Obtain a Certificate on Windows Server 2008 R2 and 2012 (Without Using IIS)

Overview

This page describes how to obtain a certificate on Windows Server 2008 R2 or 2012 without using IIS Manager. The version of certmgr.msc supplied with Windows 2003 is different and these instructions do not apply.

Step 17 of this document will generate a Certificate Signing Request (CSR) that allows the private key to be exported. Sometimes this is required because the certificate will be used on multiple hosts (clustering environment) or the application that will use the certificate can't access the Windows certificate store. CSRs with exportable keys cannot be generated from IIS Manager–you must use the Windows certificate manager.

Procedure

Generate a Certificate Signing Request (CSR)

1. Log in as an administrator
2. From a command prompt or the run menu:
    a. To create the certificate in the local machine store (recommended):
        i. Type **mmc**
        ii. On the **File** menu, click **Add/Remove Snap-in**. Click **Certificates** in the left pane, then click **Add**.
        iii. Select **Computer Account**, then click **Next**.
        iv. Select **Local Computer**, then click **Finish.**
        v. Click **OK**.
    b. To create the certificate in the logged on user's personal store:
        i. Type **certmgr.msc**
3. In the left pane expand **Certificates (Local Computer)**, expand **Personal**, then click **Certificates**.
4. On the **Action** menu, click **All Tasks**, then click **Advanced Operations**, then click **Create Custom Request**.
5. Click **Next**.
6. Select **Proceed without enrollment policy**. Click **Next**.
7. In the **Template** menu, select **(No template) CNG key**, and verify that **Suppress default extensions** is not selected. (**Note:** Some software may not be compatible with CNG keys. In this case, select **(No template) Legacy key**)(**Note:** specifically, the .Net X509Certificate2.PrivateKey method will throw an exception on CNG keys and ADFS 3.0 will refuse to accept them.)
8. Under **Request Format**, select **PKCS #10**. Click **Next**.
9. Click the arrow next to **Details** to expand the selection. Click **Properties**.
10. On the **General** tab, provide a **Friendly name** and **Description** for the certificate. These can be anything you want.
11. On the **Subject** tab, in the **Subject name** box:
    a. In the **Type** menu**,** select **Common name**. In the **Value** field, type the fully qualified domain name of the server (e.g. *myhost*.washington.edu), and click **Add**.
    b. In the **Type** menu**,** select **Organization**. In the **Value** field, type **University of Washington**. Click **Add**.
    c. In the **Type** menu**,** select **State**. In the **Value** field, type **WA**. Click **Add**.
    d. In the **Type** menu**,** select **Country**. In the **Value** field, type **US**. Click **Add**.
    e. (Optional) In the **Type** menu, select **Email**. In the **Value** field, type a contact email address. Click **Add**.
12. (Optional) On the **Subject** tab, in the **Alternative name** box, enter subject alternative names if you need them (these can also be requested when you submit the CSR).
13. (Optional) If you want to restrict how this certificate can be used, you can select the appropriate options under **Key usage** and **Extended Key Usage** on the **Extensions** tab.
14. On the **Private Key** tab, expand **Cryptographic Service Provider**. Select **RSA, Microsoft Software Key Storage Provider**. Make sure no other options are selected. (**Note:** If you selected **(No template) Legacy key** in Step 7, select **Microsoft RSA SChannel Crytographic Provider (Encryption)** instead. This option is usually at the end of the list.).
15. On the **Private Key** tab, expand **Key Options**.
16. In the **Key size** menu, select a value of at least 2048.
17. Select **Make private key exportable**. This step is only required if you will use this certificate on another computer (e.g. in a clustered environment), or with an application that does not use the Windows certificate store (e.g. Mozilla Firefox).
18. Click **OK**.
19. Click **Next**.
20. Choose a file name and location for the CSR. Select **Base 64**. Click **Finish**.
21. Submit the CSR to the InCommon or UW CA. For details on this process see UW Certificate Services.

If you generate a lot of CSRs, you may find it easier to install OpenSSL and generate them from the command line–OpenSSL for Windows is available at:

http://slproweb.com/products/Win32OpenSSL.html

OpenSSL can also convert certificates to and from various formats.

Install the Certificate

1. Download your signed certificated from the UW Certificate Services tool. For details on this process see UW Certificate Services.
2. Log in as an administrator
3. From a command prompt or the run menu:
    a. To create the certificate in the local machine store (recommended):
        i. Type **mmc**
        ii. On the **File** menu, click **Add/Remove Snap-in**. Click **Certificates** in the left pane, then click **Add**.
        iii. Select **Computer Account**, then click **Next**.
        iv. Select **Local Computer**, then click **Finish.**
        v. Click **OK**.
    b. To create the certificate in the logged on user's personal store:
        i. Type **certmgr.msc**
4. In the left pane expand **Certificates (Local Computer)**, expand **Personal**, then click **Certificates**.
5. On the **Action** menu, click **All Tasks**, then click **Import**.
6. Click **Next**. On Windows Server 2012 this screen presents an option to "select" a certificate store, but the correct store is already selected, and you can't change it.
7. Select the signed certificate you downloaded in Step 1. Click **Next**.
8. Select **Place all certificates in the following store**. Under **Certificate Store**, make sure **Personal** is selected. Click **Next**.
9. Verify the information on the screen and click **Finish**.

See also

- How to Request a Certificate With a Custom Subject Alternative Name (Microsoft)