Windows Server 2012 R2

Microsoft

Implementing a Basic PKI in Windows Server 2012 R2

Windows Server 2012 R2

Hands-on lab

In this lab, you will learn how to implement a basic public key infrastructure (PKI) in Windows Server 2012 R2 to enable services that rely on certificates.

Produced by HynesITe, Inc
Version 1.1
12/19/2013

holSystems™
Learn. Experience. Collaborate.

Introduction

Estimated time to complete this lab

90 minutes

Objectives

After completing this lab, you will be able to:

- Install and configure a stand-alone root certification authority (CA).
- Enroll an enterprise root CA.
- Modify a certificate template.
- Enable autoenrollment in a domain.
- Manage certificates using Windows PowerShell.

Prerequisites

Before working on this lab, you must have:

- Experience with Active Directory.
- Experience with Active Directory Certificate Services.
- Experience with DHCP and DNS.

Overview of the lab

In this lab, you will implement a basic public key infrastructure (PKI) in Windows Server 2012 R2 to enable services that rely on certificates.

Virtual machine technology

This lab is completed using virtual machines that run on Windows Server 2012 Hyper-V technology. To log on to the virtual machines, press CTRL+ALT+END and enter your logon credentials.

Computers in this lab

This lab uses computers as described in the following table. Before you begin the lab, you must ensure that the virtual machines are started and then log on to the computers.

Virtual Machine	Role	Configuration
RootCA	Windows Server 2012 R2 server	Server with Windows Server 2012 R2 installed
SubCA	Domain controller	Windows Server 2012 R2 domain controller
Server1	A member server with IIS installed	A member server with IIS installed
Client1	Windows 8.1 client	Windows 8.1 client with the RSAT tools installed

◇ Credentials for all virtual machines unless otherwise noted are **Contoso\Administrator** and the password **Passw0rd!**

Note regarding pre-release software

Portions of this lab may include software that is not yet released, and as such may still contain active or known issues. While every effort has been made to ensure this lab functions as written, unknown or unanticipated results may be encountered as a result of using pre-release software.

Note regarding user account control

Some steps in this lab may be subject to user account control. User account control is a technology which provides additional security to computers by requesting that users confirm actions that require administrative rights. Tasks that generate a user account control confirmation are denoted using a shield icon. If you encounter a shield icon, confirm your action by selecting the appropriate button in the dialog box that is presented.

Note on activation

The virtual machines for these labs may have been built by using software that has not been activated. This is by design in the lab to prevent the redistribution of activated software. The unactivated state of software has been taken into account in the design of the lab. Consequently, the lab is in no way affected by this state. For operating systems other than Windows 8.1, please press Cancel or Close if prompted by an activation dialog box. If you are prompted by an Activate screen for Windows 8.1, press the Windows key to display the Start screen.

Exercise 1: Install a Stand-alone Root CA

In this exercise, you will begin the process of building the PKI environment. The first item to be configured is the stand-alone root CA. This will form the trust anchor and establish the root of the trust hierarchy. You will create a new root CA with the name of ContosoRootCA, a 4096 bit key, and that is valid for 3 years.

Add the Active Directory Certificate Server role

In this task, you add the AD CS role to RootCA. RootCA is a non-domain joined stand-alone server.

✎ Begin this task logged on to **RootCA** as **Administrator** using the password **Passw0rd!**

1. Open **Server Manager**.
2. Click **Add roles and features**.
3. On the Before you begin page, click **Next**.
4. On the Select installation type page, click **Next**.
5. On the Select destination server page, click **Next**.
6. On the Select server roles page, click **Active Directory Certificate Services**.
7. In the Add Roles and Features Wizard, click **Add Features**.
8. On the Select server roles page, click **Next**.
9. On the Select features page, click **Next**.
10. On the Active Directory Certificate Services page, click **Next**.
11. On the Select roles services page, click **Next**.

    📌 Note that the only role service required for the root CA is the Certification Authority role service.

12. On the Confirm installation selections page, click **Install**.

    ◈ Wait for the installation to complete before proceeding to the next step.

13. On the Installation progress page, click **Close**.

Configure Active Directory Certificate Services on the stand-alone root CA

In this task, you will configure the AD CS for the stand-alone root CA.

✎ Ensure you are logged on to **RootCA** as **Administrator** using the password **Passw0rd!**

1. In Server Manager, in the explorer pane, click **AD CS**.
2. In AD CS, in Servers, next to Configuration required for Active Directory Certificate Services at ROOTCA, click **More**.

3. In the All Servers Task Details window, click **Configure Active Directory Certificate Services on the destination server**.
4. In the AD CS Configuration dialog box, on the Credentials page, click **Next**.
5. On the Role Services page, select **Certification Authority**, and then click **Next**.
6. On the Setup Type page, ensure **Standalone CA** is selected, and then click **Next**.
7. On the CA Type page, ensure **Root CA** is selected, and then click **Next**.
8. On the Private Key page, click **Next**.
9. On the Cryptography for CA page, modify the key length to **4096**, and then click **Next**.
10. On the CA Name page, change the Common name for this CA to **ContosoRootCA**, and then click **Next**.
11. On the Validity Period page, change the period to **3 Years**, and then click **Next**.
12. On the CA Database page, click **Next**.
13. On the Confirmation page, click **Configure**.
14. On the Results page, click **Close**.
15. Close the **All Servers Task Details** window.

Configure the CA properties

In this task, you will configure the properties of the CA with information about the subordinate CA which will actually be doing the issuance of the certificates for the Contoso domain. This will include the certificate revocation list location and the authority information access location.

✎ Ensure you are logged on to **RootCA** as **Administrator** using the password **Passw0rd!**

1. In Server Manager, on the Tools menu, click **Certification Authority**.
2. In certsrv, in the Explorer pane, click **ContosoRootCA**.
3. On the Action menu, click **Properties**.
4. In the ContosoRootCA Properties window, click the **Extensions** tab.
5. In the Extensions tab, in Select extension, select **Authority Information Access (AIA)**, and then click **Add**.
6. In the Location field, type **http://SubCA.contoso.com/certdata/**.
7. In the Variable drop down, select **<ServerDNSName>**, and then click **Insert**.
8. In the Variable drop down, select **<CaName>**, and then click **Insert**.
9. In the Variable drop down, select **<CertificateName>**, and then click **Insert**.
10. In the Add Location dialog box, click **OK**.

11. On the Extensions tab, check **Include in the AIA extension of issued certificates**.
12. In Select extension, select **CRL Distribution Point (CDP)**, and then click **Add**.
13. In the Location field, type **http://SubCA.contoso.com/certdata/**
14. In the Variable drop down, select **<CaName>**, and then click **Insert**.
15. In the Variable drop down, select **<CRLNameSuffix>**, and then click **Insert**.
16. In the Variable drop down, select **<DeltaCRLAllowed>**, and then click **Insert**.
17. In the Location field, type **.crl** at the end of the inserted fields.
18. In the Add Location dialog box, click **OK**.
19. On the Extensions tab, check **Include in CRLs. Clients use this to find delta CRL locations**.
20. On the Extensions tab, check **Include in the CDP extension of issued certificates**.
21. In the ContosoRootCA properties box, click **OK**.
22. In the Certification Authority dialog box, click **Yes**.

    ◇ Leave the certsrv mmc open for the next task.

Publish the CRL and finalize the root CA setup

In this task, you will publish the certificate revocation list and complete the root CA setup, ready to begin setting up the subordinate CA. You will ensure that all required certificates have been exported and are available for importing.

✎ Ensure you are logged on to **RootCA** as **Administrator** using the password **Passw0rd!**

1. In certsrv, in the Explorer pane, expand **ContosoRootCA**, and then select **Revoked Certificates**.
2. On the Action menu, click **All Tasks**, and then click **Publish**.
3. In the Publish CRL dialog box, click **New CRL**, and then click **OK**.
4. Close the **certsrv console**.
5. On the Start screen, type **certificates**, and then click **Manage computer certificates**.
6. In certlm, in the Explorer pane, expand **Certificates - Local Computer, Personal, Certificates**.
7. Select **ContosoRootCA**, and then on the Action menu, click **All Tasks, Export**.
8. In the Certificate Export Wizard, click **Next**.
9. On the Export Private Key page, ensure **No, do not export the private key** is selected, and then click **Next**.
10. On the Export File Format page, click **Next**.

    ◇ Depending on the destination usage, formats other than the default might be selected.

11. In the File to Export page, type **\\SubCA\LabFiles\Contoso-RootCA.cer**, and then click **Next**.
12. In the Completing the Certificate Export Wizard page, click **Finish**.

13. In the Certificate Export Wizard dialog box, click **OK**.
14. Open **File Explorer**, and then browse to **C:\windows\system32\certsrv\certenroll**.
15. Select the two files, and then copy them to **\\SubCA\LabFiles\**.

   📌 In a production environment, there would likely be no direct connection between the root CA and the subordinate CA. The certificates instead would be hand carried between the servers. The root CA would at this point be turned off and put in a secure location.

Exercise 2: Install and Configure an Enterprise Subordinate Certificate Authority

In this exercise, you continue the setup of the contoso.com private key infrastructure by installing the Active Directory Certificate Services (AD CS) server role and then configuring it with the certificates from the stand-alone root CA.

Install the Active Directory Certificate Server role

In this task, you add the AD CS role to SubCA. SubCA is a domain controller for the contoso.com domain. In an enterprise environment AD CS does not have to be installed on a domain controller but can be installed on a member server.

✎ Begin this task logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. Open **Server Manager**.
2. On the Manage menu, click **Add Roles and Features**.
3. On the Before you begin page, click **Next**.
4. On the Select installation type page, click **Next**.
5. On the Select destination server page, click **SubCA.contoso.com**, and then click **Next**.
6. On the Select server roles page, click **Active Directory Certificate Services**.
7. In the Add Roles and Features Wizard, click **Add Features**.
8. On the Select server roles page, click **Next**.
9. On the Select features page, click **Next**.
10. On the Active Directory Certificate Services page, click **Next**.
11. On the Select roles services page, select **Certification Authority** and **Certification Authority Web Enrollment**.
12. In the Add Roles and Features Wizard, click **Add Features**.
13. On the Select Role Services page, click **Next**.
14. On the Web Server Role (IIS) page, click **Next**.
15. On the Select role services page, click **Next**.
16. On the Confirm installation selections page, click **Install**.

    ◈ Wait for the installation to complete before proceeding to the next step.

17. On the Installation progress page, click **Close**.

Configure the Active Directory Certificate Services role

In this task, you will now configure the AD CS server role for the enterprise subordinate root CA.

✎ Ensure you are logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the explorer pane, click **AD CS**.
2. In AD CS, in Servers, next to Configuration required for Active Directory Certificate Services at SUBCA, click **More**.
3. In the All Servers Task Details window, click **Configure Active Directory Certificate Services on the destination server**.
4. In the AD CS Configuration dialog box, on the Credentials page, click **Change**.
5. In the Windows Security dialog box, enter the username **Contoso\Administrator** and the password **Passw0rd!** and then click **OK**.
6. In the AD CS Configuration dialog box, on the Credentials page, click **Next**.
7. On the Role Services page, select **Certification Authority** and **Certification Authority Web Enrollment**, and then click **Next**.
8. On the Setup Type page, ensure **Enterprise CA** is selected, and then click **Next**.
9. On the CA Type page, ensure **Subordinate CA** is selected, and then click **Next**.
10. On the Private Key page, click **Next**.
11. On the Cryptography for CA page, modify the key length to **4096**, and then click **Next**.
12. On the CA Name page, change the Common name for this CA to **ContosoSubCA**, and then click **Next**.
13. On the Certificate Request page, click **Next**.
14. On the CA Database page, click **Next**.
15. On the Confirmation page, click **Configure**.
16. On the Results page, click **Close**.

    📌 In the results panel there is a warning regarding the certificate request. This is expected as you are now going to complete the installation of the certificate from the root CA.

17. Close the **All Servers Task Details** window.
18. Switch to **SubCA**, and then log on as **Contoso\Administrator** using the password **Passw0rd!**
19. Open **File Explorer**, and then navigate to **C:\LabFiles**.
20. Right-click **Contoso-RootCA.cer**, and then click **Install Certificate**.
21. On the Certificate Import Wizard, select **Local Machine**, and then click **Next**.

22. On the Certificate Store page, select **Place all certificates in the following store**, and then click **Browse**.
23. In the Select Certificate Store dialog box, select **Trusted Root Certification Authorities**, and then click **OK**.
24. On the Certificate Store page, click **Next**.
25. On the Completing the Certificate Import Wizard page, click **Finish**.
26. On the Certificate Import Wizard dialog box, click **OK**.
27. Create a new directory named **C:\inetpub\wwwroot\certdata**.
28. From C:\LabFiles, copy **ContosoRootCA.crl** and **RootCA_ContosoRootCA.crt** to **C:\inetpub\wwwroot\certdata**.
29. From C:\, copy **SubCA.contoso.com_contoso-SUBCA-CA.req** to **\\RootCA\LabFiles**.
30. Switch to **RootCA**, and then ensure you are logged on as **Contoso\Administrator** using the password **Passw0rd!**
31. In Server Manager, in Tools, click **Certification Authority**.
32. Select **ContosoRootCA**, and then on the Action menu, click **All Tasks**, and then click **Submit a new request**.
33. In the Open Request File window, navigate to **C:\LabFiles**, click the **req** file, and then click **Open**.
34. In certsrv, in the explorer pane, click **Pending Requests**.

~~34.~~📌 If you do not see the request, you may need to refresh the display.

Formatted: Additional Information, No bullets or numbering

35. Select the pending request, and then on the Action menu, click **All Tasks**, and then click **Issue**.
36. In certsrv, in the explorer pane, click **Issued Certificates**.
37. Select the issued certificate, and on the Action menu, click **Open**.
38. In the Certificate dialog box, on the Details tab, click **Copy to File**.
39. In the Certificate Export Wizard, click **Next**.
40. On the Export File Format page, select the **.P7B** format, check the **Include all certificates in the certification path if possible** check box, and then click **Next**.
41. On the File to Export page, type **\\SubCA\LabFiles\ContosoCert.p7b**, and click **Next**.
42. On the Completing the Certificate Export Wizard page, click **Finish**.
43. On the Certificate Export Wizard dialog box, click **OK**.
44. Close the **Certificate** dialog box.
45. Switch to **SubCA**, and then ensure you are logged on as **Contoso\Administrator** using the password **Passw0rd!**

46. In Server Manager, on the Tools menu, click **Certification Authority**.
47. In certsrv, in the Explorer pane, click **ContosoSubCA**.
48. On the Action menu, click **All Tasks**, and then click **Install CA Certificate**.

    📌 Note that at this time the CA service is installed; however it is not started as yet. After you have installed the CA certificate, you will be able to start the service.

49. In the Select file to complete CA installation window, navigate to **C:\LabFiles**, select **ContosoCert.p7b**, and then click **Open**.
50. In certsrv, in the Explorer pane, click **ContosoSubCA**.
51. On the Action menu, click **All Tasks**, and then click **Start Service**.

    📌 The CA service is now started and able to issue certificates.

Configure external CRL and AIA publication points

In this task, you will configure SUBCA to have alternate publication points for the CRL and the AIA. This is done to enable the certificates to be used outside of the organization network.

✎ Ensure you are logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in the Explorer pane, click **AD CS**.
2. In AD CS, in Servers, right-click **SUBCA**, and then click **Certification Authority**.
3. In certsrv, in the Explorer pane, click **ContosoSubCA**.
4. On the Action menu, click **Properties**.
5. In the ContosoSubCA Properties window, click the **Extensions** tab.
6. On the Extensions tab, in Select extension, select **Authority Information Access (AIA)**, and then click **Add**.
7. In the Location field, type **http://www.contoso.com/AIA**.
8. In the Add Location dialog box, click **OK**.
9. On the Extensions tab, check **Include in the AIA extension of issued certificates**.
10. In Select extension, select **CRL Distribution Point (CDP)**, and then click **Add**.
11. In the Location field, type **http://www.contoso.com/CRL**.
12. In the Add Location dialog box, click **OK**.
13. On the Extensions tab, check **Include in CRLs. Clients use this to find Delta CRL Locations.**
14. On the Extensions tab, check **Include in the CDP extension of issued certificates**.
15. In the ContosoSubCA Properties box, click **OK**.
16. In the Certification Authority dialog box, click **Yes**.

- Leave the certsrv mmc open for the next task.

Modify the certificate templates

In this task, you will modify the certificate templates to enable the use of different certificates for the users, computers, and SSL in the domain.

✎ Ensure you are logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. In the certsrv console, click **Certificate Templates**, and then on the Action menu, click **Manage**.
2. In the Certificates Template Console, click **Computer**, and then on the Action menu, click **Duplicate Template**.
3. In the Properties of New Template dialog box, on the Compatibility tab, modify the Certification Authority to be **Windows Server 2012 R2**.
4. In the Resulting changes dialog box, click **OK**.
5. In the Properties of New Template dialog box, on the Compatibility tab, modify the Certificate recipient to be **Windows 8.1 / Windows Server 2012 R2**.
6. In the Resulting changes dialog box, click **OK**.
   - The adjustment of the compatibility settings is done to enable the more recent features of the template. The levels should be set at the minimum operating systems in the domain and that will be making certificate requests. In this case, the Contoso.com domain is Windows 8.1 and Windows Server 2012 R2.
7. In the Properties of New Template dialog box, on the General tab, in the Template display name field, type **Domain Computers Cert**.
8. In the Properties of New Template dialog box, on the Security tab, click **Domain Computers**, and then in Permissions for Domain Computers, check **Read**, **Enroll**, and **Autoenroll**.
   - The autoenroll permission does not give the permission to enroll, so both permissions must be enabled to ensure that the certificate can be autoenrolled.
9. In the Properties of New Template dialog box, click **OK**.
10. In the Certificates Template Console, click **User**, and then on the Action menu, click **Duplicate Template**.
11. In the Properties of New Template dialog box, on the Compatibility tab, modify the Certification Authority to be **Windows Server 2012 R2**.
12. In the Resulting changes dialog box, click **OK**.
13. In the Properties of New Template dialog box, on the Compatibility tab, modify the Certificate recipient to be **Windows 8.1 / Windows Server 2012 R2**.
14. In the Resulting changes dialog box, click **OK**.

15. In the Properties of New Template dialog box, on the General tab, in the Template display name, type **Domain Users Cert**.
16. In the Properties of New Template dialog box, on the Security tab, click **Domain Users**, and then in Permissions for Domain Users, check **Read**, **Enroll**, and **Autoenroll**.
17. In the Properties of New Template dialog box, click **OK**.
18. In the Certificates Template Console, click **Web Server**, and then in the Action menu, click **Duplicate Template**.
19. In the Properties of New Template dialog box, on the Compatibility tab, modify the Certification Authority to be **Windows Server 2012 R2**.
20. In the Resulting changes dialog box, click **OK**.
21. In the Properties of New Template dialog box, on the Compatibility tab, modify the Certificate recipient to be **Windows 8.1 / Windows Server 2012 R2**.
22. In the Resulting changes dialog box, click **OK**.
23. In the Properties of New Template dialog box, on the General tab, in the Template display name field, type **SSL Wildcard Cert**.
24. In the Properties of New Template dialog box on the Security tab, click **Domain Admins**.
    - 📌 Note that we are going make this certificate a manual enrollment certificate, so therefore we don't have to modify the permissions from the default.
25. In the Properties of New Template dialog box, click the **Subject Name** tab.
    - 📌 Note that the default subject name configuration for the web server template is to be "Supply in the request". This means that when you request the certificate the name of the server will need to be supplied.
26. In the Properties of New Template dialog box, click **OK**.
27. Close the **Certificate Templates Console**.

Publish the templates

In this task, you will publish the certificate templates you have created so that they can be used for requests.

✎ Ensure you are logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Certsrv, click **Certificate Templates**, and then on the Action menu, click **New**, and then click **Certificate Template to Issue**.

2. In the Enable Certificate Templates dialog box, press and hold CTRL, and then click **Domain Computers Cert**, **Domain Users Cert**, and **SSL Wildcard Cert**, and then click **OK**.

   📌 The newly added templates will appear in Certificate Templates.

   ◇ Leave the certsrv mmc open for a future task.

Enable autoenrollment in the domain for users and computers

In this task, you will continue to configure the domain to implement the public key infrastructure. The certificate templates for the users and the computers have been configured for autoenrollment; however this will not function until the Group Policy in the domain has been configured to ensure the accounts make the request automatically.

✎ Ensure you are logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, on the Tools menu, click **Group Policy Management**.
2. In Group Policy Management, expand **Group Policy Management/Forest: Contoso.com/Domains**, and then select **contoso.com**.
3. On the Action menu, click **Create a GPO in this domain, and link it here**.
4. In the New GPO dialog box, type **CA Certificate Distribution Policy**, and then click **OK**.
5. In Group Policy Management, in the explorer pane, click **CA Certificate Distribution Policy**, and then in the Group Policy Management Console dialog box, click **OK**.
6. On the Action menu, click **Edit**.
7. In the Group Policy Management Editor, expand **Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies**.
8. In Object Type, select **Certificate Services Client – Certificate Enrollment Policy**, and then on the Action menu, click **Properties**.
9. In the Certificate Services Client – Certificate Enrollment Policy dialog box, in Configuration Model, select **Enabled**, and then click **OK**.
10. In Object Type, select **Certificate Services Client – Auto-Enrollment**, and then on the Action menu, click **Properties**.
11. In the Certificate Services Client – Auto-Enrollment dialog box, in Configuration Model, select **Enabled**.
12. Check both check boxes, and then click **OK**.

    📌 The Computers will now autoenroll once the policy is applied. You now need to configure the same for the user accounts.

13. In the Group Policy Management Editor, expand **User Configuration/Policies/Windows Settings/Security Settings/Public Key Policies**.
14. In Object Type, select **Certificate Services Client – Certificate Enrollment Policy**, and then on the Action menu, click **Properties**.
15. In the Certificate Services Client – Certificate Enrollment Policy dialog box, in Configuration Model, select **Enabled**, and then click **OK**.
16. In Object Type, select **Certificate Services Client – Auto-Enrollment**, and then on the Action menu, click **Properties**.
17. In the Certificate Services Client – Auto-Enrollment dialog box, in Configuration Model, select **Enabled**.
18. Check both check boxes, and then click **OK**.
    - 📌 The configuration of the user account policies is now complete. The next time that the Group Policy policy settings are applied, the policy will apply for the account.
    - ◇ Leave the Group Policy Management Editor open for the next task.

Deploy required certificates in the domain for users and computers

In this task, you will ensure that the certificate for RootCA is deployed to all computers. This is needed to ensure that the trust chain is complete. This also ensures that if the SubCA is compromised, the certificates can be revoked.

✎ Ensure you are logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. In the Group Policy Management Editor, expand **Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Trusted Root Certification Authorities**.
2. On the Action menu, click **Import**.
3. In the Certificate Import Wizard, click **Next**.
4. On the file to import page, click **Browse**.
5. In \\SubCA\LabFiles, click **Contoso-RootCA.cer**, and then click **Open**.
6. In the File to import page, click **Next**.
7. In the Certificate Store page, click **Next**.
8. In the Completing the Certificate Import Wizard page, click **Finish**.
9. In the Certificate Import Wizard dialog box, click **OK**.
10. Close the **Group Policy Management Editor**.
11. Close **Group Policy Management**.

- 📌 The configuration of the user account policies is now complete. The next time that the Group Policy policy settings are applied, the policy will apply for the account.

Exercise 3: Manage the Certificate Environment

In this exercise, you will continue to test the implementation of the contoso.com private key infrastructure to ensure that it is all functioning. In addition, you will ensure that you can manage the issued certificates using Windows PowerShell.

Test the computer certificate autoenrollment

In this task, you will ensure that Server1 obtains a computer certificate using the autoenrollment policy.

✎ Ensure you are logged on to **Server1** as **Contoso\Administrator** using the password **Passw0rd!**

1. Press the Windows key + X, and then select **Command Prompt (Admin)**.
2. At command prompt, type the following command, and then press ENTER.

   ```
   ↪ Gpupdate /force
   ```

3. Wait for the update to complete, and then close the command prompt window.
4. Press the Windows key + X, and then select **Run**.
5. In the Run dialog box, type **MMC**, and then press ENTER.
6. In Console1, on the File menu, click **Add/Remove Snap-ins**.
7. In Add or Remove Snap-ins, select **Certificates**, and then click **Add**.
8. In the Certificates snap-in dialog box, select **Computer account**, and then click **Next**.
9. On the Select Computer dialog box, click **Finish**.
10. In Add or Remove Snap-ins, click **OK**.
11. In Console1, expand **Certificates (Local Computer), Personal, Certificates**.

    📌 Note that there is a certificate issued to Server1.contoso.com by ContosoSubCA.

12. Close **Console1**.

Test the user certificate autoenrollment

In this task, you will ensure that when a user logs onto a computer, they will obtain a user certificate using the autoenrollment policy.

✎ Ensure you are logged on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

1. Press the Windows key + X, and then select **Command Prompt (Admin)**.
2. At the command prompt, type the following commands, pressing ENTER after each line.

   ```
   ↪ Gpupdate /force
   ↪ logoff
   ```

3. Log on as **Contoso\BenSmith** using the password **Passw0rd!**

4. On the Start screen, type **MMC**, and then from the results, select **MMC**.
5. In Console1, on the File menu, click **Add/Remove Snap-in**.
6. In Add or Remove Snap-ins, select **Certificates**, and then click **Add**.
7. In Add or Remove Snap-ins, click **OK**.
8. In Console1, expand **Certificates-Current User, Personal, Certificates**.

   📌 Note that there is a certificate issued to Ben Smith by ContosoSubCA.
9. Close **Console1**.
10. Log off **Client1**, and then log on to **Client1** as **Contoso\Administrator** using the password **Passw0rd!**

Issue and test the wildcard certificate for IIS

In this task, you will enroll Server1 for a wildcard certificate, and then configure IIS to use the certificate on the default website.

✏ Ensure you are logged on to **Server1** as **Contoso\Administrator** using the password **Passw0rd!**

1. Open **Internet Explorer**, and then navigate to **https://Server1.contoso.com**.

   📌 The webpage will not be found as you have not configured it as yet to use a certificate.
2. Close **Internet Explorer**.
3. On the Start screen, type **IIS**, and then press ENTER.
4. In Internet Information Services (IIS) Manager, click **Server1**.
5. In the Internet Information Services (IIS) Manager dialog box, click **No**.
6. In Server1 Home, double-click **Server Certificates**.
7. In Server Certificates, in Actions, click **Create Domain Certificate**.
8. In the Distinguished Name Properties page, complete the form using the following information, and then click **Next**.

Item	Value
Common Name	***.contoso.com**
Organization	**Contoso Ltd**
Organizational Unit	**Information Technology**
City/locality	**Redmond**
State/province	**WA**
Country/region	**US**

9. On the Online Certification Authority page, click **Select**.

   📌 If Select is not available, exit the wizard, and then repeat steps 7 through 9.

10. On the Select Certification Authority page, select **ContosoSubCA**, and then click **OK**.
11. In Friendly Name, type **Contoso-Wildcard**, and then click **Finish**.
12. In Internet Information Services (IIS) Manager, navigate to **Server1/Sites/Default Web Site**.
13. In the Actions pane, click **Bindings**.
14. In Site Bindings, click **Add**.
15. In Add Site Binding, in Type, select **https**, and in SSL Certificate, select **Contoso-Wildcard**, and then click **OK**.
16. In Site Bindings, click **Close**.
17. Open **Internet Explorer**, and then navigate to **https://Server1.contoso.com**.

    📌 The webpage will now be shown.

18. Close **Internet Explorer**.

Revoke a user certificate

In this task, you will revoke the user certificate for Ben Smith. This would be done if the certificate was compromised and needed to be revoked or if it has expired.

✎ Ensure you are logged on to **SubCA** as **Contoso\Administrator** using the password **Passw0rd!**

1. In Server Manager, in Tools, click **Certification Authority**.
2. In certsrv, expand **Certification Authority/ContosoSubCA/Issued Certificates**.

   📌 All of the issued certificates – the Computer, User and Web Server certificates – are shown. Each of the certificates has a unique Request ID and Serial Number.

3. Click the certificate requested by **Contoso\BenSmith**, and then on the Action menu, click **All Tasks, Revoke Certificate**.

   📌 Note that a reason for revocation is required and the date and time can be set in the past.

4. In the Certificate Revocation dialog box, in Reason code, select **Superseded**, and then click **Yes**.
5. In certsrv, expand **Certification Authority/ContosoSubCA/Revoked Certificates**.

   📌 The Revoked certificate is shown.

   📌 The revocation action could also be performed in Windows PowerShell using the command *certutil –revoke <serial number> [Reason]*.

   📌 In the lab environment, you don't have an application that uses the certificate, and you also don't want to wait for the CRL publishing time period to see the effect. Instead, you will publish the CRL and then see that the certificate is now on the CRL.

6. In certsvr, click **Revoked Certificates**, and then on the Action menu, click **All Tasks**, **Publish**.
7. In the Publish CRL dialog, click **OK**.
8. Switch to **Client1**, and then log on as **Contoso\Administrator** using the password **Passw0rd!**
9. Open **Internet Explorer**, and then navigate to **http://subca.contoso.com/certsrv**.
10. In the Windows Security dialog box, enter **Contoso\Administrator** using the password **Passw0rd!** and then click **OK.**
11. In Internet Explorer, click **Download a CA certificate, certificate chain, or CRL**.
12. In Internet Explorer, click **Download latest base CRL** and then click **Open** twice.
13. In the Certificate Revocation List dialog, click the **Revocation List** tab.
14. In Revoked Certificates, select the entry.
    - 📌 This is the user certificate you have revoked.
15. Click **OK**.

Renew a computer certificate.

In this task, you will renew the computer certificate for Server1. Server1 is being placed into a location that it will not have access to SubCA and you are concerned that the certificate may expire before it will be able to renew it. You want extend the lifetime as long as possible (bound by the template restrictions).

✎ Ensure you are logged on to **Server1** as **Contoso\Administrator** using the password **Passw0rd!**

1. On the Start screen, type **MMC**, and then select **MMC** from the results.
2. In Console1, on the File menu, click **Add/Remove Snap-ins**.
3. In Add or Remove Snap-ins, select **Certificates**, and then click **Add**.
4. In the Certificates snap-in dialog box, select **Computer account**, and then click **Next**.
5. On the Select Computer dialog box, click **Finish**.
6. In Add or Remove Snap-ins, click **OK**.
7. In Console1, expand **Certificates (Local Computer), Personal, Certificates**.
8. Select **Server1.contoso.com**, and then on the Action menu, click **All Tasks, Advanced Operations, Renew this Certificate with the Same Key**.
9. In the Certificate Enrollment dialog box, click **Next**.
10. In the Request Certificates page, click **Enroll**.
11. In the Certificate Installation Results, click **Finish**.
    - 📌 The expiry date will have been extended. In the lab environment you will not see a modification as you are renewing the certificate on the same day that it was originally issued.

- 📌 Using Windows PowerShell it is possible to easily and quickly see what certificates will be expiring within a period of time using the command *Get-ChildItem -Recurse* | *where { $_.notafter -le (get-date).AddDays(75) }* | *select thumbprint, subject* In the cert: location in Windows PowerShell. In this example all the certificates that are due to expire in the next 75 days will be displayed.

12. Close **Console1**.

This is the end of the lab