Applies To: Windows 7, Windows Server 2008 R2

You can use these procedures to create a self-signed certificate using Internet Information Services (IIS), and then export the certificate for use on client computers.

You must be a member of the IIS 7 Administrators group to perform this procedure.

## To create a self-signed certificate

- 1. On Hosted-01, click **Start**, click **Run**, and then type **mmc**. The Microsoft Management Console (MMC) opens.
- In the MMC, click File, and then click Add/Remove Snap-in. The Add or Remove Snap-ins dialog box opens. In Available snap-ins, click Internet Information Services (IIS) Manager, and then click Add. Click OK.
- 3. In the IIS console, double click **Internet Information Services (IIS) Manager**, and then click **Hosted-01 (HOSTED-01)**.



4. In Hosted-01 Home, scroll to and double-click Server Certificates.

Console1 - [Console Root\Internet Information Service File Action View Favorites Window Help	s (IIS) Manager]	
← ⇒ Ž II Z Console Root Internet Information St Connections	)1 ►	Actions
Start Page HOSTED-01 (HOSTED-01	HOSTED-01 Home	Open Feature Manage Server Comparison Compar
	Management	Online Help

5. In Actions, click Create Self-Signed Certificate.

←	-01 >	<b>1</b>
Connections Start Page HOSTED-01 (HOSTED-01 Application Pools Sites Sites	Server Certificates Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.          Name       If         Image: Server can use with Web sites       If         Image: Server can use with Web sites       If         Image: Server can use with Web sites       If         Image: Server can use       Image: Server can use         Image: Server can use       Image: Server can use	Actions Import Create Certifica Complete Certifi Create Domain ( Create Self-Sign ( Help Online Help

6. The **Create Self-Signed Certificate** page opens. In **Specify a friendly name for the certificate**, type **BranchCache**.

Create Self-Signed Certificate	? ×
Specify Friendly Name	
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:	
Specify a friendly name for the certificate:	
BranchCache	
OK Can	cel (

7. Click **OK**. IIS Manager creates a self-signed certificate named **BranchCache**, which is displayed in IIS Manager. Do not close the MMC, as it is used in the next procedure.

You can use the following procedure to export the BranchCache certificate to a folder location on Hosted-01.

You must be a member of the Administrators group to perform this procedure.

## To export the BranchCache certificate

1. In the MMC, click **File**, and then click **Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog box opens. In **Available snap-ins**, click **Certificates**, and then click **Add**.

## Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor Microsoft Cor			Remove
Certificates Component Services	Microsoft Cor Microsoft Cor			Move Up
Device Manager	Microsoft Cor			Move Down
Disk Management	Microsoft and		Add >	
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
Internet Information	Microsoft Cor			
IP Security Monitor	Microsoft Cor			
IP Security Policy Ma	Microsoft Cor			
Link to Web Address	Microsoft Cor	-		Advanced
scription:				
ne Certificates snap-in allo	ows you to browse	the c	ontents of the certificate stores for yourse	elf, a service, or a computer.
				OK Cance

2. The **Certificates snap-in** page opens. On the **Certificates snap-in** page, click **Computer account**, and then click **Next**.

rtincates snap-in	of snap-ins. For
This snap-in will always manage certificates for:	
C My user account	Edit Extensions.
O Service account	
Computer account	Remove
	Move Up
	Move Down
	Advanced
< Back Next > Ca	ncel r a computer.

3. In Select Computer, ensure that Local computer is selected, and then click Finish.

- This same is will show man	uns snaphn to manage.	
Inis snap-in will always man     O	age:	Edit Extensions.
C Another computer:	Browse	Remove
Allow the selected com	puter to be changed when launching from the command line. This	Move Up
		Move Down
		Advanced
	< Back Finish Cancel	r a computer.

- 4. Click **OK**. The Certificates snap-in is added to the same MMC that contains the IIS Manager snap-in. In the MMC, double-click **Certificates** (**Local Computer**), double-click **Personal**, and then click **Certificates**. In the details pane, the BranchCache certificate issued to **Hosted-01** is displayed.
- 5. Right-click Hosted-01, click All Tasks, and then click Export.



- 6. The Certificate Export Wizard opens. Click Next.
- 7. In **Export Private Key**, ensure that **No**, **do not export the private key** is selected, and then click **Next**.

ertificate Export Wizard	
Export Private Key	
You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key wit certificate, you must type a password on a later page.	h the
Do you want to export the private key with the certificate?	
O Yes, export the private key	
No, do not export the private key	
· · · · · · · · · · · · · · · · · · ·	
Learn more about exporting private keys	
A Back Nexts	Cancel
	Cancer

8. In **Export File Format**, ensure that **DER encoded binary X.509** (.CER) is selected, and then click **Next**.

kport Wizard		
xport File Format Certificates can be exported in a variety of file formats.		
the format you want to use:		
DER encoded binary X.509 (.CER)		
Base-64 encoded X.509 (.CER)		
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)		
Personal Information Exchange - PKCS #12 (.PFX)  Include all certificates in the certification path if possible		
Delete the private key if the export is successful Export all extended properties		
Microsoft Serialized Certificate Store (.SST)		
about certificate file formats		

- 9. In **File to export**, click **Browse**, and then navigate to a folder location where you want to save the certificate. In **File name**, type **BranchCache**, and then click **Save**. The Browse dialog box closes and the **File to export** page is displayed with the file location and file name that you selected. For example, if you selected a file location of **C:** and a file name of **BranchCache**, **C:\BranchCache.cer** is displayed.
- 10. Click **Next**, and then click **Finish**. An information dialog box opens that displays the message **The export was successful**. Click **OK**.

ertificate Export Wizard		
	Completing the Certificate E Wizard You have successfully completed the Certificate wizard.	Export
	File Name Export Keys Include all certificates in the certification path File Format	C:\User No No DER En
	Certificate Export Wizar	d 🗙

11. If needed, click **Finish**. Using Windows Explorer, navigate to the file location where you saved the certificate. Copy the certificate and save the certificate to a file location on both Client-01 and Client-02.

## **1**. Requesting the Root Certification Authority Certificate by using command line:

- a. Log into the Root Certification Authority server with Administrator Account.
- b. Go to "Start" -> "Run" -> and write "Cmd" and press on "Enter" button.
- c. To export the Root Certification Authority server to a new file name "ca\_name.cer"

write:

"certutil -ca.cert ca\_name.cer". (replace ca\_name with whatever your cert authorities name is)