend subject line with text**.
8. In the **High confidence spam** box, select **Move message to Junk Email folder**.
9. In the **Prepend subject line with this text** box, type **Junk:**.
10. Scroll to the bottom of the window, and under **Applied To**, in the **If** box, select **The recipient is a member of**, click **Sales**, click **add**, and then click **OK**.
11. Click **Save**.

▶ Task 4: Test the spam-filter settings (optional)

1. Sign in to your **alias@outlook.com** account.
2. Create a new message to send to **kendra@AVXXXXa.xtremelabs.us**
3. In the body of the message, include the text **XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X**, and then send the message.
4. Create a new message to send to **francisco@AVXXXXa.xtremelabs.us**
5. In the body of the message, include the text **XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X**, and then send the message.
6. On **LON-CL1**, in the **Exchange admin center**, click **protection**, and then click **quarantine**.
7. Verify that the message sent to **Francisco** is in quarantine, but the message sent to **Kendra** is not.
8. Click the message sent to **Francisco**, click **Release Message**, and then click **Release selected message(s) to ALL recipients**.
9. In the Warning window, click **Yes**.
10. When processing is complete, click **Close**.
11. On **LON-CL2**, in Outlook on the web, verify that the message was delivered.

▶ Task 5: Enable Advanced Threat Protection

1. Switch to **LON-CL1** computer.
2. In **Exchange admin center**, click **advanced threats**, and then click **safe attachments**.
3. Click **New**.

4. In the **new safe attachments** window, in the **Name** box, type **Sales policy**.
5. Under **Safe attachments unknown malware response**, click **Replace - Block the attachments with detected malware, continue to deliver the message**.
6. Below **Applied To** in the **If** box, select **The recipient is a member of**.
7. In the **Select Members** window, click **Sales**, click **add**, and then click **OK**.
8. In the **new safe attachments policy** window, click **Save**.
9. In the **Warning** window, click **OK**.

Results: After completing this exercise, you should have configured anti-spam and antivirus settings.

Exercise 2: Configuring client access policies

▶ Task 1: Configure an Outlook Web App policy

1. On **LON-CL1**, in the **Exchange admin center**, click **permissions**, and then click **Outlook Web App policies**.
2. Click **New**.
3. In the new Outlook Web App mailbox policy window, in the **Policy name** box, type **Limited features**.
4. Clear the following check boxes:
   - **Instant messaging**
   - **Text messaging**
   - **Unified messaging**
   - **LinkedIn contact sync**
   - **Journaling**
5. Under **Private computer or OWA for devices**, clear the **Direct file access** check box, and then click **Save**.
6. Click **recipients**, click **mailboxes,** click **Kendra Sexton**, and then click **Edit**.
7. In the **Kendra Sexton** window, click **mailbox features**.
8. Under **Email Connectivity**, click **View details**.
9. In the Outlook Web App mailbox policy window, click **Browse**, click **Limited features**, click **OK**, and then click **Save**.
10. In the **Kendra Sexton** window, click **Save**.
11. On **LON-CL1**, click **Start**, type **Outlook** and then click **Outlook 2016**. If prompted, type **Holly@AVXXXXa.xtremelabs.us** and **Pa55w.rd1** in the Windows Security dialog box.
12. Click **New Email**.
13. In the new email window, in the **To** box, type **Kendra@AVXXXXa.xtremelabs.us** and then click **Check Names**.
14. In the **Subject** box, type **Attachment Test**.
15. In the ribbon, click **Attach File**, and then click **Browse This PC**.

16. In the Insert File window, browse to **C:\Windows\Logs\DISM**, click **dism**, and then click **Insert**.
17. Click **Send**.
18. On **LON-CL2**, in Outlook on the web, sign out, and then sign in again as **Kendra@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
19. On the Outlook page, select your time zone and click **Save**.
20. Read the new Attachment Test message.
21. Click the message attachment.
22. Click **OK** to close the message, indicating that you do not have permission to download files.

Note: In some cases, it may take a few minutes for the new Outlook Web App mailbox policy to take effect.

▶ Task 2: Configure mobile-device access

1. On **LON-CL1**, in the **Exchange admin center**, click **mobile**, and then click **mobile device access**.
2. Click **edit**.
3. In the Exchange ActiveSync access settings window, click **Quarantine – Let me decide to block or allow later**.
4. Under **Quarantine Notification Email Messages**, click **Add**, click **Holly Spencer**, click **add**, and then click **OK**.
5. In the Exchange ActiveSync access settings window, click **Save**.

▶ Task 3: Configure a mailbox policy for mobile devices

1. On **LON-CL1**, in the **Exchange admin center**, on the **mobile** menu, click **mobile device mailbox policies**.
2. Click **Default (default)**, and then click **Edit**.
3. In the Default window, click **security**, and then select the **Require a password** check box.
4. Select the **Allow simple passwords** check box**.**
5. Select the **Minimum password length** check box, enter a value of **4**, and then click **Save**.

▶ Task 4: Validate mobile-device management policies (optional)

1. On your mobile device, add a new ActiveSync account for **Francisco Chaves**.
2. If Autodiscover does not detect the server name, enter **outlook.office365.com**.
3. Your device will be placed into quarantine, and you must approve the device before you can send and receive messages.
4. After you configure the Exchange ActiveSync account, the security settings from the mobile-device mailbox policy will apply, and you may be prompted to create a password on your device.
5. When you finish your testing, you can delete the account from your mobile device.
6. Leave the virtual machines running for the next lab.

Results: After completing this exercise, you should have configured client access policies.

Module 8: Planning and deploying Skype for Business Online

Lab: Configuring Skype for Business Online

Exercise 1: Configuring Skype for Business Online organization settings

▶ Task 1: Download and install the Skype for Business Online module for Windows PowerShell

1. On **LON-CL1**, open **Microsoft Edge**, and then connect to **http://go.microsoft.com/fwlink/?LinkId=294688**

2. On the **Skype for Business Online, Windows PowerShell Module** page, click **Download**, click **Save**, and then click **Run**.

3. Select **I agree to the license terms and conditions**, and then click **Install**.

4. If a **User Account Control** dialog box appears, click **Yes**.

5. Click **Restart** and wait for **LON-CL1** to restart.

6. Sign in as **Adatum\Holly** by using the password **Pa55w.rd**

7. After the installation completes, in the **Skype for Business Online, Windows PowerShell Module** dialog, click **Close**.

8. Close the **Microsoft Edge** window if it opens.

▶ Task 2: Enable Skype Meeting Broadcast for the organization

1. On **LON-CL1**, in the search box on the taskbar, type **PowerShell**.
2. In the search results, right-click **Windows PowerShell**, and then click **Run as administrator**.
3. In the **User Account Control** dialog box, click **Yes**.
4. At the command prompt, type the following command, and then press Enter:

```
$cred = Get-Credential
```

5. In the **credentials** dialog box, enter the user name **Holly@AVXXXXa.xtremelabs.us** and the password **Pa55w.rd1**, and then click **OK**.
6. Type the following command, and then press Enter:

```
$SfBSession = New-CSOnlineSession –Credential $cred
```

7. Type **Y** and press Enter.
8. Type the following command, and then press Enter:

```
Import-PSSession $SfBSession
```

9. Type the following command, and then press Enter:

```
Set-CsBroadcastMeetingConfiguration –EnableBroadcastMeeting $True
```

10. Type the following command, and then press Enter:

    ```
    Get-CsBroadcastMeetingConfiguration
    ```

11. Verify that the **EnableBroadcastMeeting** parameter is set to **True**.

▶ Task 3: Configure the organization settings for Skype for Business Online

1. On **LON-CL1**, in the Windows PowerShell command-line interface window, type the following command to enable privacy mode, and then press Enter:

    ```
    Set-CSPrivacyConfiguration -EnablePrivacyMode $True
    ```

    Note the warning that you receive about enabling client version checking.

2. To disable push notifications for Apple devices, type the following command, and then press Enter:

    ```
    Set-CSPushNotificationConfiguration -EnableApplePushNotification $False
    ```

3. To verify the privacy notification settings, type the following command, and then press Enter:

    ```
    Get-CSPrivacyConfiguration
    ```

    You should see the following output:

    - Identity: **Global**
    - EnablePrivacyMode: **True**
    - AutoInitiateContacts: **True**
    - PublishLocationDataDefault: **True**
    - DisplayPublishedPhotoDefault: **True**

4. To verify the push notification settings, type the following command, and then press Enter:

    ```
    Get-CSPushNotificationConfiguration
    ```

5. To allow users to communicate with public Skype users, type the following command, and then press Enter:

    ```
    Set-CsTenantFederationConfiguration –AllowPublicUsers $True
    ```

6. To allow users to communicate with federated partners, type the following command, and then press Enter:

    ```
    Set-CsTenantFederationConfiguration –AllowFederatedUsers $True
    ```

7. To enable communication with all federated partners except for litware.com, type the following commands, and then press Enter after each command:

    ```
    $AllDomains = New-CsEdgeAllowAllKnownDomains

    $BlockedDomain = New-CsEdgeDomainPattern -Domain "litware.com"

    Set-CsTenantFederationConfiguration -AllowedDomains $AllDomains –BlockedDomains
    $BlockedDomain

    Get-CsTenantFederationConfiguration
    ```

8. Open **Microsoft Edge**, and then connect to **https://portal.office.com**
9. If needed, sign in as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
10. On the **Office 365** home page, click the **Admin** tile.
11. In the **Microsoft Office 365 admin center**, in the menu to the left, click **Admin centers**, and then click **Skype for Business**.
12. On the left-hand side, click **organization**.
13. On the **general** page, under presence privacy mode, verify that the setting is configured as **Display presence information only to a user's contacts**.
14. Under mobile phone notifications, verify that **Apple Push Notification Service** is not enabled, and then click **external communications**.
15. Under external access, verify that **On except for blocked domains** is selected.
16. Verify that under blocked or allowed domains, **litware.com** is listed.

▶ Task 4: Configure the meeting invitation settings

1. On **LON-CL1**, in the **Skype for Business admin center**, click **online meetings** and then click **meeting invitation**.
2. In the **Help URL** text box, type **http://help.adatum.com**
3. In the **Footer text** text box, type **Sample legal disclaimer**. Click **save**.
4. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-CsMeetingConfiguration
```

5. Verify that the **Help URL** and **CustomFooterText** display the correct information.
6. In Windows PowerShell, type the following command, Press Enter, and then close Windows PowerShell

```
Remove-PSSession $SfbSession
```

▶ Task 5: Validate the meeting invitation settings

1. On **LON-CL1**, click **Start**, type **Skype**, and then open **Skype for Business 2016**.
2. In the Skype for Business window, click **Change**. In the **Sign-in address** box, type **Holly@AVXXXXa.xtremelabs.us** and then click **OK**.
3. Type **Pa55w.rd1** for password and then click **Sign in**. Click **Yes**.
4. Open **Microsoft Outlook 2016**.
5. On the ribbon, click **New Items**, click **Meeting**, and then click **Skype Meeting**.
6. In the **To** text box, type **Ada**.
7. Create a meeting request for some time tomorrow using a subject of **Test Meeting**.
8. Send the meeting request.
9. Open the **calendar**, and then double-click the meeting that you just created. Verify that the meeting contains the custom footer text and that the help link references **http://help.adatum.com**

Results: After completing this exercise, you should have configured Skype for Business Online service settings.

Exercise 2: Configuring Skype for Business Online user settings

▶ Task 1: Configure Skype for Business user settings

1. On **LON-CL1**, navigate to the Office 365 admin center.
2. On the menu to the left, click **Users**, and then click **Active users**. Select **Christie Thomas**, and then click **Edit** in the Product licenses section.
3. Turn off **Skype for Business Online (Plan 2)**, **Phone System** and **Audio Conferencing**. Click **Save**, and then click **Close** twice.
4. On the menu to the left, select **Admin centers**, and then click **Skype for Business**.
5. On the menu to the left, click **Users**.
6. Verify that **Christie Thomas** is not listed as a Skype for Business user. You may need to refresh the window.
7. Select **Ada Russell**, and then click **Edit**.
8. On the **general** tab, under Audio and video, clear **Record conversations and meetings**.
9. On the menu to the left, click **external communications**, clear **External Skype users**, and then click **save**.
10. Click the **back** icon, select **Francisco Chaves**, and then click **Edit**.
11. On the **general** tab, under Audio and video, select **Audio only** from the drop-down list box. Click **save**.
12. Close **Microsoft Edge**.

▶ Task 2: Verify Skype for Business communications

1. On **LON-CL4**, ensure that you are signed in as **Ada**. Open **Outlook 2016**.
2. On the Welcome to Outlook 2016 page, click **Next**.
3. On the Add an Email Account page, click **Next**. If the Office installation wizard launches, wait for the installation to finish, and then continue.
4. On the Auto Account Setup page, fill in the following information, and then click **Next**:
   a. Your Name: **Ada Russell**
   b. E-mail address: **Ada@AVXXXXa.xtremelabs.us**
   c. Password: **Pa55w.rd**
   d. Retype Password: **Pa55w.rd**
5. In the Microsoft Outlook dialog box, type **Pa55w.rd** as the password, select **Remember my credentials**, and click **OK**.
6. Clear **Set up Outlook Mobile on my phone,** and click **Finish**.
7. Open **Skype for Business 2016**.
8. Click **Skip for now**.
9. Sign in as **Ada@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
10. Save the sign-in information. In the Help Make Skype for Business Better! dialog box, click **No**.

11. On **LON-CL1**, ensure that you are signed in as **Holly**, and verify that **Outlook 2016** and **Skype for Business 2016** are open.
12. In **Outook 2016**, create a Skype meeting request for a meeting that will start within the next 15 minutes, and then send the request to **Ada Russell**.
13. In **Skype for Business**, in the **Find someone** text box, type **Ada**.
14. Double-click **Ada Russell** to open an IM window.
15. Type a message, and then press Enter.
16. On **LON-CL4**, verify that the IM from **Holly** is received and respond to it.
17. In **Outlook 2016**, accept **Holly's** meeting request.
18. Open the meeting, and then click **Join Skype Meeting**.
19. Click **Don't join audio**, and then click **OK**.
20. Verify that **Ada** is connected to the meeting.
21. On **LON-CL1**, open the meeting request, click **Join Skype Meeting**, and then click **Don't join audio**, and click **OK**.
22. Verify that **Holly** is connected to the meeting.
23. On **LON-CL1**, in the meeting window, click the **Present** icon, and then click **Present Desktop**.
24. In the Present Desktop window, click **Present**.
25. In the Skype for Business window, click **OK**.
26. On **LON-CL4**, verify that **Holly's** desktop is visible in the meeting window.
27. On **LON-CL4**, disconnect from the meeting.
28. On **LON-CL1**, disconnect from the meeting.

Results: After completing this exercise, you should have configured Skype for Business Online user settings and validated Skype for Business Online functionality.

Exercise 3: Configuring a Skype Meeting Broadcast

▶ Task 1: Configure a Skype Meeting Broadcast

1. On **LON-CL1**, open a new tab in the Microsoft Edge browser.
2. Connect to **https://broadcast.skype.com**, and then, if needed, sign in as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
3. In the Skype Meeting Broadcast window, click **New Meeting**.
4. In the Meeting details window, fill in the following information:
    - Meeting title: **Test broadcast meeting**
    - Meeting time: **Today's date**
    - Start time: **Within the next 15 minutes**
    - Duration: **1 hour**

   - Members: **Beth Burke**
   - Access: **Invitation only**
   - Attendees: **Ada Russell**

5. Scroll back to the top of the window, and then click **Create**.
6. In the Skype Meeting Broadcast window, click **Create Outlook invitation**, **Save**, and then click **Open**.
7. If the **How do you want to open this file**? window appears, ensure that **Outlook 2016** is selected, and click **OK**.
8. In the Test broadcast meeting -Meeting window, click **Send Update**.

▶ Task 2: Validate the Skype Meeting Broadcast configuration

1. On **LON-CL3**, ensure that you are signed in as **Beth**. Open **Outlook 2016**.
2. On the Welcome to Outlook 2016 page, click **Next**.
3. On the Add an Email Account page, click **Next**.
4. On the Auto Account Setup page, fill in the following information, and then click **Next**:
   a. Your Name: **Beth Burke**
   b. E-mail address: **Beth@AVXXXXa.xtremelabs.us**
   c. Password: **Pa55w.rd**
   d. Retype Password: **Pa55w.rd**
5. In the Microsoft Outlook dialog box, type **Pa55w.rd** as the password, select **Remember my credentials**, and click **OK**.
6. Click **Finish**.
7. Open **Skype for Business 2016**.
8. Click **Skip for now**.
9. Sign in as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
10. Save the sign-in information. In the Help Make Skype for Business Better! dialog box, click **No**.
11. Open **PowerPoint 2016**. Select the option to create a blank presentation.
12. Type a title for the presentation, and then save the presentation to the Documents folder using the name **Presentation.pptx**.
13. Close **PowerPoint 2016**.
14. In **Outlook**, click the broadcast meeting request from **Holly Spencer**, click **Accept**.
15. In the Reminders pop-up window, double-click the meeting request from **Holly**.
16. Click **Join the Meeting**.
17. In the Skype for Business window, sign in as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**, and then click **Join the event**.
18. In the **Did you mean to switch apps?** window, click **Yes**.
19. In the Join Meeting Audio dialog box, click **Don’t join audio** and click **OK**.

20. Ignore the warning about setting up an audio device.
21. In the Meeting window, click **Share Content**, and then click **Share PowerPoint Files**.
22. Browse to the **Documents** folder, click **Presentation.pptx**, and then click **Open**.
23. In the right side of the meeting window, click **Content only**, and then click **Start Broadcast**.
24. Click **Start Broadcast** again. Wait for the broadcast to start.

Note: Due to current platform limitations, the broadcast will not be able to be started. Please continue onto the next Module.

25. On **LON-CL4**, signed in as **Ada**, in **Outlook 2016**, accept the meeting request from **Holly**.
26. Open the meeting request, and then click **Join the Meeting**.
27. In the Skype for Business window, sign in as **Ada@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**, and then click **Join the event**.
28. On **LON-CL3**, in the broadcast window, click **Stop Broadcast**, and then click **Stop Broadcast** again.
29. On both **LON-CL1** and **LON-CL4**, disconnect from the meeting.
30. Keep the virtual machines running for the next lab.

Results: After completing this exercise, you should have configured a broadcast meeting and verified that users can join the meeting.

Module 9: Planning and configuring SharePoint Online

Lab: Configuring SharePoint Online

Exercise 1: Configuring SharePoint Online settings

▶ Task 1: Configure settings

1. Ensure you are signed in to the **LON-CL1** virtual machine as **Holly** with the password of **Pa55w.rd**
2. In **LON-CL1**, click the desktop, on the taskbar, click **Microsoft Edge**, and then browse to **https://portal.office.com**
3. Sign in as **Holly@AVXXXXa.xtremelabs.us** with the password of **Pa55w.rd1**
4. In the **Office 365 admin center**, click **Admin centers**, and then click **SharePoint**.
5. On the leftmost side, click **settings**.
6. Under **Site Collection Storage Management**, click **Automatic**.
7. Scroll down to **Enterprise Social Collaboration**.
8. Select **Use Yammer.com service**.
9. Click **OK**.
10. On the leftmost side, click **sharing**.
11. Verify that **Allow sharing to authenticated external users and using anonymous access links** is selected, and then click **OK**.

▶ Task 2: Configure user profiles

1. On the leftmost side, click **user profiles**.
2. Under **people**, click **Manage User Profiles**.
3. In the **Find profiles** dialog box, type **Ada**, and then click **Find**.
4. In the result window, click **Ada**.
5. Click the arrow next to **Ada,** then click **edit my profile**, and in the **Manager** box, type **Holly**.
6. Click the **check names** field and verify that the field displays **Holly Spencer**.
7. In the right corner, click **Save and Close**.
8. On the left side, click **user profiles**.
9. Under **My Site settings**, click **Setup My Sites**.
10. Scroll down to **My Site Cleanup**.
11. In the **secondary owner** list, type **Holly**, and then click the **Check names** icon.
12. Scroll down, and then click **OK**.

▶ Task 3: Configure apps

1. On the leftmost side, click **apps**, and then click **Configure Store Settings**.

2. In the **Apps for Office from the Store window**, click **No** to disable apps from starting when documents are opened in the browser.

3. Click **OK**, and then close the browser.

Results: After completing this exercise, you should have configured SharePoint Online service settings.

Exercise 2: Creating and configuring SharePoint Online site collections

▶ Task 1: Create a site collection using the SharePoint admin center

1. Open **Microsoft Edge** and sign in to **https://portal.office.com** with the user name **Holly@AVXXXXa.xtremelabs.us**, and the password of **Pa55w.rd1**

2. In the Office 365 admin center, on the left side menu, click **Admin centers**, and then click **SharePoint**.

3. In the leftmost side, click **Site collections**.

4. On the Site Collections ribbon, click **New**, and then click **Private Site Collection**.

5. In the **new site collection** dialog box, in the **Title** dialog box, type **marketing**, in the **Web Site Address** empty text box, type **marketing**, and then in the **administrator** list, type **Holly** and then click the **Check Names** icon. Leave the other settings as suggested. To confirm, click **OK**.

Note: SharePoint Online provisions the new **marketing** site. This process can take a few minutes.

6. After marketing is created, select the **https://AdatumAVXXXX.sharepoint.com/sites/marketing** check box.

Note: It can take a few minutes until the **Sharing** menu on the ribbon is active. You can speed this up by refreshing the page by pressing the F5 key.

7. When the **marketing** site is selected, on the ribbon, click **Sharing**.

8. In the Sharing dialog box, select **Allow sharing with all external users, and by using anonymous access links**, and then click **Save**.

Note: The site settings changes to allow external user sharing. This process is usually done within one minute. Now, external user sharing is enabled and you can use it for this marketing site.

▶ Task 2: Create a site collection using Windows PowerShell

1. To install the **SharePoint Online Management Shell**, you must first download it from the **Microsoft Download Center**. To do so, open a new Microsoft Edge tab and browse to **http://aka.ms/f04q5o**

2. On the **SharePoint Online Management Shell download** page, in the **Select Language** drop-down box, select your appropriate language, and then click **Download**.

3. On the **Choose the download you want** page, select the check box for the 64-bit version. Click **Next**.

4. If a message about pop-ups appears, click **Allow once**.

5. In the Internet Explorer dialog box asking whether you want to run or save the file, click **Save** and then click **Run**.

6. On the **SharePoint Online Management Shell Setup** page, select the **I accept the terms in the License Agreement** check box, and then click **Install**.

7. If a **User Account Control** dialog box appears, click **Yes**.

8. When the installation completes, click **Finish**.

9. Click **Start**, type **sharep**, and right-click **SharePoint Online Management Shell**, and then click **Run as administrator**.

10. In the **User Account Control** dialog box, click **Yes**.

11. At the command prompt, type the following command, and then press Enter (where **AVXXXX** is your unique Adatum domain name):

    ```
    Connect-SPOService –Url https://AdatumAVXXXX-admin.sharepoint.com –credential
    holly@AVXXXXa.xtremelabs.us
    ```

12. In the **Enter your credentials** dialog box, in the **Password** box, type **Pa55w.rd1**, and then click **OK**.

13. At the command prompt, type the following command, and then press Enter:

    ```
    New-SPOSite -Url https://AdatumAVXXXX.sharepoint.com/sites/AcctsProj -Owner
    holly@AVXXXXa.xtremelabs.us -StorageQuota 500 -NoWait -Template PROJECTSITE#0 –Title
    “Accounts Project”
    ```

14. Close the Windows PowerShell window.

▶ Task 3: Configure permissions on the site collections

1. In **LON-CL1**, open **Microsoft Edge**, in the top-right corner, click the ellipsis, and then click **New InPrivate Window**.

2. Browse to **https://portal.office.com**

3. Sign in as **Holly@AVXXXXa.xtremelabs.us**, with the password of **Pa55w.rd1**

4. In the Office 365 admin center, click **Admin**, and then click **SharePoint**.

5. On the leftmost side, click **Site collections**.

6. Select the **https://AdatumAVXXXX.sharepoint.com/sites/marketing** check box.

7. On the ribbon, click **owners**, and then click **Manage Administrators**.

8. In the **Site Collection Administrators** text box, type **Ada**, click the **Check Names** icon, and then click **OK**.

9. Open another InPrivate window, browse to **https://AdatumAVXXXX.sharepoint.com/sites/marketing**, and sign in as **Ada@AVXXXXa.xtremelabs.us**, with the password of **Pa55w.rd**

10. On the upper-right corner, click the **Settings** icon (the wheel icon), and then navigate to **site settings**.

11. Under Users and Permissions, click **Site collection administrators** to open it.

12. Verify that **Ada Russell** appears.

13. Close the Microsoft Edge window.

▶ Task 4: Verify access to the site collections

1. In **LON-CL1**, open **Microsoft Edge**.
2. Browse to **https://AdatumAVXXXX.sharepoint.com/sites/marketing**
3. Sign in as **Beth@AVXXXXa.xtremelabs.us**, with the password of **Pa55w.rd**

Note: You need permission to access this site, and you need to send an access request for permission to view the site.

4. In the **You need permission to access this site** dialog box, type **Please enable Beth's access to this site**, and then click **Request Access**.
5. Close **Microsoft Edge**, and then reopen it.
6. Browse to **https://AdatumAVXXXX.sharepoint.com/sites/marketing**
7. Sign in as **Holly@AVXXXXa.xtremelabs.us** with the password of **Pa55w.rd1**
8. In the top-right corner, click the **Settings** icon (the wheel icon), and then click **Site settings**.
9. Under **User and Permissions**, click **Site permissions**.
10. Click **Show access requests and invitations**.
11. Verify that **Beth's** request is listed, and click **Approve**.
12. Click **Site Settings**, and then click **Site permissions**.
13. Click **marketing Members**.
14. Verify that **Beth's** account is listed.
15. Click **New**, and then click **Add Users**.
16. In the text box at the top, type **Perry**, and then click **Perry Brill**.
17. Click **Share**.
18. Close **Microsoft Edge**.
19. Open **Microsoft Edge** and connect to **https://AdatumAVXXXX.sharepoint.com/sites/marketing**
20. Sign in as **Beth@AVXXXXa.xtremelabs.us**, with the password of **Pa55w.rd**
21. Verify that you can access the site.
22. Close **Microsoft Edge**, and then reopen it.
23. Browse to **https://AdatumAVXXXX.sharepoint.com/sites/marketing**
24. Sign in as **Perry@AVXXXXa.xtremelabs.us**, with the password of **Pa55w.rd**
25. Verify that you can access the site.
26. Close **Microsoft Edge**.

Results: After completing this exercise, you should have created and configured SharePoint Online site collections.

Exercise 3: Configuring and verifying external user sharing

▶ Task 1: Configure global settings for external user sharing

1. In **LON-CL1**, open **Microsoft Edge**.
2. Browse to **https://portal.office.com**
3. Sign in as **Holly@AVXXXXa.xtremelabs.us**, with the password of **Pa55w.rd1**
4. In the **Office 365 admin center**, click **Admin**, and then click **SharePoint**.
5. On the leftmost side, click **sharing**.
6. Click **Allow sharing to authenticated external users and anonymous access links,** and then click **OK**.

▶ Task 2: Configure a site collection for external user sharing

1. In **Microsoft Edge**, click **Site Collections**.
2. Select the **https://AdatumAVXXXX.sharepoint.com/sites/AcctsProj** check box.
3. On the ribbon, in the **Manage** section, click **Sharing**.
4. In the **Sharing** dialog box, click **Allow sharing with all external users, and by using anonymous access links**.
5. Click **Save**.
6. Wait for the operation to complete, which might take about 5 minutes.
7. Close **Microsoft Edge**.
8. Open **Microsoft Edge** and browse to **https://AdatumAVXXXX.sharepoint.com/sites/AcctsProj**
9. Sign in as **Holly@AVXXXXa.xtremelabs.us** with the password of **Pa55w.rd1**
10. In the top-right corner, click **SHARE**.
11. In the **Share 'Accounts Project'** dialog box, type in the email address of the Microsoft account you used to set up Office 365.
12. In the text box, type **You can now access this shared site on Adatum Publishing**.
13. Click **Share**.
14. Browse to **https://AdatumAVXXXX.sharepoint.com/sites/marketing**
15. In the left navigation pane, click **Documents**. Click **next** until completion of the **Welcome to the new list experience**
16. Click **New**, and then click **Word document**.
17. In the Word Online window, type some text, and then wait to check if **Saved** appears in the document title, and then click the **marketing** link.
18. In the document list, click the ellipsis button (**…**) next to the document you created, and then click **Share**.
19. Click **Get a link**, and then select **Edit link – no sign-in required**.
20. Select the link, right-click it, and then click **Copy** and, if prompted click **Allow**.
21. Click **Close**.
22. In the SharePoint Online window, click the apps icon, and then click **Mail**.

23. If prompted, select your language and time zone, and then click **Save**.
24. Click **New**.
25. In the **To** box, type the email address for your Microsoft Live account, and then in the **Subject** box, type **Shared Document**.
26. In the message box, right-click, and then click **Paste**.
27. Click **SEND**.
28. Close **Microsoft Edge**.

▶ Task 3: Verify external user sharing

1. Open **Microsoft Edge** and browse to **https://outlook.com**
2. Sign in with your Microsoft Live account.

   Note: The Inbox should show two emails from Microsoft Online Services Team. If the messages are not in the Inbox, look in the Junk folder.

3. Open the message that has the subject: **Holly Spencer wants to share Accounts Projects**.
4. Click the **Accounts Project** link in the email.
5. Click **Microsoft Account**. Verify that you can access the site.
6. Close the browser tab. In your inbox, open the second invitation email message with the subject of **Holly Spencer wants to share the document**.
7. Click the **Document** link.

Note: You are redirected directly to the Word Document. Word Online opens and shows the document.

8. Verify that you can access the Word document and then click **Edit in Browser**.
9. Add some text in this document.
10. Close **Microsoft Edge**.
11. Leave the virtual machines running for the next lab.

Results: After completing this exercise, you should have configured a new site collection for external user sharing, and you should have shared a site and a document with external users.

Module 10: Planning and configuring an Office 365 collaboration solution

Lab: Planning and configuring an Office 365 collaboration solution

Exercise 1: Configuring Yammer Enterprise

▶ Task 1: Configure a Yammer organization setting

1. In **LON-CL1**, click **Desktop**, open **Microsoft Edge** from the taskbar, and then browse to **https://portal.office.com**
2. Sign in as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
3. Click the **Office 365 app launcher** icon, and then click **Yammer**.
4. On the **WHO DO YOU WORK WITH?** pop-up, click the **X** in the top right corner to close the window.
5. In **Yammer**, in the left pane above **Search**, click the **Settings** gear icon.
6. Click **NETWORK ADMIN.**
7. In **Yammer admin center**, in the left navigation pane, click **Usage Policy**.
8. In the **Usage Policy** window, select the **Require users to accept policy during sign up and after any changes are made to the policy** check box.
9. In the **Usage Policy** window, select the **Display policy reminder in sidebar** check box.
10. In the **Custom Policy Title** text box, type **Adatum Acceptable Use Policy**.
11. In the **Enter your policy in the textbox below** text box, copy and paste the following text:

    Welcome to Yammer! Our goal is to provide a collaborative environment to connect with colleagues and bridge various departments and geographic locations to share meaningful information.
12. Click **Save**.
13. In the **Adatum Acceptable Use Policy** window, click **I Accept**.
14. If needed, in **Yammer**, in the left pane above **Search**, click the **Settings** icon, and then click **NETWORK ADMIN**.
15. In the left menu of the Yammer console, click **Configuration**.
16. In the **Enabled Features** page, remove the check mark from **3rd Party Applications**.
17. Click **Save**.
18. In the left-side menu of the **Yammer console**, click **Data Retention**.
19. In the **Data Retention Policy** page, read the description of available options and click **Soft Delete** and then click **Save**.
20. In the left menu of the **Yammer console**, click **Monitor Keywords**.
21. In the **Monitor Keywords** page, type **Holly@AVXXXXa.xtremelabs.us** in the **Email Address** field.
22. In the text box below, type the following words, one in each line: **gambling**, **erotic**, **warez**.

23. Click **Save**.
24. In the left menu of the **Yammer console**, click **Success**.
25. Click **Write a welcome message** at the bottom of the page.
26. Click **All**, and in the middle pane, in the **What are you working on?** text box, type: **Welcome to all Adatum users!**, and then click **Post**.

▶ Task 2: Configure Yammer service settings, and enforce Office 365 identity

1. In **Yammer**, in the left pane, click the **Settings** icon.
2. Click **NETWORK ADMIN**.
3. In **Yammer admin center**, in the left navigation pane in the **Content and Security** section, click **Security Settings**.
4. Scroll down to **Office365 Identity Enforcement**.
5. Select the **Enforce Office 365 identity** check box.
6. In the pop-up window, click **Okay.**
7. Click **Save**.

▶ Task 3: Configure the Yammer user experience

1. In **Yammer**, in the left pane, click the **Settings** icon, and then click **EDIT SETTINGS**.
2. In the toolbar, click **Notifications**.
3. Select only the following options in the **Email me when…** section:
   - **I receive a message in my inbox**
   - **I log in from somewhere new**
   - **I post a message via email (This will send a confirmation email)**
4. Click **Save**.
5. Close **Microsoft Edge**.

▶ Task 4: Using Yammer

1. On **LON-CL3**, open **Microsoft Edge**, and then connect to **https://portal.office.com**
2. Sign in as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
3. On the Office 365 portal, click **Yammer**.
4. At the **WHO DO YOU WORK WITH** prompt, type **Christie** in the first text box, and then click **DONE** and close the window.
5. Click **I Accept** at the **Adatum Acceptable Use Policy** prompt. Scroll down and click **Get Started with Yammer**
6. Find the post from **Holly Spencer** in the post list.
7. Click **Like**, and then click **SHARE**.
8. In the **Share This Conversation** dialog box, select **Post in a Group**, type **All Company** in the drop-down box, and then in the text box, type **Welcome from me too**.

9. Click **Share**.
10. Click **All Company** and in the **What are you working on** text box, type "**free gambling here"**, and then click **Post**.
11. Close **Microsoft Edge**.
12. Open **Microsoft Edge** and browse to **https://portal.office.com**
13. Sign in as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
14. On the Office 365 portal, click **Mail**.
15. Verify that you received a message from **Yammer** with a report about a monitored keyword appearance in **Beth's** post.
16. Close **Microsoft Edge**.

Results: After completing this exercise, you should have enabled Yammer Enterprise for A. Datum Corporation.

Exercise 2: Configuring OneDrive for Business

▶ Task 1: Enable OneDrive for Business synchronization

1. On **LON-CL3**, click **Start**, click **All apps**, and then click **Word 2016**.
2. In the **Word** window, in the top right corner, verify that Word is licensed to **Beth Burke**.
3. If **Word** is licensed to another account, click **Switch account**.
4. In the **Accounts** dialog box, click **SIGN OUT**, and then click **Sign out**. In the **Remove Account** notice, click **Yes**.
5. At the top right, click **Sign in to get the most out of Office**.
6. On the **Sign in** page, in the **E-mail address** box, type **Beth@AVXXXXa.xtremelabs.us**, and then click **Next**.
7. On the **Sign in** page, in the **Password** box, type **Pa55w.rd**, and then click **Sign in**.
8. Verify that **Word** is now licensed to **Beth**. Close **Word**.
9. Open **Microsoft Edge**, and then connect to **https://portal.office.com**
10. Sign in as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
11. On the Office 365 portal, click **OneDrive**.
12. If the **Welcome to OneDrive for Business** page appears, click **You're OneDrive is ready**.
13. In the **OneDrive** window, click **New**, and then click **Word document**.
14. In the **Word Online** window, type some text, and then click **Beth Burke** at the top of the window beside **Word Online**.
15. In the **OneDrive** window, click **Sync**.
16. In the **Did you mean to switch apps?** dialog box, click **Yes**.
17. In the **Sync your OneDrive files to this PC** dialog box, click **get the latest version of OneDrive.** Click **Save,** then click **Run.** Select **Start sync.**.

18. If prompted to sign in, type **Beth@AVXXXXa.xtremelabs.us**, and then click **Next**.
19. Type **Pa55w.rd**, and then click **Sign In**.
20. Click **File Explorer** on the task bar, and then click **OneDrive - A. Datum**.
21. Note that **File Explorer** displays the location where the synchronized files will be stored. Verify that the **Word document** has been synchronized to the **local computer**.

▶ Task 2: Create files to synchronize with OneDrive for Business

1. On **LON-CL3**, ensure that the **OneDrive for Business** folder is open in **File Explorer**.
2. On the ribbon in **File Explorer**, click **Home**, click **New folder**, and then create a new folder named **Private**.
3. On the ribbon, click **Home,** click **New folder**, and then create a second new folder named **Project A**.
4. Double-click the **Private** folder. Right-click in this folder, and on the context menu, click **New**, and then click **Microsoft Word Document**. Name the document **Holidays.docx**.
5. Double-click **Holidays.docx** to open it, and then type some short text. Save the changes, and then close **Microsoft Word**.
6. See how the document icon in the taskbar changes from two blue arrows to a small green check mark icon after the synchronization process is complete. The document has been transferred to the cloud storage automatically.
7. In the **File Explorer** window, navigate to **OneDrive for Business** in the navigation address line to move one level up.
8. Double-click the folder **Project A**. Right-click in this folder, and on the context menu, click **New**, and then click **Microsoft Word Document**. Name the document **Project targets.docx**.
9. Double-click **Project targets.docx** to open it, and then type some short text. Save the changes, and then close **Microsoft Word**.
10. Verify that the document synchronizes.
11. To view the files online, switch to the **Microsoft Edge** window. Refresh the view.
12. In the **Files** list, you should see your two folders, **Private** and **Project A**.
13. Navigate to the **Private** folder. Click the synchronized document **Holidays.docx** to open it in **Word Online**.
14. Click **Edit document**, and then click **Edit in Browser**. Add some text. The document is saved automatically when **Saved** is displayed in the title bar.
15. In the menu bar right beside Word Online, click **Beth Burke** to return to **OneDrive for Business**.
16. The content of the **Private** folder changes, and you will see that you changed the document online. The **Modified** column shows that the document changed some seconds (or minutes) ago.
17. Switch back to **File Explorer**. Navigate to the **Private** folder, and then open **Holidays.docx**. You will see that the changes you made in **Word Online** are synchronized back automatically.

▶ Task 3: Share files with other users

1. In **File Explorer**, right-click the folder **Project A**, click **View online**.
2. **Microsoft Edge** opens. Open the **Project A** folder, right-click **Project Targets.docx**, and then click **Share**.
3. **SharePoint Online** automatically opens a dialog box named **Share Project targets.docx**.

4. In the upper text box, type **Holly Spencer**.
5. Ensure that the text **Anyone with this link can view and edit** is shown, add a short message in the message text box below, and then click **Send**.
6. Open a new **InPrivate Microsoft Edge** window, and then connect to **https://portal.office.com**
7. Sign in as **Holly@AVXXXXa.xtremelabs.us** by using the password **Pa55w.rd1**
8. In the **Office 365 portal**, click **Mail**.
9. Click the message with the subject **Beth Burke has shared Project Targets**.
10. In the message box, click **Project Targets**.
11. When the document opens, click **Edit in Browser**. Verify that you can open the document and edit it. All modifications are stored online in the **OneDrive for Business** cloud storage. By default, **SharePoint Online** creates a new version when the document changes. This can be viewed by the owner in the version history.
12. Close the **InPrivate Microsoft Edge** window.
13. In the **Microsoft Edge** window, click the **Shared** button of **Project targets** in Sharing column.
14. In the menu on the right click **Manage access** and then click **Stop sharing**twice.
15. Close the **Microsoft Edge** window.

Results: After completing this exercise, you should have configured Microsoft OneDrive for A. Datum.

Exercise 3: Configuring Office 365 groups

▶ Task 1: Configure a private Office 365 group

1. On **LON-CL1**, sign in to **http://portal.office.com** as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
2. Open the **Office 365 admin center** through the app launcher by clicking the **Admin** icon.
3. Select **Groups** in the left navigation pane, click **Groups**, and then click **Add a group**.
4. In the **Add a group** window, verify that **Office 365 group** is selected in the **Type** drop-down list.
5. In the **Add a group** window, configure the following settings:
   - Name: **AdatumMarketing**
   - Group Id: **Adatummarketing@AVXXXXa.xtremelabs.us**
   - Description: **Adatum Marketing Group**
   - Under **Privacy**, select **Private – Only members can see group content**.
   - Set the language to **English (United Kingdom)**
   - Group owner: **Holly Spencer**
6. Click **Add**.
7. Click **Close**.
8. Click on **AdatumMarketing**, and in the **Details** window, in the **Members** section, click **Edit**.

9. Click **Add members**, and then click **Beth Burke**.

10. Click **Save**, and then click **Close**.

▶ Task 2: Configure a public Office 365 group with Windows PowerShell

1. On **LON-CL1**, double-click **Windows Azure Active Directory Module for Windows PowerShell** on the desktop.

2. Type the following command, and then press Enter:

```
$cred = Get-Credential
```

3. In the Windows PowerShell credential request window, sign in as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**

4. Type the following command, and then press Enter:

```
$session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $cred -Authentication
Basic -AllowRedirection
```

5. Type the following command, and then press Enter:

```
Import-PSSession $Session –AllowClobber
```

6. To create a new public Office 365 group, type the following command, and then press Enter:

```
New-UnifiedGroup –DisplayName "Planning Group" -Alias "PlanningGroup" –EmailAddresses
PlanningGroup@AVXXXXa.xtremelabs.us
```

7. To add a user to the owners group, type the following command, and then press Enter:

```
Add-UnifiedGroupLinks "Planning Group" –Links Holly@AVXXXXa.xtremelabs.us  –LinkType
Owner
```

8. To add a user to the members group, type the following command, and then press Enter:

```
Add-UnifiedGroupLinks "Planning Group" –Links Francisco@AVXXXXa.xtremelabs.us  –
LinkType Member
```

▶ Task 3: Explore the Office 365 group components

1. On **LON-CL1**, open **Microsoft Edge**, and then sign in to **https://portal.office.com** as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**

2. Click the app launcher in the upper-left corner.

3. Click **Mail**.

4. On the left pane, click **Planning Group**, and then click **Start a conversation**. If pop-up window is blocked, click **Always allow**.

5. In the message window, type **Planning Group** in the **To** line, type a subject and some content, and then click **Send**.

6. Click **Calendar** on the toolbar, and then view the group calendar.

7. Click **New**. In the **Details** pane, fill out the data for the meeting, type **Planning meeting** for the subject, schedule it for tomorrow, and then click **Save**.
8. Ensure that the calendar item synchronizes with **Holly's** personal calendar.
9. Click the **Office365 apps** icon, and then click **Mail**.
10. In the navigation pane, select **Planning Group**.
11. Click **Files** on the toolbar, and then wait for the files store to be created. It should take few minutes.
12. Click **New**, and then click **New Word document**.
13. Type some text, and when you see **Saved** in the title bar, close the **Microsoft Edge tab**.
14. In the **Mail** window, click **Files**, and then verify that the document has been added to the group.
15. On **LON-CL3**, open Microsoft Edge, and then sign in to **https://portal.office.com** as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**. Select **English (United States)** for language and select your time zone and click **Save**.
16. Click **Mail**. Verify that the **AdatumMarketing** group appears in your **Groups** list.
17. Under Groups, click **Browse** or **Discover**.
18. Click **Planning Group**, and then click **Join**. Because this is a public group, you can join the group.
19. In the left navigation pane, click **Planning Group**, and then click **Conversations**. Verify that you see the message that **Holly** sent to the group.
20. Click **Files**, and then verify that you see the document that **Holly** created.
21. Close **Microsoft Edge**.
22. Keep the virtual machines running for the next lab.

Results: After completing this exercise, you should have configured Microsoft Office 365 groups at A. Datum.

Module 11: Planning and configuring Rights Management and compliance

Lab: Configuring Rights Management and compliance

Exercise 1: Configuring Rights Management in Office 365

▶ Task 1: Activate Rights Management in Office 365

1. On **LON-CL1**, open **Microsoft Edge**, and then connect to **http://portal.office.com**
2. Sign in to the Microsoft Office 365 portal as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
3. In the app launcher, click the **Admin** icon.
4. In the Office 365 admin center, select **Settings** and then click **Services & add-ins**.
5. Click **Microsoft Azure Information Protection**.
6. On the **Microsoft Azure Information Protection** page, click **Manage Microsoft Azure Information Protection settings**.
7. On the **Rights Management** page, click **activate**.
8. When prompted with **Do you want to activate Rights Management?**, click **activate**.

▶ Task 2: Configure Rights Management for Exchange Online

1. Open the Windows Azure Active Directory Module for Windows PowerShell from the desktop.
2. Type the following commands, pressing Enter after each command, to connect to remote Exchange Online with remote PowerShell. Use **Holly's** credentials to connect.

```
$Cred = Get-Credential

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://outlook.office365.com/powershell-liveid/ -Credential $Cred -Authentication
Basic -AllowRedirection

Import-PSSession $Session
```

3. Type the following command, and then press Enter to set the IRM sharing location to the region you are in.

```
Set-IRMConfiguration -RMSOnlineKeySharingLocation “https://sp-
rms.eu.aadrm.com/TenantManagement/ServicePartner.svc”
```

Note: Depending on the location of your tenant, replace the link in the preceding command with one of the following:

- For North America: **https://sp-rms.na.aadrm.com/TenantManagement/ServicePartner.svc**
- For Asia: **https://sp-rms.ap.aadrm.com/TenantManagement/ServicePartner.svc**
- For South America: **https://sp-rms.sa.aadrm.com/TenantManagement/ServicePartner.svc**

4. Type the following command, and then press Enter to configure Azure Information Protection as a trusted publishing domain.

```
Import-RMSTrustedPublishingDomain -RMSOnline -name "RMS Online"
```

5. Type the following command, and then press Enter to set the IRM configuration for licensed users only.

```
Set-IRMConfiguration -InternalLicensingEnabled $true
```

6. Type the following command, and then press Enter to test the configuration.

```
Test-IRMConfiguration -Sender holly@AVXXXXa.xtremelabs.us
```

7. Type the following command, press Enter, and then close Windows PowerShell.

```
Remove-PSSession $Session
```

▶ Task 3: Configure Rights Management for SharePoint Online

1. In Microsoft Edge, access the Office 365 admin center by using App launcher icon.
2. In the left navigation pane, under **Admin centers**, click **SharePoint**.
3. In the SharePoint admin center, in the left pane, click **settings**.
4. On the **settings** page, in the Information Rights Management (IRM) section, click **Use the IRM service specified in your configuration**, and then click **Refresh IRM Settings**.

▶ Task 4: Validate the Azure Rights Management functionality

1. On **LON-CL1**, open Word 2016.
2. In the Word window, at the top-right corner, click **Switch account** or **Sign in**
3. In the **Accounts** dialog box, click **Add Account**.
4. In the **Sign in** dialog box, type **Holly@AVXXXXa.xtremelabs.us**, and then click **Next**.
5. Type **Pa55w.rd1**, and then click **Sign in**.
6. Close Word 2016.
7. On **LON-CL1**, open Microsoft Outlook 2016.
8. Create a new email with **Beth Burke** as the recipient.
9. Type a subject, and then type some text in the message body.
10. On the **Options** tab, click **Permission**, and then click **Connect to the Rights Management Server and get templates**. If a Windows Security window appears, click **OK** and sign in with **Holly's** credentials.

Note: It can take an hour or longer for **Permission** to appear as an option

11. Click **Permission** again, and then click **Do Not Forward**.

12. Send the message.
13. In Microsoft Edge, connect to **https://adatumAVXXXX.sharepoint.com/sites/marketing**
14. Click **Documents**, click the **settings** icon, and then click **Library settings**.
15. On the **Settings** page, under Permissions and Management, click **Information Rights Management**.
16. On the **Information Rights Management Settings** page, select the **Restrict permissions on this library on download** checkbox.
17. In the **Create a permission policy title** box, type **Marketing Policy**.
18. In the **Add a permission policy description** box, type **Marketing policy for downloads.**
19. Click **SHOW OPTIONS**.
20. Under Configure document access rights, select the **Allow viewers to write on a copy of the downloaded document** checkbox.
21. Click **OK**.
22. Close **Microsoft Edge**.
23. Open **Microsoft Edge**, and then connect to **https://portal.office.com**. Sign in as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
24. In the Office 365 portal, in the App launcher, click **Mail**.
25. On the Outlook page, select your time zone and click **Save**.
26. Verify that you received an email from **Holly** that is IRM protected. Click the message.
27. Click the down arrow beside **Reply all**, and then verify that you do not have the option to forward or print the message.
28. In **Microsoft Edge**, connect to **https://adatumAVXXXX.sharepoint.com/sites/marketing**
29. Click **Documents**, and then click **document**.
30. After the document opens, try to edit it in Word Online. Verify that you get a message that the document is read-only.
31. Close **Microsoft Edge**.

Results: After completing this exercise, you will have configured Rights Management for Exchange Online and SharePoint Online.

Exercise 2: Configuring compliance features

▶ Task 1: Configure Security & Compliance Center permissions and audit logging

1. On **LON-CL1**, open **Microsoft Edge**, and then connect to **https://portal.office.com**
2. Sign in to the Office 365 portal as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
3. In the app launcher, click the **Admin** icon.

4. In the Office 365 admin center, in the left side menu, select **Admin centers**, and then click **Security & Compliance**. If you are connected to the Compliance Center, click **Check out your new Office 365 Security & Compliance Center**.
5. In the Security and Compliance Center, click **Permissions**.
6. Click **Compliance Administrator**, and then click **Edit role group**.
7. On the **Compliance Administrator** page, click **Choose Members**, click **Choose mombers**.
8. In the Choose Members window, click **Add,** click **Beth Burke**, click **add**, and then click **Done**.
9. Click **Save**.
10. After **To assign permissions for archiving, auditing, and retention policies,** click **go to the Exchange admin center**.
11. Click **Compliance Management**, and then click **Edit**.
12. On the **Compliance Management** page, under **Members**, click **Add**.
13. In the Select Members window, click **Beth Burke**, click **add**, and then click **OK**.
14. Click **Save**.
15. Click **Recipient Management**, and then click **Edit**.
16. On the **Recipient Management** page, under **Members**, click **Add**.
17. In the Select Members window, click **Beth Burke**, click **add**, and then click **OK**.
18. Click **Save**.
19. Close the Exchange role groups window.
20. Click **eDiscovery Manager**, and then click **Edit role group**.
21. On the **eDiscovery Manager** page, under **Choose eDiscovery Manager**, click **Choose eDiscovery Manager**.
22. In the Select Members window, click **Add**, click **Christie Thomas**, click **add**, and then click **Done**.
23. Click **Save**.
24. Click **Search & Investigation**.
25. Click **Audit log search**.
26. On the **Audit log search** page, click **Start recording user and admin activities**, and then click **Turn on**. Note that it can take a couple of hours before this option is enabled.
27. Close **Microsoft Edge**.

▶ Task 2: Configure archive mailboxes

1. On **LON-CL1**, open **Microsoft Edge**, and then connect to **https://protection.office.com**
2. Sign in to the Office 365 portal as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**. **Beth** is a member of the Compliance Administrator role, so she can connect to the protection website.
3. In the navigation pane, click **Data governance**, and then click **Archive**.
4. In the Archive window, click **Christie Thomas**, and then Ctrl + click **Catherine Richard**.
5. Under **Bulk Edit**, click **Enable**. In the warning message, click **Yes**, and then click **Close**.

6. Click **Refresh**, and then verify that **Christie** and **Catherine** have been enabled for an archive mailbox.

▶ Task 3: Configure retention tags and policies

1. On **LON-CL1**, open **Microsoft Edge**, and then connect to **https://portal.office.com**.
2. Sign in to the Office 365 portal as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
3. In the app launcher, click the **Admin** icon.
4. In the Office 365 admin center, in the left side menu, select **Admin centers** and then click **Exchange**.
5. Under **compliance management**, click **retention tags**.
6. On the **retention Tags** page, click **New tag**, which is the plus sign (**+**), and then select **applied automatically to entire mailbox (default)**.
7. Type **Research User 1 year move to archive** as the name.
8. Select **Move to Archive** as the **Retention action**.
9. Type **365** as the **Retention period**.
10. Click **Save**.
11. On the toolbar, click **New tag**, and then select **applied automatically to entire mailbox (default)**.
12. Type **Default 2 years move to Deleted Items** as the name.
13. Select **Delete and Allow Recovery** as the **Retention action**.
14. Type **730** as the **Retention period**.
15. Click **Save**.
16. On the toolbar, click **New tag**, and then select **applied automatically to a default folder**.
17. Type **Purge Deleted Items 30 days** as the name.
18. Under Apply this tag to the following default folder, select **Deleted Items**.
19. Select **Permanently Delete** as the **Retention action**.
20. Type **30** as the **Retention period**.
21. Click **Save**.
22. On the toolbar, click **New tag**, and then select **applied by users to items and folders (personal)**.
23. Type **2 Year Delete** as the name.
24. Select **Delete and Allow Recovery** as the **Retention action**.
25. Type **730** as the **Retention period**.
26. Click **Save**.
27. On the toolbar, click **New tag**, and then select **applied by users to items and folders (personal)**.
28. Type **Never archive** as the name.
29. Select **Move to Archive** as the **Retention action**.
30. Select **Never** as the **Retention period**.
31. Click **Save**.
32. Click **retention policies**.

33. On the toolbar, click **New**.
34. On the **new retention policy** page, type **Research MRM Policy** as the name.
35. Click **Add** below **Retention tags**.
36. In the select retention tags window, Ctrl+click the following retention tags:

- **Research User 1 year move to archive**
- **Never Archive**
- **2 year delete**

37. Click **add**, and then click **ok**. Click **Save**.
38. In the left-hand menu, click **recipients**.
39. On the **mailboxes** page, click **ChristieThomas**, and then click **Edit**.
40. Click **mailbox features** and under **Retention policy** select **Research MRM Policy**, and then click **Save**.
41. Close Microsoft Edge.

▶ Task 4: Configure content deletion and preservation policies

1. In the **Security & Compliance center**, expand **Classifications**, and then click **Labels**
2. On the Labels page, click **+Create a label**.
3. Type **Retain contract details 7 years** in the Name box, and click **Next**.
4. On the Label settings pane, turn **Retention** "**On**"
5. Verify that **Retain the content** is selected, that it is set for **7 years**, and that **Nothing. Leave the content as is** is selected under **What do you want to do after this time**. Click **Next**.
6. Click **Create this label**.
7. On the Retain contract details 7 years pane, click **Auto-apply label**.
8. On the **Choose a label to auto-apply** pane, verify that **Retain contract details 7 years 7 years keep** is listed, and click **Next**.
9. Select **Apply label to content that contains specific words or phrases**, and click **Next**.
10. Type: **contract** in the **Keyword query editor** box, and click **Next**.
11. On the **Name your policy** pane, type: **Retain contract details**, and click **Next**.
12. On the **Choose locations** pane, select: **Let me choose specific locations**.
13. Turn "**off**" the switch for **Office 365 groups**.
14. Next to **Exchange email**, click **Choose recipients**. On the **Edit locations pane**, click: **Choose recipients**. Select **Francisco Chaves**, click **Choose**, then click **Done**.
15. Next to **SharePoint sites**, click **Choose sites**. On the **Edit locations** pane, click **Choose sites**.
16. In the **Edit locations** pane, type **https://AdatumAVXXXX.sharepoint.com/sites/AcctsProj/** in the search box, and then click the **Search** icon. Select the **Accounts Project** checkbox, and then click **Choose**. Click **Done**, then click **Next**.
17. Verify the settings, then click **Auto-apply**.

18. Notice the Status is **On (Pending)** and click **Close**.

Task 5: Configure data loss protection policies

1. Open **Microsoft Edge**, and then connect to **https://protection.office.com**
2. Sign in to the Office 365 portal as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
3. In the navigation pane, click **Data loss prevention** and then click **Policy**.
4. Click **Create a policy**.
5. On the **Start with a template or create a custom policy** page, verify that **Custom** is selected, and then click **Next**.
6. On the **Name your policy** page, type **Test DLP** in Name textbox, and then click **Next**.
7. On the **Choose locations** page, select **All locations in Office 365** and click **Next**.
8. On the **Customize the types of sensitive info you want to protect** page, select **Use advanced settings**, and click **Next**.
9. On the **Customize the types of sensitive info you want to protect** page, click **New rule**.
10. On the **Create a new rule** page, in the **Name** field, type **Scan for IP address**.
11. Under **Conditions,** click **Add** under **Content contains**, and then select **Sensitive info types**.
12. In **Sensitive info types** window, click **Add**. Select **IP Address** from the list and click **Add**. Click **Done**.
13. Click **Add a condition**, click **Content is shared**, and then select **with people outside my organization**.
14. Click **Add an action**, and then click **Restrict access to the content**.
15. Under User notifications, enable **Email notifications**.
16. Under Incident reports, enable the option to **Use email incident reports to notify you when a policy match occurs**. Click **Add or remove people,** click **Add,** select **Holly Spencer,** click **Add,** then click **Done**
17. Click **Save**, and then click **Next**.
18. On the **Do you want to turn on the policy or test things out first?** page, select **Yes, turn it on right away** and click **Next** and then click **Create**.

▶ Task 6: Create compliance check content

1. Open **Microsoft Edge**, and then connect to **https://portal.office.com**
2. Sign in to the Office 365 portal as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
3. On the Office 365 home page, click **Mail**.
4. Click **New**, type the new Microsoft account email address that you created for this course in the **To** line, type **Server IP address** as the **Subject**, type **My IP is 192.168.1.15** as the message body, and then wait for a minute or two until the policy tip appears at the top of message.
5. At the top of the message, click **Show details**.
6. Click **Override**, and then click **Send**.
7. Close **Microsoft Edge**.

▶ Task 7: Validate the configuration

1. Open **Microsoft Edge**, and then connect to **https://outlook.com**. Sign in with your Microsoft account.

2. Click the **message** from **Beth Burke** with the subject **Server IP address**.
3. Close **Microsoft Edge**.
4. Open **Microsoft Edge**, and then connect to **https://portal.office.com**
5. Sign in to the Office 365 portal as **Christie@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
6. Click **Mail**.
7. Select your time zone, and then click **Save**.
8. In the left pane of **Christie's** mailbox, under Folders, click **More**.
9. Verify that a folder named **In-Place Archive - Christie Thomas** has been created.
10. Close **Microsoft Edge**.
11. Open **Microsoft Edge**, and then connect to **https://portal.office.com**
12. Sign in to the Office 365 portal as **Beth@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd**
13. Click **Mail**.
14. Verify that you have received notification about message you sent to your personal account. This message should have **Rule detected** words in the subject.

Results: After completing this exercise, you will have implemented the Office 365 compliance features.

Module 12: Monitoring and troubleshooting Microsoft Office 365

Lab: Monitoring and troubleshooting Office 365

Exercise 1: Monitoring Office 365

▶ Task 1: Send an email to a nonexistent domain

1. On **LON-CL1**, on the taskbar, click **Microsoft Edge**.
2. Browse to **https://portal.office.com/**, and then sign in as **Holly@AVXXXXa.xtremelabs.us** by using the password **Pa55w.rd1**
3. Click **Mail**, and then click **New**.
4. In the **To** text box, type **user@alt.none**.
5. Enter a subject and some body text, and then click **Send**.

▶ Task 2: Track mail delivery

1. Wait for the delivery failure message to appear.
2. Note the reason for the failure ("The domain name in the email address is incorrect.").
3. Select the body text of the message, including the phrase **"Generating server"** down to **"X-OriginatorOrg: AVXXXXa.xtremelabs.us"** and then press **Ctrl+C** to copy it to the Clipboard.
4. In **Microsoft Edge**, press **Ctrl+T** to create a new tab.
5. In the new tab, browse to **testconnectivity.microsoft.com**
6. On the **Microsoft Remote Connectivity Analyzer** page, click the **Message Analyzer** tab.
7. Under **Message Header Analyzer**, paste the message, and then click **Analyze headers**.
8. Note the diagnostic information and the time taken for the message to be rejected.
9. Click **Clear** to reset the **Message Header Analyzer**.

▶ Task 3: Send an email to a nonexistent user

1. In **Microsoft Edge**, click **Holly's Mail** tab.
2. Click **New**, and then in the **To** text box, type **difflop48999@outlook.com**.
3. Enter a subject and some body text, and then click **Send**.

▶ Task 4: Track mail delivery

1. Wait for the delivery failure message to appear.
2. Note the reason for the "550 Requested action not taken: mailbox unavailable" failure.
3. Select the body text of the message including the phrase **"Generating server"** down to **"X-OriginatorOrg: AVXXXXa.xtremelabs.us"** and then press **Ctrl+C** to copy it to the Clipboard.
4. In **Microsoft Edge**, switch to the **Microsoft Remote Connectivity Analyzer** tab.

5. On the **Microsoft Remote Connectivity Analyzer** page, ensure that you are on the **Message Analyzer** tab.
6. Under **Message Header Analyzer**, paste the message, and then click **Analyze headers**.
7. Note the diagnostic information and the time taken for the message to be rejected.
8. Close the **Microsoft Remote Connectivity Analyzer** page.

▶ Task 5: Analyze mail flow

1. On **Holly's Mail** tab in the **Microsoft Office 365 portal**, click the **Apps** launcher in the top task bar, and click **Admin.**
2. Access the new **Office 365 admin center**, click **Admin centers**, click **Exchange**, and then click **mail flow**.
3. In **mail flow**, click **message trace**.
4. In **message trace**, next to Sender, click **add sender**.
5. In the **Select Members** dialog box, click **Holly**, click **add**, and then click **OK**.
6. Under Date range, select **Past 24 hours**.
7. Under Delivery status, select **Failed**, and then click **search**. Note the two messages.
8. Double-click each message to view the sender, recipient, message size, ID, and IP address information.
9. Note the differences between the message processing events: Receive, Submit, Spam Diagnostics, and Fail for the nonexistent domain, and Submit, Receive, Spam Diagnostics, and Fail for the nonexistent user.
10. Close the **Message Trace** window.

Results: After completing this exercise, you should have used the Message Header Analyzer to identify why email failed to deliver.

Exercise 2: Monitoring service health and analyzing reports

▶ Task 1: View Office 365 service health

1. In the new Office 365 admin center, click **Home**.
2. On the **Home** page, in the left menu, select **Health**, and then click **Service health**.
3. Click **Go to the v2 Service Health page** link.
4. Select **Exchange Online** in the left column.
5. On the right side of the page, click **View history**.
6. Click any entry in the calendar that is colored yellow to see further details about incident. Details appear below the calendar.
7. Click the **Home** icon on the menu to the left.

▶ Task 2: View reports in the Office 365 admin center

1. In the **Office 365 admin center**, click **REPORTS**.
2. On the **Reports** page, in the **Usage** section, click **Email Activity**.

Note: There might be little or no data shown because there is not much mailbox usage in the lab environment.

3. Close the open window.
4. On the **Reports** page, in the **Security & compliance** section, click **Malware detections**.
5. Close the open window.
6. On the **Reports** page, in the **Security & compliance** section, click **Spam detections**.
7. Close the open window.
8. Keep the virtual machines running for the next lab.

Results: After completing this exercise, you should have monitored the health of Office 365 services and viewed reports in the Office 365 admin center.

Module 13: Planning and configuring identify federation

Lab: Planning and configuring identity federation

Exercise 1: Deploying Active Directory Federation Services (AD FS) and Web Application Proxy

▶ Task 1: Add DNS records required for AD FS

1. On **LON-DS1**, click **Start** and then click **Windows PowerShell**.
2. Type **IPConfig** and press Enter.
3. Record the IPv4 address assigned to the server.
4. On **LON-DC1**, open **Server Manager**, click **Tools**, and then click **DNS**.
5. Expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **AVXXXXa.xtremelabs.us**.
6. Right-click **AVXXXXa.xtremelabs.us**, and then click **New Host (A or AAAA)**.
7. In the New Host dialog box, leave the **Name box** empty, in the **IP address** box, type the External IP address provided by **XtremeLabs**.
8. Click **Add Host**, and then click **OK**.
9. In the New Host dialog box, leave the **Name box** empty, in the **IP address** box, type the **LON-DS1** IP address that you recorded in Step 3.
10. Click **Add Host**, click **OK**, and then click **Done**.

▶ Task 2: Install and configure the AD FS server role

1. Sign in to the **LON-DS1** virtual machine as **ADATUM\Administrator** with a password of **Pa55w.rd**
2. Click Start, right click **Windows PowerShell**, and then click **Run as Administrator**.
3. At the command prompt, type the following command and press Enter. This command creates the Key Distribution Services root key to generate group Managed Service Account passwords for the account that will be used later in this lab. You should receive a Guid value as a response to this command.

   ```
   Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))
   ```

4. Click Start and then click **Server Manager**.
5. In Server Manager, click **Manage**, and then click **Add Roles and Features**. If you get a Server Manger message about collecting inventory data, click **OK**. Wait a minute and then try this step again.
6. In the **Add Roles and Features Wizard**, on the **Before you begin page**, click **Next**.
7. On the **Select installation type** page, click **Role-based or Feature-based installation**, and then click **Next**.
8. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
9. On the **Select server roles** page, click **Active Directory Federation Services**, and then click **Next**.

10. On the **Select features** page, click **Next**.
11. On the **Active Directory Federation Service (AD FS)** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**.
13. When installation completes, on the **Installation progress** page, click **Close**.
14. Click the **exclamation mark icon** on the toolbar, and then click **Configure the federation service on this server**.
15. In the **Active Directory Federation Services Configuration Wizard**, on the **Welcome** page, click **Create the first federation server in a federation server farm**, and then click **Next**.
16. On the **Connect to AD DS** page, click **Next**.
17. On the **Specify Service Properties** page, use the following settings, and then click **Next**:
    - For **SSL Certificate**, click the wild card certificate provided by XtremeLabs.
    - For **Federation Service Name**, type **AVXXXXa.xtremelabs.us**, replacing **AVXXXXa** with your unique Adatum domain name.
    - For **Federation Service Display Name**, type **Adatum Corporation**.
18. On the **Specify Service Account** page, select the option **Create a Group Managed Service Account**, for **Account Name** type **svc-ADFS**, and then click **Next**.
19. On the **Specify Configuration Database**, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
20. On the **Review Options** page, click **Next**.
21. Once the prerequisites check is complete, on the **Pre-requisite Checks** page, click **Configure**. Note : Some warnings are expected to be shown.
22. When the configuration completes, on the **Results** page, click **Close**.
23. Restart the computer.

▶ Task 3: Install the Web Application Proxy server role service

1. Sign in to the **LON-WAP1** virtual machine as **Adatum\Administrator** with a password of **Pa55w.rd**
2. Click **Start** and then click **Server Manager**.
3. In **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
4. In the **Add Roles and Features Wizard**, on the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, click **Role-based or Feature-based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
7. On the **Select server roles** page, click **Remote Access**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Remote Access** page, click **Next**.
10. On the **Select role services** page, click **Web Application Proxy**, in the popup window, click **Add Features**, and then click **Next**.

11. On the **Confirm installation selections** page, click **Install**.
12. When the installation is complete, on the **Installation progress** page, click **Close**.

▶ Task 4: Configure the Web Application Proxy server

1. On **LON-WAP1**, in Server Manager, click **Tools**, and then click **Remote Access Management**.
2. In the **Remote Access Management Console**, in the left navigation pane, click **Web Application Proxy**. In the middle navigation pane, click **Run the Web Application Proxy Configuration Wizard**.
3. In the **Web Application Proxy Configuration Wizard**, on the **Welcome** page, click **Next**.
4. On the **Federation Server** page, use the following settings, and then click **Next**:
   - Federation service name: **AVXXXXa.xtremelabs.us**, replacing **AVXXXXa** with your unique Adatum domain name.
   - User name: **Adatum\Administrator**
   - Password: **Pa55w.rd**
5. On the **AD FS Proxy Certificate** page, select the ***.xtremelabs.us** certificate, and then click **Next**.
6. On the **Confirmation** page, click **Configure**.
7. When the configuration is complete, on the **Results** page, click **Close**.

▶ Task 5: Verify that the AD FS server is working

1. Switch to the **LON-DS1** virtual machine.
2. In Server Manager, click **Tools**, and then click **Event Viewer**.
3. In **Event Viewer**, in the **details pane**, expand **Applications and Services Logs**, expand **AD FS**, and then click **Admin**.
4. In the **Event ID** column, verify that event ID **100** displays.

Note: If the federation server is configured properly, you should see a new event with event ID 100 in the Event Viewer Application log. This event verifies that the federation server was able to communicate successfully with the Federation Service.

5. On **LON-DC1**, open **Internet Explorer** and connect to **https://AVXXXXa.xtremelabs.us/adfs/fs/federationserverservice.asmx**, replacing **AVXXXXa** with your unique Adatum domain name, and then press Enter.
6. If you get a message stating **There is a problem with this website's security certificate**, click **Continue to this website**.

Note: The expected output is a display of XML with the service description document. If this page displays, then Microsoft Internet Information Services (IIS) on the federation server is operational and serving pages successfully.

Results: After completing this exercise, you should have deployed the AD FS server in a federation server farm, and deployed the Web Application Proxy server to support AD FS.

Exercise 2: Configuring federation with Microsoft Office 365

▶ Task 1: Switch the Office 365 tenant to federated mode

1. Switch to the **LON-DS1** virtual machine.
2. Open **Internet Explorer**, and then connect to **https://portal.office.com**
3. Sign in as **Holly@AVXXXXa.xtremelabs.us** with the password **Pa55w.rd1**
4. Click **Admin**.
5. If you are connected to the previous **Office 365 admin center**, click the banner at the top of the page to access the new Office 365 admin center
6. Click **Users** and then click **Active Users**.
7. Click **Holly Spencer**, and then, in the **User name/Email Aliases** section, click **Edit**.
8. Change the primary email alias to **AdatumAVXXXX.onmicrosoft.com**. In the Warning window, click **Save**, and then click **Sign Out**.
9. Close **Internet Explorer**. **Holly** cannot change the **AVXXXXa.xtremelabs.us** to a federated domain if she is logged in using an account from this domain.
10. Click Start, and then click the **Windows PowerShell** icon.
11. At the Windows PowerShell prompt, type the following commands, pressing Enter at the end of each line:

    ```
    Set-ExecutionPolicy Unrestricted –force

    Import-Module MSOnline
    ```

12. At the Windows PowerShell prompt, type the following command, and then press Enter:

    ```
    $msolcred = Get-Credential
    ```

13. In the **Windows PowerShell Credential** dialog box, enter the following credentials, and then click **OK**:
    - User name: **Holly@AdatumAVXXXX.onmicrosoft.com**
    - Password: **Pa55w.rd1**
14. At the Windows PowerShell prompt, type the following command, and then press Enter:

    ```
    Connect-MsolService -Credential $msolcred
    ```

15. At the Windows PowerShell prompt, type the following command, and then press Enter:

    ```
    Get-MsolDomain
    ```

16. Verify that your lab domain, **AVXXXXa.xtremelabs.us**, is listed as **Verified and Managed**.

Note: If you were running this from a computer other than the AD FS federation server, you would need to use the **Set-MsolAdfsContext** to reference the AD FS server.

17. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Convert-MsolDomainToFederated -DomainName AVXXXXa.xtremelabs.us
```

18. Verify that you get a **Successfully updated AVXXXXa.xtremelabs.us domain** message.

19. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-MsolFederationProperty -DomainName AVXXXXa.xtremelabs.us
```

Note: This command reports the status of the domain federation, and provides details of URLs and certificates.

Results: After completing this exercise, you should have enabled a federation trust between your on-premises Active Directory domain and Office 365 through your AD FS federation server, and you should have converted your domain for federated authentication in Office 365.