Nuance Management Center

Server installation and configuration guide

For:

Nuance®
Dragon® Professional
Group

Nuance®
Dragon® Legal
Group

Nuance®
Dragon®
Law Enforcement

NUANCE

Copyright

Nuance ® Management Center

This material may not include some last-minute technical changes and/or revisions to the software. Changes are periodically made to the information provided here. Future versions of this material will incorporate these changes.

Nuance Communications, Inc. has patents or pending patent applications covering the subject matter contained in this document. The furnishing of this document does not give you any license to such patents.

Disclaimer

Nuance makes no warranty, express or implied, with respect to the quality, reliability, currentness, accuracy, or freedom from error of this document or the product or products referred to herein and specifically disclaims any implied warranties, including, without limitation, any implied warranty of merchantability, fitness for any particular purpose, or noninfringement.

Nuance disclaims all liability for any direct, indirect, incidental, consequential, special, or exemplary damages resulting from the use of the information in this document. Mention of any product not manufactured by Nuance does not constitute an endorsement by Nuance of that product.

Notice

Nuance Communications, Inc. is strongly committed to creating high quality voice and data management products that, when used in conjunction with your own company's security policies and practices, deliver an efficient and secure means of managing confidential information.

Nuance believes that data security is best maintained by limiting access to various types of information to authorized users only. Although no software product can completely guarantee against security failure, Dragon software contains configurable password features that, when used properly, provide a high degree of protection.

We strongly urge current owners of Nuance products that include optional system password features to verify that these features are enabled! You can call our support line if you need assistance in setting up passwords correctly or in verifying your existing security settings.

Published by Nuance Communications, Inc., Burlington, Massachusetts, USA

Visit Nuance Communications, Inc. on the Web at www.nuance.com.

10/31/2018

Contents

NMC Install and Configuration **1**

About this guide ..... **v**

Guide overview vi

Audience vi

Additional resources vii

Documentation vii

Training viii

Support viii

Chapter 1: Introduction **1**

About Nuance Management Center 2

Physical architecture 3

Chapter 2: Installation checklist **4**

Checklist—Planning the installation 5

Chapter 3: Preparing for your installation **7**

Software requirements—Server 8

NMC server and database server 8

NMC console 9

Hardware requirements—Server 11

Server installation prerequisites 12

Other considerations 13

Network bandwidth recommendations 13

Using a network traffic switch 13

Obtaining required server software 14

Opening required ports 15

Chapter 4: Installing the servers **16**

Installing SQL Server 17

Installing Nuance Management Center 18

Chapter 5: Post-installation tasks **24**

Installing and binding the SSL certificate 25

About certificates 25

Install the SSL certificate—Installing on the server 25

Install the SSL certificate—Installing on a load balancing switch 28

Testing and troubleshooting your SSL configuration 28
Verifying the NMS Platform service is running 30
Starting the NMS Platform service manually 30
Configuring your network switch 31
Logging in to the NMC console 32
Determining your database backup method 33
Configuring the Dragon client for use with Nuance Management Center 34
Chapter 6: Upgrading Nuance Management Center 35
About upgrading Nuance Management Center 36
Upgrading Nuance Management Center 37
Chapter 7: Preparing for your Active Directory single sign-on configuration 40
Single sign-on overview 41
Before you begin 42
Software requirements 42
Other requirements 42
Checklist—Planning the single sign-on setup 42
Creating an NMC console Administrator user for Active Directory 45
Setting the Active Directory connection string 46
Creating and configuring user accounts for single sign-on 47
Creating user accounts 47
Configuring user accounts 47
Running the SetSPN.exe Windows utility 48
About SetSPN.exe 48
Downloading SetSPN.exe 48
Executing SetSPN.exe 48
Chapter 8: Installing the Local Authenticator 49
About the Local Authenticator 50
Local Authenticator logs 50
Downloading the Local Authenticator 51
Creating organization tokens 52
Installing and binding the SSL certificate 53
About signed certificates 53
Install the SSL certificate 53
Testing and troubleshooting your SSL configuration 56
Installing the Local Authenticator 57
Editing the configuration file 61

Starting the Local Authenticator service 62
Appendix A: Database backups and data retention 63
About database backups 64
Disabling automatic database backups 64
About data retention 65

About this guide

Guide overview ..... **vi**
Audience vi
Additional resources ..... **vii**
Documentation vii
Training viii
Support viii

Guide overview

This guide contains installation and configuration instructions for on-premise NMC servers. It also contains instructions for configuring single-sign-on authentication, which you can implement regardless of whether you are hosting your own NMC server on-premise or using Nuance's cloud-hosted NMC server. Use the following table to determine the chapters that are applicable to you:

NMC server type	Applicable chapters
On-premise	All, except chapter 7
Nuance cloud-hosted	1, 6, 7 Also see "Opening required ports" on page 15 for information on opening port 443.

If you are using a Dragon desktop product with Nuance Management Center, you must install Dragon clients and configure them for Nuance Management Center when you have completed the server installation and configuration. For more information, see the *Dragon Client Installation Guide*.

Audience

This guide is intended for IT administrators, database administrators, and Dragon administrators whose responsibility is to perform the following:

- Install and configure an on-premise NMC server.
- Set up and manage single sign-on user authentication.
- Install and manage a SQL Server database.

This guide assumes you have experience in hardware configuration, software installation, database management, and networking.

Additional resources

The following resources are available in addition to this guide to help you manage your Dragon installation.

Documentation

Document	Description	Location
Dragon Group Citrix Administrator Guide	Hardware, software, and network requirements for deploying Dragon in a network of client computers that connect to a Citrix server to access published applications.	Dragon Support web site
Nuance Management Center Administrator Guide	Information on creating and maintaining objects and managing Dragon clients from the Nuance Management Center (NMC) console.	Dragon Support web site
Nuance Management Center Help	Instructions for configuring and managing the Nuance Management Center (NMC) console and Dragon clients.	When Nuance Management Center is open, click the NMC console Help button ().
Dragon client Help	Commands and instructions for dictating, correcting, and more with the Dragon client.	When Dragon is open, click the Help icon () on the DragonBar, and then select **Help Topics**.
Dragon Release Notes	New features, system requirements, client upgrade instructions, and known issues.	Dragon Help. Do the following: 1. When Dragon is open, click the Help icon () on the DragonBar, and then select **Help Topics**. 2. Click **Get started**. 3. Click **Dragon**

Document	Description	Location
		release notes.

Training

Nuance provides several training offerings, like webinars, demos, and online training courses. For more information, see the Nuance University web site:

https://www.nuance.com/about-us/nuance-university-training.html

Support

The Dragon Support web site provides many resources to assist you with your Dragon installation, like forums and a searchable knowledgebase. For more information on Support offerings, see the Dragon Support web site at:

https://www.nuance.com/dragon/support/dragon-naturallyspeaking.html

Chapter 1: Introduction

About Nuance Management Center 2
Physical architecture 3

About Nuance Management Center

Nuance Management Center allows Dragon administrators to manage all Dragon clients from a single central console. The Nuance Management Center (NMC) console allows you to do the following:

- Configure options for clients at the site and group level
- Centrally manage your Dragon product licensing
- Share data, like words and auto-text commands, with Dragon clients and across other Nuance products
- Audit user session events
- Monitor client usage and trends through reporting

You can choose to install, configure, and maintain your own Nuance Management Center (NMC) server on-premise, or you can use the Nuance cloud-hosted NMC server.

Physical architecture

Nuance Management Center is a standard Microsoft ASP .NET MVC web application that is hosted by Internet Information Services (IIS). The Nuance Management Center components include the following:

- **Nuance Management Center (NMC) server**—Stores application data, such as organizations, sites, groups, and users. It also stores transient data, such as log files.
- **Nuance Management Center (NMC) console**—Allows NMC administrators to create and manage objects, like groups and users, assign licenses, run reports, and more. The NMC console does not have permanent data storage. However, it does use a file share for temporary data storage to support file uploads and downloads.
- **Database instance**—Stores license information, partial speech profiles, application usage information, and audit data.
- **Dragon clients**—Users log in to their client computers where Dragon is installed and connect to your NMC server to access shared words and commands.

Initially, you install the NMC server, NMC console, and the database instance on the same server. However, you can optionally move your database instance to a separate database server after the installation. Your NMC server can be one of the following:

- A single physical machine (smaller installations)
- Multiple physical machines load-balanced by a network traffic switch (larger installations)

Chapter 2: Installation checklist

Checklist—Planning the installation 5

Checklist—Planning the installation

Use this checklist to perform your Nuance Management Centeron-premise installation.

❒	Task	Reference
❒	Ensure all system requirements have been met.	"Software requirements—Server" on page 8 "Hardware requirements—Server" on page 11
❒	Ensure all server installation prerequisites have been met.	"Server installation prerequisites" on page 12
❒	Review all other considerations.	"Network bandwidth recommendations" on page 13 "Using a network traffic switch" on page 13
❒	Obtain the required server software.	"Obtaining required server software" on page 14
❒	Ensure required ports are open.	"Opening required ports" on page 15
❒	Install SQL Server.	"Installing SQL Server" on page 17
❒	Install the SSL certificate.	"Installing and binding the SSL certificate" on page 25
❒	Install Nuance Management Center.	"Installing Nuance Management Center" on page 18
❒	Verify that the NMS Platform service is running.	"Verifying the NMS Platform service is running" on page 30
❒	If you're using multiple NMC servers, configure your network traffic switch.	"Configuring your network switch" on page 31

❒	Task	Reference
❒	Log in to the NMC console. If you're using a network traffic switch, ensure you access the NMC console using the name or address of the switch in the URL.	“Logging in to the NMC console” on page 32
❒	Determine your database backup method.	“Determining your database backup method” on page 33
❒	Install Dragon clients if you have not already done so, and then configure the clients for use with Nuance Management Center. **Applies to:** Dragon desktop products only	“Configuring the Dragon client for use with Nuance Management Center” on page 34

Chapter 3: Preparing for your installation

Software requirements—Server **8**
NMC server and database server 8
NMC console 9
Hardware requirements—Server **11**
Server installation prerequisites **12**
Other considerations **13**
Network bandwidth recommendations 13
Using a network traffic switch 13
Obtaining required server software **14**
Opening required ports **15**

Software requirements—Server

Ensure that your environment meets the following software requirements before installing Nuance Management Center.

NMC server and database server

The Nuance Management Center installation suite installs your NMC server and database instance on the same server by default. However, you can optionally move the database instance to a separate server post-installation. The following table provides software requirements for both scenarios.

Feature	NMC server	Database server	Combined NMC server and database server
Operating system	One of the following: • Microsoft® Windows Server 2008 R2, Service Pack 1, Service Pack 2 • Microsoft® Windows Server 2008 R2, 32-bit and 64-bit • Microsoft® Windows Server 2008 R2 64 bit Service Pack 2 • Microsoft® Windows Server 2012 • Microsoft® Windows Server 2012 R2 (64 bit) • Microsoft® Windows Server 2016 Ensure you have all current service packs installed.	One of the following: • Microsoft® Windows Server 2008 R2, Service Pack 1, Service Pack 2 • Microsoft® Windows Server 2008 R2, 32-bit and 64-bit • Microsoft® Windows Server 2008 R2 64 bit Service Pack 2 • Microsoft® Windows Server 2012 • Microsoft® Windows Server 2012 R2 (64 bit) • Microsoft® Windows Server 2016 Ensure you have all current service packs installed.	One of the following: • Microsoft® Windows Server 2008 R2, Service Pack 1, Service Pack 2 • Microsoft® Windows Server 2008 R2, 32-bit and 64-bit • Microsoft® Windows Server 2008 R2 64 bit Service Pack 2 • Microsoft® Windows Server 2012 • Microsoft® Windows Server 2012 R2 (64 bit) • Microsoft® Windows Server 2016 Ensure you have all current service packs installed.
Operating System com-ponents	Internet Information Services (IIS), version installed with each platform For information on versions that get installed, see https://support.microsoft.com/en-us/help/224609/how-to-obtain-versions-of-internet-	Internet Information Services (IIS), version installed with each platform For information on versions that get installed, see https://support.microsoft.com/en-us/help/224609/how-to-obtain-versions-of-internet-	Internet Information Services (IIS), version installed with each platform For information on versions that get installed, see https://support.microsoft.com/en-us/help/224609/how-to-obtain-versions-of-internet-

Feature	NMC server	Database server	Combined NMC server and database server
	information-server-iis.	information-server-iis.	information-server-iis.
Windows com-ponents	• Microsoft .NET Framework 3.5, including the ASP.NET component • Microsoft .NET Framework 4.5.2, including the ASP .NET component Both version 3.5 and 4.5.2 are required. Version 3.5 is required for some service tools and for Help installation. • Internet Information Services (IIS) 7, 7.5, or 8.0	None.	• Microsoft .NET Framework 3.5, including the ASP.NET component • Microsoft .NET Framework 4.5.2, including the ASP .NET component Both version 3.5 and 4.5.2 are required. Version 3.5 is required for some service tools and for Help installation. • Internet Information Services (IIS) 7, 7.5, or 8.0
Database	None.	• SQL Server 2012 or 2014	• SQL Server 2012 or 2014
Security	• SSL certificate, signed by a third party certificate authority Nuance Management Center does not support self-signed certificates. For more information on SSL certificates, see "Installing and binding the SSL certificate" on page 25.	None.	• SSL certificate, signed by a third party certificate authority Nuance Management Center does not support self-signed certificates. For more information on SSL certificates, see "Installing and binding the SSL certificate" on page 25.

NMC console

- Microsoft Internet Explorer 10 or 11, or latest version of Chrome or Edge
- Microsoft .NET Framework 3.5

- Microsoft .NET Framework 4.5.2

  Both version 3.5 and 4.5.2 are required. Version 3.5 is required for some service tools and for Help installation.

Hardware requirements—Server

If you're hosting your own Nuance Management Center (NMC) server and database server on-premise, ensure the servers meet the following hardware requirements.

For every 1,000 users:

- One Quad-Core physical server to host the SQL database, NMC server, and NMC console
    - **Processor**: Quad-Core 2 GHz CPU
    - **Minimum RAM**: 8 GB
    - **Core Application Disk Storage**: 4.0 GB for the NMC server
- **If using Roaming user profiles**: A server, separate machine, or RAID array to host the Master user profiles directory
    - **Processor**: Intel® Pentium 4® or later, or AMD Athlon 64 or later
        - **CPU**: 1 GHz minimum (2.4 GHz recommended)
        - **RAM**: 8 GB
        - **Cache**: 512 KB minimum L2 Cache (1 MB recommended)
- One Database Server
    - **Processor**: Dual-Core 2GHz CPU
    - **Minimum RAM**: 8 GB

Server installation prerequisites

Ensure you have the following available before installing Nuance Management Center.

Prerequisite	Additional Information
Local Administrator privileges	You must have Local Administrator privileges on the NMC server to install Nuance Management Center, as the installation process creates an IIS application.
NMS service user	Windows user account that runs the NMS service. Requirements: • Has **Log on as a service** rights to log on to your NMC server as a service • Has Local Administrator rights to enable the service to bind to port 443 and to ensure the service has write access throughout the file system • Has read/write/delete access to the NMS file share You provide this account name and password during the Nuance Management Center installation.
Database server and database user	During the Nuance Management Center installation, you'll need to select the database server to which you're installing, and the authentication method. Choose from: • Windows authentication • SQL Server authentication If you choose SQL Server authentication, you must provide the database user login and password. This user must have **dbcreator** privileges.
NMS file share location	• Used as temporary data storage by the NMC console to support file uploads and downloads. • Used as permanent data storage by the NMC server for application data, such as sites, groups, and users. • Used as transient data storage by the HIM system for log files and audio if you are a medical customer using the HIM reports.

Other considerations

Network bandwidth recommendations

Nuance recommends the following network bandwidth speeds for Nuance Management Center.

Number of clients	Minimum network speed
100	10 Mbps
>100	100 Mbps

Using a network traffic switch

If you have a large organization and you're implementing more than one NMC server, you can include a network traffic switch in your network to balance the load on the servers.

The following table describes the recommended settings for your device.

Component	Setting
Network Interface Card (NIC)—Gigabit cards	Automatic. Switches and gigabit cards must have the same setting.
Network Interface Card (NIC)—10/100Mb cards	Network link speed and duplex must be set the same on all servers, workstations, and other network equipment, or performance and recognition degradation could occur.
Network speed—100 Mbps	Full Duplex

Obtaining required server software

The following server software is required. You can obtain the software from microsoft.com.

- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 4.5.2

  > Both version 3.5 and 4.5.2 are required. Version 3.5 is required for some service tools and for Help installation.

- SQL Server 2012 or 2014
- One of the following:
  - Microsoft® Windows Server 2008, Service Pack 1, Service Pack 2
  - Microsoft® Windows Server 2008 R2, 32-bit and 64-bit
  - Microsoft® Windows Server 2008 R2 64 bit Service Pack 2
  - Microsoft® Windows Server 2012
  - Microsoft® Windows Server 2012 R2 (64 bit)
  - Microsoft® Windows Server 2016
- Internet Information Services (IIS), version installed with each platform

  For information on versions that get installed, see https://support.microsoft.com/en-us/help/224609/how-to-obtain-versions-of-internet-information-server-iis.

Opening required ports

You must open the following ports to allow communication between components.

Port	Location	Description
389 TCP	NMC server	Allows communication between the NMC server and your Active Directory, if you are using single sign-on authentication.
443	NMC server	Allows communication between Dragon clients and the NMC server. Also allows communication between NMC console workstations and the NMC server. You must open port 443 regardless of whether you are using the Nuance cloud-hosted NMC server or you're hosting your own NMC server on-premise.
1433 Custom	Database server	Allows communication between the NMC server and the database server if they are on separate physical machines.

Chapter 4: Installing the servers

Installing SQL Server 17
Installing Nuance Management Center 18

Installing SQL Server

Install SQL Server according to the product instructions. On the screens indicated below, specify the settings recommended for Nuance Management Center.

1. On the **Feature Selection** screen, select the following features:
    - **Database Engine Services**
    - **Management Tools – Basic**
    - **Management Tools – Complete**
2. On the **Instance Configuration** screen, ensure the **Default instance** option is selected.
3. On the **Server Configuration** screen, select **Use the same account for all SQL Server Services**.
    1. Enter the username and password of the Windows user account under which the SQL Server services should run. Use the same account as you're using for the NMS service user.

        > If your application server and database server are on the same physical machine, Nuance recommends using an account in a workgroup.

    2. Enter the password that other servers and clients on the Dragon network use to access the database.
4. On the **Database Engine Configuration** screen:
    - Add at least three user accounts to administer the SQL database, including the account you created to run all NMS services.
5. On the **Reporting Services Configuration** screen, select **Install the native mode default configuration**.
6. If the **Complete with failures** screen appears, save the log to a location where you can retrieve it.

    Nuance Technical Support can use this log file if any network issues arise.

Installing Nuance Management Center

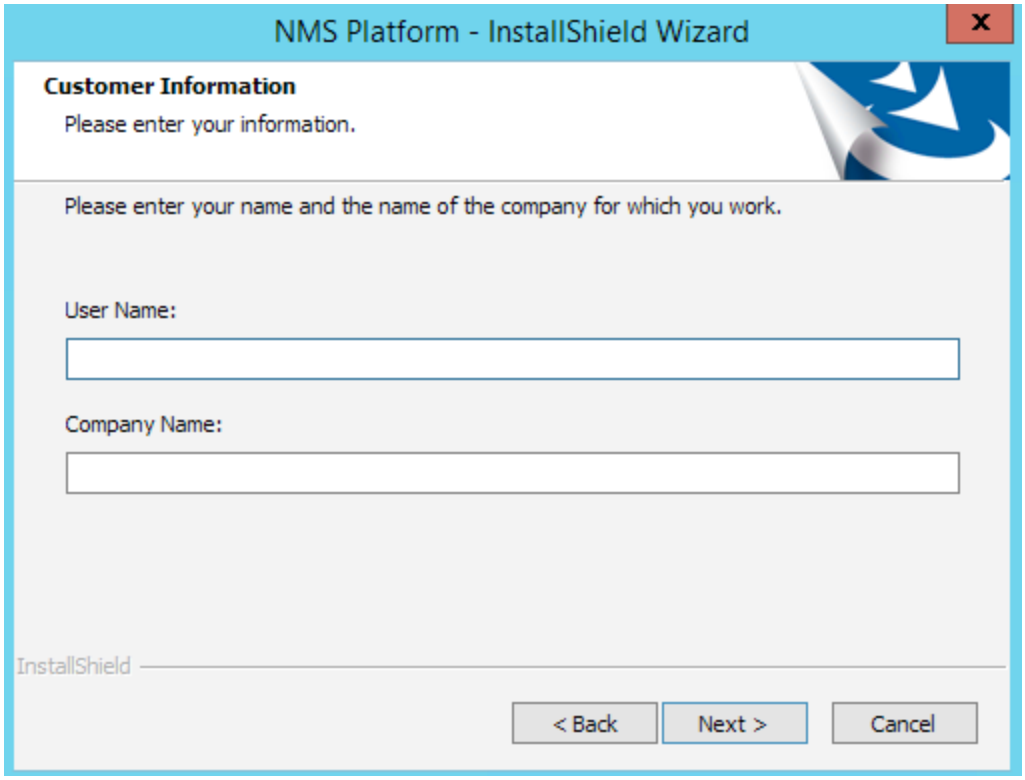
You install all Nuance Management Center components on the same machine using a single installation wizard. When the installation is complete, you can optionally move the database instance to a different server if your database server is a separate physical machine.

1. On the NMC server (for single-node installations) or each node (for multiple-node installations), run `NMS Suite Installer - Full.exe`.

   The installation wizard opens, and the **Choose Setup Language** screen appears.

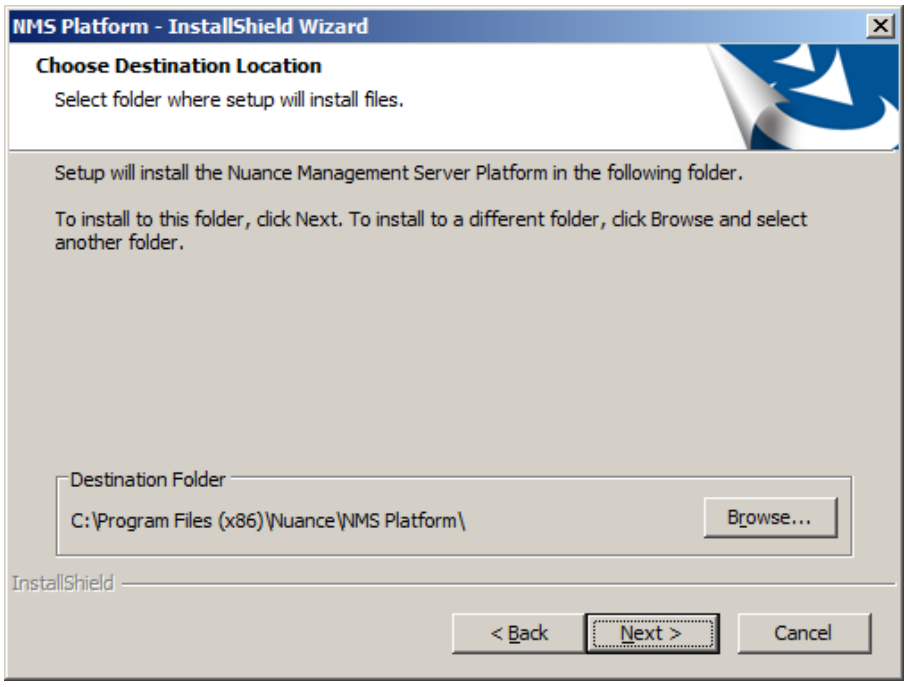
2. Select a language from the drop-down list, and then click **Next**.
3. Accept the license agreement, and then click **Install**.

   The wizard installs several components, and then the **Customer Information** screen appears.



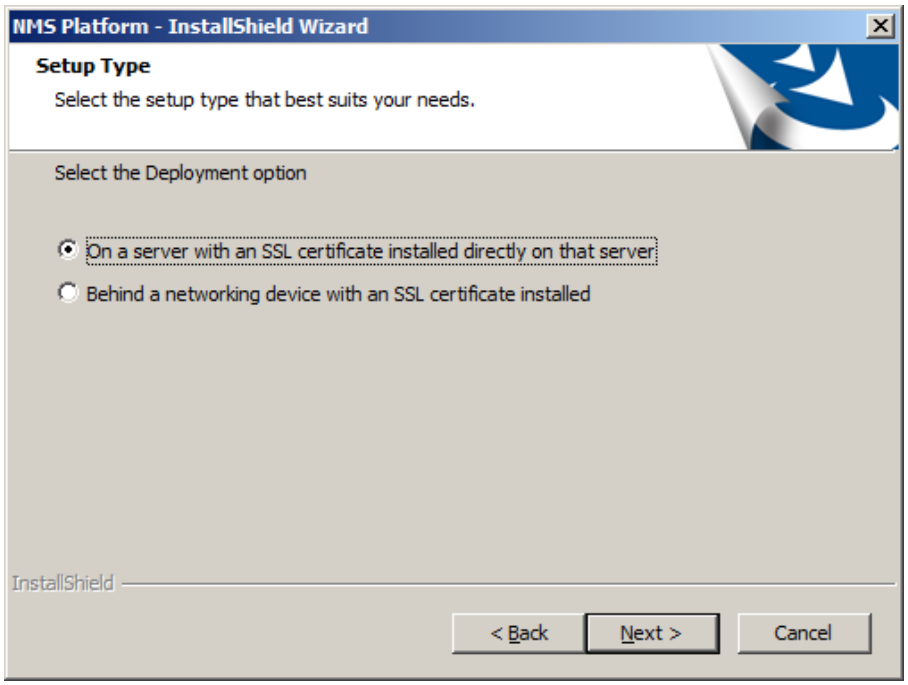
4. Enter a user name and company name, and then click **Next**.

The **Choose Destination Location** screen appears.



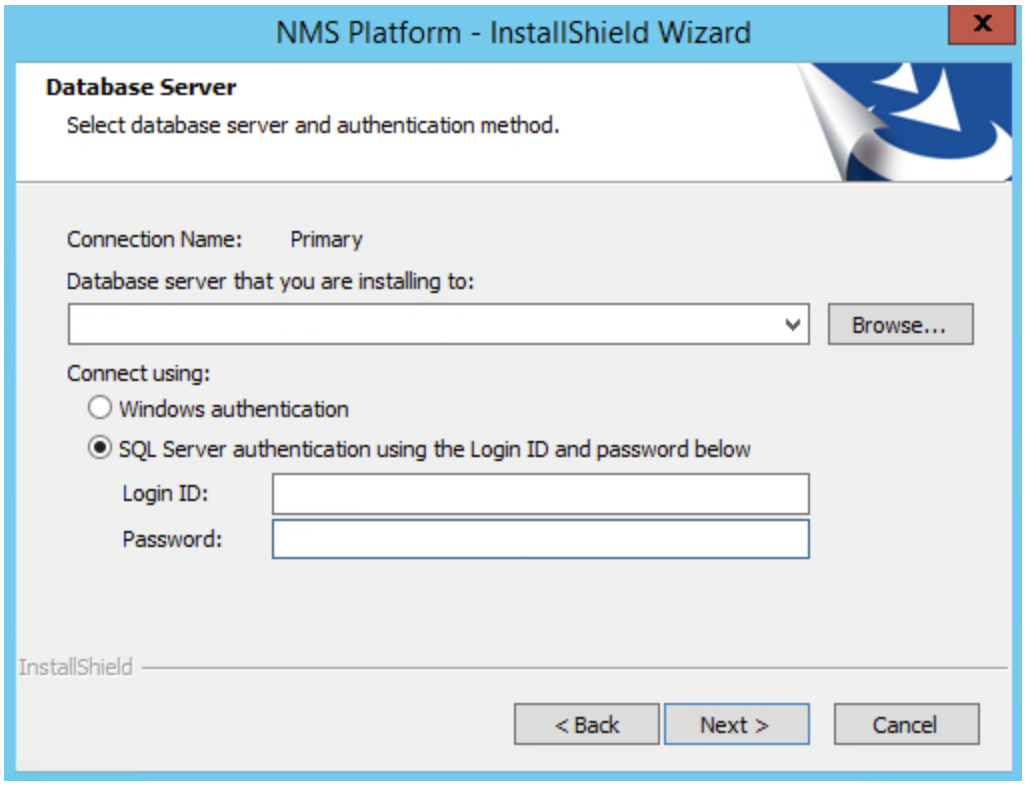
5. Choose where to install the NMS platform (default recommended), and then click **Next**.

   The **Setup Type** screen appears.



6. Choose a setup configuration:
   - **On a server with an SSL certificate installed directly on that server**—Select if you are performing a single-node installation.
   - **Behind a networking device with an SSL certificate installed**—Select if you are performing a multi-node installation.

Click **Next**. The **Database Server** screen appears.

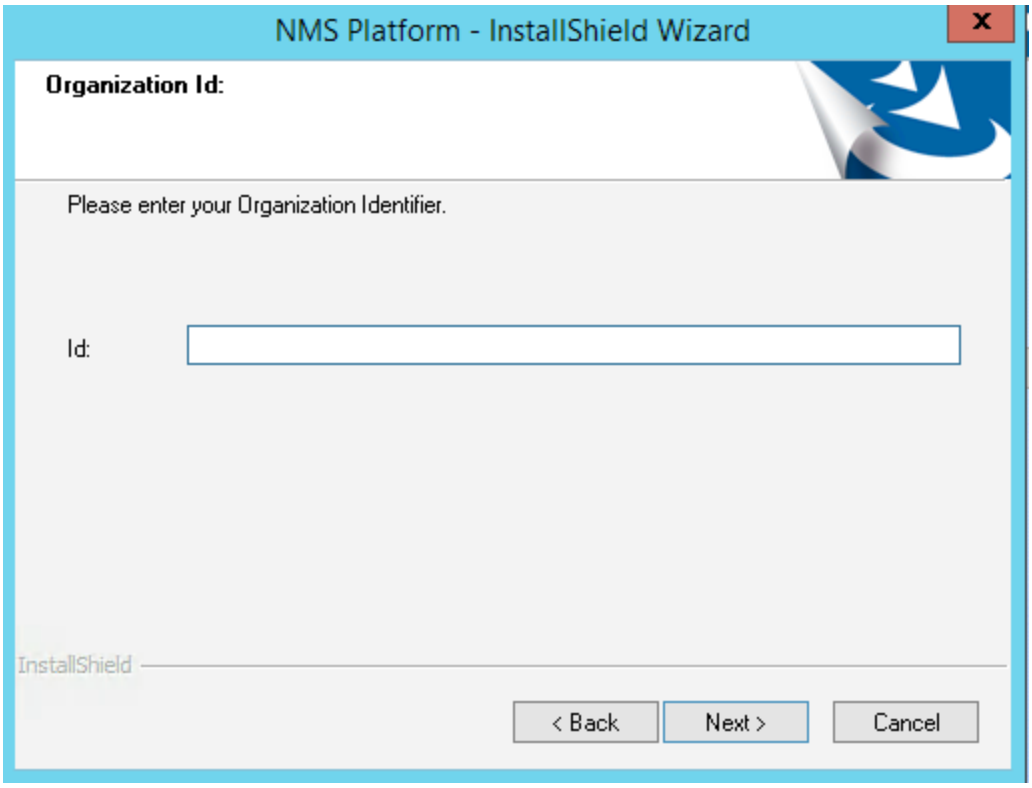


7. Enter the required database information:
    1. Enter the machine name or IP address of the physical server where you have installed the SQL database server software.

       The wizard creates the database and its backup directory in default locations on that server automatically.
    2. Select a method of validating connections to the server:
        - **Windows authentication**—Use a Windows login and password to authorize access.
        - **SQL Server authentication**—Use a SQL Server login and password.

       Choose the same type of authentication for access to the database that you chose when you installed SQL Server.
    3. If you selected SQL server authentication, enter the database administrator login name and password.
    4. Click **Next**.

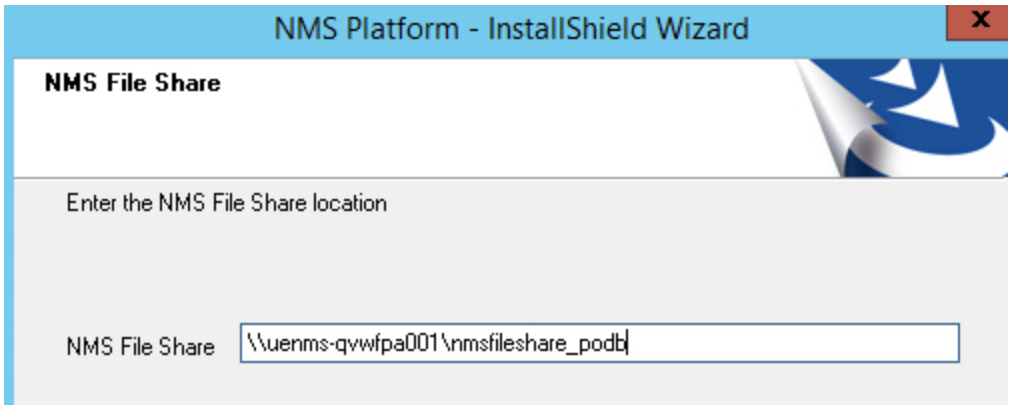
The Organization ID screen appears.



8. Enter the unique ID that Nuance assigned to your organization, and then click **Next**.

   You should have received this ID with your Dragon welcome information. Later, you can access your organization ID in the NMC console.

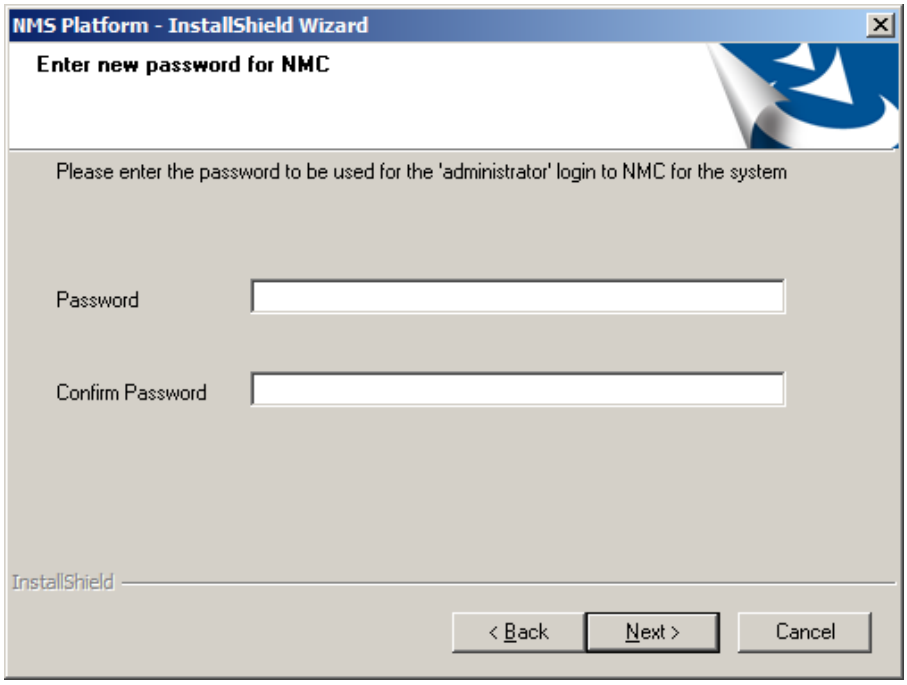
   The **NMS File Share** screen appears.



9. Enter the NMS file share location, and then click **Next**.

   For more information on the file share usage, see "Server installation prerequisites" on page 12.

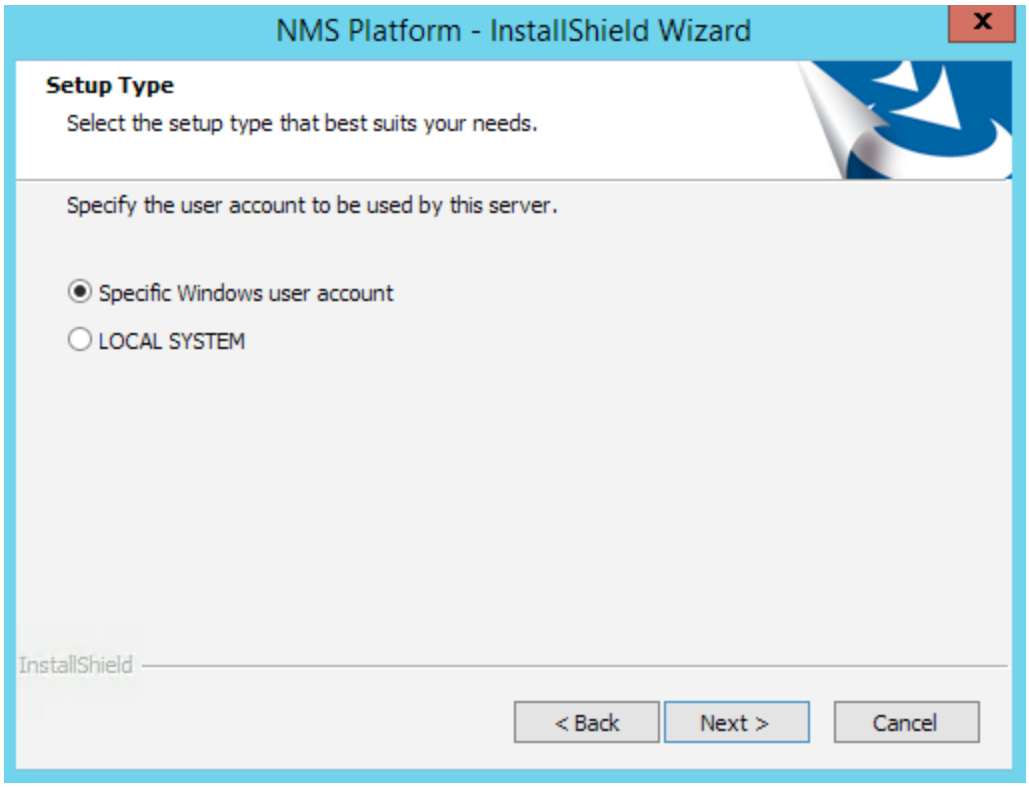
   The **Enter new password for NMC** screen appears.



10. Enter a password for the NMC administrator account, and then click **Next**.

    You use the administrator login (**admin** by default) and this password when you log into the NMC console.

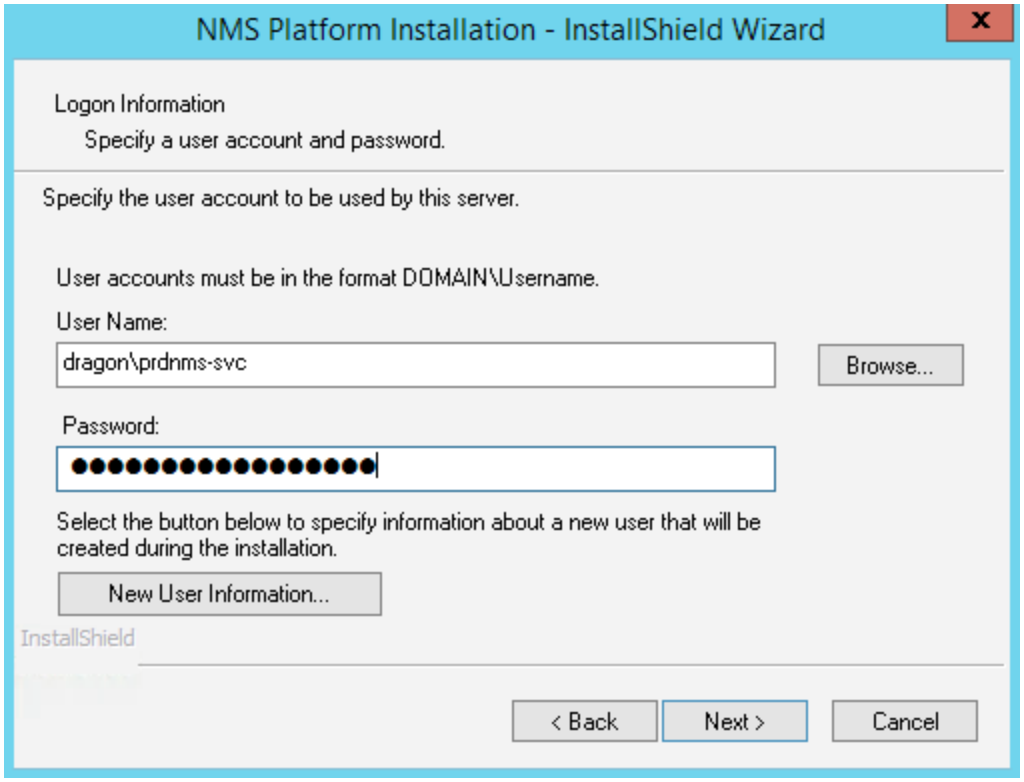
    The **Setup Type** screen appears.



11. Select the type of account to be used as the NMS service user, and then click **Next**.

- **Specific Windows user account**—A specific Windows user account that has rights to log on to your NMC server as a service. For more prerequisites for this account, see "Server installation prerequisites" on page 12.
- **LOCAL SYSTEM**—The predefined local account used by the service control manager.

The **Logon Information** screen appears.



12. Enter the user name and password of the Windows service user account, then click **Next**.

    The wizard installs the NMC console.

13. Click **Finish** when the installation is complete.
14. If the Windows Server firewall was turned on during the installation, you must now open port 443 to allow the NMC console to communicate with the NMS platform.

Chapter 5: Post-installation tasks

Installing and binding the SSL certificate **25**
About certificates 25
Install the SSL certificate—Installing on the server 25
Install the SSL certificate—Installing on a load balancing switch 28
Testing and troubleshooting your SSL configuration 28
Verifying the NMS Platform service is running **30**
Starting the NMS Platform service manually 30
Configuring your network switch **31**
Logging in to the NMC console **32**
Determining your database backup method **33**
Configuring the Dragon client for use with Nuance Management Center **34**

Installing and binding the SSL certificate

About certificates

Using SSL requires that you obtain a signed SSL certificate. Nuance Management Center does not support self-signed certificates. You can obtain signed certificates from certificate authorities, such as GoDaddy or Verisign. The certificate authority must be a trusted authority known to both the client computer and the server via a root certificate. To obtain a signed certificate, you'll need to provide information to the certificate authority about your organization and the server on which you are installing the certificate in the Certificate Signing Request (CSR). Each certificate authority may require different information. Typically, the information can include the following:

- Organization name
- Organization location information, such as town and state
- Computer name for the server on which you are installing the certificate
- Extended Key Usage value, such as 2.5.29.37. Extended key usage further refines key usage extensions, which define the purpose of the public key contained in the certificate.
- Key Size, such as 2048 bits or 4096 bits. Determines the length of the public key in the certificate. A longer key provides stronger security. You determine the level of security that is appropriate for your environment.

You obtain this information from your IT department, or from the person who installed and configured your server.

All SSL Certificates require a private key to work. The private key is a separate file that’s used in the encryption and decryption of data sent between your server and the connecting clients. A private key is created by you—the certificate owner—when you request your certificate with a Certificate Signing Request (CSR). The Certificate Authority providing your certificate (such as DigiCert) does not create or have your private key.

For more detailed information on installing SSL certificates, see:

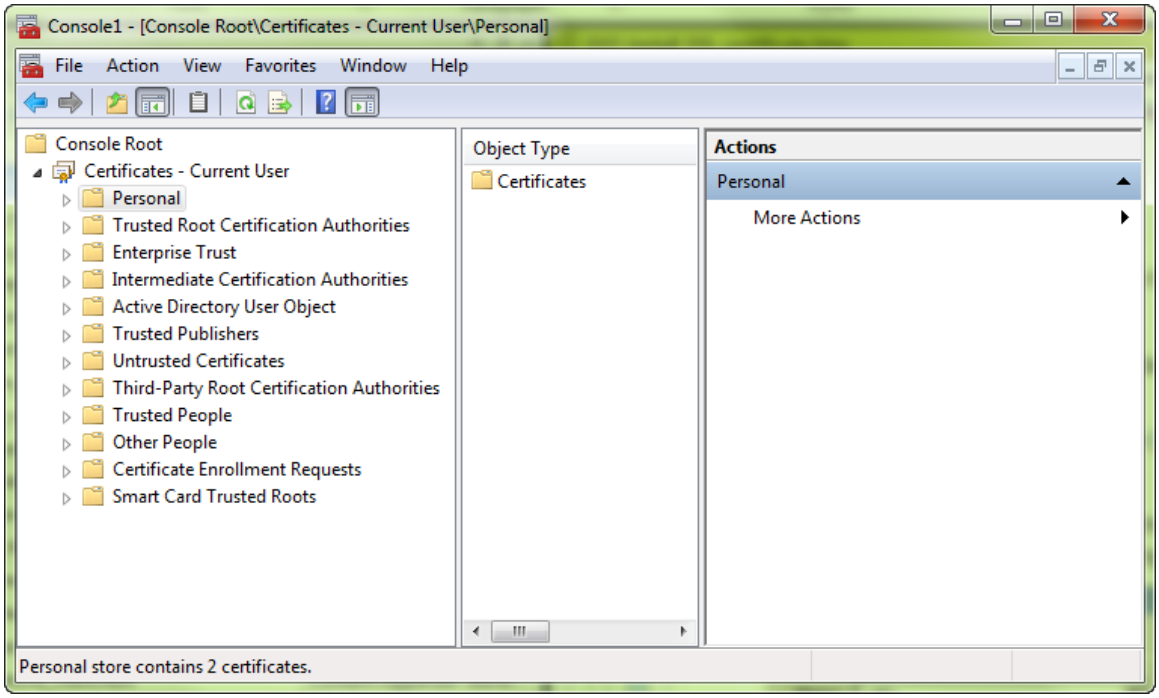
http://msdn.microsoft.com/en-us/library/ms733791.aspx

Install the SSL certificate—Installing on the server

Clients contact the NMC server on the standard HTTP ports 80 and 443.

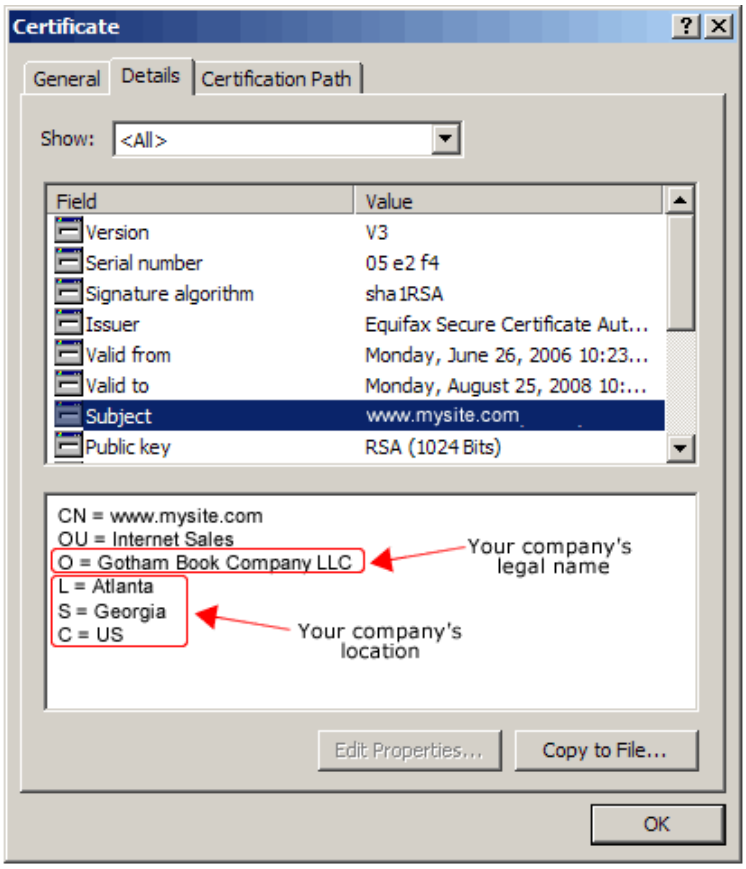
1. Install an SSL certificate in the Personal Store under the Local Computer section for the "logon as" user account under which the NMS service is running.

   To add the Certificates Snap-in and view the certificates installed on the local computer, see https://-technet.microsoft.com/en-us/library/cc754431(v=ws.11).aspx.



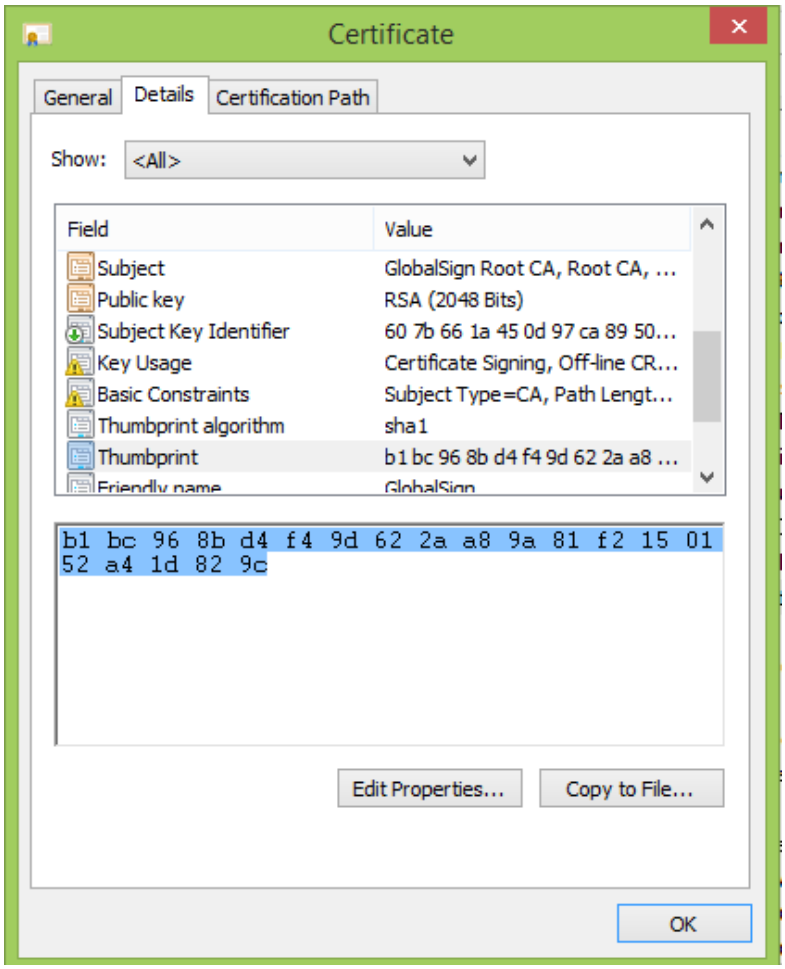
2. Note the subject of the certificate.

   This should match the computer name that the certificate is deployed on, or be a wild card. This must match exactly the host used in the endpoints. For information on viewing the subject, see https://-technet.microsoft.com/en-us/library/cc754686(v=ws.10).aspx.



3. Copy the thumbprint of the certificate. You use the thumbprint to bind the certificate to the port used by the primary NMS services in the next step.

   For information on retrieving the thumbprint, see https://msdn.microsoft.com/en-us/library/ms734695.aspx.



4. Verify that the `UseSSL` setting is set to true (this should have been done by the installer):
   a. In `Nuance.NMS.Server.exe.config`, located in the NMS Platform installation folder, find the line near the top that contains the `key="UseSSL"` tag.
   b. Change the `value` to `true`:

      ```
      <add key="UseSSL" value="true"/>
      ```

5. Bind the SSL certificate under IIS to port 443.
   a. In the IIS Manager, from the left panel, click **Default Web Site**.
   b. From the right panel, click **Bindings...**.

      The Site Bindings dialog box opens.
   c. Click **Add**.

      The Add Site Binding dialog box opens.
   d. From the **Type** drop-down list, select **https**.
   e. From the **SSL certificate** drop-down list, select the certificate that you installed.

f. Click **OK**.

The Site Bindings dialog box appears. Ensure that the binding is displayed correctly.

6. Restart the NMS Platform server to allow any configuration changes to take effect.

Install the SSL certificate—Installing on a load balancing switch

Nuance uses this mode when the NMC server is behind a load balancing switch that also decrypts SSL. In this scenario, the load balancing switch would strip the SSL encryption and forward the messages on to the appropriate NMC server. Inside the firewall, these messages would be unencrypted, and the NMC server would receive them as HTTP with no SSL encryption.

> This should only be configured by experienced networking personnel. It requires in-depth knowledge about load-balancing switches, which is outside the scope of this guide.

1. Verify that `UseSSL` is set to false (this should have been done by the installer):
   a. In `Nuance.NMS.Server.exe.config`, located in the NMC Platform installation folder, find the line near the top that contains the `key="UseSSL"` tag.
   b. Change the `value` to `false`:

   ```
   <add key="UseSSL" value="false"/>
   ```

2. Restart the NMC server to allow the configuration changes to take effect.

Testing and troubleshooting your SSL configuration

> Run these tests on a different computer. Do not run them on the NMC server.

Use the browser

1. Can you access and log into the NMC console?
   a. Connect to `https://<SERVER_NAME>/NMCHTML/`.

   If you see the Nuance Management Center login page, port 443 is working, and the NMC console is being deployed properly.

   b. Log in to the NMC console. If successful, the console is able to communicate with the server.
2. Can you access the NMC console status interface?
   1. Connect to `https://<SERVER_NAME>/NMS/Platform/ConfigurationSvc/v1/Status`.

   An XML response should appear in the browser.
3. Can you make RESTful web service calls?

   Attempt to create an NMS session using the browser.
   a. Connect to `https://<SERVER_NAME>/NMS/Platform/AuthenticationSvc/v1/ValidateCredentials?location=Test&productGuid=9D62C366-6F85-4C4C-9333-6FE21798D7F4`

   A prompt for a login and password appears.

   b. Use any valid NMC console login and password.
   c. If some XML is returned, the NMC console is configured properly and working with SSL.

4. Can you access the NMS API Help pages?
    1. Connect to `https://<SERVER-NAME>/NMS/Platform/UserManagementSvc/v1/help`
    2. Enter any credentials if prompted.
    3. An HTML page with help for one of the NMS API sets should appear. If you see this help, the NMC server is configured and working properly.

Check the Bindings

If the NMC console is not working, ensure that the ports are properly bound to the SSL certificate. To do this, specify the following from the command prompt:

```
netsh http show sslcert
```

Verify that port 443 is bound to the certificate.

Verifying the NMS Platform service is running

When the installation completes, the NMS Platform service starts automatically if the NMS service user has the correct privileges. Post-installation, you should verify that the service is running.

To verify, do the following:

1. Open the Services dialog box.
    a. Click the Windows Start menu.
    b. In the Search field, enter `services.msc`, and then press **Enter**.
    c. Specify your administrator username and password when prompted.
2. Locate the NMS Platform service.

    If the service is not running, you must start it manually.

Starting the NMS Platform service manually

Before starting the service manually, verify that the NMS service user has the correct privileges. For more information, see “Server installation prerequisites” on page 12.

If the account has the correct privileges, do the following to start the service manually:

1. Open the Services dialog box.
    a. Click the Windows Start menu.
    b. In the Search field, enter `services.msc`, and then press **Enter**.
    c. Specify your administrator username and password when prompted.

        The Services window opens.
2. Locate the NMS Platform service.
3. Right-click the service, and then select **Properties**.

    The NMS Platform Properties dialog box opens
4. From the **Startup type** drop-down list, select **Automatic**.
5. Click the **Start** button to start the service.
6. Click **OK**.

    The dialog box closes.

Configuring your network switch

If you have multiple NMC servers in your environment, you can use a network traffic switch to balance the incoming client activity among your servers. You can configure the switch to make an API call periodically to your servers to ensure they are operational.

Configure the switch to make the following API call:

```
https://<NMS-Server-Name>:443/Nuance.NMS.Services/
  NMSServiceStatus/Rest/Status
```

If operational, the NMC servers return the following XML response:

```
<ServiceStatusResponse xmlns=
"http://schemas.datacontract.org/2004/07/Nuance.NAS.Connector.
DictationTranscription" xmlns:i="http://www.w3.org/2001/
XMLSchema-instance">
  <Status>Running</Status>
  <ServerDateTimeUTC>2010-12-13T20:50:13.0969590Z
    </ServerDateTimeUTC>
  <InterfaceType>basicHttpTransport</InterfaceType>
</ServiceStatusResponse>
```

If the servers are down, the switch receives an error. If the switch receives anything other than the expected response, the switch can tag a specific server as down and reroute network traffic.

Logging in to the NMC console

Ensure you can log in to the NMC console using the administrator login and password.

If you have multiple NMC servers in your environment and you are using a network traffic switch to balance the load, ensure you substitute the name or IP address of the switch for the NMC server name in the URL when you access the NMC console.

1. Open a browser.
2. Enter the NMC console URL in the address bar.

   You should have received this address in your welcome email from Nuance. The URL is in the format: `https://<servername>/nmchtml`
3. Enter the following information:

   User Name: admin

   Password: The password you specified for the administrator account during the installation.
4. Click **Login**.

   The NMC console opens.

Determining your database backup method

The NMC server schedules database backups automatically. However, you can choose to manage database backups yourself and disable the automatic backups. You should determine your database backup method before users begin regular Nuance Management Center use.

For more information on Nuance Management Center database backups, see “About database backups” on page 64.

Configuring the Dragon client for use with Nuance Management Center

Applies to: Dragon desktop products only

When you have finished the NMC server installation and configuration, you must install Dragon clients if you have not already done so, and then configure the Dragon clients for use with Nuance Management Center.

For more information on configuring Dragon clients for use with Nuance Management Center, see the "Configuring the Dragon client for Nuance Management Center" chapter in the *Dragon Client Installation Guide*.

Chapter 6: Upgrading Nuance Management Center

About upgrading Nuance Management Center 36
Upgrading Nuance Management Center 37

About upgrading Nuance Management Center

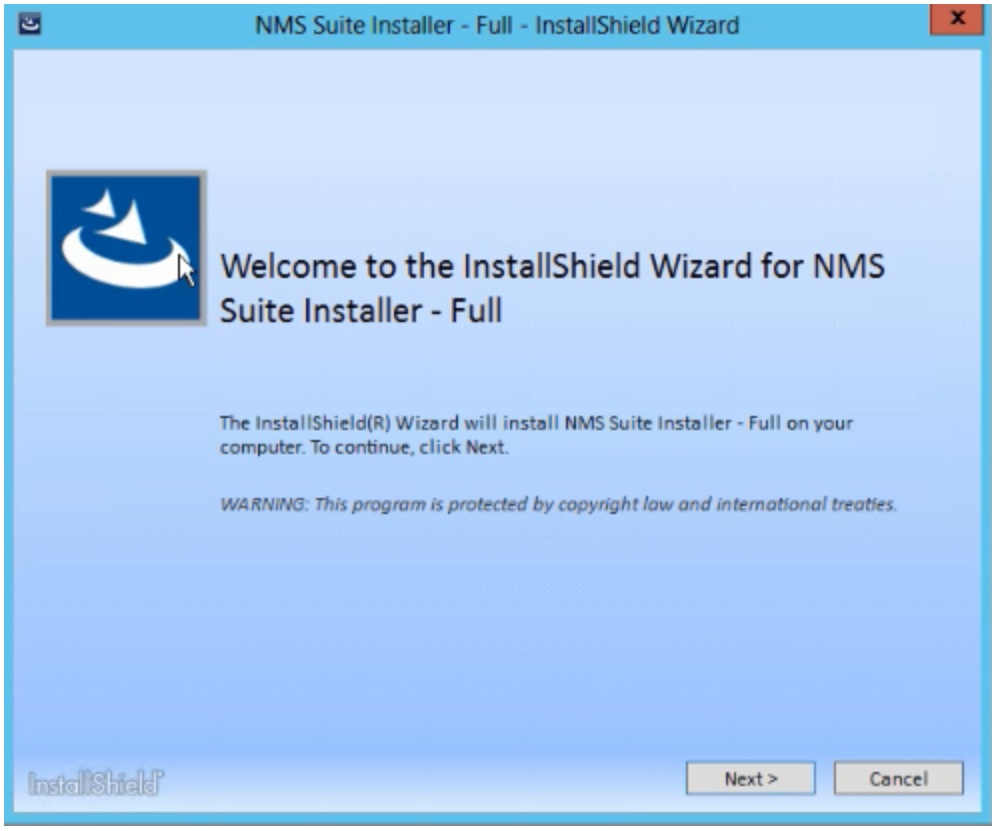
To upgrade Nuance Management Center, you run the `NMS Suite Installer - Full.exe` installation file on your NMC server. You must have Local Administrator privileges to launch the upgrade. The installer upgrades your existing version; you do not need to uninstall Nuance Management Center before you begin.

If you have multiple nodes, run the installer on each node.

Upgrading Nuance Management Center

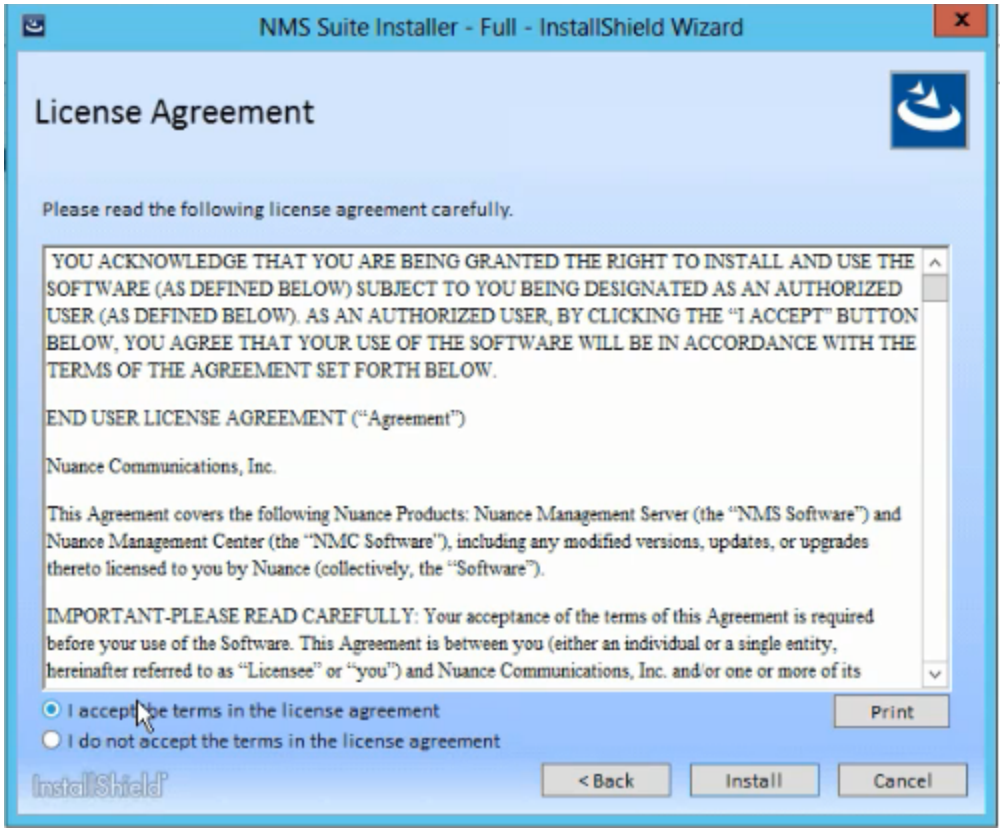
1. On your NMC server, right-click the `NMS Suite Installer - Full.exe` file, and then select **Run as administrator**.

   The InstallShield Wizard opens.



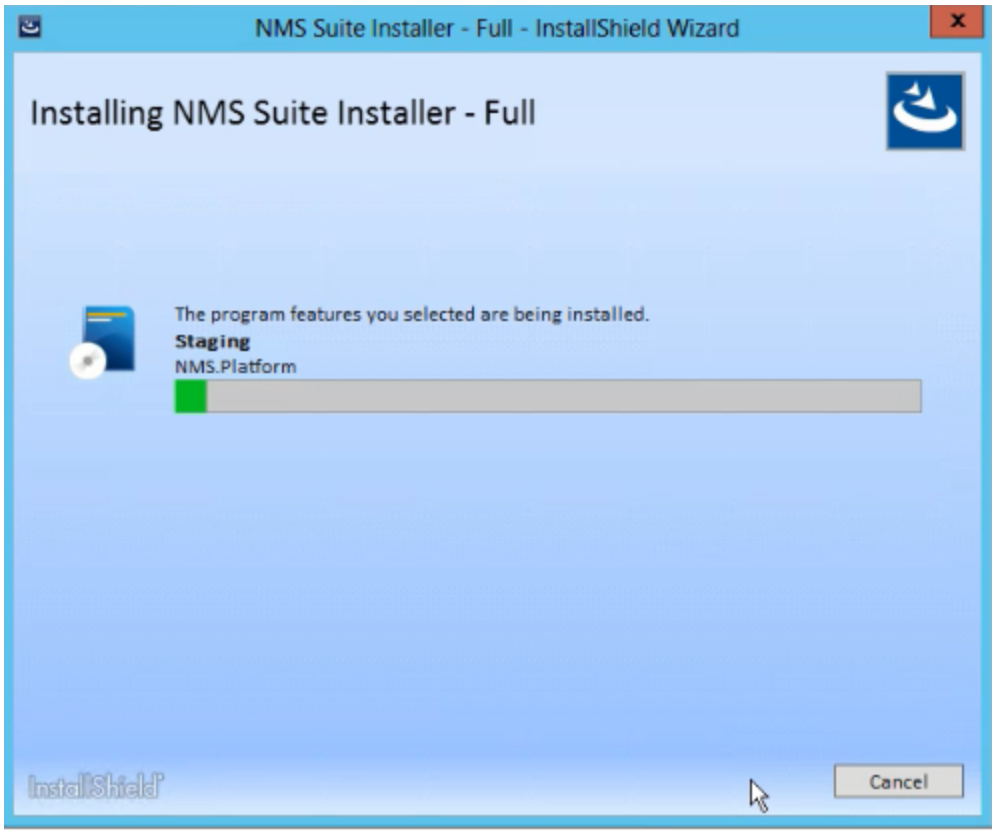
2. Click **Next**.

   The License Agreement screen appears.

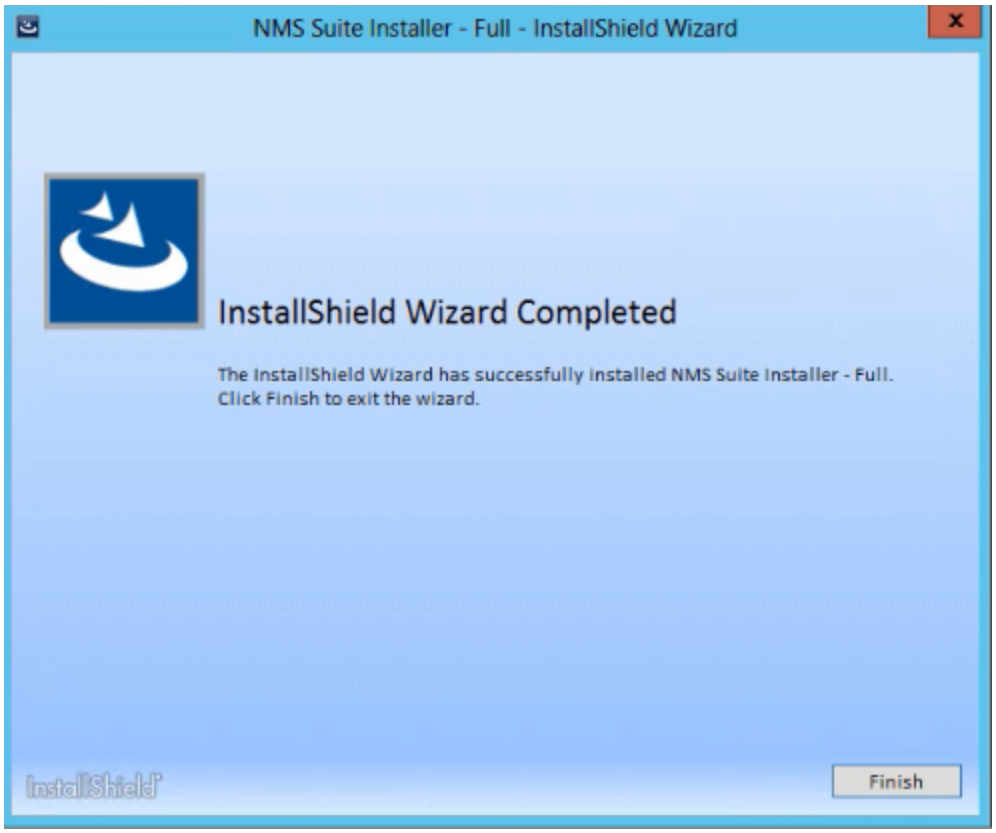


3. Select **I accept the terms in the license agreement**, and then click **Install**.

   The upgrade begins.



4. When the upgrade completes, click **Finish**.



Chapter 7: Preparing for your Active Directory single sign-on configuration

Single sign-on overview **41**
Before you begin **42**
Software requirements 42
Other requirements 42
Checklist—Planning the single sign-on setup 42
Creating an NMC console Administrator user for Active Directory **45**
Setting the Active Directory connection string **46**
Creating and configuring user accounts for single sign-on **47**
Creating user accounts 47
Configuring user accounts 47
Running the SetSPN.exe Windows utility **48**
About SetSPN.exe 48
Downloading SetSPN.exe 48
Executing SetSPN.exe 48

Single sign-on overview

You can optionally implement Active Directory single sign-on authentication rather than using the native Nuance Management Center authentication. With single sign-on, users can simply use their Windows login and password to access the Dragon client and other applications.

Ideally, you should decide to use single sign-on before you install Dragon clients, as you can configure some of the required settings during a batch or push install. However, it is possible to enable single sign-on after client installation.

Both on-premise customers and customers using the Nuance cloud-hosted NMC server can implement single sign-on.

Before you begin

Review the following before beginning your single sign-on configuration.

Software requirements

Cloud NMC server

- Local Authenticator service

  You download the Local Authenticator installation file from your NMC console. For more information, see "About the Local Authenticator" on page 50.

- Server on which to install the Local Authenticator with the following:
  - Latest version of the Microsoft .NET Framework installed
  - One of the following operating systems:
    - Microsoft® Windows Server 2008 R2, Service Pack 1, Service Pack 2
    - Microsoft® Windows Server 2008 R2, 32-bit and 64-bit
    - Microsoft® Windows Server 2008 R2 64 bit Service Pack 2
    - Microsoft® Windows Server 2012
    - Microsoft® Windows Server 2012 R2 (64 bit)
    - Microsoft® Windows Server 2016
- SSL certificate, signed by a third party certificate authority

  > Nuance Management Center does not support self-signed certificates.

On-premise NMC server

None. On-premise installations do not require the Local Authenticator for single sign-on.

Other requirements

- When you create user accounts in the NMC console, each user's login must match that user's Windows Domain login exactly.

  For more information on creating user accounts, see the *Nuance Management Center Administrator Guide*.

Checklist—Planning the single sign-on setup

If you're using single sign-on authentication, use these checklists to help you prepare for the configuration.

Cloud NMC server

If you're using the Nuance cloud-hosted NMC server, use this checklist to help you prepare for the configuration.

	Task	Reference
❐	Review software requirements	"Software requirements" on page 42

	Task	Reference
❒	Ensure port 389 TCP is open.	“Opening required ports” on page 15
❒	Create an NMC console administrator account for Active Directory	“Creating an NMC console Administrator user for Active Directory” on page 45
❒	Set the Active Directory connection string	“Setting the Active Directory connection string” on page 46
❒	Create and configure user accounts in the NMC console	“Creating and configuring user accounts for single sign-on” on page 47
❒	Run the SetSPN.exe Windows utility	“Running the SetSPN.exe Windows utility” on page 48
❒	Download the Local Authenticator	“Downloading the Local Authenticator” on page 51
❒	Create an organization token	“Creating organization tokens” on page 52
❒	Install and bind the SSL certificate on the Local Authenticator server	“Installing and binding the SSL certificate” on page 53
❒	Install the Local Authenticator	“Installing the Local Authenticator” on page 57
❒	Edit the Local Authenticator configuration file	“Editing the configuration file” on page 61
❒	Start the Local Authenticator service	“Starting the Local Authenticator service” on page 62
❒	Associate Dragon clients with the Local Authenticator **Applies to:** Dragon desktop products only	See the "Configuring the Dragon Client for Nuance Management Center" chapter in the *Dragon Client Installation Guide*. This step assumes you have already installed Dragon clients.

On-premise NMC server

If you're hosting your own NMC server on-premise, use this checklist to help you prepare for the configuration.

	Task	Reference
❒	Ensure port 389 TCP is open.	“Opening required ports” on page 15
❒	Create an NMC console administrator account for Active Directory	“Creating an NMC console Administrator user for Active Directory” on page 45
❒	Set the Active Directory connection string	“Setting the Active Directory connection string” on page 46
❒	Create and configure user accounts in the NMC console	“Creating and configuring user accounts for single sign-on” on page 47

	Task	Reference
❒	Run the SetSPN.exe Windows utility	“Running the SetSPN.exe Windows utility” on page 48
❒	Associate Dragon clients with the NMC server **Applies to:** Dragon desktop products only	See the "Configuring the Dragon Client for Nuance Management Center" chapter in the *Client Installation Guide*. This step assumes you have already installed Dragon clients.

Creating an NMC console Administrator user for Active Directory

To configure Active Directory single sign-on and manage settings, you must create an administrator user in the NMC console. You cannot use the initial NMC console login that Nuance provides (Nuance cloud-hosted NMC server) or the login that you create (on-premise NMC server). The administrator user must match a user that exists in Active Directory.

1. Log in to the NMC console.
2. From the Menu bar, select **User Accounts**.
3. In the **User Accounts** ribbon, click the **Add** icon.

   The **User Account Details** window opens.
4. Configure the following minimum settings:
   - **Details tab**—First Name, Last Name, and Login.
   - **Group Memberships tab**—Add the administrator to a group.
   - **Messaging tab**—Configure email settings to allow the administrator to receive messages from the NMC console.
5. Click **Save**.

Setting the Active Directory connection string

1. In the NMC console menu bar, click **Sites**, then click the **Organization Overview** icon. Click your organization, and then click the **Details** icon in the **Organizations** area.

   The **Organization Details** screen appears.
2. Click the **Domains** tab.
3. Click **Add**.

   The **Domain** dialog box appears.
4. Enter the following:

   Name—Your domain name. For example, **ABCCompany**.

   Active Directory connection strings—The Active Directory connection string. For example, **LDAP://nuance.com**.

   Ask your Active Directory domain administrator for the correct connection string. When Active Directory is enabled, Nuance Management Center sends all authentication requests to this server.
5. Click **Save**.
6. Repeat steps 3-5 as needed for each domain.

Creating and configuring user accounts for single sign-on

Creating user accounts

If you have not already created user accounts in the NMC console, you must create them before enabling single sign-on. When you create user accounts, each user's login must match that user's Windows domain login exactly.

On the User Account Details screen (click **User Accounts** in the menu bar, then click the **Add** icon), enter the user's Windows domain login name in the **Login** field:

For example, enter "John_Doe" in the **Login** field if the user's Windows domain login name is one of the following:

- "Domain\John_Doe"
- "John_Doe@domain.example.com"

Configuring user accounts

When you have created user accounts, do the following to add the users to your domain:

1. From the menu bar, click **User Accounts**.
2. Click **Search** to search for a user.
3. Specify search criteria, and then click **Search**.

   Search results appear.
4. Right-click a user, and then select **User Account Details**.
5. Click the **Credentials** tab.
6. Click the **NTLM** tab.
7. Click **Add**.

   The **New NTLM Credential** dialog box appears.
8. Select your domain from the **Domain** drop-down list.
9. Enter the user's Windows domain login in the **Login** field.
10. Click **Save**.

Running the SetSPN.exe Windows utility

About SetSPN.exe

SetSPN.exe is a Windows utility that registers the Nuance Management Center Service Principal Name (SPN) with the Windows domain. You run this utility to indicate to the Windows domain that the Nuance Management Center service is valid and trusted on the domain.

To authenticate using single sign-on, Dragon clients securely pass users' Windows credentials to the Nuance Management Center service. The credentials are then validated on the NMC server. Dragon clients cannot connect to Nuance Management Center until you register the SPN for the Nuance Management Center service.

You must run the utility for single sign-on authentication regardless of whether you're using the Nuance cloud-hosted NMC server or your own on-premise NMC server.

Downloading SetSPN.exe

SetSPN.exe is included with Microsoft's Windows Support Tools. If this package is not already installed on a computer in your domain, you can download it from Microsoft's web site:

https://social.technet.microsoft.com/wiki/contents/articles/2170.windows-server-2008-and-windows-server-2008-r2-support-tools-dsforum2wiki.aspx

Executing SetSPN.exe

You run the utility on any computer that is a member of the Windows domain you're using for your single sign-on users. You do not need to run the utility on the NMC server. You must be a domain administrator to run this utility.

You run the SetSPN.exe utility only once.

To run the utility, specify the following from the command line:

```
SETSPN -A http/nms_spn <computer name>
```

where `<computer name>` is the name of your NMC server.

Chapter 8: Installing the Local Authenticator

About the Local Authenticator **50**
Local Authenticator logs 50
Downloading the Local Authenticator **51**
Creating organization tokens **52**
Installing and binding the SSL certificate **53**
About signed certificates 53
Install the SSL certificate 53
Testing and troubleshooting your SSL configuration 56
Installing the Local Authenticator **57**
Editing the configuration file **61**
Starting the Local Authenticator service **62**

About the Local Authenticator

The Local Authenticator is a service that provides Dragon clients with Active Directory single sign-on authentication. The Local Authenticator validates Dragon client credentials when the clients attempt to connect to the Nuance cloud-hosted NMC server, and then passes the validate credential call to the cloud NMC server to create a session.

You must install the Local Authenticator to use single sign-on with the Nuance cloud-hosted NMC server. You do not need the Local Authenticator if you're hosting your own NMC server on-premise.

Install the Local Authenticator on a local server that is accessible to both the NMC server and your Dragon clients. You must have Administrator privileges on the server where you are installing the Local Authenticator.

For software system requirements for the Local Authenticator, see “Software requirements” on page 42.

Local Authenticator logs

The Local Authenticator uses the same service trace logs as Nuance Management Center. These logs can be found in:

```
C:\ProgramData\NMS\Logs
```

Downloading the Local Authenticator

You download the `LocalAuthenticator.exe` file from your NMC console. You then install the Local Authenticator on a local server that is accessible to both NMC server and your Dragon clients.

To download the Local Authenticator:

1. Log in to your NMC console as an administrator.
2. In the Utilities ribbon, click **Tools**.

   The Tools page appears.
3. Click **Install local authenticator**.

   A message appears, prompting you to save or run the Local Authenticator executable.
4. Click **Save**.

   The `LocalAuthenticator.exe` file is saved to your local Downloads folder.
5. Copy the `LocalAuthenticator.exe` file to the local server on which you are installing it.

Creating organization tokens

The Local Authenticator installation requires an organization token. You create a token in the NMC console.

To create an organization token:

1. From the menu bar, select **Sites** > **Organization Overview**.
2. Right-click your organization, and then select **Details**.

   The Organization Details page appears.
3. Click the Organization Token tab.
4. Click **Add** to generate a new organization token.

   The Organization Token Info dialog box appears. The **Organization Token** field is pre-populated with a system-generated token.
5. Optionally, enter a value in the **Comment** field.
6. Write down the token number.

   You must enter this number during the Local Authenticator installation.
7. Click **Save**.

   The new token appears in the **Organization Token** table.

Installing and binding the SSL certificate

About signed certificates

Using SSL requires that you obtain a signed SSL certificate. Nuance Management Center does not support self-signed certificates. You can obtain signed certificates from certificate authorities, such as GoDaddy or Verisign. The certificate authority must be a trusted authority known to both the client computer and the server via a root certificate. To obtain a signed certificate, you'll need to provide information to the certificate authority about your organization and the server on which you are installing the certificate in the Certificate Signing Request (CSR). Each certificate authority may require different information. Typically, the information can include the following:

- Organization name
- Organization location information, such as town and state
- Computer name for the server on which you are installing the certificate
- Extended Key Usage value, such as 2.5.29.37. Extended key usage further refines key usage extensions, which define the purpose of the public key contained in the certificate.
- Key Size, such as 2048 bits or 4096 bits. Determines the length of the public key in the certificate. A longer key provides stronger security. You determine the level of security that is appropriate for your environment.

You obtain this information from your IT department, or from the person who installed and configured your server.

All SSL Certificates require a private key to work. The private key is a separate file that’s used in the encryption and decryption of data sent between your server and the connecting clients. A private key is created by you—the certificate owner—when you request your certificate with a Certificate Signing Request (CSR). The Certificate Authority providing your certificate (such as DigiCert) does not create or have your private key.

For more detailed information on installing SSL certificates, see:

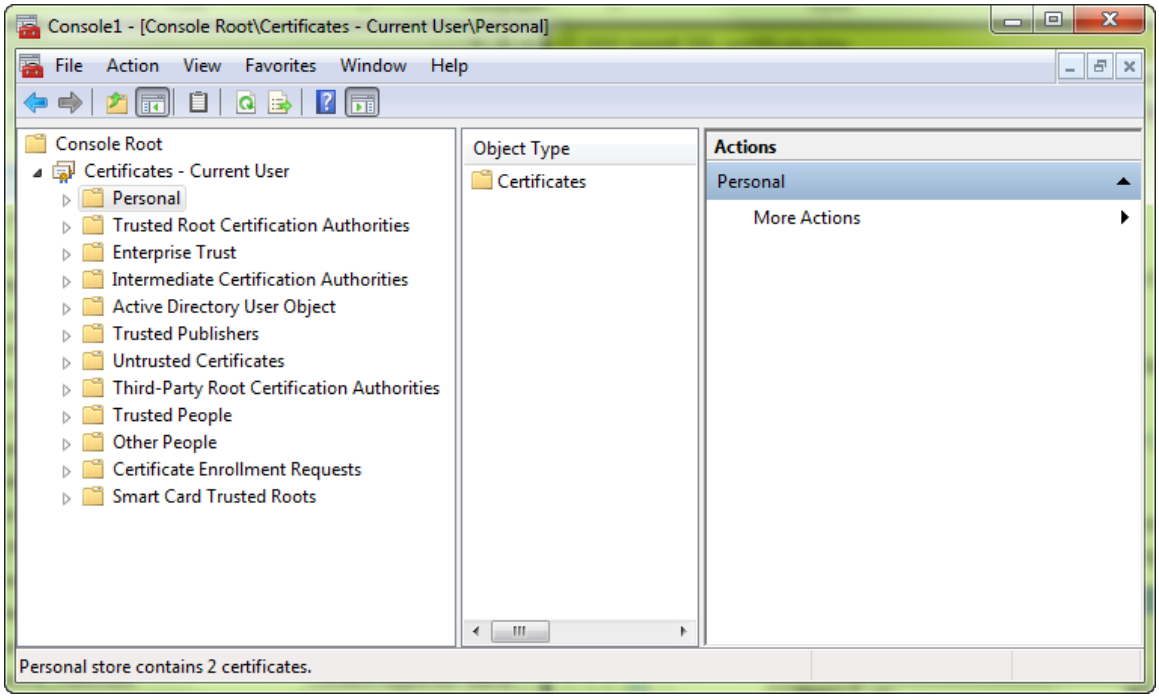
http://msdn.microsoft.com/en-us/library/ms733791.aspx

Install the SSL certificate

Clients contact the Local Authenticator on the standard HTTP ports 80 and 443.

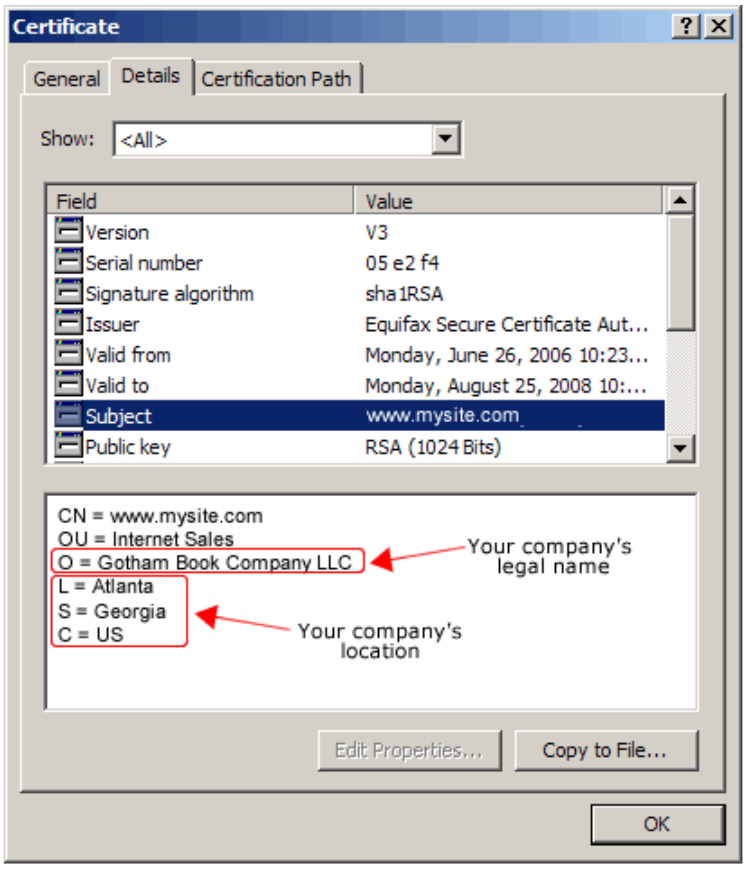
1. Install an SSL certificate in the Personal Store under the Local Computer section for the "logon as" user account under which the NMS service is running.

   To add the Certificates Snap-in and view the certificates installed on the local computer, see https://-technet.microsoft.com/en-us/library/cc754431(v=ws.11).aspx.



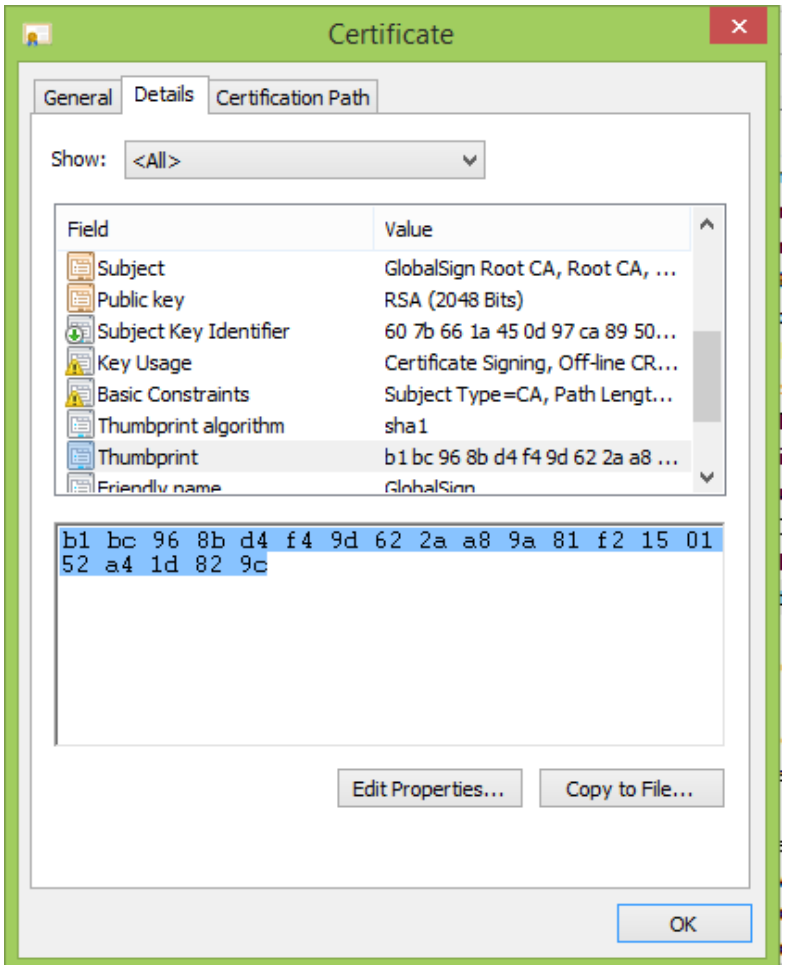
2. Note the subject of the certificate.

   This should match the computer name that the certificate is deployed on, or be a wild card. This must match exactly the host used in the endpoints. For information on viewing the subject, see https://-technet.microsoft.com/en-us/library/cc754686(v=ws.10).aspx.



3. Copy the thumbprint of the certificate. You use the thumbprint to bind the certificate to the port used by the primary NMS services in the next step.

   For information on retrieving the thumbprint, see https://msdn.microsoft.com/en-us/library/ms734695.aspx.



4. Verify that the `UseSSL` setting is set to true. This should have been set during the installation.
   a. In `Nuance.NMS.Server.exe.config`, located in the NMS Platform installation folder, find the line near the top that contains the `key="UseSSL"` tag.
   b. Change the `value` to `true`:

      ```
      <add key="UseSSL" value="true"/>
      ```

5. Bind the SSL certificate under IIS to port 443.
   a. In the IIS Manager, from the left panel, click **Default Web Site**.
   b. From the right panel, click **Bindings...**

      The Site Bindings dialog box opens.
   c. Click **Add**.

      The Add Site Binding dialog box opens.
   d. From the **Type** drop-down list, select **https**.
   e. From the **SSL certificate** drop-down list, select the certificate that you installed.

f. Click **OK**.

The Site Bindings dialog box appears. Ensure that the binding is displayed correctly.

6. Restart the Local Authenticator server to allow any configuration changes to take effect.

Testing and troubleshooting your SSL configuration

Run these tests on a different computer. Do not run them on the NMC server server.

Use the browser

1. Can you access and log into the NMC console?
   a. Connect to `https://<SERVER_NAME>/NMCHTML/`.

      If you see the Nuance Management Center login page, port 443 is working, and the NMC console is being deployed properly.

   b. Log in to the NMC console. If successful, the console is able to communicate with the server.
2. Can you access the NMC console status interface?
   a. Connect to `https://<SERVER_NAME>/NMS/Platform/ConfigurationSvc/v1/Status`.

      An XML response should appear in the browser.
3. Can you make RESTful web service calls?

   Attempt to create an NMS session using the browser.
   a. Connect to `https://<SERVER_NAME>/NMS/Platform/AuthenticationSvc/v1/ValidateCredentials?location=Test&productGuid=9D62C366-6F85-4C4C-9333-6FE21798D7F4`

      A prompt for a login and password appears.

   b. Use any valid NMC console login and password.
   c. If some XML is returned, the NMC console is configured properly and working with SSL.
4. Can you access the NMS API Help pages?
   a. Connect to `https://<SERVER-NAME>/NMS/Platform/UserManagementSvc/v1/help`
   b. Enter any credentials if prompted.
   c. An HTML page with help for one of the NMS API sets should appear. If you see this help, the NMS is configured and working properly.

Check the Bindings

If the NMC console is not working, ensure that the ports are properly bound to the SSL certificate. To do this, specify the following from the command prompt:

```
netsh http show sslcert
```

Verify that port 443 is bound to the certificate.

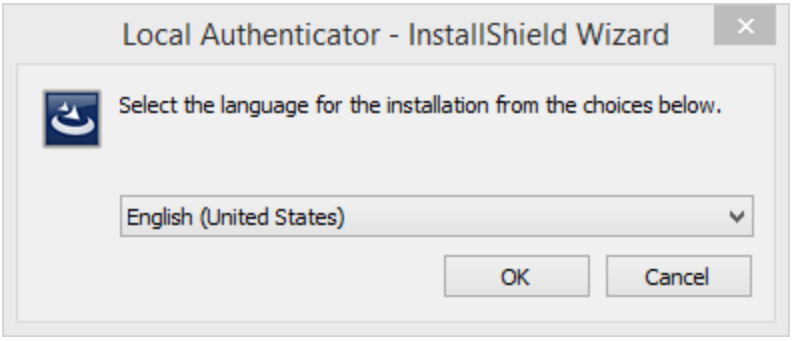
Installing the Local Authenticator

On the server where you are installing the Local Authenticator:

1. Run the `LocalAuthenticator.exe` file.

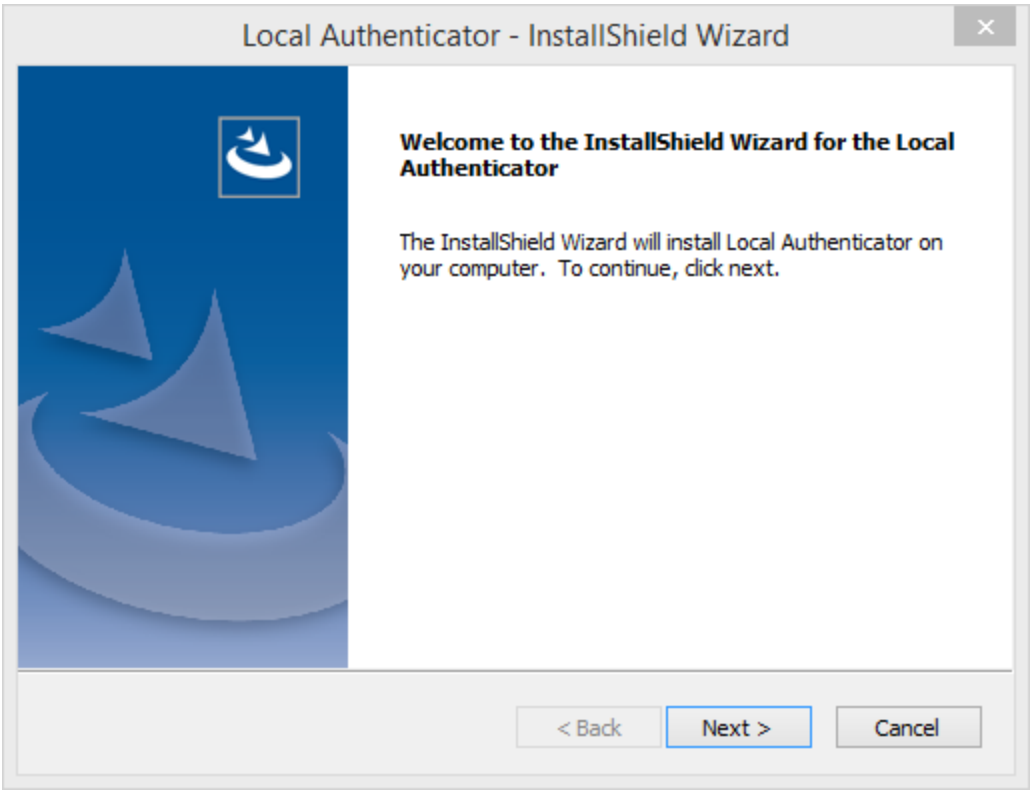
   A dialog box appears, prompting you to select a language for the installation.

2. Select your language from the drop-down list, and then click **OK**.

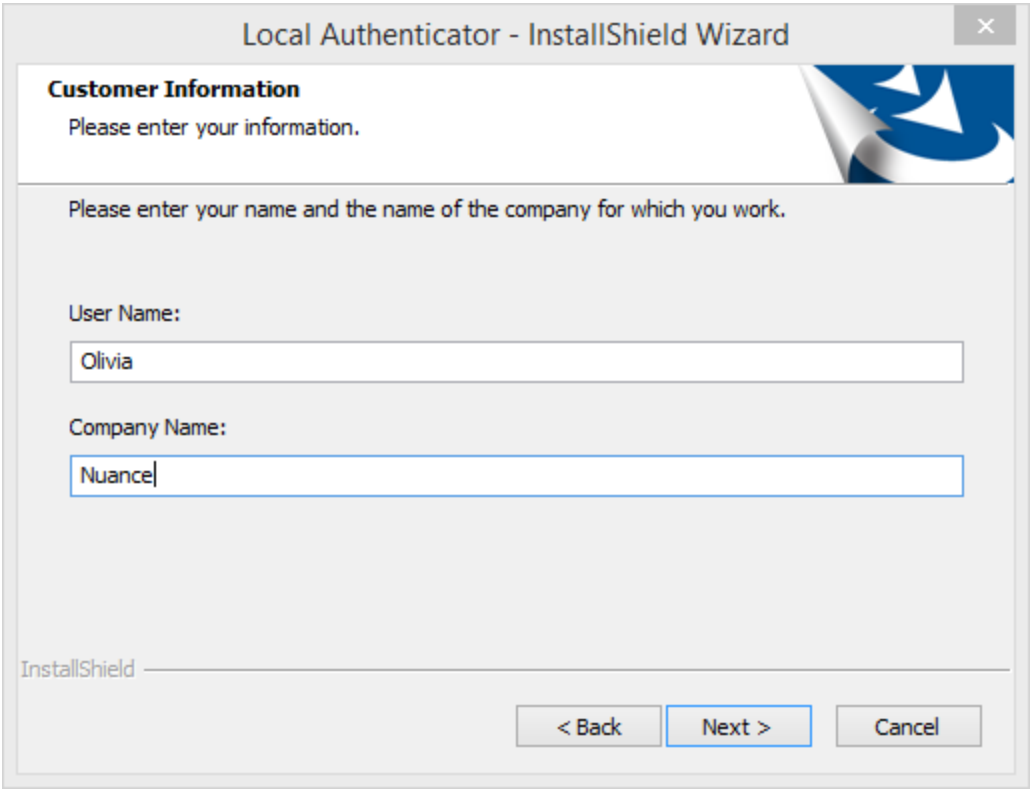


   The InstallShield Wizard opens.

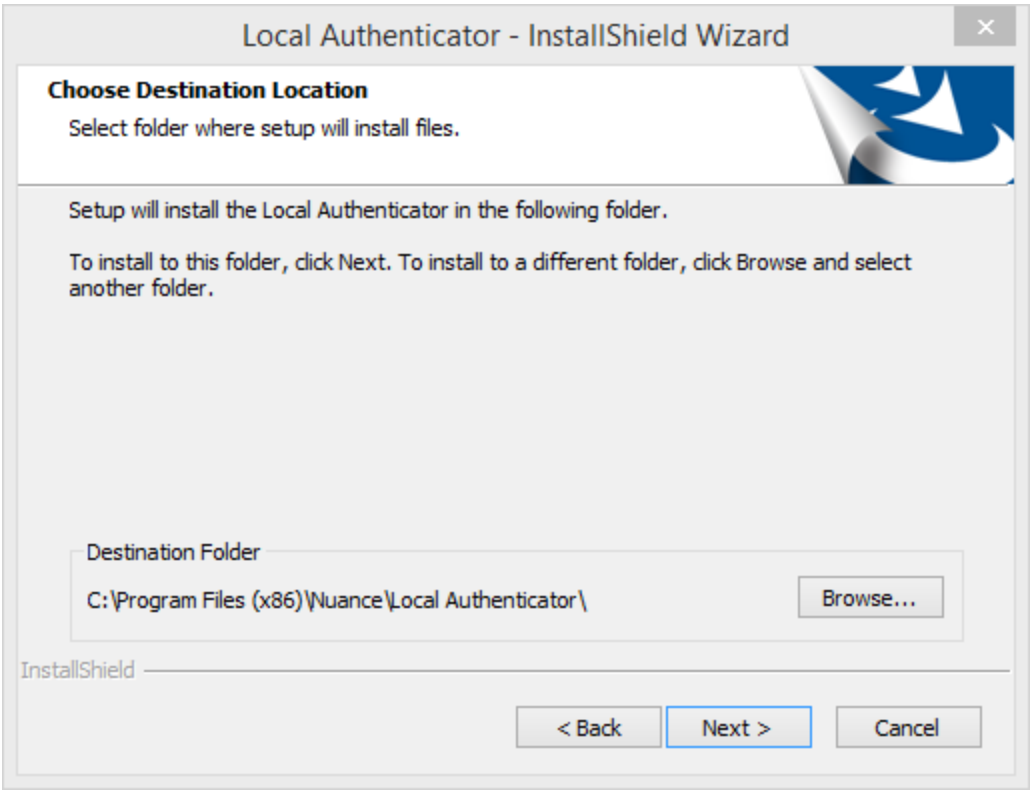
3. Click **Next**.



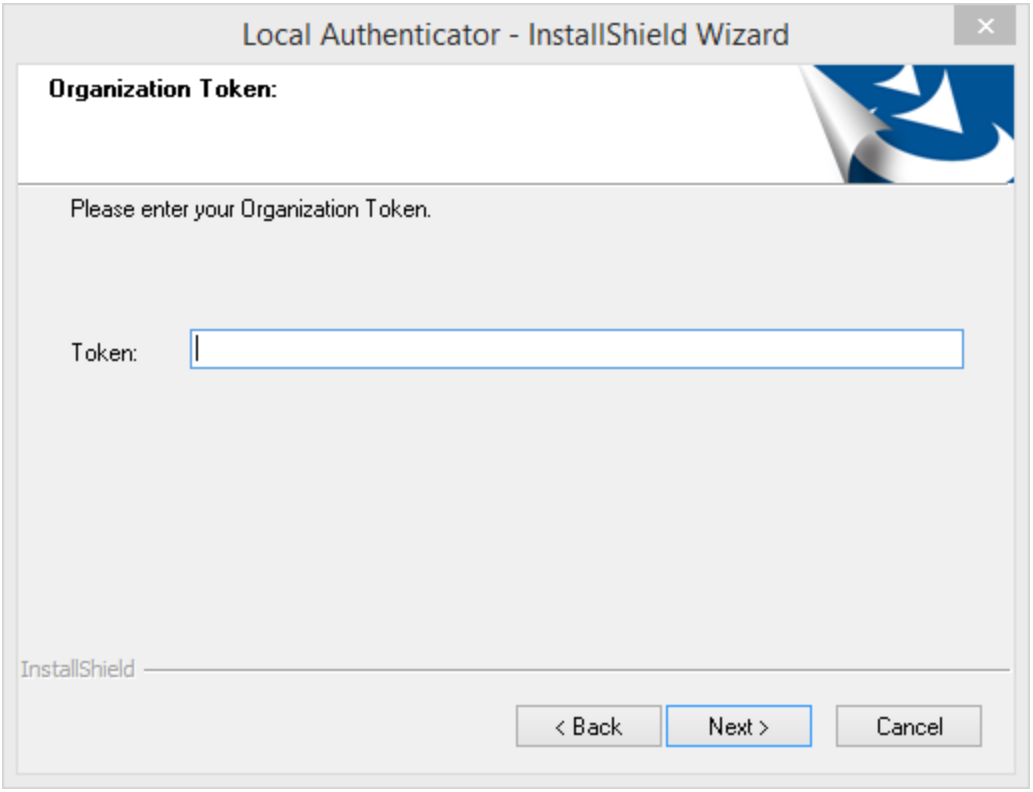
4. Leave the default value in the **User Name** field, and enter your company name in the **Company** field. Then, click **Next**.



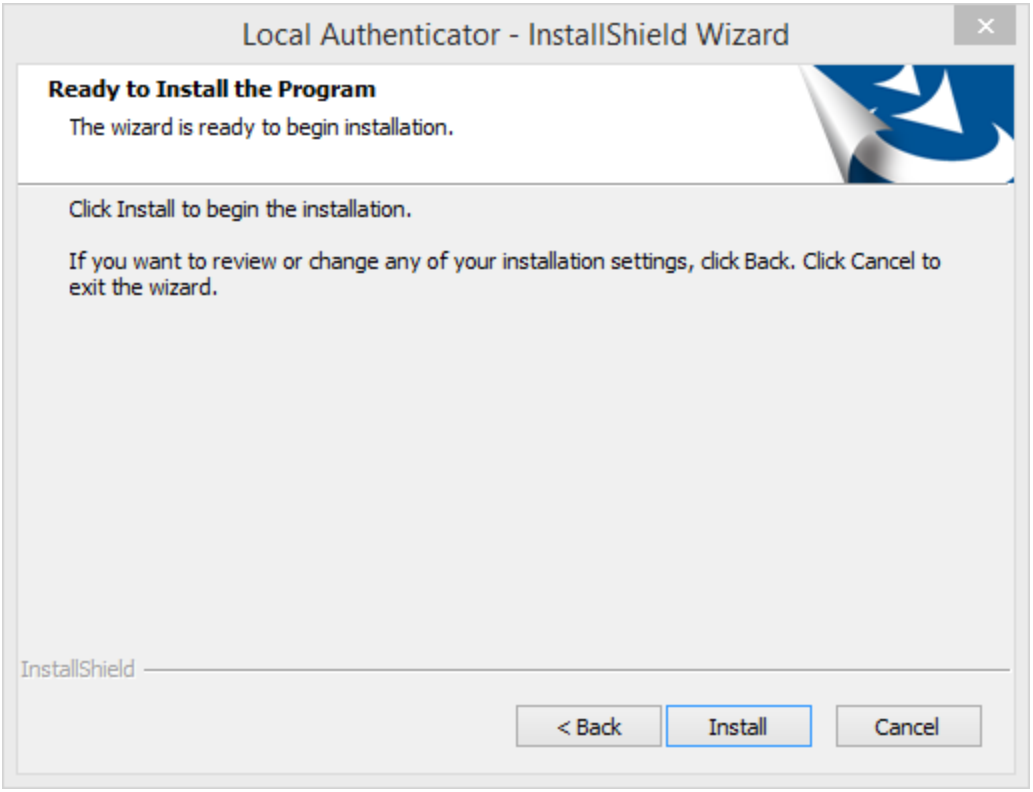
5. Set the location in which to install the Local Authenticator, and then click **Next**.



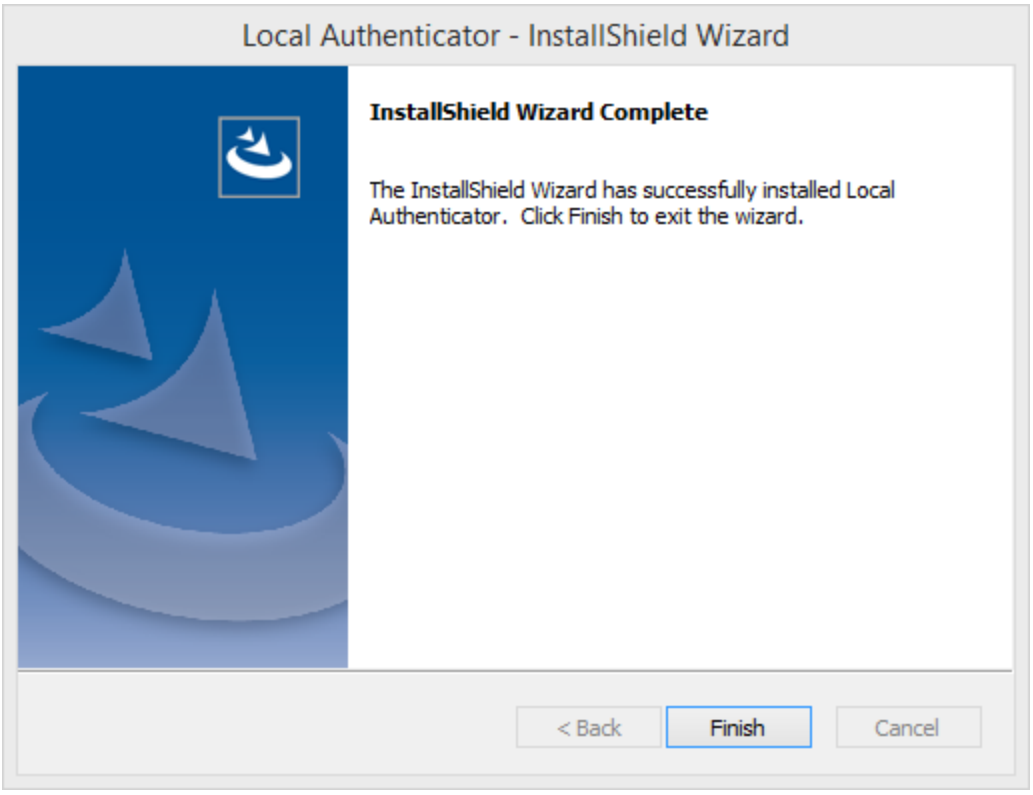
6. In the **Token** field, enter the organization token that you generated in the NMC console, and then click **Next**.



7. Click **Install**.



8. When the installation is complete, the InstallShield Wizard Complete dialog appears. Click **Finish** to exit the installer.



Editing the configuration file

You edit the Local Authenticator configuration file to change the NMC server address to the Nuance cloud-hosted NMC server URL. You should have received this address in your welcome information from Nuance.

1. Open the folder where the Local Authenticator is installed. By default, the Local Authenticator is installed in:

   ```
   C:\Program Files\Nuance\Local Authenticator
   ```

2. In any text editor, open `NMS.LocalAuthenticator.Service.exe.config`.
3. Locate the following line and verify that the value is set to the token that you entered during Local Authenticator installation:

   ```
   <add key=”CustomerToken” value=”{Organization token ID added in NMC}” />
   ```

4. Locate the following line and change the value to the address of the Nuance cloud-hosted NMC server:

   ```
   “<add key=”NMSServerAddress” value=”nms server address” />
   ```

5. Save your changes.

Starting the Local Authenticator service

1. Open the Services dialog box.
    a. Click the Windows Start menu.
    b. In the Search field, enter `services.msc`, and then press **Enter**.
    c. Specify your administrator username and password when prompted.
2. Locate the **NMS Local Authenticator Service**.
3. Right-click the service, and then select **Start**.

Appendix A: Database backups and data retention

About database backups **64**
Disabling automatic database backups 64
About data retention **65**

About database backups

If you are hosting your own NMC server on-premise, database backups occur on a regular basis at scheduled intervals automatically. The backup process places backup files in the `C:\NMSDBBACKUP` folder on the database server by default, unless you specified a different drive and directory during installation. The backup includes database objects, like sites and groups, and includes the Windows communication foundation service logs generated for each user account. Backups occur on the following schedule:

- **Transaction log backup**—Hourly
- **Differential database backup**—Daily at 2AM
- **Full database backups**—Weekly at 2AM

The database server retains one month of backups on disk. To retain more data, you must copy the files to another location before the end of the month. The backup process purges files older than one month.

Disabling automatic database backups

Optionally, you can choose to disable the automatic backups and manage database backups yourself outside Nuance Management Center. To disable automatic backups:

1. From the NMC menu button (), select **System Settings**.

   The System Settings dialog box opens.
2. In the General section, select the **Disable scheduled NMS database backups** check box.
3. Click **Save**.

About data retention

Your SQL Server database stores application data, such as license information, partial speech profiles, application usage information, and audit data. The data is purged at predefined intervals. The following table describes the purge schedule.

Data Type	Purge Schedule
Audit data	Every 1 year and 1 day
Log files	Every 45 days
Raw usage data	Every 90 days **Note:** Converted usage data is never purged.
SMTP messages	Every 90 days
Unread system messages	Every 90 days
Client version information	Every 90 days
License usage	Every 90 days
Alerts	Every 90 days