

Deploying Ekran System

The following steps are required for successful installation of Ekran System. Please see detailed instructions on deploying the system in the manual.

Step 1. Configure the computer where Management Tool will be installed.

- 1.1. [Turn on the Internet Information Service](#) (IIS) on your computer.
- 1.2. Install .NET Framework 4.5.
- 1.3. [Configure](#) the Internet Information Service.
- 1.4. Generate a self-signed certificate or import the purchased one.
- 1.5. Export a self-signed certificate and add it to [Trusted Root Certification Authorities](#).
- 1.6. [Set HTTPS binding](#) for default web-site.

Step 2. Install the Server.

- 2.1. For MS SQL database, install the full edition of MS SQL Server 2008 or higher with standard license or higher.
- 2.2. If the Server is not installed on the same computer with the Management Tool, install .NET Framework 4.5.
- 2.3. During installation, select the type of database (MS SQL or Firebird) and define the administrator's password that will be used when opening the Management Tool.
- 2.4. If during Server installation Firewall was turned off, add Server executable to the list of Firewall exceptions.

Step 3. Install the Management Tool.

- 3.1 If access to the Management Tool is performed from other computers, configure Firewall to enable remote access to the Management Tool.

Step 4. If the Clients are installed remotely on Windows operating system via the Management Tool, configure the computer where the Clients will be installed.

- 4.1. Make sure shared folders are accessible on the remote computer. For workgroup computers, simple file sharing must also be disabled.
- 4.2. Make sure the Server and Remote Procedure Call (RPC) system services are running on the target computer.
- 4.3. Configure Firewall on the target computer for remote Client installation.

Step 5. Install the Windows Clients.

- 5.1. Open the Management Tool: open the browser and enter `https://<name of the computer or IP on which the Management Tool is installed>/<URL address that has been specified during the Management Tool installation>` in the address line. For example, `https://john-pc/MyMonitoringSystem`.
Log in as admin using the password set at the Server installation.
- 5.2. Install the Clients remotely from the Management Tool.

Step 6. Install the Linux Clients.

6.1. Open the Management Tool: open the browser and enter `https://<name of the computer or IP on which the Management Tool is installed>/<URL address that has been specified during the Management Tool installation>` in the address line. For example, `https://john-pc/MyMonitoringSystem`.

Log in as admin using the password set at the Server installation.

6.2. Download Client installation files from the Management Tool.

6.3. Install the Clients locally using the Linux command line.

Step 7. License the Clients.

Step 8. Install Tray Notifications application if necessary.

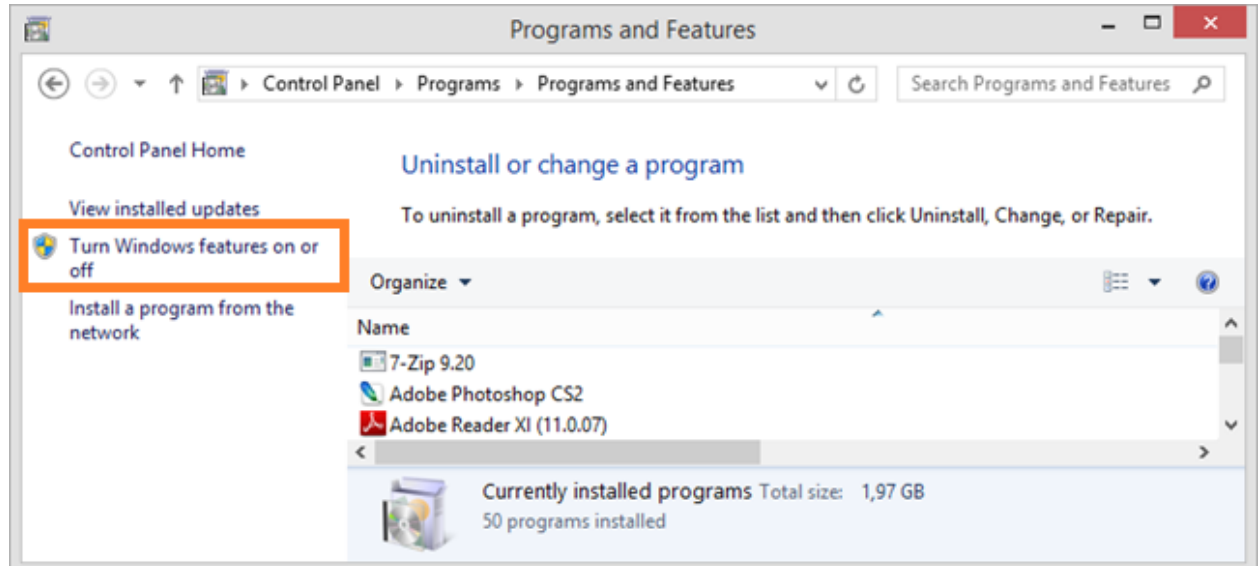
Appendices

Appendix 1. Turning on Internet Information Service (IIS)

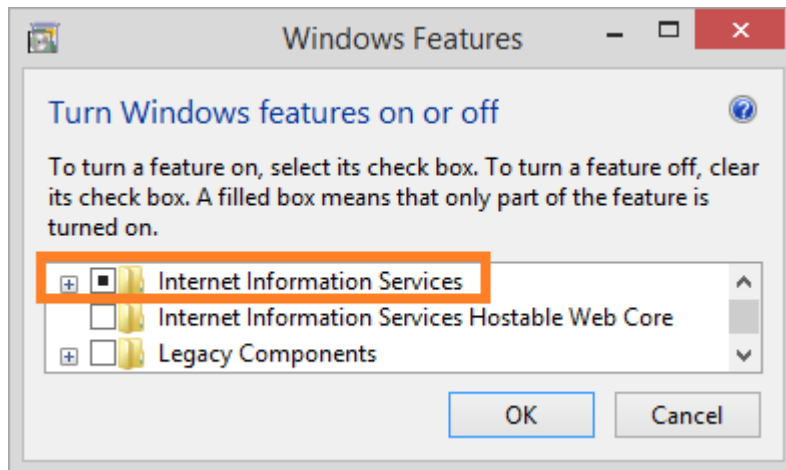
Turning on IIS for Windows 8, Windows 7, and Windows78

To turn on the Internet Information Service for Windows 8, Windows 7, and Windows Vista, do the following:

1. Select **Control Panel > Programs and Features** (Program uninstallation).



2. Click the **Turn Windows features on or off** navigation link.
3. The **Windows Features** window opens.
4. In the features tree-view, select the **Internet Information Services** check box.

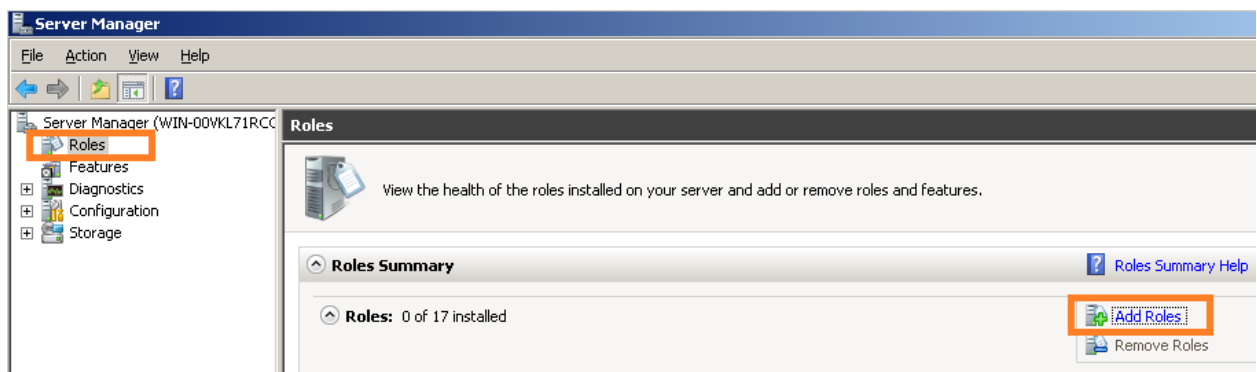


5. Click **OK**.

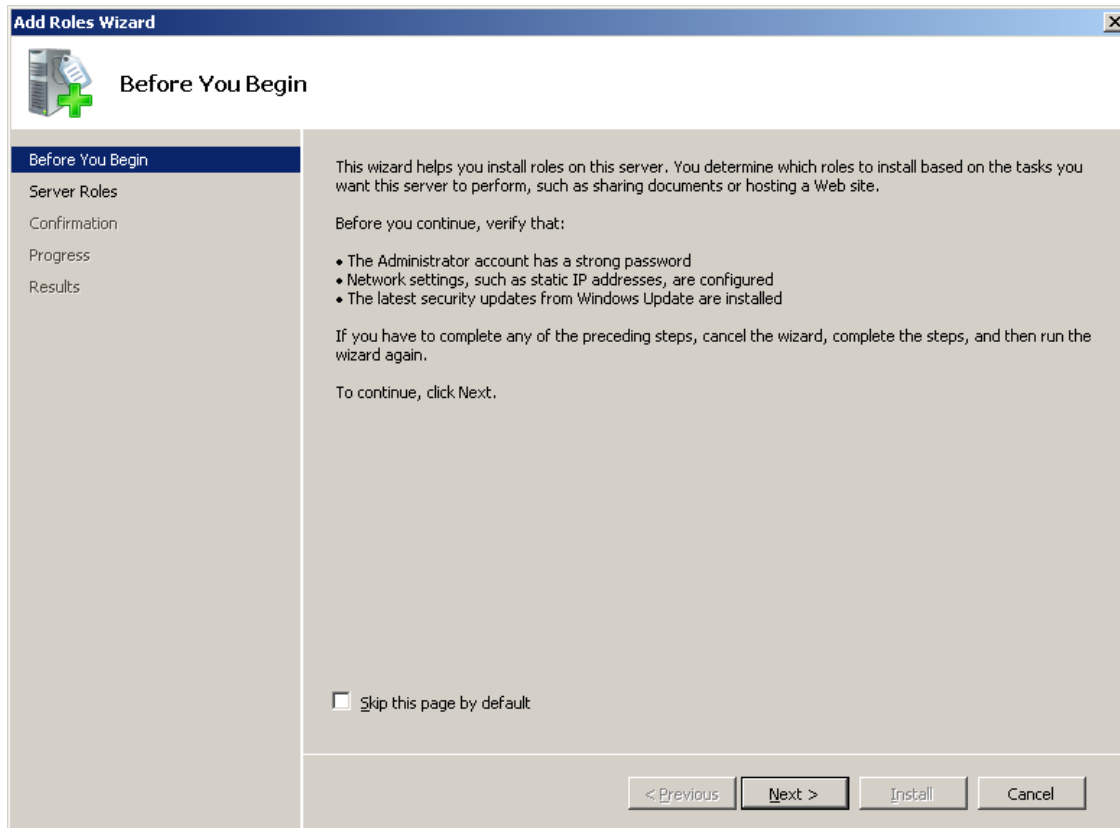
Turning on IIS for Windows Server 2008 and Windows Server 2008 R2

To turn on the Internet Information Service for Windows Server 2008 and Windows Server 2008 R2, do the following:

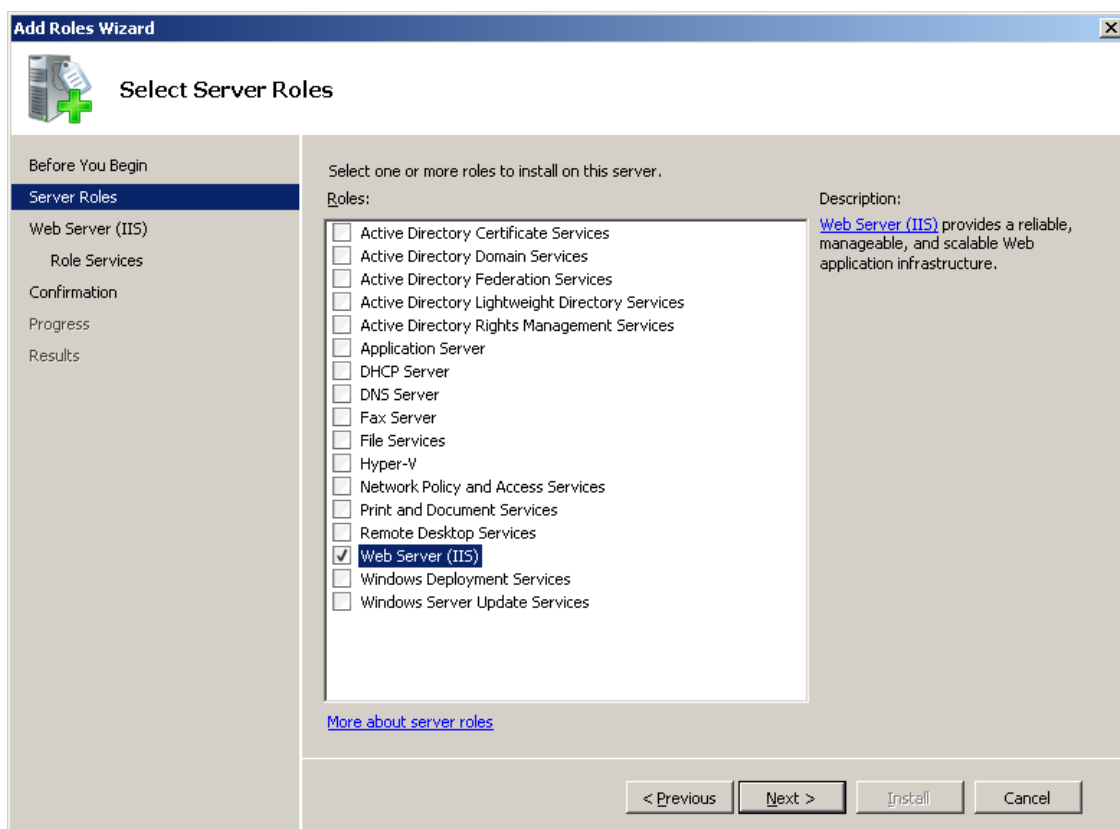
1. In the **Start** menu, select **All Programs > Administrative Tools > Server Manager**.
2. In the navigation pane, select **Roles**, and then click **Add Roles**.



3. The **Add Roles Wizard** opens.
4. On the **Before You Begin** page, click **Next**.



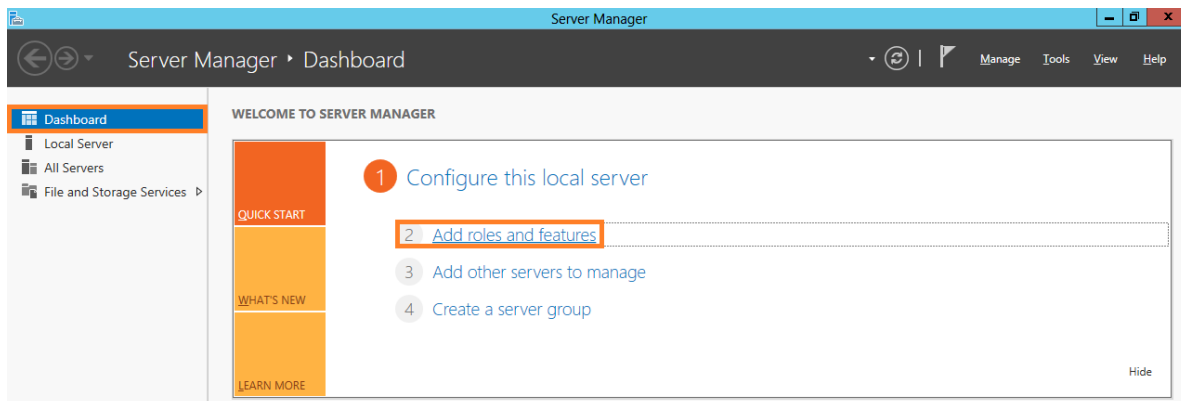
5. On the **Server Roles** page, select **Web Server (IIS)**, click **Next**, and then go to the **Role Services** page to start configuring **Web Server (IIS)**.



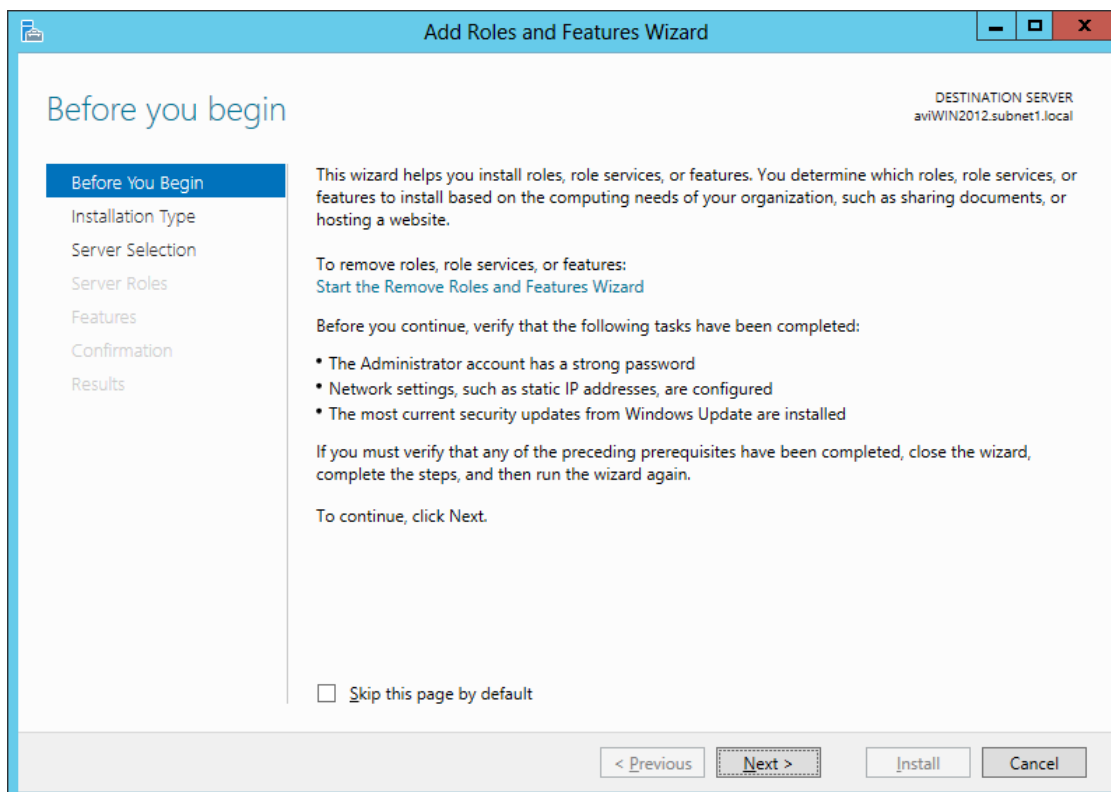
Turning on IIS for Windows Server 2012

To turn on the Internet Information Service for Windows Server 2012, do the following:

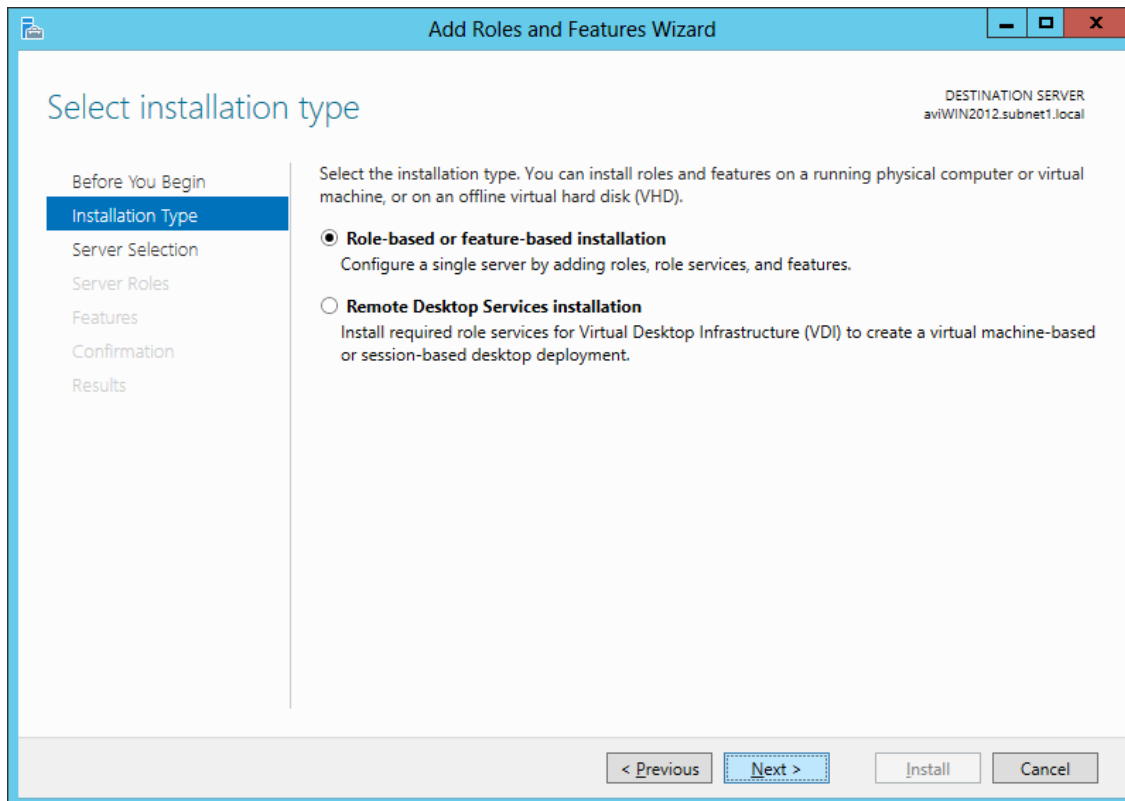
1. In the **Start** menu, select **Server Manager**.
2. In the navigation pane, select **Dashboard**, then click **Manage > Add roles and features**.



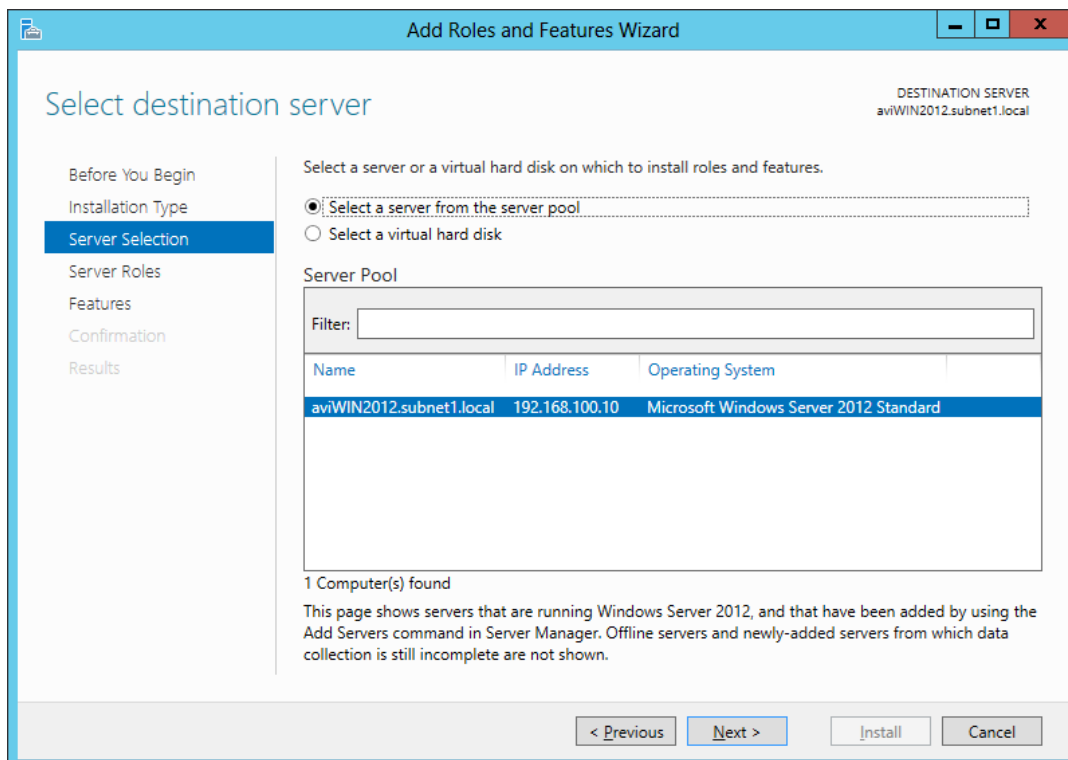
3. The **Add Roles and Features Wizard** opens.
4. On the **Before You Begin** page, click **Next**.



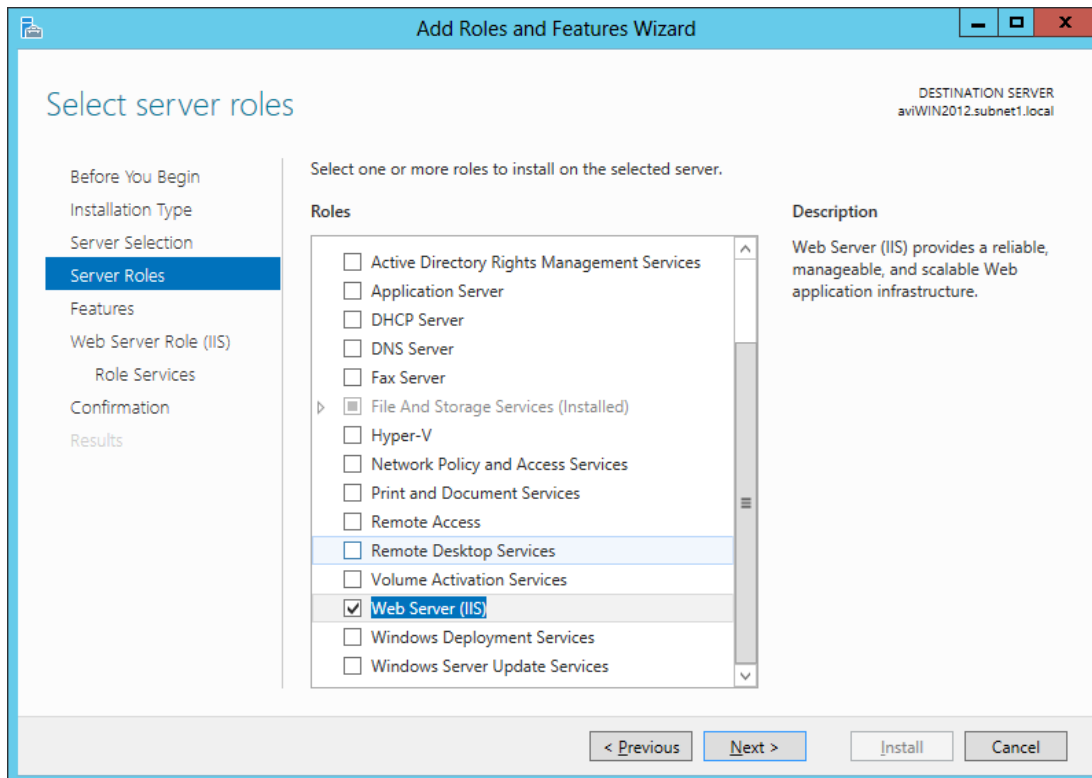
5. On the **Installation type** page, select **Role-based or feature-based installation**, and then click **Next**.



- On the **Server Selection** page, select **Select a server from the server pool**, select your server from **Server Pool** list, and then click **Next**.

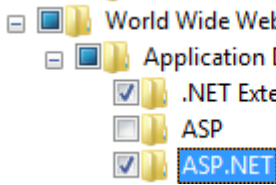
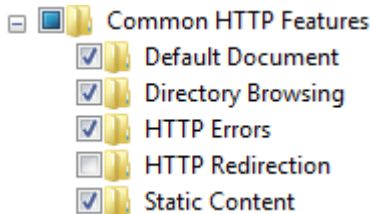
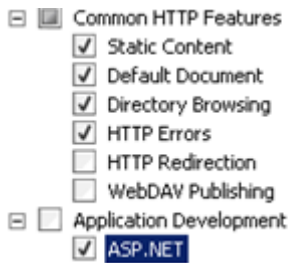


- On the **Server Roles** page, select **Web Server (IIS)**, click **Next** and then click **Add Features** to start configuring **Web Server (IIS)**.



Appendix 2. Configuring Internet Information Service (IIS)

Windows 8	Make sure that all the following check boxes are selected in the Windows Features window and then click OK: • .NET Framework 3.5 and .NET Framework 4.5 Advanced Services; ☒  .NET Framework 3.5 (includes .NET 2.0 and 3.0) ☒  Windows Communication Foundation HTTP Activation ☒  Windows Communication Foundation Non-HTTP Activation ☒  .NET Framework 4.5 Advanced Services • Internet Information Services > Web Management Tools > IIS Management Console; ☒  Internet Information Services ☒  FTP Server ☒  Web Management Tools ☒  IIS 6 Management Compatibility ☒  IIS Management Console • Internet Information Services > World Wide Web Services > Application Development Features > ASP.NET 3.5 and ASP.NET 4.5; ☒  .NET Extensibility 3.5 ☒  .NET Extensibility 4.5 ☐  Application Initialization ☐  ASP ☒  ASP.NET 3.5 ☒  ASP.NET 4.5 • Internet Information Services > World Wide Web Services > Common HTTP Features > Static Content. ☒  Common HTTP Features ☒  Default Document ☐  Directory Browsing ☐  HTTP Errors ☐  HTTP Redirection ☒  Static Content
Windows Vista/Windows 7	Make sure that all the following check boxes are selected in the Windows Features window and then click OK: • Internet Information Services > Web Management Tools > IIS Management Console; ☒  Internet Information Services ☒  FTP Server ☒  Web Management Tools ☒  IIS 6 Management Compatibility ☒  IIS Management Console

	• Internet Information Services > World Wide Web Services > Application Development Features > ASP.NET;  • Internet Information Services > World Wide Web Services > Common HTTP Features > Static Content. 
Windows Server 2008	1. In the Add Roles Wizard window, on the Role Services page, make sure that the following check boxes are selected: • Common HTTP Features > Static Content; • Application Development > ASP.NET.  2. Click Next and then click Add Required Role Services. 3. On the Role Services page, make sure that the following check boxes are selected: • Management Tools > IIS Management Console.  4. Click Next and then click Install. 5. After the end of installation, click Close.
Windows Server 2012	1. In the Add Roles and Features Wizard window, on the Server Roles page, make sure that the Web Server (IIS) check box is selected and then click Next.

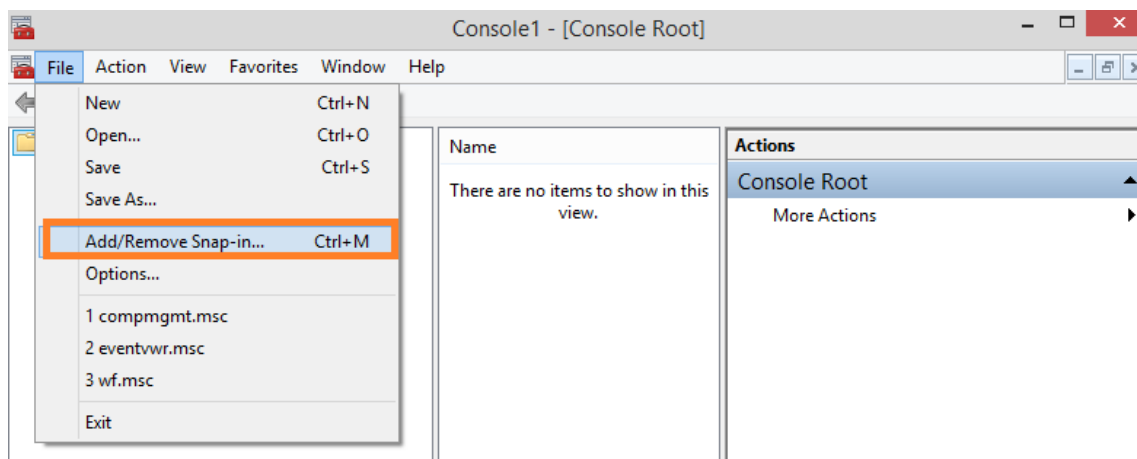
	☒ Web Server (IIS) 2. On the Features page, make sure that the following check boxes are selected: • .NET Framework 3.5 Features (Installed) > .NET Framework 3.5; • .NET Framework 4.5 (Installed) > ASP.NET 4.5. ☒ .NET Framework 3.5 Features (Installed) ☒ .NET Framework 3.5 (includes .NET 2.0 and 3.0) ☐ HTTP Activation ☐ Non-HTTP Activation ☒ .NET Framework 4.5 Features (Installed) ☒ .NET Framework 4.5 (Installed) ☒ ASP.NET 4.5 3. Click Next. 3. On the Web Server Role IIS page, click Next. 4. On the Role Services page, select the ASP.NET 4.5 check box (under Application Development). ☐ Application Development ☐ .NET Extensibility 3.5 ☐ .NET Extensibility 4.5 ☐ Application Initialization ☐ ASP ☐ ASP.NET 3.5 ☒ ASP.NET 4.5 5. Click Next and then click Add Features. 6. On the Role Services page, make sure that the following check boxes are selected: • Application Development > .NET Extensibility 4.5 > ASP > NET 4.5 > ISAPI Extensions > ISAPI Filters. ☒ Application Development ☐ .NET Extensibility 3.5 ☒ .NET Extensibility 4.5 ☐ Application Initialization ☐ ASP ☐ ASP.NET 3.5 ☒ ASP.NET 4.5 ☐ CGI ☒ ISAPI Extensions ☒ ISAPI Filters 7. Click Next and then click Install. 8. After the end of installation, click Close.
--	--

Appendix 3. Adding Certificate to Trusted Root Certification Authorities

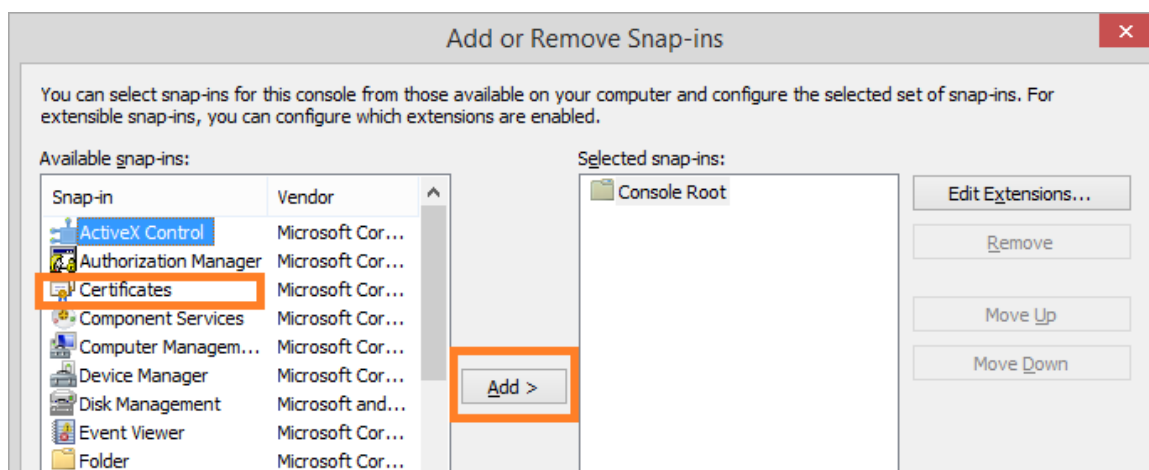
Before adding the self-signed certificate to the Trusted Root Certification Authorities, it should be exported. For purchased certificates that were issued for your computer this procedure is not needed.

To add the certificate to the Trusted Root Certification Authorities, do the following:

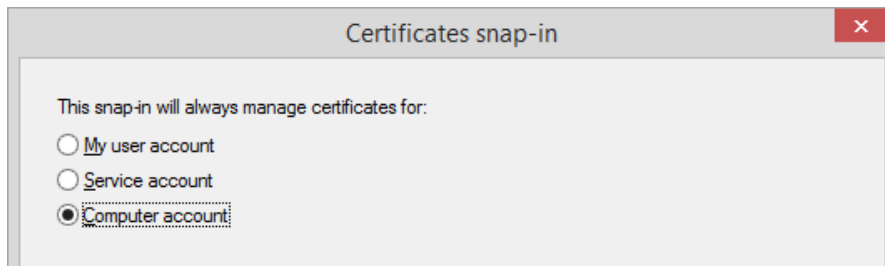
1. Press **Windows+R**, type **mmc** in the **Run** text box and press **Enter**.
2. In the opened **User Account Control** window, click **Yes**.
3. In the **Console** window, select **File > Add/Remove Snap-in**.



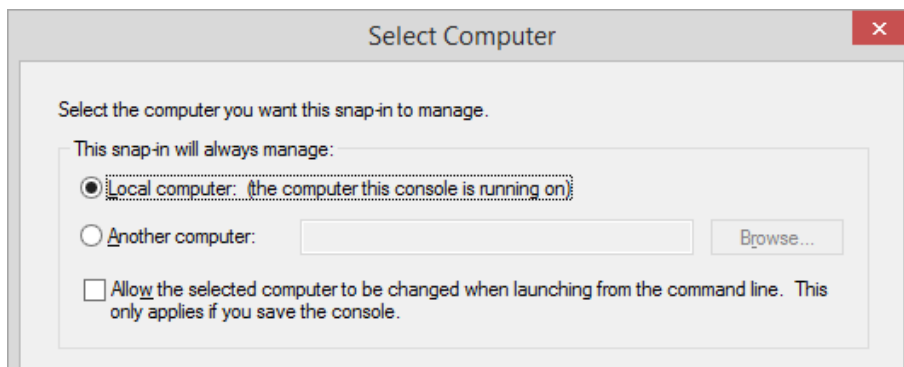
4. In the opened **Add or Remove Snap-ins** window, select **Certificates > Add**.



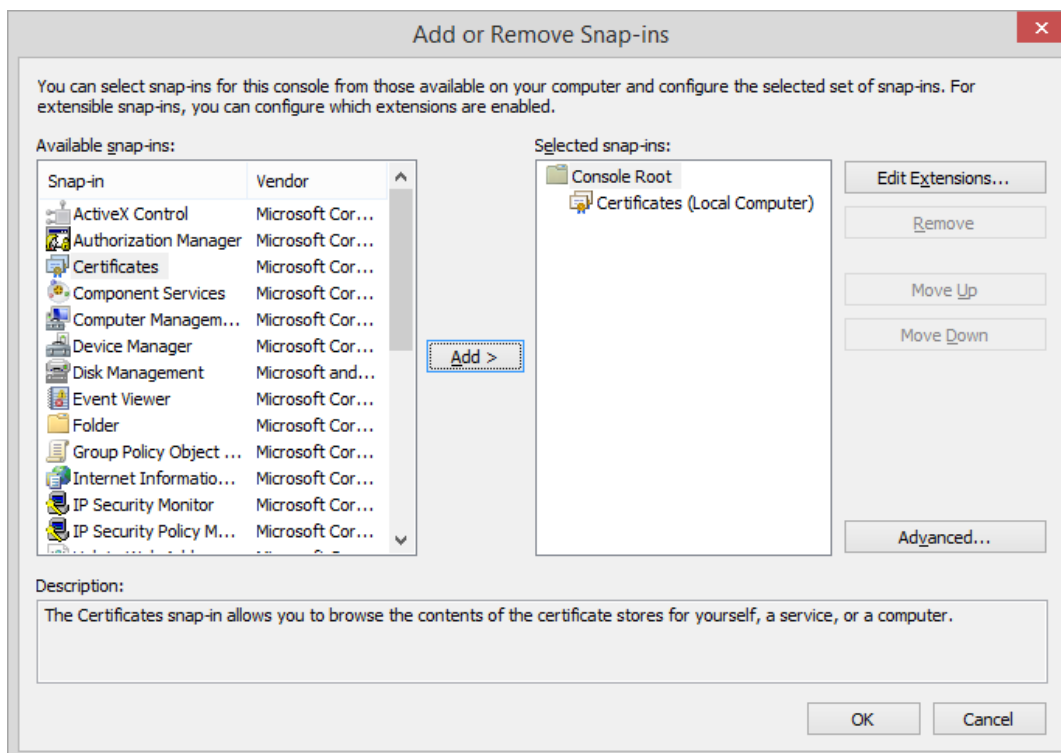
5. In the opened **Certificates snap-in** window, select **Computer account** and click **Next**.



6. In the opened **Select Computer** window, select **Local computer: (the computer this console is running on)** and click **Finish**.

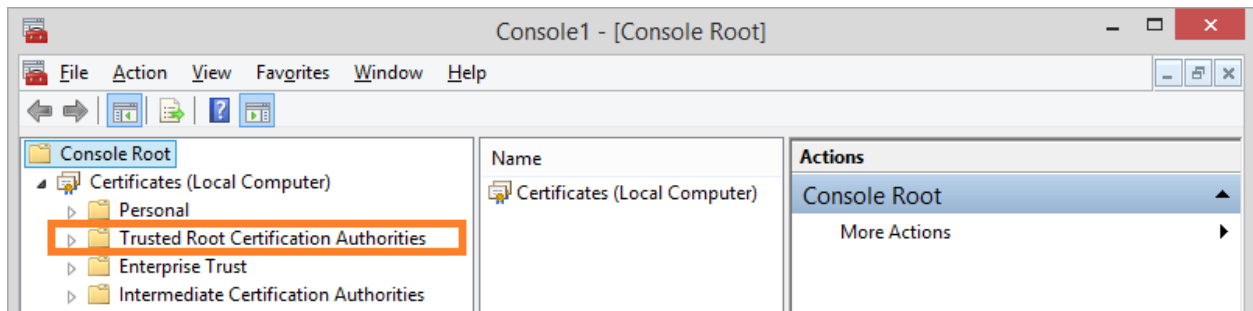


7. In the **Add or Remove Snap-ins** window, click **OK**.

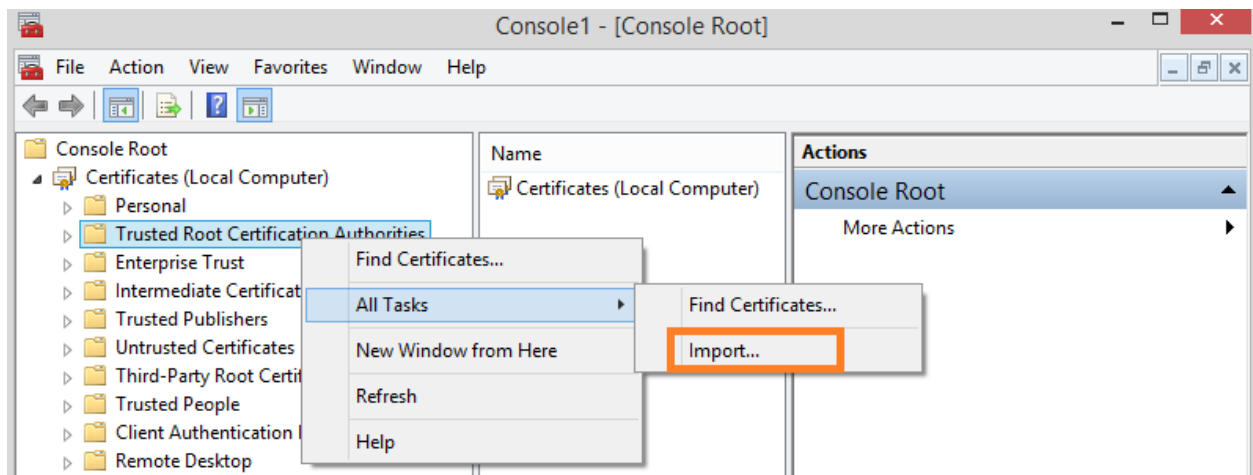


8. In the **Console** window, expand the **Certificates (Local computer)** node.

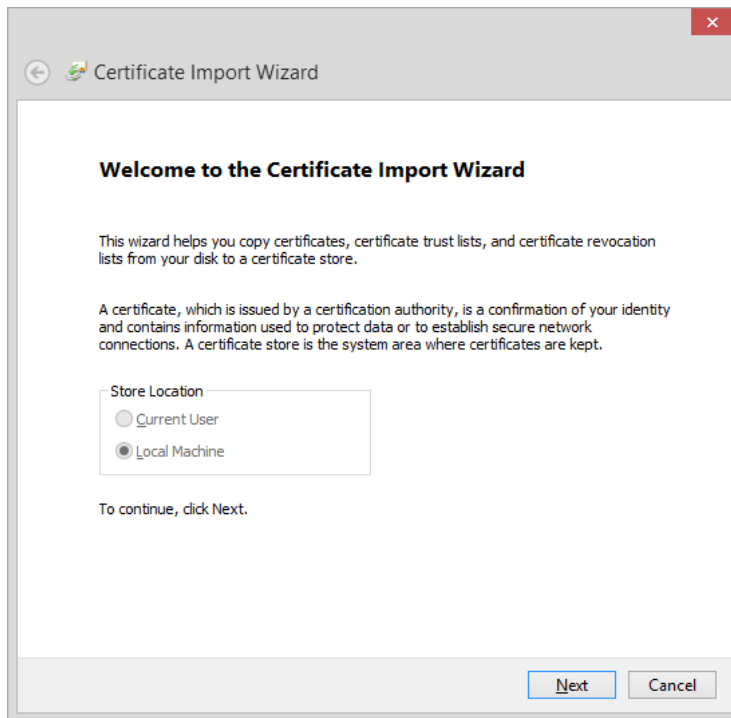
9. In the **Certificates (Local computer)** tree-view, find the **Trusted Root Certification Authorities** node.



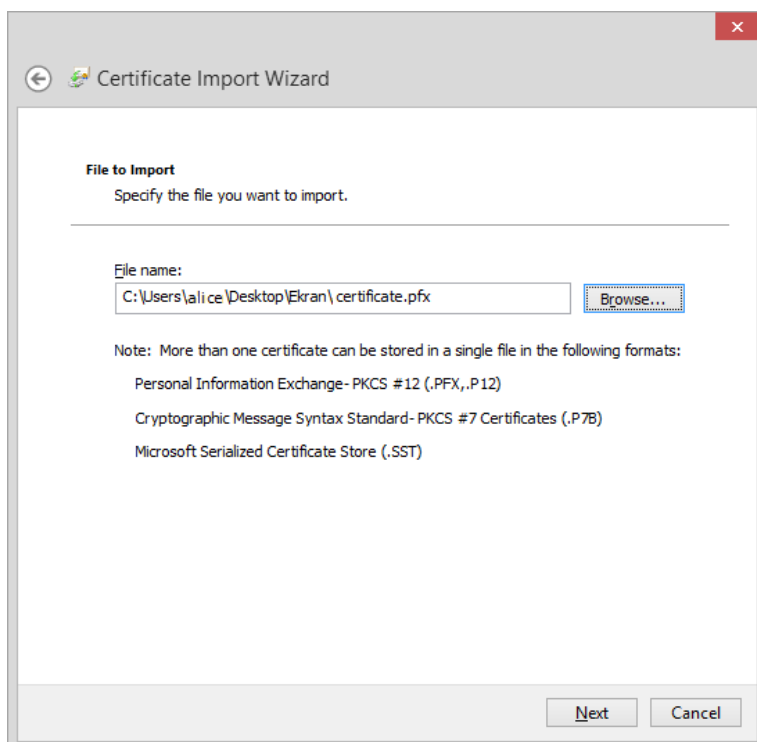
10. In the right-click menu of the **Trusted Root Certification Authorities** node, select **All Tasks > Import**.



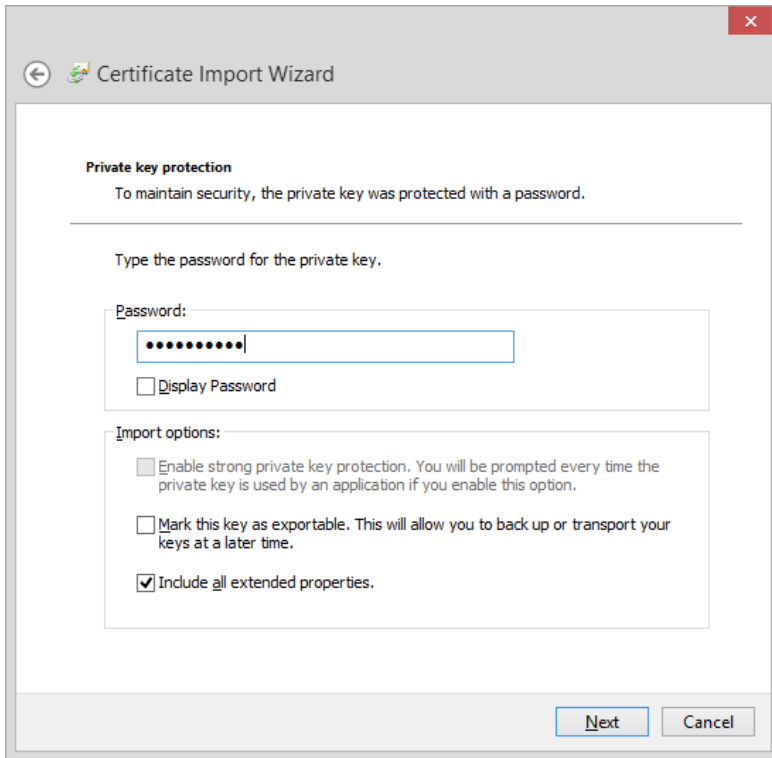
11. The **Certificate Import Wizard** opens.
12. On the Certificate Import Wizard **Welcome** page, click **Next**.



13. On the **File to Import** page, click **Browse** to find the certificate to be imported and then click **Next**.

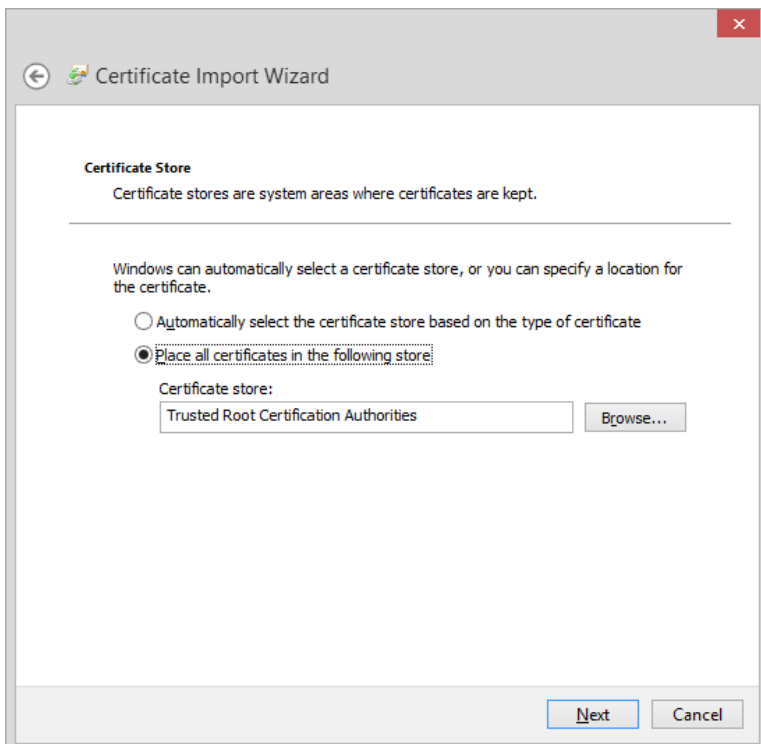


14. On the **Private key protection** page, enter the certificate password and then click **Next**.



The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Private key protection' step. The window has a title bar with a back arrow, a forward arrow, and a close button. The main content area is titled 'Private key protection' and contains the text: 'To maintain security, the private key was protected with a password.' Below this, it says 'Type the password for the private key.' There is a text box for the password, currently filled with dots, and a checkbox labeled 'Display Password'. Below the password field, there is a section titled 'Import options:' with three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), and 'Include all extended properties.' (checked). At the bottom right, there are 'Next' and 'Cancel' buttons.

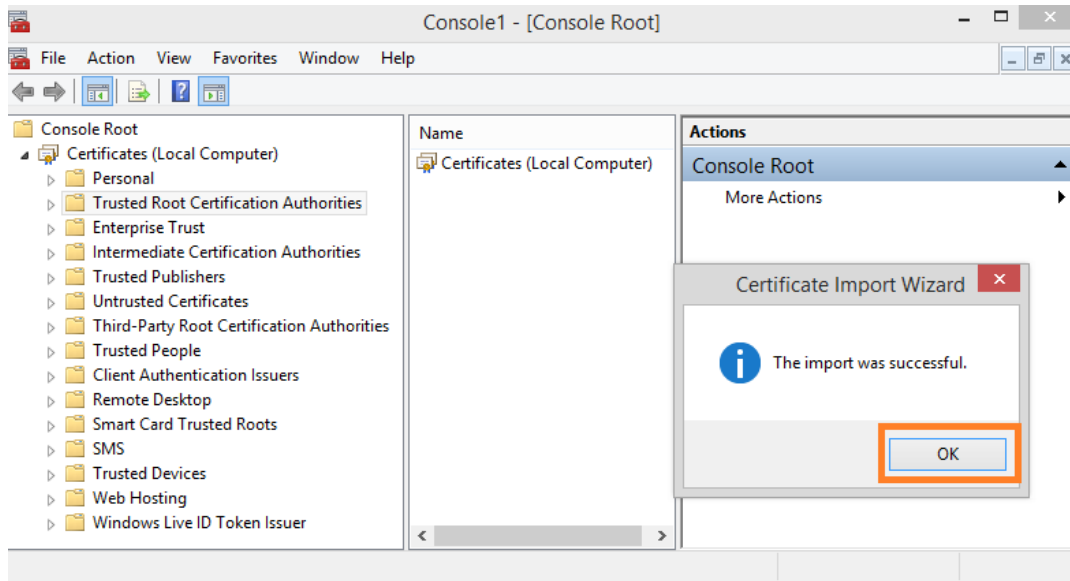
15. On the **Certificate Store** page, click **Next**.



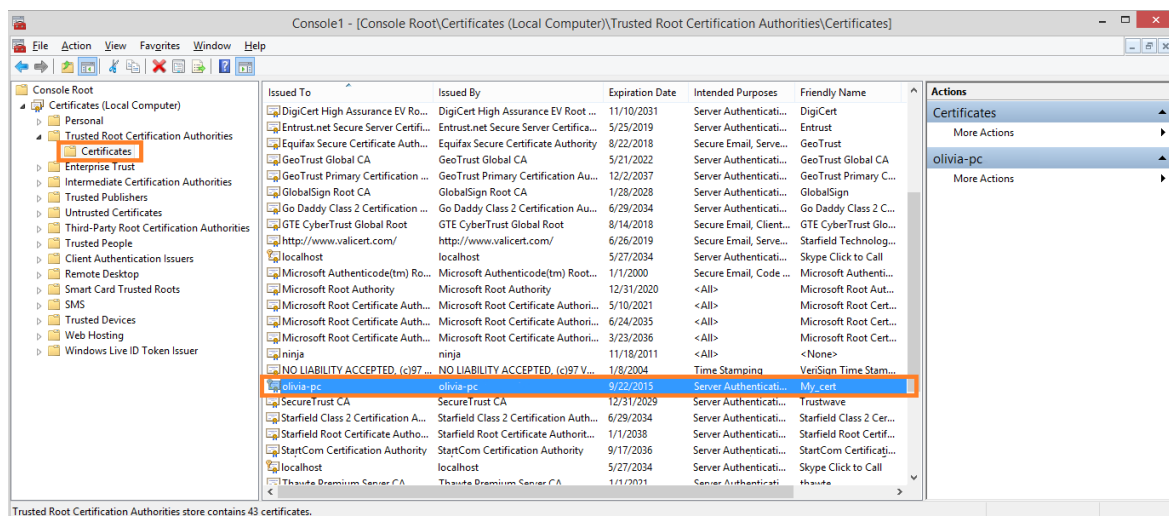
The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Certificate Store' step. The window has a title bar with a back arrow, a forward arrow, and a close button. The main content area is titled 'Certificate Store' and contains the text: 'Certificate stores are system areas where certificates are kept.' Below this, it says 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio buttons: 'Automatically select the certificate store based on the type of certificate' (unchecked) and 'Place all certificates in the following store:' (checked). Below the second radio button, there is a text box labeled 'Certificate store:' containing the text 'Trusted Root Certification Authorities', and a 'Browse...' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

16. On the last page of the **Certificate Import Wizard**, click **Finish**.

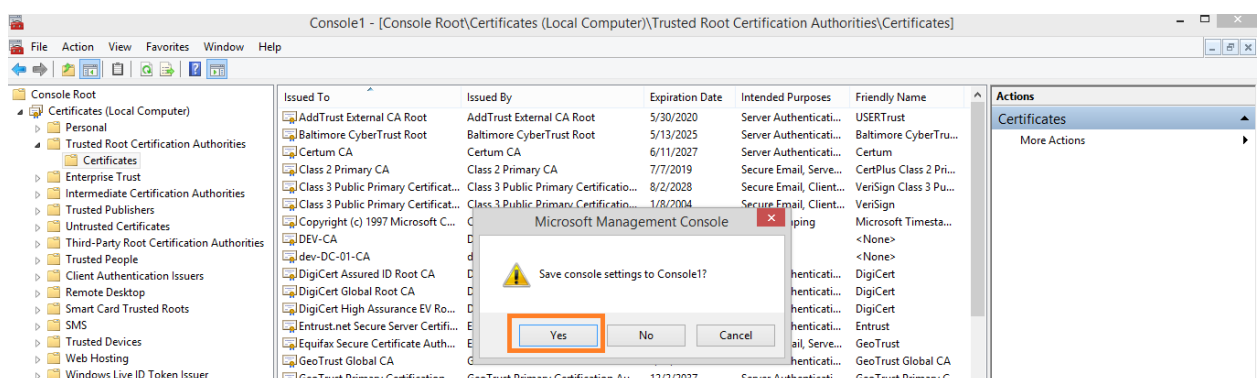
17. In the confirmation message, click **OK**.



18. The certificate is imported and is displayed in the **Console** window in the **Certificates** node. Please note that the **Issued To** field contains the name of the computer, on which the Management Tool will be installed in the format that will be used when opening the Management Tool.



19. Close the **Console** window.



Appendix 4. Setting HTTPS Binding for a Default Web-Site

To set HTTPS binding for a default web-site, do the following:

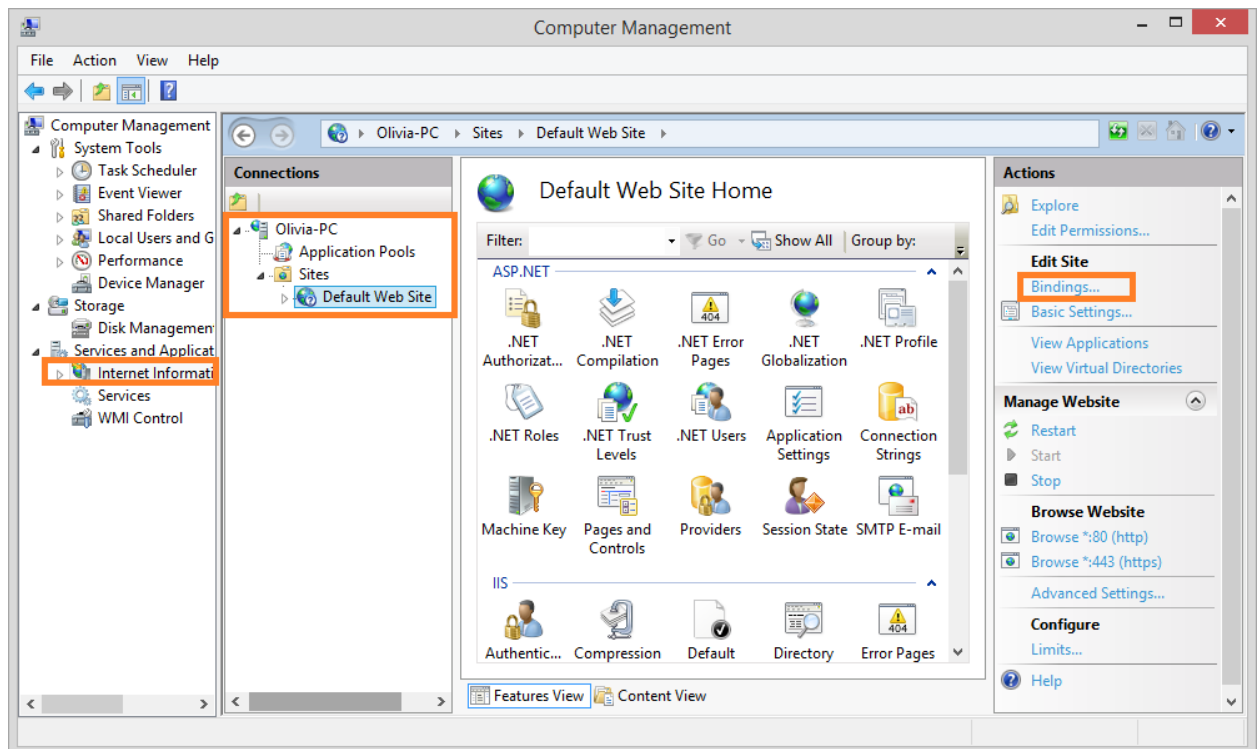
1. Open the **Internet Information Service Manager**:

- For **Windows 7** or **Windows 8**: Open Computer > Manage > Services and Applications > Internet Information Services (IIS) Manager.
- For **Windows Server 2008** or **2012**: Press **Windows+R**, enter **inetmgr** in the **Run** window and then press **Enter**.

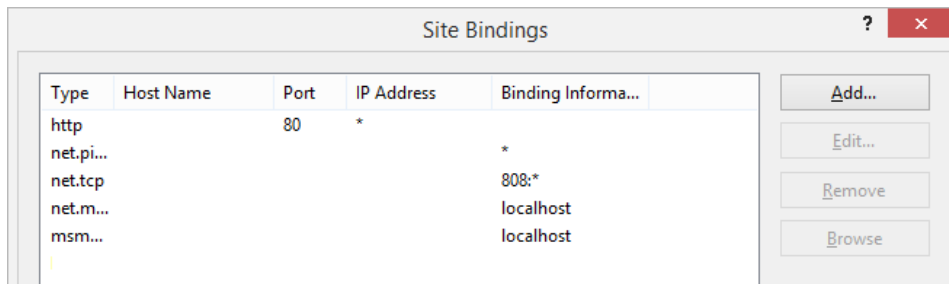
NOTE: Using the inetmgr command is a common way of opening the Internet Information Service Manager for any version of the Windows operating system.

2. Expand the node with the name of the target computer in the central pane.
3. Expand the **Sites** node.
4. Select the **Default Web Site**.

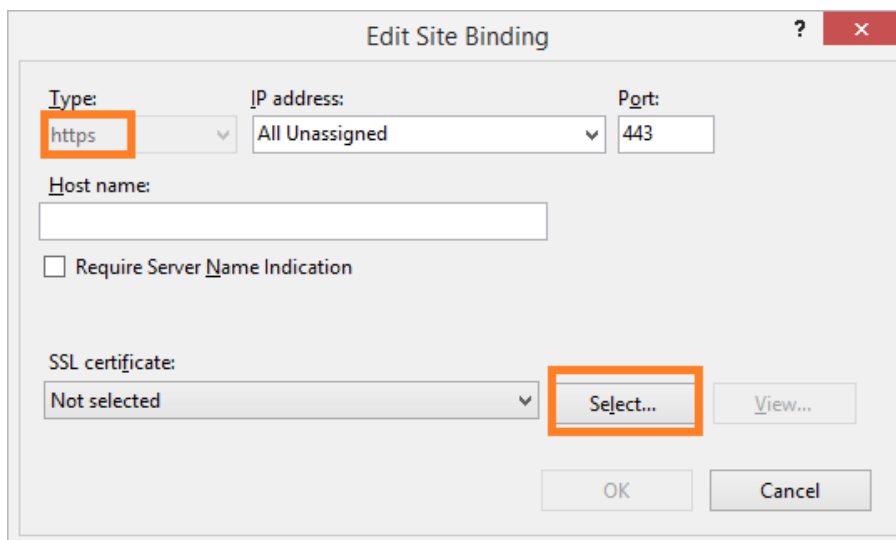
NOTE: If there is no such site in the Internet Information Services (IIS) Manager of your computer, you can select any other site (the name of the site does not matter).



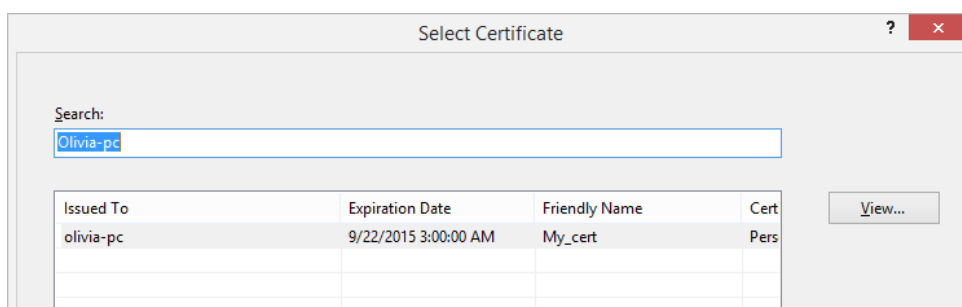
5. Click the **Bindings** navigation link on the right.
6. The **Site Bindings** window opens.



7. If there is no binding of HTTPS type in the **Site Bindings** window, click **Add**.
2. The **Edit Site Binding** window opens.
3. In the **Type** box, select **https**.



4. Next to the SSL certificate drop-down list, click **Select**.
5. The **Select Certificate** window opens, where the list of existing certificates is displayed.
6. In the **Select Certificate** window, select the certificate generated for the Management Tool and then click **OK**.



7. In the **Add Site Binding** window, click **OK**.
8. In the **Site Bindings** window, click **Close**.
9. Now the **Internet Information Service** is fully adjusted and you can start installing the Management Tool.

