

# Lab Answer Key: Module 3: Planning message transport

## Lab: Planning message transport

### Exercise 1: Planning for a redundant and secure message transport

#### Task 1: Plan a message transport plan

Review the information in the Exercise Scenario and answer the following questions:

1. **Question:** What additional Exchange Servers does your deployment require, if any?

**Answer:** Yes, you would need to deploy an Edge Transport server in the Berlin perimeter network. This would meet the requirement of sending/receiving email between the internal users and the internet.

2. **Question:** Will you need to make any DNS changes to meet the requirements? If so, what are the changes?

**Answer:** Yes, you would need to setup an MX Domain Name System (DNS) record that refers to the Edge Transport server at the secondary site. Then, you need to configure it with a higher priority than the MX DNS record that refers to the Edge Transport server at the primary site. This addresses the requirement that email from senders on the internet to your internal recipients has a higher preference to use the primary site's Exchange Servers for message delivery. It also addresses the requirement that email remains available regardless of whether either site is unavailable.

3. **Question:** Will you need to make any changes to the Send or Receive connectors to meet the requirements? If so, what are the changes?

**Answer:** Yes, you will need to enable Edge subscriptions for each Edge Transport server and configure the Send connectors as scoped Send connectors. Additionally, you will need to enable a new Receive connector on the Edge Transport server in the Berlin site.

4. **Question:** Will you need to make any changes to the transport rules to meet the requirements? If so, what are the changes?

**Answer:** No, most transport rules are located on the Mailbox servers, so no changes are necessary. A small subset of transport rule conditions are available on Edge Transport servers (Edge rule agent).

5. **Question:** What are the certificate requirements in your deployment?

**Answer:** You will need to generate a certificate for each of your Exchange Edge servers from a public certification authority (CA) or from your internal public key infrastructure (PKI). If you, or Contoso, generate the certificate from an internal PKI, a certificate and certificate keys exchange will need to occur with one another. When generating the certificate, the domain name property on the certificate should include the fully qualified domain name (FQDN) of the Exchange Edge transport servers, as defined on the MX DNS records. Also, you will need to assign the respective certificate to the Simple Mail Transport Protocol (SMTP) service on each Edge server.

6. **Question:** Will you need to make any changes to the transport configuration to meet the requirements? If so, what are the changes?

**Answer:** Yes, you need to use the **Get-TransportConfig** Exchange Management Shell cmdlet to set the following properties:

- o TLSReceiveDomainSecureList: **Adatum.com**
- o TLSSendDomainSecureList: **Contoso.com**

7. **Question:** Will you need to create any Receive connectors to meet the requirements?

**Answer:** Yes, you will need to create a new Receive connector on each of the Edge Transport servers with the following criteria:

- o Type: **Partner**
- o Remote network settings: IP address(es) of the Contoso SMTP servers
- o Transport Layer Security (TLS): Enabled
- o Enable domain security (mutual Auth TLS): Enabled
- o Permission groups: Partners

8. **Question:** Will you need to create any Send connectors to meet the requirements?

**Answer:** Yes, you will need to create a new Send connector on each of the Edge Transport servers with the following criteria:

- o Type: **Partner**
- o Smart host: Not enabled
- o Address spaces: **smtp:Contoso.com**
- o DomainSecureEnabled: **True**

9. **Question:** Will you need to configure the anti-spam policy to meet the requirements?

**Answer:** No, the Edge Transport server will not inspect emails for spam if the inbound email is from a partner.

## Task 2: Discuss your design with the class

- Discuss the proposed solutions of all students to find the solution that best meets Adatum's requirements.

**Result:** After this exercise, you should have created a message transport plan that meets the requirements.

## Exercise 2: Planning for transport compliance

### Task 1: Plan a compliance plan for message transport

Review the information in the Exercise Scenario and answer the following questions:

1. **Question:** Do you need transport rules in order to meet the requirements? If so, how many transport rules do you need and how will you implement them?

**Answer:** Yes, transport rules are necessary to meet the requirements. You need to create four transport rules to fulfill the requirements, and create them in the Exchange admin center.

2. **Question:** Do you need journaling? If so, how will you implement it?

**Answer:** Journaling is necessary to journal all messages sent from the distribution group Research to internal and external recipients. Because this type of journaling is a Premium feature, it requires an Enterprise client

access license.

3. **Question:** Do you need recipient moderation? If so, how will you implement it?

**Answer:** Recipient moderation is necessary for the management team to approve all messages that are sent to the AllCompany distribution group.

4. **Question:** How can you protect messages during the message delivery? Is Information Rights Management (IRM) an option? If so, which features can you use to meet the requirements?

**Answer:** Transport protection rules allow you to use transport rules to protect messages with IRM by applying Active Directory Rights Management Service (AD RMS) rights-policy templates.

## Task 2: Discuss your design with the class

- Discuss the proposed solutions of all students to find the solution that best meets Adatum's requirements.

**Result:** After this exercise, you should have created a compliance plan for message transport based on your compliance requirements.

## Exercise 3: Implementing transport compliance

### Task 1: Configure the required transport rules

1. On LON-EX1, open Internet Explorer, in the address bar, type <https://lon-ex1.adatum.com/ecp>, and then press Enter to open the Exchange admin center.
2. Sign in as **Adatum\administrator** with the password **Pa55w.rd**.
3. On the **Choose your preferred display language and home time zone below** page, on the **Time Zone** menu, select your time zone, and then click **Save**.
4. In the Exchange admin center, navigate to **mail flow – rules**.
5. Click **New**, and then click **Apply disclaimers**.
6. In the **Name** text box, type **Adatum External Disclaimer**.
7. In the **Apply this rule if** drop-down list, select the **The recipient is located** condition.
8. In the **select recipient location** dialog box, in the drop-down list, select **Outside the organization**, and then click **OK**.
9. Under Do the following, click **Append the disclaimer**.
10. Next to **Append the disclaimer**, click **Enter text**, and then type **This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute, or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system.** Click **OK**.
11. Next to **Append the disclaimer**, click **Select one**, and then in the **specify fallback action** page, click **Reject**, and then click **OK**.

12. Click **Save**.
13. To create another rule, based on the **Apply disclaimers** built-in rule template, click **New**, and then click **Apply disclaimers**.
14. In the **Name** text box, type **Adatum Info Disclaimer**.
15. In the **Apply this rule if** dropdown list, click **The sender is**, and then click the mailbox **info@adatum.com**. Click **Add**, and then click **OK**.

**Note:** If info@adatum.com is not visible, in the **Items per page** drop down list, select **100**, and then click refresh.

16. Under Do the following, click **Append the disclaimer**.
17. Next to **Append the disclaimer**, click **Enter text**, and then type **This message is sent on behalf of the Information Department of Adatum and is intended for internal recipients of Adatum only. If you are not the intended recipient, you are notified that disclosing, copying, distributing, or taking any action in reliance on the contents of this information is strictly prohibited**. Click **OK**.
18. Next to **Append the disclaimer**, click **Select one**, and then in the **specify fallback action** page, click **Reject**, and then click **OK**.
19. Click **Save**.
20. Select **Start**, expand **Microsoft Exchange Server 2019**, and then click **Exchange Management Shell**.
21. In the Exchange Management Shell, type the following command to create the **Adatum Customer Approval** transport rule, and then press Enter:

```
New-TransportRule -Name "Adatum Customer Approval" -SubjectOrBodyMatchesPatterns
"\d\d\d\d(-|.)\d\d\d" -ModerateMessageByUser Benjamin@adatum.com
```

22. In the Exchange Management Shell, type the following command to create the **ADatum Internal Confidential** transport rule, and then press Enter:

```
New-TransportRule -Name "Adatum Internal Confidential" -SubjectOrBodyContainswords
"Confidential" -SentToScope NotInOrganization -RejectMessageReasonText "You are not
allowed to send confidential messages outside the organization"
```

## Task 2: Configure the required message-moderation settings

1. In the Exchange admin center, navigate to **recipients – groups**.
2. In the result pane, click the **AllCompany** distribution group, and then click **Edit**.
3. On the **AllCompay** page, click **message approval**, and then complete the following:
  - a. Select the **Messages sent to this group have to be approved by a moderator** check box.
  - b. In the **group moderators** list, click **Add**.

- c. In the **Select group moderators** dialog box, find and select **Aidan**, click **Add**, and then click **OK**.
  - d. On the **AllCompany** page, in **Select moderation notifications**, select **Notify senders in your organization when their messages aren't approved**.
4. Click **Save**.

### Task 3: Configure the required journal rules

1. Navigate to **compliance management**, click **journal rules**, and then click **New**.
2. On the **new journal rule** page, in the **Send journal reports to** field, type **Journal**.
3. In the **Name** text box, type **Research Journal Rule**.
4. In the **If the message is sent to or received from** field, click **A specific user or group**. Search for **Research**, select **Research**, click **add**, and then click **OK**.
5. In the **Journal the following messages** field, click **All messages**.
6. Click **Save**.
7. Navigate to **recipients – mailboxes**. Search for the **Journal** mailbox, and then double-click to open the properties.
8. Click **mailbox delegation**, navigate to **Full Access**, and then click **Add**.
9. Search for the **Managers** group, select the **Managers** group, click **add**, and then click **OK**.
10. Click **Save** and if there is a warning window, click **Yes**.
11. Switch to LON-DC1.
12. From Server Manager, click **Tools**, open **Active Directory Users and Computers**, expand **Adatum.com**, and then click the **Users** container.
13. Right-click **Journal**, and then click **Disable Account**. Click **OK**.
14. Sign out of LON-DC1.

### Task 4: Validate the security configuration for message transport

1. On LON-EX1, close Internet Explorer.
2. Open Internet Explorer, and then connect to **https://LON-EX1.adatum.com/owa**. Sign in to Outlook on the web as **Adatum\Info** with the password **Pa55w.rd**.
3. On the **Choose your preferred display language and home time zone below** page, in the **Time Zone** menu, select your time zone, and then click **Save**.
4. In Outlook on the web, click **New**, and in the **To** field type **Erin@adatum.com**.
5. In the subject and message body type your choice and then click **Send**.

**Note:** If you receive an alert when trying to send the message, verify that all Exchange services are started and then try sending the message again.

6. Sign out of Outlook on the web.
7. Sign in to Outlook on the web as **Adatum\Erin** with the password **Pa55.wrd**.
8. On the **Choose your preferred display language and home time zone below** page, on the **Time Zone** menu, select your time zone, and then click **Save**.
9. Check that the message from info@adatum.com contains the correct disclaimer.
10. In Outlook on the web, click **New**, in the **To** field, type **Adam@adatum.com**, in the subject type **Customer Information**, in the body type **number 2012-19**, and then click **Send**.
11. Sign out of LON-CL1 and then sign in to LON-CL1 as user **Adatum\Benjamin** with the password **Pa55w.rd**.
12. Open Outlook. Create the Outlook profile for Benjamin.
13. If you receive a warning that Microsoft Office is not activated, in the Microsoft Office Activation Wizard window, click **Close**.
14. Check that the message from Erin is in your Inbox and waiting for approval.
15. Click **Reject** and **OK** to reject the message from Erin. Close Outlook. Sign Benjamin out of LON-CL1.
16. On LON-EX1, check Erin's inbox in Outlook on the web for the rejected message.
17. Read the information.
18. Validate the **Adatum Internal Confidential** transport rule, which rejects messages that have the word Confidential in the subject or body, if the recipients are outside the organization.
19. Signed in to Outlook on the web as **Adatum\Erin**, create an email message that has the word Confidential in the subject or body, and then send it to **Troy@treymresearch.net**.
20. In Outlook on the web, create and send an email message to the distribution group **AllCompany**.
21. Check that a MailTip window informs you that the group is moderated.
22. Sign out Erin from Outlook on the web.
23. Sign in to LON-CL1 as user **Adatum\Aidan** with the password **Pa55w.rd**.
24. Open Outlook, and then create the user profile as requested.
25. If you receive a warning that Microsoft Office is not activated, in the Microsoft Office Activation Wizard window, click **Close**.
26. Check that the message from Erin is in your Inbox and waiting for approval.
27. Click **Approve**.
28. Close Outlook. Sign out Aidan from LON-CL1.
29. Sign in to LON-CL1 as user **Adatum\Benjamin** with the password **Pa55w.rd**.
30. Open Outlook.
31. If you receive a warning that Microsoft Office is not activated, in the Microsoft Office Activation Wizard window, click **Close**.

32. Create and send an email message to **Camille@adatum.com**.
33. Close Outlook. Sign Benjamin out of LON-CL1.
34. Sign in to LON-CL1 as user **Adatum\Aidan** with the password **Pa55w.rd**.
35. Open Outlook.
36. If you receive a warning that Microsoft Office is not activated, in the Microsoft Office Activation Wizard window, click **Close**.
37. Click **File**, and then click **Add Account**.
38. On the **Welcome to Outlook** page, in the text field, type **Journal@adatum.com**. Click **Connect**.
39. Select **Exchange**.
40. Click **OK**.
41. Verify that the Journaling mailbox is listed in Outlook.
42. Check for the journaled message sent from Benjamin to Camille.

#### Task 5: Prepare for the next module

When you are finished with the lab, revert all virtual machines to their initial state:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20345-2B-LON-EX2**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat step 2 and 3 for **20345-2B-LON-CL1**, **20345-2B-LON-EX1**, and **20345-2B-LON-DC1**.

**Result:** After this exercise, you should have implemented message transport security.