Module 1 – Web Application Proxy (WAP)
Estimated Time: 120 minutes

The remote access deployment is working well at A. Datum Corporation, but IT management also wants to enable access to some internal applications for users from partner companies. These users should not have access to any internal resources except for the specified applications. You must implement and test Web Application Proxy for these users. Furthermore, administrators at A. Datum should be able to remotely manage servers in the internal network in the most secure manner possible.

**NOTE:** To save time in the lab, we have completed Tasks 1 – 7 for you. You can start the lab on Task 8. But, please take a minute to read the other tasks so you get a complete picture of what needs to be done to configure WAP.

**Objectives**
After completing this lab, students will be able to:

- Implement Web Application Proxy.
- Validate the Web Application Proxy deployment.

**Lab environment**
The lab consists of the following computers:

- **LON-DC1** (172.16.0.10) – a Windows Server 2016 domain controller in the adatum.com single-domain forest. You will use it to host the Enterprise Certification Authority.

  - In general, you should avoid using AD domain controllers to host PKI roles. We are not following this approach in the lab strictly in order to optimize use of lab VMs. The process of deploying and configuring a Certification Authority server would be identical when using a domain member server.

- **LON-SVR1** (172.16.0.11) – a Windows Server 2016 domain member server with Remote Server Administrative tools installed. This server will host the Active Directory Federation Services server role.

- **LON-SVR2** (172.16.0.12) – a Windows Server 2016 domain member server with Remote Server Administrative tools installed. This server will host the Web Application Proxy role service and will function as a Certificate Revocation List (CRL) Distribution Point for external clients.

  - You might want to consider implementing WAP on a workgroup computer. The procedure described in this lab would, for the most part, apply in such cases as well.

- **LON-SVR3** (172.16.0.13) – a Windows Server 2016 domain member server with Remote Server Administrative tools installed. This will be used to host a Web application published via Web Application Proxy.

- **LON-CL1** (172.16.0.101) – a Windows 10 Pro or Enterprise version 1607 (or newer) domain member computer

All computers have Windows PowerShell Remoting enabled and have Internet connectivity.
Exercise 1: Implement Web Application Proxy.

In this exercise, you will step through implementing Web Application Proxy in a Windows Server 2016 environment. The main tasks for this exercise are as follows:

1. Prepare LON-SVR2 to become a CRL Distribution Point (Completed)
2. Configure DNS on LON-DC1 (Completed)
3. Install and configure an Enterprise CA on LON-DC1 (Completed)
4. Enroll LON-SVR1 for a certificate issued by Enterprise CA (Completed)
5. Install the AD FS server role on LON-SVR1 (Completed)
6. Install a sample Web application on LON-SVR3 (Completed)
7. Configure an AD FS relying party on LON-SVR1 (Completed)
8. Install AD FS SSL certificate on LON-SVR2
9. Install Web App certificate on LON-SVR2
10. Install adatum-root-CA root certificate on LON-SVR2
11. Install the WAP role service on LON-SVR2
12. Publish the sample Web application on LON-SVR2

▶ Task 1: Prepare LON-SVR2 to become a CRL Distribution Point (Completed)

1. Sign in to the LON-SVR2 Windows Server 2016 lab virtual machine with the following credentials:
   - USERNAME: ADATUM\Administrator
   - PASSWORD: Pa55w.rd

2. On LON-SVR2, click Start, in the Start menu, right-click Windows PowerShell ISE, in the right-click menu, click More and click Run as administrator.

3. From the Administrator: Windows PowerShell ISE window, create a file share named certdata and grant Read and Change Permissions share level permissions and Full Control file system permissions on the certdata folder to the LON-DC1 computer account by running the following:

   ```powershell
   New-Item -Path c:\certdata -ItemType Directory
   New-SMBShare -Name certdata -Path 'c:\certdata' -ChangeAccess 'ADATUM\LON-DC1$'
   Grant-SmbShareAccess -Name certdata -AccessRight Change -AccountName 'Administrators' -Force
   $acl = Get-Acl 'c:\certdata'
   $acl.SetAccessRule($car)
   Set-Acl 'c:\certdata' $acl
   ```

4. Click Start and then click Server Manager.

5. Click Manage and, in the drop-down menu, click Add Roles and Features.

6. If the Before You Begin page appears, select the Skip this page by default check box, and then click Next.

7. On the Select installation type page, ensure that the Role-based or feature-based installation option is selected and click Next.

8. On the Server destination server page, ensure that LON-SVR2 is selected and click Next.
9. On the Select server roles page, expand the **Web Server (IIS)** entry and click the **Web Server (IIS)** check box. When prompted whether to add features that are required for Web Server (IIS), click **Add Features**, and then click **Next**.

10. On the Select features page, click **Next**.

11. On the Web Server Role (IIS) page, click **Next**.

12. On the Select role services page, accept the default settings and click **Next**.

13. On the Confirm installation selections page, select the **Restart the destination server automatically if required** checkbox, when prompted to confirm, click **Yes**, and click **Install**.

14. Wait for the installation to complete and, on the Installation progress page, click **Close**.

15. On LON-SVR2 click **Start**, in the Start menu click **Windows Administrative Tools** and click **Internet Information Services (IIS) Manager**.

16. In the Internet Information Services (IIS) Manager console, expand the Sites folder, right click **Default Web Site**, and, in the right-click menu, click **Add Virtual Directory**.

17. In the Add Virtual Directory dialog box, set **Alias** to **certdata** and **Physical path** to **C:\certdata** and click **OK**.

**► Task 2: Configure DNS on LON-DC1 (Completed)**

1. Sign in to the LON-DC1 Windows Server 2016 lab virtual machine with the following credentials:
   - **USERNAME**: ADATUM\Administrator
   - **PASSWORD**: Pa55w.rd

2. Click **Start** and then click **Server Manager**.

3. In Server Manager, click **Tools** and then click **DNS**.

4. In the DNS Manager console, navigate to the **Adatum.com** zone.

5. Right-click **Adatum.com** and, in the right-click menu, click **New Host (A or AAAA)**.

6. In the **New Host** dialog box, type the following and click **OK**:
   - **Name**: adfs
   - **IP address**: 172.16.0.11

7. In the **DNS** dialog box, click **OK**.

8. In the **New Host** dialog box, type the following and click **OK**:
   - **Name**: cdp
   - **IP address**: 172.16.0.12

9. In the **DNS** dialog box, click **OK**.

10. In the **New Host** dialog box, type the following and click **OK**:
    - **Name**: webapp
• IP address: 172.16.0.13

11. In the **DNS** dialog box, click **OK**.

12. In the **New Host** dialog box, click **Done**.

**Task 3: Install and configure an Enterprise CA on LON-DC1 (Completed)**

1. From the LON-DC1 Windows Server 2016 lab virtual machine, in Server Manager, in the **Manage** menu, click **Add Roles and Features**. This will start the **Add Roles and Features Wizard**.

2. On the **Select installation type** page, ensure that the **Role-based or feature-based installation** option is selected and click **Next**.

3. On the **Server destination server** page, ensure that **LON-DC1** is selected and click **Next**.

4. On the **Select server roles** page, select the **Active Directory Certificate Services** check box. When prompted whether to add features that are required for Active Directory Certificate Services, click **Add Features**, and then click **Next**.

5. On the **Select features** page, click **Next**.

6. On the **Active Directory Certificate Services** page, click **Next**.

7. On the **Select role services** page, ensure that the **Certification Authority** check box is selected and then click **Next**.

8. On the **Confirm installation selections** page, click **Install**. Wait for the installation to complete.

9. Once the installation completes, click **Configure Active Directory Certificate Services on the destination server**.

10. On the **Specify credentials to configure role services**, click **Next**.

11. On the **Select Role Services to configure** page, select the **Certification Authority** checkbox and click **Next**.

12. On the **Specify the setup type of the CA** page, click **Enterprise CA**, and then click **Next**.

13. On the **Specify the type of the CA** page, ensure that **Root CA** is selected, and then click **Next**.

14. On the **Specify the type of the private key** page, ensure that the **Create a new private key** option is selected and then click **Next**.

15. On the **Specify the cryptographic options** page, set the key length to **4096**, accept the remaining settings with their default values and click **Next**.

16. On the **Specify the name of the CA** page, specify the following settings and click **Next**:
   - **Common name for this CA**: **adatum-root-CA**
   - **Distinguished name suffix**: **DC=adatum,DC=com**
   - **Preview of distinguished name**: **CN=adatum-root-CA,DC=adatum,DC=com**

17. On the **Specify the validity period** page, accept the default validity period and click **Next**.

18. On the **Specify the database locations** page, accept the default location of the certificate database and its log and click **Next**.
19. On the Confirmation page, click **Configure**.

20. Wait until the configuration completes and click **Close**.


22. In Server Manager, from the Tools menu, start **Certification Authority** console.

Next, you will modify the default Certificate Revocation List (CRL) Distribution Point (DP) settings in order to facilitate CRL verification by external computers in Exercise 2 of this lab.

23. In the Certification Authority console, right-click the **adatum-root-CA** node and, in the right-click menu, click **Properties**.

24. In the **Properties** dialog box, switch to the **Extension** tab, ensure that **CRL Distribution Point (CDP)** entry appears in the **Select extension** drop down list, and click **Add**.

25. In the Add Location dialog box, in the Location text box, specify the following

   `http://cdp.adatum.com/certdata/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`

   and click **OK**. You can use the **Insert** command button to insert individual entries in the **Variable** drop-down list into the location string, rather than typing them.

26. Back on the Extensions tab, with the newly added CDP entry selected, select the **Include in the CDP extensions of issued certificates** and the **Include in CRLs. Client use this to find Delta CRL locations** checkboxes.

27. Ensure that **CRL Distribution Point (CDP)** entry appears in the **Select extension** drop down list and click **Add**.

28. In the Add Location dialog box, in the Location text box, specify the following

   `file://cdp.adatum.com/certdata/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl`

   and click **OK**. You can use the **Insert** command button to insert individual entries in the **Variable** drop-down list into the location string, rather than typing them.

29. Back on the Extensions tab, with the newly added CDP entry selected, select the **Publish CRLs to this location** and **Publish Delta CRLs to this location** checkboxes.

30. In the Select extension drop down list, click the **Authority Information Access (AIA)** entry and click **Add**.

31. In the Add Location dialog box, in the Location text box, specify

   `http://cdp.adatum.com/certdata/<ServerDNSName><CaName><CertificateName>.crt`

   and click **OK**. You can use the **Insert** command button to insert individual entries in the **Variable** drop-down list into the location string, rather than typing them.

32. Back on the Extensions tab, with the newly added CDP entry selected, select the **Include in AIA extensions of issued certificates** checkbox and click **OK**.

33. When prompted to restart Active Directory Certificate Services, click **Yes**.

34. Back in the Certification Authority console, expand the **adatum-root-CA** node, right-click **Revoked Certificates** folder, click **All Tasks** and click **Publish**.

35. In the Publish CRL dialog box, click **OK**.

Next, you will create a certificate template that you will subsequently use to enroll the domain member server on which you will install the sample web application.
36. In the Certification Authority console, expand the adatum-root-CA node, right-click Certificate Templates and, in the right-click menu, click Manage. This will open the Certificate Templates console.

37. In the Certificate Templates console, right-click the Web Server template and select Duplicate Template.

38. In Properties of New Template window, on the Compatibility tab, in the Compatibility Settings section, in the Certification Authority drop down list, click Windows Server 2016. When prompted, in the Resulting changes dialog box, click OK.


40. Switch to the Security tab and click Add.

41. In the Enter the object names to select text box, type Domain Computers and click OK.

42. With Domain Computers selected, check Read, Enroll, and Autoenroll permissions.

43. On the Request Handling tab, check the Allow private key to be exported box.

44. On the General tab, change the template display name to Adatum Web Server.

45. Click OK to save the new template.

46. Switch back to the Certification Authority console, right-click the Certificate Templates folder, click New, and then click Certificate Template to Issue.

47. In the Enable Certificate Templates dialog box, click Adatum Web Server and click OK.

 ► Task 4: Enroll LON-SVR1 for a certificate issued by Enterprise CA (Completed)

1. Sign in to the LON-SVR1 Windows Server 2016 lab virtual machine with the following credentials:
   - USERNAME: ADATUM\Administrator
   - PASSWORD: Pa55w.rd

2. While signed in to LON-SVR1 as ADATUM\Administrator, click Start, right-click Windows PowerShell, click More and then click Run as Administrator.

3. From the Administrator: Windows PowerShell window, type the following and press Enter:

   gpupdate /force
certlm

   This will open the Microsoft Management Console (MMC) with the Certificates - Local Computer snap-in loaded.

4. Expand the Certificates – Local Computer top level node, right-click the Personal folder, click All Tasks, and click Request New Certificate. This will start the Certificate Enrollment wizard.

5. On the Before You Begin page, click Next.
6. On the **Select Certificate Enrollment Policy** page, ensure that **Active Directory Enrollment Policy** is selected and click **Next**.

7. On the **Request Certificates** page, select the checkbox next to the **Adatum Web Server** certificate, click **Details** to view properties of the certificate, and click **Properties**.

8. In the **Certificate Properties** window, on the General tab, in the Friendly name section text box, type **Adatum AD FS**.

9. In the **Certificate Properties** window, click the **Subject** tab. On the Subject tab, in the Subject name section, in the Type drop-down list, click **Common name**, in the Value text box, type ***.adatum.com**, and click **Add**.

10. In the Alternative name section, in the Type drop-down list, click **DNS** and, add the following names by typing them in the Value text box and clicking **Add** each time:
   - ***.adatum.com**
   - **adfs.adatum.com**
   - **enterpriseregistration.adatum.com**
   - **certauth.adfs.adatum.com**

11. Click the **Private Key** tab.

12. Under Key options, ensure the **Make private key exportable** option is checked and click **OK**.

13. Back on the Request Certificates wizard page, ensure the checkbox for the template is checked and click **Enroll**.

14. On the Certificate Installation Results page, click **Finish**.

15. Back in the Certificates console, expand the **Trusted Root Certification Authorities** folder and click **Certificates**.

16. Right-click **adatum-root-CA** entry, in the right-click menu, click **All Tasks** and then click **Export**. This will start the Certificate Export Wizard.

17. On the Welcome to the Certificate Export Wizard page, click **Next**.

18. On the Export File format page, click **Next**.

19. On the File to Export page, in the **File name** text box, type **C:\adatum-root-CA.cer** and click **Next**.

20. On the Completing the Certificate Export Wizard page, click **Finish**.

21. In the **Certificate Export Wizard** dialog box, click **OK**.

---

**Task 5: Install the AD FS server role on LON-SVR1 (Completed)**

1. Switch back to LON-DC1, click **Start**, in the **Start** menu, right-click **Windows PowerShell**, in the right-click menu, click **More** and click **Run as administrator**.

2. From the **Administrator: Windows PowerShell** window, create the Key Distribution Services KDS Root Key by running the following:

```
Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
```
This will allow you to use a Managed Service Account when deploying AD FS.

3. Switch to the console of LON-SVR1,

4. Click Start and then click Server Manager.

5. From the Manage menu in Server Manager, select Add Roles and Features. This will launch Add Roles and Features Wizard.

6. On the Before you begin page, click Next

7. On the Select installation type page, ensure that Role-based or feature-based installation option is selected and click Next.

8. On the Select destination server page, ensure that the local server is selected and click Next.

9. On the Server Roles page, select the Active Directory Federation Services checkbox and click Next

10. On the Select features page, click Next.

11. On the Active Directory Federation Services page, click Next

12. On the Confirm installation selections page, select the Restart the destination server automatically if required checkbox, click Yes when prompted for confirmation, and click Install. Wait for the installation to complete.

13. Once the installation completes, on the Installation progress page, click Configure the federation service on this server. This will start Active Directory Federation Services Configuration Wizard.

14. On the Welcome page, ensure that the Create the first federation server in a federation server farm option is selected and click Next.

15. On the Connect to AD DS page, accept the default settings and click Next.


17. On the Specify Service Account page, click the Create a Group Managed Service Account option, in the Account Name text box, type gmsvc-adfs, and then click Next.

18. On the Specify Configuration Database page, ensure that the Create a database on this server using Windows Internal Database option is selected and then click Next.


20. On the Pre-requisite Checker page, verify that all prerequisites have been satisfied and click Configure.

21. Wait until the configuration completes, review the detailed operation results, and click Close.


► Task 6: Install a sample Web application on LON-SVR3 (Completed)

1. Sign in to the LON-SVR3 Windows 2016 lab virtual machine with the following credentials:
• USERNAME: ADATUM\Administrator
• PASSWORD: Pa55w.rd

2. While signed in to LON-SVR3 as ADATUM\Administrator, click Start, in the Start menu, right-click Windows PowerShell, in the right-click menu, click More and click Run as administrator.

3. From the Administrator: Windows PowerShell window, type the following and press Enter:
   ```powershell
gpupdate /force
certlm
```
   This will open the Microsoft Management Console (MMC) with the Certificates - Local Computer snap-in loaded.

4. Expand the Certificates – Local Computer top level node, right-click the Personal folder, click All Tasks, and click Request New Certificate. This will start the Certificate Enrollment wizard.

5. On the Before You Begin page, click Next.

6. On the Select Certificate Enrollment Policy page, ensure that Active Directory Enrollment Policy is selected and click Next.

7. On the Request Certificates page, select the checkbox next to the Adatum Web Server certificate, click Details to view properties of the certificate, and click Properties.

8. In the Certificate properties window, on the General tab, in the Friendly name section text box, type Adatum Sample Web App.

9. In the Certificate properties window, on the Subject tab, in the Subject name section, in the Type drop-down list, click Common name, in the Value text box, type webapp.adatum.com, and click Add.

10. In the Alternative name section, in the Type drop-down list, click DNS and, add the following names by typing them in the Value text box and clicking Add each time:
    - webapp.adatum.com
    - LON-SVR3.adatum.com

11. Click the Private Key tab.

12. Under Key options, ensure the Make private key exportable option is checked and click OK.

13. Back on the Request Certificates wizard page, ensure the checkbox for the template is checked and click Enroll.


15. From the Administrator: Windows PowerShell window, type the following and press Enter:
   ```powershell
   ```
   This installs all role services and features required by the sample application and, if needed, restart the operating system.
16. If LON-SVR3 restarts, sign in back with the ADATUM\Administrator user account, start Windows PowerShell as administrator, and from the **Administrator: Windows PowerShell** window, run the following:

```powershell
New-ADUser -Name Svc_AppPool -AccountPassword (ConvertTo-SecureString -AsPlainText "Pa55w.rd1234" -Force) -Company Adatum -Description "App Pool Account" -DisplayName Svc_AppPool -Enabled $true -PasswordNeverExpires $true -SamAccountName Svc_AppPool -UserPrincipalName Svc_AppPool@adatum.com
```

This creates a new domain user that will be used to provide the security context for the AppPool in which our sample application will be running.

17. From the **Administrator: Windows PowerShell ISE** window, run the following:

```powershell
Add-LocalGroupMember -Group IIS_IUSRS -Member ADATUM\Svc_AppPool
```

This adds the newly created user to the IIS_IUSRS group on the local server.

18. Start Internet Explorer and download the sample app from https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/telligent.evolution.components.attachments/01/8598/00/00/03/64/54/88/SampApp%20and%20Rules.zip

19. Extract the **SampleApp** folder from the downloaded archive (**SampApp and Rules.zip**) and copy the folder, including its content, into the **C:\inetpub\wwwroot** folder.

20. From the **Administrator: Windows PowerShell** window, run the following:

```powershell
Invoke-Command -ComputerName LON-SVR1 -ScriptBlock {Get-AdfsCertificate -CertificateType Token-Signing | Select-Object -ExpandProperty Thumbprint}
```

This displays the thumbprint of the AD FS token signing certificate.

21. Copy the output to Clipboard.

22. From the **Administrator: Windows PowerShell** window, run the following:

```powershell
Notepad C:\inetpub\wwwroot\SampApp\Web.config
```

23. Search for the word thumbprint in Notepad. There will be three matches. Replace the value within the double quotes immediately following **thumbprint** with the content of the Clipboard.

24. Search for every occurrence of **app1.contoso.com** in Notepad (there will be two matches) and replace them with **webapp.adatum.com**

25. Search for every occurrence of **sts.contoso.com** and replace them with **adfs.adatum.com** (there will be nine matches).

26. Save your changes and close Notepad.

27. From the **Administrator: Windows PowerShell** window, run the following:
28. Search for every occurrence of app1.contoso.com in Notepad and replace it with webapp.adatum.com (there will be four matches).

29. Save your changes and close Notepad.

30. Start Internet Information Services (IIS) Manager console.

31. In the console, click the Application Pools node, next, right-click DefaultAppPool and click Advanced Settings.

32. In the Advanced Settings dialog box, select Identity, click on the ellipses (...) to the right of the ApplicationPoolIdentity. In the ApplicationPoolIdentity dialog box, click Custom account and then click Set...

33. In the Set Credentials dialog box, specify the following and click OK twice:
   - User name: ADATUM\Svc_AppPool
   - Password: Pa55w.rd1234
   - Confirm password: Pa55w.rd1234

34. In the Advanced Settings dialog box, set Load User Profile to True and click OK.

35. Back in the console, expand the Sites folder, expand the Default Web Site node, right-click SampApp, click Convert To Application.

36. In the Add Application dialog box, accept the default settings and click OK.

37. Back in the console, click Default Web Site in the Connections pane and then click Bindings in the Actions pane.

38. In the Site Bindings dialog box, click Add...

39. In the Add Site Bindings dialog box, set Type to https, set Host name to webapp.adatum.com, click Select... next to the SSL certificate drop down list, select the Adatum Sample Web App certificate and click OK.

40. If prompted for confirmation, click Yes.

41. In the Site Bindings dialog box, click Close.

42. Click Default Web Site and then click Restart in the Actions pane.

---

Task 7: Configure an AD FS relying party on LON-SVR1 (Completed)

1. Sign back into the LON-SVR1 Windows Server 2016 lab virtual machine with the following credentials:
   - USERNAME: ADATUM\Administrator
   - PASSWORD: Pa55w.rd

2. While signed in to the LON-SVR1 Windows Server 2016 lab virtual machine as ADATUM\Administrator, start Internet Explorer and download the sample app from https://msdnshared.blob.core.windows.net/media/TNBlogsFS/prod.evol.blogs.technet.com/tell

4. Click Start and then click Windows PowerShell.

5. From the Administrator: Windows PowerShell window, run the following:

   ```powershell
   ```

   This creates a relying party representing our sample application.

6. Click Start and then click Server Manager.

7. In the Server Manager window, click Tools and, in the drop-down menu, click AD FS Management.

8. In the AD FS Management console, click the Relying Party Trusts folder and verify that the relying party named Sample Claims Aware Application was created successfully.

   ▶ Task 8: Install AD FS SSL certificate on LON-SVR2

First, you will export the AD FS SSL certificate from the AD FS server (LON-SVR1)

1. While signed in to LON-SVR1 as ADATUM\Administrator, click Start, right-click Windows PowerShell, click More and then click Run as administrator.

2. From the Administrator: Windows PowerShell window, type the following and press Enter:

   ```powershell
certlm
   ```

   This will open the Microsoft Management Console (MMC) with the Certificates - Local Computer snap-in loaded.

3. In the console, navigate to the Personal\Certificates folder, right-click the *.adatum.com certificate, in the right-click menu, click All Tasks and then click Export. This will start the Certificate Export Wizard.

4. On the Welcome to the Certificate Export Wizard page, click Next

5. On the Export Private Key page, click the Yes, export the private key option and click Next.


7. On the Security page, click the Password checkbox and then, type in Pa55w.rod in the Password and Confirm password text boxes.


11. In the **Certificate Export Wizard** dialog box, click **OK**.

Next, you will import the AD FS certificate on the WAP server (LON-SVR2)

12. Switch to the LON-SVR2 Windows Server 2016 lab virtual machine where you are signed in as ADATUM\Administrator.

13. Right-click **Start** and, in the right-click menu, click **Command Prompt (Admin)**

14. From the **Administrator: Command PowerShell** window, run the following:

```
robocopy \172.16.0.11\c$ c: \adfs.adatum.com.pfx
```

In real-life scenarios, you would copy the certificate via a removable media.

15. From the **Command Prompt (Admin)** window, run the following:

```
certlm
```

This will open the Microsoft Management Console (MMC) with the **Certificates - Local Computer** snap-in loaded.

16. Expand the **Certificates – Local Computer** top level node, right-click the **Personal** folder, click **All Tasks**, and click **Import**. This will start the **Certificate Import Wizard**.

17. On the **Welcome to the Certificate Import Wizard** page, click **Next**

18. On the **File to Import** page, click **Browse...**

19. In the **Open** dialog box, switch the filter to **Personal Information Exchange (*.pfx)**, browse to the root of C, click **adfs.adatum.com.pfx**, and click **Open**.

20. Back on the **File to import** page, click **Next**.

21. On the **Private key protection** page, in the **Password** text box, type **Pa55w.rd** and click **Next**.

22. On the **Certificate Store** page, accept the default setting and click **Next**.

23. On the **Completing the Certificate Import Wizard** page, click **Finish**.

24. In the **Certificate Import Wizard** dialog box, click **OK**.

**Task 9: Install Web App certificate on LON-SVR2**

First, you will export the Web App certificate from the Web App server (LON-SVR3)

1. Switch to the console session to LON-SVR3 Windows Server 2016 lab virtual machine, where you are signed in as ADATUM\Administrator.

2. While signed on to LON-SVR3 Windows Server 2016 lab virtual machine, click **Start**, right-click **Windows PowerShell**, click **More** and then click **Run as administrator**.

3. From the **Administrator: Windows PowerShell** window, type the following and press Enter:

```
certlm
```
4. This will open the Microsoft Management Console (MMC) with the **Certificates - Local Computer** snap-in loaded.

5. In the console, navigate to the **Personal\Certificates** folder, right-click the **webapp.adatum.com** certificate, in the right-click menu, click **All Tasks** and then click **Export**. This will start the **Certificate Export Wizard**.

6. On the **Welcome to the Certificate Export Wizard** page, click **Next**

7. On the **Export Private Key** page, click the **Yes, export the private key** option and click **Next**.

8. On the **Export File Format** page, click **Next**.

9. On the **Security** page, click the **Password** checkbox and then, type in **Pa55w.rd** in the **Password** and **Confirm password** text boxes.

10. On the **File to Export** page, type **C:\webapp.adatum.com.pfx** and click **Next**.

11. On the **Completing the Certificate Export Wizard** page, click **Finish**.

12. In the **Certificate Export Wizard** dialog box, click **OK**. Next, you will import the Web App SSL certificate on the WAP server (LON-SVR2)

13. Switch to the console session on LON-SVR2 Windows Server 2016 lab virtual machine, where you are signed in as Administrator.

14. From the **Administrator: Command PowerShell** window, run the following:

   ```powershell
gerobocopy \172.16.0.13\c$ c:\webapp.adatum.com.pfx
```

In real-life scenarios, you would copy the certificate via a removable media.

15. While signed on to LON-SVR2 Windows Server 2016 lab virtual machine, switch to the **Certificates – Local Computer** console.

16. Expand the **Certificates – Local Computer** top level node, right-click the **Personal** folder, click **All Tasks**, and click **Import**. This will start the **Certificate Import Wizard**.

17. On the **Welcome to the Certificate Import Wizard** page, click **Next**

18. On the **File to Import** page, click **Browse**...

19. In the **Open** dialog box, switch the filter to **Personal Information Exchange (*.pfx)**, browse to the root of C:, click **webapp.adatum.com.pfx**, and click **Open**.

20. Back on the **File to import** page, click **Next**.

21. On the **Private key protection** page, in the **Password** text box, type **Pa55w.rd** and click **Next**.

22. On the **Certificate Store** page, accept the default setting and click **Next**.

23. On the **Completing the Certificate Import Wizard** page, click **Finish**.

24. In the **Certificate Import Wizard** dialog box, click **OK**.
Task 10: Install adatum-root-CA root certificate on LON-SVR2

Now, you will import the adatum-root-CA root certificate into the Trusted Root Certification Authorities store on the WAP server (LON-SVR2)

1. In the Certificates – Local Computer console, in the Personal folder, right-click the adatum-root-CA certificate, click All Tasks, and click Export. This will start the Certificate Export Wizard.
2. On the Welcome to the Certificate Export Wizard page, click Next.
3. On the Export File format page, click Next.
4. On the File to Export page, in the File name text box, type C:\adatum-root-CA.cer and click Next.
6. In the Certificate Export Wizard dialog box, click OK.
7. In the Certificates – Local Computer top level node, expand the Trusted Root Certification Authorities folder, and double click the Certificates folder. Verify that adatum-root-CA certificate is already present. If not, proceed with the next step (8). Otherwise, go directly to task 11.
8. In the Certificates folder, click All Tasks, and click Import. This will start the Certificate Import Wizard.
10. On the File to Import page, click Browse...
11. In the Open dialog box, browse to the root of C:, click adatum-root-CA.cer, and click Open.
13. On the Certificate Store page, accept the default setting and click Next.
15. In the Certificate Import Wizard dialog box, click OK.

Task 11: Install the WAP role service on LON-SVR2

1. On LON-SVR2, click Start and then click Server Manager.
2. Click Manage and, in the drop-down menu, click Add Roles and Features.
3. If the Before You Begin page appears, select the Skip this page by default check box, and then click Next.
4. On the Select installation type page, ensure that the Role-based or feature-based installation option is selected and click Next.
5. On the Server destination server page, ensure that LON-SVR2 is selected and click Next.
6. On the Select server roles page, select the Remote Access check box and then click Next.
7. On the Select features page, click Next.

9. On the Select role services page, click Web Application Proxy. This will display an additional dialog box prompting you to add features required for Web Application Proxy. Click Add Features and then click Next.

10. On the Confirm installation selections page, select the Restart the destination server automatically if required checkbox, click Yes when prompted for confirmation, and click Install. Wait for the installation to complete.

11. Once the installation completes, on the Installation progress page, click Open the Web Application Proxy Wizard. This will start Web Application Proxy Configuration Wizard.

12. On the Welcome page, click Next.

13. On the Federation Server page, specify the following settings:
   - Federation Server name: adfs.adatum.com
   - User name: ADATUM\Administrator
   - Password: Pa55w.rd

14. On the AD FS Proxy Certificate page, in the Select a certificate to be used by the ADFS proxy drop-down list, click *.*.adatum.com and click Next.

15. On the Confirmation page, click Configure.

16. Wait until the configuration completes, review the detailed operation results, and click Close. This will automatically open Remote Access Management console.

◆ Task 12: Publish the sample Web application on LON-SVR2

1. On LON-SVR2, in the Remote Access Management console click Publish in the Tasks pane. This will start the Publish New Application Wizard.

2. On the Welcome page, click Next.

3. On the Preauthentication page, change to Pass-through and click Next.


5. On the Confirmation page, click Publish

6. On the Results page, click Close.
Results: After completing this exercise, you will have installed Enterprise CA and its CRL Distribution Point, AD FS, Web Application Proxy, a sample Web app, and published it using pass-through authentication.

Exercise 2: Validate the Web Application Proxy deployment

Now that you have deployed the Web Application Proxy role service, you need to verify that external users can access the internal application through the proxy. The main tasks for this exercise are as follows:

1. Test application access from an internal client
2. Test application access from an external client

▶ Task 1: Test application access from an internal client

1. Sign in to the LON-CL1 Windows 10 lab virtual machine using the following credentials:
   - USERNAME: ADATUM\Administrator
   - PASSWORD: Pa55w.rd

2. While signed in to LON-SVR1 as ADATUM\Administrator, click Start, in the Start menu, expand the Windows PowerShell folder, right-click Windows PowerShell, click More and then click Run as administrator.

3. From the Administrator: Windows PowerShell window, type the following and press Enter:

   ```
   gpupdate /force
   ```

   If you receive any error messages regarding group policy processing, restart LON-CL1 and repeat steps 1-3.

4. From the Administrator: Windows PowerShell window, type the following and press Enter:

   ```
   certlm
   ```

   This will open the Microsoft Management Console (MMC) with the Certificates - Local Computer snap-in loaded.

5. Expand the Certificates – Local Computer top level node, expand the Trusted Root Certification Authorities folder and click its Certificates subfolder. Note that it includes the adatum-root-CA self-issued certificate.


7. Next, browse to https://webapp.adatum.com/SampApp/ and when prompted provide Administrator and Pa55w.rd credentials.

8. Verify the page displays the list of claims of the current user.