Generate CSR and install SSL on IIS servers in Load Balanced Environment - SSL Behind a Load Balancer

To install SSL certificate in a Load Balanced environment, for example with 3 host web servers.

- **On the first server create a certificate request - CSR by doing the following:**

Generating a CSR (IIS7)

1. From **Start**, select **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
2. In the Connections panel on the left, click the server name for which you want to generate the CSR.
3. In the middle panel, double-click **Server Certificates**.
4. In the **Actions** panel on the right, click **Create Certificate Request**....
5. Enter the following **Distinguished Name Properties**, and then click **Next**:
6. NOTE: The following characters are not accepted when entering information: ~ ! @ # $ % ^ * / \ ( ) ? &
    - **Common Name** — The fully-qualified domain name (FQDN) — or URL — for which you plan to use your certificate (the area of your site you want customers to connect to using SSL).
        - An SSL certificate issued for *www.domain.com.au* is not valid for *sub.domain.com.au*. If you want your SSL to cover *sub.domain.com.au*, make sure the common name submitted in the CSR is *sub.domain.com.au*.
        - If you are requesting a wildcard certificate, add an asterisk (*) on the left side of the Common Name (e.g.,**.domain.com.au* or **.sub.domain.com.au*).
    - **Organization** — The name in which your business is legally registered. The organization must be the legal registrant of the domain name in the certificate request.
    - NOTE: If you are enrolling as an individual, enter the certificate requester's name in the Organization field, and the Doing Business As (DBA) name in the Organizational Unit field.
    - **Organizational Unit** — Use this field to differentiate between divisions within an organization (such as "Digital" or "IT").
    - **City/Locality** — The full name of the city in which your organization is registered/located. Do not abbreviate.
    - **State/Province** — The full name of state or province where your organization is located. Do not abbreviate.
    - **Country** — The two-letter International Organization for Standardization- (ISO-)

format country code for the country in which your organization is legally registered.

7. For Cryptographic service provider, select **Microsoft RSA SChannel Cryptographic Provider** .
8. For Bit length, select **2048**, and then click **Next**.
9. Click …, enter the location and file name for your CSR, and then click **Finish**.

- **After CSR has been created, submit it to the Certification Authoroty (CA)**
- **When the certificate has been issued it is time to install it - to COMPLETE THE CSR REQUEST ON THE FIRST SERVER WHERE CSR WAS CREATED.**

Installing a SSL cert (IIS7)

1. Click **Start**, mouse-over **Administrative Tools**, and then click **Internet Services Manager**.
2. In the **Internet Information Services (IIS) Manager** window, select your server.
3. Scroll to the bottom, and then double-click **Server Certificates**.
4. From the Actions panel on the right, click **Complete Certificate Request**....
5. To locate your certificate file, click ....
6. In the **Open** window, select *.* as your file name extension, select your certificate (it might be saved as a .txt, .cer, or .crt), and then click Open.
7. In the **Complete Certificate Request** window, enter a **Friendly name** for the certificate file, and then click OK.
8. NOTE: For Wildcard SSL certificates make sure your Friendly Name to matches your Common Name (i.e. *.domain.com.au)

NEXT INFO IS ONLY FOR NEW CERTIFICATES - RENEWALS WILL ALREADY HAVE ALL THE INFO IN - YOU JUST HAVE TO SELECT THE RENEWED SSL IN EDIT SITE BINDING (BINDINGS>HTTPS>EDIT>SSL Certificate>Select the renewed one - if you named both old and renewed SSL with the same friendly name, you can select one and click view to see the expiry date)

1. In the **Internet Information Services (IIS) Manager** window, select the name of the server where you installed the certificate.
2. Click + beside **Sites**, select the site to secure with the SSL certificate.
3. In the Actions panel on the right, click **Bindings**....
4. Click **Add**....
5. In the **Add Site Binding** window:
    - For **Type**, select **https**.
    - For **IP address**, select **All Unassigned**, or the IP address of the site.
    - For **Port**, type **443**.

    - For **SSL Certificate**, select the SSL certificate you just installed, and then click OK.
6. Close the **Site Bindings** window.
7. Close the **Internet Information Services (IIS) Manager** window. Your SSL certificate installation is complete

- **Now we need to install the certificate on the other web servers behind Load Balancer. To do so we need to Export the certificate from the first server and import it into other two**

Exporting to a .pfx File on the first server where we installed the new(or renewed) SSL.

1. On the Start menu click **Run** and then type *mmc*.
2. Click **File > Add/Remove Snap-in**.
3. Click **Certificates > Add**.
4. Select **Computer Account** and then click **Next**. Select **Local Computer** and then click **Finish**. Then close the add standalone snap-in window and the add/remove snap-in window.
5. Click the **+** to expand the certificates (local computer) console tree and look for the personal directory/folder. Expand the certificates folder.
6. Right-click on the certificate you want to backup and select **ALL TASKS > Export**.
7. Choose **Yes, export the private key** and **include all certificates in certificate path if possible**.
8. Warning: Do not select the delete private key option.
9. Leave the default settings and then enter your password if required.
10. Choose to save the file and then click **Finish**. You should receive an "export successful" message. The .pfx file is now saved to the location you selected

- **After we exported the certificate from the first server, it needs to be imported in the rest of the servers. Follow this procedure on any remaining web server**

Importing from a .pfx File

1. On the Start menu click **Run** and then type *mmc*.
2. Click **File > Add/Remove Snap-in**.
3. Click **Certificates > Add**.
4. Select **Computer Account** and then click **Next**. Select **Local Computer** and then click **Finish**. Then close the add standalone snap-in window and the add/remove snap-in

window.

5. Click the **+** to expand the certificates (local computer) console tree and look for the personal directory/folder. Expand the certificates folder.
6. Right-click on the certificate you want to backup and select **ALL TASKS > Import**.
7. Follow the certificate import wizard to import your primary certificate from the .pfx file. When prompted, choose to **automatically place the certificates in the certificate stores based on the type of the certificate**.

- **When the importing is complete, you have to select the new certificate in the site bindings**

All done