# Lab Answer Key: Module 7: Planning and configuring Exchange Online services

# Lab A: Configuring message transport in Exchange Online

## Exercise 1: Configuring message-transport settings

#### Task 1: 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://portal.office.com**, and press Enter.
3. At the login page, sign in as **Holly@Gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number, with the password ‘Pa55w.rd’.
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.

1. In the Exchange admin center, on the **connectors** tab, click **New**.
2. On the **Select your mail flow scenario** page, in the **From** box, select **Partner organization**.
3. In the **To** box, select **Office 365**, and then click **Next**.
4. On the **New connector** page, in the **Name** box, type **Humongous Insurance Incoming**, and then click **Next**.
5. Click **Use the sender's domain**, and then click **Next**.
6. Click **Add**, type **humongousinsurance.com**, click **OK**, and then click **Next.**
7. Select the **Reject email messages if they aren't sent over TLS** check box, and then click **Next**.
8. 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://portal.office.com**, and then press Enter.
18. Sign in as **Francisco@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number, 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@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number, and **Pa55w.rd** 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**.

**Result**: 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@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number.
7. Select the **Notify administrator about undelivered messages from external senders** check box.
8. In the **Administrator email address** box, type **Holly@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number, 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@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number.
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@Gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number.
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**.

**Result**: 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**

1. Under **Private computer or OWA for devices**, clear the **Direct file access** check box, and then click **Save**.
2. Click **recipients**, click **mailboxes,** click **Kendra Sexton**, and then click **Edit**.
3. In the Kendra Sexton window, click **mailbox features**.
4. Under **Email Connectivity**, click **View details**.
5. In the Outlook Web App mailbox policy window, click **Browse**, click **Limited features**, click **OK**, and then click **Save**.
6. In the Kendra Sexton window, click **Save**.
7. On LON-CL1, click **Start**, type **Outlook** and then click **Outlook 2016**. If prompted, type **Holly@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number, and **Pa55w.rd** in the Windows Security dialog box.
8. Click **New Email**.
9. In the new email window, in the **To** box, type **Kendra@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number, and then click **Check Names**.
10. In the **Subject** box, type **Attachment Test**.
11. In the ribbon, click **Attach File**, and then click **Browse This PC**.
12. In the Insert File window, browse to **C:\Windows\Logs\DISM**, click **dism**, and then click **Insert**.
13. Click **Send**.
14. On LON-CL2, in Outlook on the web, sign out, and then sign in again as **Kendra@gsp.Adatumvsxxxx.virsoftlabs.com**, where *xxxx* is your unique Adatum number, with the password ‘Pa55w.rd’.
15. On the Outlook page, select your time zone and click **Save**.
16. Read the new Attachment Test message.
17. Click the message attachment.
18. 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.

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

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.