**為DocTracker安裝SSL**

要增強DocTracker的安全性，應在Microsoft IIS上安裝SSL。
本文討論如何在IIS上安裝SSL，並配置DocTracker和OCR 伺服器以支持SSL。在繼續執行以下步驟之前，請停止所有OCR伺服器和DocTracker服務。

# 獲得SSL憑證

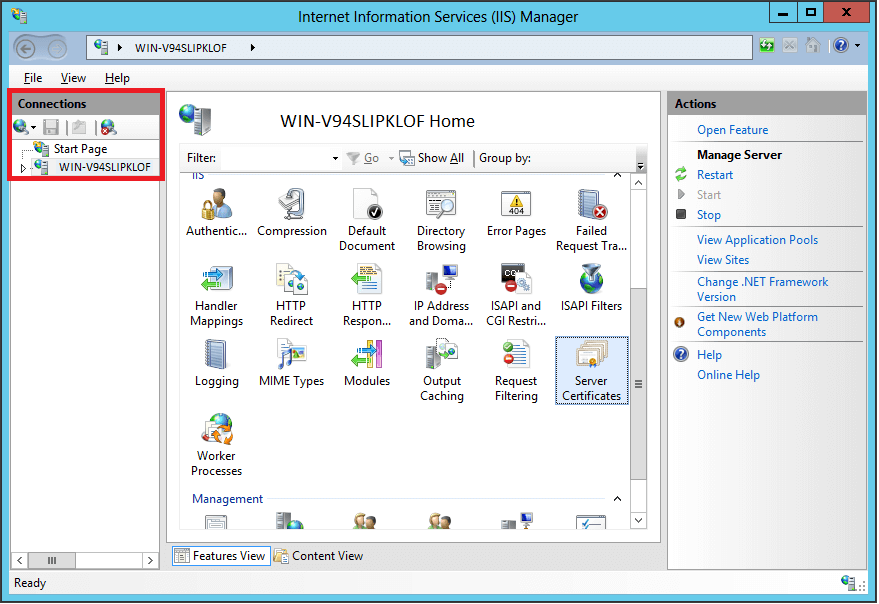
您需要獲取SSL憑證才能實施SSL。請按照以下步驟獲取憑證。

## 1. 打開 Internet Information Services (IIS) 管理員

單擊**“開始”，“控制台”，“系統管理工具”，**然後選擇**“Internet Information Services (IIS) 管理員”。**

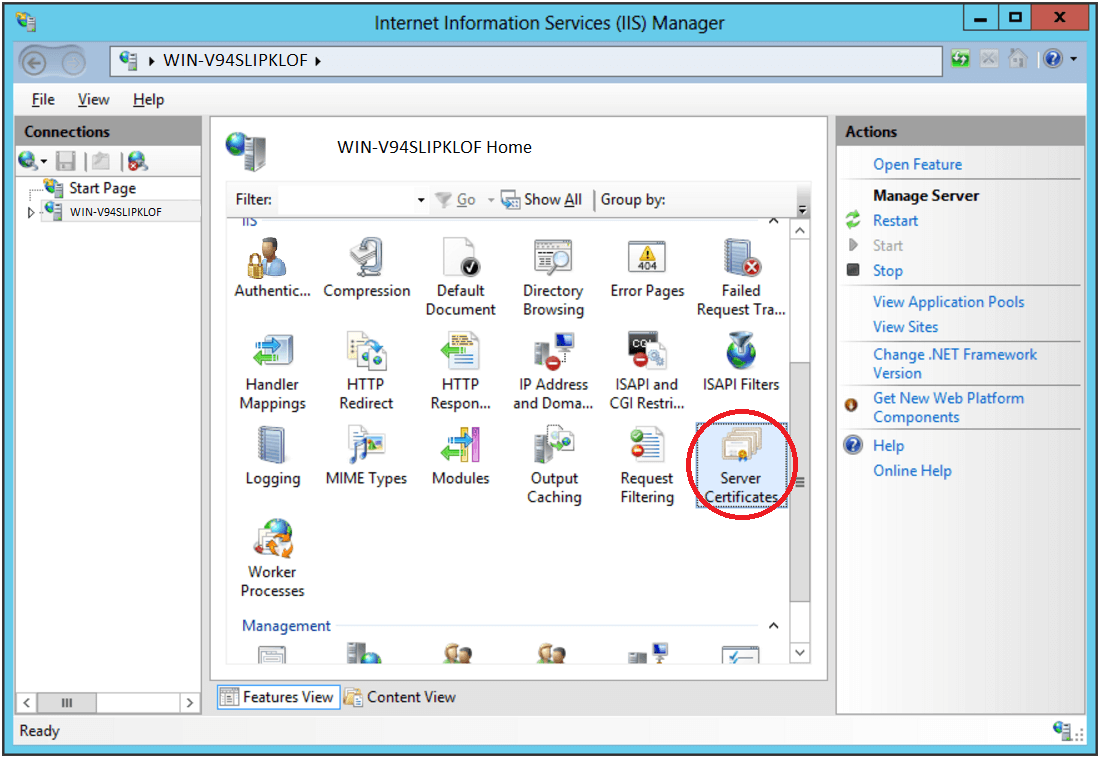
## 2. 選擇要生成憑證的伺服器。

In the left **Connections** menu, select the **server name** (host) where you want to generate the request.



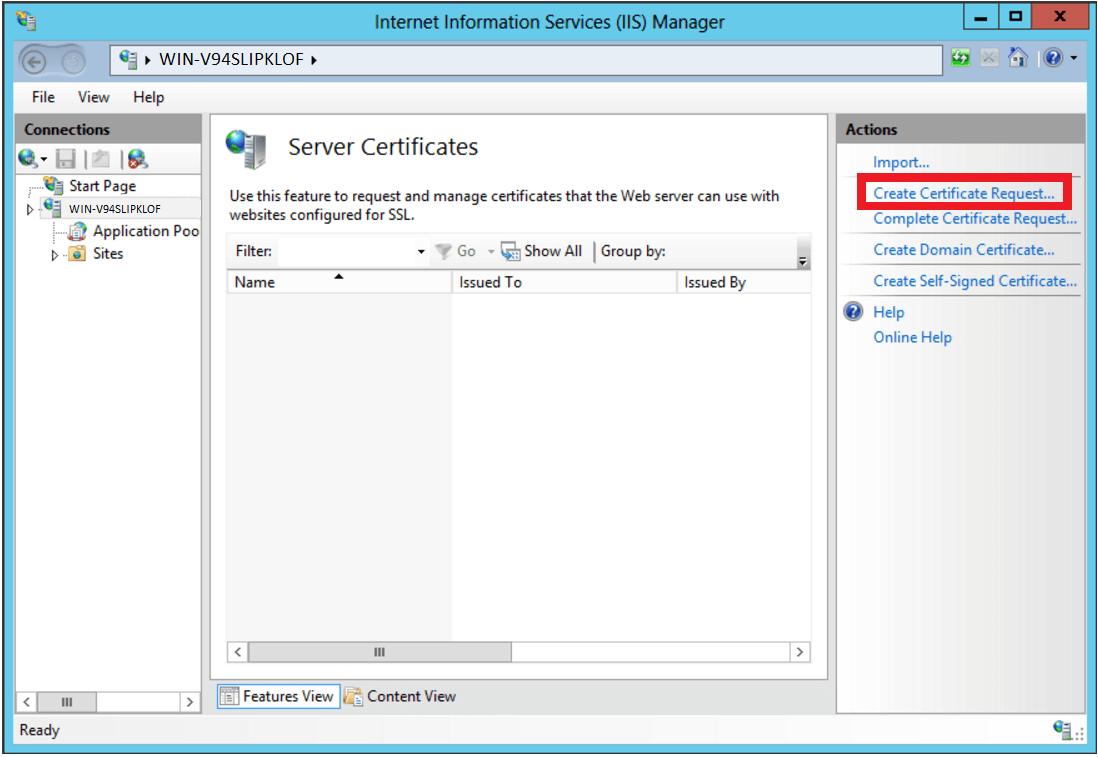
## 3. Navigate to Server Certificates

In the center menu, click the **Server Certificates**icon under the **Security**section near the bottom.



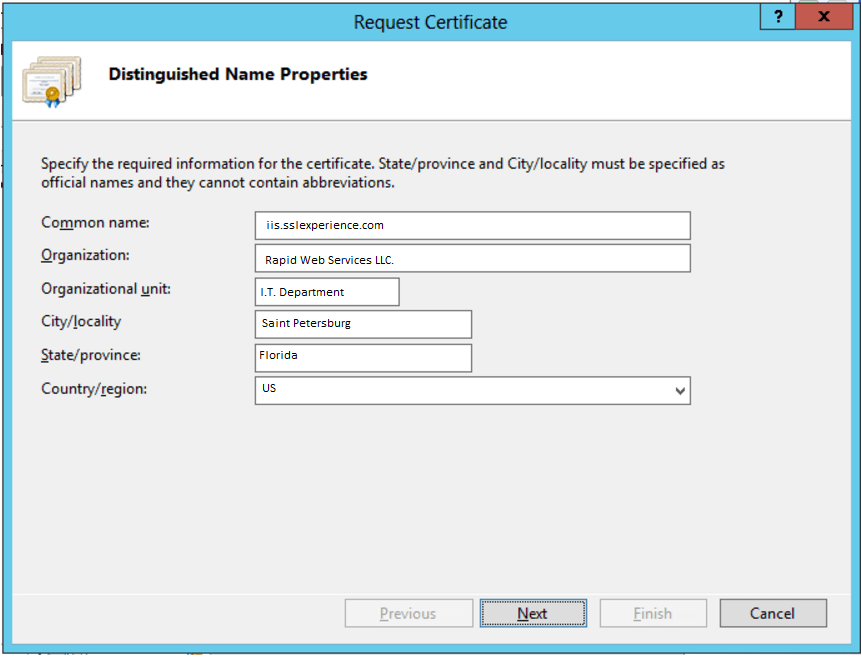
## 4. Select Create a New Certificate

In the right **Actions** menu, click **Create Certificate Request.**



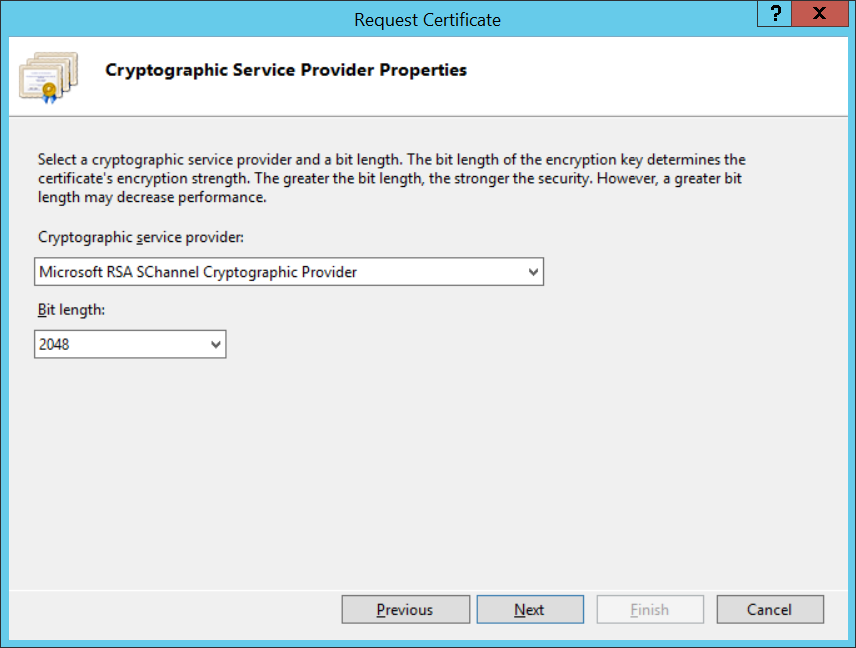
## 5. Enter your CSR details

In the **Distinguished Name Properties**window, enter in the required **CSR details**and then click **Next.**

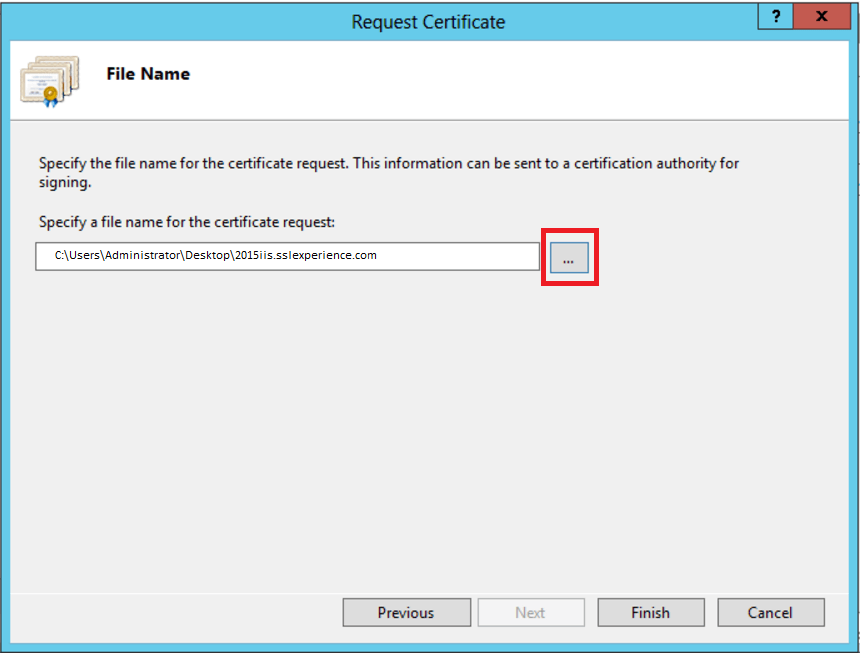


## 6. Select a cryptographic service provider and bit length

In the **Cryptographic Service Provider Properties**window, select **Microsoft RSA SChannel Cryptographic Provider**and **Bit Length** of **2048**, then click **Next.**

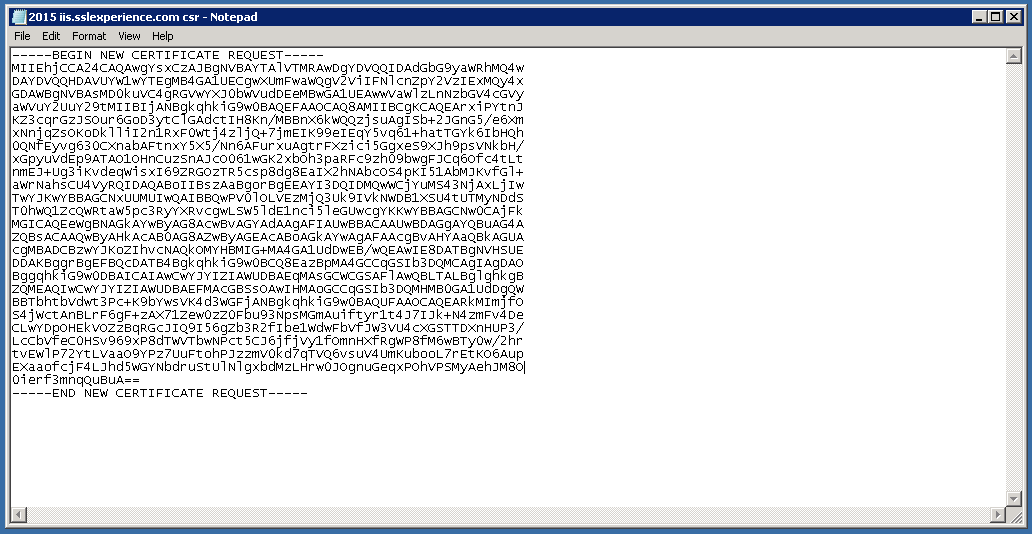


## 7. Save the CSR



## 8. Generate the Order

Locate and open the newly created CSR from the specified location you choose in a text editor such as Notepad and copy all the text including:



Upon generating your CSR, your order will enter the validation process with the issuing Certificate Authority (CA) and require the certificate requester to complete some form of validation depending on the certificate purchased. After you complete the validation process and receive the trusted SSL Certificate from the issuing Certificate Authority (CA), proceed with the next step of installing the SSL Certificate in IIS.

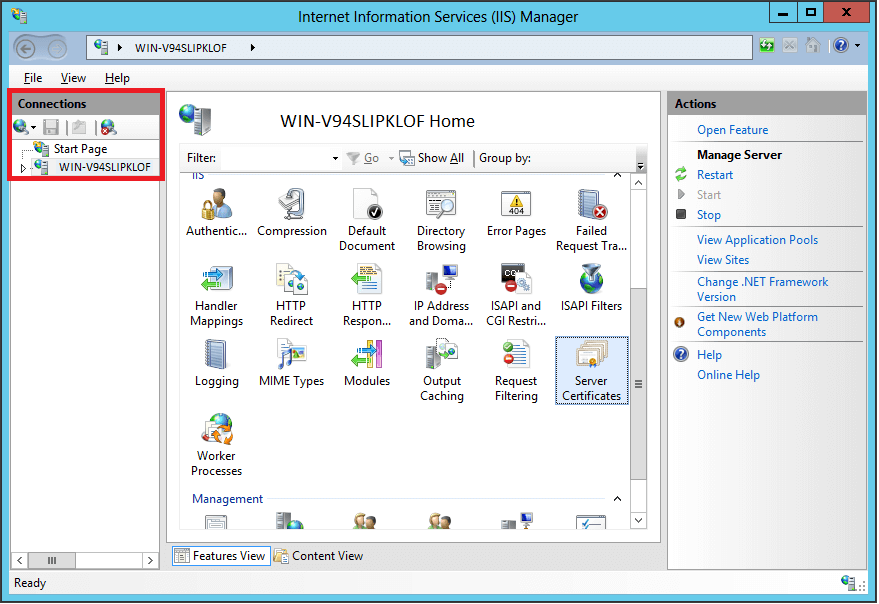
# Install SSL in IIS

### 1. Launch IIS Manager

單擊**“開始”，“控制台”，“系統管理工具”，**然後選擇**“Internet Information Services (IIS) 管理員”。**

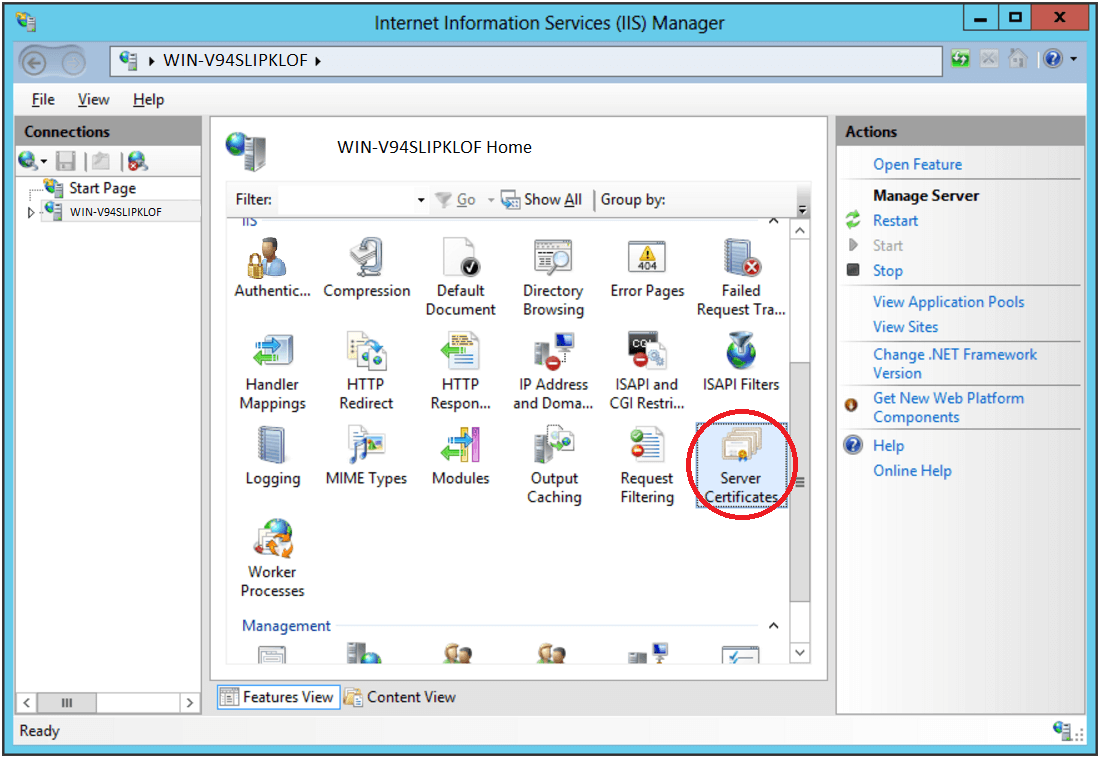
### 2. Select your server name

In the left **Connections** menu, select the **server name** (host) where you want to install the SSL certificate.



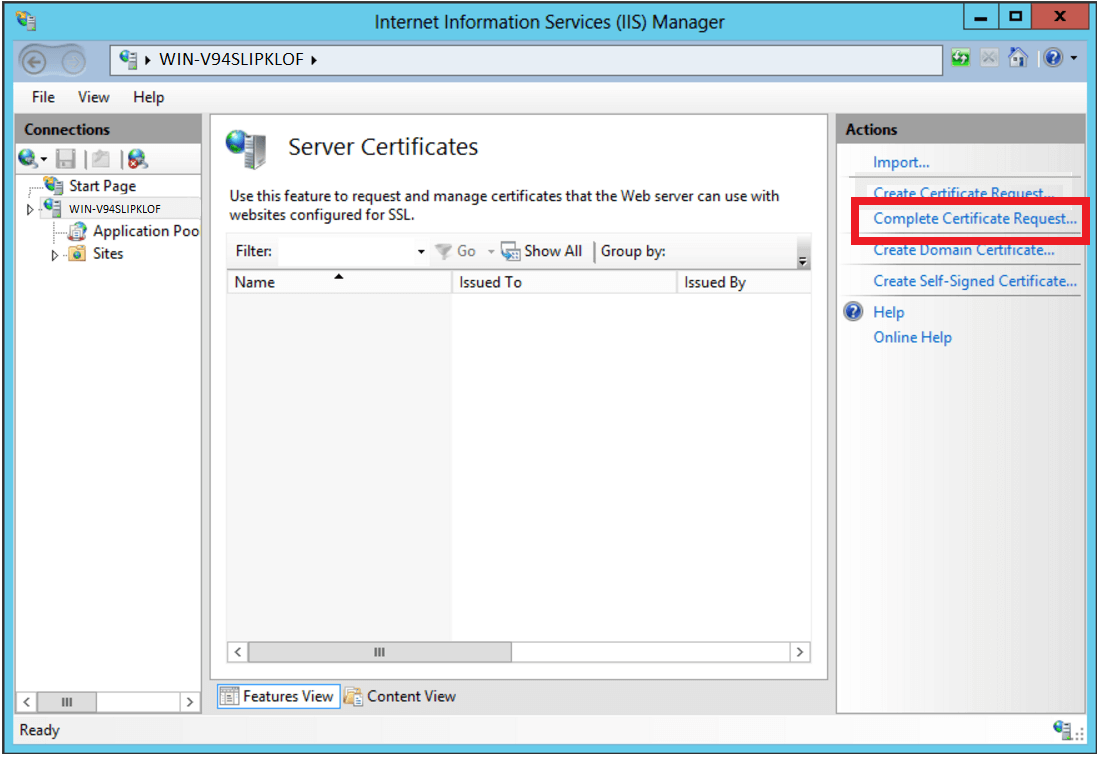
### 3. Click Server Certificates

In the center menu, click the **Server Certificates**icon under the **Security**section near the bottom.



### 4. Click Complete Certificate Request…

In the right **Actions**menu, click **Complete Certificate Request…**



### 5. Browse to your server certificate

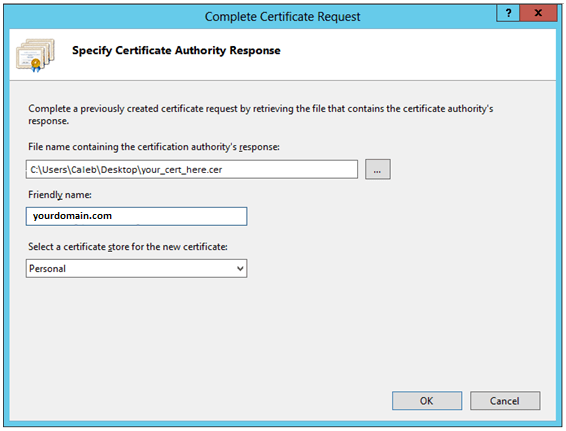
In the **Complete Certificate**Request wizard, click “**…**” to browse and select **Your Server Certificate** file that was previously saved on your server’s desktop.

### 6. Name your certificate

Enter a **Friendly Name,** which is an internal reference name to distinguish the file later. We recommend including the CAs name and expiration date.

### 7. Select Personal

Select **Personal** as your certificate store for the new certificate.

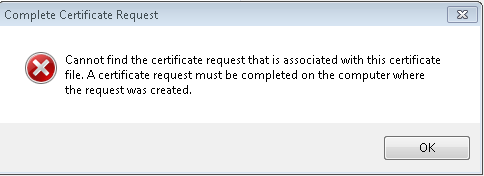


### 8. Click OK

Click **OK** and the newly installed certificate should appear in the refreshed Server Certificate List.

### 9. Additional case on IIS 7

When installing a certificate using Microsoft IIS 7 Manager, you may receive the following error message even though the certificate is installed.

  
NOTE: The certificate may still install successfully, in spite of the error message.

* 1. Cause  
     This issue occurs because IIS Manager performs a lookup operation to look for a friendly name of the certificate during the installation. However, the code that performs this lookup operation misses this specific case, and it does not know how to retrieve the friendly name of a certificate in a PKCS#7 file. Therefore, the lookup operation fails, and the error message is displayed.  
     This is a known issue with IIS 7. Please see Microsoft Knowledge Base Article 959216.
  2. Solution  
     To resolve this problem, check if the certificate is installed by performing the following steps:

**Step 1: Create a 'Certificates' snap-in within the MMC**

From IIS Web Server:  
1. Click **Start** > **Run** > type **MMC**  
2. From the **Microsoft Management Console (MMC)**, click **File** > **Add/Remove Snap-in**  
3. From the list of snap-ins, select **Certificates**  
4. Click **Add**  
5. Select **Computer Account**  
6. Click **Next**  
7. Select **Local Computer** (the computer this console is running on)  
8. Click **Finish**  
9. In the **Add/Remove Snap-in** window, click **OK**

**Step 2: Locate the SSL certificate**  
1. Go to **Personal** > **Certificates**  
2. Right-click the SSL Certificate  
3. Select **Properties**  
4. Enter a **Friendly Name** value  
5. Click **Apply**, then click **OK**  
6. Go back to **Personal** > **Certificates**  
7. Double-click on the SSL certificate

* 1. On the General tab, under the validity dates, there should be a key with the following message:

"You have a private key that corresponds to this certificate"

* 1. Close the certificate and the MMC

Reference link:  
<https://knowledge.digicert.com/solution/SO22029.html>

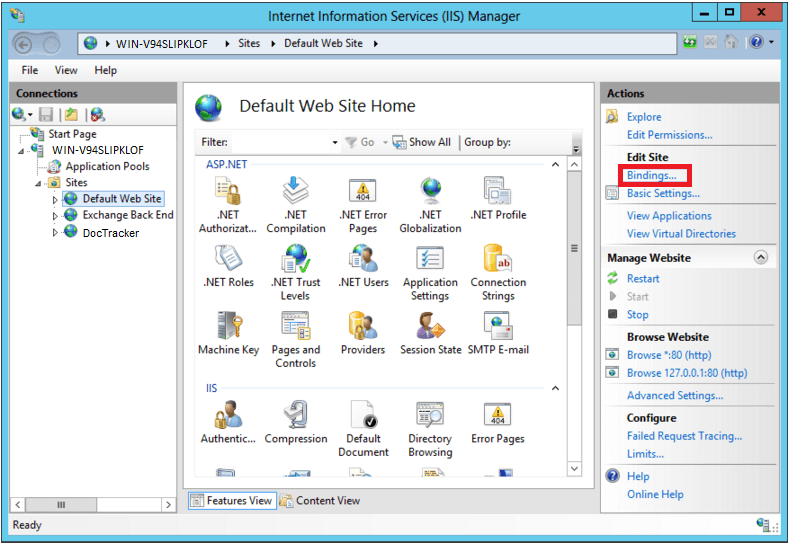
# Binding Your Certificate to Your Website

### 1. Access your Sites folder

From the left **Connections**menu, expand your server’s name, expand the **Sites**folder, and then select the site (e.g. DocTracker) that you want to secure.

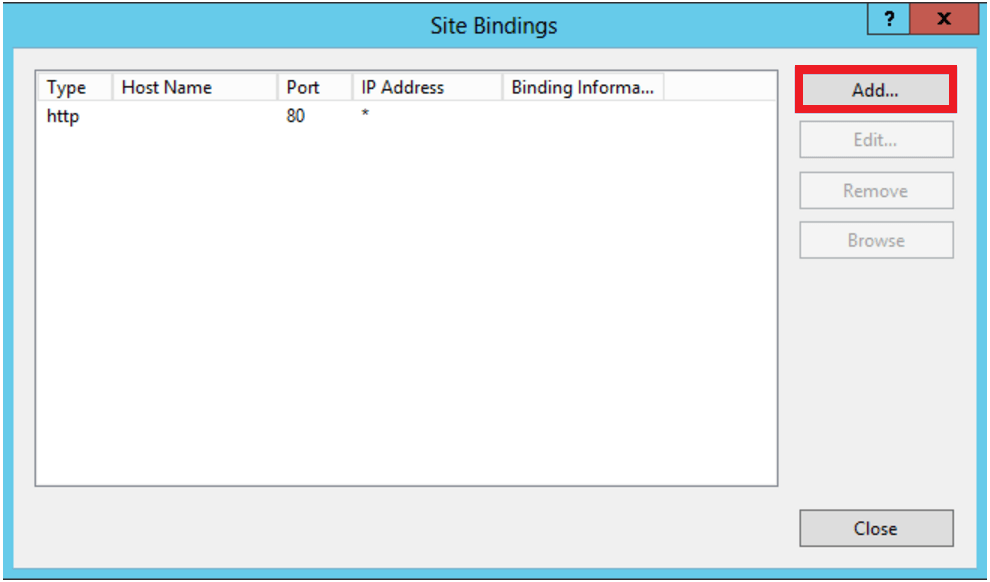
### 2. Click Bindings…

In the right **Actions**menu, click **Bindings…**



### 3. Click Add

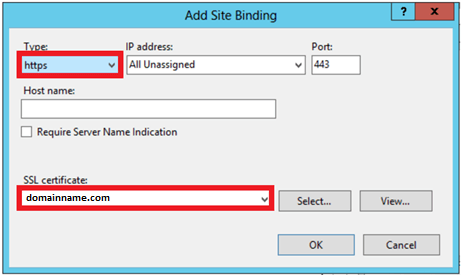
In **Site Bindings…**, click **Add.**



### 4. Input the following

In **Add Site Binding,**enter the following information:

1. **Type –** Select “https.”
2. **IP Address – Select “All unassigned.” Now, if you have multiple IP address, select the correct one that applies.**
3. **Port – Enter “443” unless you are listening to SSL traffic on another port (e.g. 992).**
4. **SSL Certificates – Select the “friendly name” of the SSL certificate you just installed.  You can always click “View” to confirm the certificates validity details.**



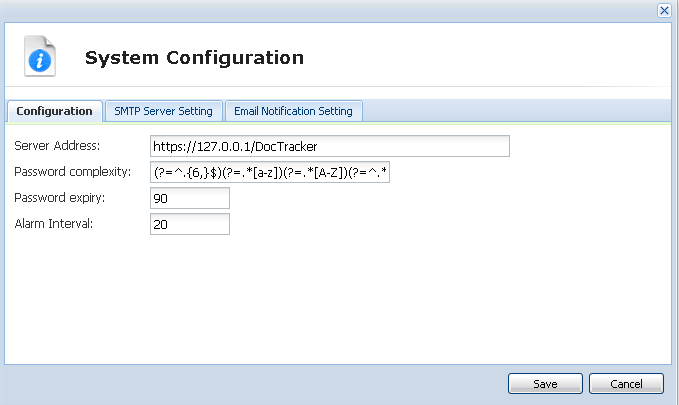
### 5. Click Ok

Click **Ok** to finish binding the SSL certificate to your live website.

# DocTracker Configuration

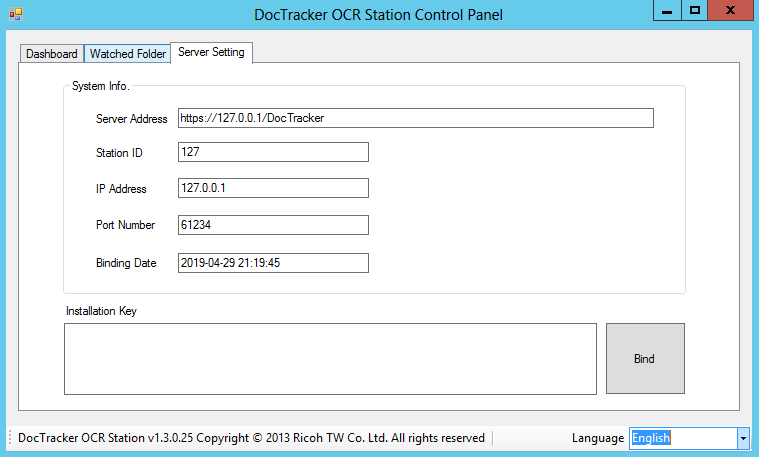
Once the DocTracker site is configured for SSL, follow the steps below to configure the DocTracker Server and OCR Station.

**DocTracker Server**

1. Logon DocTracker with a User of IT role.
2. Click the **System** menu and select the **System Configuration**. 
3. Change the **Server Address** value from http:// to https:// and click the **Save** button.
4. Click the **System** menu and select the **OCR Station Management**.
5. Click the **Installation key icon**. A text file with the OCR Installation Key will be created and downloaded to your desktop.
6. Follow the next steps to bind the OCR Station.

**OCR Station**

1. Launch the OCR Station Console.
2. Click the **Server Settings** tab.



1. Open the Installation key file and copy all of its content. Paste in the Installation Key text box.
2. Click the Bind button and the **Server Address** value will be changed to https://
3. Repeat the above steps for each OCR Station until every one of them is re-binded.
4. Now, DocTracker and OCR Station(s) are SSL enabled.