Module 10: Implementing and administering AD FS

Lab: Implementing AD FS

(VMs: 20742B-LON-SVR1, 20742B-TREY-DC1, 20742B-LON-CL1)

Exercise 1: Configuring the AD FS prerequisites

Task 1: Configure the DNS forwarders

1. On **LON-DC1**, in the **Server Manager** window, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC1**, and then click **Conditional Forwarders**.
3. Right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
4. In the **New Conditional Forwarder** window, in the **DNS Domain** box, type **TreyResearch.net**.
5. In the **IP addresses of the master servers** box, type ***172.16.10.10*** and then press Enter.

Note: *If you receive a notification that the IP address is not authoritative for the required zone, you can safely ignore and proceed.*

6. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box, select **All DNS servers in this forest**, and then click **OK**.
7. Close DNS Manager.
8. On **TREY-DC1**, in the **Server Manager** window, click **Tools**, and then click **DNS**.
9. In DNS Manager, expand **TREY-DC1**, and then click **Conditional Forwarders**.
10. Right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
11. In the **New Conditional Forwarder** window, in the **DNS Domain** box, type ***Adatum.com***
12. In the **IP addresses of the master servers** box, type ***172.16.0.10*** and then press Enter.

Note: *If you receive a notification that the IP address is not authoritative for the required zone, you can safely ignore and proceed.*

13. Select the **Store this conditional forwarder in Active Directory, and replicate it as follows** check box, select **All DNS servers in this forest**, and then click **OK**.
14. Close DNS Manager.

Note: *In a production environment, you probably will use Internet DNS instead of conditional forwarders.*

Task 2: Configure the certificate trusts

1. On **LON-DC1**, open **File Explorer**, go to ***\\TREY-DC1\CertEnroll*** and then copy **TREY-DC1.TreyResearch.net_TreyResearchCA.crt** to **C:**.
2. Close File Explorer.
3. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
4. In Group Policy Management, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
5. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Public Key Policies**, and then click **Trusted Root Certification Authorities**.
6. Right-click **Trusted Root Certification Authorities**, and then click **Import**.
7. In the **Certificate Import Wizard**, on the **Welcome to the Certificate Import Wizard** page, click **Next**.
8. On the **File to Import** page, type: ***C:\TREY-DC1.TreyResearch.net_TreyResearchCA.crt*** and then click **Next**.
9. On the **Certificate Store** page, click **Place all certificates in the following store**, select **Trusted Root Certification Authorities**, and then click **Next**.
10. On the **Completing the Certificate Import Wizard** page, click **Finish**, and then click **OK** to close the success message.
11. Close the Group Policy Management Editor.
12. Close Group Policy Management.
13. On **TREY-DC1**, open **File Explorer**, and then go to ***\\LON-DC1\CertEnroll***
14. Right-click **LON-DC1.Adatum.com_AdatumCA.crt**, and then click **Install Certificate**.
15. In the **Certificate Import Wizard**, on the **Welcome to the Certificate Import Wizard** page, click **Local Machine**, and then click **Next**.
16. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Browse**.
17. In the **Select Certificate Store** window, click **Trusted Root Certification Authorities**, and then click **OK**.
18. On the **Certificate Store** page, click **Next**.
19. On the **Completing the Certificate Import Wizard** page, click **Finish**, and then

click **OK** to close the success message.
20. Close File Explorer.
21. On **LON-SVR1**, click **Start** and then click **Windows PowerShell**.
22. At the **Windows PowerShell** command prompt, type ***gpupdate*** and then press Enter.
23. Close Windows PowerShell.

Note: *If you obtain certificates from a trusted certification authority (CA), you do not need to configure a certificate trust between the organizations.*

Task 3: Request and install a certificate for the web server

1. On **LON-SVR1**, open **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In Microsoft Internet Information Services (IIS) Manager, click **LON-SVR1 (ADATUM\Administrator)**, and then double-click **Server Certificates**.
3. In the **Actions** pane, click **Create Domain Certificate**.
4. In the **Create Certificate** wizard, on the **Distinguished Name Properties** page, type the following information, and then click **Next**:
o Common name: ***lon-svr1.adatum.com***
o Organization: ***A. Datum Corporation***
o Organizational unit: ***IT***
o City/locality: ***London***
o State/Province: ***England***
o Country/region: ***GB***
5. On the **Online Certification Authority** page, click **Select**.
6. In the **Select Certification Authority** page, click **AdatumCA**, and then click **OK**.
7. On the **Online Certification Authority** page, in the **Friendly name** box, type ***AdatumTestApp Certificate*** and then click **Finish**.
8. In IIS Manager, expand **LON-SVR1 (ADATUM\Administrator)**, expand **Sites**, click **Default Web Site**, and then in the **Actions** pane, click **Bindings**.
9. In the **Site Bindings** window, click **Add**.
10. In the **Add Site Binding** window, in the **Type** list, select **https**.
11. In the **SSL certificate** list, select **AdatumTestApp Certificate**, and then click **OK**.
12. In the **Site Bindings** window, click **Close**.
13. Close IIS Manager.

***Results**: After completing this exercise, you should have enabled DNS resolution and certificate trusts between the domains successfully. Also, you will have enabled an SSL certificate for the website and validated access to it.*

Exercise 2: Installing and configuring AD FS

Task 1: Create a DNS record for AD FS

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the **New Host** window, in the **Name** box, type ***adfs***
5. In the **IP address** box, type ***172.16.0.10*** and then click **Add Host**.
6. In the **DNS** window, click **OK**.
7. Click **Done**, and then close DNS Manager.

Task 2: Install AD FS

1. On **LON-DC1**, click **Start**, right-click **Windows PowerShell**, and then click **Run as Administrator**.
2. At the command prompt, type the following command, and then press Enter:

Add-KdsRootKey –EffectiveTime ((Get-Date).AddHours(-10))

This command creates the Microsoft Group Key Distribution Service root key to generate group Managed Service Account (gMSA) passwords for the account that you will use later in this lab. You should receive a globally unique identifier (GUID) as a response to this command.

3. Click **Start**, click **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**, click **LON-DC1.Adatum.com**, and then click **Next**.
7. On the **Select server roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.

8. On the **Select features** page, click **Next**.
9. On the **Active Directory Federation Services (AD FS)** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the installation is complete, click **Close**.

Task 3: Configure AD FS

1. On **LON-DC1**, in **Server Manager**, click the **Notifications** icon, and then click **Configure the federation service on this server**.
2. 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**.
3. On the **Connect to Active Directory Domain Services** page, click **Next** to use **Adatum\Administrator** to perform the configuration.
4. On the **Specify Service Properties** page, in the **SSL Certificate** list, select **adfs.adatum.com**.
5. In the **Federation Service Display Name** box, type **A. Datum Corporation**, and then click **Next**.
6. On the **Specify Service Account** page, click **Create a Group Managed Service Account**.
7. In the **Account Name** box, type ***ADFSService*** and then click **Next**.
8. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
9. On the **Review Options** page, click **Next**.
10. On the **Pre-requisite Checks** page, click **Configure**.
11. On the **Results** page, click **Close**.

Note: *The adfs.adatum.com certificate was preconfigured for this task. In your own environment, you must obtain this certificate.*

Task 4: Verify AD FS functionality

1. On **LON-CL1**, click **Start**, click **Windows Accessories**, and then click **Internet Explorer**.
2. In Internet Explorer, on the address bar, type ***https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml*** and then press Enter.
3. Verify that the file loads, and then close Internet Explorer.

***Results**: After completing this exercise, you should have installed and configured AD FS successfully. You also should have verified that it is functioning by viewing the contents of the **FederationMetaData.xml** file.*

Exercise 3: Configuring an internal application for AD FS

Task 1: Configure the Active Directory claims provider trust

1. On **LON-DC1**, in Server Manager, click **Tools**, and then click **AD FS Management**.
2. In the **AD FS** management console, click **Claims Provider Trusts**.
3. In the list of **Claims Provider Trusts**, right-click **Active Directory**, and then click **Edit Claim Rules**.
4. In the **Edit Claims Rules for Active Directory** window, on the **Acceptance Transform Rules** tab, click **Add Rule**.
5. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** list, select **Send LDAP Attributes as Claims**, and then click **Next**.
6. On the **Configure Rule** page, in the **Claim rule name** box, type ***Outbound LDAP Attributes Rule***
7. In the **Attribute store** list, select **Active Directory**.
8. In the **Mapping of LDAP attributes to outgoing claim types** section, select the following values for the **LDAP Attribute** and the **Outgoing Claim Type**, and then click **Finish**:
   - o E-Mail-Addresses: **E-Mail Address**
   - o User-Principal-Name: **UPN**
   - o Display-Name: **Name**
9. In the **Edit Claim Rules for Active Directory** window, click **OK**.

Task 2: Configure the application to trust incoming claims

1. On **LON-SVR1**, open **Server Manager**, click **Tools**, and then click **Windows Identity Foundation Federation Utility**.
2. On the **Welcome to the Federation Utility Wizard** page, in the **Application configuration location** box, type: ***C:\inetpub\wwwroot\AdatumTestApp\web.config*** for the location of the sample **web.config** file.

3. In the **Application URI** box, type: **https://lon-svr1.adatum.com/AdatumTestApp/** to indicate the path to the sample application that will trust the incoming claims from the federation server, and then click **Next**.
4. On the **Security Token Service** page, click **Use an existing STS**, and then in the **STS WS-Federation metadata document location** box, type **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**. Click **Next**.
5. On the **STS signing certificate chain validation error** page, click **Disable certificate chain validation**, and then click **Next**.
6. On the **Security token encryption** page, click **No encryption**, and then click **Next**.
7. On the **Offered claims** page, review the claims that will be offered by the federation server, and then click **Next**.
8. On the **Summary** page, review the changes that will be made to the sample application by the **Federation Utility Wizard**, scroll through the items to understand what each item is doing, and then click **Finish**.
9. In the **Success** window, click **OK**.

Task 3: Configure a relying party trust for the claims-aware application

- On **LON-DC1**, at the **Windows PowerShell** command prompt, type the following command to add a relying party trust, and then press Enter:

Add-ADFSRelyingPartyTrust –Name 'A. Datum Corporation Test App' –MetadataURL 'https://lon-svr1.adatum.com/AdatumTestApp/federationmetadata/2007-06/federationmetadata.xml'

Task 4: Configure claim rules for the relying party trust

1. On **LON-DC1**, in the **AD FS** management console, in the list of **Relying Party Trusts**, click **A. Datum Corporation Test App**, and then select **Edit Claim Issuance policy**.
2. In the **Edit Claim Issuance Policy for A. Datum Corporation Test App** window, on the **Issuance Transform Rules** tab, click **Add Rule**.
3. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
4. In the **Claim rule name** box, type ***Pass through Windows account name***
5. In the **Incoming claim type** list, click **Windows account name**, and then click

Finish.
6. On the **Issuance Transform Rules** tab, click **Add Rule**.
7. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
8. In the **Claim rule name** box, type ***Pass through E-Mail Address***.
9. In the **Incoming claim type** list, click **E-Mail Address**, and then click **Finish**.
10. On the **Issuance Transform Rules** tab, click **Add Rule**.
11. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
12. In the **Claim rule name** box, type ***Pass through UPN***.
13. In the **Incoming claim type** list, click **UPN**, and then click **Finish**.
14. On the **Issuance Transform Rules** tab, click **Add Rule**.
15. In the **Claim rule template** dialog box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
16. In the **Claim rule name** box, type ***Pass through Name***.
17. In the **Incoming claim type** list, click **Name**, and then click **Finish**.
18. On the **Issuance Transform Rules** tab, click **OK**.
19. In the **AD FS** management console, in the list of **Relying Party Trusts**, click **A. Datum Corporation Test App**, and then select **Edit Access Control Policy**.
20. In **Edit Access Control Policy for A. Datum Corporation Test App**, select **Permit everyone**, and click **OK**.

Task 5: Test access to the claims-aware application

1. On **LON-CL1**, open **Internet Explorer**.
2. In Internet Explorer, on the address bar, type: ***https://lon-svr1.adatum.com/AdatumTestApp/*** and then press Enter.

Note: *It is critical to use the trailing forward slash (/) in the URL for step 2.*

3. In the **Windows Security** window, sign in as **Adatum\Adam** with the password **Pa55w.rd**.
4. Review the claim information that the application displays.
5. Close Internet Explorer.

Task 6: Configure Internet Explorer to pass local credentials to the application automatically

1. On **LON-CL1**, click **Start**, type **Internet Options**, and then click **Internet Options**.

2. In the **Internet Properties** window, on the **Security** tab, click **Local intranet**, and then click **Sites**.
3. In the **Local intranet** window, click **Advanced**.
4. In the **Local intranet** window, in the **Add this website to the zone** box, type: ***https://adfs.adatum.com*** and then click **Add**.
5. In the **Add this website to the zone** box, type ***https://lon-svr1.adatum.com*** click **Add**, and then click **Close**.
6. In the **Local intranet** window, click **OK**.
7. In the **Internet Properties** window, click **OK**.
8. On **LON-CL1**, open **Internet Explorer**.
9. In Internet Explorer, on the address bar, type: **https://lon-svr1.adatum.com/AdatumTestApp/** and then press Enter.

Note: *It is critical to use the trailing forward slash (/) in the URL for step 9.*

10. Notice that you were not prompted for credentials.
11. Review the claim information that is displayed by the application.
12. Close Internet Explorer.

Results*: After completing this exercise, you should have configured AD FS successfully to support application authentication.*

Exercise 4: Configuring AD FS for federated business partners

Task 1: Create a DNS record for AD FS at Trey Research

1. On **TREY-DC1**, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **TREY-DC1**, expand **Forward Lookup Zones**, and then click **TreyResearch.net**.
3. Right-click **TreyResearch.net**, and then click **New Host (A or AAAA)**.
4. In the **New Host** window, in the **Name** box, type ***adfs***
5. In the **IP address** box, type ***172.16.10.10*** and then click **Add Host**.
6. In the **DNS** window, click **OK**.
7. Click **Done**, and then close DNS Manager.

Task 2: Create a certificate for AD FS at Trey Research

1. On **TREY-DC1**, in Server Manager, click **Tools**, and then click **Internet Information Services (IIS) Manager**.

2. In IIS Manager, click **TREY-DC1 (TREYRESEARCH\Administrator)**, and then double-click **Server Certificates**.
3. In the **Actions** pane, click **Create Domain Certificate**.
4. In the **Create Certificate** window, on the **Distinguished Name Properties** page, type the following information, and then click **Next**:
o Common name: ***adfs.TreyResearch.net***
o Organization: ***Trey Research***
o Organizational unit: ***IT***
o City/locality: ***London***
o State/Province: ***England***
o Country/region: ***GB***
5. On the **Online Certification Authority** page, click **Select**.
6. In the **Select Certification Authority** window, click **TreyResearchCA**, and then click **OK**.
7. On the **Online Certification Authority** page, in the **Friendly name** box, type ***adfs.TreyResearch.net*** and then click **Finish**.
8. Close IIS Manager.

Task 3: Install AD FS for Trey Research

1. On **TREY-DC1**, click **Start**, right-click **Windows PowerShell** and then click **Run as Administrator**.
2. At the command prompt, type the following command, and then press Enter:
Add-KdsRootKey –EffectiveTime ((Get-Date).AddHours(-10))
This command creates the Key Distribution Service root key to generate gMSA passwords for the account that you will use later in this lab. You should receive a GUID as a response to this command.
3. Click **Start**, click **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**, click **TREY-DC1.TreyResearch.net**, and then click **Next**.
7. On the **Select server roles** page, select the **Active Directory Federation**

Services check box, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **Active Directory Federation Services (AD FS)** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. When the installation completes, click **Close**.

Task 4: Configure AD FS for Trey Research

1. On **TREY-DC1**, in Server Manager, click the **Notifications** icon, and then click **Configure the federation service on this server**.
2. 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**.
3. On the **Connect to Active Directory Domain Services** page, click **Next** to use **TreyResearch\Administrator** to perform the configuration.
4. On the **Specify Service Properties** page, in the **SSL Certificate** list, select **adfs.treyresearch.net**.
5. In the **Federation Service Display Name** box, type ***Trey Research*** and then click **Next**.
6. On the **Specify Service Account** page, click **Create a Group Managed Service Account**.
7. In the **Account Name** box, type ***ADFSService*** and then click **Next**.
8. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
9. On the **Review Options** page, click **Next**.
10. On the **Pre-requisite Checks** page, click **Configure**.
11. On the **Results** page, click **Close**.
12. Right-click **Start**, select **Shut down or sign out**, select **Restart,** and then click **Continue**.
13. Wait until **TREY-DC1** is online before continuing to the next step.

Task 5: Configure a claims provider trust for the Trey Research AD FS server

1. On **LON-DC1**, at the **Windows PowerShell** command prompt, type the following command to add a claims provider trust, and then press Enter:
Add-AdfsClaimsProviderTrust –Name 'Trey Research' –MetadataUrl 'https://adfs.treyresearch.net/federationmetadata/2007-06/federationmetadata.xml'

2. Because of compatibility issues with Internet Explorer 11 (including Microsoft Edge), type the following command to disable token binding in AD FS, and then press Enter: ***Set-AdfsProperties –IgnoreTokenBinding $true***
3. On **LON-DC1**, open the **AD FS** management console.
4. In the list of **Claims Provider Trusts**, right-click **Trey Research**, and then select **Edit Claim Rules…**.
5. In the **Edit Claim Rules for Trey Research** window, on the **Acceptance Transform Rules** tab, click **Add Rule**.
6. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** list, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
7. On the **Configure Rule** page, in the **Claim rule name** box, type ***Pass through Windows account name***
8. In the **Incoming claim type** list, select **Windows account name**.
9. Select **Pass through all claim values**, and then click **Finish**.
10. In the **AD FS Management** dialog box, click **Yes** to acknowledge the warning.
11. In the **Edit Claim Rules for Trey Research** window, click **OK**, and then close the **AD FS** management console.

Task 6: Configure a relying party trust for the A. Datum Corporation application

1. On **TREY-DC1**, open the **Windows PowerShell** command prompt.
2. At the **Windows PowerShell** command prompt, type the following to create a new relying party trust, and then press Enter:
Add-ADFSRelyingPartyTrust –Name 'A. Datum Corporation' –MetadataURL 'https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml'
3. In the Server Manager, click **Tools**, and then click **AD FS Management**.
4. In the **AD FS** management console, click **Relying Party Trusts**.
5. In the **Actions** pane, click **Edit Claim Issuance Policy**.
6. In the **Edit Claim Issuance Policy for A. Datum Corporation** window, click **Add Rule**.
7. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
8. On the **Configure Rule** page, in the **Claim rule name** box, type ***Pass through***

Windows account name

9. In the **Incoming claim type** list, select **Windows account name**.
10. Click **Pass through all claim values**, click **Finish**, and then click **OK**.
11. In the **Edit Claim Issuance Policy for A. Datum Corporation** window, click **OK**.
12. In the list of **Relying Party Trusts**, click **A. Datum Corporation**, and then select **Edit Access Control Policy**.
13. In **Edit Access Control Policy for A. Datum Corporation**, select **Permit everyone**, and click **OK**.
14. Close the **AD FS** management console.

Task 7: Verify access to the website

1. On **TREY-DC1**, in Internet Explorer, open **Internet Options**, select **Privacy**, and then select **Sites**.
2. On the **Per Site Privacy Actions** page, in the **Address of website** box, type ***adatum.com*** click **Allow**, click **OK** to close the **Per Site Privacy Actions** page, and then click **OK** to close the **Internet Options** window.
3. In Internet Explorer, on the address bar, type: ***https://lon-svr1.adatum.com/adatumtestapp/*** and then press Enter.
4. On the **A. Datum Corporation** page, click **Trey Research**.

Note: *If you receive the error message* ***This page cannot be displayed****, click* ***Refresh*** *and try this step again.*

5. In the **Windows Security** dialog box, sign in as **TreyResearch\April** with the password **Pa55w.rd**.
6. After the application loads, close Internet Explorer.
7. Open **Internet Explorer**.
8. In Internet Explorer, on the address bar, type: ***https://lon-svr1.adatum.com/adatumtestapp/*** and then press Enter.
9. In the **Windows Security** dialog box, sign in as **TreyResearch\April** with the password **Pa55w.rd**.
10. Close Internet Explorer.

Note: *You are not prompted for a home realm on the second access. After a user selects a home realm and a realm authority authenticates that user, the relying party's federation server issues a* ***_LSRealm*** *cookie. The default lifetime for the*

cookie is 30 days. Therefore, to sign in multiple times, you should delete that cookie after each sign-in attempt to return to a clean state.

Task 8: Configure issuance-authorization claim rules to allow access only for specific groups

1. On **TREY-DC1**, in Server Manager, click **Tools**, and then click **AD FS Management**.
2. In the **AD FS** management console, click **Relying Party Trusts**.
3. Right-click **A. Datum Corporation**, and then click **Edit Claim Issuance Policy**.
4. In the **Edit Claim Issuance Policy for A. Datum Corporation** window, on the **Issuance Transform Rules** tab, click **Remove Rule**, and then click **Yes**.
5. Click **Add Rule**.
6. In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim** and then click **Next**.
7. On the **Claim rule name** box, type ***Allow Production Members***
8. On the **Incoming claim type**, select **Group**.
9. Click **Pass through only a specific claim value**, and then in the Incoming claim value, type ***TreyResearch-Production***
10. Click **Finish** and then click **OK**.
11. In the **AD FS** management console, click **Claims Provider Trusts**, right-click **Active Directory**, and then click **Edit Claim Rules**.
12. In the **Edit Claim Rules for Active Directory** window, click **Add Rule**.
13. In the **Add Transform Claim Rule Wizard**, on the **Select Rule Template** page, in the **Claim rule template** box, select **Send Group Membership as a Claim**, and then click **Next**.
14. On the **Configure Rule** page, in the **Claim rule name** box, type ***Production Group Claim***
15. To set the **User's group**, click **Browse**, type ***Production*** and then click **OK**.
16. In the **Outgoing claim type** box, select **Group**.
17. In the **Outgoing claim value** box, type ***TreyResearch-Production*** and then click **Finish**.
18. In the **Edit Claim Rules for Active Directory** window, click **OK**.
19. Close the **AD FS** management console.

Task 9: Verify access to the website with the group restrictions

1. On **TREY-DC1**, in Internet Explorer, on the address bar, type:

https://lon-svr1.adatum.com/adatumtestapp/

2. In the **Windows Security** dialog box, sign in as ***TreyResearch\Ben*** with the password ***Pa55w.rd***
3. Verify that you can access the application because Ben is a member of the TreyResearch\Production group.
4. Close Internet Explorer.

Results*: After completing this exercise, you should have successfully configured access for a claims-aware application in a partner organization.*

Task 10: Prepare for the next module

When you finish the lab, revert the VMs to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742B-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742B-LON-SVR1**, **20742B-TREY-DC1**, and **20742B-LON-CL1**.