TECHNICAL SPECIFICATIONS MAESTRO*MOBILE

OBJECTIVE

This document consolidates the various components or recommended configurations to run the **maestro*MOBILE** application in an optimal manner. It must be provided to your technician in order for him to be properly informed and validate the required configurations.

If you have questions, you can reach our technicians by contacting the Software Support Department by one of the following options:

- by phone, at 514-990-1897 or toll-free at 1-877-833-1897;
- by email at support@maestro.ca.

SUMMARY

To quickly access a topic, click on one of the following hyperlinks:

Installation Prerequisites

General Prerequisite

It is important that the version of **maestro*** is the same as the version of the installed mobile application. The two products must also be updated at the same time.

Server Environment

- **Maestro*** version 3.04.32 or higher;
- IIS 7.5 or higher (present on Windows 2008R2 (or higher) or Windows 7 (or higher) allowing access by Internet (http and/or https); this server must be able to communicate with the **maestro*** server;
- Microsoft .NET 4.8;
- Static IP address / External DNS address for the IIS server.

Client Environment

The mobile application is tested and functions optimally on the following devices:

- iOS – The current version or the version just before;
- Android – Version 4.3 and higher.

The application works and is tested on devices, regardless of operating system, with a minimum screen size of 4" (diagonal). If the device shows minor display problems, in this case, contact **Maestro** to request that we correct these situations.

Display Settings

iOS

Maestro*MOBILE can be obtained from a Web browser by typing the URL address from which your mobile instance is called in the search field. However, the application is displayed as a Web site and the status and navigation bars are limiting the **maestro*MOBILE** content. In order to mask those bars and access the application from an icon on the homepage, perform the following steps:

1. Access to **maestro*MOBILE** from the Web browser of your device.
2. Tap on the icon ⇪ in order to display a menu and some additional icons.
3. Tap on the icon +.

Maestro*MOBILE is now accessible from the homepage of the device and is shown as a new icon * .

> **iOS update**
>
> When an iOS update is performed (for example, the iOS 9 to iOS 10 migration), error messages can be displayed in the application or during its launch. It is required to delete the **maestro*MOBILE** icon on the device's homepage. The user must access the application from a Web browser and add again the icon on the homepage, as described previously.

Recommendations for Technicians

Hosting

The **maestro*MOBILE** service must imperatively be hosted on <u>your own servers</u>. **Maestro*MOBILE** can be installed directly on your **maestro*** DATA server or on another server in the same network.

Address

Generally, the mobile application will be accessible from two IP addresses.

- First, the internal IP address that the internal network server uses (Intranet).
- Secondly, the external IP address accessible from the Internet that exposes the external router or the firewall machine and that redirects calls to the mobile server.

Example:

Internal Address = 192.168.1.101

External Address = 24.224.1.196

Router / Firewall

Your router/firewall must be configured to allow external access to **maestro*MOBILE**:

- This configuration allows external mobile requests to reach the server where **maestro*MOBILE** is installed;
- This configuration should be prepared by your IT service.

If this configuration is not achieved, **maestro*MOBILE** won't be accessible outside of your office.

Vew sections **Ports** and **DMZ**.

DNS

Instead of accessing the application with the IP address of the internal machine or with the external IP address, it is recommended to create a DNS alias for the application to be easily accessible, regardless of the location of the calls.

Example:

Internal DNS (Infra intranet) = maestro.client.com that points to 192.168.1.101

External DNS (Domaine management) = maestro.client.com that points to 24.224.1.196

Ports

Web applications such as the **maestro*MOBILE** application use the ports 80 and 443 by default. However, it is possible to use other ports if the infrastructure or the needs are particular.

It is possible to change these settings during the installation of the application or directly in the server's IIS console.

The communication ports between the **maestro*** and mobile servers must also be opened, as stated in the **DMZ section**.

Web Site

Scenario 1: Create a new Web site

During the installation, it will be possible to directly create a new Web site. It must specify a port available on the machine. By creating a new site, the application will be directly accessible at the root.

Example 1: Create a new Web site on port 80

The application will be accessible from the address: http://maestro.client.com

Example 2: Create a new Web site on port 90

The application will be accessible from the address: http://maestro.client.com:90

Scenario 2: Install on an existing site

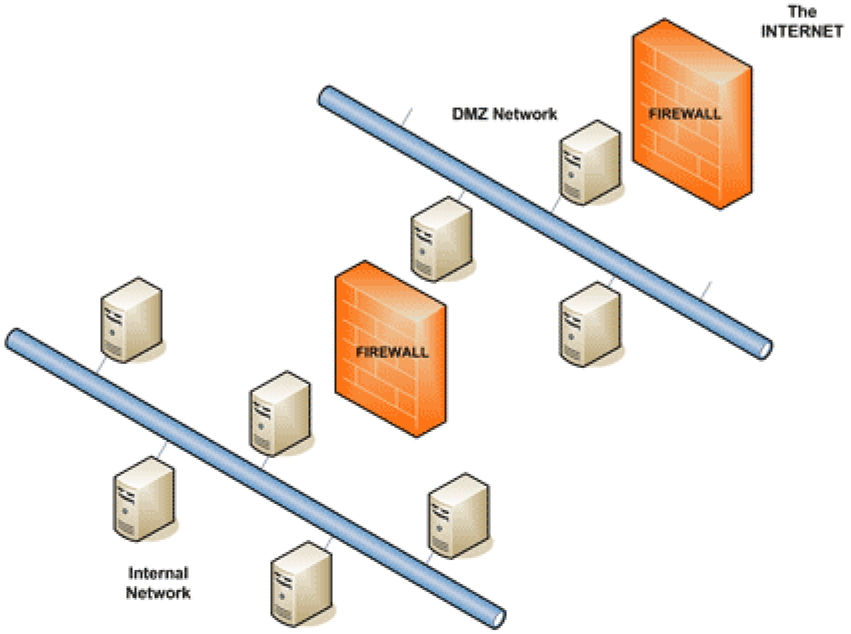
It is possible to install the application on an already existing site. To do so, you must select the desired site during the installation.

Example: Use an existing site that is on port 80

The application will be accessible from the address: http://maestro.client.com/maestro

DMZ

Although it is possible to install the mobile server on the **maestro*** server, it is recommended that the mobile server should be placed in a DMZ. The Web server displaying the mobile application on the Internet communicates on the internal network by secure ports and gives access to **maestro***'s data (port 15001 for mobile services, port 1583 for **maestro*** in Pervasive mode, or port 1433 for **maestro*** in MS SQL mode). This ensures that the **maestro*** server is not directly exposed on Internet and reduces the potential attacks on the internal infrastructure.



SSL

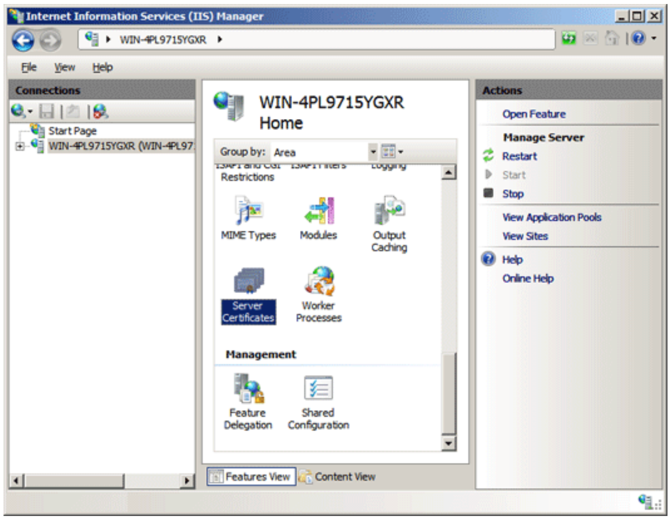
If the option for the creation of Web sites has been selected during installation, the process configures a Web site in IIS which is configured as just HTTP. It is a good practice to expose the public web sites in HTTPS so that exchanges between the server and the mobile devices are secure. You must install a certificate in IIS to activate the binding HTTPS on the site. Here are the details for the configuration.

> **Secure Mode Activation**
>
> The use of HTTPS secure mode is strongly recommended.

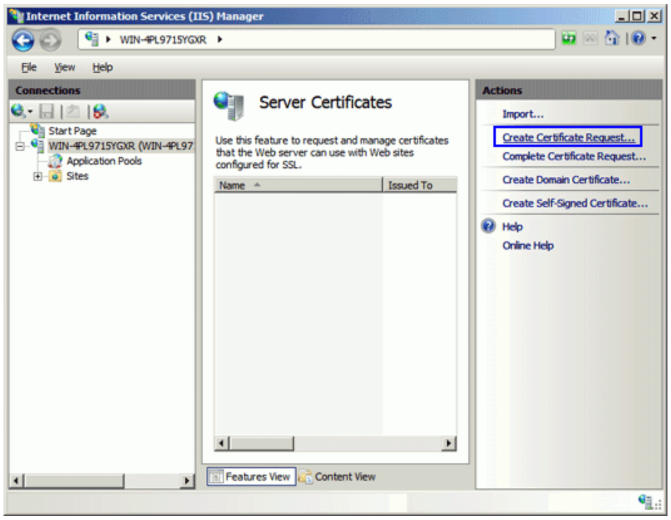
HTTPS

Install a certification in IIS 7.5

1. Click on **Start**, then **Administrative Tools**, and then on Internet Information **Services (IIS) Manager**.
2. Click on the server name.
3. From the center menu, double-click on the Server **Certificates** button in the **Security** section (it is near the bottom of the menu).



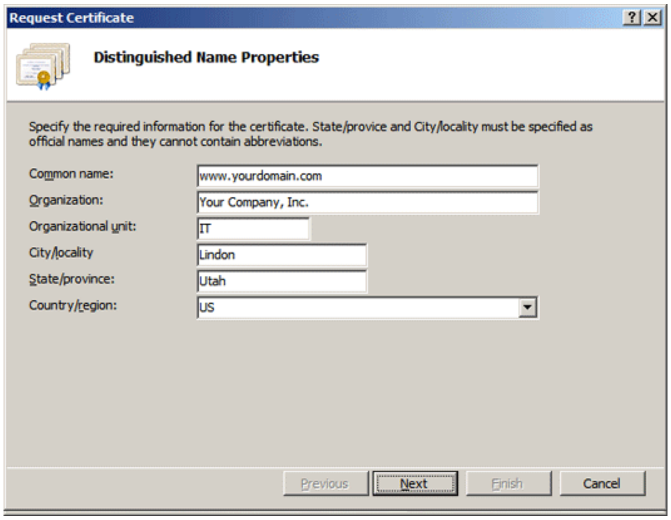
4. Next, from the **Actions** menu (on the right), click on **Create Certificate Request**. This will open the **Request Certificate** wizard.


Internet Information Services (IIS) Manager
WIN-4PL9715YGXR
File
View
Help
Connections
Start Page
WIN-4PL9715YGXR (WIN-4PL97
Application Pools
Sites
Server Certificates
Name
Issued To
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

5. In the **Distinguished Name Properties** window, enter the information as follows:

Field	**Description**
Common Name	The name through which the certificate will be accessed (usually the fully-qualified domain name, ex: www.domain.com or mail.domain.com).
Organization	The legally registered name of your organization/company.
Organizational Unit	The name of your department within the organization (frequently this entry will be listed as "IT," "Web Security," or is simply left blank).
City/Locality	The city in which your organization is located.
State/Province	The state / province in which your organization is located.
Country/Region	Canada or United States.

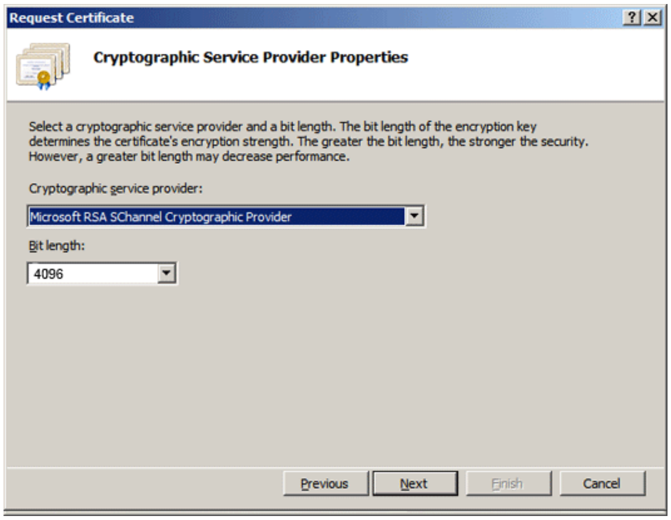


Distinguished Name Properties

Specify the required information for the certificate. State/provice and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: www.yourdomain.com
Organization: Your Company, Inc.
Organizational unit: IT
City/locality Lindon
State/province: Utah
Country/region: US

6. Click on **Next**.
7. In the **Cryptographic Service Provider Properties** window, leave both settings at their defaults (Microsoft RSA SChannel and 4096) and then click **Next**.



Cryptographic Service Provider Properties

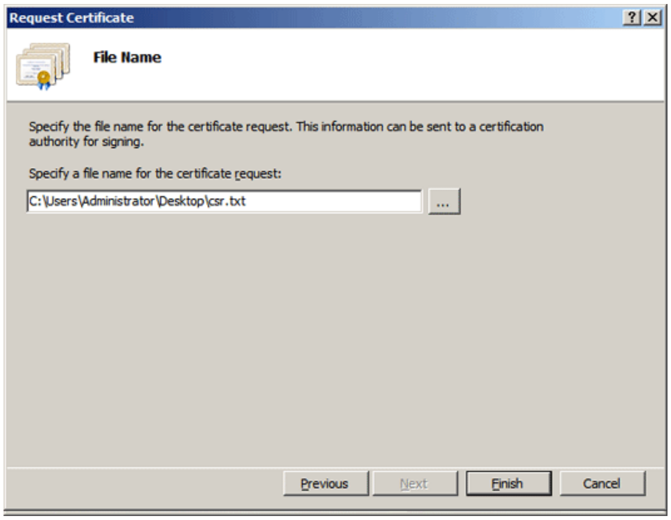
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 4096

8. Enter a filename for your CSR file.

> It is important to make note of the filename that you choose and the location to which you save it. You will need to open this file as a text file and copy the entire body of it (including the Begin and End Certificate Request tags) into the online order process when prompted.



Request Certificate

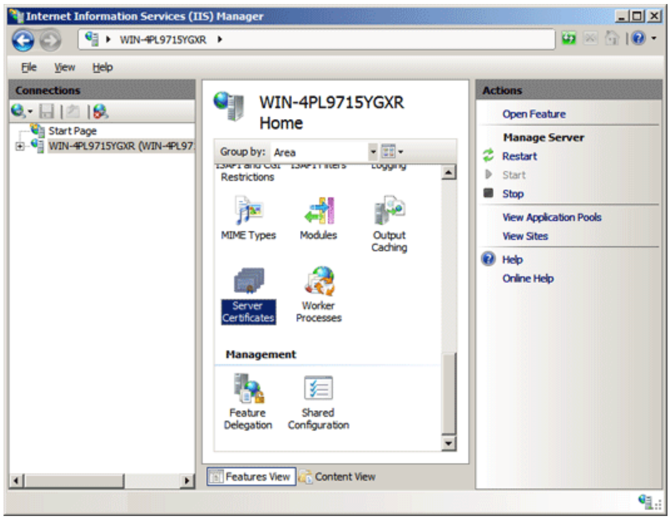
File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

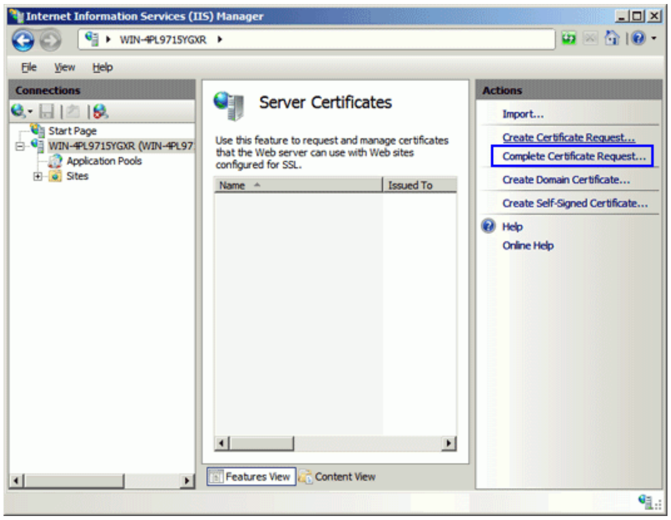
Specify a file name for the certificate request:

C:\Users\Administrator\Desktop\csr.txt

9. Open this file in a text editor, like *Notepad* or *WordPad*, copy the entire contents of this file and copy it to your computer's clipboard.
10. Choose an online SSL certificate provider such as *GoDaddy*, *Thawte*, *Verisign* or other. Create a certificate request with the information in your clipboard. Please follow the procedure given by the provider of your choice. The whole process can take a few minutes to a few days depending of the chosen provider and the type of certificate selected.
11. Once the certificate issuing process is finished and you receive the certificate confirmation, go back to the Internet Information Services (IIS) Manager in the Administrative Tools.
12. Click on the server name.
13. From the center menu, double-click the **Server Certificates** button in the **Security** section (it is near the bottom of the menu).



14. From the **Actions** menu (on the right), click on **Complete Certificate Request**. This will open the **Complete Certificate Request** wizard.

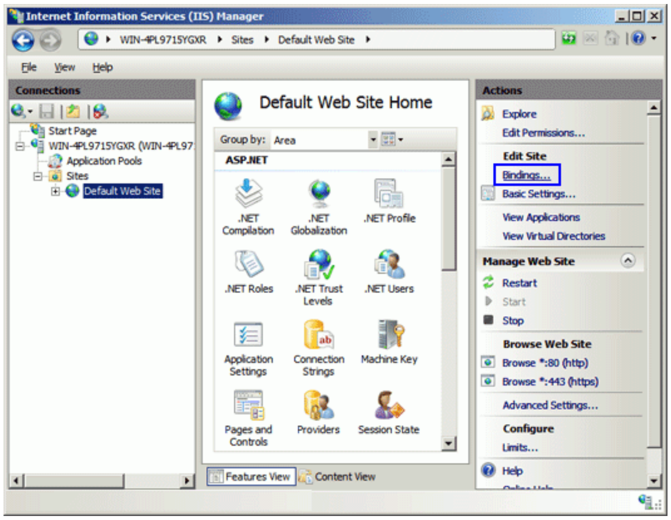

Internet Information Services (IIS) Manager
WIN-4PL9715YGXR
File
View
Help
Connections
Start Page
WIN-4PL9715YGXR (WIN-4PL97
Application Pools
Sites
Server Certificates
Name
Issued To
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

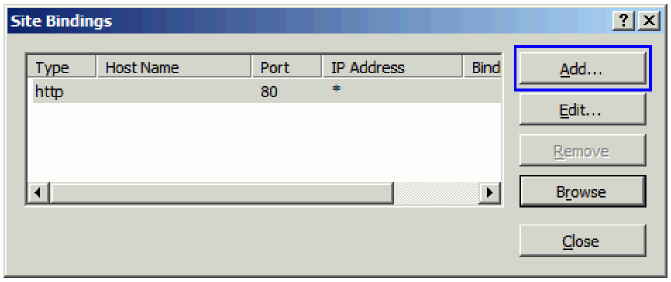
15. Browse to the certificate file that you received from your provider. You will then be required to enter a friendly name. The friendly name is not part of the certificate itself, but is used by the
16. Clicking **OK**, will install the certificate on the server.

> There is a known issue in IIS 7 giving the following error: "Cannot find the certificate request associated with this certificate file. A certificate request must be completed on the computer where it was created." You may also receive a message stating "ASN1 bad tag value met". If this is the same server that you generated the CSR on then, in most cases, the certificate is actually installed. Simply cancel the dialog and press **F5** to refresh the list of server certificates. If the new certificate is now in the list, you can continue with the next step. If it is not in the list, you will need to reissue your certificate using a new CSR.

17. Once the SSL certificate has been successfully installed to the server, you will need to assign that certificate to the appropriate website using IIS
18. From the **Connections** menu in the main Internet **Information Services (IIS) Manager** window, select the name of the server to which the certificate was installed.
19. In the **Sites** section, select the site to be secured with SSL.
20. From the **Actions** menu (on the right), click on **Bindings**. This will open the **Site Bindings** window.

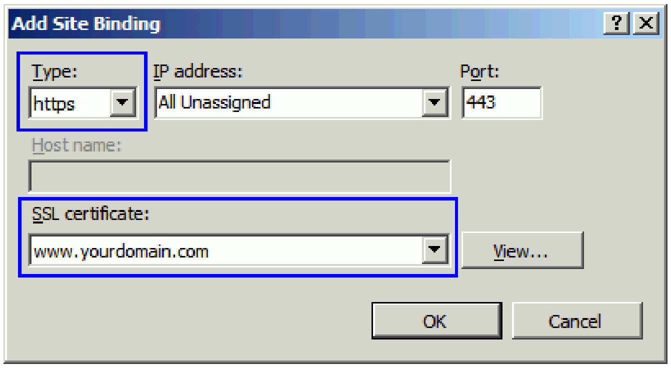


21. In the **Site Bindings** window, click **Add...** This will open the **Add Site Binding** window.



Type	Host Name	Port	IP Address	Bind
http		80	*	

22. Under **Type**, choose *https*. The IP address should be the **IP address** of the site or *All Unassigned*, and the **Port** over which traffic will be secured by SSL is usually *443*. The **SSL Certificate** field should specify the certificate that was installed in step 15.



Type: https

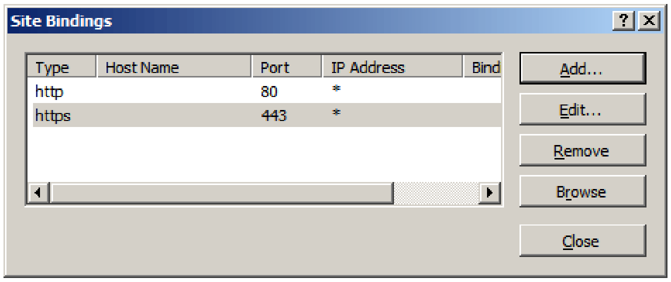
IP address: All Unassigned

Port: 443

Host name:

SSL certificate: www.yourdomain.com

23. Click on **OK**.



Type	Host Name	Port	IP Address	Bind
http		80	*	
https		443	*	

24. Your SSL certificate is now installed, and the website is configured to accept secure connections.

Procedure for the Initial Installation

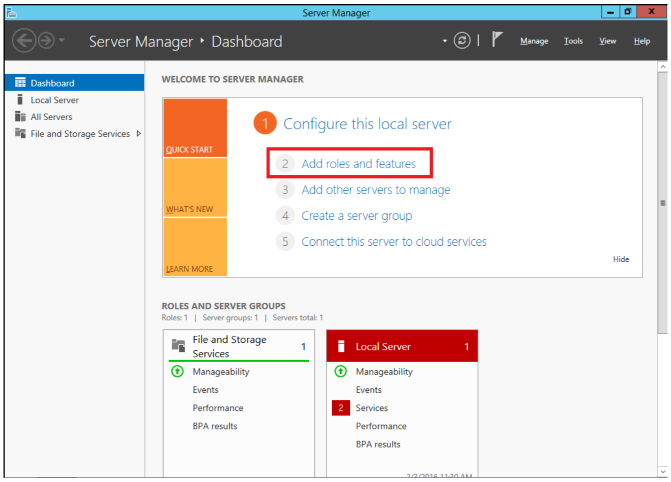
The package must be copied onto the Web server.

Required information to complete the installation:

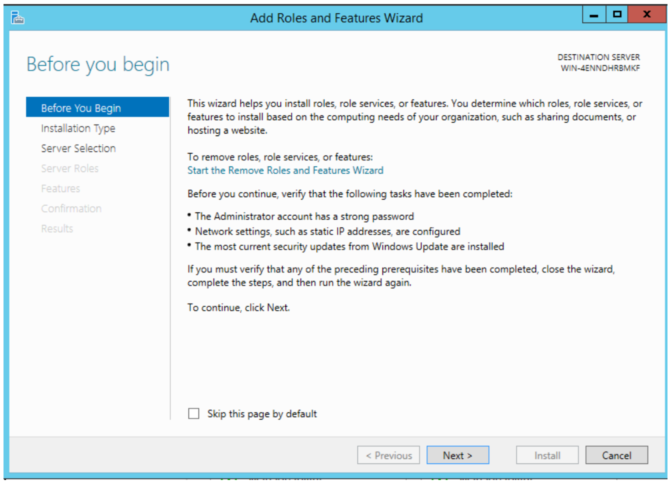
- Internal IP Address (DNS if used)
- External IP Address (DNS if used)
- Port
- **Maestro*** Pervasive server Address

A. Create a Web Server

1. In the **Server Manager**, click on **Add roles and features**.



2. At the **Before you begin** wizard window, click on the **Next** button.



Before you begin

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

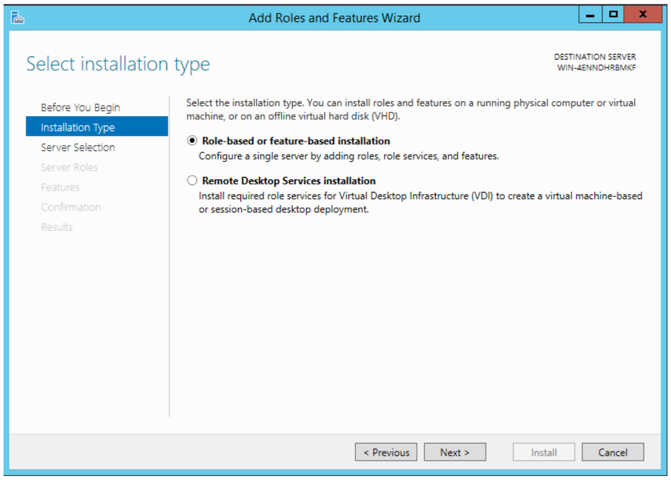
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

3. In the **Select installation type** section, chose the *Role-base or feature-based installation* option and then click on the **Next** button.



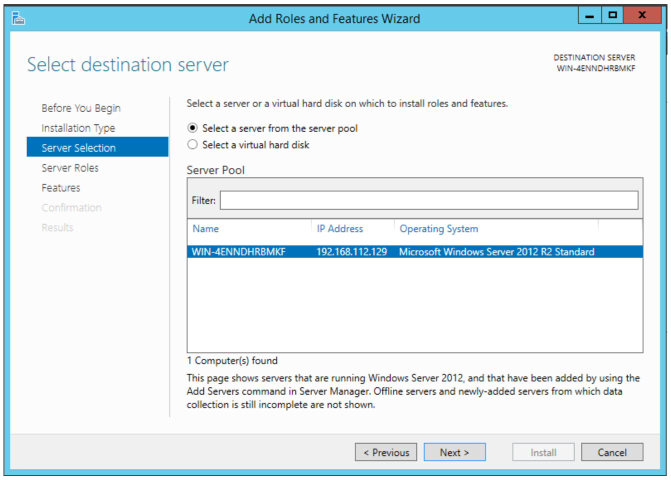
Select installation type

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

4. In the **Select destination server** section, chose the *Select a server from the server pool* option and then click on the **Next** button.



Select destination server

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

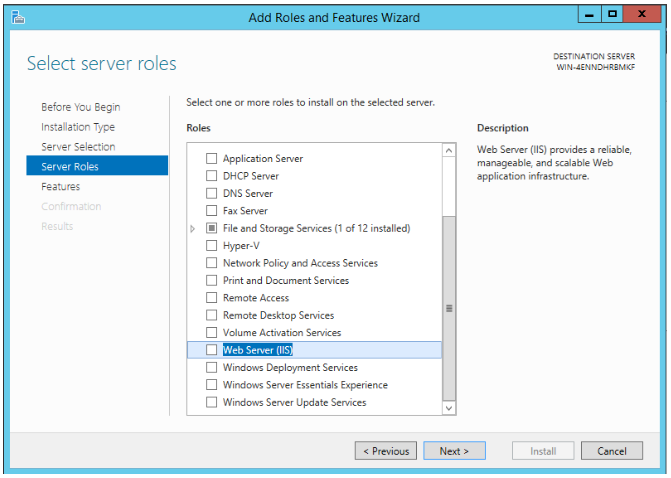
Filter:

Name	IP Address	Operating System
WIN-4ENNDHRBMKF	192.168.112.129	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

5. In the **Select server roles** section, select the *Web Server (IIS)* option.



Select server roles

Select one or more roles to install on the selected server.

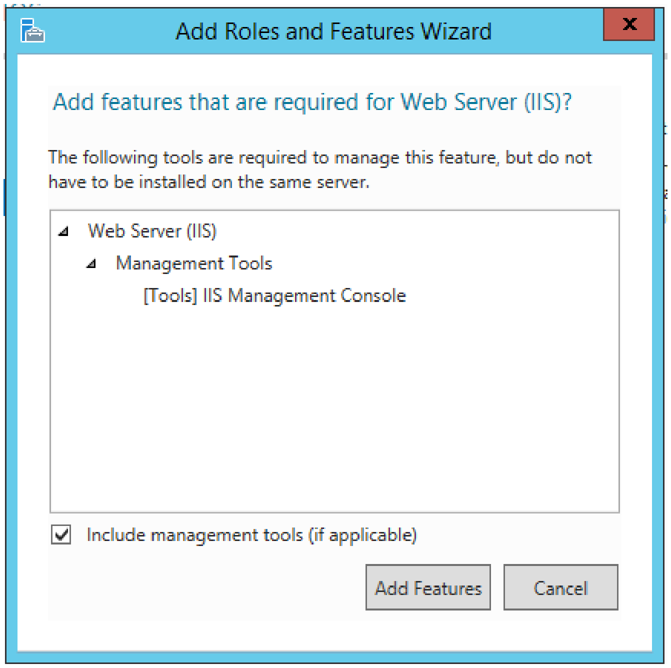
Roles

- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

6. In the **Add features that are required for Web Server (IIS)?** window that appears, click on **Add Features**.



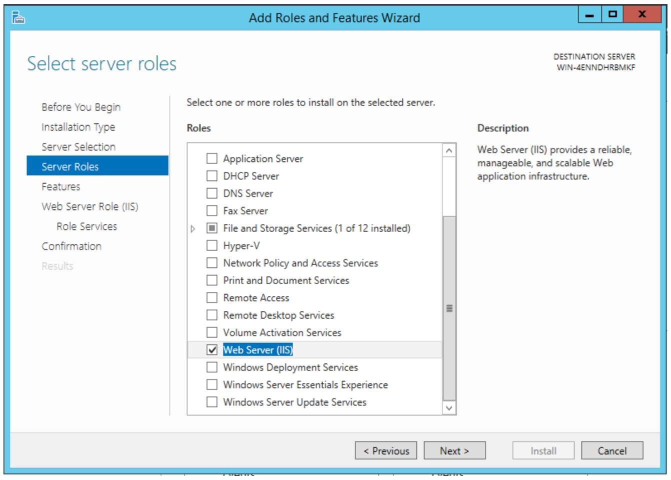
Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)

7. Back in the **Select server roles** section, click on **Next**.



Select server roles

DESTINATION SERVER
WIN-4ENNDHRBMKF

Select one or more roles to install on the selected server.

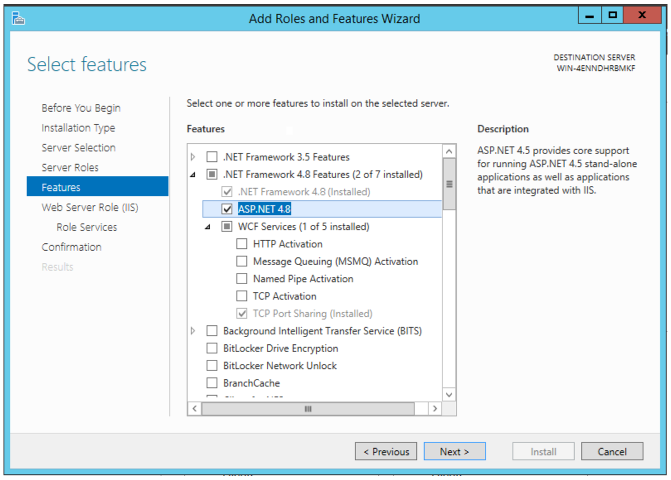
Roles

- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☑ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

8. In the **Select features** section, click on **.Net Framework 4.8 Features**, and then on **ASP.NET 4.8**. Click on **Next**.



Select features

DESTINATION SERVER
WIN-4ENNDHRBMKF

Select one or more features to install on the selected server.

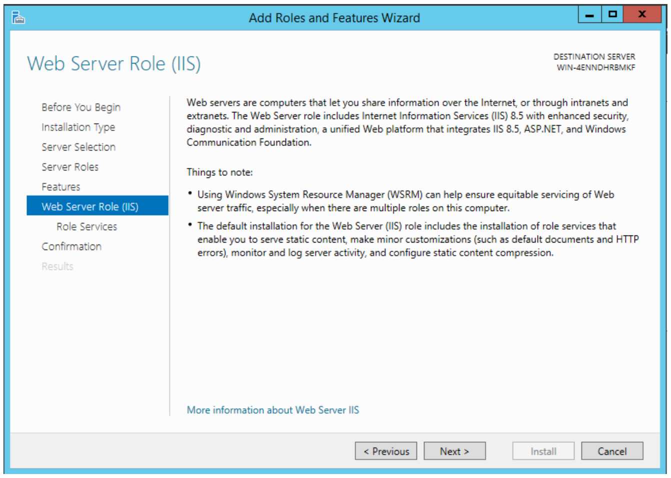
Features

- ☐ .NET Framework 3.5 Features
- ▣ .NET Framework 4.8 Features (2 of 7 installed)
  - ☑ .NET Framework 4.8 (Installed)
  - ☑ ASP.NET 4.8
  - ▣ WCF Services (1 of 5 installed)
    - ☐ HTTP Activation
    - ☐ Message Queuing (MSMQ) Activation
    - ☐ Named Pipe Activation
    - ☐ TCP Activation
    - ☑ TCP Port Sharing (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache

Description

ASP.NET 4.5 provides core support for running ASP.NET 4.5 stand-alone applications as well as applications that are integrated with IIS.

9. At the **Web Server Role (IIS)** function, click on **Next**.



Web Server Role (IIS)

DESTINATION SERVER
WIN-4ENNDHRBMKF

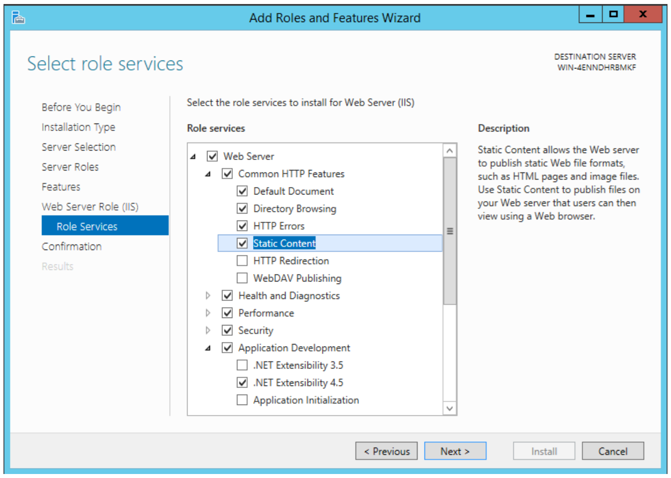
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 8.5 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 8.5, ASP.NET, and Windows Communication Foundation.

Things to note:

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

10. At the **Select role services** function, ensure that the options **Web Server**, **Common HTTP Features** and **Static Content** are checked.



Select the role services to install for Web Server (IIS)

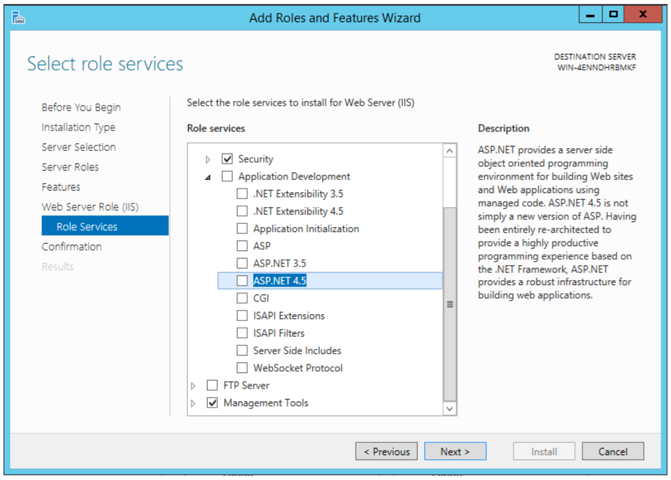
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☐ HTTP Redirection
    - ☐ WebDAV Publishing
  - ☑ Health and Diagnostics
  - ☑ Performance
  - ☑ Security
  - ☑ Application Development
    - ☐ .NET Extensibility 3.5
    - ☑ .NET Extensibility 4.5
    - ☐ Application Initialization

Description

Static Content allows the Web server to publish static Web file formats, such as HTML pages and image files. Use Static Content to publish files on your Web server that users can then view using a Web browser.

11. Still in the **Select role services** section, slide the scroll bar to the **Application Development** option, select it, and then check the **ASP.NET 4.5** option.



Select the role services to install for Web Server (IIS)

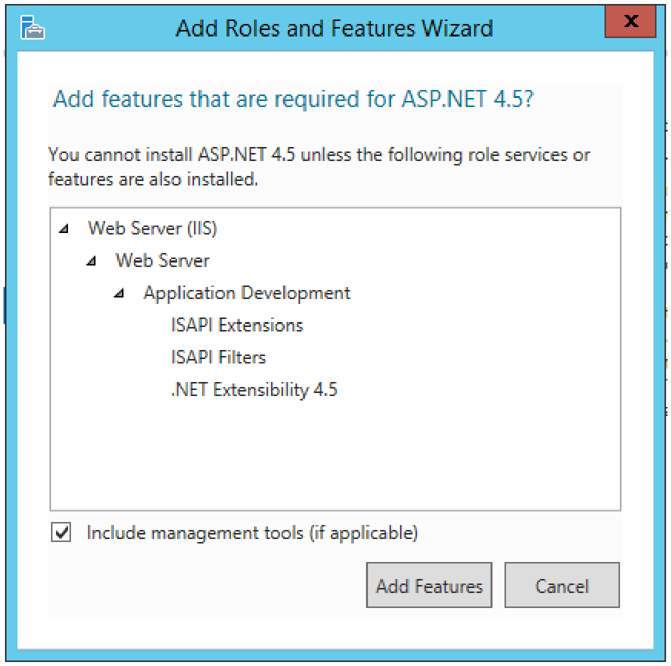
Role services

- ☑ Security
- ☐ 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
  - ☐ Server Side Includes
  - ☐ WebSocket Protocol
- ☐ FTP Server
- ☑ Management Tools

Description

ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET 4.5 is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

12. In the **Add features that are required for ASP.NET 4.5?** window that appears, click **Add Features**.



Add Roles and Features Wizard

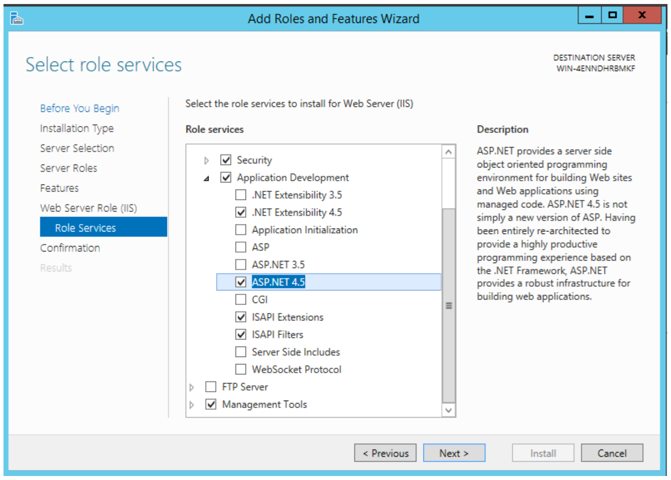
Add features that are required for ASP.NET 4.5?

You cannot install ASP.NET 4.5 unless the following role services or features are also installed.

- Web Server (IIS)
  - Web Server
    - Application Development
      - ISAPI Extensions
      - ISAPI Filters
      - .NET Extensibility 4.5

☑ Include management tools (if applicable)

13. Back in the **Select role services** section, click on **Next**.



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN-4ENNDHRBMKF

Select the role services to install for Web Server (IIS)

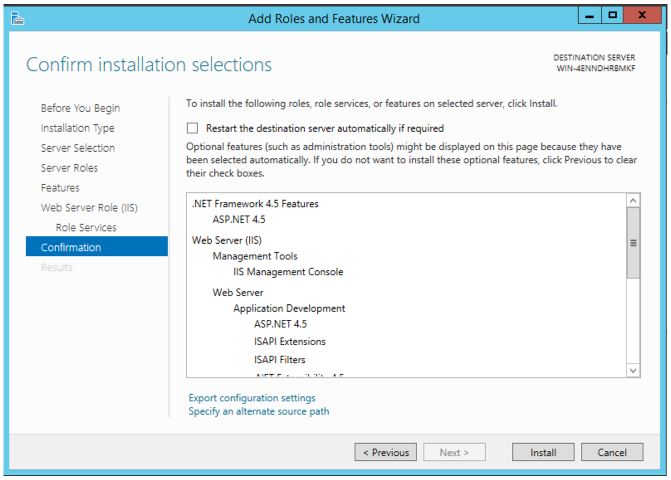
Role services

- ☑ Security
- ☑ 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
  - ☐ Server Side Includes
  - ☐ WebSocket Protocol
- ☐ FTP Server
- ☑ Management Tools

Description

ASP.NET provides a server side object oriented programming environment for building Web sites and Web applications using managed code. ASP.NET 4.5 is not simply a new version of ASP. Having been entirely re-architected to provide a highly productive programming experience based on the .NET Framework, ASP.NET provides a robust infrastructure for building web applications.

14. In the **Confirm installation selections** section, click on **Install**.



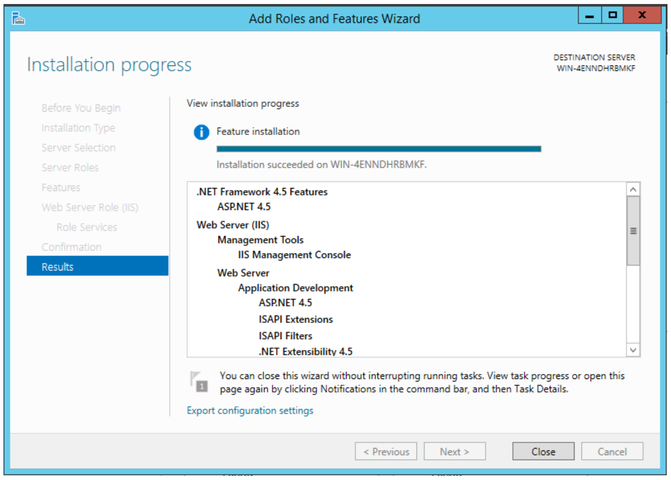
To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

```
.NET Framework 4.5 Features
    ASP.NET 4.5
Web Server (IIS)
    Management Tools
        IIS Management Console
    Web Server
        Application Development
            ASP.NET 4.5
            ISAPI Extensions
            ISAPI Filters
```

15. In the **Installation progress** section, click on **Close**.



View installation progress

Feature installation

Installation succeeded on WIN-4ENNDHRBMKF.

```
.NET Framework 4.5 Features
    ASP.NET 4.5
Web Server (IIS)
    Management Tools
        IIS Management Console
    Web Server
        Application Development
            ASP.NET 4.5
            ISAPI Extensions
            ISAPI Filters
            .NET Extensibility 4.5
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

B. Install the Mobile Application

The **maestro*MOBILE** installation must be performed by a qualified Maestro Technologies technician. Please communicate with the Software Support Department to request the assistance of a technician.

C. Update the Mobile Application

- If **maestro*MOBILE** is installed on the data server, simply update **maestro*** using the normal procedure; **maestro*MOBILE** will automatically be updated.
- If **maestro*MOBILE** is installed on a different server, but on which the **maestro*** client is also installed, simply launch **maestro*** and the update will begin. Once the update begin, just follow the displayed

instructions.

- If **maestro*MOBILE** is installed on a separate server, start by updating **maestro*** on the data server.

  Then copy on the **maestro*MOBILE** server the same kit used to update the **maestro*** server and launch it. The mobile update will begin; simply follow the displayed instructions.

Validation of the Installation

Once the application has been installed, validate the installation by accessing it through a browser.

1. Depending on the type of installation, access the application in *Google Chrome* by entering the address of your website for **maestro*MOBILE**.
2.
   Enter a **maestro*** user and password to confirm that the installation is successful.
   If the configuration screen appears, the application is functional.
3. To perform a diagnosis in case of error:
   a. In *Google Chrome*, go to the developers options (F12) and then select the **Network** tab.
   b. Press the **Login** button to see the server call appear.
   c. Diagnose the error by double-clicking on the message.

Last modification: April 06, 2021