



nsi™ mobile™



NSi™ Mobile™ Installation Guide

Version 7.0



Revision History

Version	Date
1.0	October 2, 2012
2.0	September 18, 2013
2.0.1	March 6, 2014
3.0	March 11, 2015



TABLE OF CONTENTS

PREFACE5

- Purpose of this Document 5
- Version Compatibility 5
- Related Documentation 5

OVERVIEW6

PREREQUISITES7

- Hardware 7
- Software 7
- AutoStore and Microsoft SQL Server 7

INSTALLING MOBILE SERVER8

INSTALLING SUPPORT SERVICE IN STAND-ALONE MODE13

CONFIGURING NSI MOBILE WITH CONFIGURATION MANAGER15

- Accessing Configuration Manager 15
- Database Configuration 16
- AutoStore Configuration 20
- Mobile Server Configuration 21
- Support Service Configuration 23
- Support Service Configuration in Stand-Alone Mode 24
- Output Manager Configuration 26
- Security Keys Configuration 27

LAUNCH ADMIN TOOLS29

CONFIGURING WEBCAPTURE ENDPOINT FOR NSI MOBILE SERVER30

- Configuring WebCapture for Authentication of NSi Mobile Users 31
- Configuring WebCapture to Support My Files 32

SETTING UP SSL FOR NSI MOBILE35

- Configuring SSL for the Mobile Client 35



Add site bindings in IIS:	35
Configure SSL in the NSi Mobile Server Configuration Manager	40
Specify server name on the Mobile Client.....	40
Configuring SSL for WebCapture	41
Configure NSi Mobile Server.....	41
Add the Certificate to the AutoStore Server.....	44
Configure WebCapture for SSL	48
Configuring SSL for Output Manager	50
Steps on the Output Manager Server	50
Steps on the NSi Mobile Server	53
LICENSING	58
Licensing a new installation of NSi Mobile.....	58



PREFACE

PURPOSE OF THIS DOCUMENT

This document provides instructions for installing NSi Mobile Server. The document is designed for use by the System Administrator for NSi Mobile Server and NSi AutoStore.

The NSi Mobile solution consists of the following software:

- Mobile Server
- Support Service
- NSi Mobile application for iOS/Android devices
- WebCapture (part of AutoStore)

VERSION COMPATIBILITY

The information in this document applies to:

- NSi Mobile version 7.0
- AutoStore version 7.0
- SecurePrint version 6.0
- Output Manager 3.2 (optional)

RELATED DOCUMENTATION

NSi Mobile includes the following documentation:

- NSi Mobile Administrator Guide
- NSi Mobile Installation Guide
- NSi Mobile Release Notes (<http://www.nsiastore.com/documentation>)

For more information about AutoStore and other NSi software, refer to the documentation provided with the products.



OVERVIEW

NSi Mobile Server is installed with an installation program that can be downloaded from the Web and run locally. (This is done via Software Updates in AutoStore.) The installation program will guide you through the steps for installing Mobile Server.

Mobile Server must be installed on a computer with access to the AutoStore server. It is typically installed on the same server as AutoStore, although some organizations install it on a different computer either in front of or behind the corporate firewall. Figure 1 shows an example AutoStore system with NSi Server installed on the same computer as AutoStore.

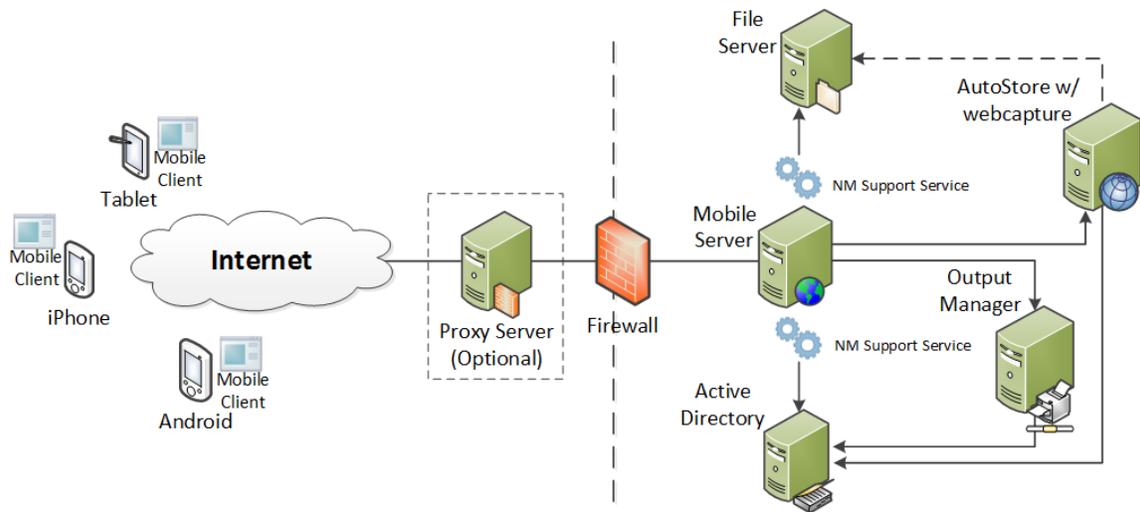


Figure 1. Example AutoStore System with NSi Mobile Server

Once NSi Mobile Server is installed, you must run the NSi Mobile Configuration Manager to set up the Web Server and various other settings required for the installation. You must also run AutoStore Process Designer to configure the Web Capture endpoint and Mobile Server licensing. The pertinent procedures are provided in this guide.



PREREQUISITES

HARDWARE

- Windows operating system (OS) running on a computer with at least a 2 GHz processor
- Minimum 2 GB of RAM is necessary, but 4 GB or greater is recommended
- Minimum of 20 GB of hard disk space
- NIC Card

SOFTWARE

Supported Windows operating systems:

- Windows Server 2008 R2 SP1 Enterprise
- Windows Server 2008 (32/64 bit) Standard /Enterprise – with the latest service pack
Important: Make sure that the Windows Server 2008 has Microsoft Visual C++ 2005 SP1 (VC80) Redistributable Package 8.0.50727.4027 or later, which can be downloaded from the Microsoft web site. Versions of mscrt80.dll earlier than 8.0.50727.4027 will not work with the NSi Mobile Server database. Windows Server2008 R2 SP1 does not require any update as it already has the later version of mscrt80.dll.
- Windows 7 Professional
Note: Windows 7 is not recommended for environments with more than 100 users

Additional software:

- NSi AutoStore 7.0
- Microsoft .NET Framework 4.0
- Microsoft IIS 7.0
 - (IIS Role, Application Server Role + Web Server IIS Support)
- SQL Server 2005/2008

Remaining prerequisites are installed during the installation process.

AUTOSTORE AND MICROSOFT SQL SERVER

AutoStore and Microsoft SQL Server should be installed and configured prior to installing NSi Mobile.

Refer to your AutoStore documentation for instructions for installing that product.

Note: The authentication mode for Microsoft SQL Server must be configured to use Mixed Mode Authentication or SQL Server Authentication. Contact your system administrator for assistance.



INSTALLING MOBILE SERVER

Follow these steps to install Mobile Server.

1. Download the NSi Mobile Server installation from Software Updates in AutoStore.
2. Run **Setup.exe** as administrator.
3. On the **Welcome** page of the installation wizard, click **Next** to continue.



Figure 2. Welcome page

4. On the **License Agreement** page, review the license agreement. To accept the license agreement, choose **I accept the terms of the license agreement**. Then, click **Next** to continue.



Figure 3. License Agreement

5. On the **Customer Information** page, type your **User Name** and **Organization** name. Then, click **Next** to continue.

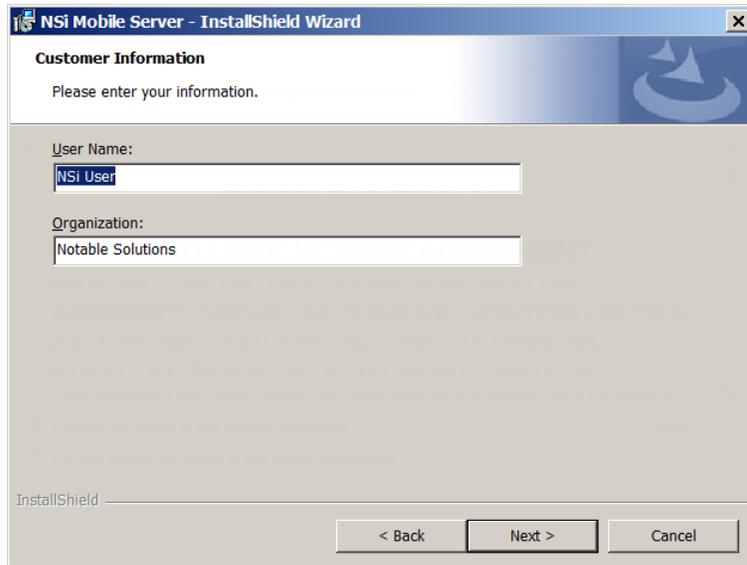


Figure 4. Customer Information



INSTALLING MOBILE SERVER

6. The default installation location is shown. To specify a different path, you can click **Change** and specify the different location. Then, click **Next** to continue.

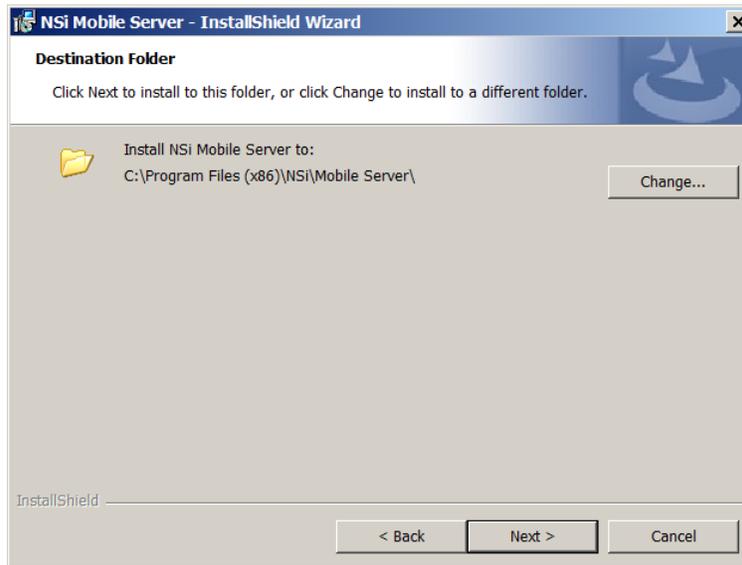


Figure 5. Destination Folder



INSTALLING MOBILE SERVER

7. On the **Setup Type** page, choose **Complete** (recommended) if you want to install all components (Mobile WebServer and Support Service). Choose **Custom** only if you are installing the Support Service and Mobile Server on different host machines. Then, click **Next** to continue.

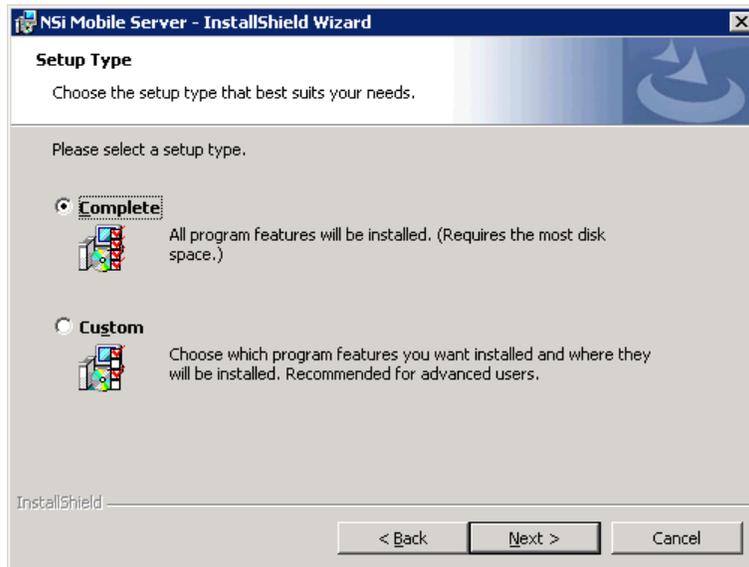


Figure 6. Setup Type

8. If you chose the **Custom** option, click the drop-down menu next to a component and click either **This feature will be installed on local drive** or **This feature will not be available** to specify whether a component will be installed.



INSTALLING MOBILE SERVER

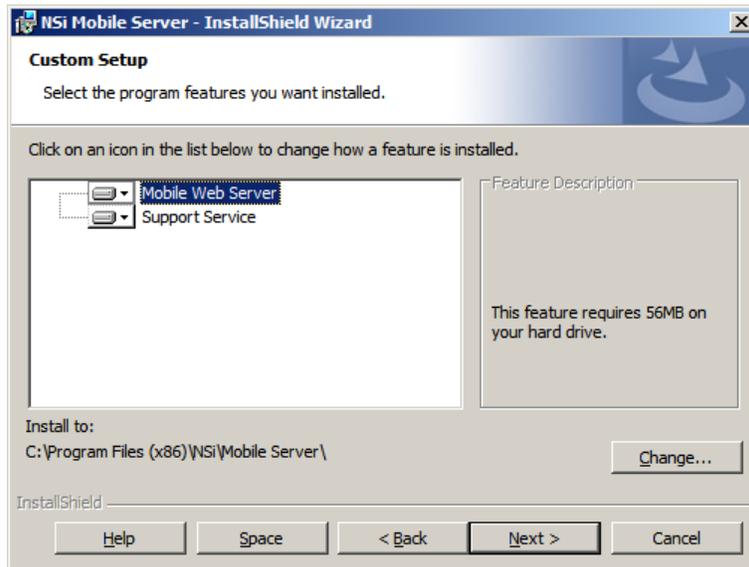


Figure 7. Custom Setup

To change the location where NSi Mobile Server is installed, click the **Change** button. You can click the **Space** button to view available and required space on local drives.

After you finish configuring the custom install, click **Next** to continue.

9. On the **Ready to Install** page, click **Install** to install the software.

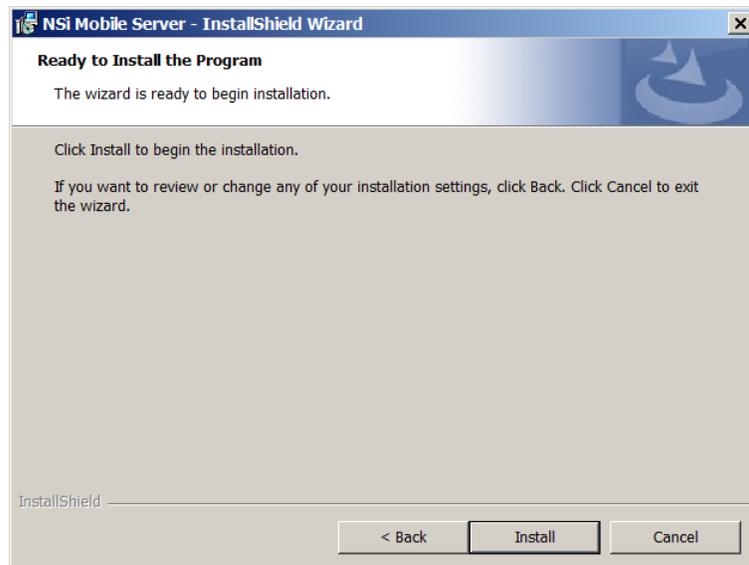


Figure 8. Ready to Install



INSTALLING SUPPORT SERVICE IN STAND-ALONE MODE

10. Along with the NSi Mobile Server files, the installation program installs the Configuration Manager, which is a utility that allows you to set up the Web Server and other required settings after you install the NSi Mobile Server. On the **InstallShield Wizard Completed** page, leave the **Launch Configuration Manager** check box selected to launch Configuration Manager when installation is complete.

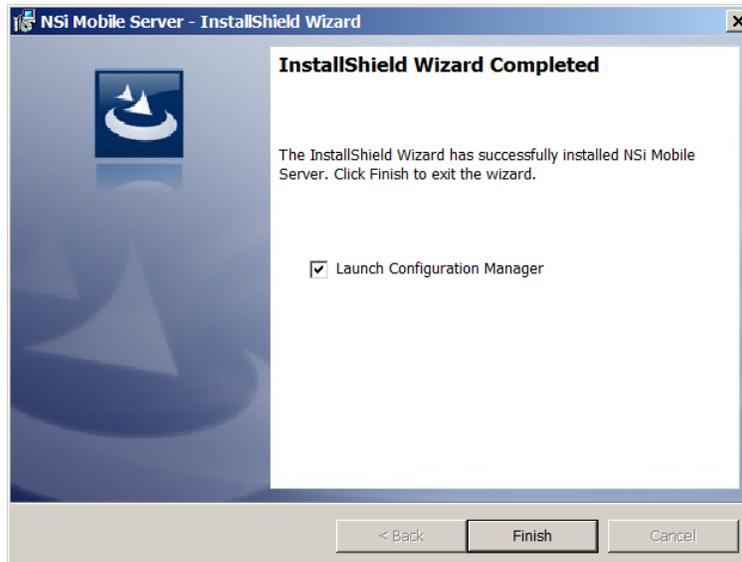


Figure 9. Installation Complete

11. Click **Finish** to complete the installation
12. Proceed to the next section to use Configuration Manager to configure NSi Mobile.

INSTALLING SUPPORT SERVICE IN STAND-ALONE MODE

The Support Service can be installed separately from the Mobile Server on a different virtual machine or server, however this is not the recommended deployment approach.

Follow steps 1-6 of the Mobile Server installation, then proceed to the following steps:

1. Choose Custom for the **Setup Type**
2. Choose **This feature will be installed on local drive** only for Support Server, and choose **This feature will not be available** for Mobile Web Server
3. Continue to steps 9-12 of the Mobile Server Installation



INSTALLING SUPPORT SERVICE IN STAND-ALONE MODE



Figure 10. Welcome page



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

Once Mobile Server is installed, you must open the Mobile Server Configuration Manager to configure various settings.

Note: Configuration Manager is available in the **NSi** group on the Windows **Start** menu. The Configuration Manager will open automatically after the installation wizard completes if you did not clear the **Launch Configuration Manager** check box.

ACCESSING CONFIGURATION MANAGER

To access Configuration Manager:

1. Allow NSi Mobile Server Configuration Manager to start after installation is complete, or click **Start > All Programs > Notable Solutions > Mobile Server > Configuration Manager** to launch the Configuration Manager after you install NSi Mobile Server. The **Database** tab is shown in Figure 11.

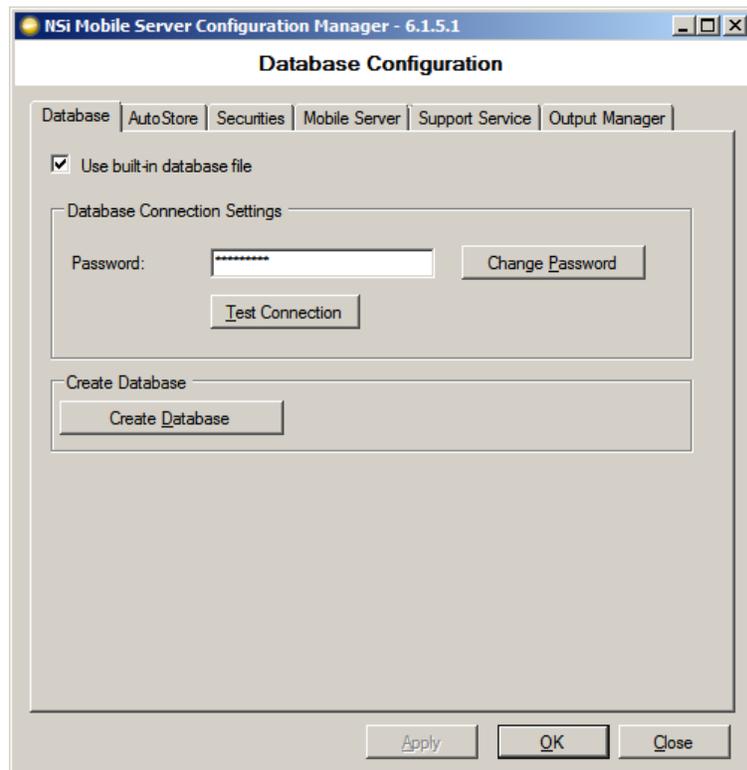


Figure 11. Configuration Manager



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

DATABASE CONFIGURATION

NSi Mobile relies on a Microsoft SQL Server database to manage transactions. Users in an enterprise environment often require the functionality of a separate database server. Those users should use the second procedure in this section to configure the NSi Mobile database. Other users may choose to use the Microsoft SQL Server Compact database that is embedded in NSi Mobile Server. The following procedure describes how to configure NSi Mobile Server to use the embedded database.

To configure the embedded SQL Server Compact database:

This procedure describes how to configure the embedded Microsoft SQL Server Compact database.

1. To use the embedded Microsoft SQL Server Compact database, leave the **Use built-in database file** check box selected.
2. Click the **Change Password** button to create a unique database password for your installation, and then click **OK**.

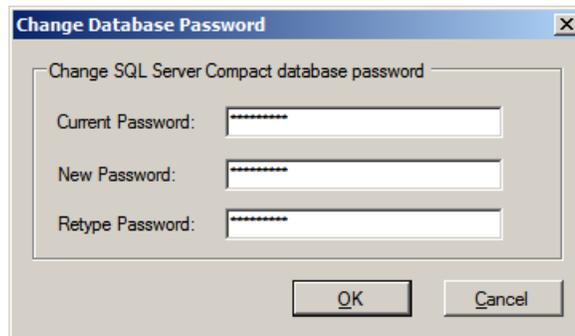


Figure 12. Change Password dialog box

Important: For **Current Password**, type the default password, which is "nsimobile". Then type your new password in the **New Password** and **Retype Password** boxes.



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

3. You can click the **Test** button to check the database connection.
4. Click the **Apply** button to save your changes.

Note: The initial SQL Server Compact database is created automatically. Anytime in the future you can come back and click the **Create Database** button to replace an existing SQL Server Compact database.

To configure a database on a Microsoft SQL Server database server:

Use this procedure to create a database on a separate Microsoft SQL Server database server.

1. Clear the **Use built-in database file** check box.

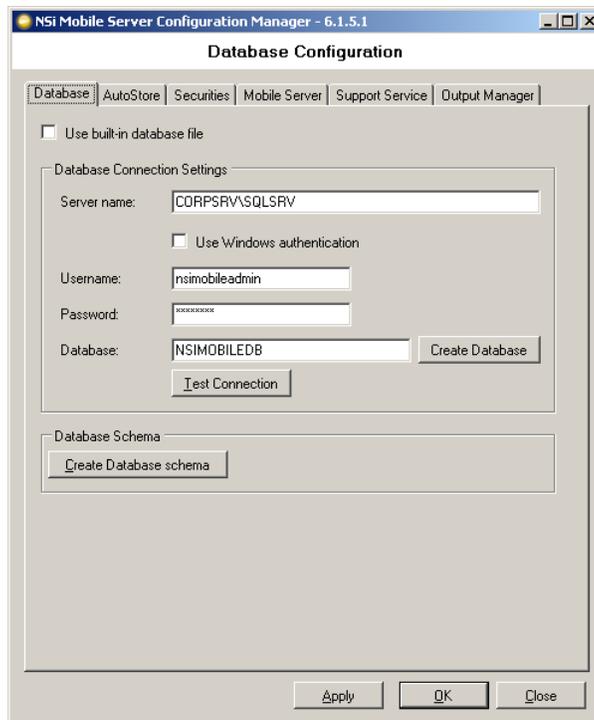


Figure 13. SQL Server database server configuration

2. Enter the name for the instance of SQL Server in the **Server name** box.
A named instance of SQL Server is normally identified by *hostname\instancename* (for example: CORPSRV\SQLSRV). The default instance of SQL Server is referred to by the *hostname* for the server.
3. Enter the **Username** and **Password** that will be used to connect to the Mobile Server database.
To use a Windows domain user name and password, first select the **Windows Authentication User** check box.



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

Note: If a SQL Server user name already exists, Configuration Manager will use that user. If a user name does not exist, Configuration Manager will add the user to SQL Server. The user name specified here will be assigned database roles required by NSi Mobile server.

4. For **Database**, enter the name for the database that will be associated with NSi Mobile Server.
5. For a new database, click **Create Database** to create the database.
6. In the **SQL Server Authentication** dialog box, specify a user account that is authorized to create or update the specified database on the database server, and then click **OK**.



Figure 14. Authorized account specification

- Click **Windows Authentication** to create the database using your current domain logon credentials.
 - Click **SQL Server Authentication** to enter an authorized SQL Server **Username** and **Password**.
7. Click **Test Connection** to test the connection to the server. If the connection fails, make sure that the database server is running, and that you entered the correct **Server name** along with valid credentials for the database or for creating the database.
 8. Once successful, click **OK** to dismiss the **Test connection succeeded** message.

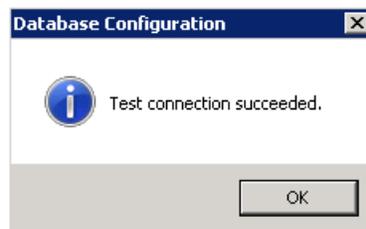


Figure 15. Connection Succeeded



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

9. Click **Create Database schema**. A message appears, indicating that any data in the database will be deleted.

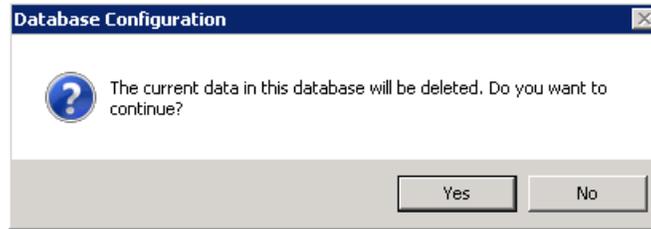


Figure 16. Database deletion prompt

10. Click **Yes** unless you want to save any existing data.

Note: If you click **No**, the database will not be created. Specify a different database, one which contains no data or contains data that can be deleted.

11. Once the database is successfully created, click **Apply** to save the settings. Then, proceed to the next procedure to continue the configuration.



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

AUTOSTORE CONFIGURATION

1. From Configuration Manager, click the **AutoStore** tab:

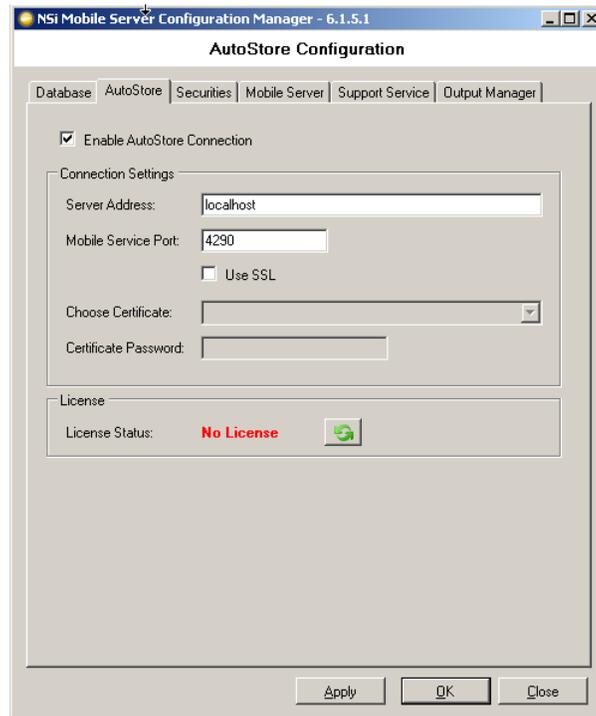
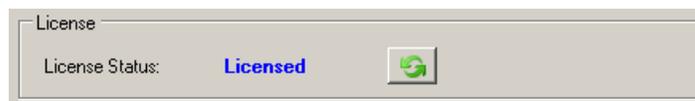


Figure 17. Mobile Server Configuration

2. Select the **Enable AutoStore Connection** check box to use AutoStore to provide workflows. This option is selected by default.
3. Make sure that **Server Address** shows the correct address for the AutoStore server. You can enter "localhost" if NSi Mobile Server is running on the same machine as AutoStore.
4. In the **Mobile Service port**, enter the port you will be using for Mobile Server communication.
5. Click **Apply**, and then click the refresh button in the **License** box.
The License Status should change to "Licensed" if NSi Mobile Server connects successfully to the AutoStore server.



Important: For NSi Mobile Server to communicate with AutoStore and show the "Licensed" status, the WebCapture service must be running, and the port number shown here must match



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

the **Mobile service port** number in the WebCapture **Mobile Server** settings. See [Configuring WebCapture Endpoint for NSi Mobile Server](#) in this document.

MOBILE SERVER CONFIGURATION

1. From Configuration Manager, click the **Mobile Server** tab:

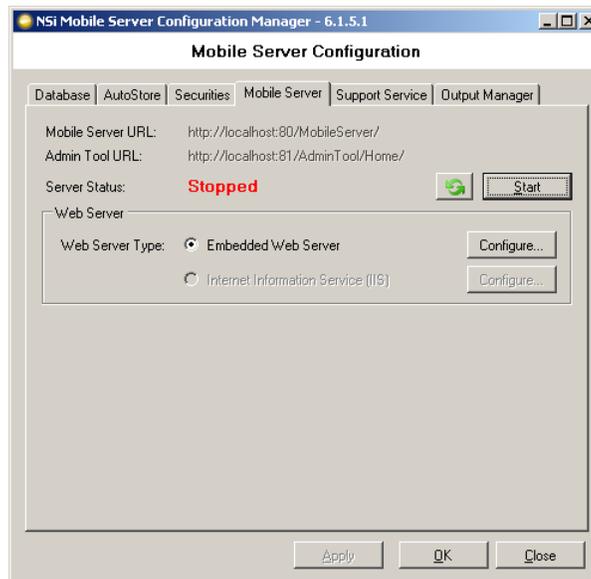


Figure 18. AutoStore Configuration

2. Note the URLs of Mobile Server and Admin Tool.

Note: The URLs for Admin Tools and Mobile Server shown in Configuration Manager start with “http://localhost.” When providing the link to client users and for accessing Admin Tools remotely, replace the the “http://localhost” portion with the actual server address (for example, 192.168.10.86 or www.companyURL.com).

Note: After Mobile Server is installed and configured, the Admin Tools web page is used by NSi Mobile administrators to monitor and maintain general Mobile Server settings, locations, users, and more. Refer to the *NSi Mobile Administrator Guide* for details.

3. If the **Server Status** is "Running", click **Stop**.
4. Choose the **Web Server Type**. If you are using IIS, click **Internet Information Service (IIS)**. Otherwise, click **Embedded Web Server**.

Note: If you want to use IIS, it must already be installed. See [Software Prerequisites](#) in this document for information on the required roles and services for IIS.



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

5. Click **Configure**. The Configuration window appears.

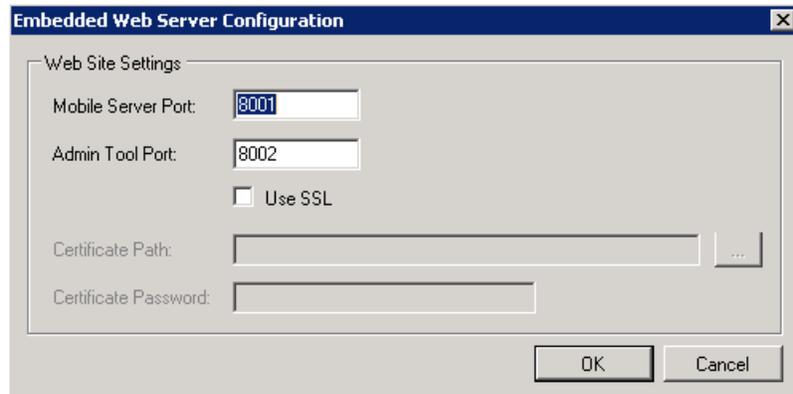


Figure 19. Embedded Web Server Configuration Window

6. Configure the Web Site settings that you want to use. Then click **OK** to close the configuration window.
7. Click **Apply** to save the settings.
8. Click **Start** to start the service.
9. Then, proceed to the next procedure to perform the **Support Service** configuration with Configuration Manager.



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

SUPPORT SERVICE CONFIGURATION

If you performed a [complete installation of NSi Mobile features](#), the Support Service will already be configured when you launch the Configuration Manager. Note that the “Connect to Support Service on local machine” checkbox is already checked, and the Service Status is “Running”.

1. In the NSi Mobile Server Configuration Manager, click the **Support Service** tab.

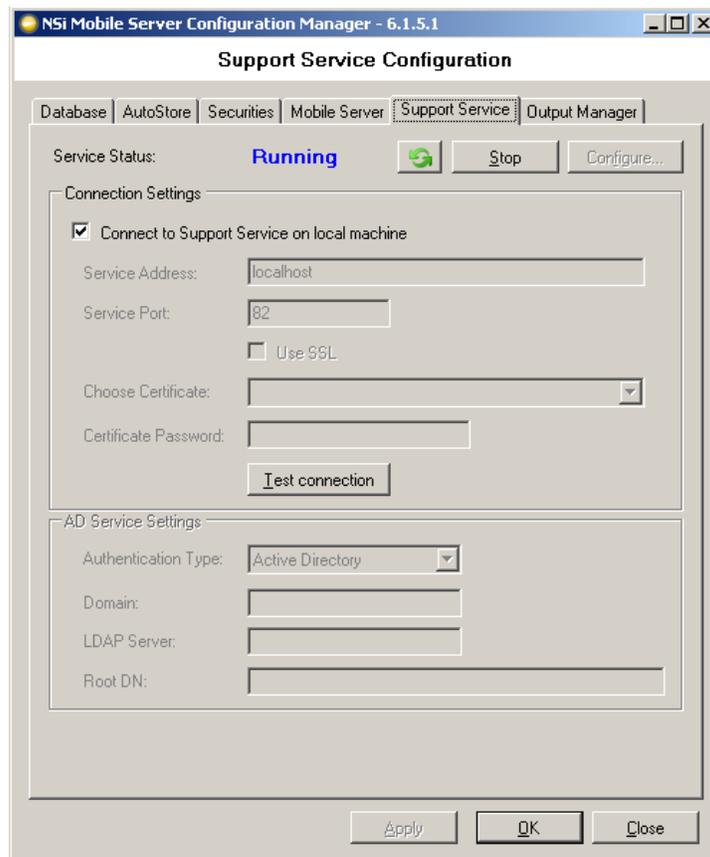
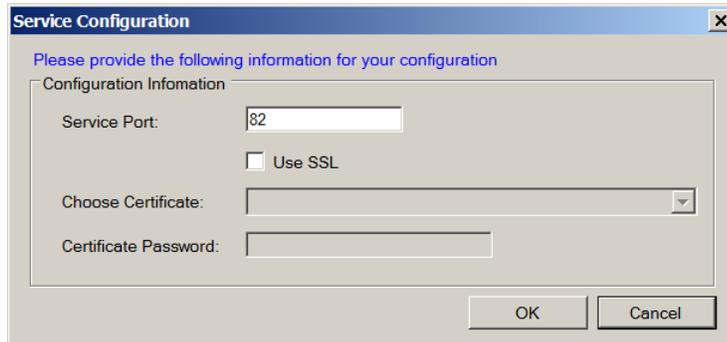


Figure 20. Support Service options



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

2. If needed, you can change the **Service Port**.
 - a. If the service is running, click **Stop** to stop the service.
 - b. Click the **Configure** button.
 - c. Enter a different port number in **Service Port**, and click **OK**.



- d. Click **Start** to start the service again.
3. Click **Apply** to save the settings. Then, proceed to the next section to configure Security Keys with the NSi Mobile Server Configuration Manager.

SUPPORT SERVICE CONFIGURATION IN STAND-ALONE MODE

If you [installed the Support Service separately from Mobile Server](#), you will need to set the connection settings in Configuration Manager to connect to the remote Support Service. You will also have to configure the Support Service on the remote server.

1. In the NSi Mobile Server Configuration Manager, click the **Support Service** tab.
 - a. If the service is running, click **Stop** to stop the service.
 - b. Enter the service address where the remote Support Service is running
 - c. Enter the port number in **Service Port**, and click **OK**.
2. Launch the NSi Mobile Server Configuration Manager on the remote server
 - a. If the service is running, click **Stop** to stop the service.
 - b. Enter the port number in **Service Port**, and click **OK**.



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

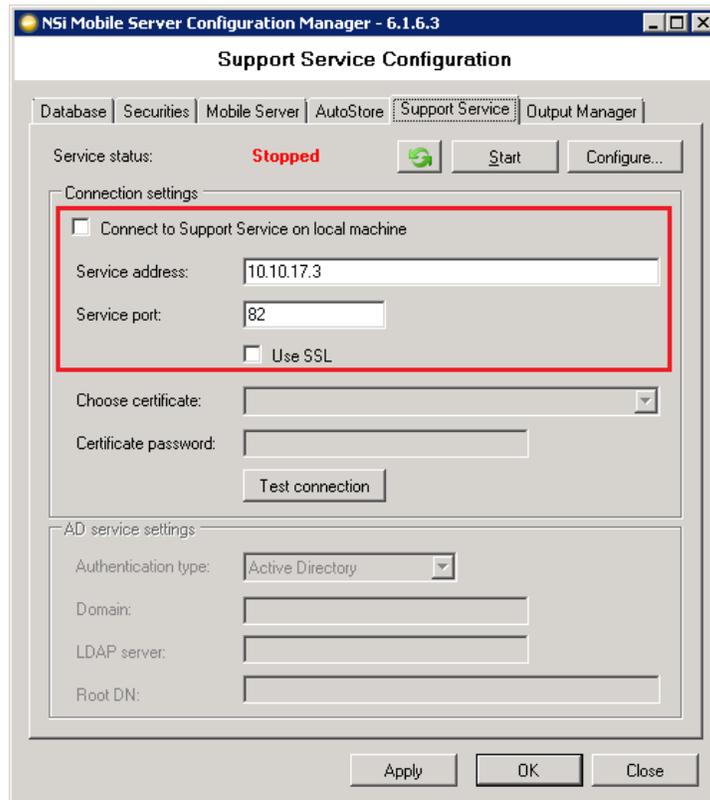


Figure 21. Support Service options in stand-alone mode

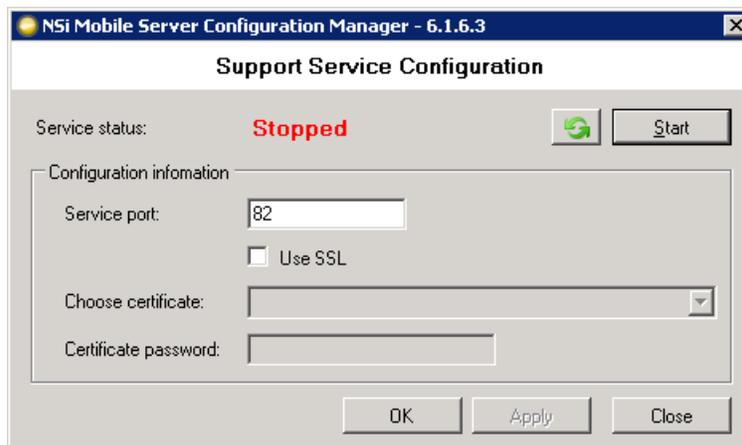


Figure 22. Support Service configuration on remote server



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

OUTPUT MANAGER CONFIGURATION

Settings on the **Output Manager** tab configure NSi Mobile Server to communicate with Output Manager.

To configure Output Manager settings:

1. In the Configuration Manager, click the **Output Manager** tab.
This displays the **Output Manager Connection settings**.

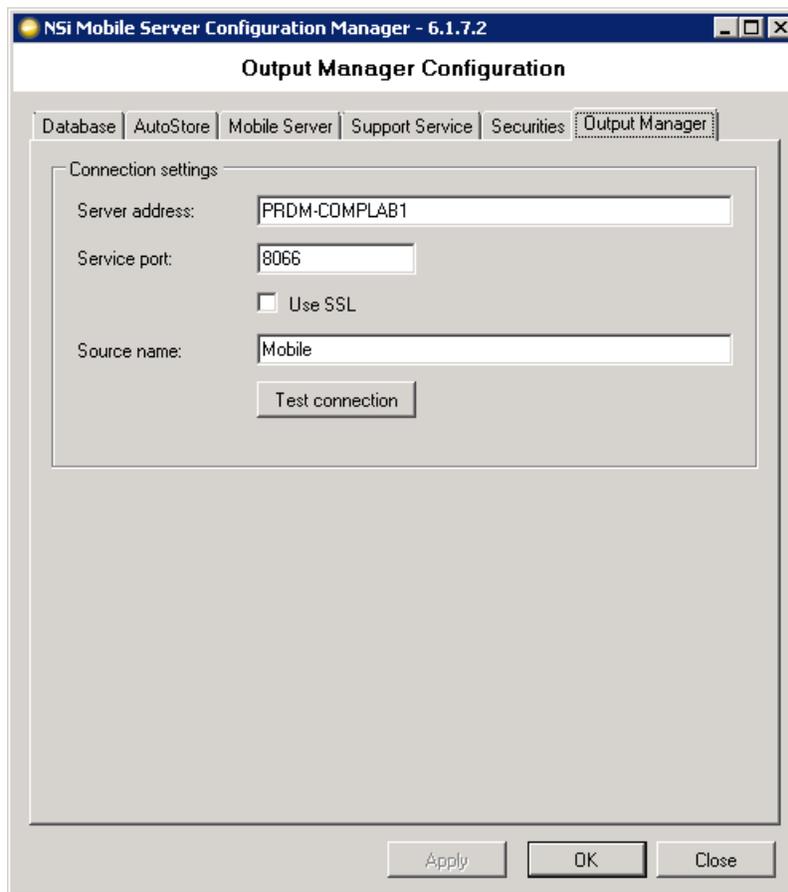


Figure 23. Output Manager Configuration



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

2. For **Server Address**, specify the host name for the Output Manager server.
For **Service Port**, type the port used by the Output Manager server to communicate with clients, and click **OK**. **Note:** By default, port 8066 is used to connect to Output Manager, and 8067 when SSL is checked.
3. For **Source Name**, enter the name of the input source specified in Output Manager

SECURITY KEYS CONFIGURATION

This tab is for the security keys needed to encrypt the credentials that are sent between the client and the server. Every time the Mobile Server is installed, a new set of keys must be generated.

To configure security keys:

1. In the Configuration Manager, click the **Securities** tab.



Figure 24. Security Keys Configuration



CONFIGURING NSi MOBILE WITH CONFIGURATION MANAGER

2. Enter a **Password**, then click **Create**.
A confirmation message appears, indicating that the security keys were successfully created.
3. Next to **Built-in Admin password**, type the password for the "admin" user.
The admin user password allows an NSi Mobile administrator to access the NSi Mobile Administrator Tool using the "admin" user name. The default password is "admin".
4. Click **Apply** to save the security settings. If necessary, you can review the configuration settings on any of the tabs.
5. Proceed to the next procedure to continue configuration.



LAUNCH ADMIN TOOLS

At this point, you can log into Admin Tools to perform initial setup before other users are configured as administrators using the default "admin" user name.

You can launch Admin Tools from a link in Configuration Manager. Or, you can note the Admin Tool URL and enter it in your browser. You may want to add it to your browser Favorites.

To launch Admin Tools:

1. In NSi Mobile Server Configuration Manager, click the **Mobile Server** tab.
2. Click the link to **Admin Tool URL**.

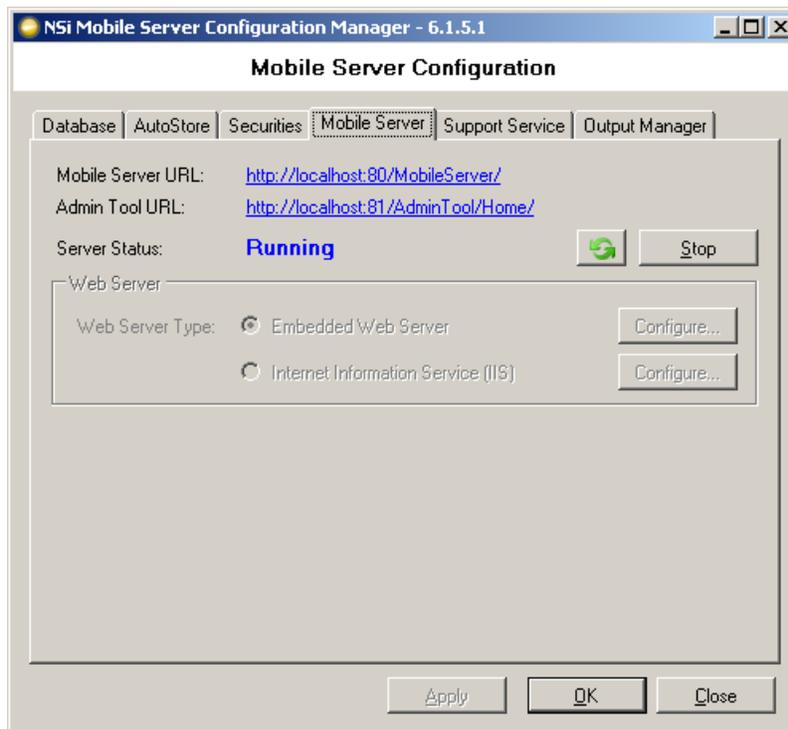


Figure 25. Admin Tools URL

3. Log in with the user name "admin" and the password entered on the **Securities** tab. The default password if you did not change it is "admin".

Note: At this point, switch back to the Configuration Manager to close it. Click **OK** to make sure your settings are saved. Then, click **Close**.

4. Refer to the *NSi Mobile Administrator Guide* for information about using Admin Tools.



CONFIGURING WEBCAPTURE ENDPOINT FOR NSi MOBILE SERVER

CONFIGURING WEBCAPTURE ENDPOINT FOR NSi MOBILE SERVER

Attention: Use the instructions in this section only if you selected the **Enable AutoStore Connection** check box on the **AutoStore** tab of NSi Mobile Configuration Manager (see [AutoStore Configuration](#)).

WebCapture must open a communication port that is accessible to Mobile Server. You do this from AutoStore Process Designer (APD).

Note: Refer to your AutoStore documentation for more information about AutoStore Process Designer.

Note: If WebCapture is already in use in a configuration, it is highly recommended that you set up a new and separate task dedicated to NSi Mobile.

To configure WebCapture communication port for Mobile Server:

1. APD, double-click the **WebCapture** icon in a workflow.
2. Click the **Mobile Server** tab.

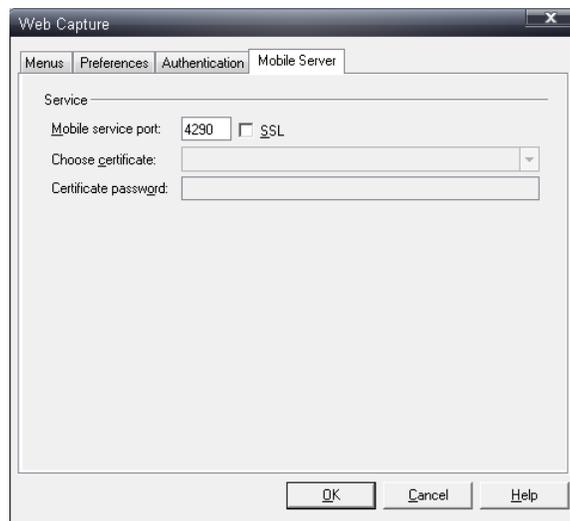


Figure 26. Service settings for Mobile Server in WebCapture

3. For **Mobile Service port**, enter the port you will be using for Mobile Server communication.

Important: The value entered here must match the value entered for **Mobile Service Port** in the on the **AutoStore** tab of NSi Mobile Server Configuration Manager. See [AutoStore Configuration](#) in this document.

4. Save and restart the task.



CONFIGURING WEBCAPTURE ENDPOINT FOR NSi MOBILE SERVER

5. On the **AutoStore** tab of the NSi Mobile Configuration Manager, confirm that the AutoStore **Server Address** is correct and that the **Mobile Service Port** number is the same that you specified for Web Capture in step 3.

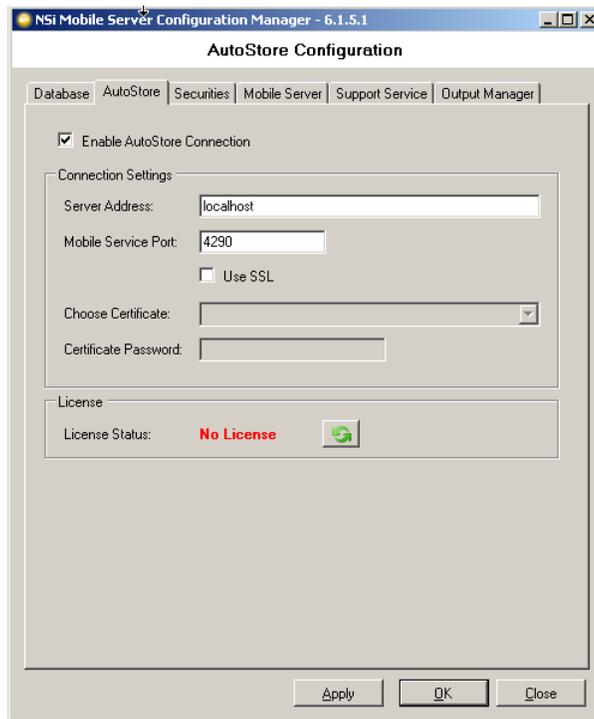
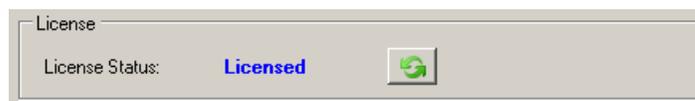


Figure 27. AutoStore options

If NSi Mobile Server is installed on the same host as AutoStore, enter "localhost" for **Server Address**. If AutoStore is on a different machine, enter the IP address or host name for the AutoStore server.

6. If you make any changes, click the **Apply** button, and after you click the refresh button in the **License** box, the **License Status** should switch to "Licensed".



CONFIGURING WEBCAPTURE FOR AUTHENTICATION OF NSi MOBILE USERS

To configure WebCapture for authentication of NSi Mobile users:

1. If not already there, start APD and double-click the **Web Capture** icon in the workflow.



CONFIGURING WEBCAPTURE ENDPOINT FOR NSi MOBILE SERVER

2. Click the **Authentication** tab.

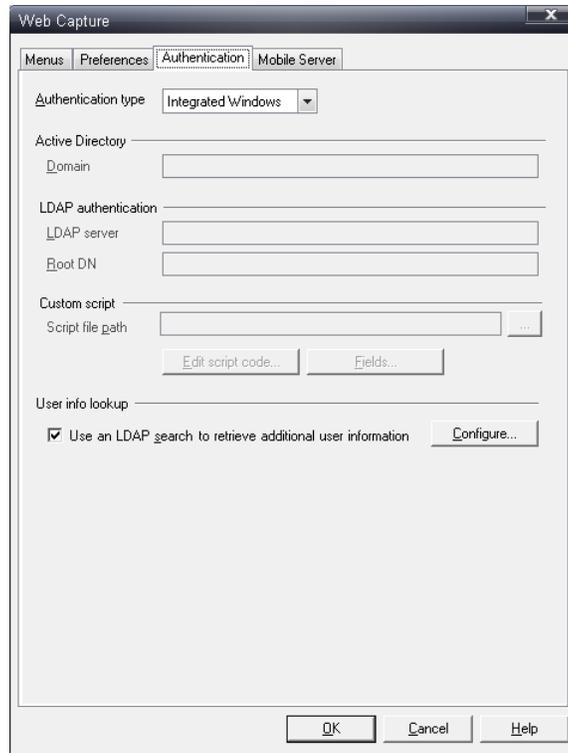


Figure 28. WebCapture Authentication

3. For **Authentication Type**, choose the authentication type that you are using.
 - Active Directory
 - LDAP authentication
 - Custom script (requires a Custom Development license)
4. Configure the settings to authenticate users and groups for the selected authentication type.

CONFIGURING WEBCAPTURE TO SUPPORT MY FILES

Webcapture can be configured to retrieve additional user attributes from the directory service. The home directory attribute is used to retrieve the path of a user's home directory, which is used for the My Files feature. If this attribute is not retrieved (by webcapture), the user's home directory path can be entered manually in Admin Tools.

1. If not already there, start APD and double-click the **WebCapture** icon in the workflow.
2. Click the **Authentication** tab.



CONFIGURING WEBCAPTURE ENDPOINT FOR NSi MOBILE SERVER

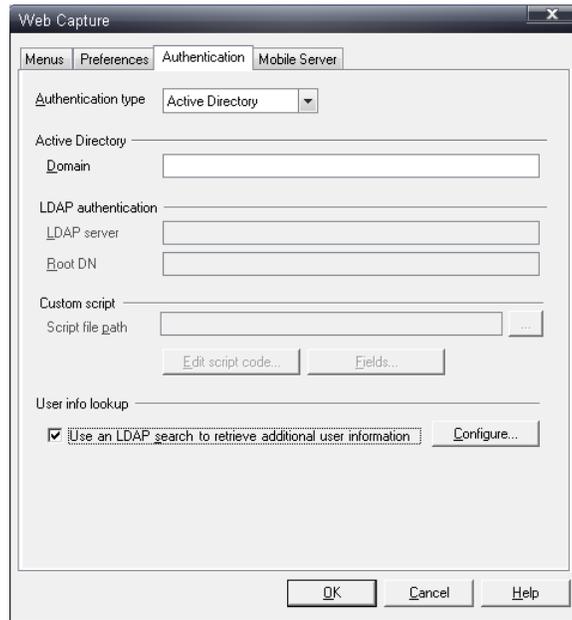


Figure 29. WebCapture Authentication

3. Select the **Use an LDAP search to retrieve additional user information** check box.
4. Click **Configure** to open the LDAP Lookup Settings dialog box.

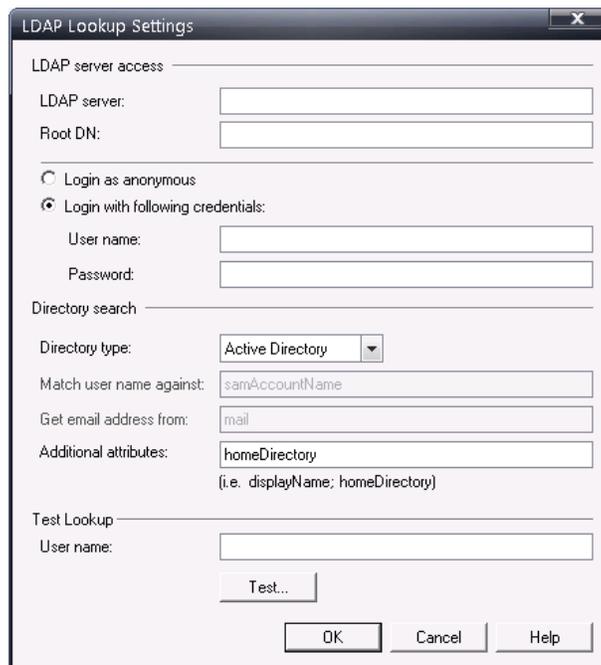


Figure 30. LDAP Lookup Settings



CONFIGURING WEBCAPTURE ENDPOINT FOR NSi MOBILE SERVER

5. Fill in the following fields:

For this option	Do this
LDAP server	Enter the LDAP server address. This is the same as the address for the domain controller.
Root DN	Enter the domain's Root Distinguished Name.
Login credentials	<ul style="list-style-type: none">• If the LDAP server allows anonymous login, choose the Login as anonymous option.• If it does not, choose the Login with following credentials and provide the User name and Password.
Directory Type	Choose Active Directory .
Additional Attributes	Enter homeDirectory. If there are additional attributes that are needed for workflows, enter them here as well and separate them with “;”



SETTING UP SSL FOR NSi MOBILE

This section describes the how to configure SSL for NSi Mobile. When you choose to use SSL, you need to configure SSL settings and specify a certificate for both ends of a communication link. NSi Mobile enables administrator to set up an SSL connection between any of the components of the NSi Mobile solution.

CONFIGURING SSL FOR THE MOBILE CLIENT

Important: When Mobile Server is deployed behind the corporate firewall:

- The address of the router/proxy server must be used in generating the SSL certificate.
- Port forwarding must be set up on the router/external server to point to the internal Mobile Server port. For example:
https://office.yourcompany.com:35016 forwards to https://10.16.35.106:443

Important: The generated SSL certificate must be issued for the specific URL/address of the external server/proxy. Examples:

- office.yourcompany.com
- *.yourcompany.com

Important: The SSL certificate must be issued by a trusted certificate authority. Examples:

- Computer Associates
- GoDaddy
- Symantec (formerly VeriSign)

To configure SSL for the Mobile Client, complete the following three tasks:

1. Add site bindings in IIS.
2. Configure SSL in NSi Mobile Server Configuration Manager
3. Specify the NSi Mobile Server name on the Mobile Client

ADD SITE BINDINGS IN IIS:

1. Launch IIS 7.0 Manager, and select the Server node.
2. In the IIS section, double-click "Server Certificates".



SETTING UP SSL for NSi MOBILE

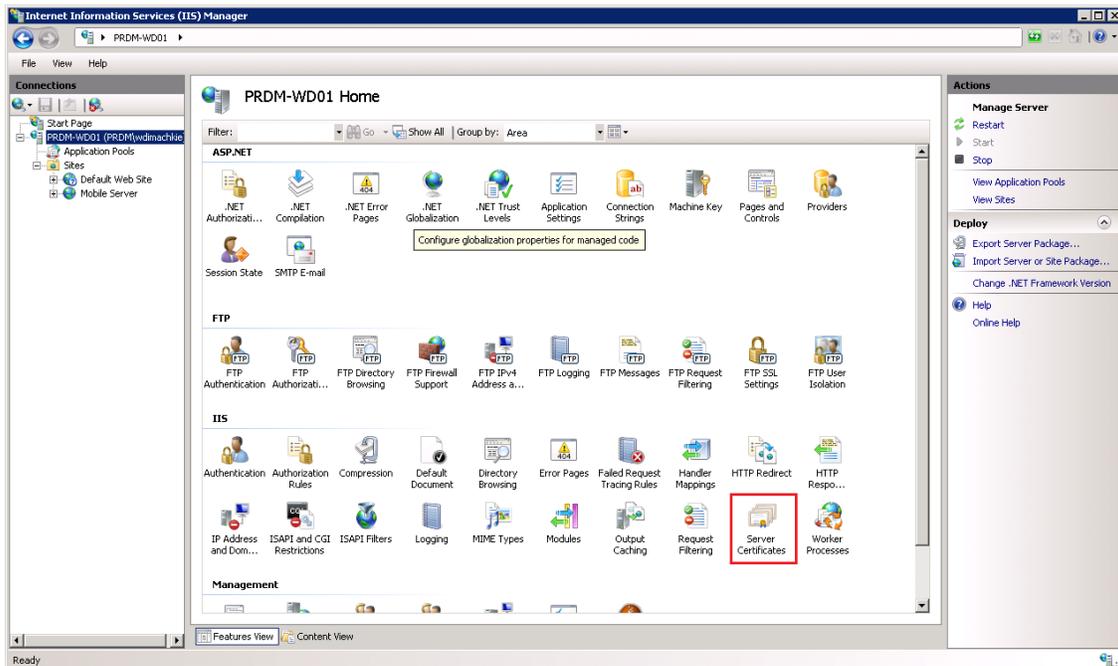


Figure 31. Server Certificates in IIS

3. In the IIS section, double-click "Server Certificates".
4. In the **Actions** pane, click **Import**, and then click the browse (...) button.

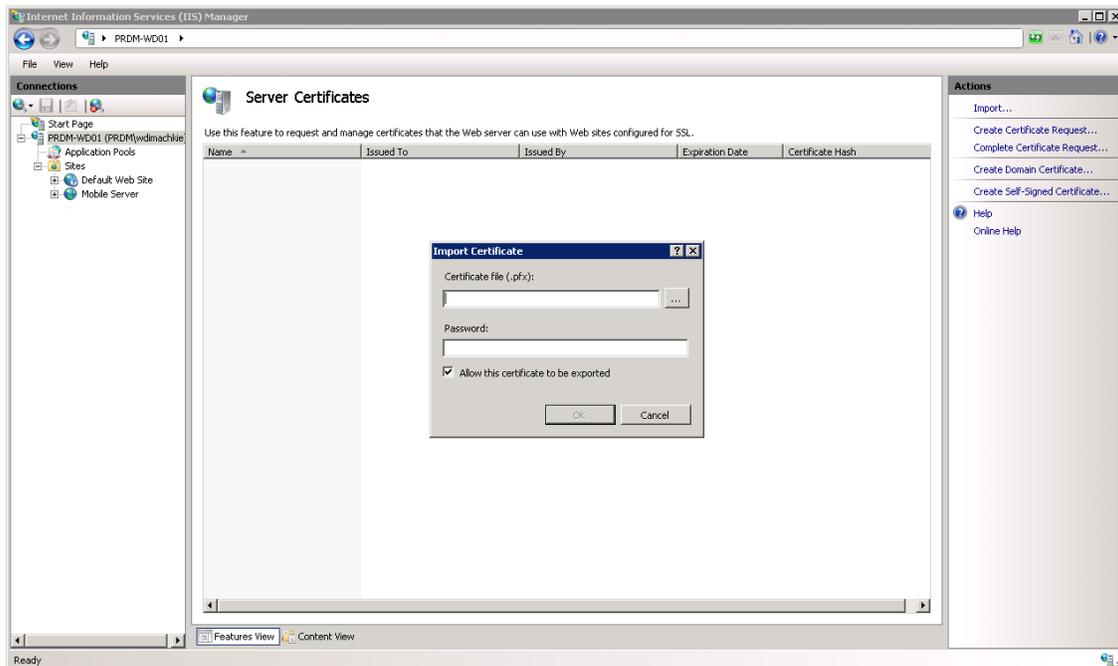


Figure 32. Import Certificate dialog box



5. In the **Open** dialog box, locate the certificate (.pfx) file, and click **Open**.

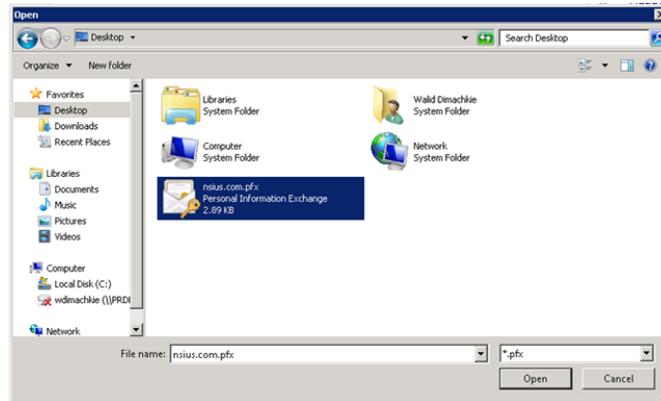


Figure 33. Open dialog box

6. Enter the password for the certificate, and click **OK**.

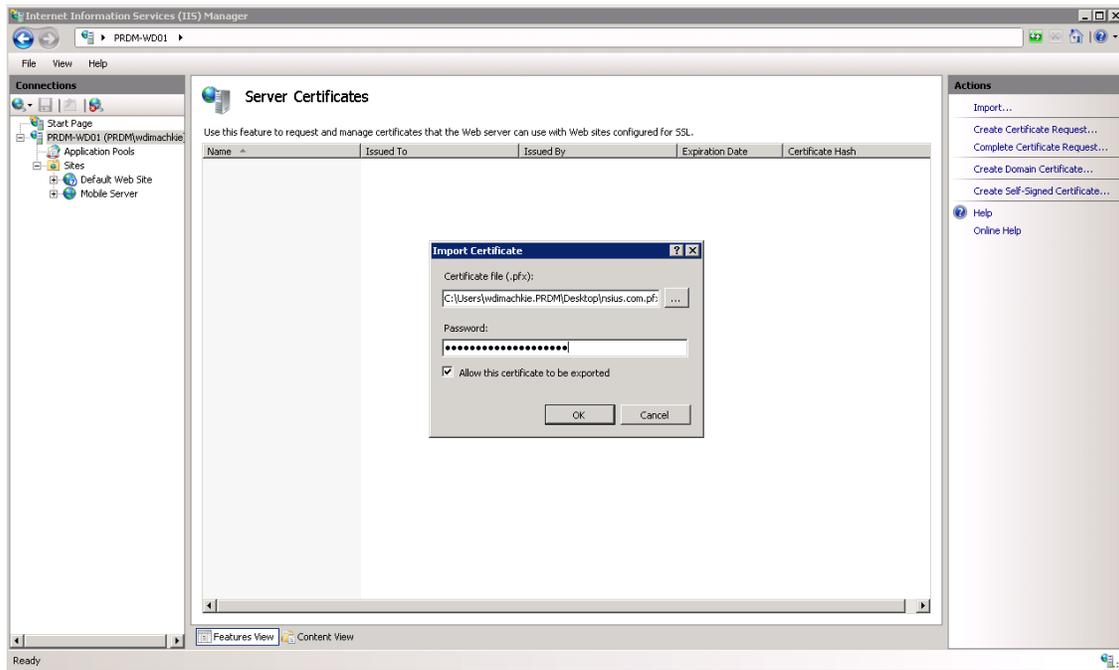


Figure 34. Certificate password

7. The **Server Certificates** list should now show the installed certificate.



SETTING UP SSL for NSi MOBILE

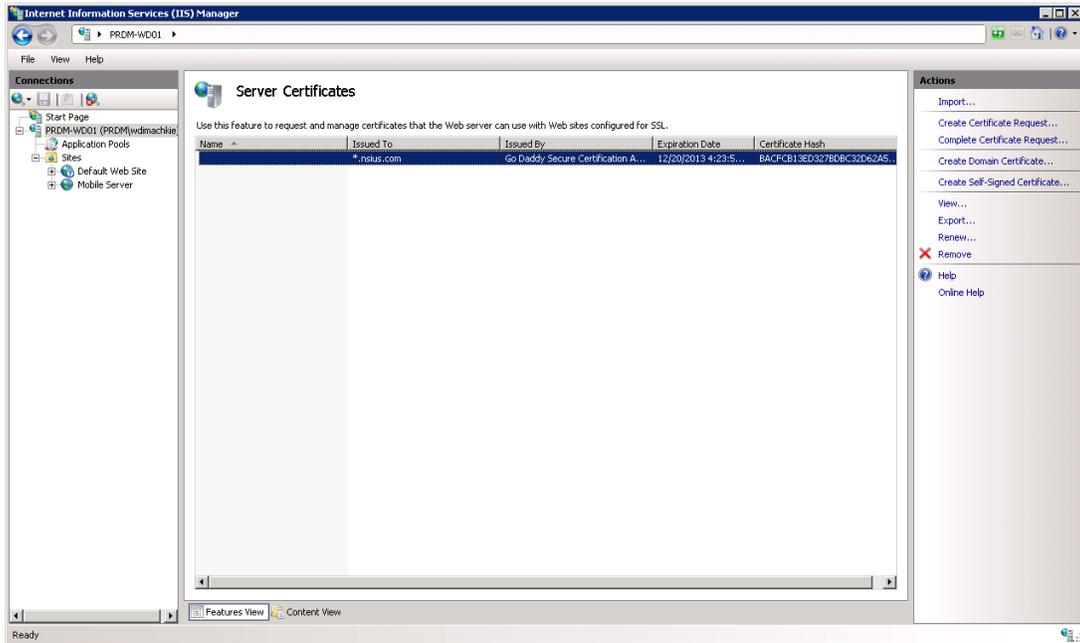


Figure 35. Server Certificates list

8. In the **Connections** pane, click the Mobile Server application node.
9. In the **Actions** pane, click **Bindings**.

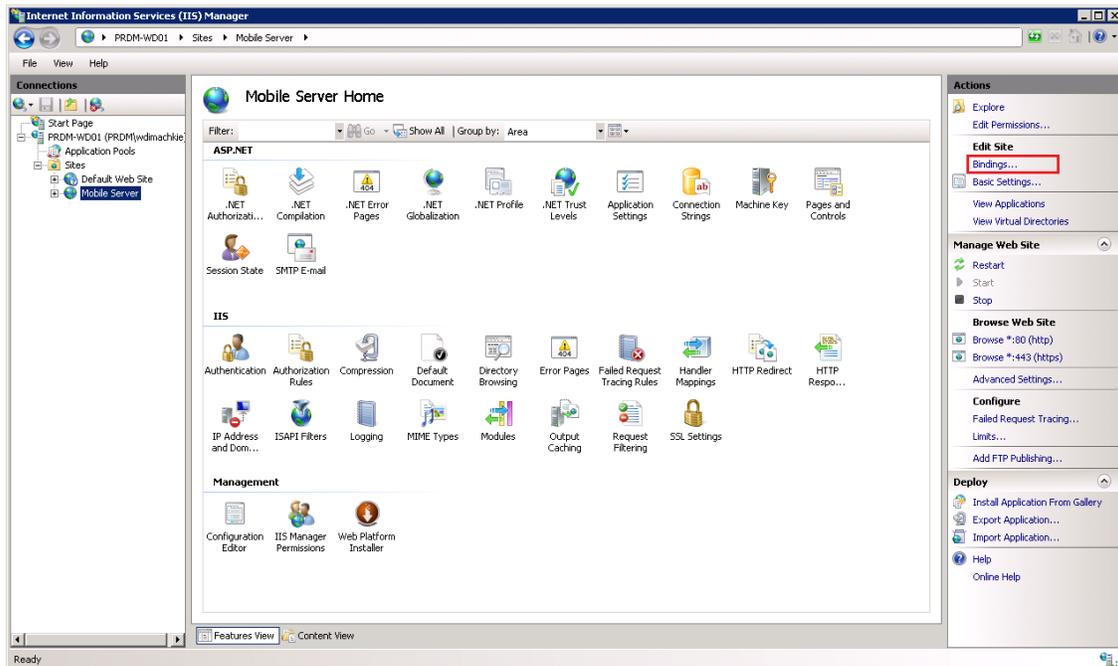


Figure 36. Mobile Server site in IIS



10. In the **Site Bindings** dialog box, click the **Add** button.

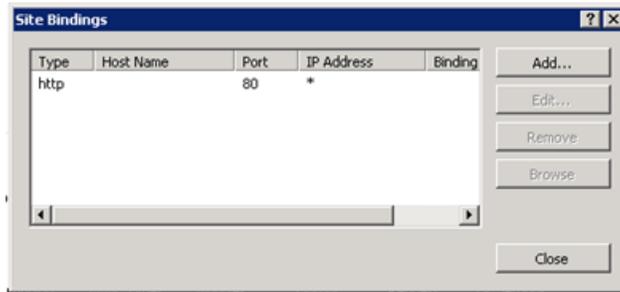


Figure 37. Site Bindings dialog box

11. In the **Type** box, select "https".

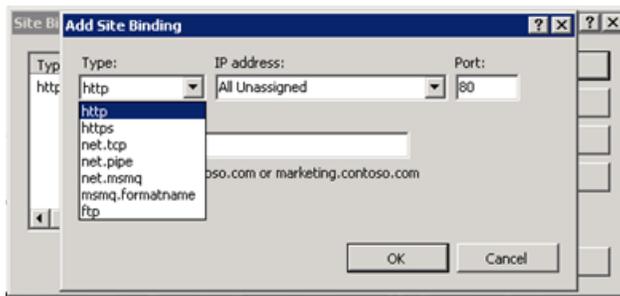


Figure 38. Site binding type

12. In the **SSL certificate** box, select the certificate, and click **OK**.

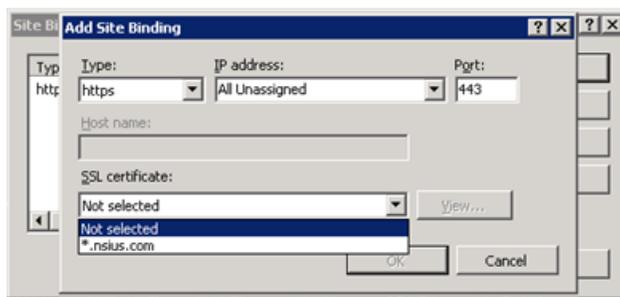


Figure 39. SSL certificate list

13. The **Site Bindings** list box should now show both the http (80) and https (443) bindings.



SETTING UP SSL for NSi MOBILE

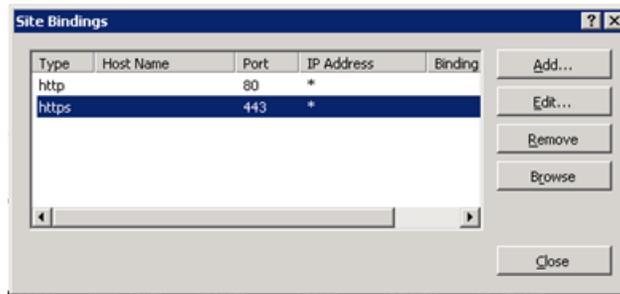


Figure 40. Site bindings list

14. Click the **Close** button.

CONFIGURE SSL IN THE NSi MOBILE SERVER CONFIGURATION MANAGER

1. On the **Mobile Server** tab of NSi Mobile Server Configuration Manager, choose **Internet Information Service (IIS)** and click the **Configure** button.
2. In the IIS Configuration dialog box, only specify the http port (80).

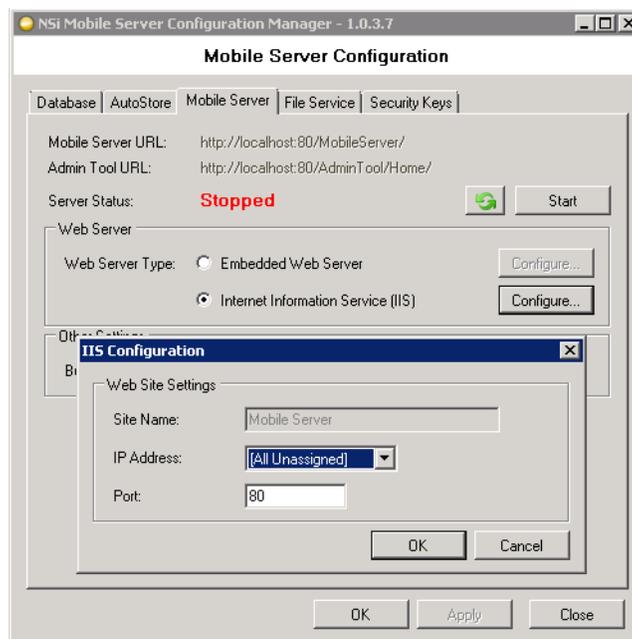


Figure 41. IIS configuration

SPECIFY SERVER NAME ON THE MOBILE CLIENT

- In NSi Mobile Client, specify the https URL that points (internally) to the https port (443), either: <https://mobile.yourcompany.com/mobileserver>



- or -

<https://mobile.yourcompany.com:8523/mobileserver>

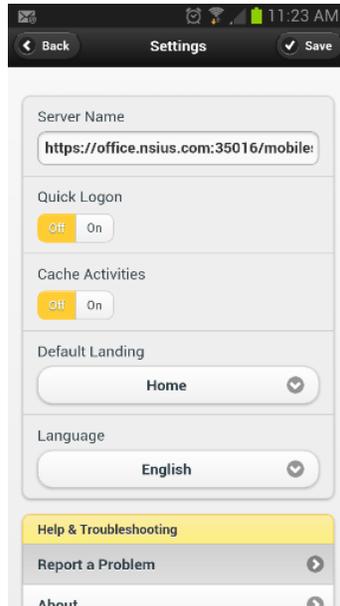


Figure 42. Server settings

CONFIGURING SSL FOR WEBCAPTURE

CONFIGURE NSI MOBILE SERVER

1. Launch NSi Mobile Server Configuration Manager.
2. Click on the **AutoStore** tab.



SETTING UP SSL for NSi MOBILE



Figure 43. AutoStore configuration

3. Select the **Use SSL** check box.
4. In the **Choose Certificate** box, select “New self-signed...”.

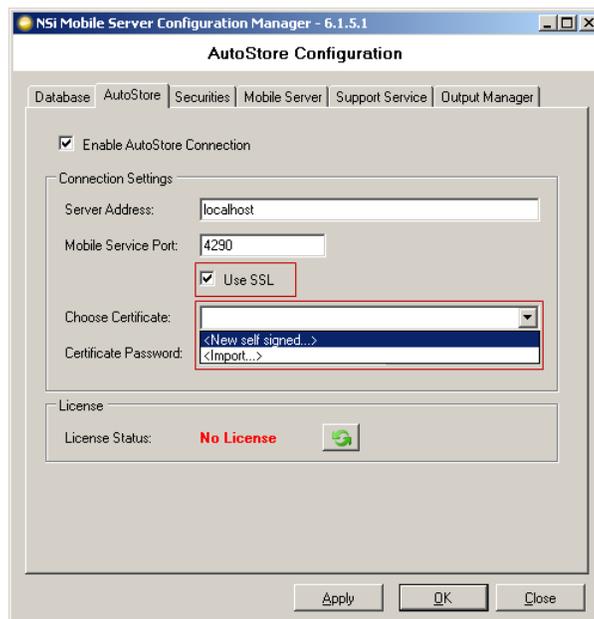


Figure 44. Specifying SSL for AutoStore connection

5. In the **New Self Signed Certificate** dialog box, type your **Company** name.



6. Set the **Expire Date** to create the desired period.
7. Type a **Password** for the certificate.

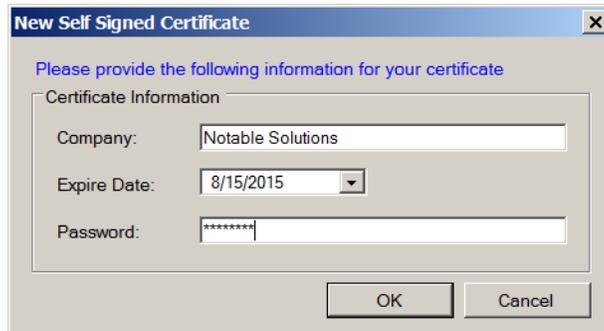


Figure 45. Certificate password

8. Click **OK**.

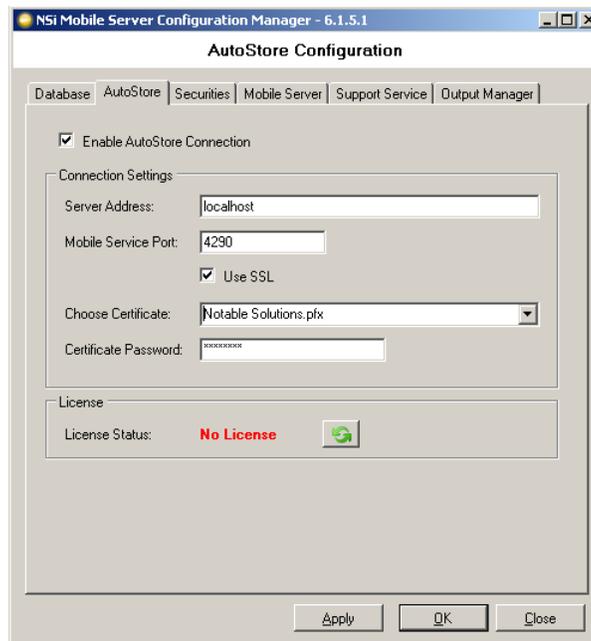


Figure 46. After configuring SSL for the AutoStore connection

9. Open My Computer or Windows Explorer and locate the certificate file in the Mobile Server\Config folder in the NSi program files directory.



SETTING UP SSL for NSi MOBILE

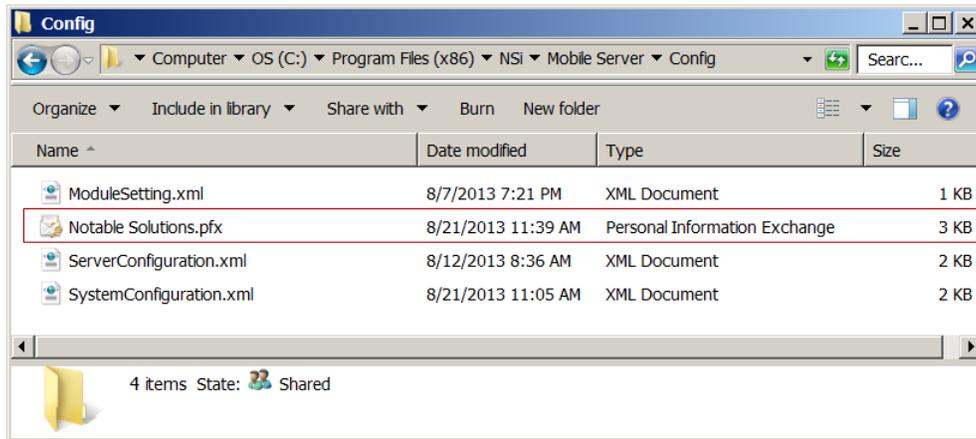


Figure 47. Certificate file that was saved in the Config folder

This is the file that you will need to install on the AutoStore server.

ADD THE CERTIFICATE TO THE AUTOSTORE SERVER

1. Copy the certificate to the host machine that is running AutoStore server.
2. Click on the **AutoStore** tab.
3. Start the Microsoft Management Console.
On the Windows **Start** menu, click **Run**, type **mmc**, and then click **OK**.
4. Click **File > Add/Remove Snap-in**.

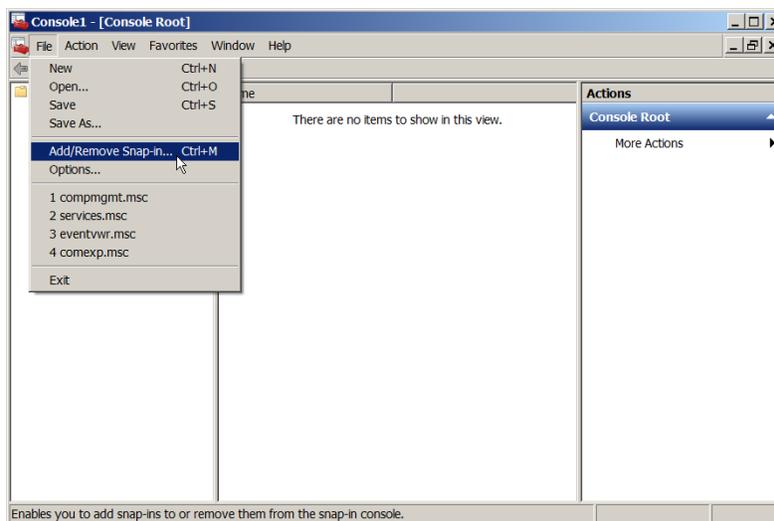


Figure 48. Adding a new snap-in

5. In the **Available snap-ins** box, double-click **Certificates**.



SETTING UP SSL for NSi MOBILE

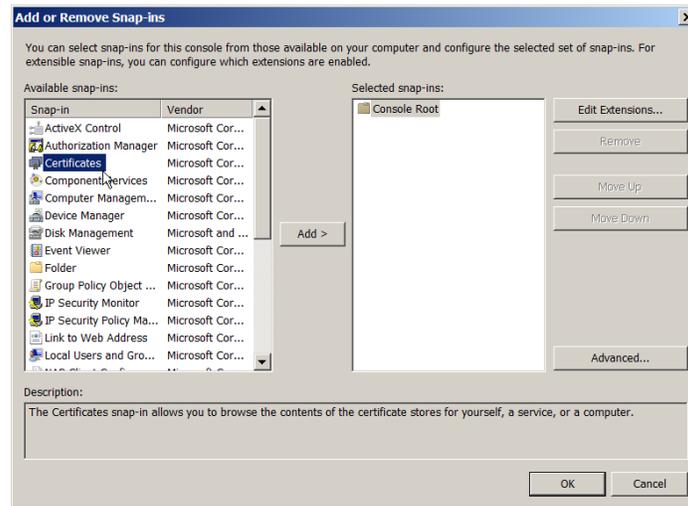


Figure 49. Selecting the Certificates snap-in

6. In the **Certificates snap-in** dialog box, choose to manage certificates for **Computer account** and click **Next**.

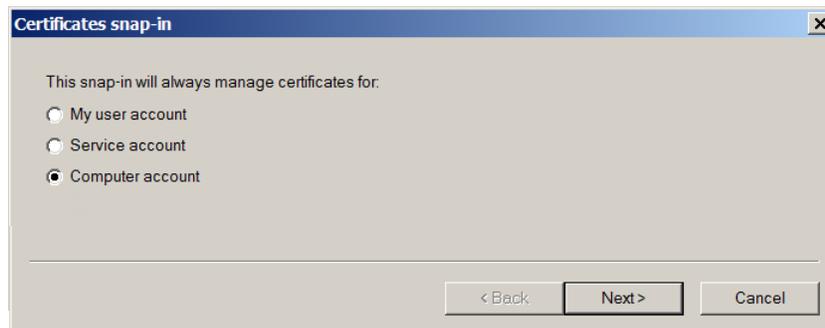


Figure 50. Specifying target for certificates snap-in

7. Click **Finish** to set up the MMC Certificates snap-in to manage the **Local computer**, and then click **OK** to close the **Add or Remove Snap-in** dialog box.

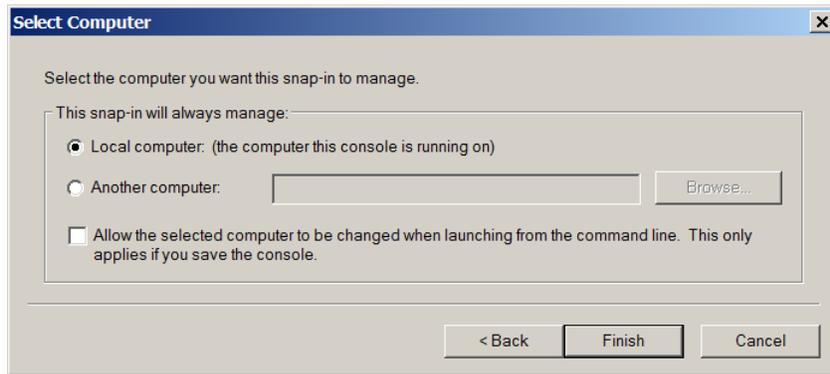


Figure 51. Computer managed by Certificates snap-in

8. In the tree pane of the MMC console, expand "Certificates (Local Computer)".
9. Right-click "Trusted Root Certificate Authorities" and click **All Tasks > Import**.

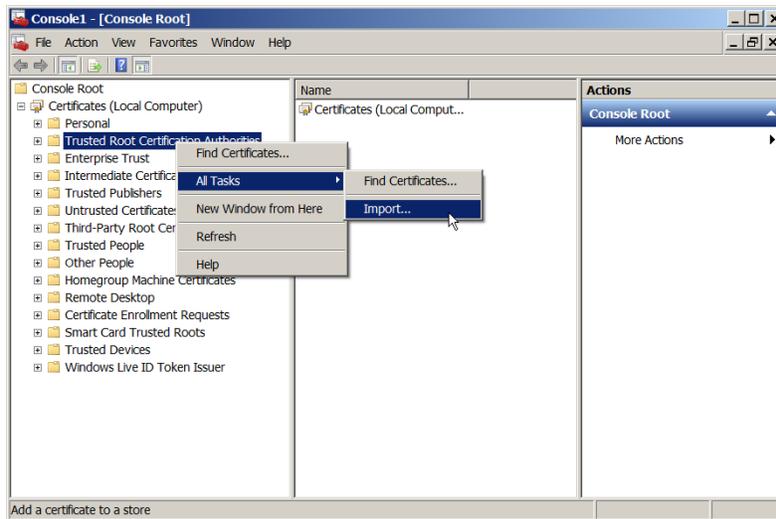


Figure 52. Importing Certificate

10. On the Welcome page of the Certificate Import Wizard click **Next**,
11. Click **Browse**, and in the **Open** dialog box, select the Personal Information Exchange (.pfx) file that was copied to the host machine in step 1 of this procedure, and **Open**, and then click **Next**.



SETTING UP SSL for NSi MOBILE

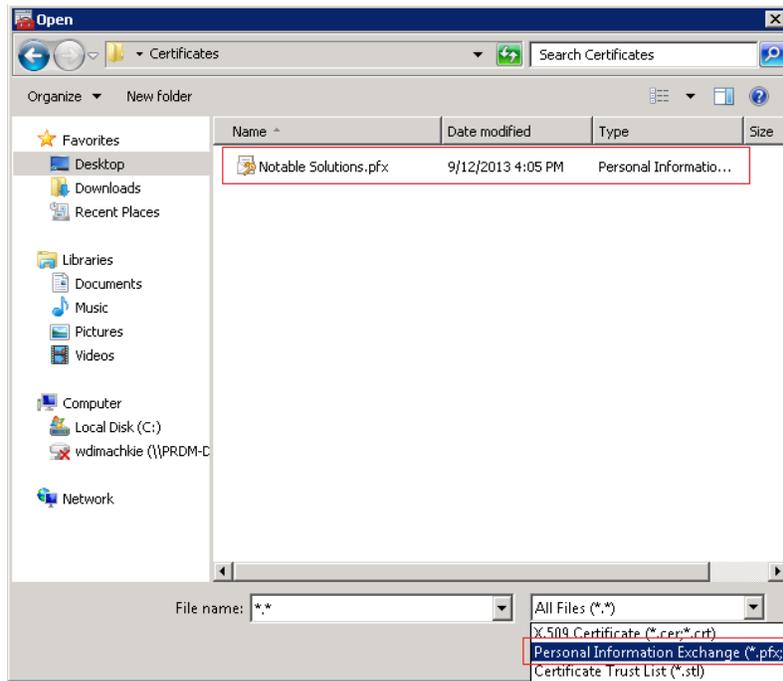


Figure 53. Selecting the Personal Information Exchange file

12. In the **Password** box type the password that was used to generate the certificate on the NSi Mobile Server, and then click **Next**.

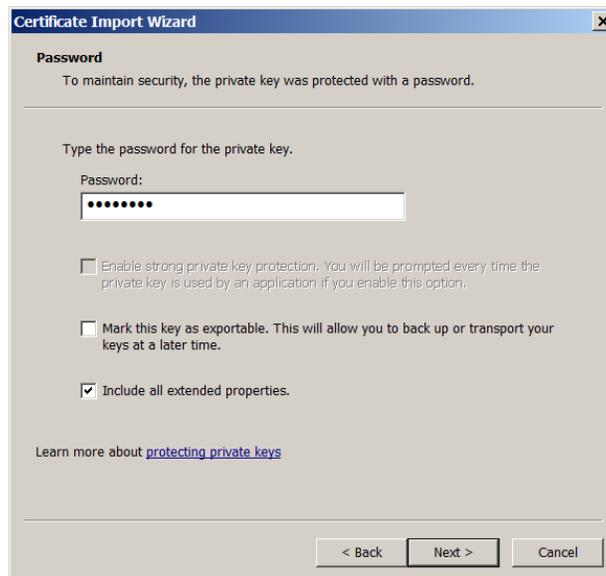


Figure 54. Specifying the password for the certificate



13. Make sure the **Certificate store** is set to “Trusted Root Certification Authorities”, click **Next**, and then click **Finish**.

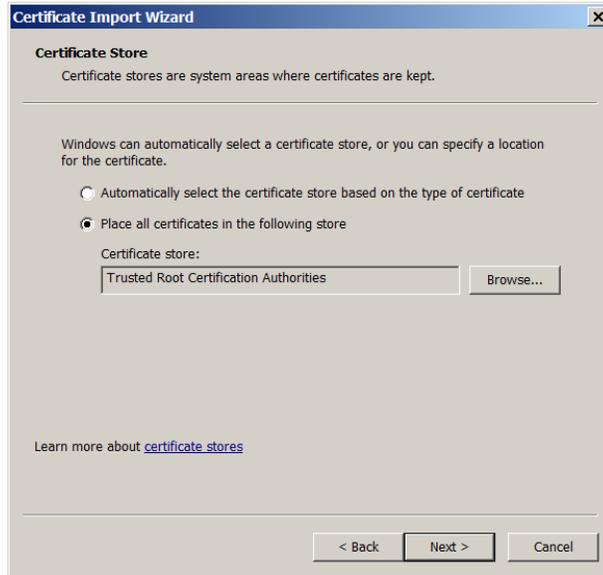


Figure 55. Specifying the certificate store

14. In the MMC console tree, expand "Trusted Root Certification Authorities", and in the "Certificates" folder, confirm that the certificate has been added.

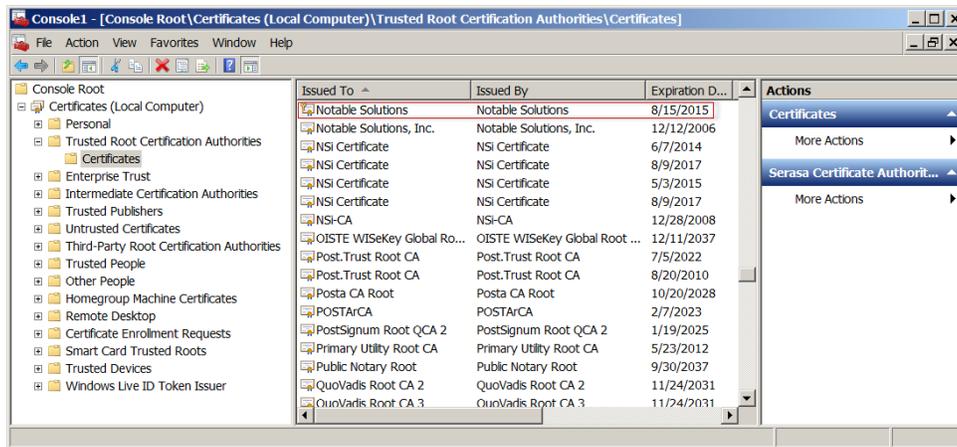


Figure 56. Confirming that the certificate has been added

CONFIGURE WEBCAPTURE FOR SSL

1. On the AutoStore server, launch the AutoStore Workflow Process Designer. Click **Start > Notable Solutions > AutoStore 7 > AutoStore 7 Process Designer**.



2. On the AutoStore server, launch the AutoStore Workflow Process Designer.
3. In the workflow, double-click the Web Capture icon to open the **WebCapture** properties dialog box.
4. On the **Mobile Server** tab, select **SSL**.
5. In the **Choose certificate** box, select the certificate that was configured earlier.
6. In the **Certificate password** box, type the password for the certificate.

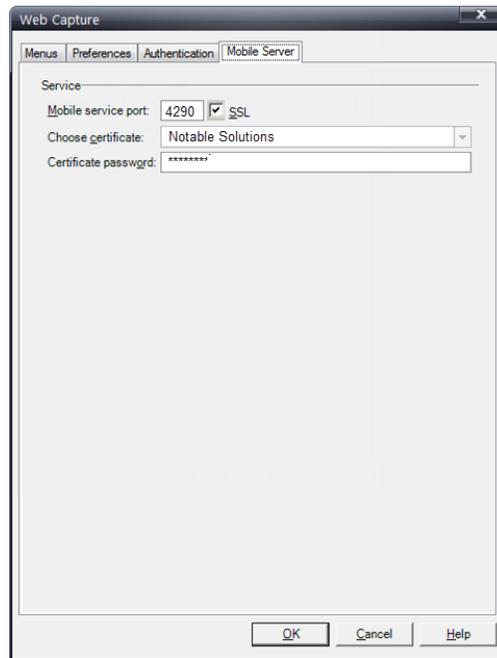


Figure 57. Specifying the certificate in Web Capture

7. Click **OK**, and restart the AutoStore Service.
8. On the NSi Mobile Server, open NSi Mobile Server Configuration Manager and on the AutoStore tab, verify that the connection to AutoStore has been successfully established.

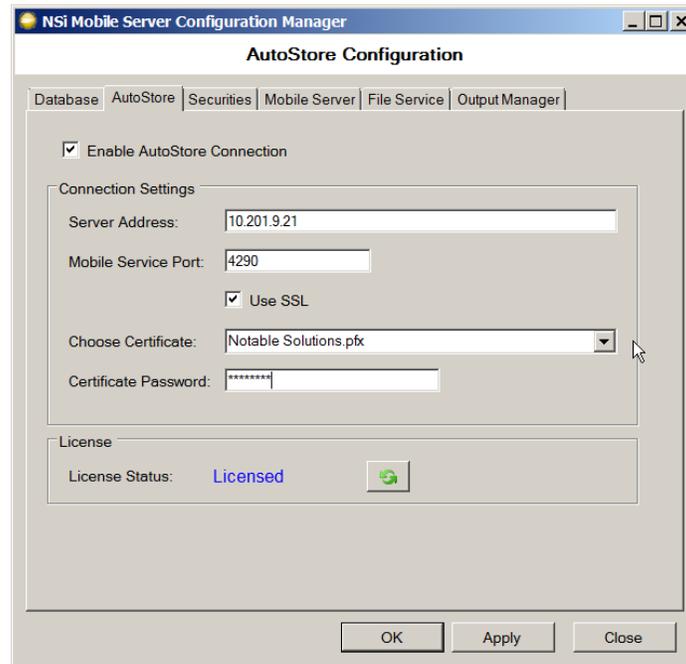


Figure 58. Verifying the SSL connection to AutoStore

CONFIGURING SSL FOR OUTPUT MANAGER

The following procedures describe how to configure NSi Mobile Server and Output Manager to communicate using SSL.

STEPS ON THE OUTPUT MANAGER SERVER

1. Start the Output Manager Server Configuration Utility (click **Start > NSi > Output Manager Server > OM Server Configuration**).
2. Click the **SSL Certificate Manager** tab.



SETTING UP SSL for NSi MOBILE

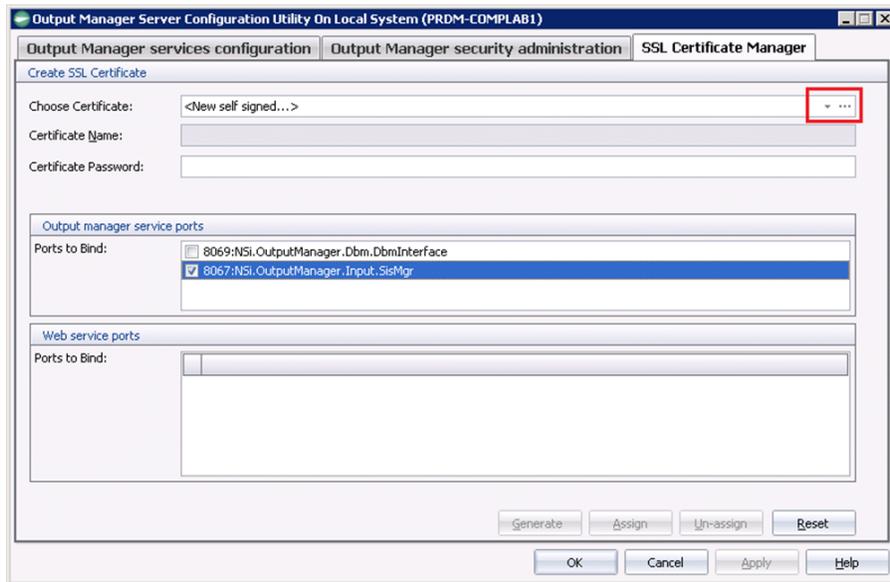


Figure 59. SSL Certificate Manager tab in the OM Server Configuration Utility

3. In the **Ports to Bind** box, select the **8067:NSi.OutputManager.Input.SisMgr** checkbox.
4. In the **Choose Certificate** box, select **<new self signed...>**.
5. Click the browse button (...) to open the **Browse for Folder** dialog box.

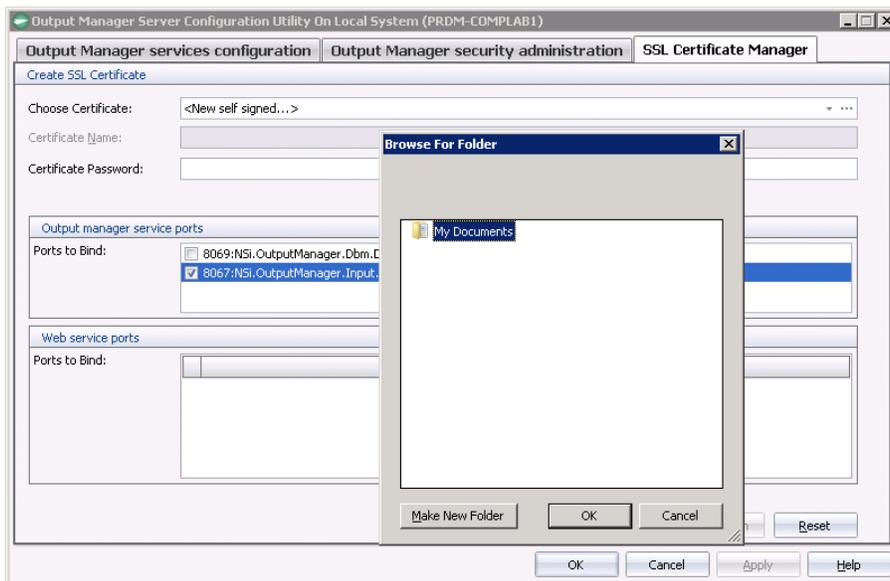


Figure 60. Specifying the certificate folder

6. Specify or create a folder under my documents, and click **OK**.
7. Enter and confirm the **Certificate Password**.



SETTING UP SSL for NSi MOBILE

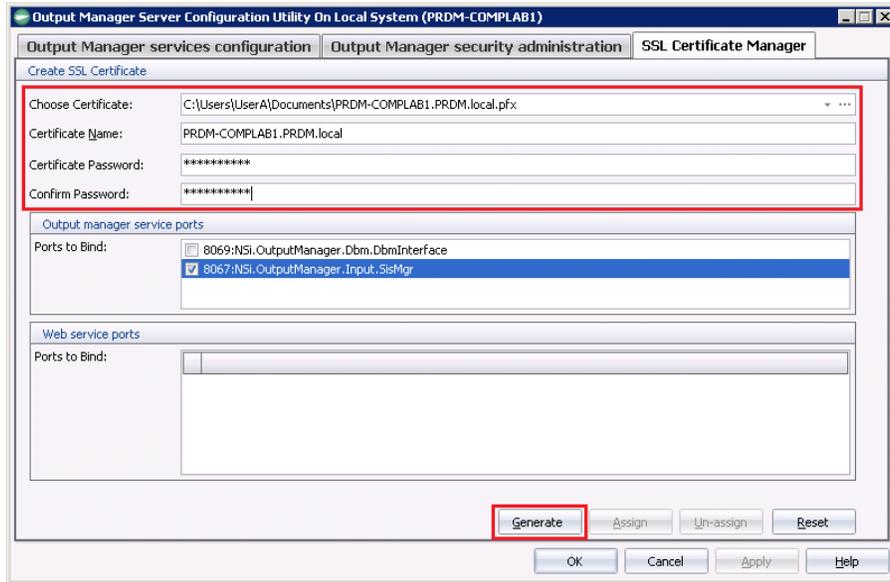


Figure 61. Generating the certificate

- 8. Click the **Generate** button.

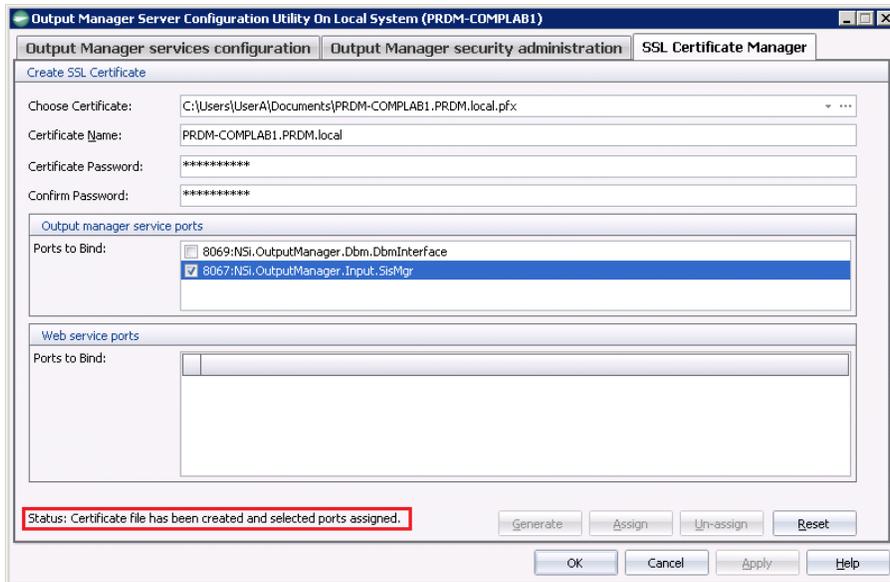


Figure 62. Verifying certificate generation

The **Status** message indicates the success or failure of the certificate generation.



SETTING UP SSL for NSi MOBILE

9. Navigate to the location specified by **Choose Certificate**, and copy the generated certificate file.

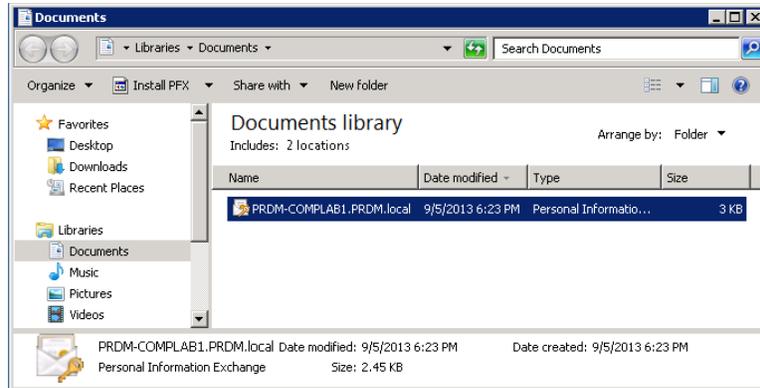


Figure 63. Copying the certificate file

10. Perform the following procedure to install this file on the Mobile Server.

STEPS ON THE NSI MOBILE SERVER

1. Save the certificate file on the Mobile Server (for example, C:\Certs\ABC.pfx)
2. On the **Start** menu, click **Run** and enter "mmc.exe" to start the Microsoft Management Console (MMC).
3. Click **File > Add/Remove Snap-in**.
4. In the **Available snap-ins** box, click **Certificates**, and then click the **Add >** button.

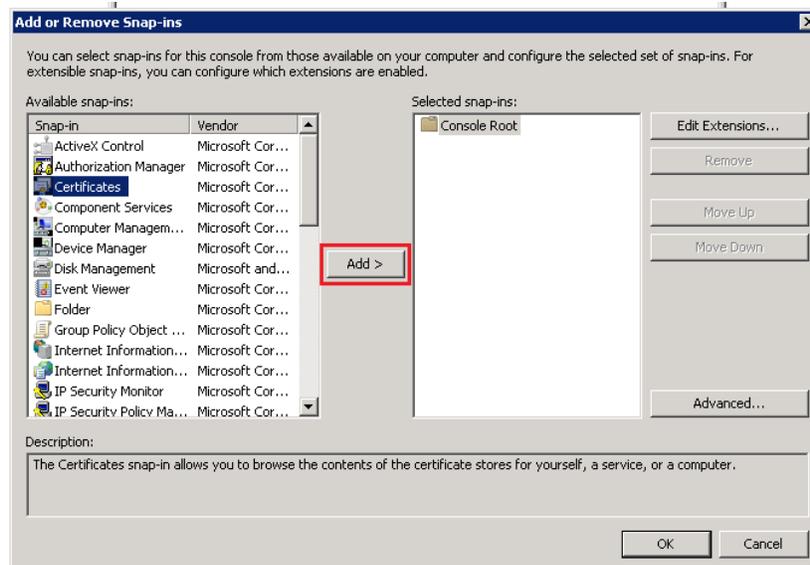


Figure 64. Adding the Certificates snap-in to the MMC console



5. In the **Certificates snap-in** dialog box, choose **Computer account**, and then click **Next**.

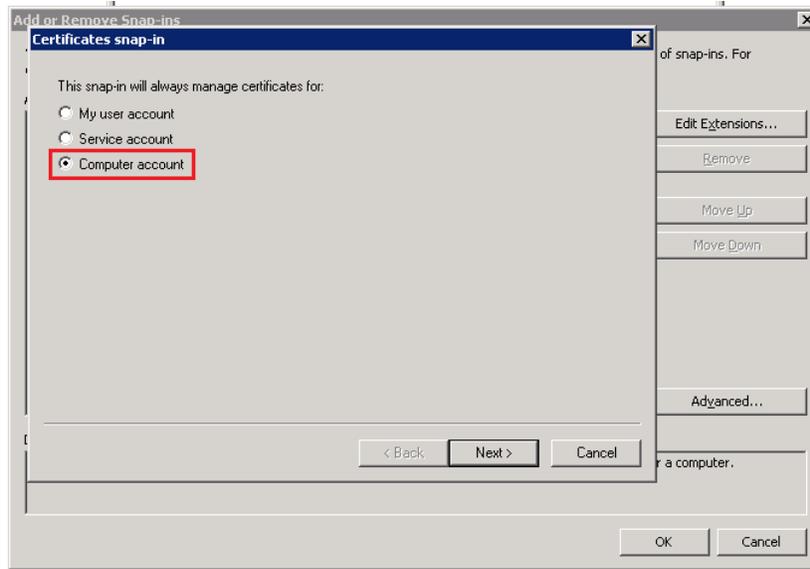


Figure 65. Specify that the Certificates snap-in manages Computer account

6. Click **Finish**.

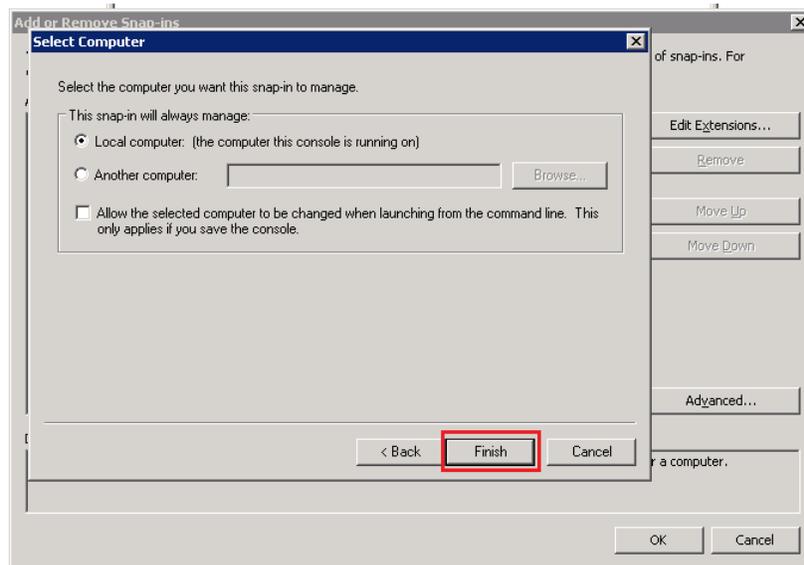


Figure 66. Completing configuration of the Certificates snap-in

7. In the Console Root tree, expand Certificates.



- Right-click "Trusted Root Certification Authorities", and on the shortcut menu, click **All Tasks > Import**.

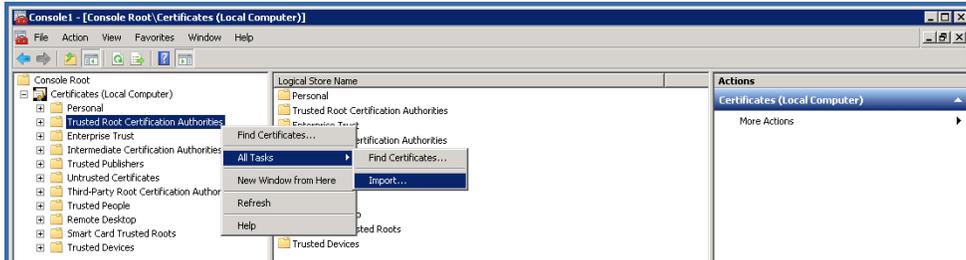


Figure 67. Importing the certificate to the store

- Select the certificate that you saved in step 1.

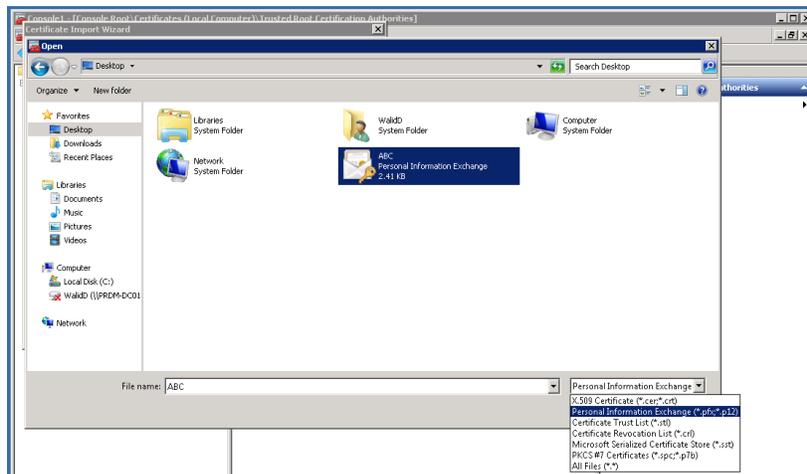


Figure 68. Selecting the certificate

- Enter the password that was used to generate the certificate on the Output Manager server.



SETTING UP SSL for NSi MOBILE

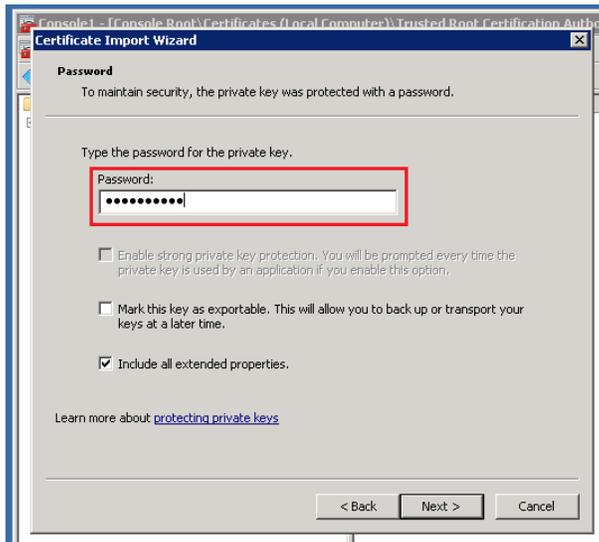


Figure 69. Specifying the certificate password

11. Make sure that the **Certificate store** is set to "Trusted Root Certification Authorities", and then click **Next**.

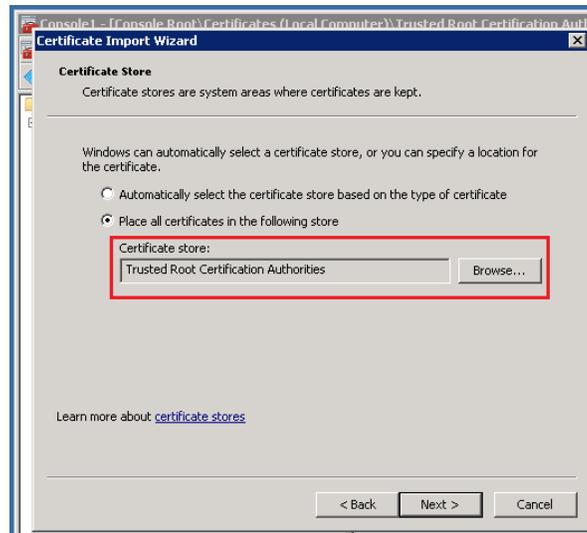


Figure 70. Confirming the certificate store

12. Navigate to the Certificates folder and make sure the generated certificate has been added.



SETTING UP SSL for NSi MOBILE

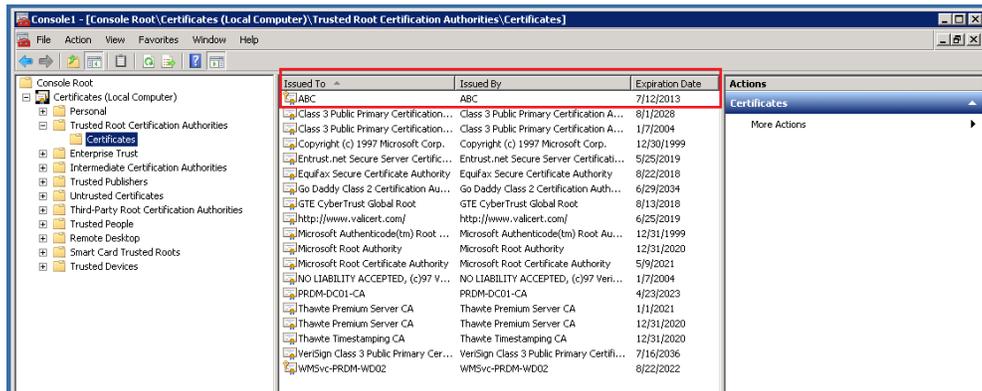


Figure 71. Confirm that the certificate has been added

13. Start the NSi Mobile Configuration Manager.
14. On the **Output Manager** tab, select the **Use SSL** check box.
15. In the **Service Port** box, enter the port number for the Output Manager service port that showed in the **Ports to Bind** box in the Output Manager **SSL Certificate Manager** settings (for example 8067:NSi.OutputManager.Input.SisMgr).
The default port is 8067.
16. Click the **Test Connection** button, to test the connection.

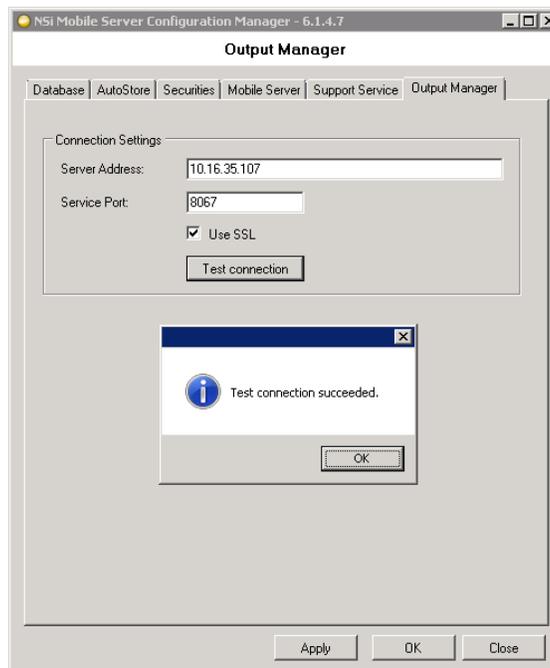


Figure 72. Testing the SSL connection to Output Manager

The message box displays whether the test connection was successful.



17. If the connection was successful, click **OK**, and restart the Mobile Server Web Service.

LICENSING

LICENSING A NEW INSTALLATION OF NSI MOBILE

1. Click **Start > All Programs > Notable Solutions > AutoStore 7 > AutoStore 7 Process Designer**.

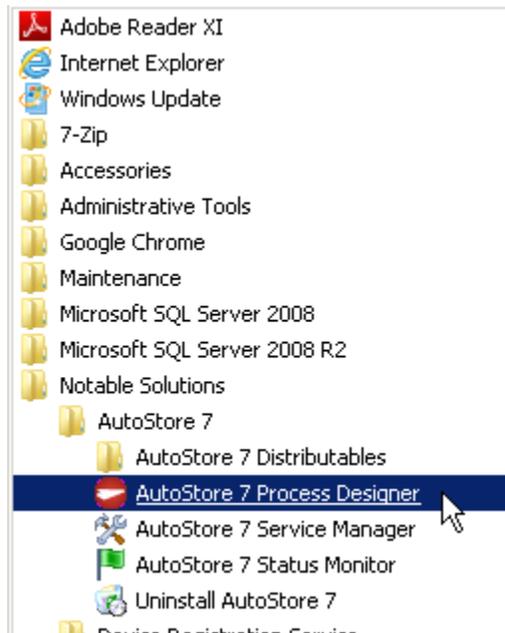


Figure 73. AutoStore Process Designer



2. Click **License Manager**.

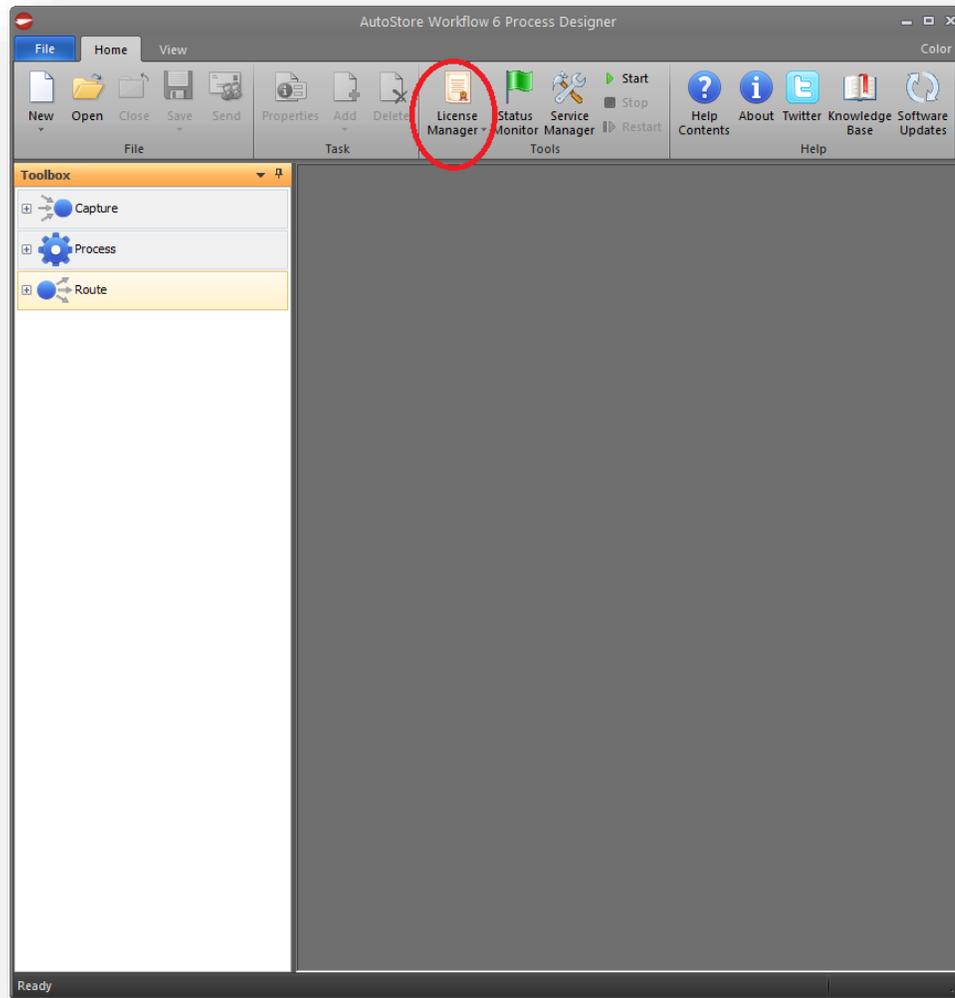


Figure 74. License Manager



3. The license for NSi Mobile is included as part of WebCapture.

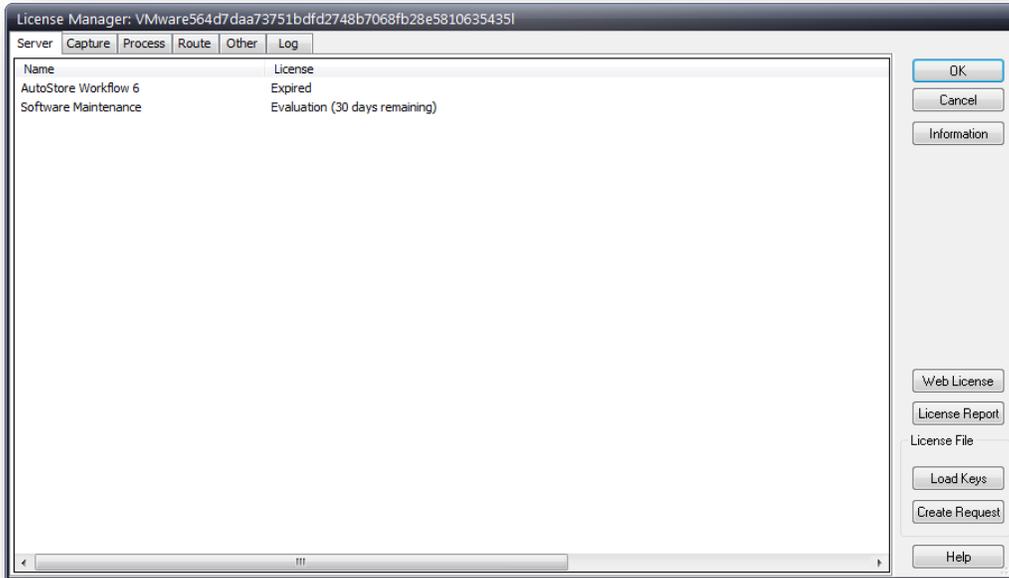


Figure 75. License Manager – Server licenses



4. The user must register online to receive a license. A request must first be created. Click **Create Request**.

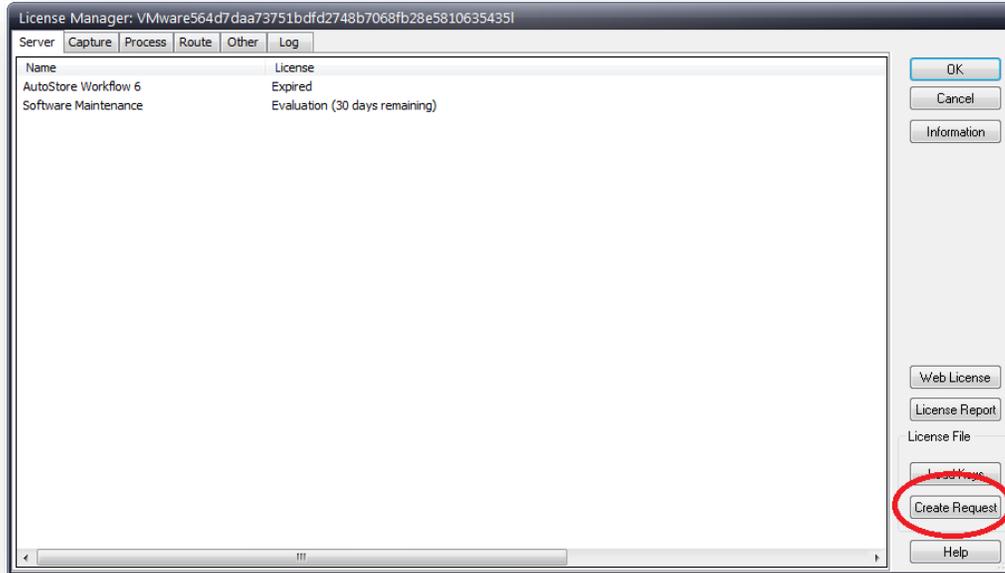


Figure 76. License Manager – Create NSi license request



5. Name and save the license file locally (selecting a file type is not required). Note the location of this file.

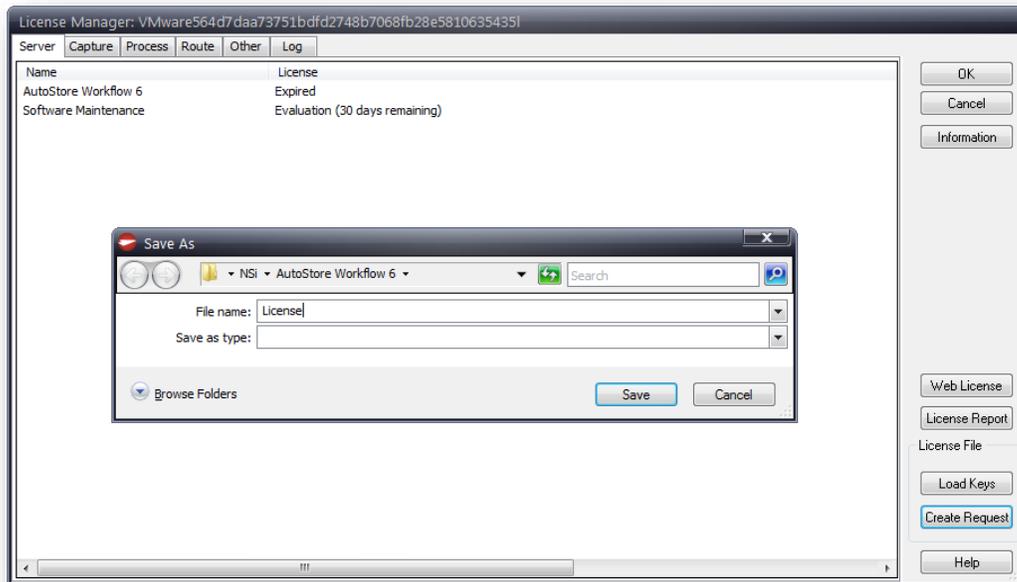


Figure 77. License Manager – Save the license request



6. Click **Web License**.

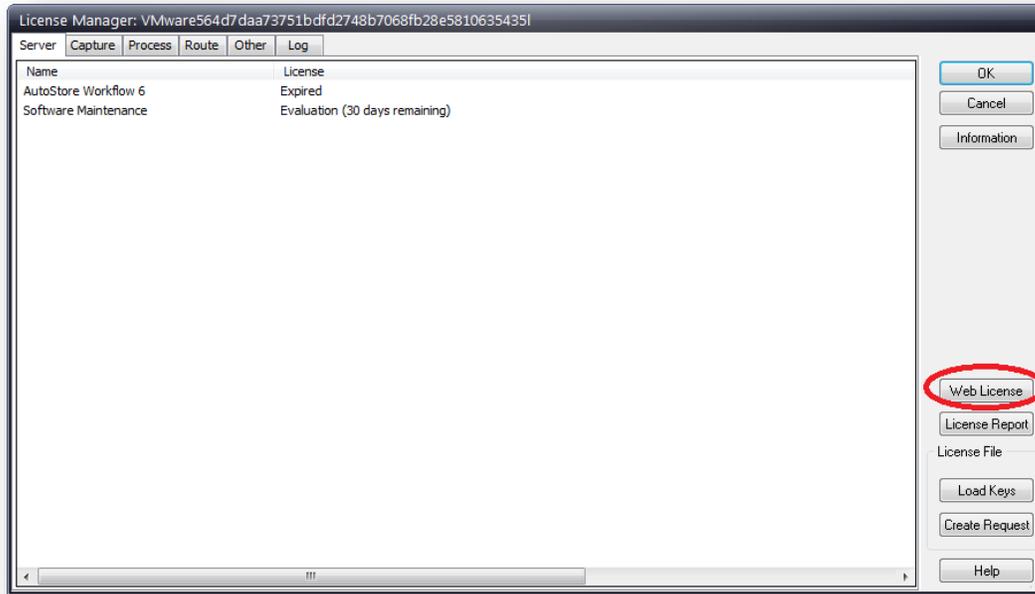


Figure 78. License Manager – Web License

7. You will be directed to the following website: <https://weblicense.nsius.com>. Enter your login information. If you have not previously registered, click **New User**.



Figure 79. NSi Web License Login



8. If you are a new user, enter your information.

Note: When you enter an email address, addresses from free email accounts such as Hotmail or Google will not be accepted. After you have filled out your information, click **Create My Account**.

Figure 80. Create New Account



9. You will receive a confirmation email.
10. Click the link in the email to confirm your account registration.
11. Return to the licensing website and login into your newly created account.

NSi Web License

Login

Email

Password

[Login >>](#) [Forgot Password](#)
[New User? Create account](#)

Figure 81. NSi Web License Login



12. Select license information:

- a. At **License Type**, select **Production** as the license type from the drop-down menu.
- b. At **License Request File**, browse and enter the location of the request file that was created.
- c. At **License/Activation Number**, enter a License/Activation Number.

The screenshot shows a mobile application interface titled "NSi Web License". At the top, there is a navigation bar with "Downloads" and "License Activation" (the latter is highlighted). Below this is a "License Activation" section with a dropdown menu for "License Type" set to "Production/NFR" and an information icon. The "Order and License Request" section contains a "License Request File" field with a "Choose File" button and "No file chosen" text, a "Server Friendly Name" field with "Server Nick Name" text, and a "License/Activation Number" field with "Order Number" text. A blue "Submit >>" button is at the bottom.

Figure 82. License Information



- 13. The next screen will show the list of available licenses. Select the available license for NSi Mobile Server. Then click **Submit**.

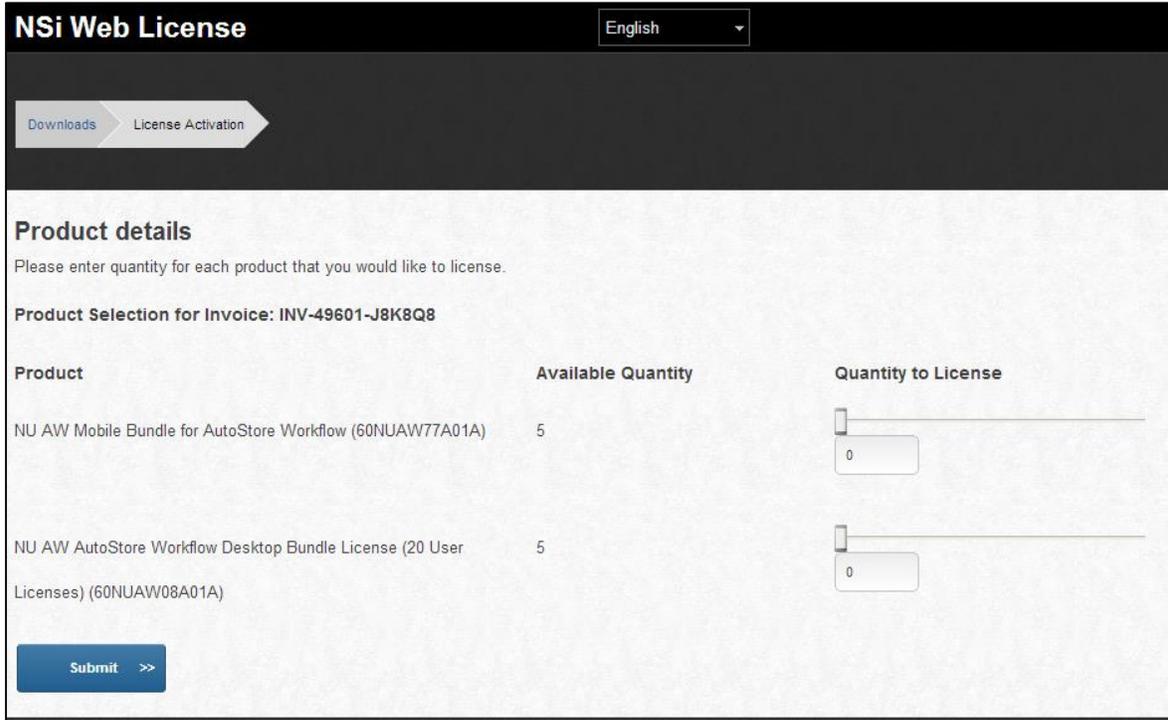


Figure 83. Submit

- 14. Click **Download License**.

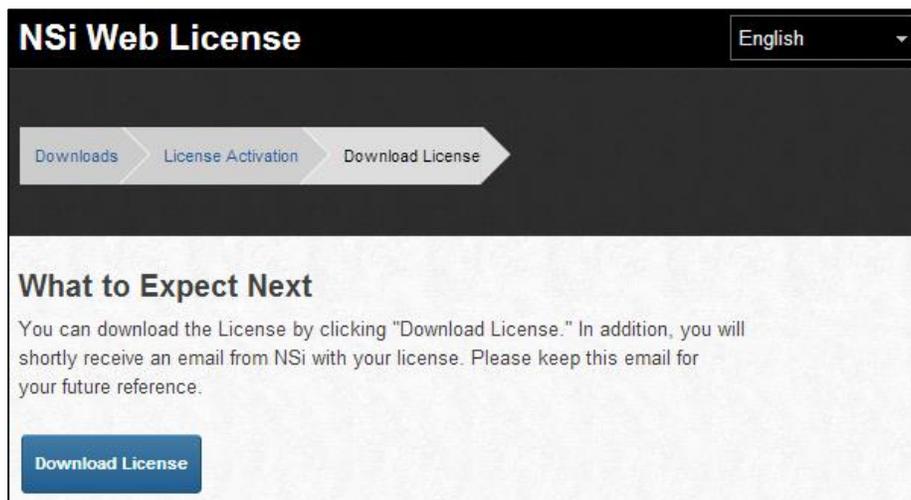


Figure 84. Click to Download



15. Save the file locally and note the location of this file.

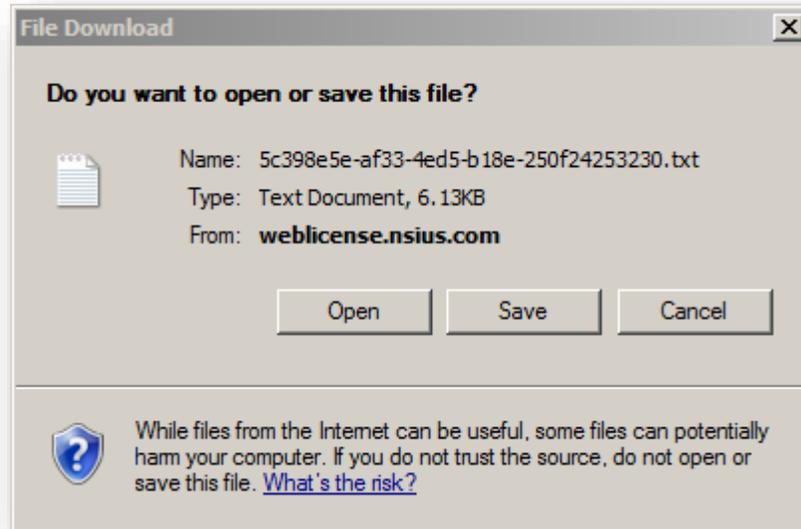


Figure 85. File Download



16. Open Process Designer, and click **License Manager** on the toolbar.

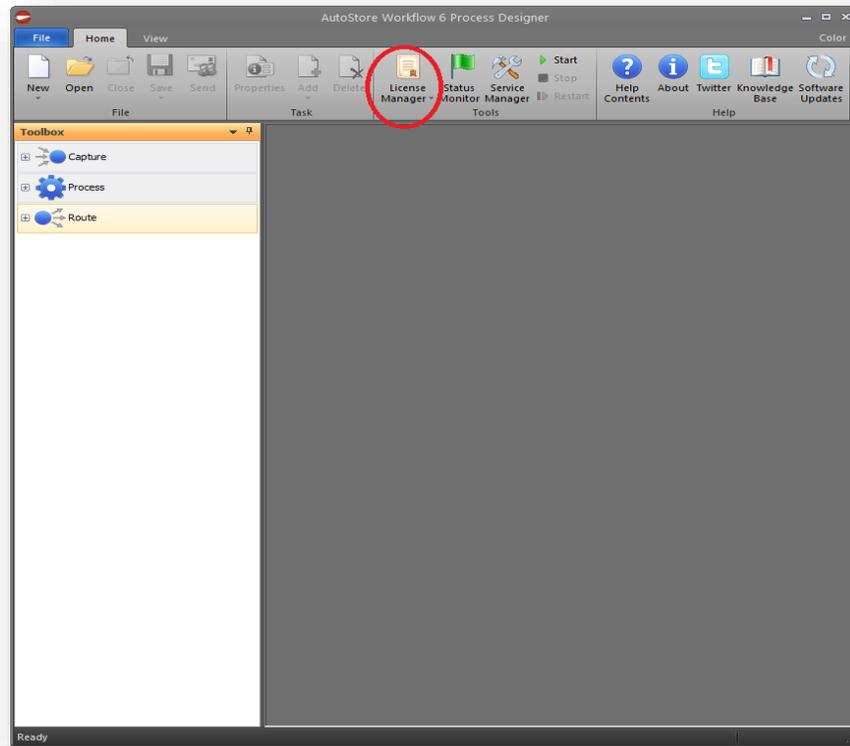


Figure 86. License Manager



17. Click **Load Keys**. Then select the location of the license file that was downloaded.

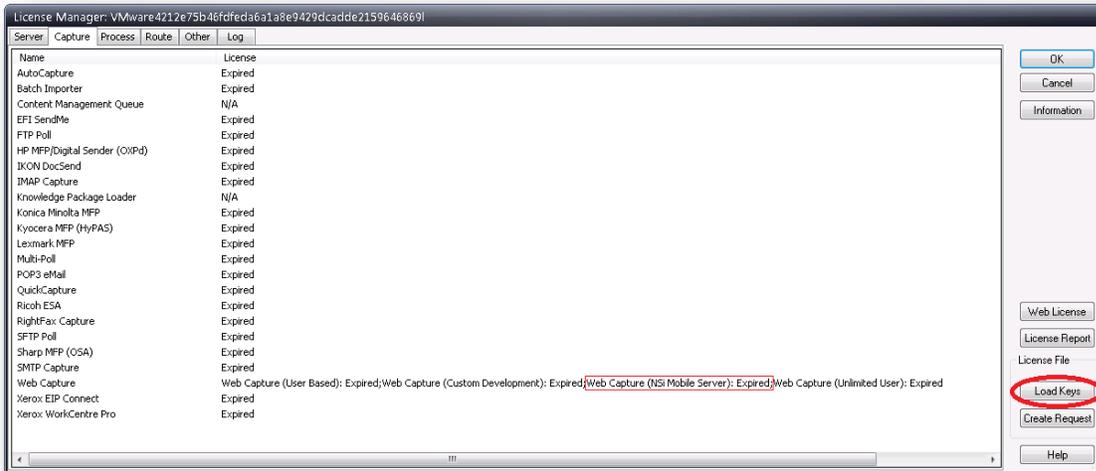


Figure 87. Load Keys

18. The new license status will be displayed for "Web Capture" on the **Capture** tab.

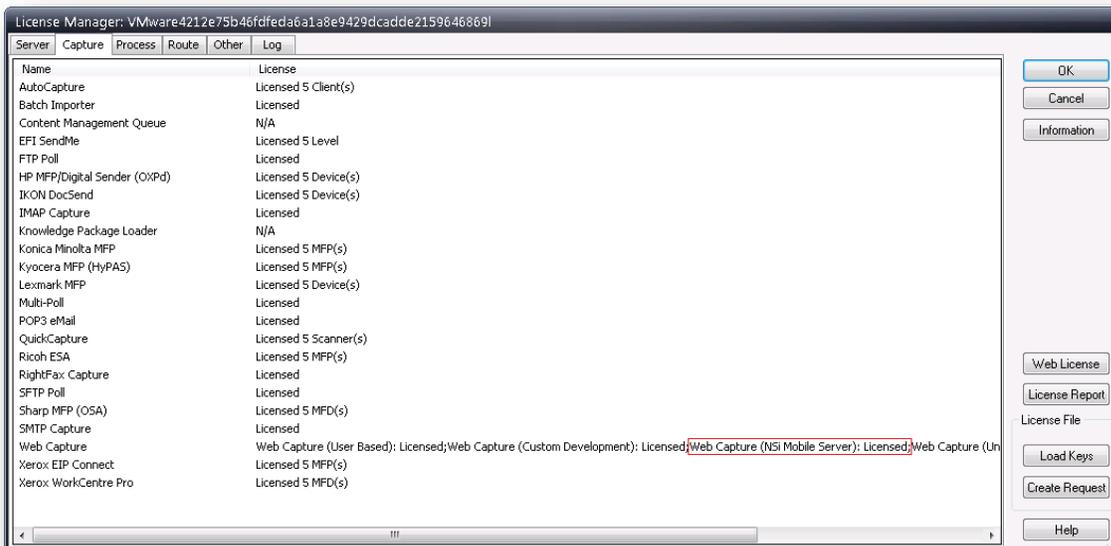


Figure 88. New License Status

6. Click **Finish** to complete the installation process.