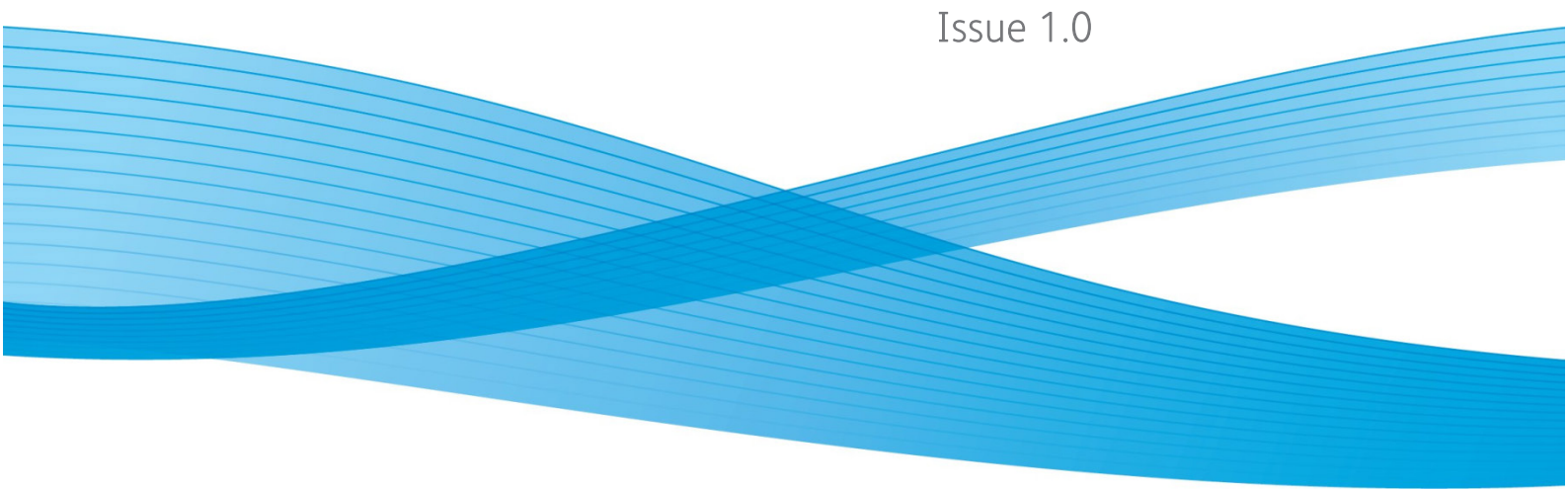


Installation Guide

Mobile Print for Business version 1.0

July 2014

Issue 1.0



Fuji Xerox Australia

101 Waterloo Road

North Ryde NSW 2113

For technical queries please contact the Fuji Xerox Australia Customer Support Centre on:
1800 028 962

© Fuji Xerox Australia Pty Limited. All rights reserved.

Xerox and the sphere of connectivity design are trademarks or registered trademarks of Xerox Corporation in the U.S. and/or other countries.

Note: By using this document you acknowledge that you have read and agree to the terms and conditions in the Mobile Print for Business Software Licence Agreement.

Issue History

Date	Issue	Reason
Jul 2014	1.0	First Issue

Contents

Introduction.....	5
Overview.....	5
Help Desk.....	5
Installation Prerequisites.....	6
How to Install <i>Mobile Print for Business</i>	8
Post-installation Configurations.....	15
How to Enable HTTPS for Default Web Site in Windows Server.....	15
How to Configure SDK Certificate Settings in Windows Server	19
How to Import SharePoint 2010 SSL Certificate in Mobile Print for Business Server	27
Getting the Application Ready to Work.....	36
Assigning Administrator Privilege to New Users.....	37
Client Application Availability.....	38
Troubleshooting.....	39
Appendix A – How to Get the Application Pool Identity in Windows Server	50
Appendix B – How to Export SSL Certificate in Windows Server	53
Appendix C – How to Verify If the PowerShell Feature is Enabled or Installed.....	54
For Windows 7, Windows 8 and Windows 8.1	54
For Windows Server 2008 and 2008 R2.....	57
For Windows Server 2012 and 2012 R2.....	59
Appendix D – How to Configure A User Account to Have ‘Logon as a service’ Permission.....	62
Appendix E – How to Assign db_owner Permission on the Database of SQL Server	66
Appendix F – How to Add A User to the IIS_IUSRS Group	72

Introduction

This document provides information on how to install the *Mobile Print for Business* application. It also explains the prerequisites for installation and the post-installation configurations.

Overview

The *Mobile Print for Business* application helps you to perform the following tasks:

- Printing files from the mobile device, printing files by capturing images using the device camera or printing files from Document Management System (DMS) on Android, iOS devices and Windows phones

Note: DMS is a computer system used to track and store electronic documents. Usually, it is also capable of keeping track of the different versions modified by different users (history tracking). The term has some overlap with the concepts of content management systems. It is often viewed as a component of enterprise content management (ECM) systems and related to digital asset management, document imaging, workflow systems and records management systems.

Mobile print for Business supports the following DMSs:

- DocuShare 6.5, 6.6.1
 - DocuShare Express 6.5, 6.6.1
 - Trim Context 7.0
 - WorkSite 8.5
 - SharePoint 2010
- Uploading files to DMS from the mobile device, device gallery or by capturing images using the mobile camera in Android, iOS devices and Windows phones
 - Scanning files of any format (PDF, PDF/A, Tiff/Single, Tiff/Multi, DocuWorks, JPEG, XPS) from the multi-function device (MFD) and saving copies in the mobile device (All other customisations such as filename, format, resolution, colour and plex can also be done.)

Note: The Scan feature does not work if the mobile uses 3G network.
For scanning, the Windows phones support only two formats, JPEG and PDF.

- Email Printing – Printing files by sending mails to the email ID set up for a device or print queue

Help Desk

If you require further assistance, contact the Fuji Xerox Australia Customer Support Centre on:
1800 028 962

Installation Prerequisites

Note: While installing the application, you must log in as a **domain user with administrative rights** and ensure that your machine is in the desired domain. After successful installation, you become the Administrator of the application by default. You can access the application later using the Administrator credentials and assign admin access to other users.

Following are the prerequisites required for the installation of *Mobile Print for Business*:

- The machine on which the application is going to be installed must have any of the following Operating Systems (OS):
 - Windows Server 2008 (32 bit and 64 bit)
 - Windows Server 2008 R2 Service Pack1
 - Windows Server 2012 (64 bit)
 - Windows Server 2012 R2 (64 bit)
 - Windows 7 (32 bit and 64 bit)
 - Windows 8 (32 bit and 64 bit)
 - Windows 8.1 (32 bit and 64 bit)

Note: Ensure that:

- The latest service packs are applied on the machine.
 - The latest Windows updates are installed on the machine and the machine is restarted after the updates are installed.
-
- The PowerShell feature [for Internet Information Services (IIS)] must be enabled or installed on Windows Server 2008 or higher versions. For information on how to verify if the PowerShell feature is enabled or installed, refer to [Appendix C](#).
 - SQL Server 2008 R2 or 2012 must be installed either on the same machine or on any other machine in the same network. The application supports all editions of SQL Server 2008 R2 or 2012. It supports SQL Server instances having either SQL Server authentication or Windows authentication.

Note: The SQL Server used for the application must not have a database named **APEOS_CORE**.

- You must configure Windows Firewall exceptions for the following ports:
 - Port 80 (HTTP)
 - Port 443 (SSL or HTTPS)
 - Port 1433 (SQL)
 - Port 515 (LPR)
 - Port 9933 (Trim)
 - Port 389 (LDAP)
 - Port 110 (POP3)
 - Port 25 (SMTP)
 - Port 995 (POP3 SSL)
 - Port 465 (SMTP SSL)
 - Ports assigned for DMS Servers (DocuShare, DocuShare Express and SharePoint 2010)

Note: The specified ports are the default ports. If you modify any of the default ports, please ensure that the ports are added as exceptions in firewall.

For example, SMTP default port is 25. If you change it to 29, firewall should be enabled for port 29.

For information on how to open a port in Windows firewall, refer to the following link:

<http://windows.microsoft.com/en-in/windows/open-port-windows-firewall#1TC=windows-7>

How to Install *Mobile Print for Business*

This section describes how to install *Mobile Print for Business*.

1. Right-click the **MobilePrintforBusiness.exe** file and select **Run as administrator**.

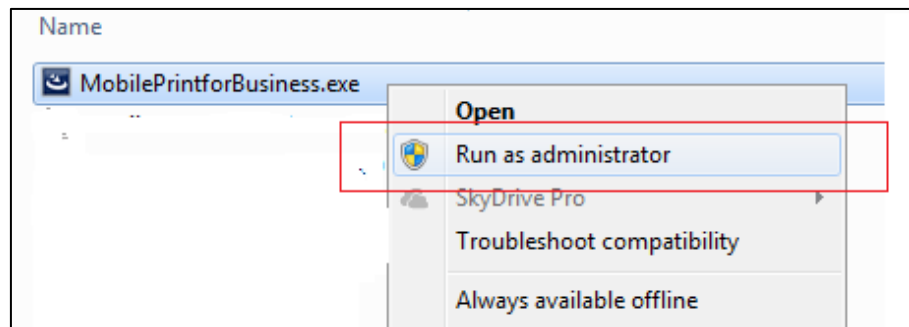


Figure 1

The *Mobile Print for Business* setup prepares the InstallShield Wizard.

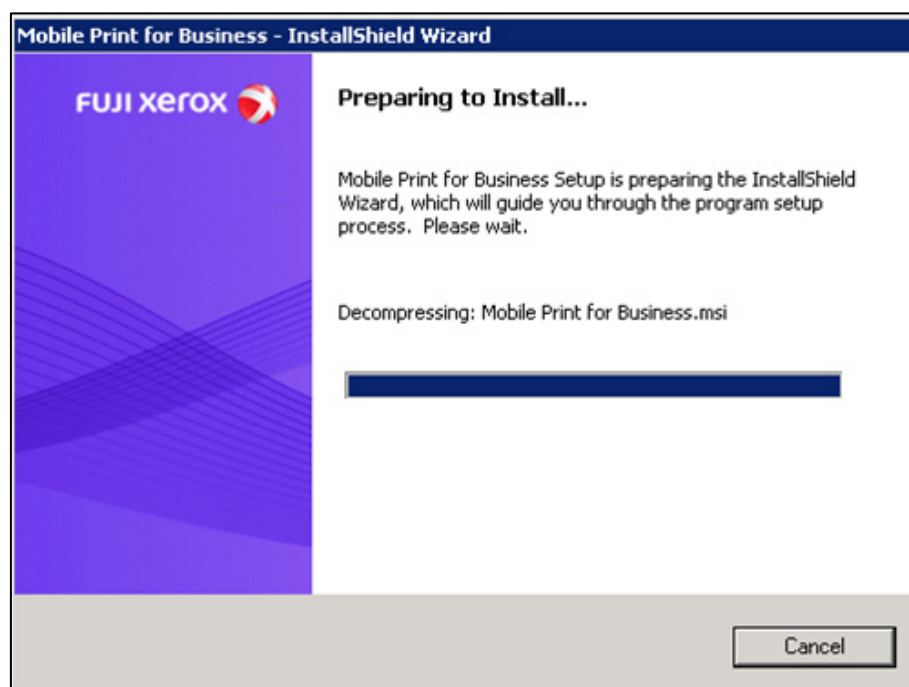


Figure 2

2. When the following screen is displayed, click **Next**.

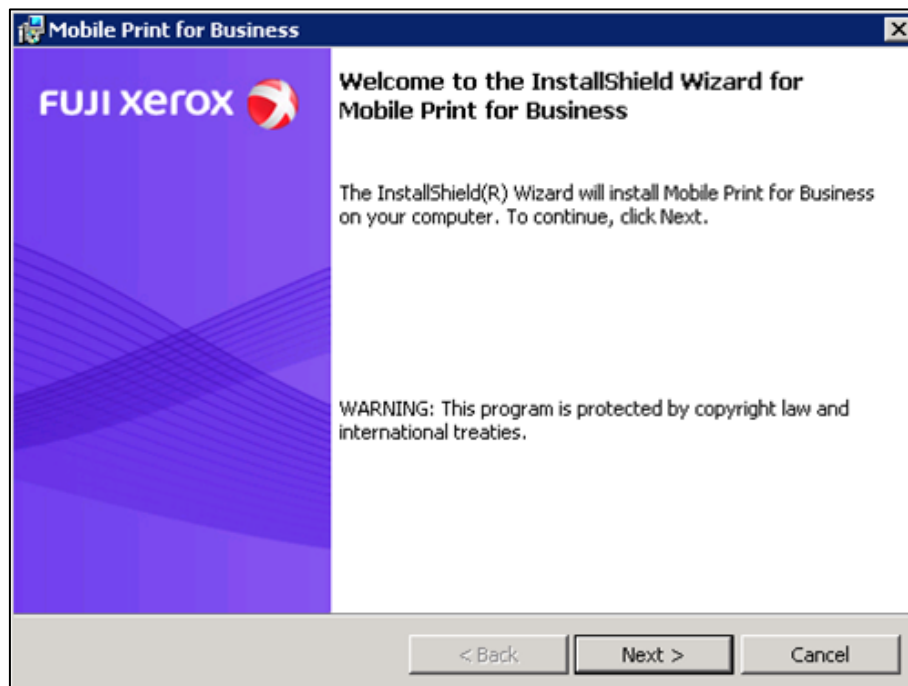


Figure 3

The *Licence Agreement* screen is displayed.

3. Select the **I accept the terms in the licence agreement** option and click **Next**.



Figure 4

The *Destination and Share Folder* screen is displayed.

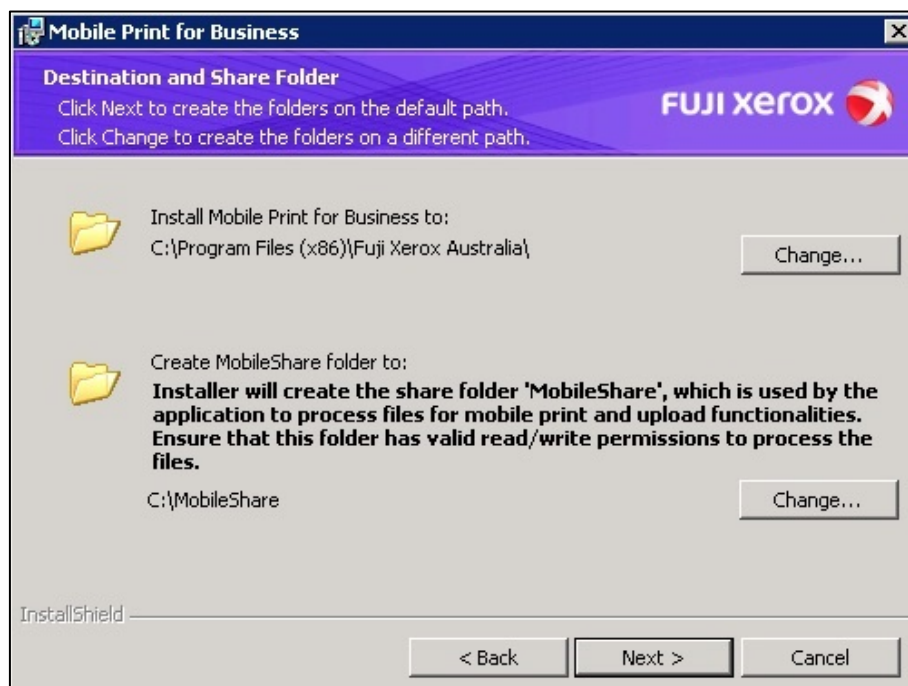


Figure 5

Note:

- The **MobileShare** share folder created by the installer is used to manage printing and uploading of files and attachments.
- Following is the default installation path:
 - For 32 bit machine:
C:\Program Files\Fuji Xerox Australia\Mobile Print for Business
 - For 64 bit machine:
C:\Program Files (x86)\Fuji Xerox Australia\Mobile Print for Business

4. Click **Next**.

The *Database Server Details* screen is displayed.

The screenshot shows the 'Database Server Details' window from the 'Mobile Print for Business' installer. The window has a purple header with the title 'Database Server Details' and the Fuji Xerox logo. Below the header, it says 'Select database server and authentication method'. The main area contains instructions: 'Provide the database server name and corresponding authentication details using which the application will install the required database scripts.' There is a text box for 'Database server name:' with a 'Browse...' button next to it. Below this, it says 'Connect using:' with two radio button options: 'Windows authentication credentials of current user' (which is selected) and 'Server authentication using the Login ID and password below'. Under the second option, there are text boxes for 'Login ID:' and 'Password:'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

Figure 6

Note 1: The logged-in user must have the **db_owner** permission on the **master** database of the SQL Server if they want to use the **Windows authentication credentials of current user** option.

For information on how to assign **db_owner** permission to the desired user on the database of the SQL Server, refer to [Appendix E](#).

Note 2: The following screen is displayed when you select **Windows authentication credentials of current user**:

The screenshot shows the 'Logon Information' window from the 'Mobile Print for Business' installer. The window has a purple header with the title 'Logon Information' and the Fuji Xerox logo. Below the header, it says 'Specify a domain user name and password'. The main area contains instructions: 'Specify user credentials to be used for IIS Application Pools.' There are three text boxes for 'Domain name:', 'User name:', and 'Password:'. Below these, there is a checkbox labeled 'I confirm that user entered above has below privileges:' followed by a list of four requirements: 1. Member is a valid domain user, 2. Member of local administrators group, 3. Member of IIS_IUSRS group, and 4. Assigned user rights for 'Log on as a service'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

Figure 7

If the **Windows authentication credentials of current user** option is selected, ensure that:

- Valid **Domain name**, **User name** and **Password** are provided.
- The user is added to the **IIS_IUSRS** group.
For information on how to add a user to the **IIS_IUSRS** group, refer to [Appendix F](#).
- The user account is assigned with the **Log on as a service** permissions.
For information on how to configure a user account to have **Logon as a service** permission, refer to [Appendix D](#).
- The user has Read-Write permission to the Mobile Share Folder created during installation.
- The user has the **db_owner** permission on the **master** database of the SQL Server.
For information on how to assign **db_owner** permission to the desired user on the database of the SQL Server, refer to [Appendix E](#).

5. Click **Next**.

The *Ready to Install the Program* screen is displayed.

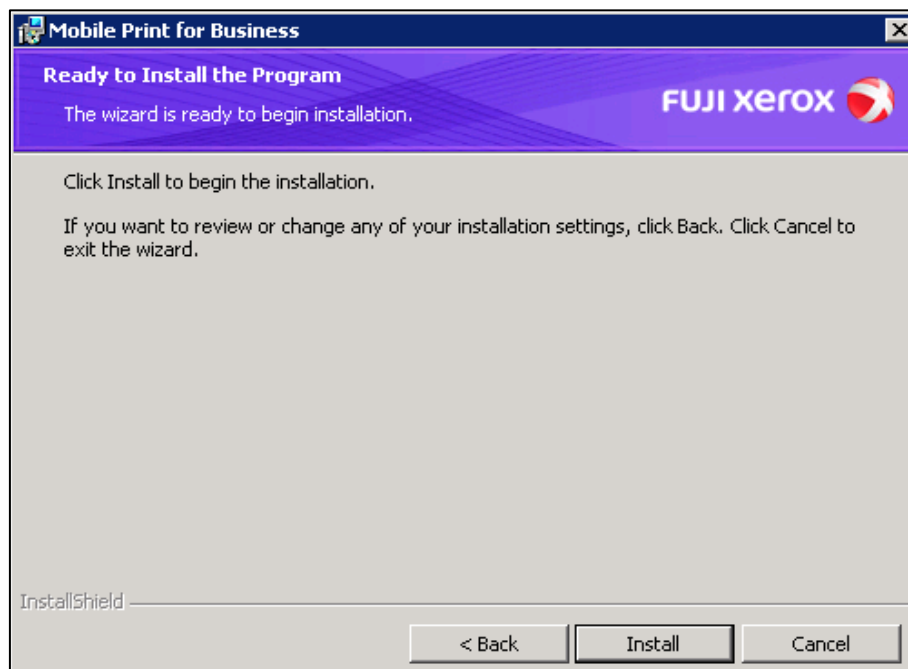


Figure 8

6. Click **Install**.

The installation continues.

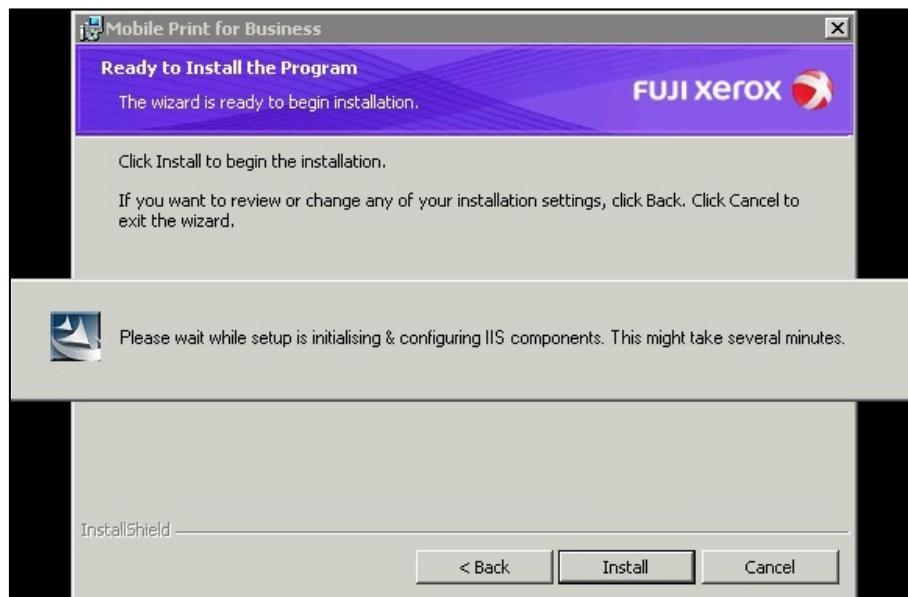


Figure 9

After the installation is complete, the following screen is displayed:

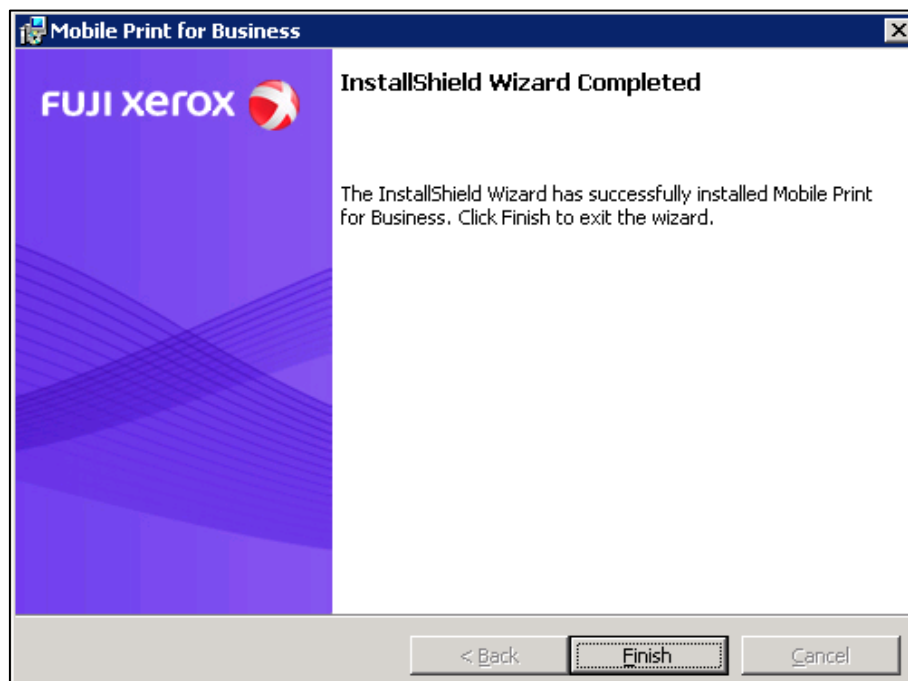


Figure 10

7. Click **Finish** to close the wizard.

Note:

- Please restart the machine if you are asked to do so at the end of the installation.
- After the installation, the shortcut for Mobile Print for Business Admin is created in the following path:

START > All Programs > Fuji Xerox Australia > Mobile Print for Business > Admin

- Following is the Mobile Print for Business Admin URL:

http://<Machine Name/IP>/MobilePrintforBusiness

Post-installation Configurations

This section provides information on the following configurations that must be done after the installation of *Mobile Print for Business*.

- Enabling HTTPS for Default Web Site in IIS
- Configuring SDK Certificate Settings
- Importing SharePoint 2010 Secure Sockets Layer (SSL) Certificate in Mobile Print for Business Server

How to Enable HTTPS for Default Web Site in Windows Server

The installer automatically enables HTTPS bindings for Default Web Site in Windows Server 2008, 2008 R2, 2012, 2012 R2, Windows 7, Windows 8 and Windows 8.1. If it is not enabled, perform the following steps to enable it:

1. Type *inetmgr* in **Run** prompt and click **OK**.

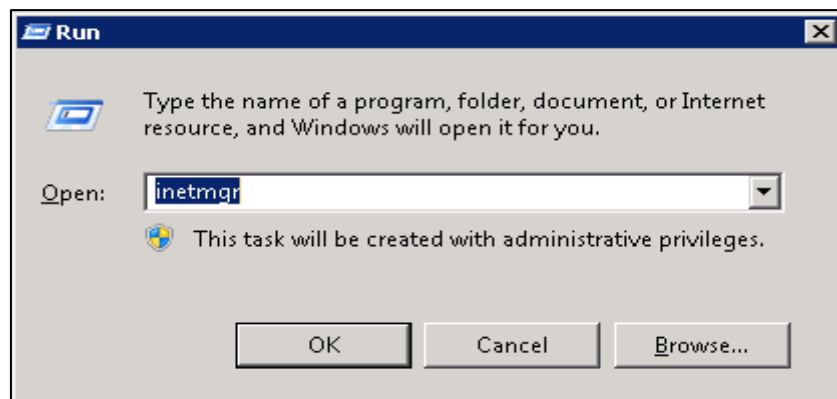


Figure 11

The following screen is displayed:

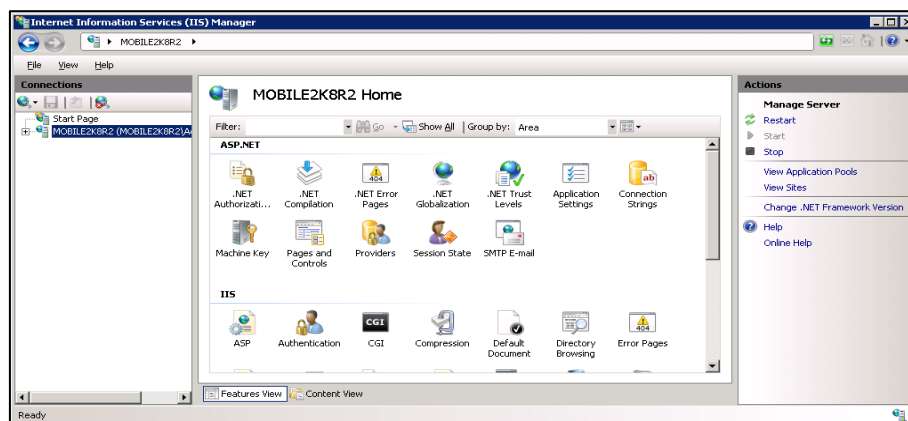


Figure 12

2. Expand the node under **Connections** section (in the left pane) and click **Default Web Site** as displayed in the screenshot below:

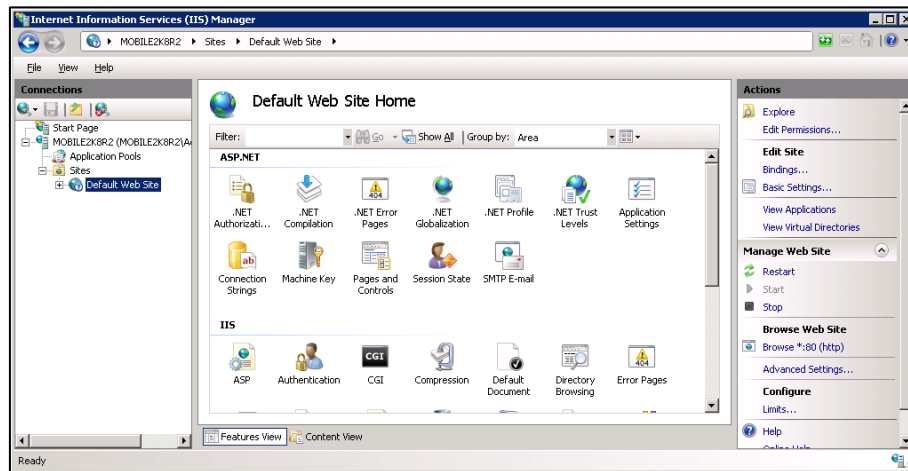


Figure 13

3. Click **Bindings** in the right pane under **Actions > Edit Site**. (Refer to the figure above.)
The *Site Bindings* screen is displayed:

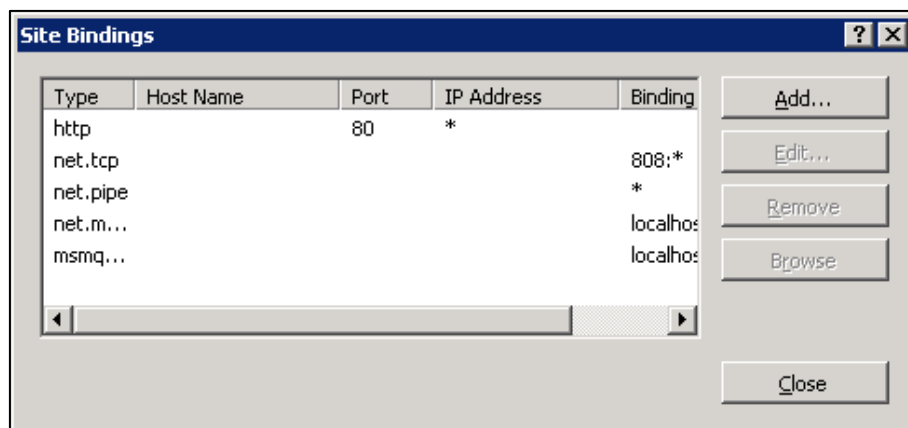
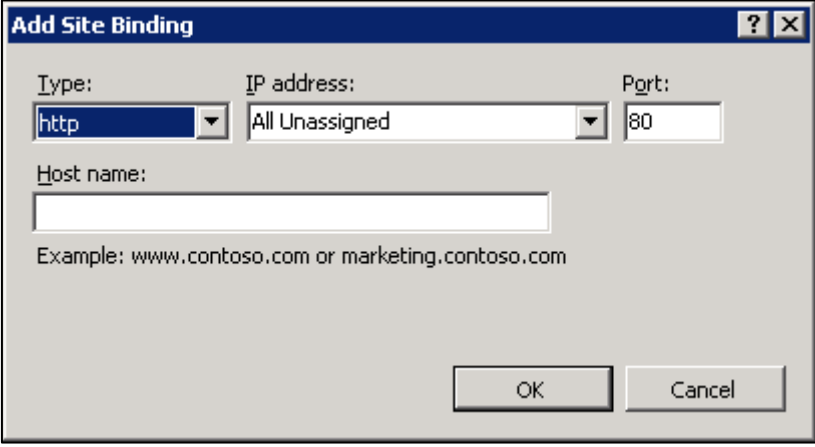


Figure 14

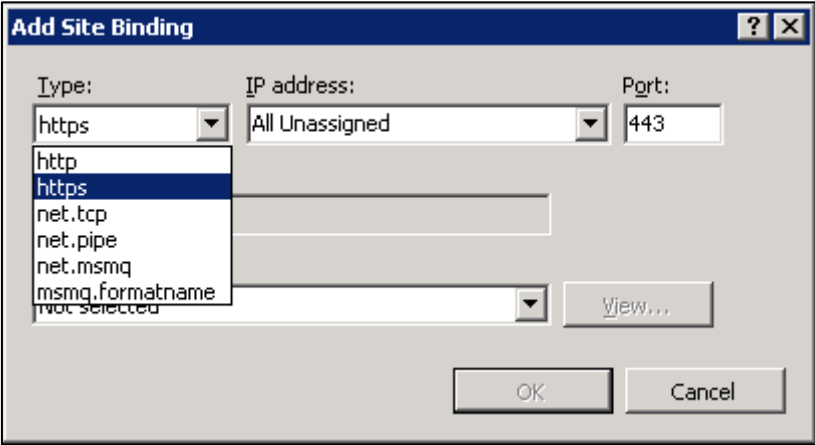
4. Click **Add...** on the Site Bindings screen.
The *Add Site Binding* screen is displayed:



The **Add Site Binding** dialog box is shown. It has a title bar with a question mark and a close button. The main area contains three fields: **Type:** with a dropdown menu showing 'http', **IP address:** with a dropdown menu showing 'All Unassigned', and **Port:** with a text box containing '80'. Below these is a **Host name:** text box. An example text 'Example: www.contoso.com or marketing.contoso.com' is shown below the host name field. At the bottom right are **OK** and **Cancel** buttons.

Figure 15

5. Select **https** from the **Type:** drop-down list.



The **Add Site Binding** dialog box is shown with the **Type:** dropdown menu open. The dropdown list shows the following options: 'http', 'https' (highlighted), 'net.tcp', 'net.pipe', 'net.msmq', 'msmq.formatname', and 'not selected'. The **IP address:** dropdown menu still shows 'All Unassigned', and the **Port:** text box now contains '443'. A **View...** button is visible next to the **Host name:** field. The **OK** and **Cancel** buttons are at the bottom right.

Figure 16

6. Select the appropriate certificate from the **SSL certificate:** drop-down list and click **OK**.

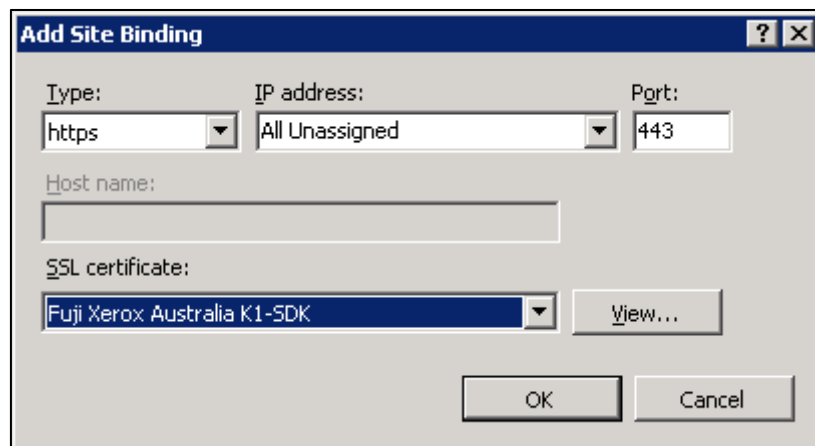


Figure 17

The following screen is displayed:

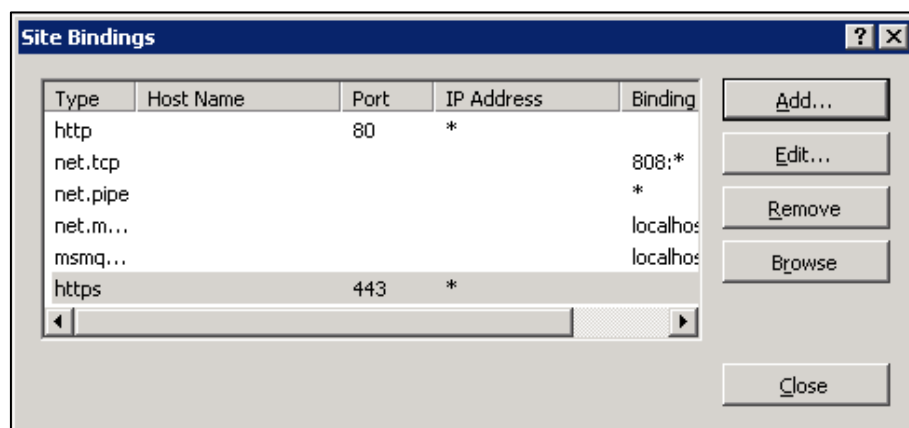


Figure 18

7. Click **Close**.

How to Configure SDK Certificate Settings in Windows Server

The following section explains the procedure to provide permission to access the private key of the FXA-K1SDK Certificate for the identity user with which the Mobile Print for Business App Pool (MPBASPNET4) is running. This procedure is applicable for Windows Server 2008, 2008 R2, 2012, 2012 R2, Windows 7, Windows 8 and Windows 8.1.

Note: For information on how to get the application pool identity in Windows Server 2008, 2008 R2, 2012, 2012 R2, Windows 7, Windows 8 and Windows 8.1, refer to [Appendix A](#).

1. Open **Run** prompt, type **mmc** and click **OK**.

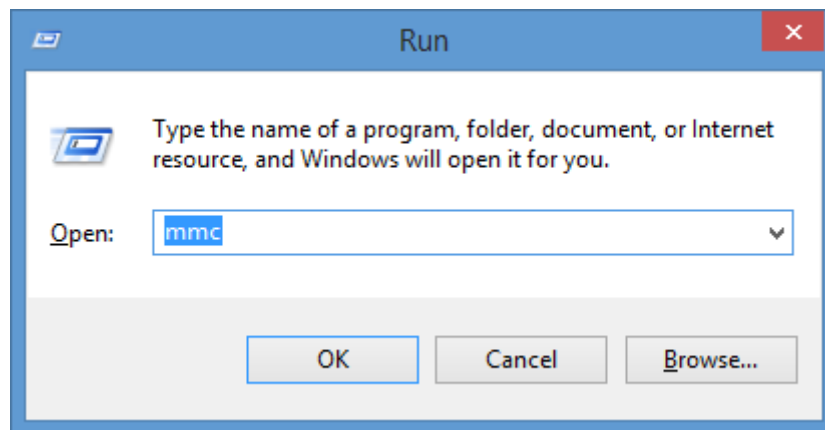


Figure 19

The Microsoft Management Console opens.

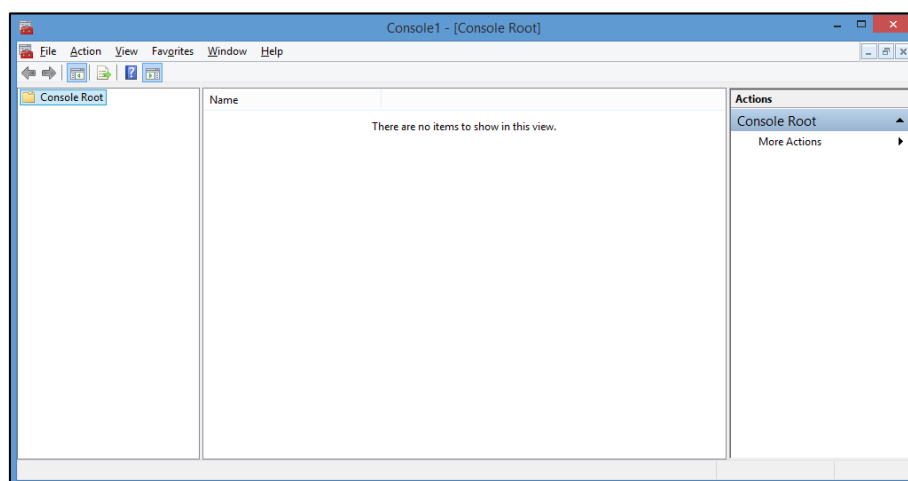


Figure 20

2. From the File drop-down list, click **Add/Remove Snap-in....**

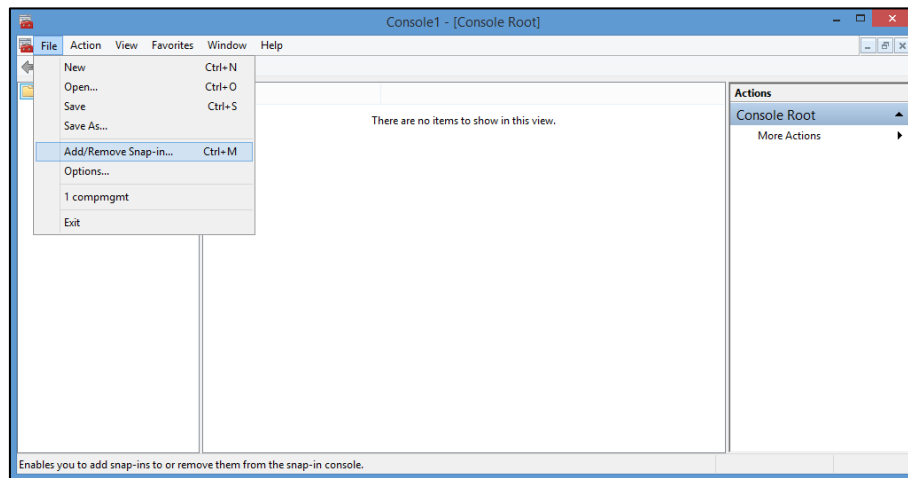


Figure 21

The Add or Remove Snap-ins window opens.

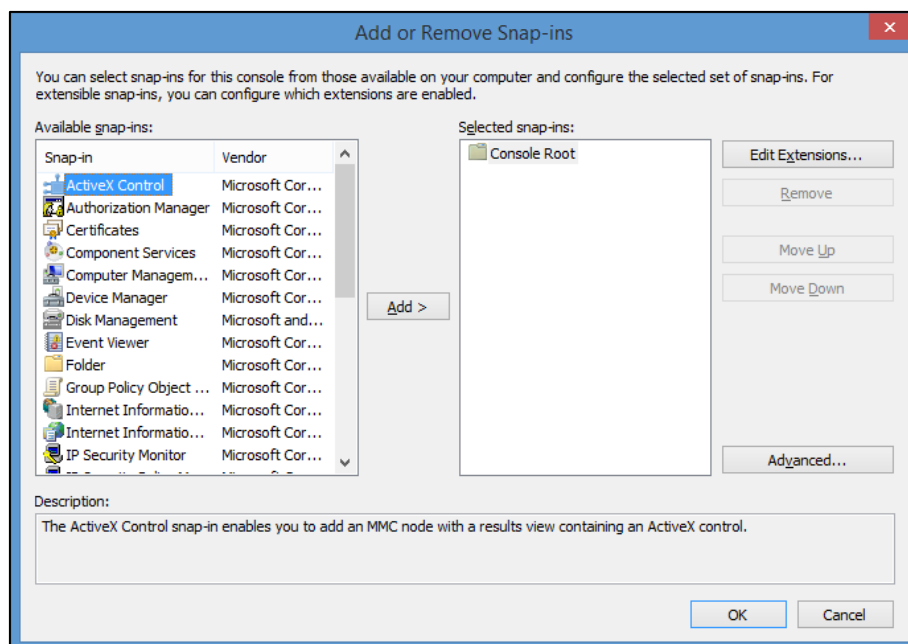


Figure 22

3. Select **Certificates** from the available snap-ins in the left pane, click **Add**.

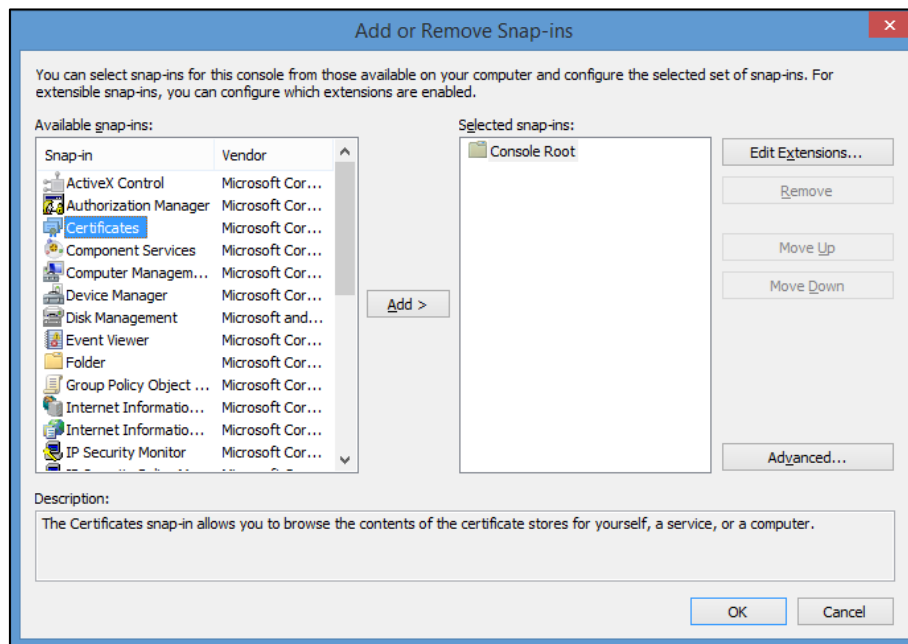


Figure 23

The Certificates snap-in window opens.

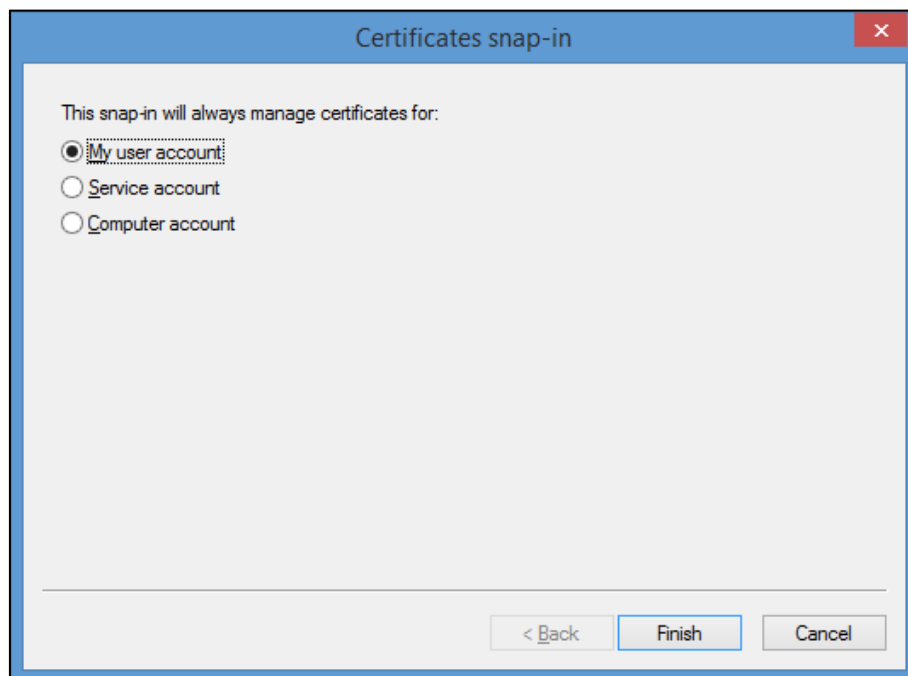


Figure 24

4. Select **Computer Account** from the available options and click **Next**.

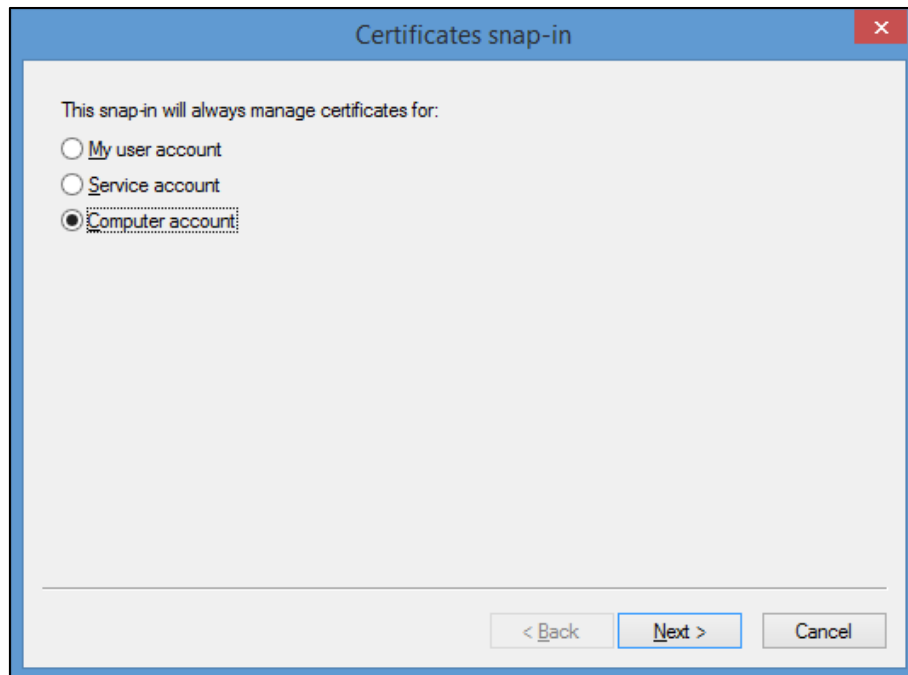


Figure 25

The Select Computer window opens.

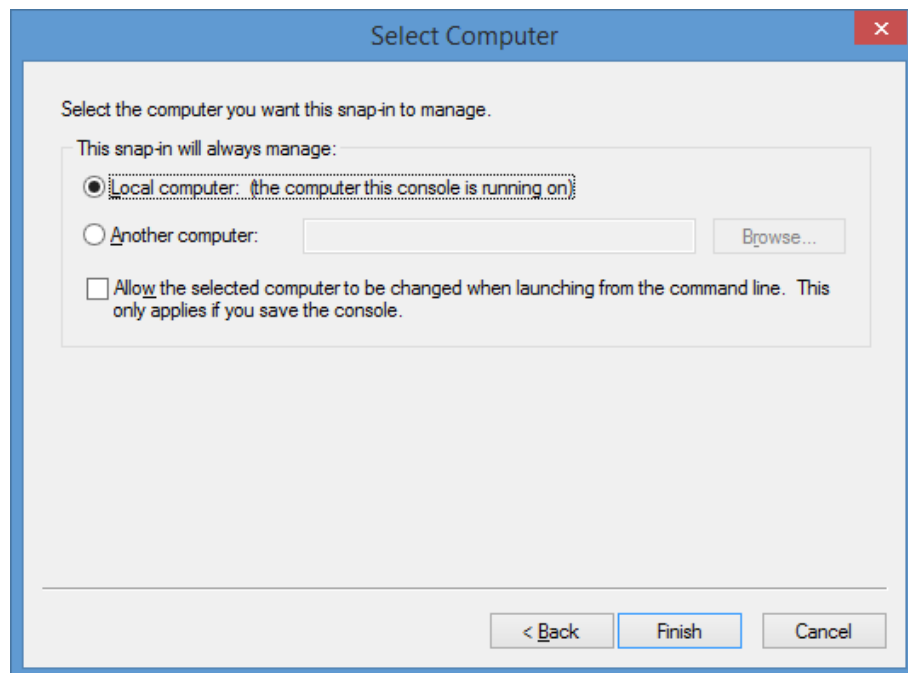


Figure 26

5. Click **Finish**.
The Certificates snap-in is added.
6. Click **OK** on the following screen:

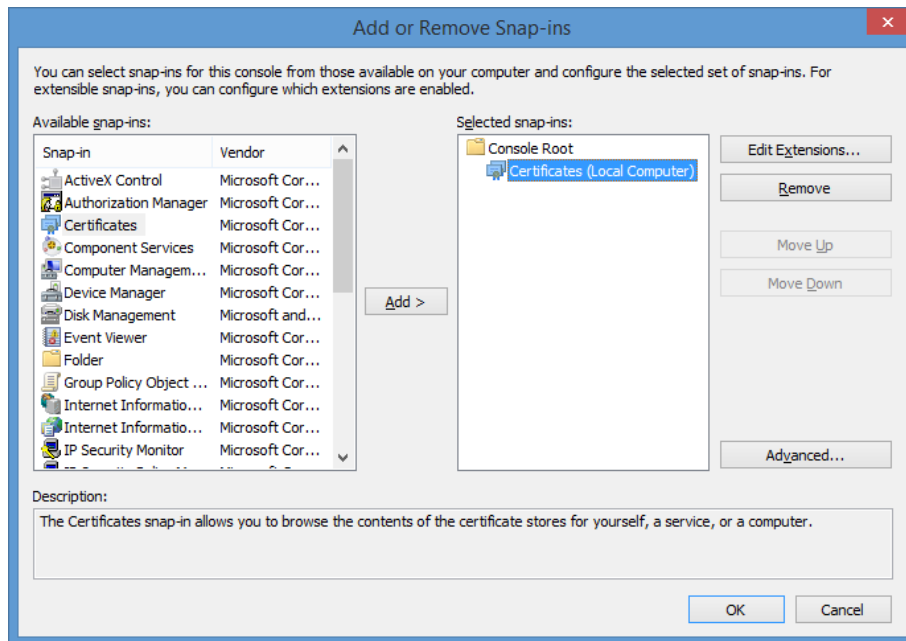


Figure 27

7. Expand the **Certificates** node *first* and *then*, the **Personal** node, in the left pane. Click **Certificates**.
The certificate (FXA-K1SDK here) is displayed in the middle pane.

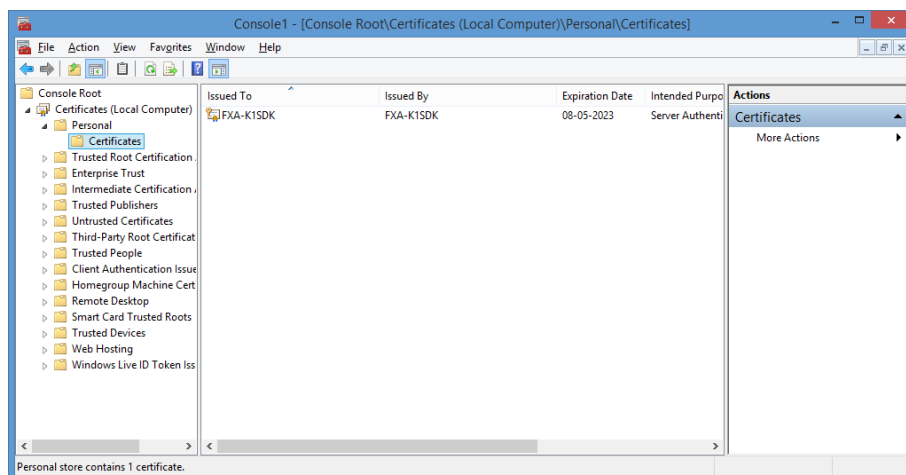


Figure 28

8. Right-click on the certificate, point to **All Tasks**, and select **Manage Private Keys....**

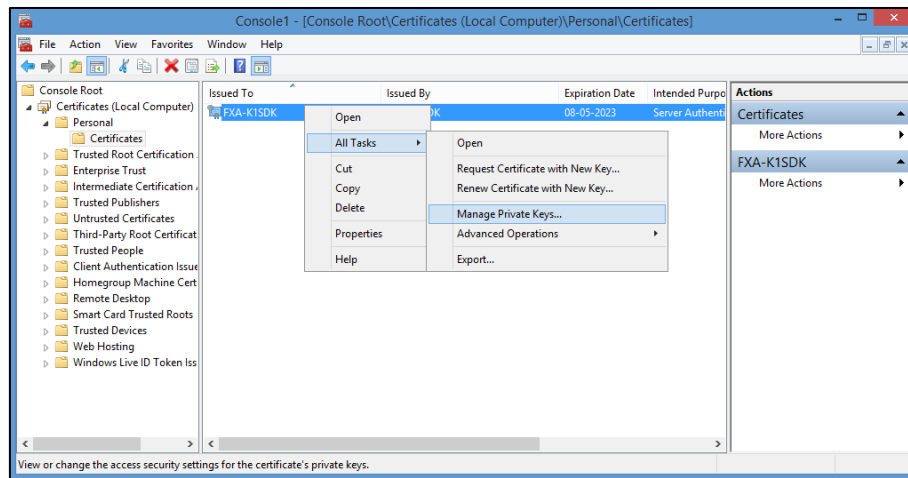


Figure 29

The following screen is displayed:

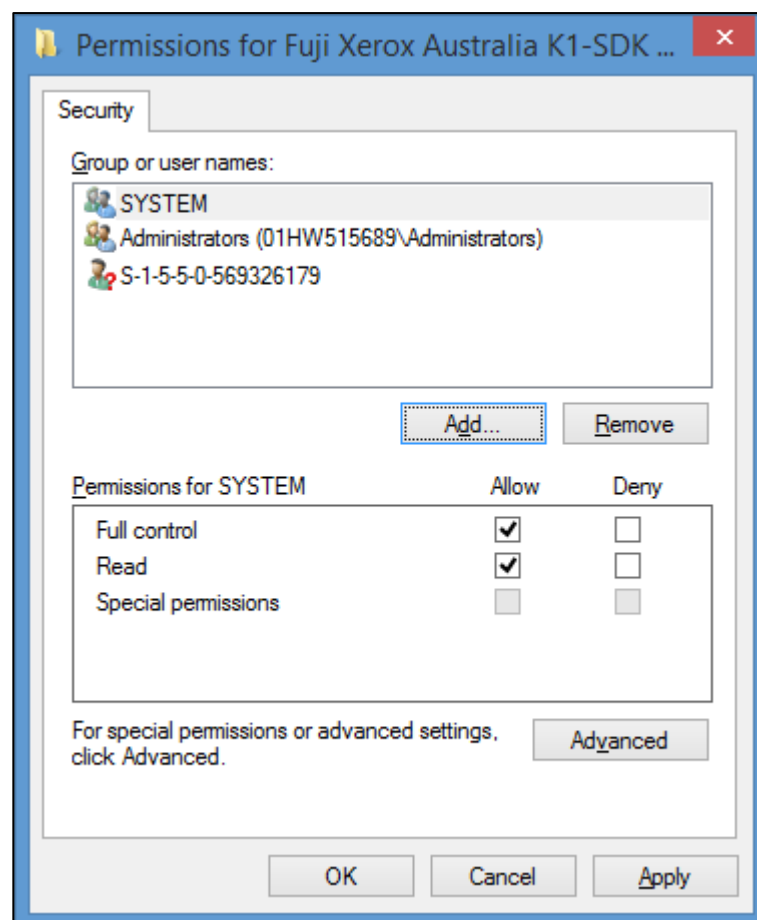


Figure 30

9. Click **Add**.

The following screen is displayed:

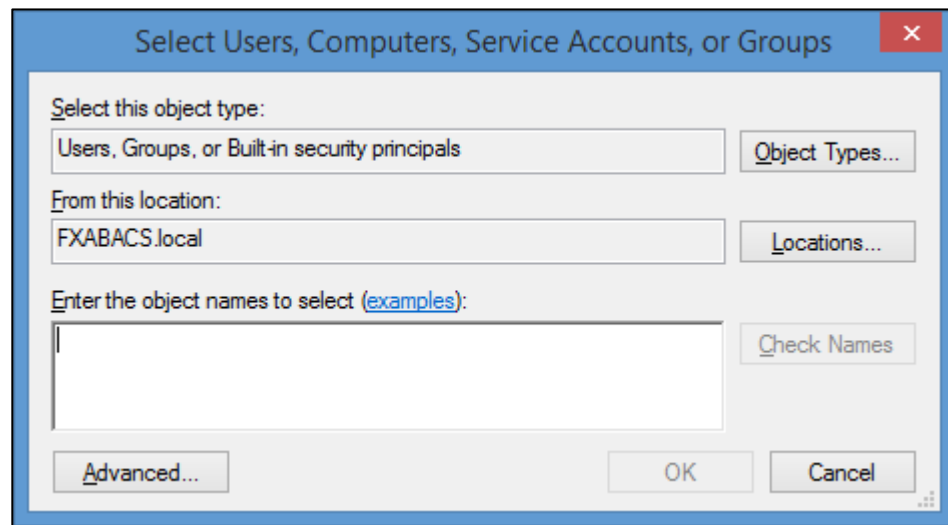


Figure 31

10. Type the identity name (*local service* in the screenshot) with which the Mobile Print for Business application pool is running in the **Enter the object names to select** field, and click **Check Names**:

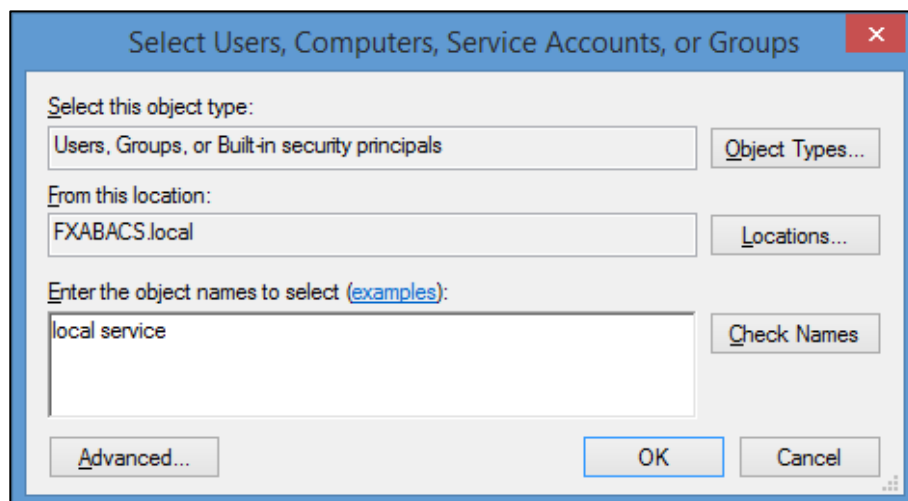


Figure 32

The following screen is displayed:

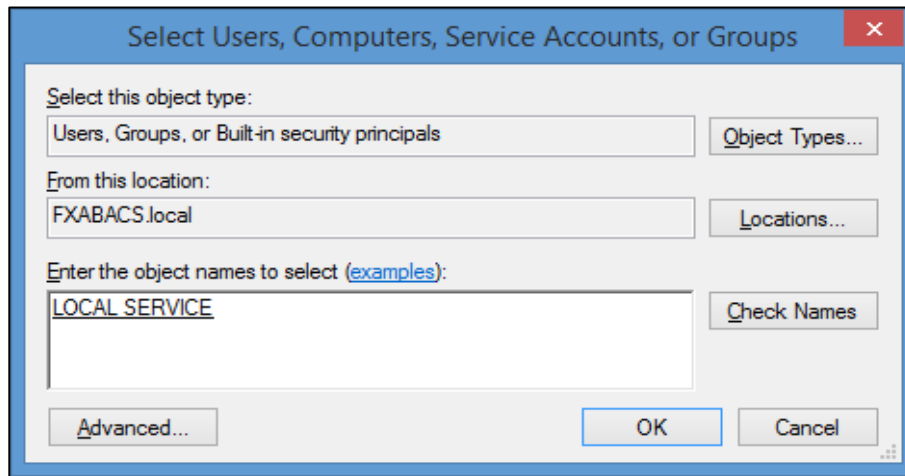


Figure 33

11. Click **OK**.

The following screen is displayed:

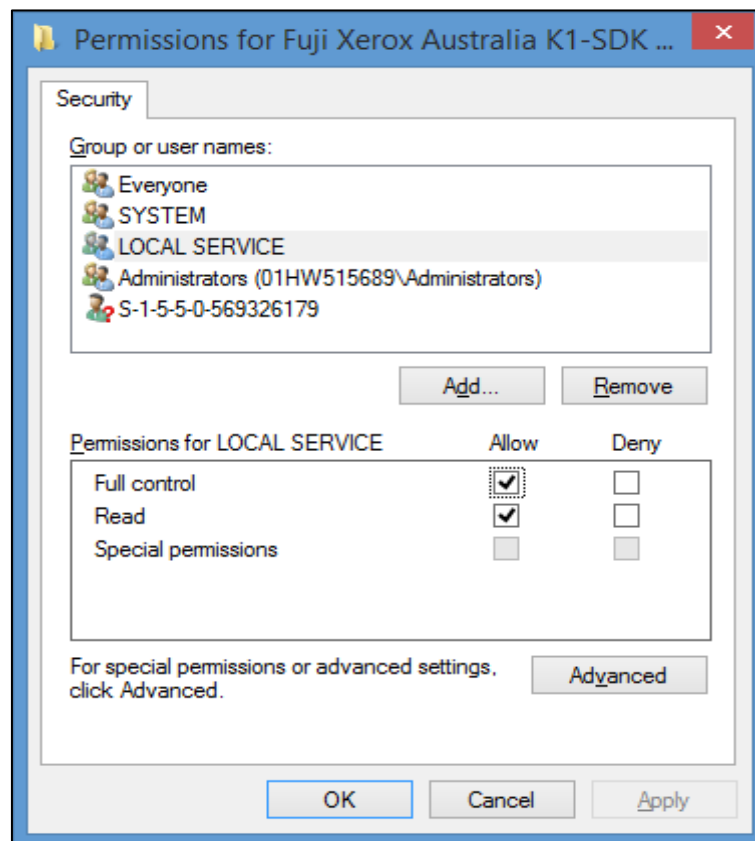


Figure 34

12. Click **OK**.

How to Import SharePoint 2010 SSL Certificate in Mobile Print for Business Server

Note: If the SharePoint 2010 Server is enabled with SSL, you must export the SSL certificate of SharePoint Site from the SharePoint 2010 Server and import it to the Mobile Print for Business server. For information on how to export the SSL certificate on Windows Server, refer to [Appendix B](#).

To import the SharePoint 2010 SSL certificate into the Mobile Print for Business Server in Windows Server 2008, 2008 R2, 2012, 2012 R2, Windows 7, Windows 8 and Windows 8.1:

1. Open **Run** prompt, type *mmc* and click **OK**.

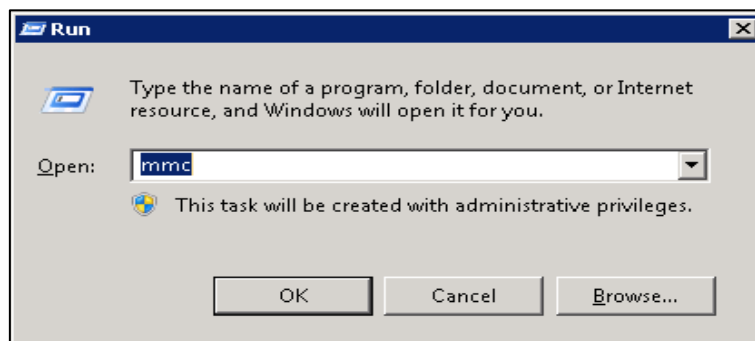


Figure 35

The *Console Root* window is displayed:

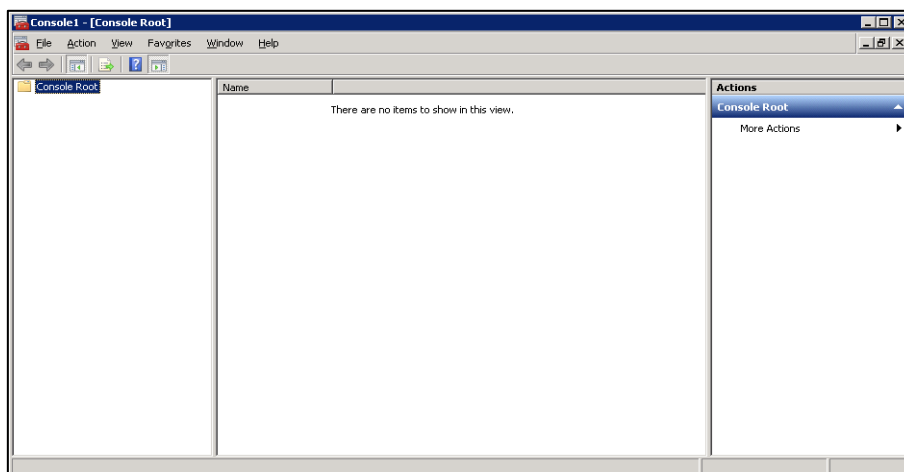


Figure 36

2. From the **File** menu, click **Add/Remove Snap-ins**.
The *Add or Remove Snap-ins* window is displayed:

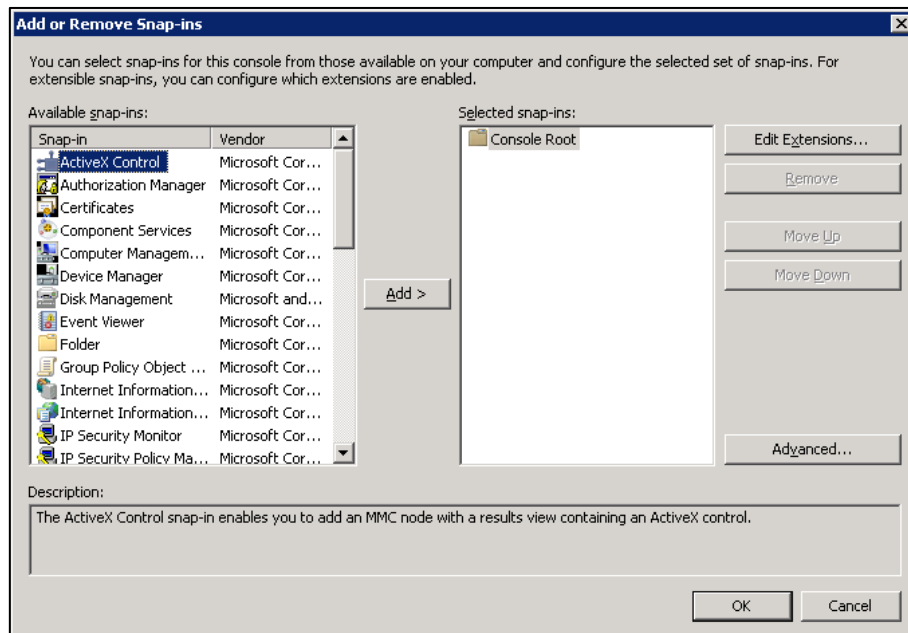


Figure 37

3. Select **Certificates** in the left list box and click the **Add** button.

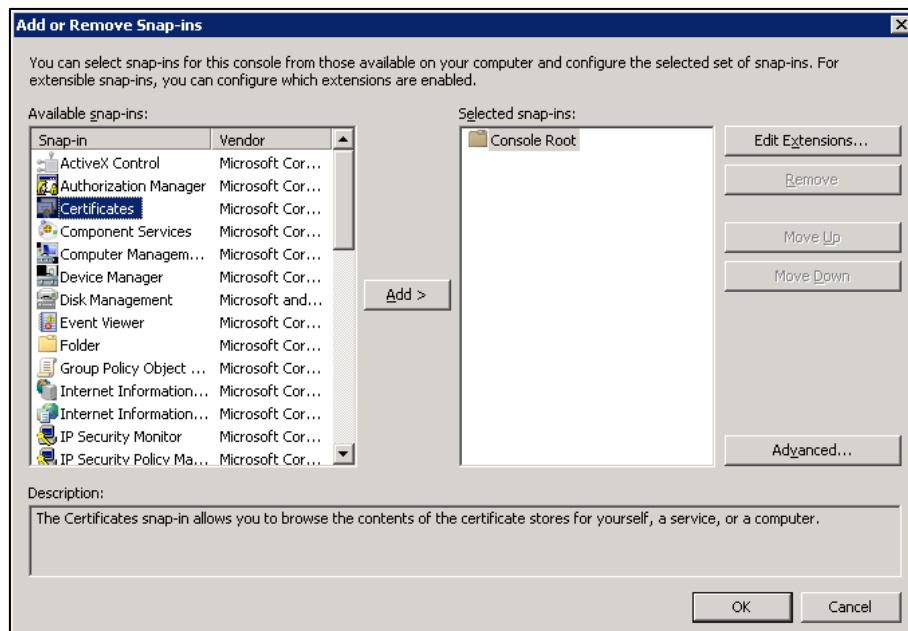


Figure 38

The *Certificates Snap-in* window is displayed:

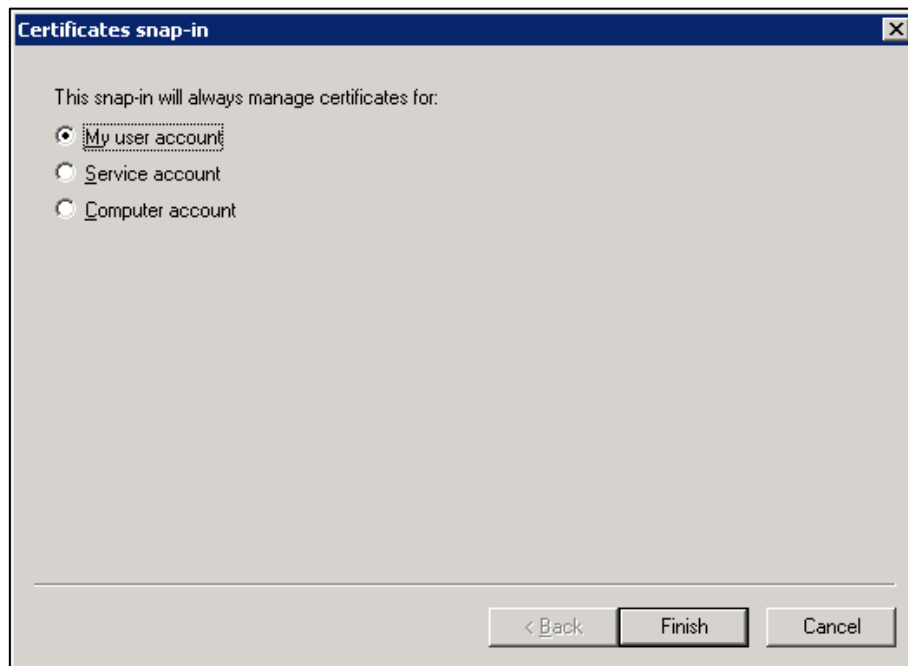


Figure 39

4. Select **Computer account** and click **Next**.

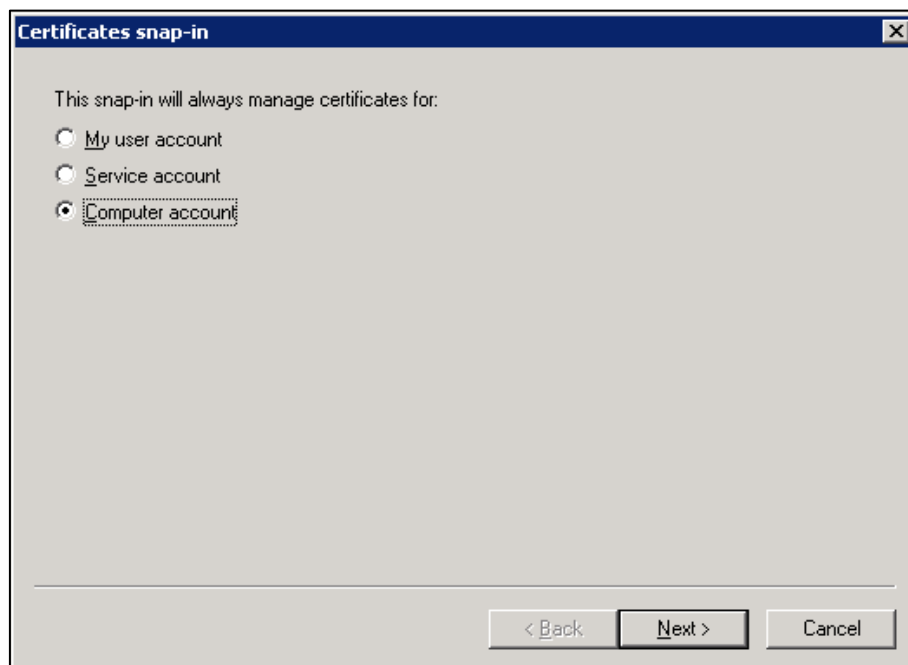


Figure 40

The *Select Computer* window is displayed:

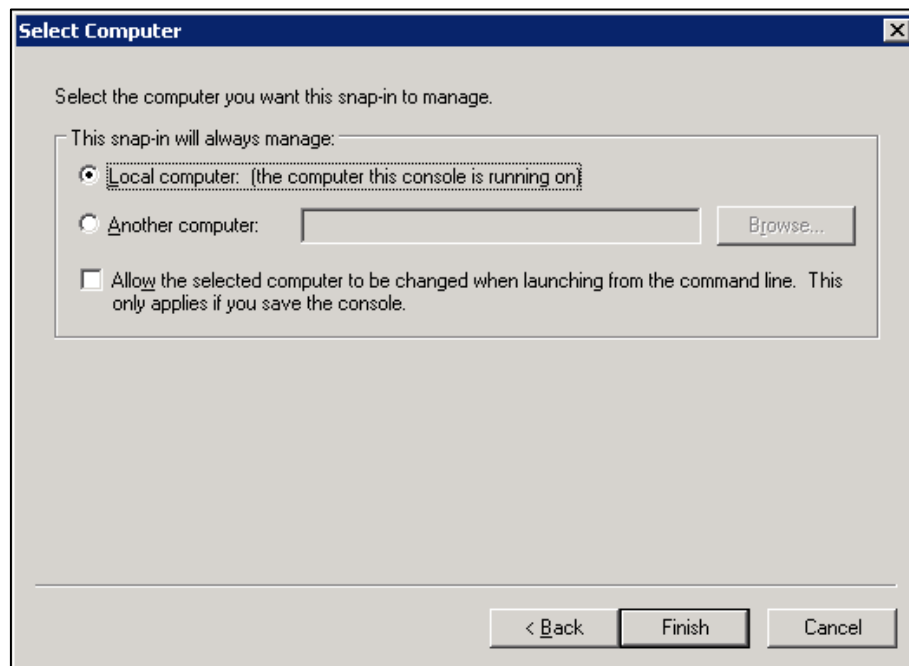


Figure 41

5. Click **Finish**.

The following screen is displayed (with Certificates added to the Console Root):

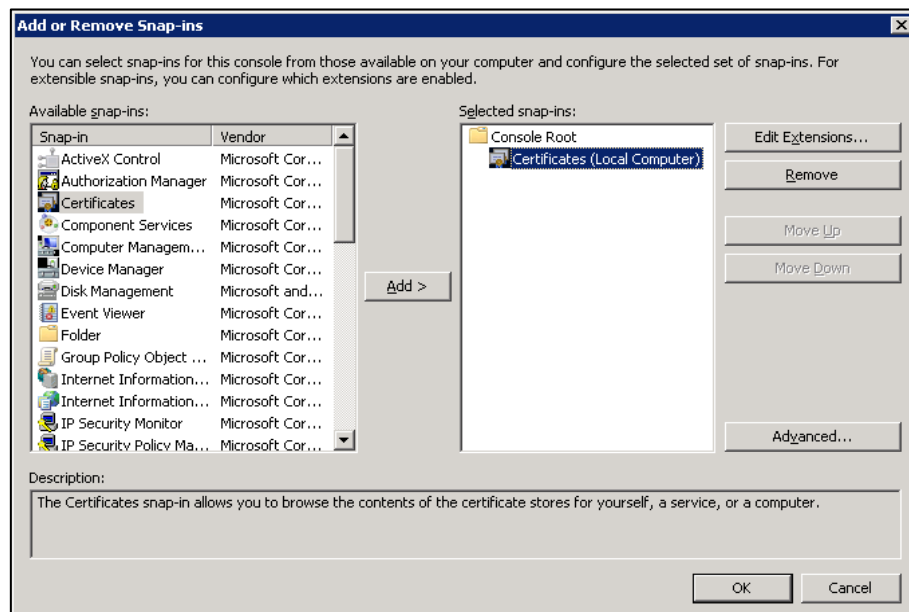


Figure 42

6. Click **OK**.

7. Click the **Certificates** node under *Console Root* in the left panel:

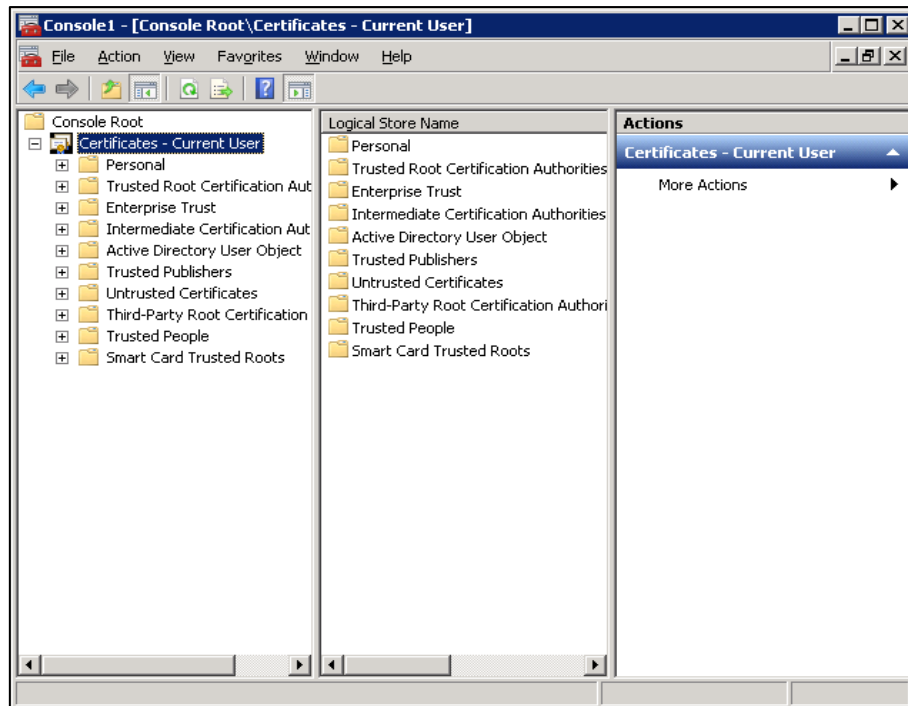


Figure 43

8. Click **Trusted Root Certification Authorities**.

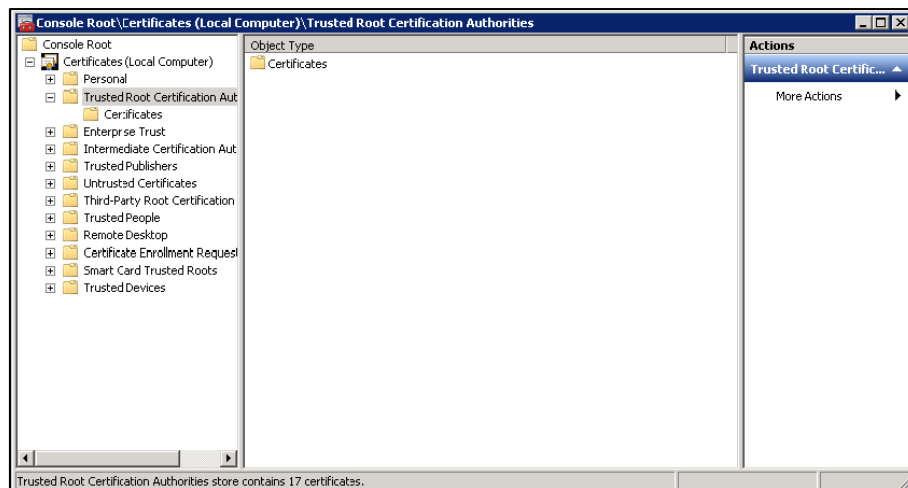


Figure 44

9. Right-click on **Certificates** under Object Type, point to **All Tasks** and click **Import....**

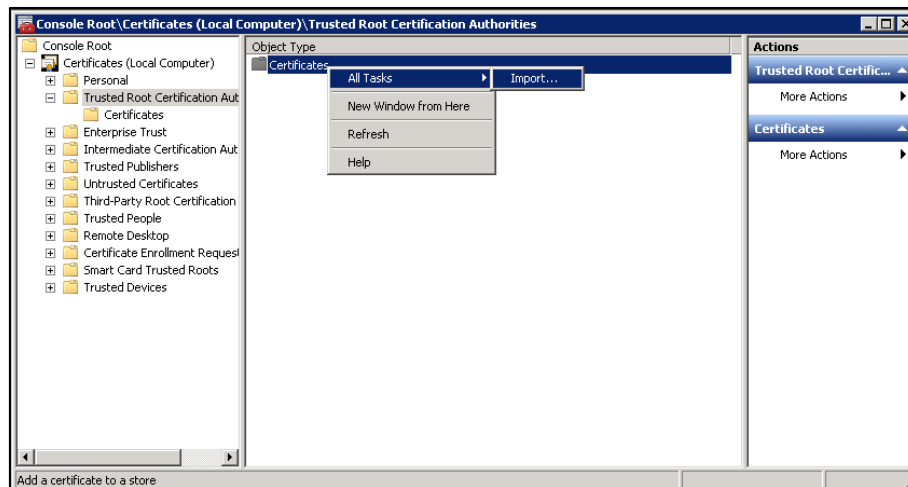


Figure 45

The *Certificate Import Wizard* is displayed:



Figure 46

10. Click **Next**.

11. Click **Browse** to browse the appropriate certificate file and click **Next**:

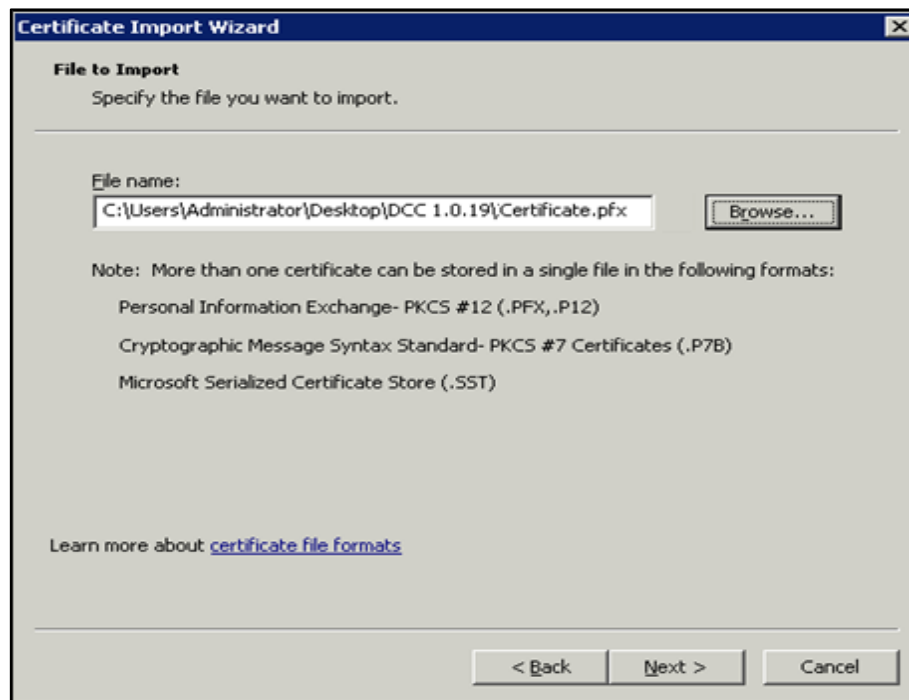


Figure 47

12. Type the password which is set for the certificate file and click **Next**.

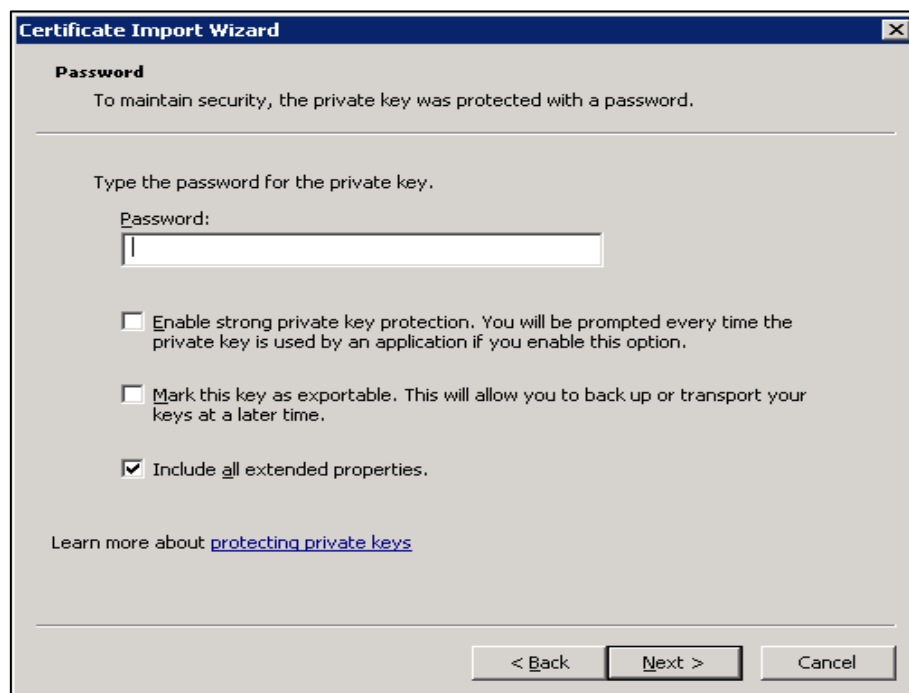


Figure 48

The following screen is displayed with the **Place all certificates in the following store** option selected by default:

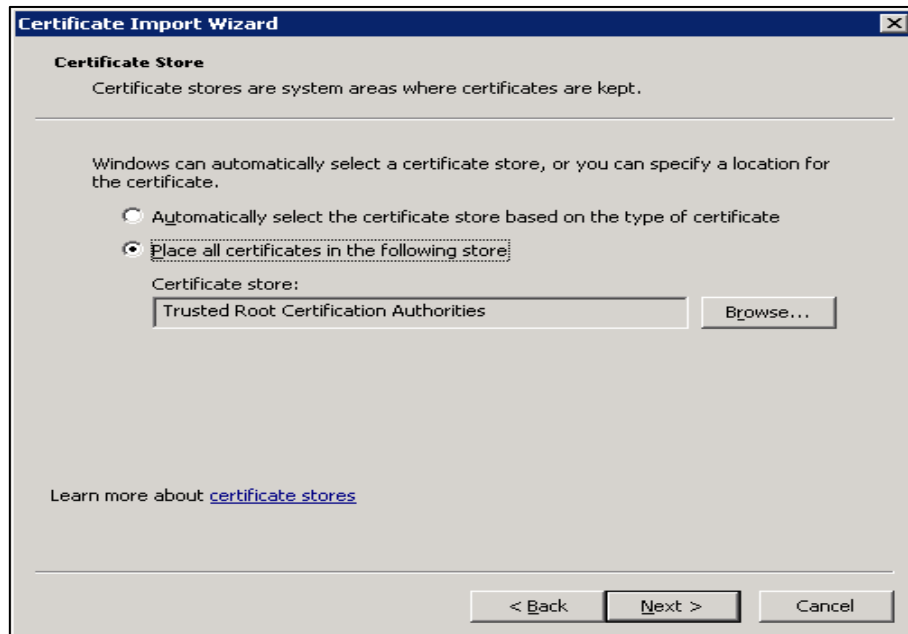


Figure 49

13. Click **Next**.

The following screen is displayed:

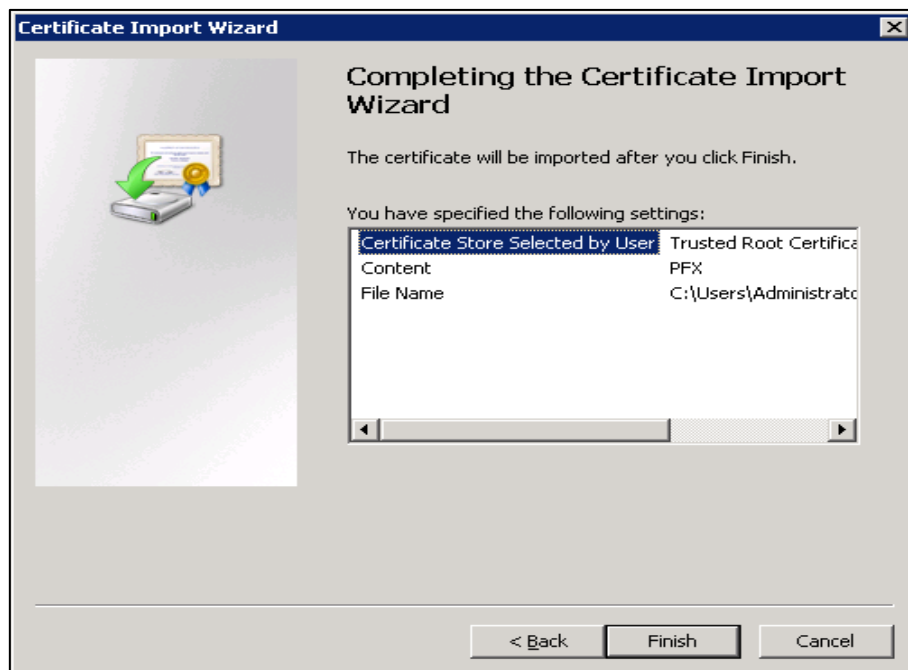


Figure 50

14. Click **Finish**.

The following pop-up window is displayed:

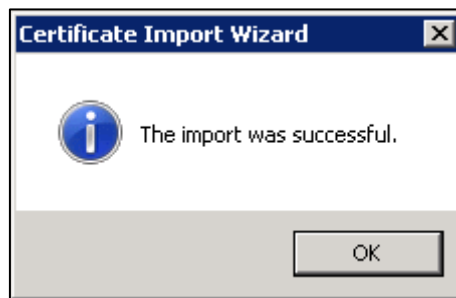


Figure 51

15. Click **OK** to close the pop-up window.

Getting the Application Ready to Work

After the post-installation configurations are complete, perform the following steps to get the application ready to work:

1. Click **Start > All Programs > Fuji Xerox Australia > Mobile Print for Business > Admin.**

Note: Accessing the application varies depending upon the OS installed on the machine.

The application window opens.

2. Click **Please click here to configure LDAP Settings.**

The *Manage Servers* page opens.

3. Enter the details of **LDAP Settings** and **MFD Username** and **Password**.

4. Click **Save Settings**.

A confirmation message *Common Setting saved successfully* is displayed.

5. Click the **Users** tab on the left pane.

6. Click **Import AD Users**.

7. Type the required search criteria to import the users from Active Directory in the text box and click the **Get Users** button.

8. Select the users you want to allow **Admin Access** and **Mobile Access** privileges of the application.

9. From the **Devices/Queues** tab, add devices or queues by following the steps provided in the *Mobile Print for Business Online Help*.

10. If you want to use the email print functionality, go to the **Servers** tab, click **Email Settings**, modify the required details and click **Save Settings**.

11. From **Manage DMS** tab, enable the DMS (which you want to access from your mobile device) and configure the DMS server settings.

Now the application is ready to work.

Note: The trial licence of the application is valid for 30 days. You must buy a perpetual licence to use the application beyond the trial period.

For additional information, refer to the *Mobile Print for Business Help* (online help embedded in the application). You can access this help by clicking the *Help* link displayed on the top left side of the application web page.

Assigning Administrator Privilege to New Users

To assign Administrator privilege (for the application) to new users:

1. Browse the **web.config** file from the path *<Installation Directory>\Fuji Xerox Australia\Mobile Print for Business\Admin>*.
2. Open the file with notepad.
3. Look for the **DefaultAdministrator** value in the **<appSettings>** section as displayed in the following screenshot:

```
<appSettings>
  <add key="webpages:Version" value="1.0.0.0" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="ApplicationKeyForLogging" value="SMS_WebUI" />
  <add key="RoboHelpURL" value="/MobilePrintforBusiness/Help/Overview.htm"/>
  <add key="DefaultAdministrator" value="Administrator"/>
```

Figure 52

4. Replace the **DefaultAdministrator** value with the **Windows login ID** of the new user to whom you want to assign Administrator privilege.

Client Application Availability

For **Android** devices – Download the *Mobile Print for Business* client application from the Google Play Store.

For **iOS** devices – Download the *Mobile Print for Business* client application from the Apple App Store.

For **Windows** devices – Download the *Mobile Print for Business* client application from the Windows App Store.

Troubleshooting

Problem 1: *While trying to access the application, the following screen with the error message is displayed. What should I do?*

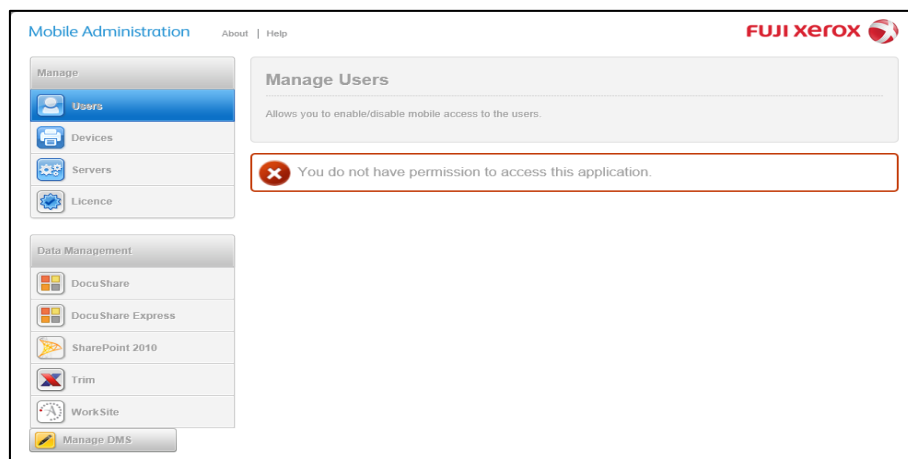


Figure 53

Solution: This error message is displayed for users who have not been assigned with the administrator's privileges. Please contact the administrator of the application.

Problem 2: *Display of contents on the application page is distorted. What should I do?*

Solution: Change your browser settings to **Compatibility View** mode. The application is compatible with the following browsers:

- Mozilla Firefox 30.0
- Google Chrome 35.0.1916.153
- Safari 7.0.4 for OS X and Safari 5.1.7 for Microsoft Windows
- Internet Explorer 10 and 11

Problem 3: *I am not able to access the online help of the application. What should I do?*

Solution:

Browse the **web.config** file (from the path <Installation Directory>\Fuji Xerox Australia\Mobile Print for Business\Admin>) for the Mobile Print for Business application in the installation directory and open the file with notepad. Look for the <appSettings> section and ensure that the *RoboHelpURL* value is /MobilePrintforBusiness/Help/Overview.htm. You can then access the online help of the application. (Refer to Figure 52.)

Also ensure that the hostname of the Mobile Print for Business server is added as an exception in the browser settings if you have proxy settings enabled for your Internet connection.

Problem 4: While installing the application, the following error screen is displayed. What should I do?

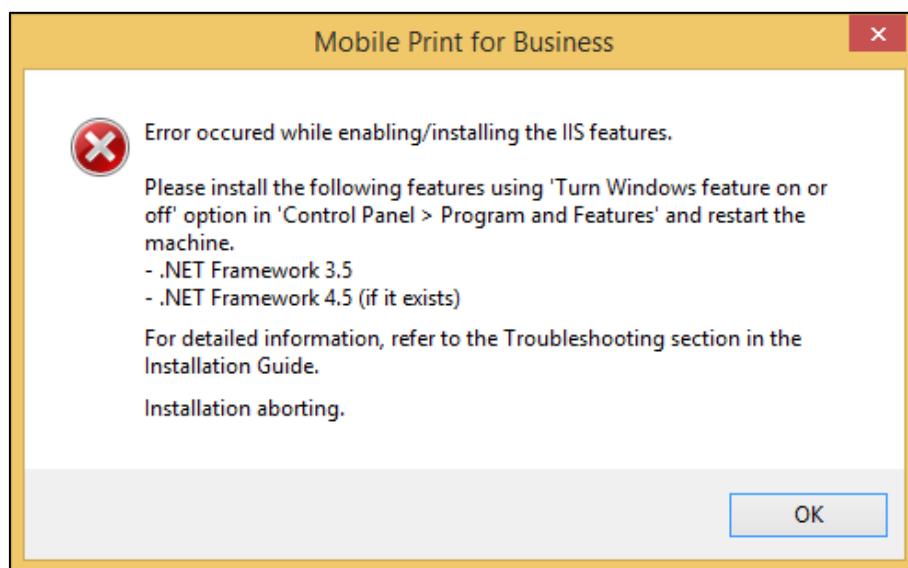


Figure 54

Solution: Install the .NET Framework feature manually. Refer to the appropriate screenshot suiting to your environment:

For Windows Server 2008 and 2008 R2:

1. Navigate to **Start > Server Manager > Add Roles and Features**.

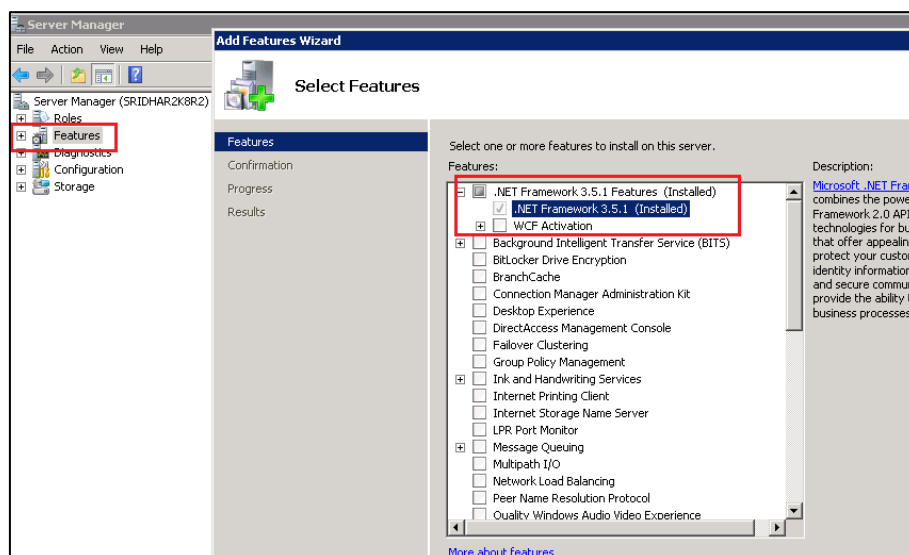


Figure 55

For Windows Server 2012 and 2012 R2:

1. Navigate to **Start > Server Manager > Add Roles and Features**.

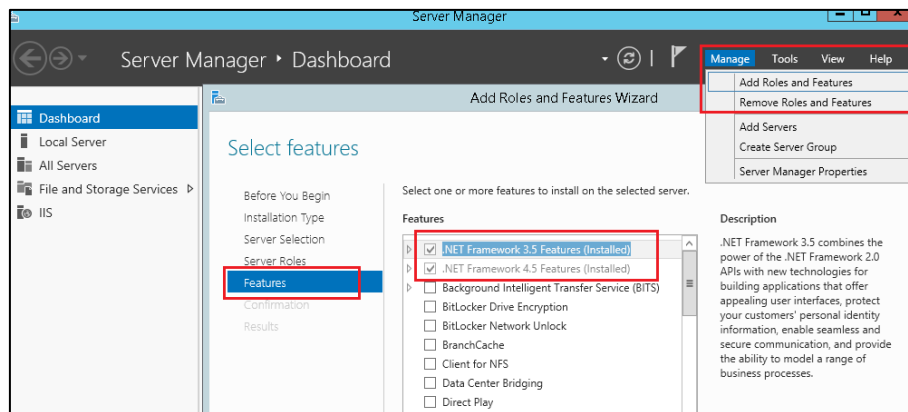


Figure 56

For Windows 7:

1. Navigate to **Start > Control Panel > Programs and Features**.

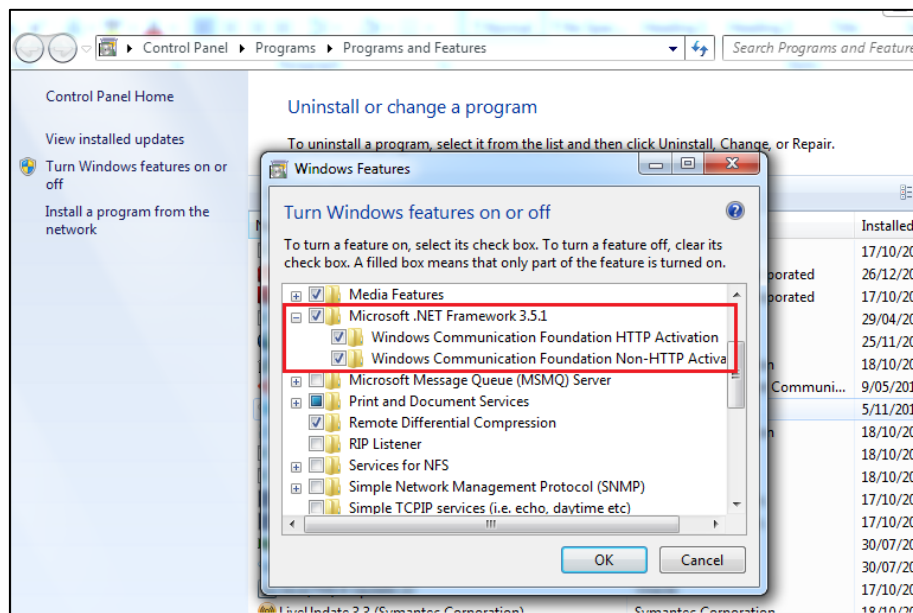


Figure 57

For Windows 8 and Windows 8.1:

1. Navigate to **Start > Control Panel > Programs and Features**.

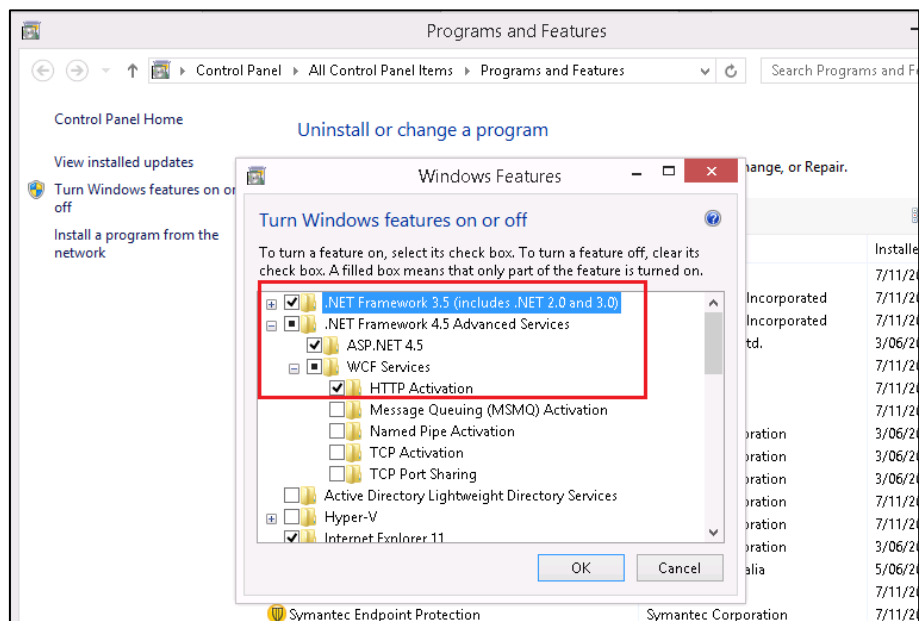


Figure 58

Problem 5: While browsing the URL to access the application, the following screen is displayed. What should I do?

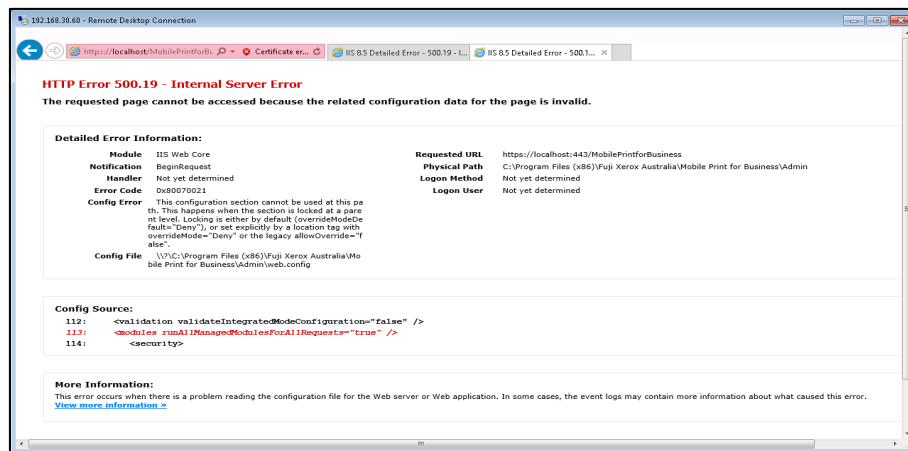


Figure 59

Solution: Ensure that the .NET Framework 3.5 feature is enabled on your machine. For Windows Server 2012, 2012 R2, Windows 8 and 8.1, you also enable the .NET Framework 4.5 feature.

For specific details, refer to the following screenshots appropriate to your environment:

For Windows 7:

1. Navigate to **Control Panel > Programs > Programs and features** and click **Turn Windows features on or off**.

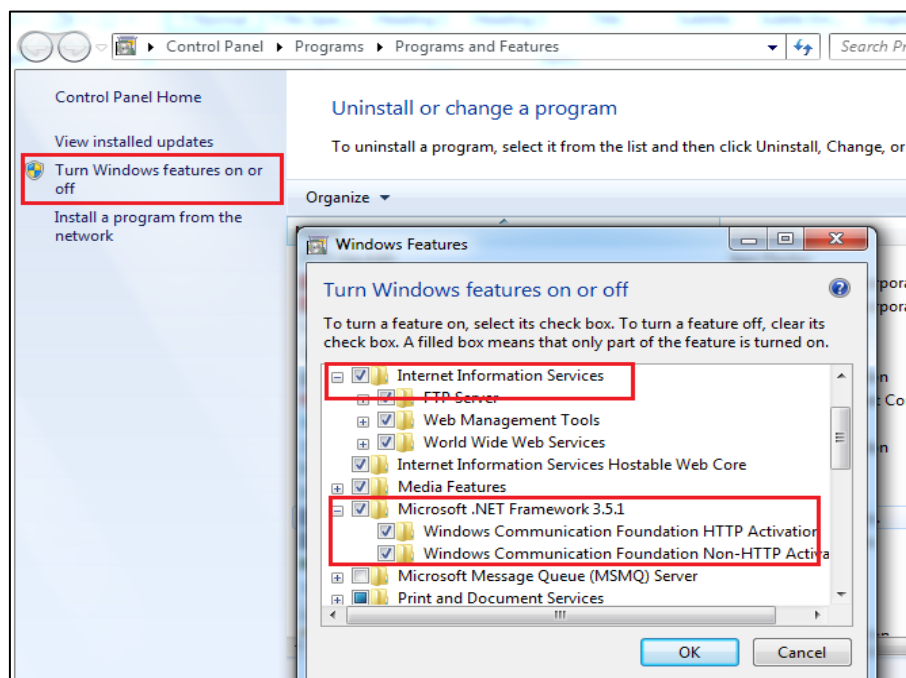


Figure 60

2. Ensure that the features selected in **Figure 60** and **Figure 61** are installed.

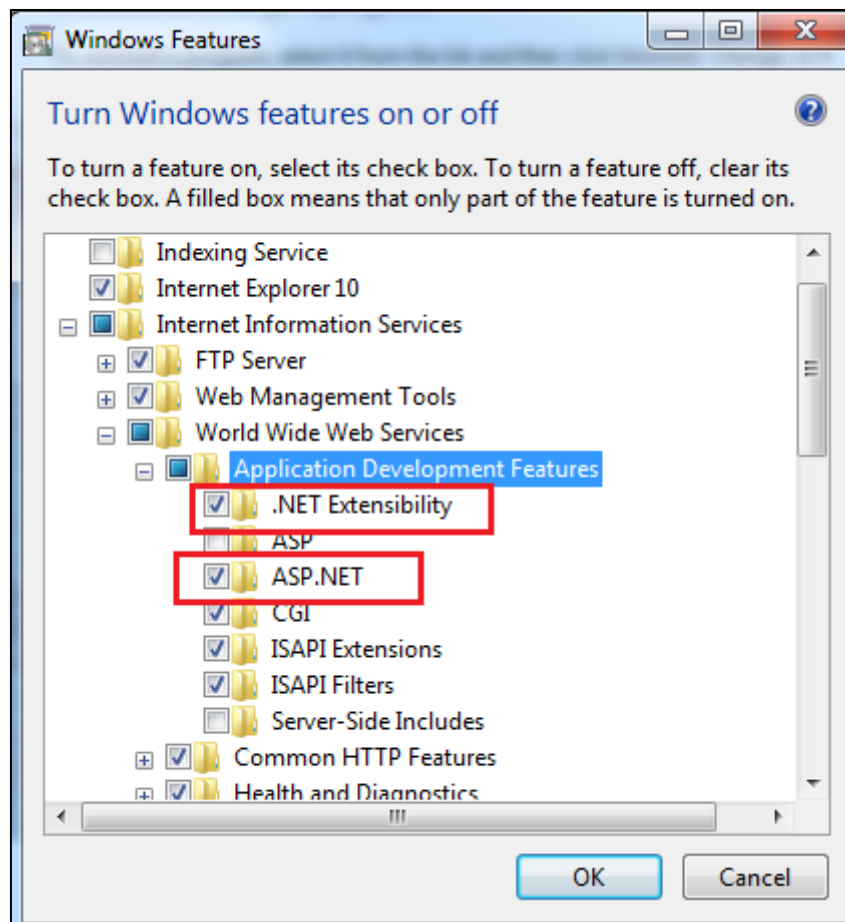


Figure 61

For Windows 8 and Windows 8.1:

1. Navigate to **Control Panel > Programs > Programs and features** and click **Turn Windows features on or off**.

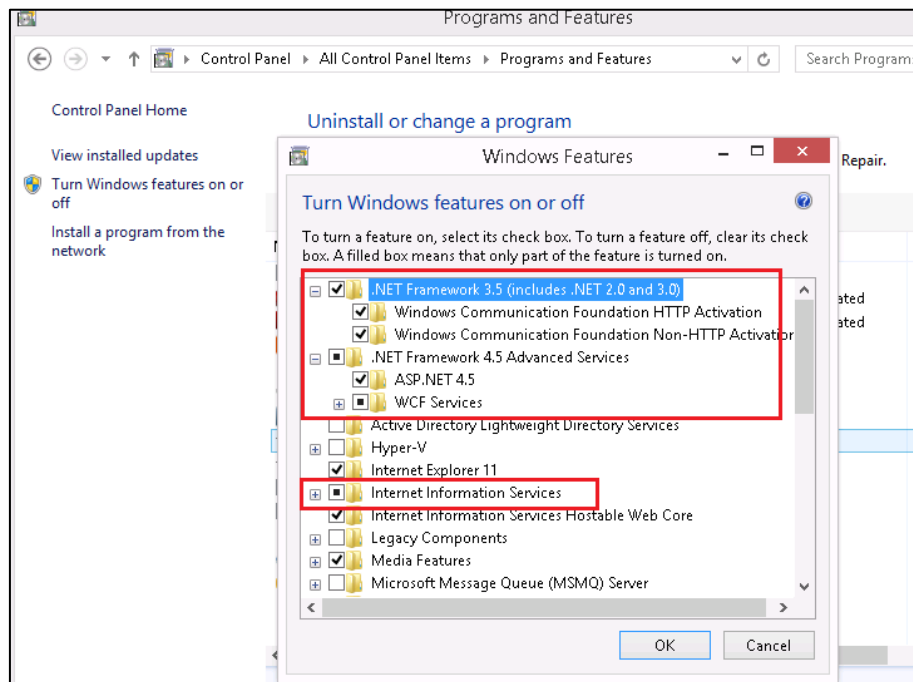


Figure 62

2. Ensure that the features selected in **Figure 62** and **Figure 63** are installed or enabled.

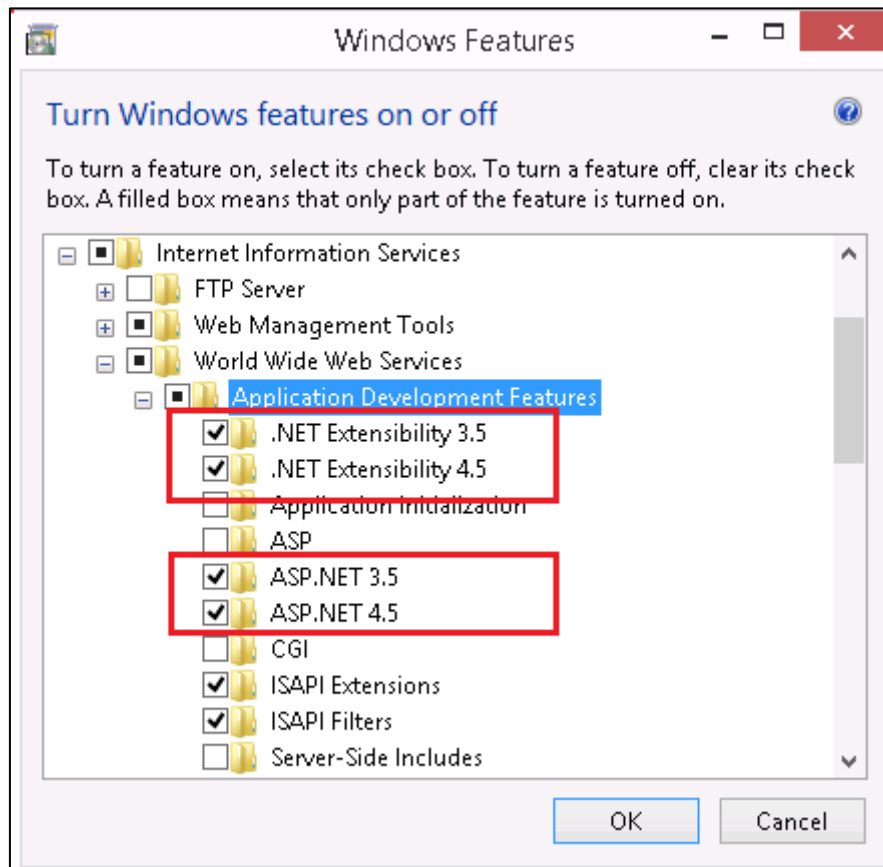


Figure 63

For Windows Server 2008 and 2008 R2:

1. Open **Server Manager**, click **Roles**, and then click **Add Role Services**.

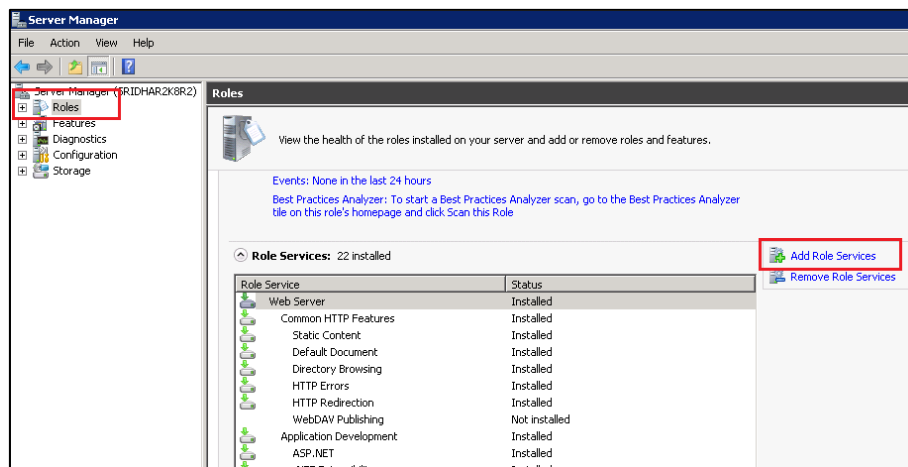


Figure 64

2. Ensure that the **features** selected on the following screenshot are installed on your machine:

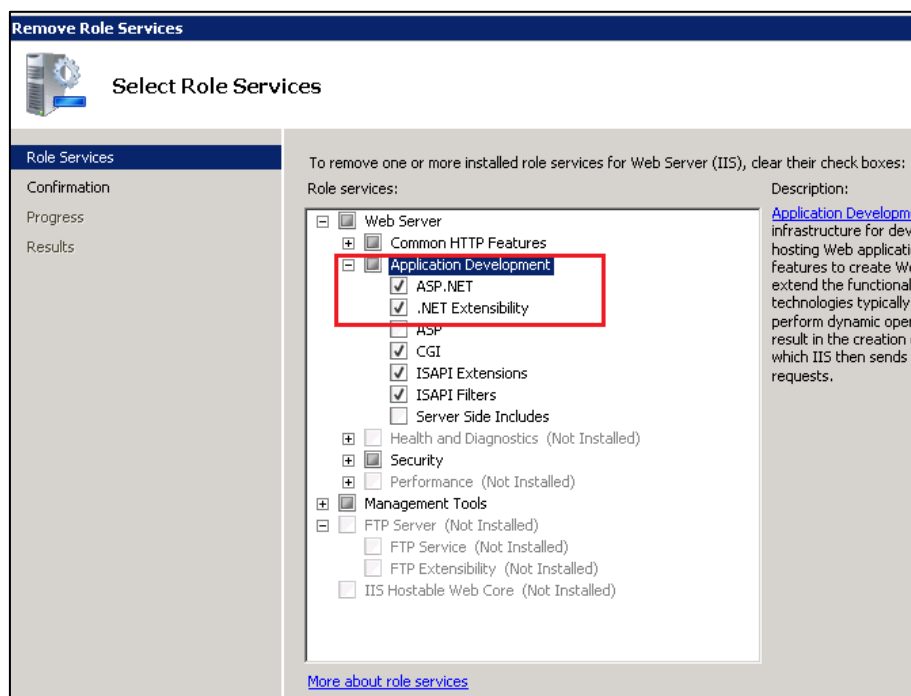


Figure 65

For Windows Server 2012 and 2012 R2:

1. Open **Server Manager**, click **Manage** and then click **Add Roles and Features**.

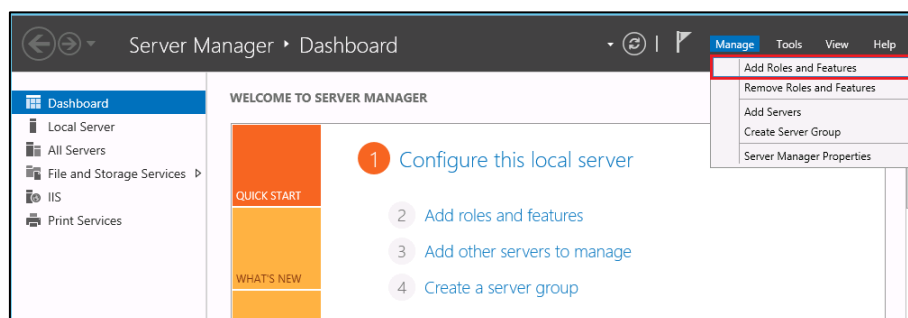


Figure 66

2. Click **Server Roles** on the left pane and ensure that the **roles** selected on the following screenshot are installed:

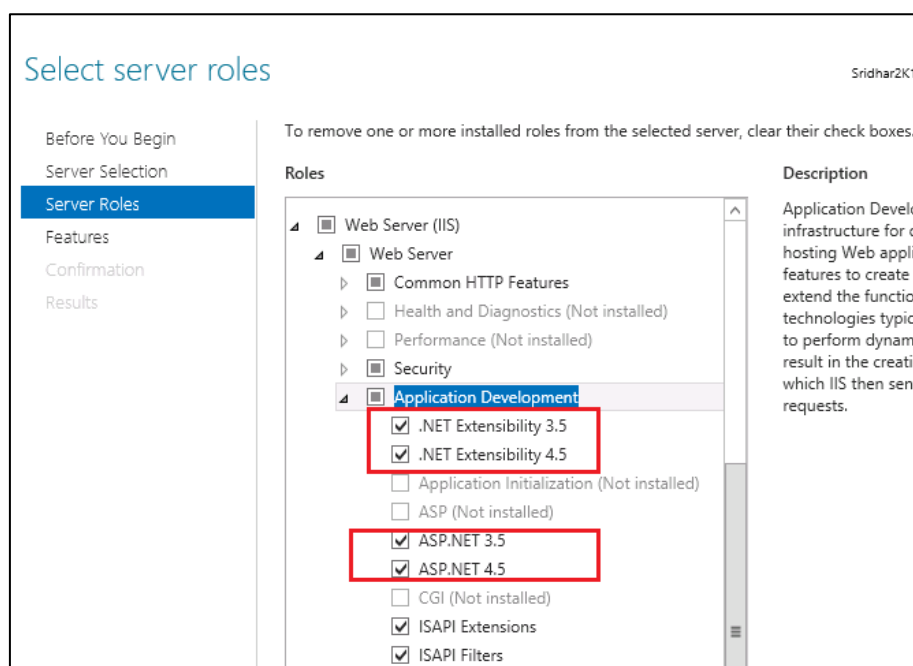


Figure 67

3. Click **Features** on the left pane and ensure that the **features** selected on the following screenshot are installed:

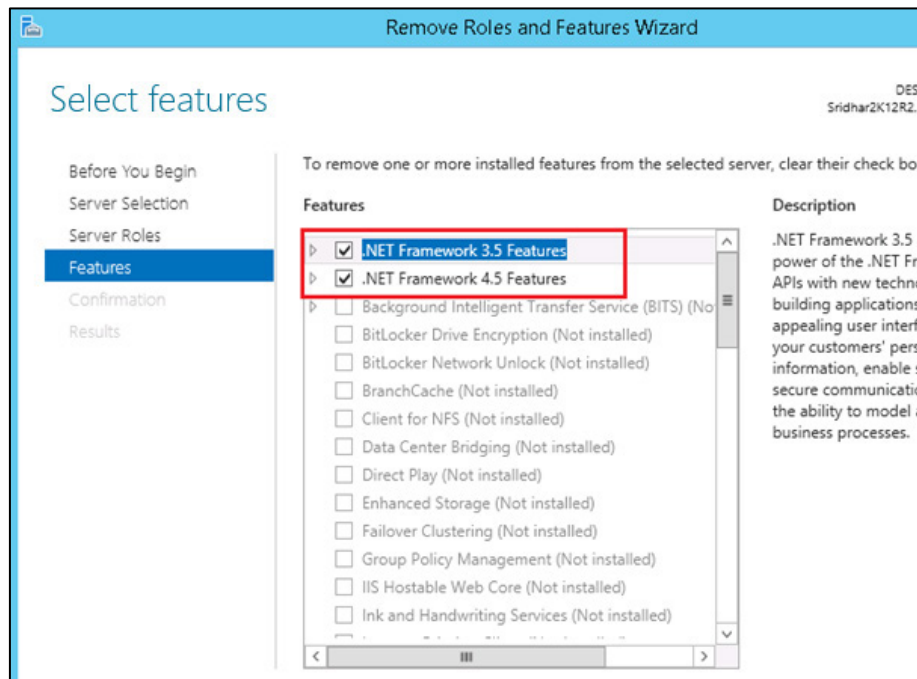


Figure 68

Appendix A – How to Get the Application Pool Identity in Windows Server

The following procedure to get the application pool identity is applicable for Windows Server 2008, 2008 R2, 2012, 2012 R2, Windows 7, Windows 8 and Windows 8.1.

1. Type *inetmgr* in **Run** prompt and click **OK**.

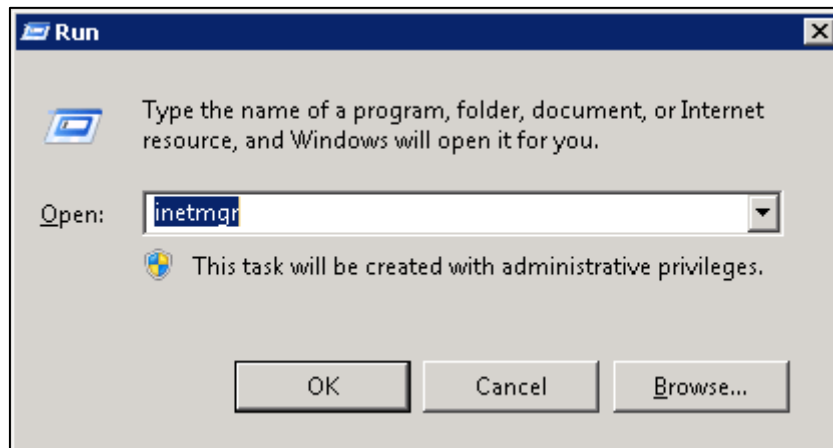


Figure 69

The following screen is displayed:

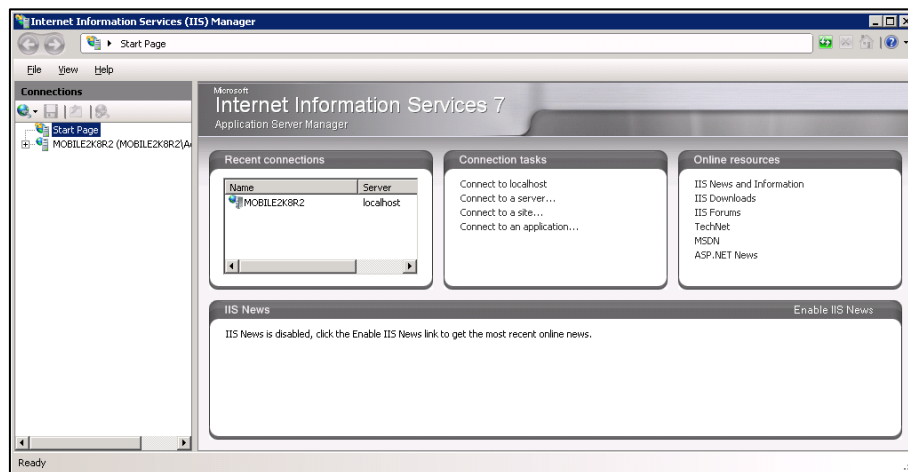


Figure 70

2. Expand the node under **Connections** section in the left pane as displayed in the screenshot below:

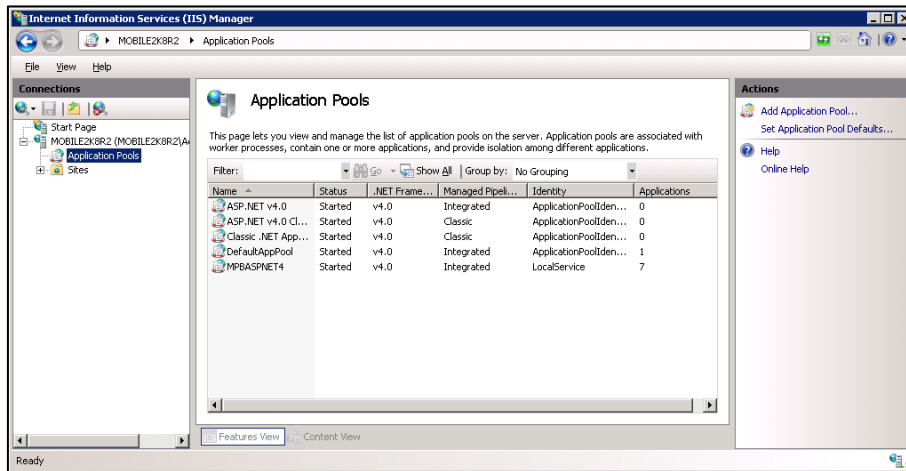


Figure 71

3. Select the **MPBASPNET4** application pool from the list and click **Advanced Settings...** on the right pane.

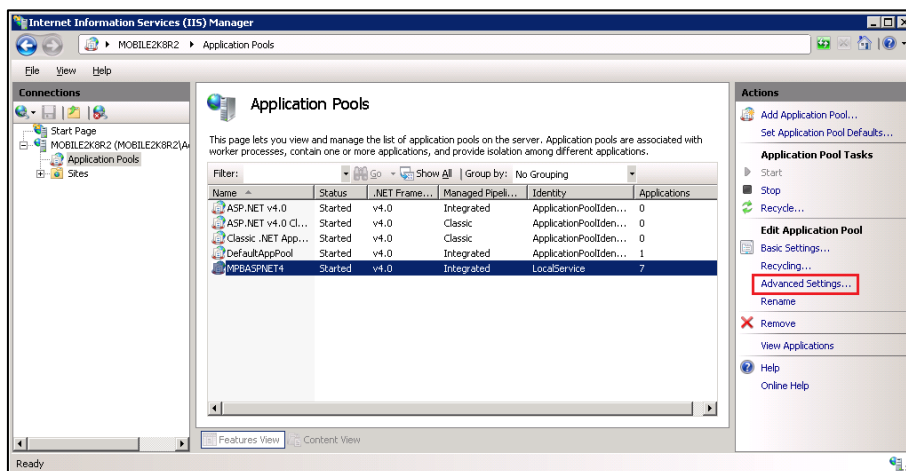


Figure 72

The following screen is displayed:

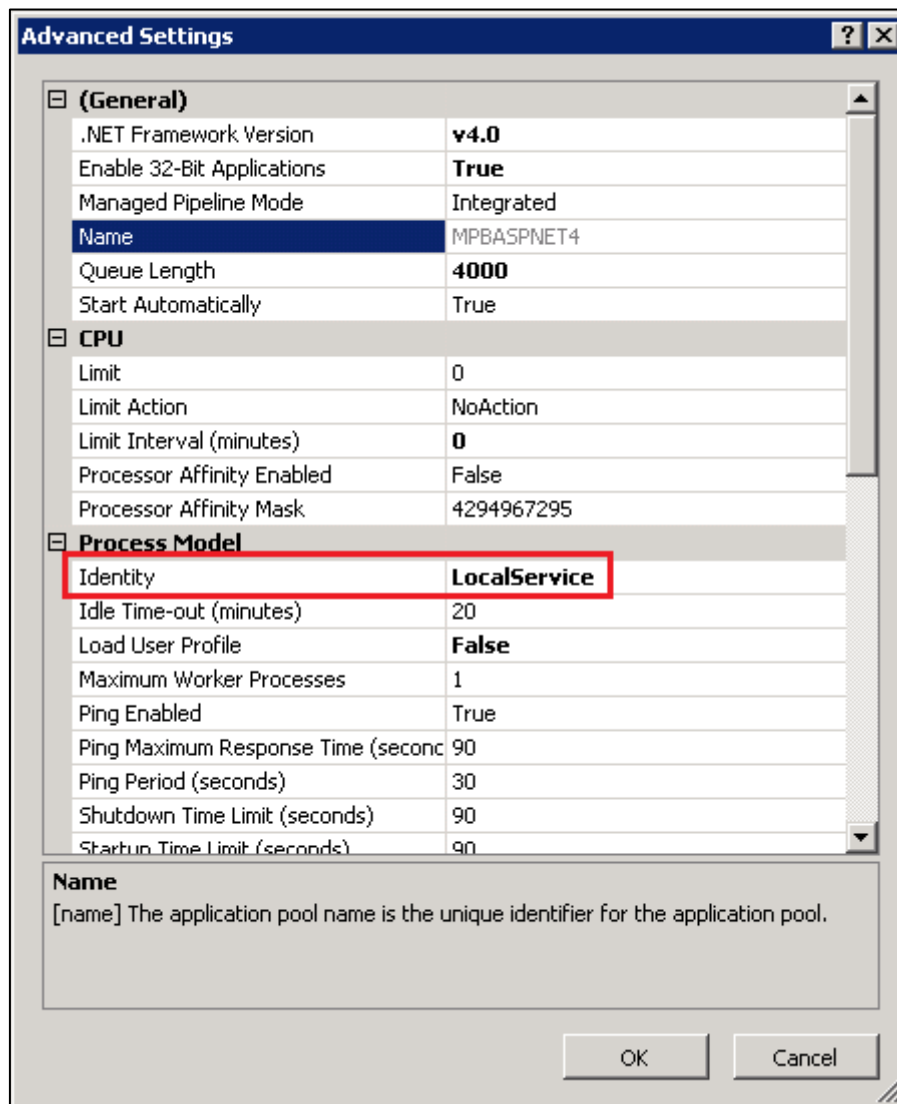


Figure 73

You can find the identity details under Process Model as highlighted in the above screenshot.

Appendix B – How to Export SSL Certificate in Windows Server

The following procedure to export SSL certificates is applicable for Windows Server 2008, 2008 R2, 2012, 2012 R2, Windows 7, Windows 8 and Windows 8.1.

1. Click **Start > Run** and type **inetmgr**.
The IIS Manager opens.
2. Navigate to the level you want to manage.
3. In **Features View**, double-click **Server Certificates**.
4. Select a certificate and click **Export** from the **Actions** pane.
5. In the **Export Certificate** dialog box, do the following:
 - a. Type a file name in the **Export to** box or click the browse button (...) to navigate to the name of a file in which to store the certificate for exporting.
 - b. Type a password in the **Password** box if you want to associate a password with the exported certificate.
 - c. Retype the password in the **Confirm password** box and then click **OK**.

Appendix C – How to Verify If the PowerShell Feature is Enabled or Installed

The following sections provide information about how to verify if the PowerShell feature is enabled or installed on the machine.

For Windows 7, Windows 8 and Windows 8.1

1. Open **Run** prompt, type **appwiz.cpl** and click **OK**.

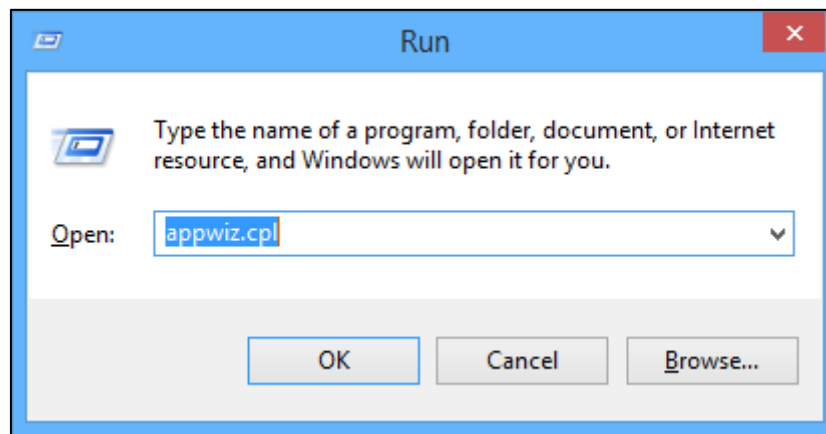


Figure 74

The following screen is displayed:

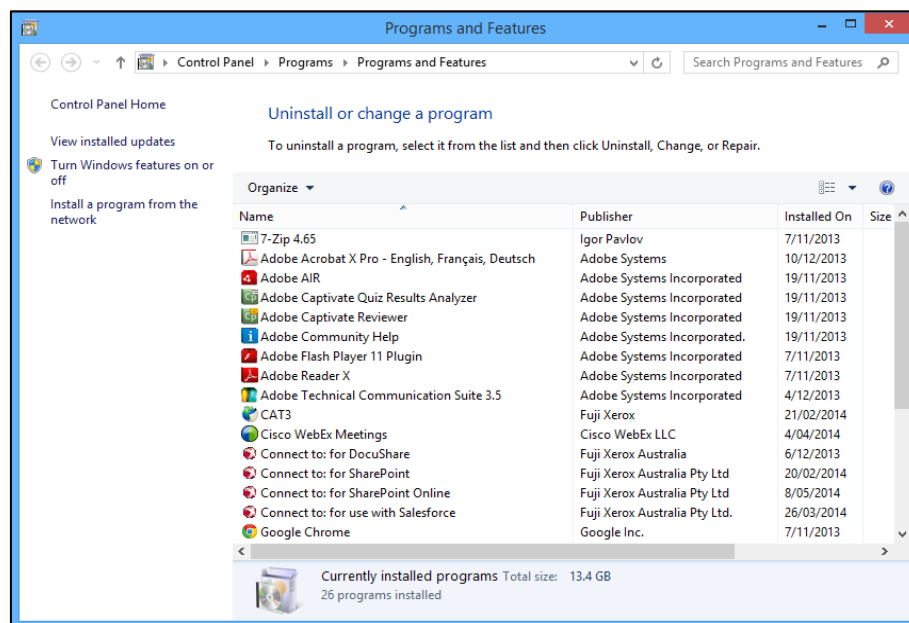


Figure 75

2. Click **Turn Windows features on or off** on the top left pane.

The *Windows Features* screen is displayed:

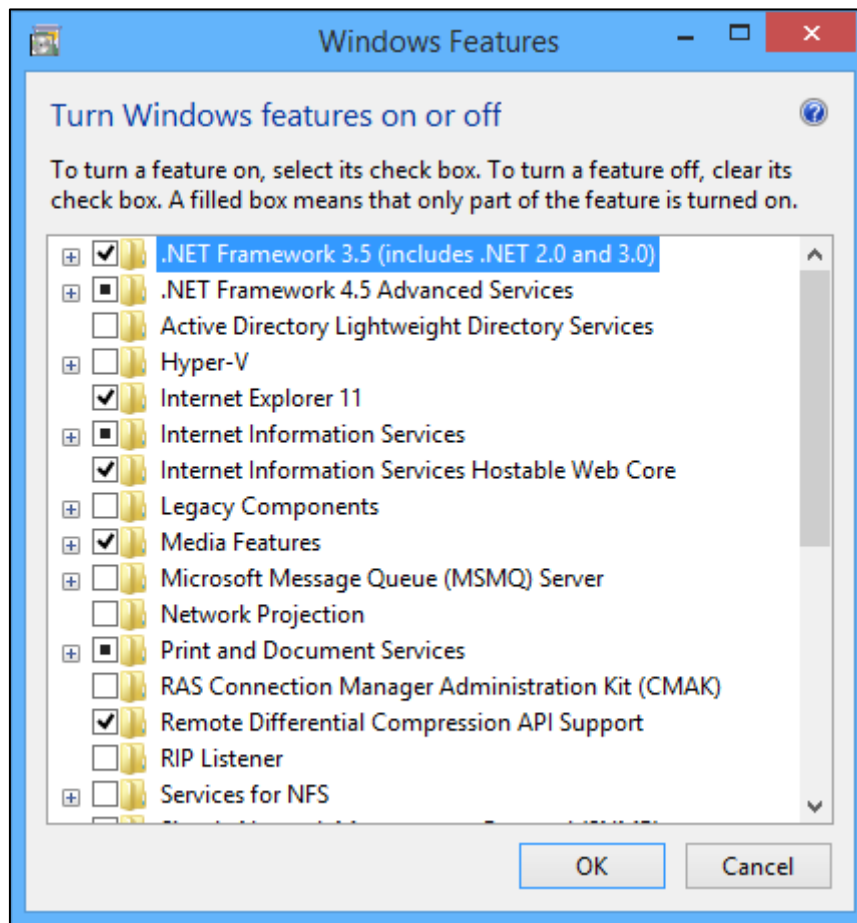


Figure 76

3. Scroll down the list of features and ensure that the **Windows PowerShell (2.0)** feature is selected:

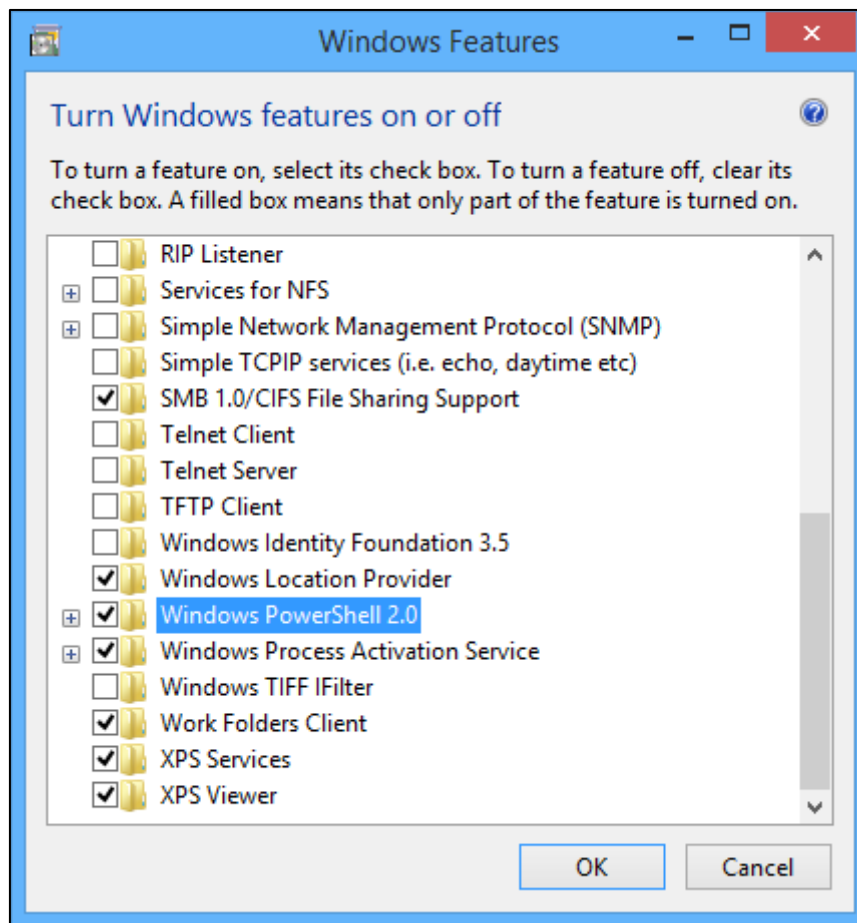


Figure 77

For Windows Server 2008 and 2008 R2

1. Click **Start**, point to **Administrative Tools** and click **Server Manager**.

The following screen is displayed:

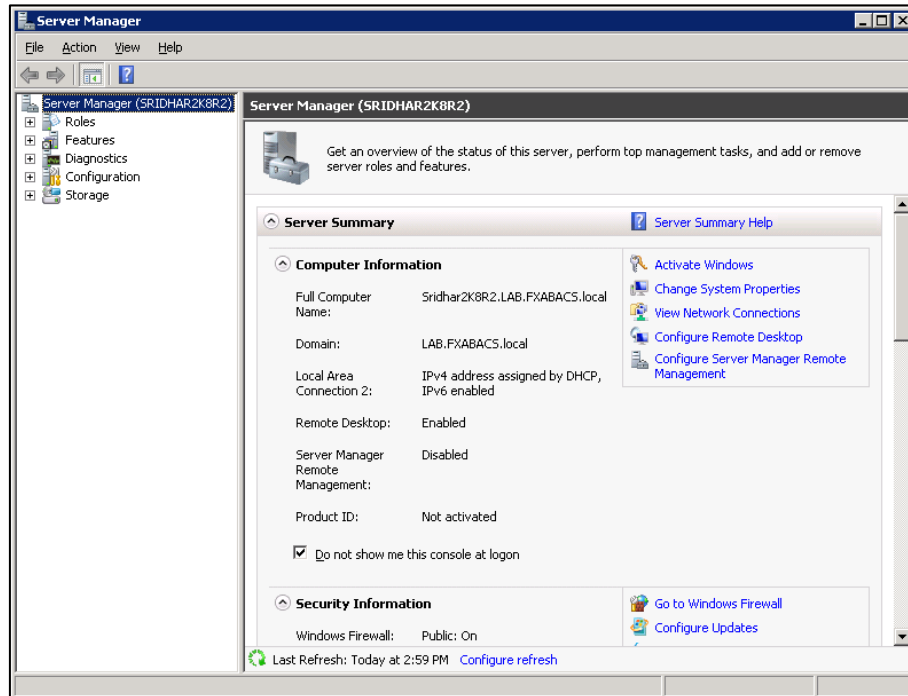


Figure 78

2. Click **Features** on the left pane.

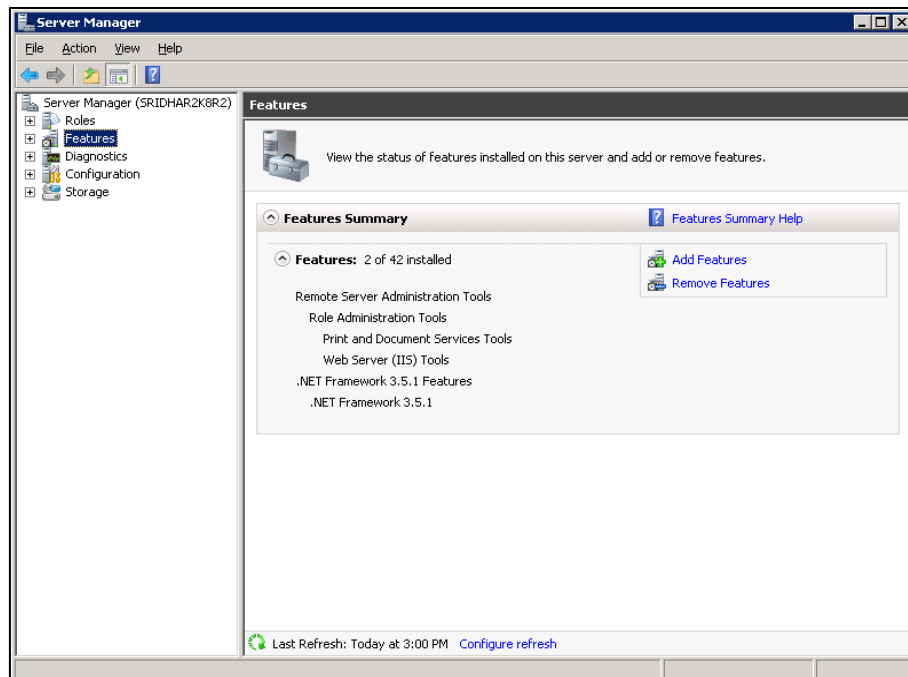


Figure 79

3. Click **Add Features**.
The *Add Features Wizard* screen is displayed.

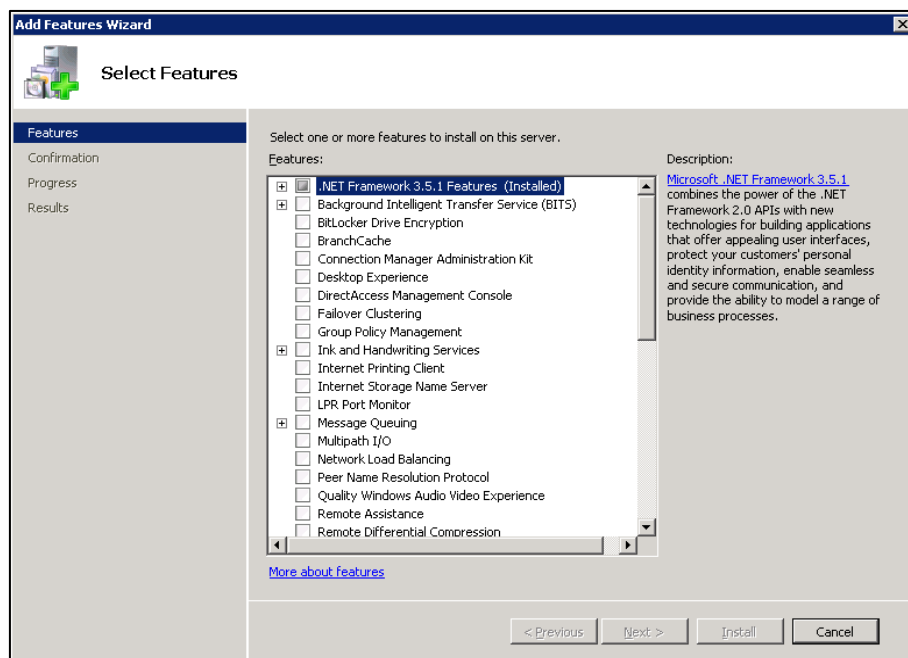


Figure 80

4. Scroll down the list of features and ensure that the **Windows PowerShell Integrated Scripting Environment (ISE)** is selected (as shown in the following screenshot).

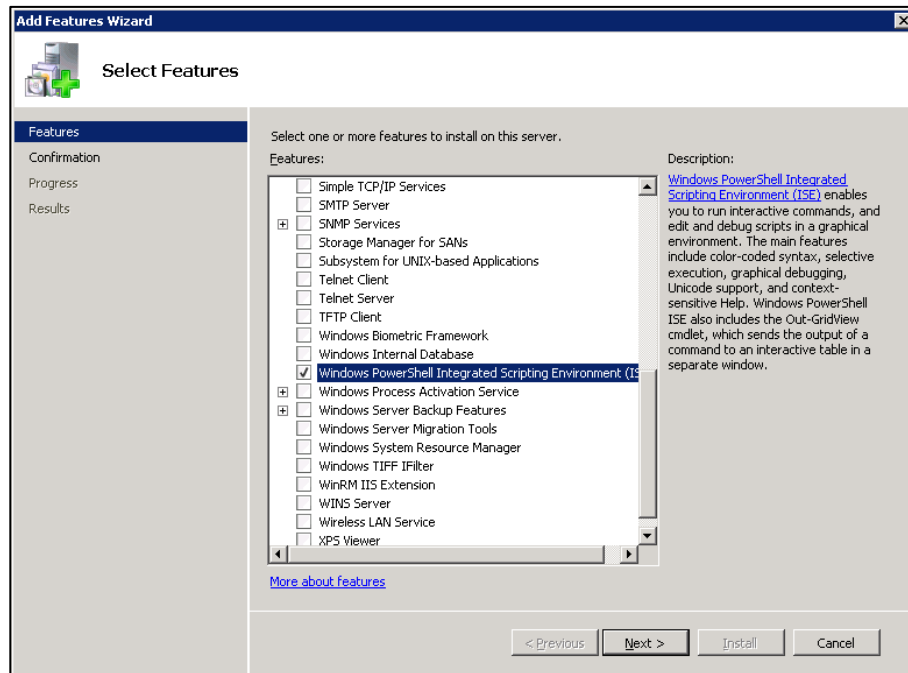


Figure 81

For Windows Server 2012 and 2012 R2

1. From **Start** page, click **Server Manager**.

The following screen is displayed:

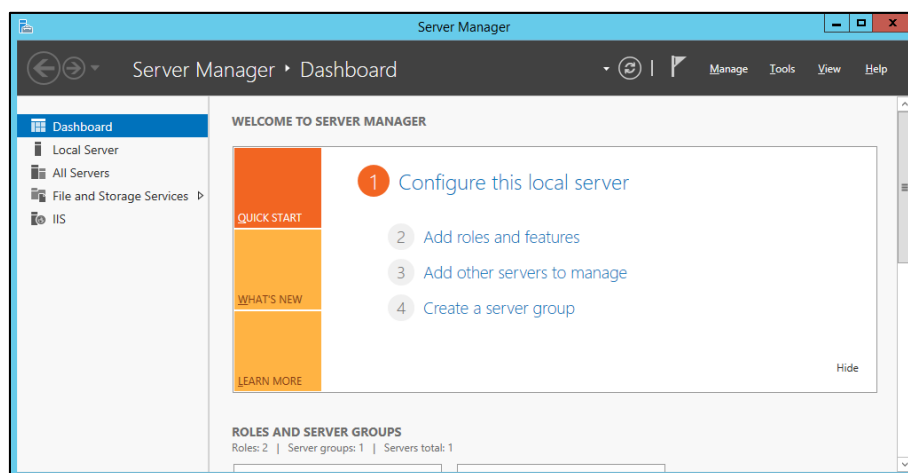


Figure 82

2. Click **Add roles and features**.

The following screen is displayed:

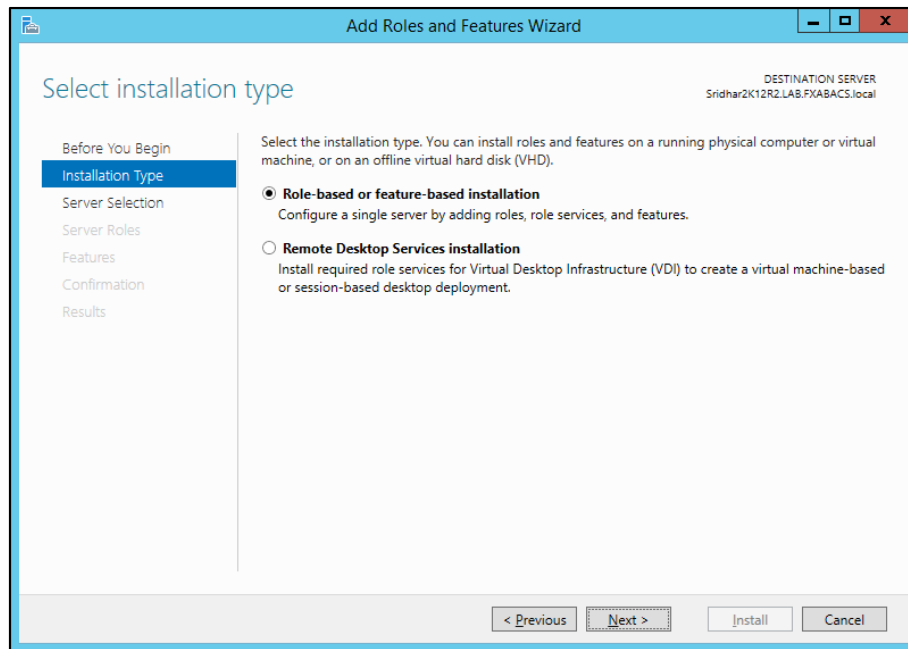


Figure 83

3. Click **Next**.

The following screen is displayed:

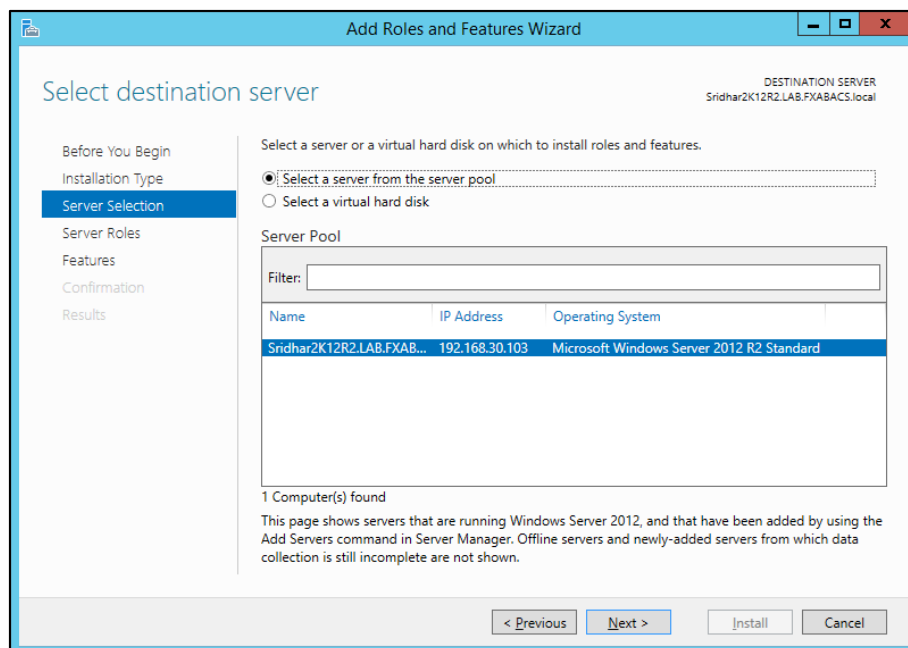


Figure 84

4. Click **Features** on the left side.
The following screen is displayed:

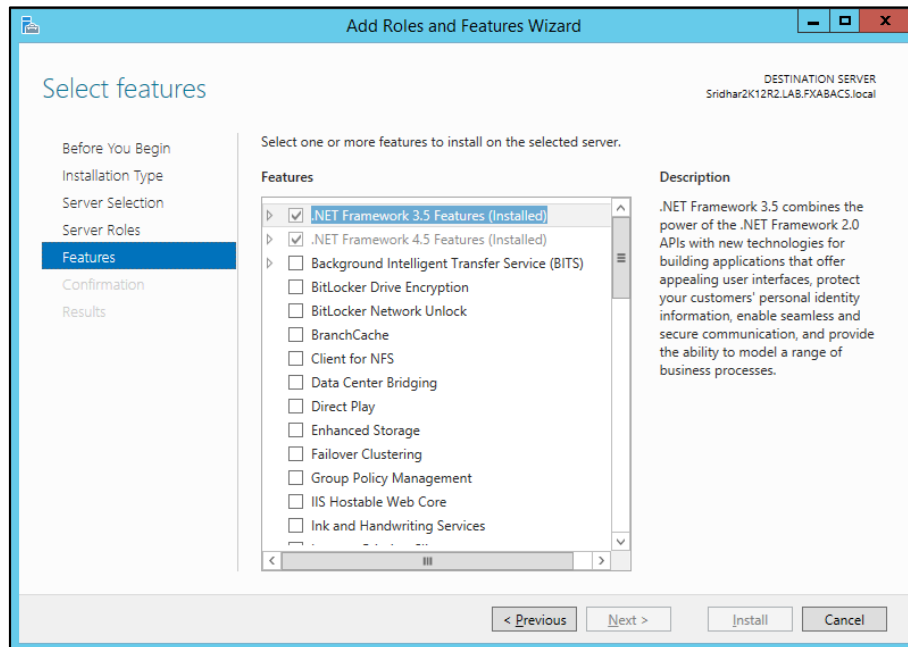


Figure 85

5. Scroll down the list of features and ensure that the **Windows PowerShell** feature is selected.

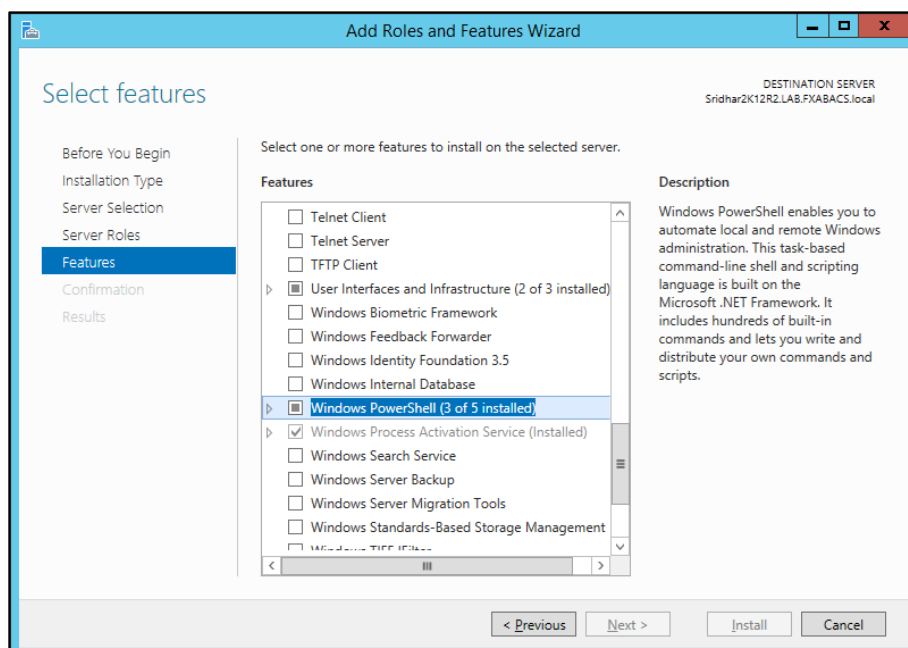


Figure 86

Appendix D – How to Configure A User Account to Have ‘Logon as a service’ Permission

To configure a user account to have *Logon as a service* permission:

1. Type ***secpol.msc*** in **Run** prompt and click **OK**.

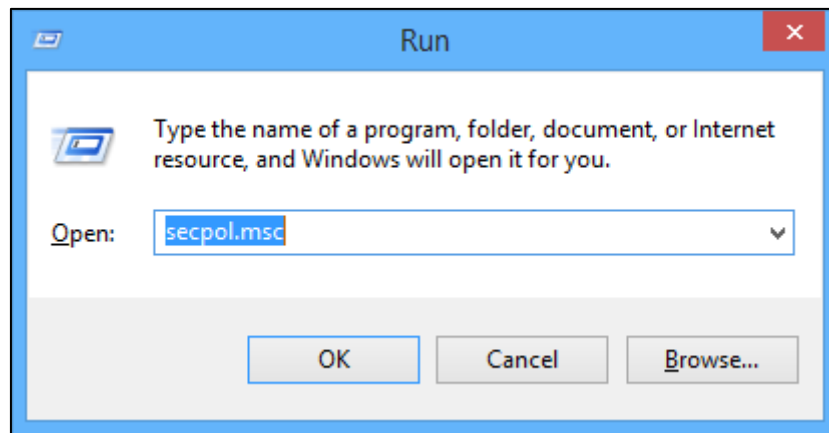


Figure 87

The following screen is displayed:

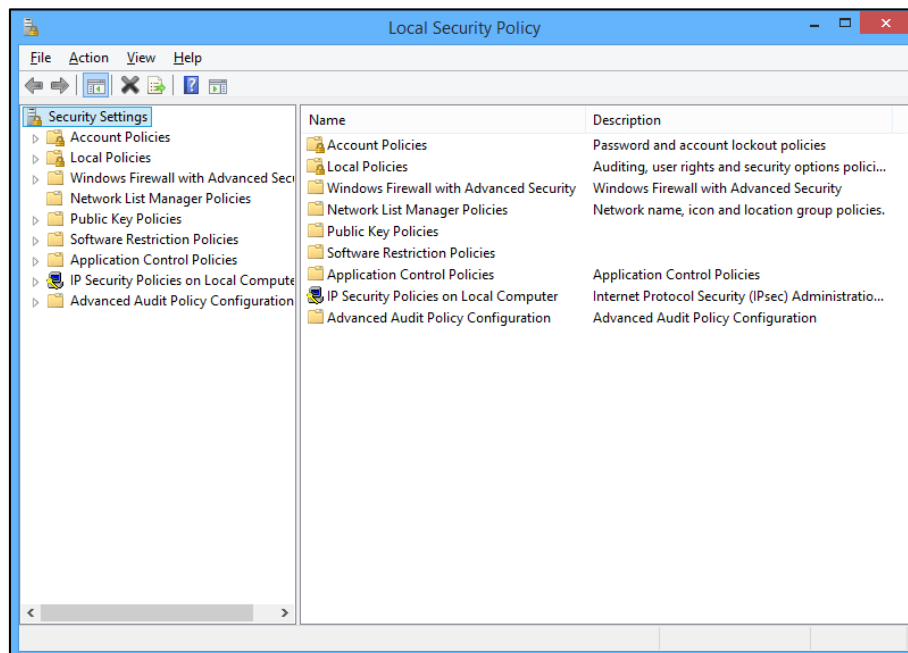


Figure 88

2. Go to **Security Settings > Local Policies > User Rights Assignment** and then double-click **Log on as a service**.

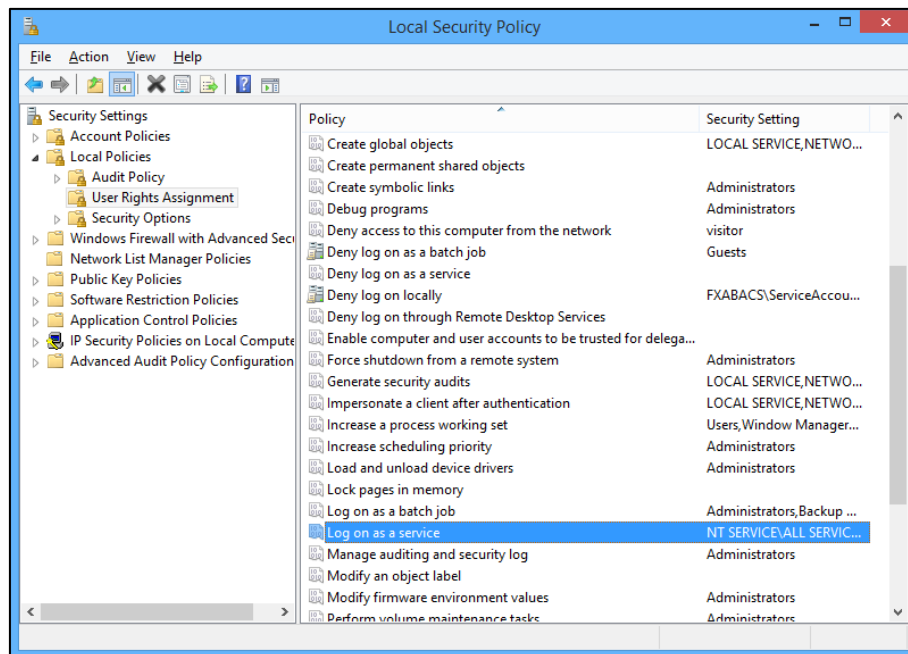


Figure 89

The *Log on as a service properties* screen is displayed.

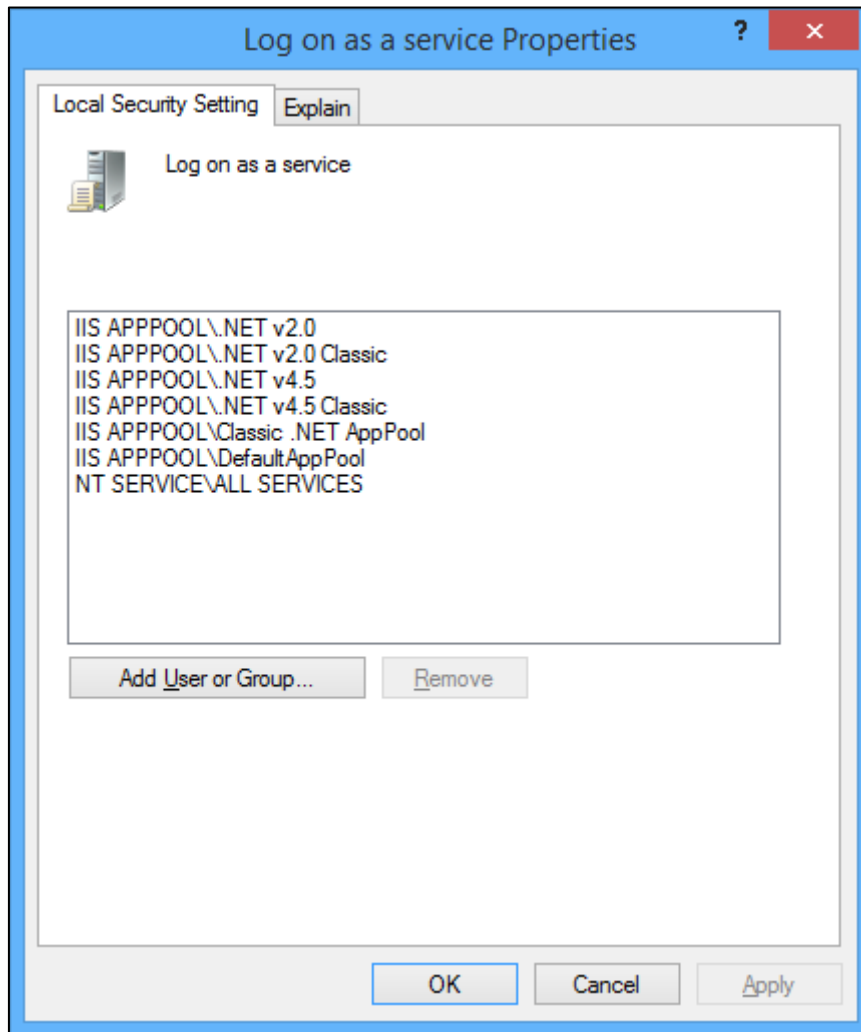


Figure 90

3. Click **Add User or Group**

The following screen is displayed:

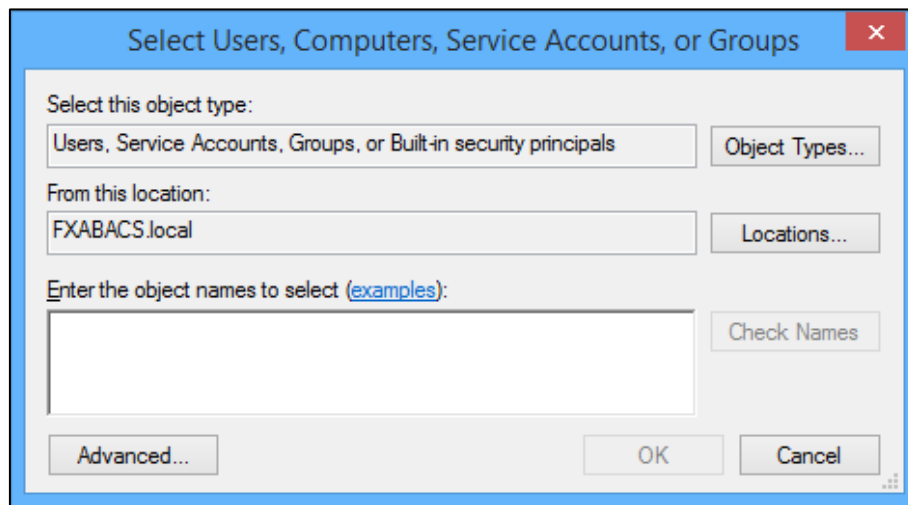


Figure 91

4. Type the desired user account name in the text box and click **Check Names**.

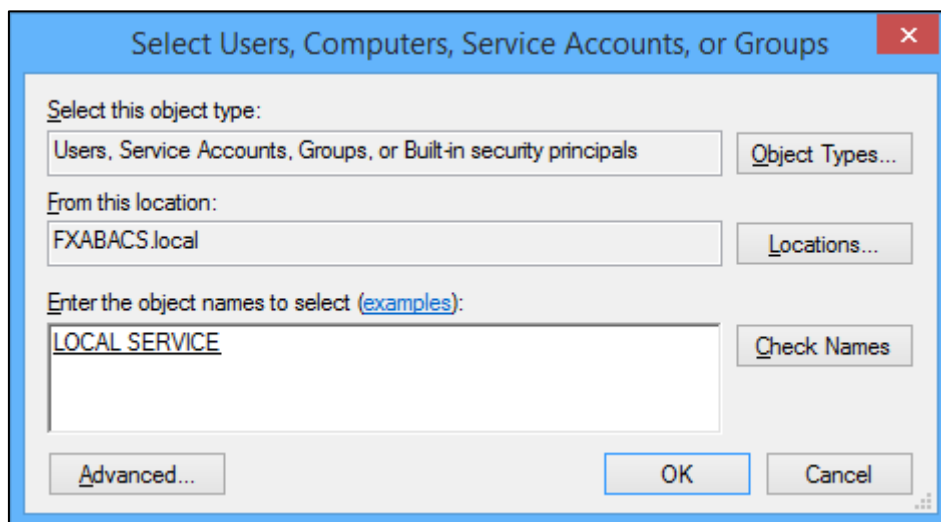


Figure 92

5. Click **OK**.

Note: Ensure that that user account has NOT been added to the **Deny log on as a service policy**.

Appendix E – How to Assign db_owner Permission on the Database of SQL Server

To assign *db_owner* permission to a user on the database of the SQL Server:

1. Type *ssms* in **Run** prompt and click **OK**.

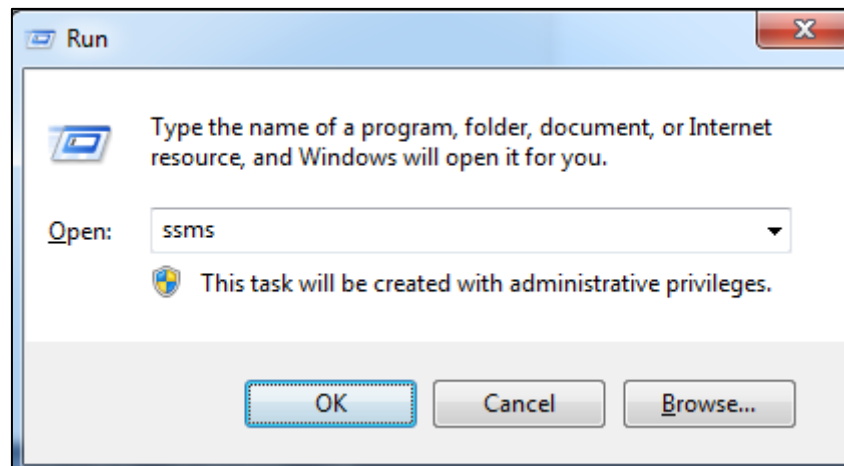


Figure 93

The *Connect to Server* screen is displayed.

2. Type valid admin credentials to connect to the SQL Server and click **Connect**.

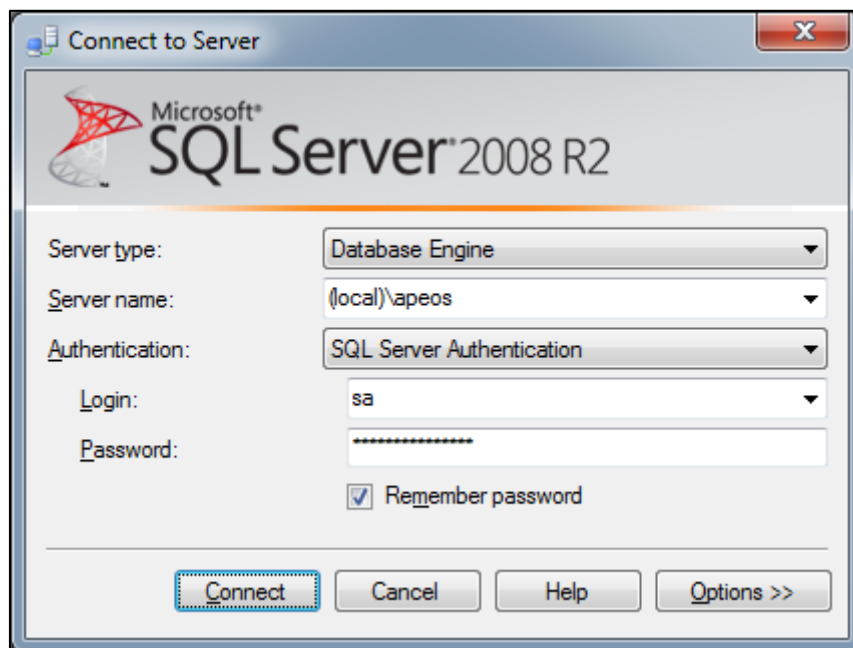


Figure 94

3. Navigate to **Databases > Security > Logins** and then click **New Login....**

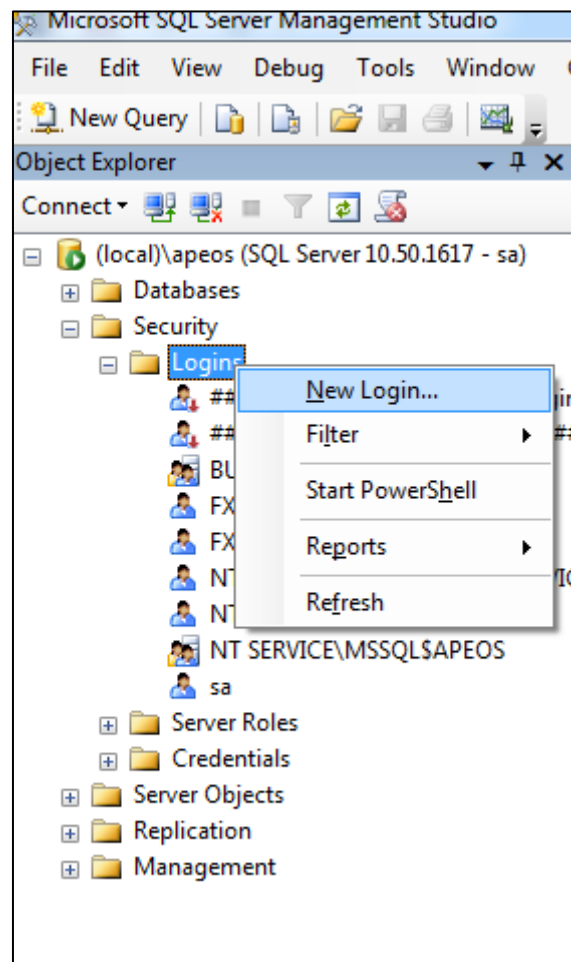


Figure 95

The following screen is displayed:

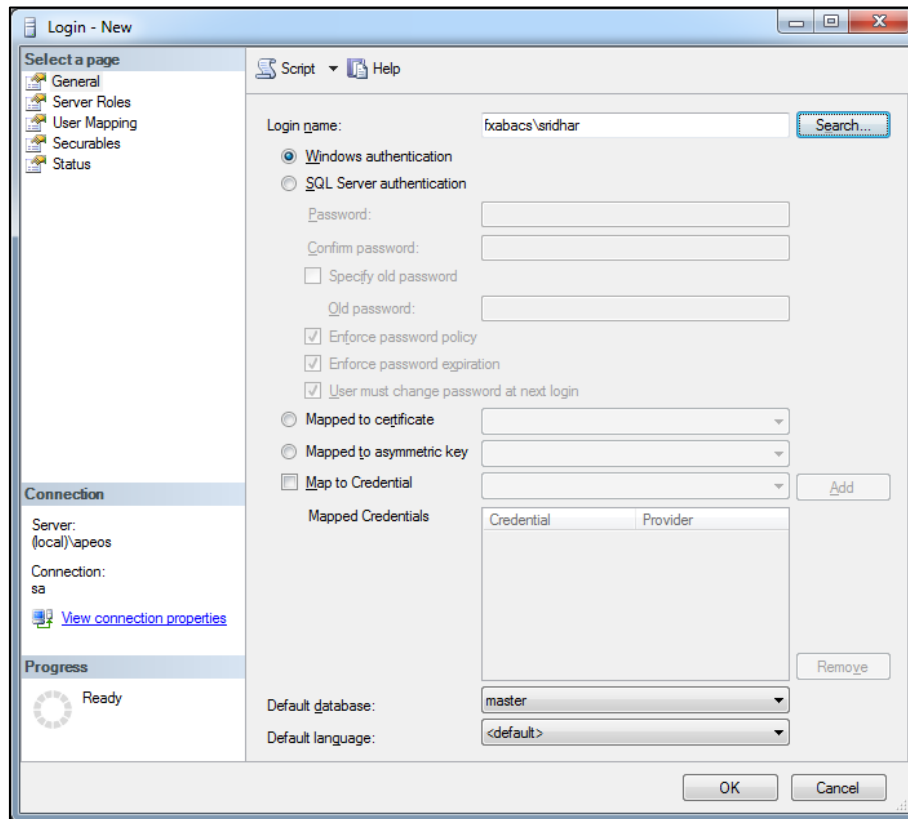


Figure 96

4. Type the desired domain or local user name with which the Mobile Print for Business application is going to be installed in the **Login name** field in the previous screen.
5. Click **Server Roles** on the left pane.

6. Select the **public** and **sysadmin** roles as displayed in the following screenshot and click **OK**:

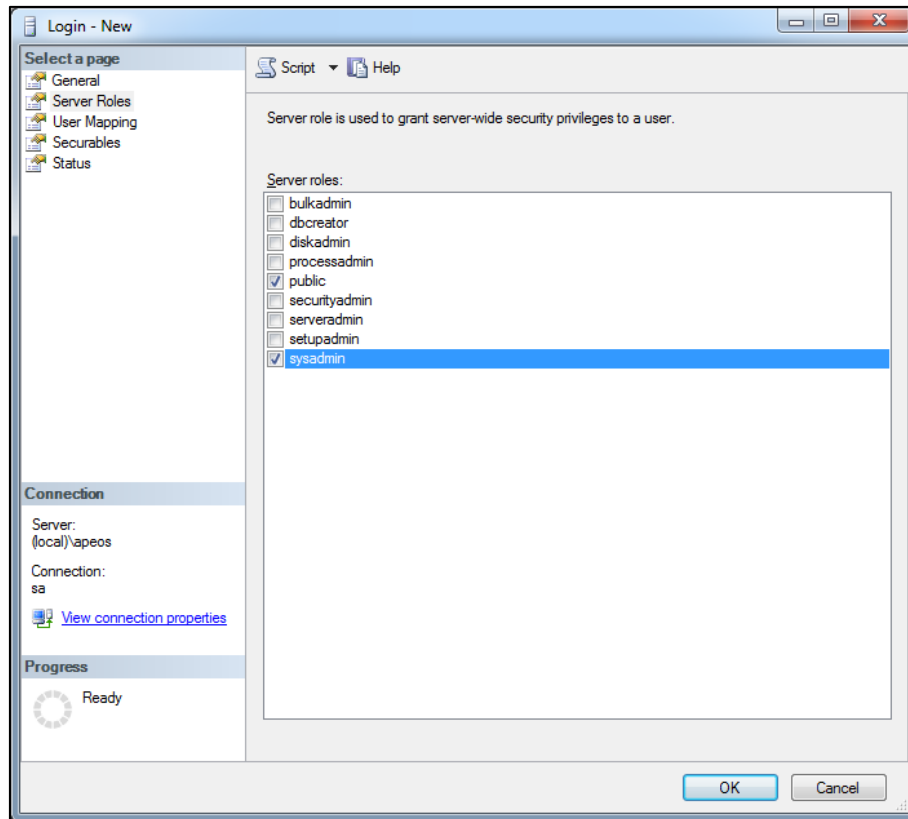


Figure 97

7. Select the desired option (<master> here) under the **Users mapped to this login** section, and **db_owner** and **public** under the **Database role membership for: <master>** section (as displayed in the following screenshot), and then click **OK**.

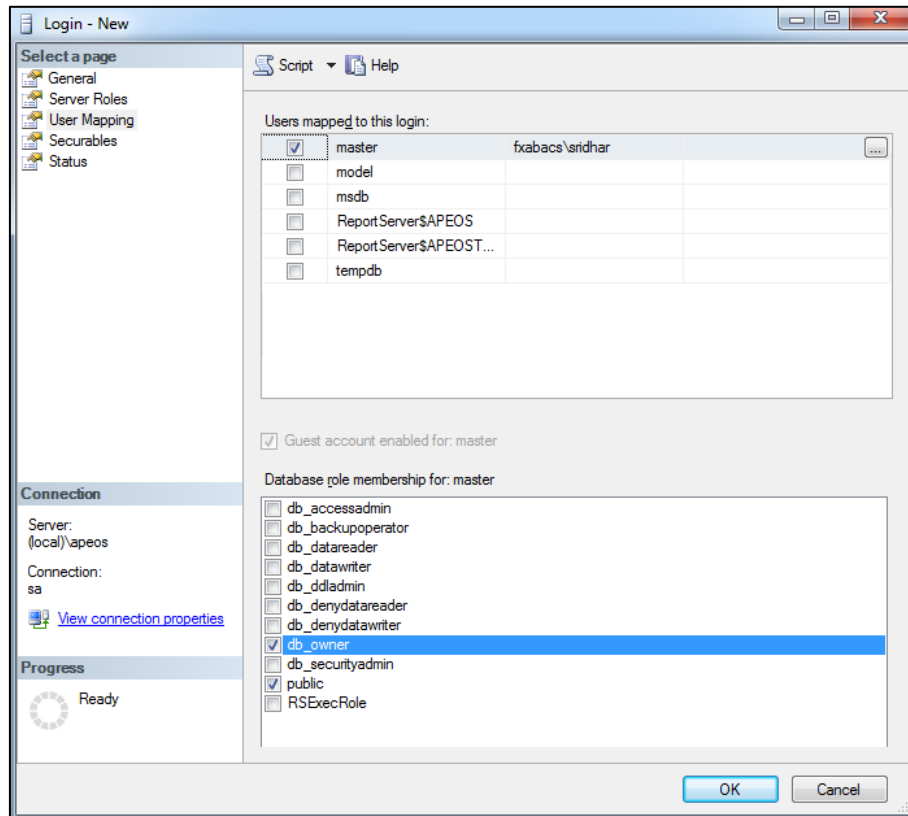


Figure 98

8. Navigate to **Databases > Security > Logins** and verify if the new user is added as a new login.

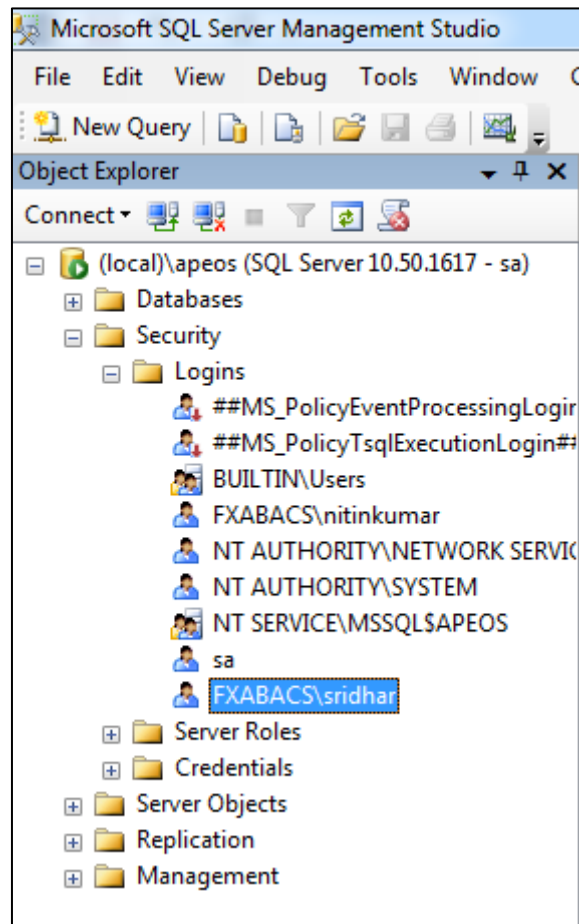


Figure 99

Appendix F – How to Add A User to the IIS_IUSRS Group

1. Type *secpol.msc* in **Run** prompt and click **OK**.

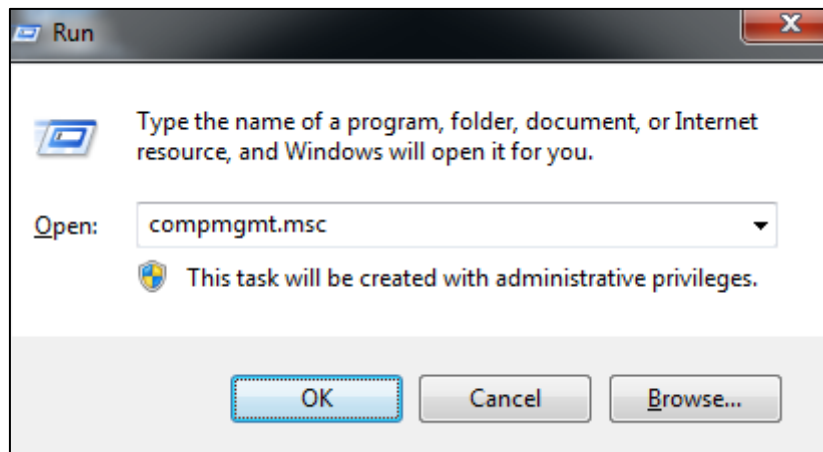


Figure 100

The *Computer Management* screen is displayed.

2. Navigate to **System Tools > Local Users and Groups > Groups** on the left pane, right-click **IIS_IUSRS** and click **Properties**.

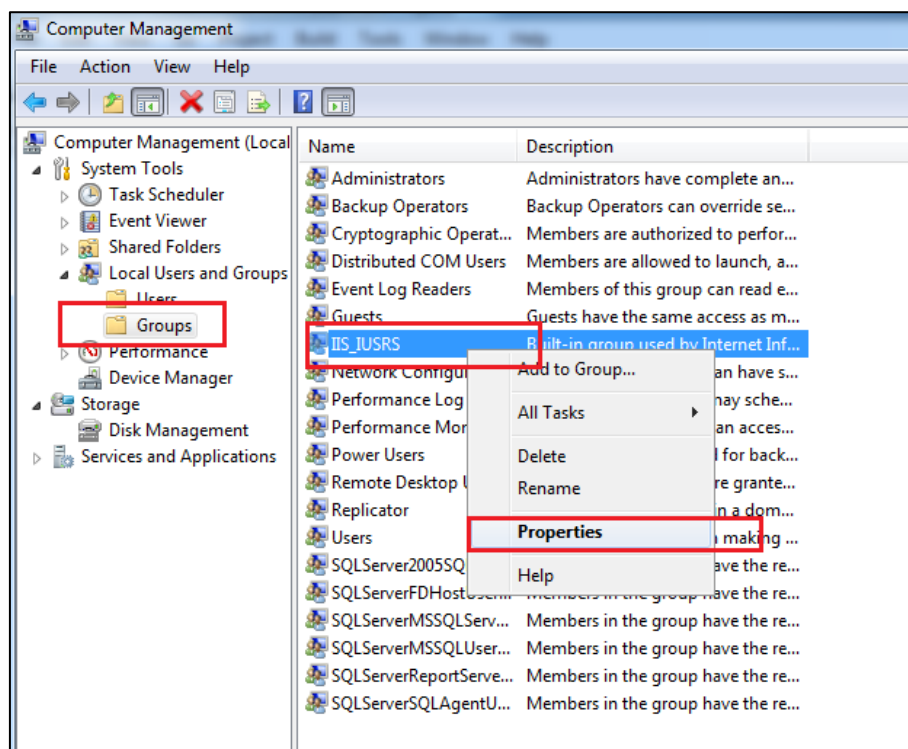


Figure 101

The following screen is displayed:

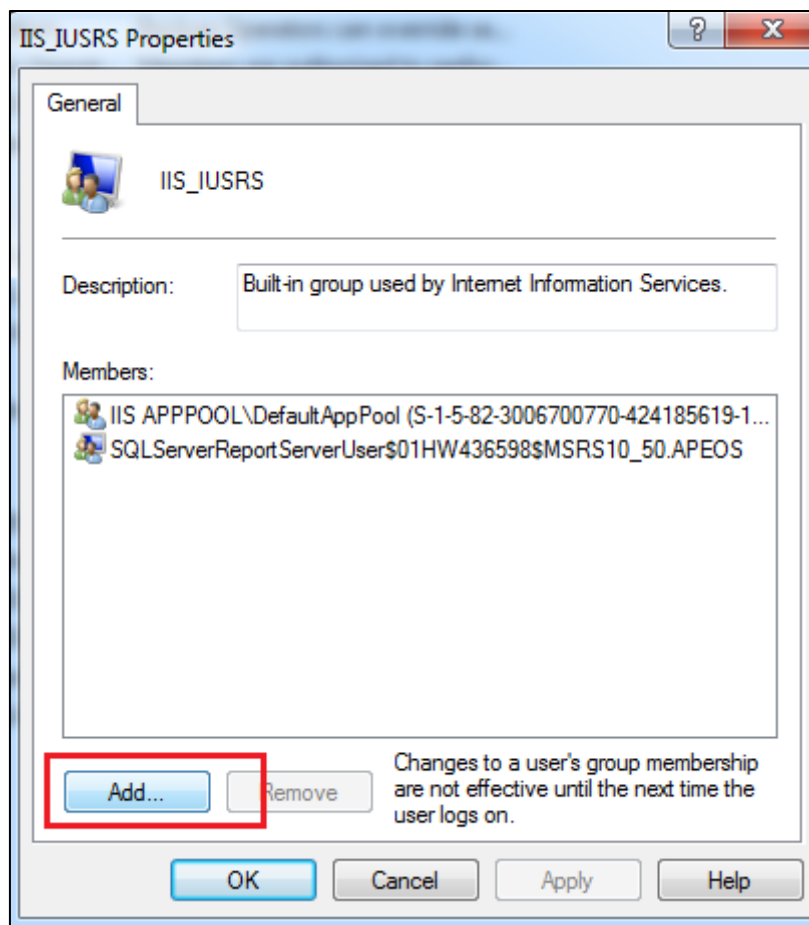


Figure 102

3. Click **Add....**

The following screen is displayed:

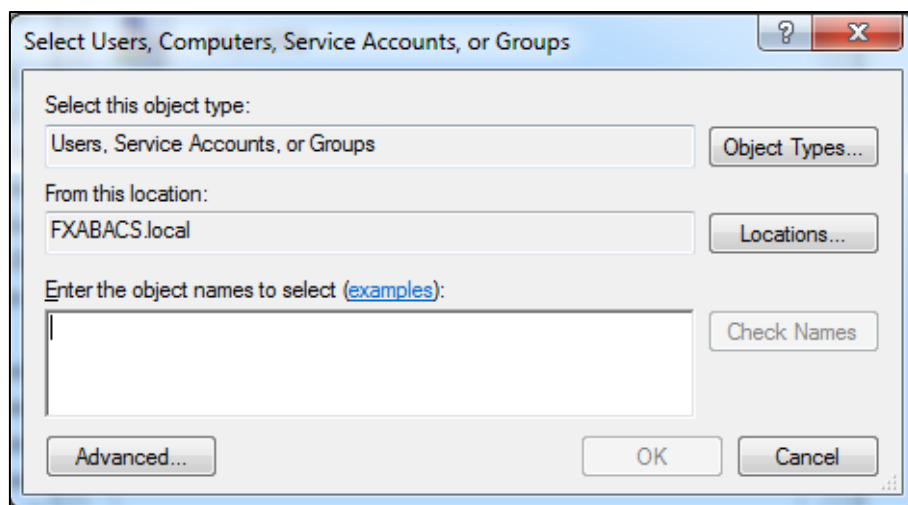


Figure 103

4. Type the desired user account name in the text box and click **Check Names**.

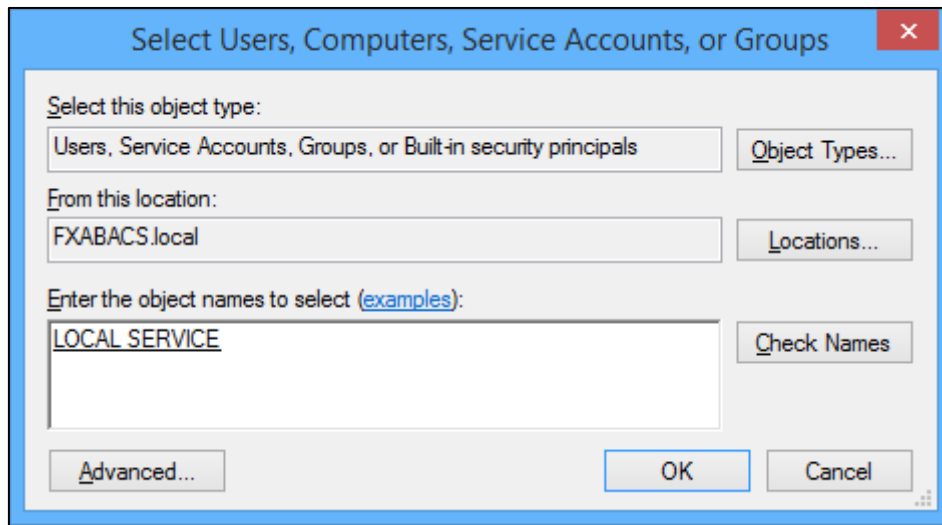


Figure 104

5. Click **OK**.