

Nuance Management Center

Server installation and configuration guide

For:

Nuance®
Dragon® Professional
Group

Nuance®
Dragon® Legal
Group

Nuance®
Dragon®
Law Enforcement

On-premise
version 2022.3.3

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.

No part of this manual or software may be reproduced in any form or by any means, including, without limitation, electronic or mechanical, such as photocopying or recording, or by any information storage and retrieval systems, without the express written consent of Nuance Communications, Inc. Specifications are subject to change without notice.

© Nuance Communications Inc. 2022

Nuance, the Nuance logo, the Dragon logo, Dragon, and RealSpeak are registered trademarks or trademarks of Nuance Communications, Inc. in the United States or other countries. All other names and trademarks referenced herein are trademarks of Nuance Communications or their respective owners. Designations used by third-party manufacturers and sellers to distinguish their products may be claimed as trademarks by those third-parties.

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.

11/2/2022

Contents

Dragon_NMCInstallGuideCover_20160929_v4	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: Preparing for your installation	4
About on-premise deployment options	5
Comparison: Single-node and multi-node deployments	5
Installation checklists	7
Pre-installation checklist	7
Installation checklists	7
Post-installation checklists	8
Software requirements—Nuance Management Center	9
NMC server and database server	9
NMC console	11
Hardware requirements—Server	12
Server installation prerequisites	13
Security considerations	15
General security principles	15
Installing and configuring Nuance Management Center securely	15
Nuance Management Center security features	16
Authentication methods	16
Password settings	16
Assigning privileges	17
Assigning grants	17
Disabling inactive users	17

Installing and configuring IIS securely	17
Other considerations	18
Network bandwidth recommendations	18
Using a load balancer	18
Obtaining required server software	19
Opening required ports	20
Chapter 3: Installing the servers	21
Installing SQL Server	22
Installing Nuance Management Center	23
Installing Nuance Management Center—Single-node	23
Installing Nuance Management Center—Multi-node	33
Chapter 4: Post-installation tasks	44
Installing and binding the SSL certificate	45
About certificates	45
Installing the SSL certificate on the server (single-node deployments)	45
Installing the SSL certificate on a load balancer (multi-node deployments)	48
Testing and troubleshooting your SSL configuration	48
Verifying the NMS Platform service is running	50
Starting the NMS Platform service manually	50
Configuring your load balancer	51
Logging in to the NMC console	52
Determining your database backup method	53
Configuring the Dragon client for use with Nuance Management Center	54
Chapter 5: Upgrading Nuance Management Center	55
About upgrading Nuance Management Center	56
Upgrading Nuance Management Center 5.x or 6.x	57
Upgrade other software	57
Upgrade Nuance Management Center	57
Chapter 6: Preparing for your Active Directory single sign-on configuration	60
Single sign-on overview	61
Before you begin	62
Software requirements	62
Other requirements	62
Checklist—Planning the single sign-on setup	62
Creating an NMC console Administrator user for Active Directory	64
Setting the Active Directory connection string	65

- Creating and configuring user accounts for single sign-on 66
 - Creating user accounts 66
 - Configuring user accounts 66
- Running the SetSPN.exe Windows utility 67
 - About SetSPN.exe 67
 - Downloading SetSPN.exe 67
 - Executing SetSPN.exe 67
- Appendix A: Database backups and data retention 68**
 - About database backups 69
 - Disabling automatic database backups 69
 - About data retention 70

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.

Audience

This guide is intended for 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
<i>Dragon Group Citrix Administrator Guide</i>	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
<i>Nuance Management Center Administrator Guide</i>	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 .
<i>Dragon Release Notes</i>	New features, system requirements, client upgrade instructions, and known issues.	Dragon Help. Do the following: <ol style="list-style-type: none"> 1. When Dragon is open, click the Help icon () on the DragonBar, and then select Help Topics. 2. Click Get started. 3. Click Dragon 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: Preparing for your installation

About on-premise deployment options	5
Comparison: Single-node and multi-node deployments	5
Installation checklists	7
Pre-installation checklist	7
Installation checklists	7
Post-installation checklists	8
Software requirements—Nuance Management Center	9
NMC server and database server	9
NMC console	11
Hardware requirements—Server	12
Server installation prerequisites	13
Security considerations	15
General security principles	15
Installing and configuring Nuance Management Center securely	15
Nuance Management Center security features	16
Installing and configuring IIS securely	17
Other considerations	18
Network bandwidth recommendations	18
Using a load balancer	18
Obtaining required server software	19
Opening required ports	20

About on-premise deployment options

You can select from the following on-premise deployment options for your Nuance Management Center installation:

- **Single-node**—You install Nuance Management Center on a single NMC server.
- **Multi-node**—You install Nuance Management Center on multiple NMC servers. The servers are load-balanced by a network traffic switch.

The installation checklists and the Nuance Management Center installation instructions address both single-node and multi-node deployments.

Comparison: Single-node and multi-node deployments

The following table describes the differences between single-node and multi-node deployments.

Single-node	Multi-node
<ul style="list-style-type: none"> • Does not require a common file share. 	<ul style="list-style-type: none"> • Requires a common file share for all nodes to access. For more information, see the "Shared drive and user account/password (multi-node deployments)" row in "Server installation prerequisites" on page 13.
<ul style="list-style-type: none"> • You install Nuance Management Center on a single node. 	<ul style="list-style-type: none"> • You install Nuance Management Center on each node in your deployment.
<ul style="list-style-type: none"> • During the installation, you select the following: <ul style="list-style-type: none"> • On the Setup Type screen, select On a server with an SSL certificate installed directly on that server to indicate your SSL certificate will be installed on a server. • On the Common File Store Settings screen, select Single node deployment. 	<ul style="list-style-type: none"> • During the installation, you select the following: <ul style="list-style-type: none"> • On the Setup Type screen, select Behind a networking device with an SSL certificate installed to indicate your SSL certificate will be installed on the load balancer. • On the Common File Store Settings screen, select Shared drive for multi-nodes deployment and provide the common file store, user account, and

Single-node	Multi-node
	password.
<ul style="list-style-type: none"><li data-bbox="293 285 911 310">• You install the SSL certificate on your NMC server.	<ul style="list-style-type: none"><li data-bbox="1052 285 1425 348">• You install the SSL certificate on your load balancer.
<ul style="list-style-type: none"><li data-bbox="293 380 919 470">• Configure your clients for use with Nuance Management Center by providing your NMC server address in the client.	<ul style="list-style-type: none"><li data-bbox="1052 380 1425 506">• Configure your clients for use with Nuance Management Center by providing your load balancer address in the client.

Installation checklists

Use the following checklists to perform your Nuance Management Center on-premise installation.

Pre-installation checklist

<input type="checkbox"/>	Task	Reference
<input type="checkbox"/>	Review your deployment options.	“About on-premise deployment options” on page 5
<input type="checkbox"/>	Ensure all system requirements have been met.	“Software requirements—Nuance Management Center” on page 9 “Hardware requirements—Server” on page 12
<input type="checkbox"/>	Ensure all server installation prerequisites have been met.	“Server installation prerequisites” on page 13
<input type="checkbox"/>	Review security considerations.	“Security considerations” on page 15
<input type="checkbox"/>	Review other considerations.	“Network bandwidth recommendations” on page 18 “Using a load balancer” on page 18
<input type="checkbox"/>	Obtain the required server software.	“Obtaining required server software” on page 19
<input type="checkbox"/>	Open required ports.	“Opening required ports” on page 20

Installation checklists

Single-node deployment

<input type="checkbox"/>	Task	Reference
<input type="checkbox"/>	Install SQL Server.	“Installing SQL Server” on page 22
<input type="checkbox"/>	Install Nuance Management Center.	“Installing Nuance Management Center—Single-node” on page 23

Multi-node deployment

<input type="checkbox"/>	Task	Reference
<input type="checkbox"/>	Install SQL Server.	“Installing SQL Server” on page 22
<input type="checkbox"/>	Install Nuance Management Center on each node.	“Installing Nuance Management Center—Multi-node” on page 33

Post-installation checklists

Single-node deployment

<input type="checkbox"/>	Task	Reference
<input type="checkbox"/>	Install the SSL certificate on your server.	“Installing the SSL certificate on the server (single-node deployments)” on page 45
<input type="checkbox"/>	Verify that the NMS Platform service is running.	“Verifying the NMS Platform service is running” on page 50
<input type="checkbox"/>	Log in to the NMC console.	“Logging in to the NMC console” on page 52
<input type="checkbox"/>	Determine your database backup method.	“Determining your database backup method” on page 53
<input type="checkbox"/>	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 54

Multi-node deployment

<input type="checkbox"/>	Task	Reference
<input type="checkbox"/>	Install the SSL certificate on your load balancer.	“Installing the SSL certificate on a load balancer (multi-node deployments)” on page 48
<input type="checkbox"/>	Verify that the NMS Platform service is running.	“Verifying the NMS Platform service is running” on page 50
<input type="checkbox"/>	Configure your load balancer.	“Configuring your load balancer” on page 51
<input type="checkbox"/>	Log in to the NMC console. Ensure you access the NMC console using the load balancer address.	“Logging in to the NMC console” on page 52
<input type="checkbox"/>	Determine your database backup method.	“Determining your database backup method” on page 53
<input type="checkbox"/>	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 54

Software requirements—Nuance Management Center

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	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft® Windows Server 2012 • Microsoft® Windows Server 2012 R2 (64 bit) • Microsoft® Windows Server 2016 • Microsoft® Windows Server 2019 <p>Ensure you have all current service packs installed.</p> <p>Note: Nuance Management Center does not comply with the Federal Information Processing Standards (FIPS). Do not enable FIPS Compliance Mode on your NMC server.</p>	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft® Windows Server 2012 • Microsoft® Windows Server 2012 R2 (64 bit) • Microsoft® Windows Server 2016 • Microsoft® Windows Server 2019 <p>Ensure you have all current service packs installed.</p>	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft® Windows Server 2012 • Microsoft® Windows Server 2012 R2 (64 bit) • Microsoft® Windows Server 2016 • Microsoft® Windows Server 2019 <p>Ensure you have all current service packs installed.</p> <p>Note: Nuance Management Center does not comply with the Federal Information Processing Standards (FIPS). Do not enable FIPS Compliance Mode on your NMC server.</p>
Windows components	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.1, including the ASP .NET component • Internet Information Services (IIS), version installed with each platform 	None.	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.7.1, including the ASP .NET component • Internet Information Services (IIS),

Feature	NMC server	Database server	Combined NMC server and database server
			version installed with each platform
Database	None.	<ul style="list-style-type: none"> • SQL Server 2014, 2016, 2017, or 2019 • Microsoft OLE DB Driver for SQL Server <p>Note: The NMS installation prompts you to download and install this component. However, if you do not have internet connectivity from your server, you must download and install this component manually prior to your NMS installation.</p>	<ul style="list-style-type: none"> • SQL Server 2014, 2016, 2017, or 2019 • Microsoft OLE DB Driver for SQL Server <p>Note: The NMS installation prompts you to download and install this component. However, if you do not have internet connectivity from your server, you must download and install this component manually prior to your NMS installation.</p>
Security	<ul style="list-style-type: none"> • SSL certificate, issued by a certificate authority (CA) Nuance Management Center does not support self-signed certificates. For more information on SSL certificates, see “Installing and binding the SSL certificate” on page 45. • Some clients, such as Dragon Professional, 	None.	<ul style="list-style-type: none"> • SSL certificate, issued by a certificate authority (CA) Nuance Management Center does not support self-signed certificates. For more information on SSL certificates, see “Installing and binding the

Feature	NMC server	Database server	Combined NMC server and database server
	<p>require the use of TLS 1.2 to connect to the NMC server. If your client requires TLS 1.2, you must enable it on your NMC server to allow the clients to communicate with Nuance Management Center.</p>		<p>SSL certificate” on page 45.</p> <ul style="list-style-type: none"> • Some clients, such as Dragon Professional, require the use of TLS 1.2 to connect to the NMC server. If your client requires TLS 1.2, you must enable it on your NMC server to allow the clients to communicate with Nuance Management Center.

NMC console

- One of the following:
 - Google Chrome version 85.0.4183.121 (Official Build) (64-bit)
 - Microsoft Edge version 85.0.564.68 (Official build) (64-bit)
- Microsoft .NET Framework 4.7.1

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 2,000 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 you choose to have a separate database server for your SQL database, your server should meet the following requirements:

- **Processor:** Dual-Core 2GHz CPU
- **Minimum RAM:** 8

If you're using Roaming user profiles, you'll need a server, separate machine, or RAID array to host the Master user profiles directory with the following:

- **Processor:** Intel® Pentium family (<http://ark.intel.com/products/family/29862/Intel-Pentium-Processor#@Desktop>), or AMD Athlon (<http://www.amd.com/en-us/-products/processors/desktop/athlon#>)
- **CPU:** 1 GHz minimum (2.4 GHz recommended)
- **RAM:** 8 GB
- **Cache:** 512 KB minimum L2 Cache (1 MB recommended)

Server installation prerequisites

Ensure you have the following available before installing Nuance Management Center. You must provide the following during the installation.

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 deploys a Windows service.
NMS service user	<p>Windows user account that runs the NMS Platform service. Can be LOCAL SYSTEM account, network service, or another Windows account.</p> <p>If you choose another Windows account, it must meet the following requirements:</p> <ul style="list-style-type: none"> • Has Log on as a service rights to log on to your NMC server as a service • Has Read/Write/Delete access to the NMS file share <p>You provide this account name and password during the Nuance Management Center installation.</p>
Database server and database user	<p>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:</p> <ul style="list-style-type: none"> • Windows authentication • SQL Server authentication <p>If you choose SQL Server authentication, you must provide the database user login and password. This user must have dbcreator privileges.</p>
NMS file share location	<p>UNC root path used as permanent data storage by the NMC server for application data, such as sites, groups, and users.</p> <p>Required for both single and multi-node deployments. If you do not specify a location, the default location is used (C:\ProgramData\NMS\Filestore).</p> <p>For multi-node deployments, you must specify the same file share location for each node on which you install Nuance Management Center.</p> <p>The NMS service user is used to access this location by default.</p>
Shared drive and user account/password (multi-node deployments)	<ul style="list-style-type: none"> • Common file store for all nodes to access. • User account and password for the user with permission to access the shared drive. <p>This can be the NMS service user or a different user account. If you choose a different user account, the user must have Create/Read/Update/Delete permissions.</p>

Prerequisite	Additional Information
	You must specify the same shared drive for each node on which you install Nuance Management Center.

Security considerations

When your organization implements Nuance Management Center, it is critical to install the software and its system components using secure installation methods to protect the integrity and confidentiality of your data. It is equally important to manage and monitor your system once installed to ensure that your data is protected from unauthorized access and misuse.

The following sections provide secure installation and configuration guidelines, and describe the security features provided in Nuance Management Center to help you manage and monitor your system.

General security principles

- Require strong, complex user account passwords.

Create a password policy to establish password requirements. For example, require a minimum password length and one aspect of complexity, such as non-alphabetical characters.

- Keep passwords secure.

When you initially create user accounts in Nuance Management Center, send users their username and initial password in separate email messages. Instruct your users not to share or write down passwords, or store passwords in files on their computers. In addition, require users to change their default passwords upon first use, and on a regular basis.

For more information, see the **Users must change their password after first login** Organization option and the **Maximum password age - password will expire in *n* days** Organization option in the NMC Help.

- Keep software up-to-date.

Keep all software versions current by installing the latest patches for all components, such as SQL Server and Microsoft® Windows Server, including all critical security updates.

- Implement the principle of Least Privilege.

In implementing the principle of Least Privilege, you grant users the least amount of permissions needed to perform their jobs. You should also review user permissions regularly to determine their relevance to users' current job responsibilities.

- Monitor system activity.

Review user audit records regularly to determine which user activities constitute normal use, and which may indicate unauthorized use or misuse.

- Promote policy awareness.

Ensure your employees are aware of Acceptable Use policies, best practices, and standard operating procedures that are relevant to Nuance Management Center.

Installing and configuring Nuance Management Center securely

The Nuance Management Center installation instructions include procedures that install the application and system components into a secure state by default. In addition to performing the standard installation procedures, you can do the following to secure Nuance Management Center.

- Establish best practices for downloading report data.

Nuance Management Center provides the option to save report data to a CSV file. Establish best practices for downloading data to ensure the data remains secure outside of Nuance Management Center.

Nuance Management Center security features

Nuance Management Center provides the following security features to help you secure your system.

Authentication

You can choose from three different authentication methods. You can also select from flexible password options to establish a user account password policy.

Authentication methods

Nuance Management Center requires users to authenticate by logging in with a unique username and password. You can use the following authentication methods.

- **Single sign-on via Active Directory**—On premise deployments can enable single sign-on to allow users to log in to Nuance Management Center using their Windows credentials. This is the most secure method for on-premise deployments as users do not have to manage a separate set of credentials for Nuance Management Center and administrators do not have to manage a password policy.
- **Native Nuance Management Center authentication**—Users log in to Nuance Management Center using a login and password that you create when you create user accounts in the NMC console.

Password settings

Nuance Management Center provides password options that you can select to establish a user account password policy for your user accounts. Using the options, you can require specific password content, complexity, and expiration. Nuance Management Center audits changes to these options so you know which user changed them and when.

You can view audit records for these options in the Audit report.

For more information, see the "Organization Details page" topic or the "Viewing audit events" topic in the NMC Help.

Auditing

The Nuance Management Center auditing feature is a standard feature that cannot be disabled. Auditing tracks specific system events that occur in the NMC console, capturing information about those events to allow you to better monitor the actions that occur. The NMC console allows administrators to audit specific events, such as user or administrator logins, over a specific period of time.

By default, Nuance Management Center retains event data for one year.

For more information, see the "Viewing audit events" topic in the NMC help.

User Access Control

Nuance Management Center allows you to implement user access control using roles and permissions to restrict user access to only what is necessary for users to perform their job responsibilities. Before implementing user access control, establish an access control policy based on business and security requirements for each user. Review your access control policy periodically to determine if changes to roles and permissions are necessary.

Assigning privileges

Privileges determine the ribbons, menus, and options that users can access in the NMC console. You assign or unassign privileges to show or hide those options. You should assign the least amount of privileges that users require to perform all tasks relevant to their job responsibilities.

For more information on privileges and assigning them, see the **Configuring group security** section in the "Managing groups" topic in the NMC help and the "Privileges reference" appendix in the *Nuance Management Center Administrator's Guide*.

Assigning grants

Grants determine the objects that users can access in the Nuance Management Center database, such as sites, groups, and users. Generally, you assign different grants to providers than you would to administrators. You should also assign the least amount of grants that users require to perform their job responsibilities.

For more information on grants and assigning them, see the **Configuring group security** section in the "Managing groups" topic in the NMC help.

Disabling inactive users

Nuance Management Center allows you to disable inactive user accounts after a number of days of inactivity. Disabled users can no longer authenticate to Nuance Management Center. By disabling inactive user accounts, you can prevent unauthorized system access by employees who have left your organization.

For more information, see the **Disable inactive users after *n* days** Organization option in the "Organization Details page" topic in the NMC help.

Installing and configuring IIS securely

The IIS web application returns the X-AspNet-Version HTTP response header. The value of this header is used to determine the version of ASP.NET in use. It is not required for your Nuance Management Center on-premise installation, and can be disabled to prevent application information exposure.

To disable the response header, change the following setting in the web.config file:

```
<System.Web>
  <httpRuntime enableVersionheader="false" />
</System.Web>
```

For more information, see the following Microsoft article:

<https://docs.microsoft.com/en-us/archive/blogs/varunm/remove-unwanted-http-response-headers>

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 load balancer

If you have a large organization and you're implementing more than one NMC server, you can include a load balancer 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 4.7.1
- SQL Server 2014, 2016, 2017, or 2019
- One of the following:
 - Microsoft® Windows Server 2012
 - Microsoft® Windows Server 2012 R2 (64 bit)
 - Microsoft® Windows Server 2016
 - Microsoft® Windows Server 2019
- 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	<p>Allows communication between Dragon clients and the NMC server. Also allows communication between NMC console workstations and the NMC server.</p> <div style="border: 1px solid black; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>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.</p> </div>
1433 Custom	Database server	Allows communication between the NMC server and the database server if they are on separate physical machines.

Chapter 3: Installing the servers

Installing SQL Server	22
Installing Nuance Management Center	23
Installing Nuance Management Center—Single-node	23
Installing Nuance Management Center—Multi-node	33

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 **Database Engine Services** feature.
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.

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.

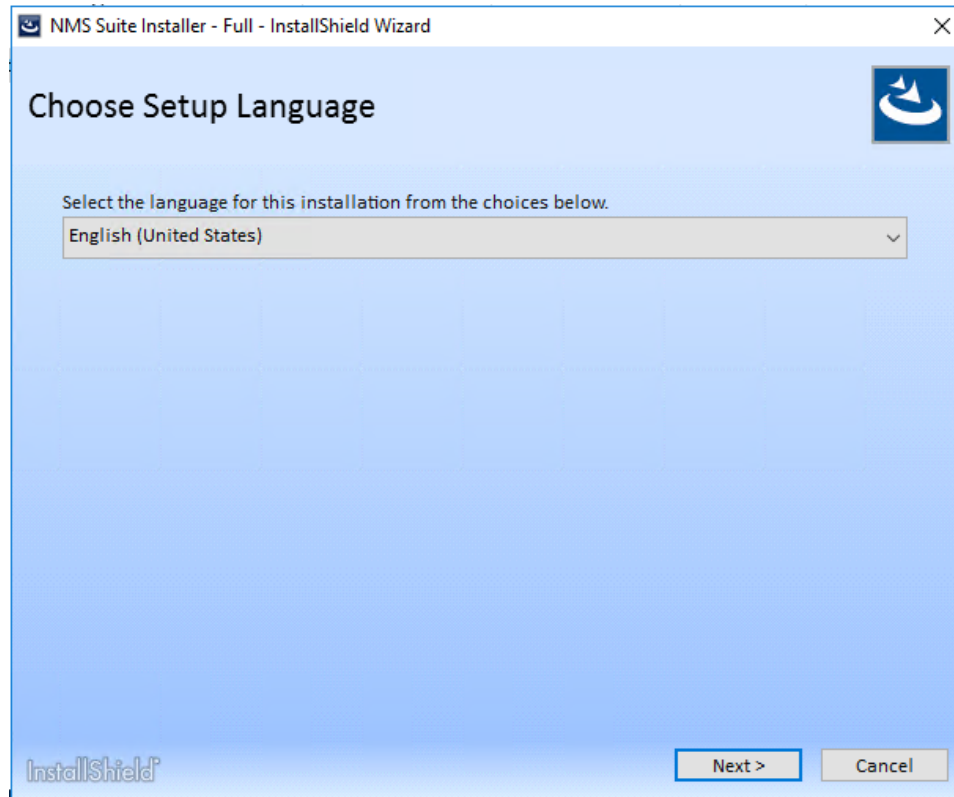
Installing Nuance Management Center

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.

Installing Nuance Management Center—Single-node

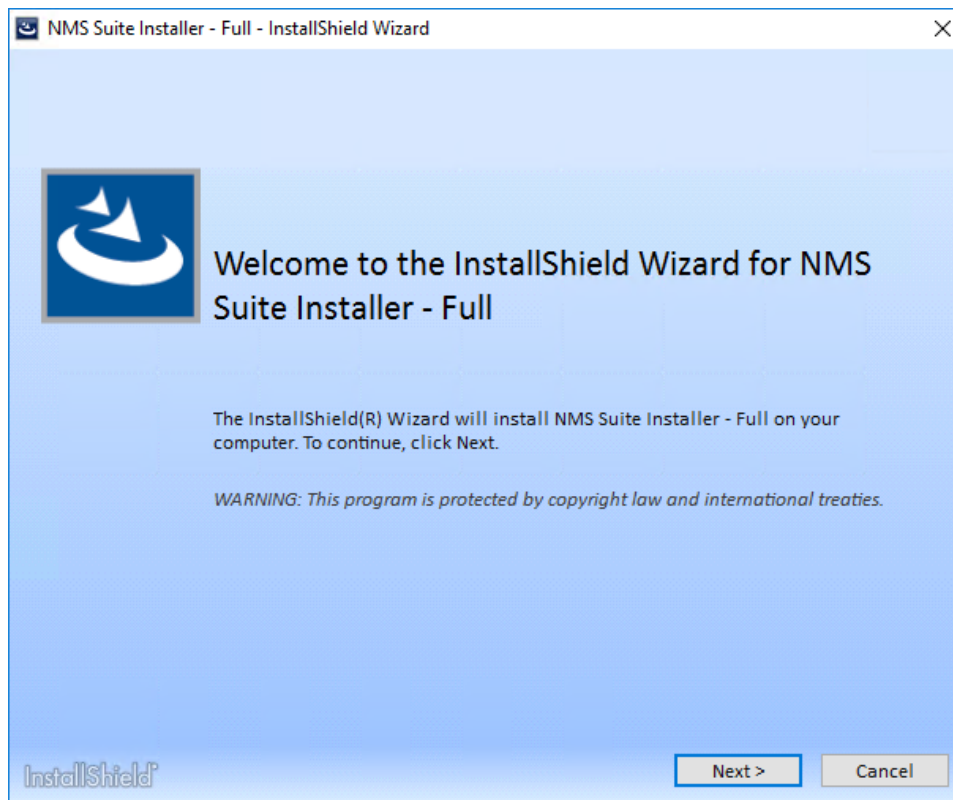
1. On the NMC server, run `NMS Suite Installer - Full.exe`.

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



2. Select a language from the drop-down list, and then click **Next**.

The **Welcome** screen appears.



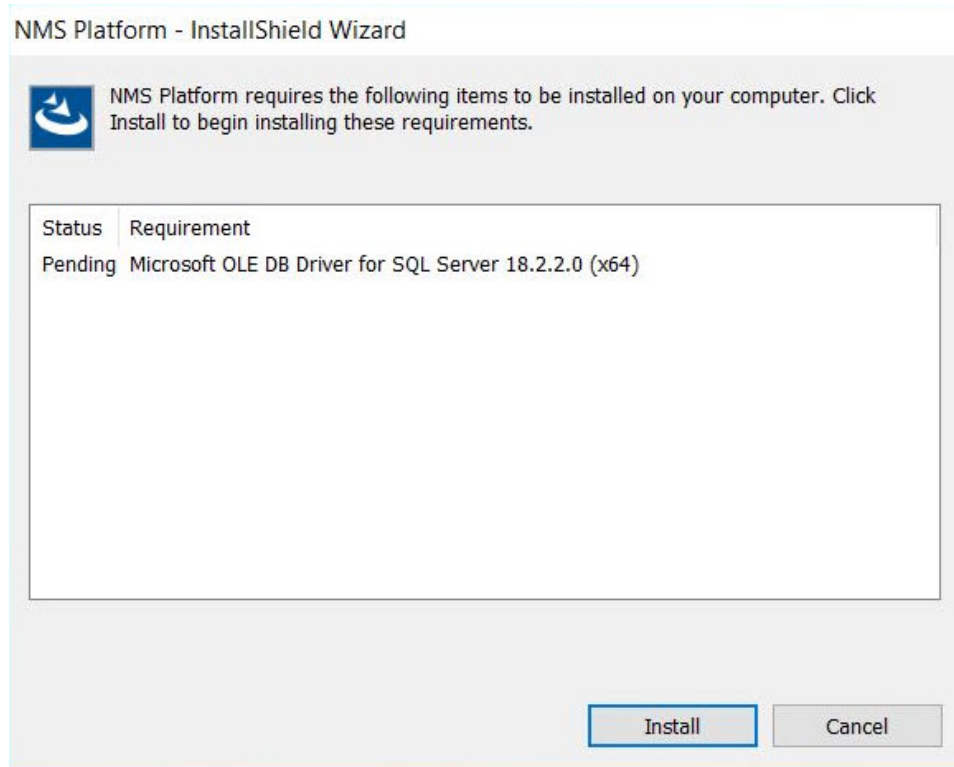
3. Click **Next**.

The **License Agreement** screen appears.



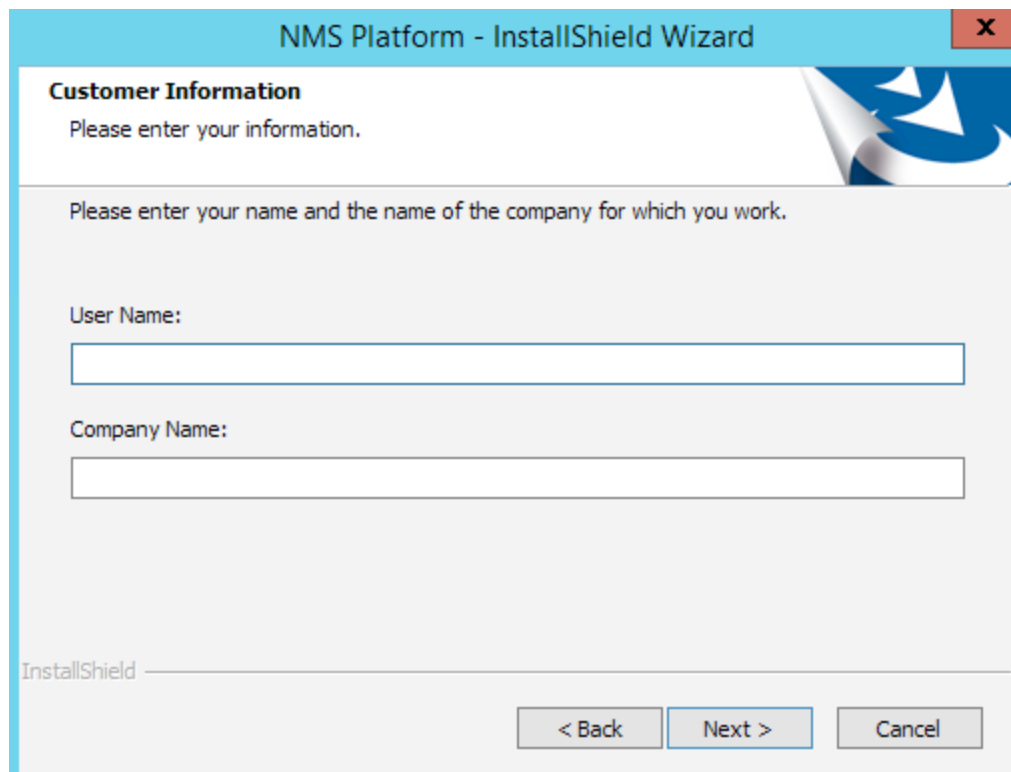
4. Select **I accept the terms in the license agreement**, and then click **Install**.

5. If the Microsoft OLE DB Driver is not already installed on your server, a prompt appears.



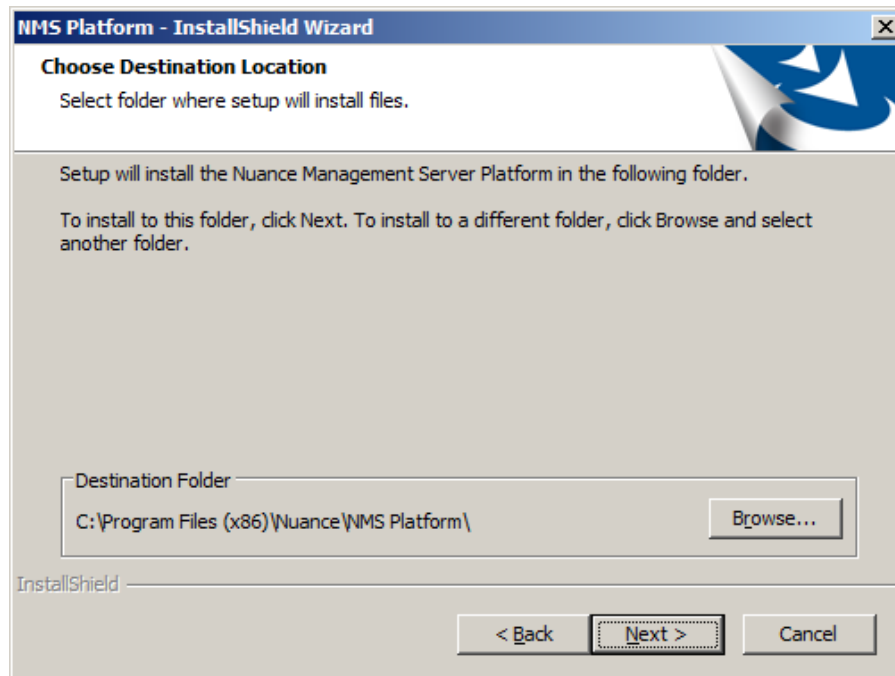
6. Click **Install**.

The client is installed, and the **Customer Information** screen appears.



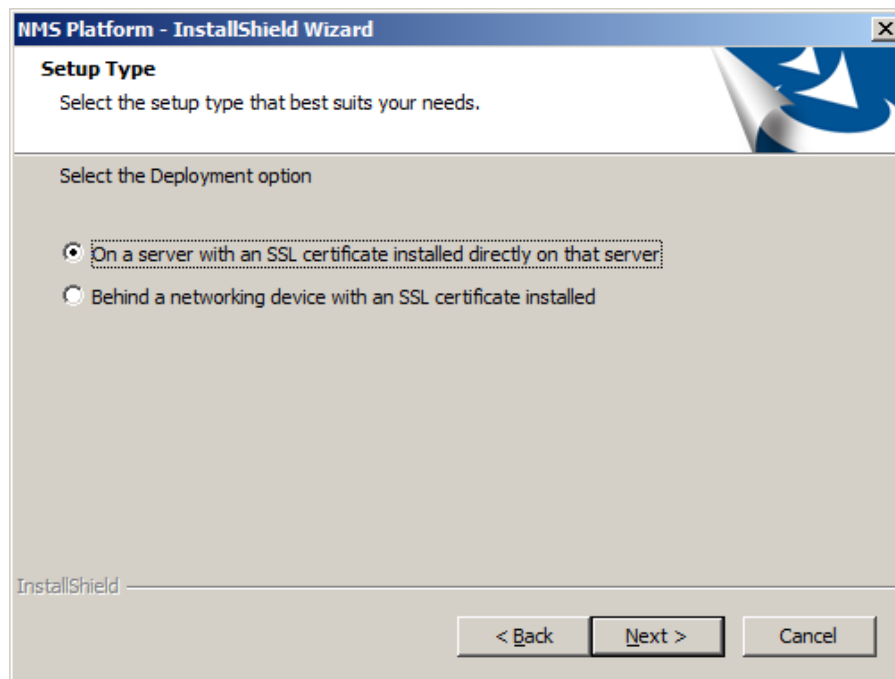
7. Enter a user name and company name, and then click **Next**.

The **Choose Destination Location** screen appears.



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

The **Setup Type** screen appears.



9. Select **On a server with an SSL certificate installed directly on that server** (for single-node installations).

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

10. 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.

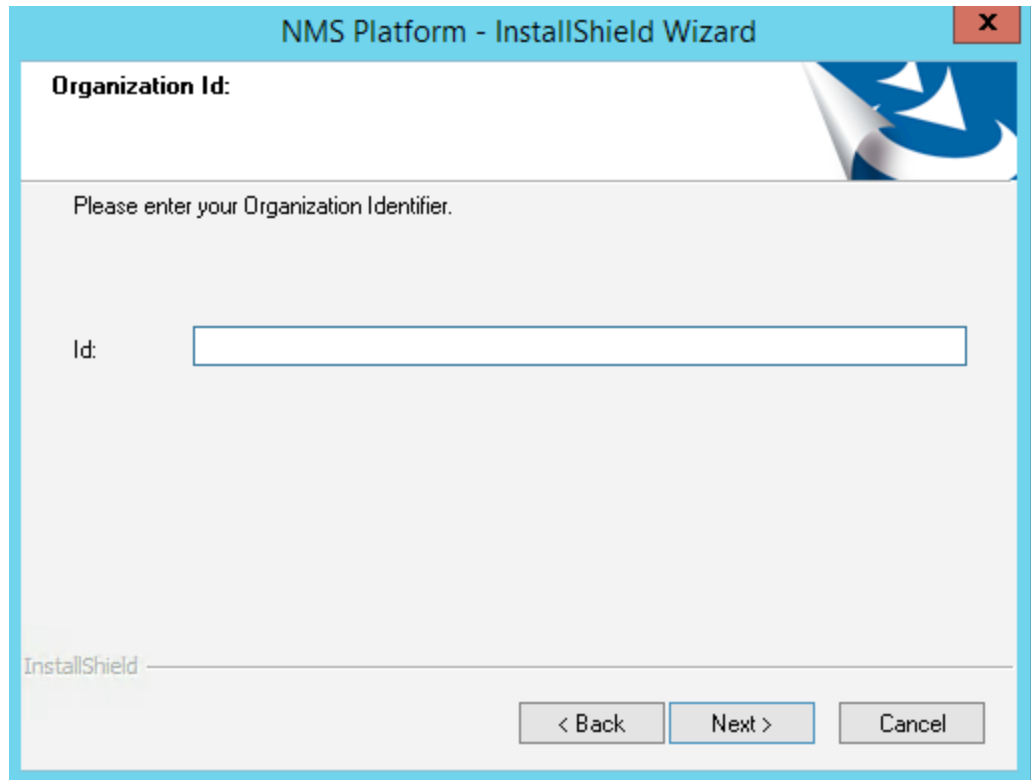
2. Select a method of validating connections to the server:

- **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.

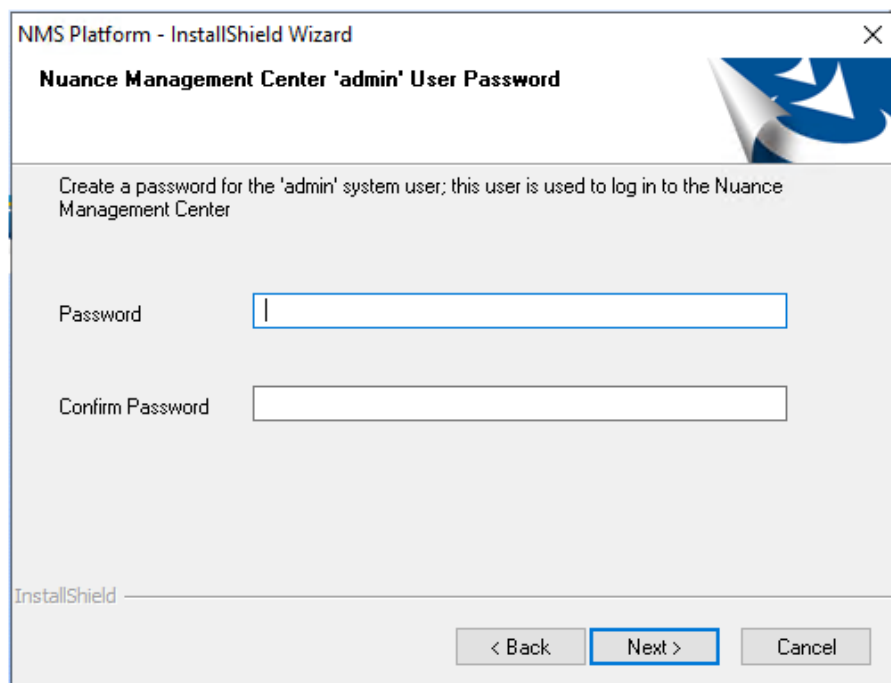


The screenshot shows a window titled "NMS Platform - InstallShield Wizard" with a close button (X) in the top right corner. The main heading is "Organization Id:". Below this, there is a sub-heading "Please enter your Organization Identifier." and a label "Id:" followed by a text input field. At the bottom left, the "InstallShield" logo is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

11. 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 **Nuance Management Center 'admin' User Password** screen appears.



The screenshot shows a window titled "NMS Platform - InstallShield Wizard" with a close button (X) in the top right corner. The main heading is "Nuance Management Center 'admin' User Password". Below this, there is a sub-heading "Create a password for the 'admin' system user; this user is used to log in to the Nuance Management Center". There are two text input fields: "Password" and "Confirm Password". At the bottom left, the "InstallShield" logo is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

12. 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 Dragon Medical Server System User Password screen appears.

13. Specify a password for the default system user created during the installation, and then click **Next**.

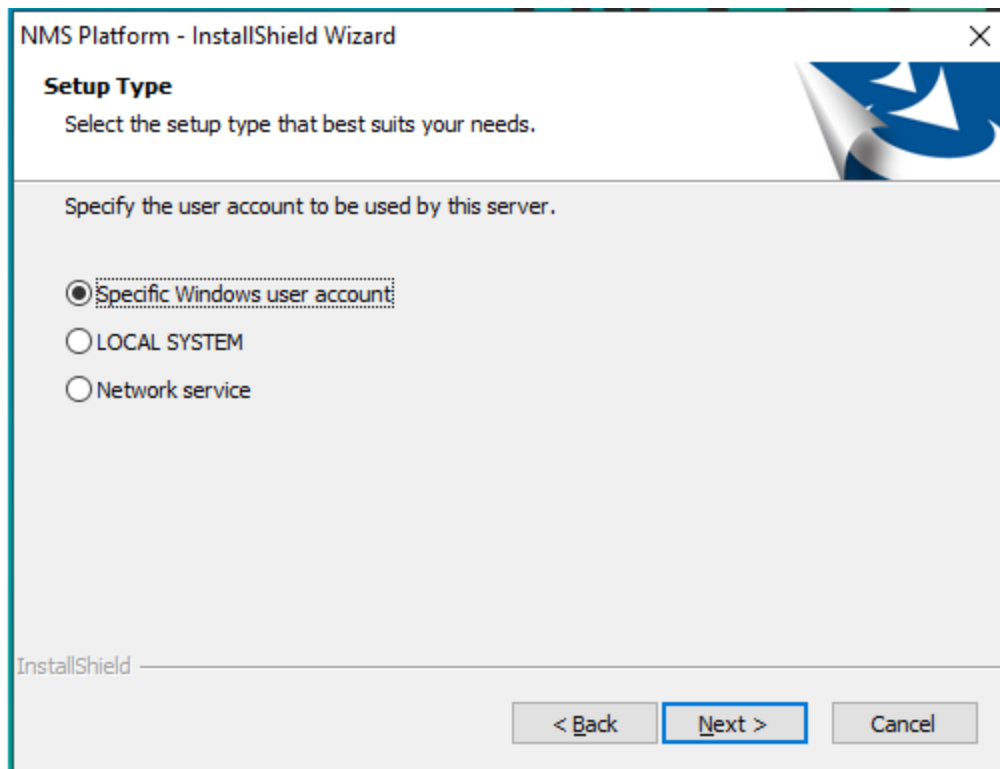
The **NMS File Share** screen appears.

14. Enter the file share location for the NMC server, and then click **Next**.

You must specify a UNC root path. For example, \\had001\nmsfileshare_001. If you do not specify a location, the default location is used (C:\ProgramData\NMS\Filestore).

For more information on the NMS file share, see [“Server installation prerequisites” on page 13](#).

The **Setup Type** screen appears.



15. 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 13](#).
 - **LOCAL SYSTEM**—The predefined local account used by the service control manager.
 - **Network service**—Network service that has access to NMS log file directories.

The **Logon Information** screen appears.

NMS Platform Installation - InstallShield Wizard

Logon Information
Specify a user account and password.

Specify the user account to be used by this server.

User accounts must be in the format DOMAIN\Username.

User Name:

Password:

Select the button below to specify information about a new user that will be created during the installation.

InstallShield

16. Enter the user name and password of the Windows service user account, then click **Next**.
The Setup Type screen appears.

NMS Platform - InstallShield Wizard

Setup Type
Select the setup type that best suits your needs.

Do you want the installation to create a database backup device?

Yes
 No

InstallShield

17. Indicate whether the installation should enable automatic database backups, and then click **Next**.

- **Yes**—Enables automatic SQL Server database backups. You must be a system administrator to enable this option.
- **No**—Disables automatic SQL Server database backups. You must manage your database backups outside of Nuance Management Center.

If you select **No**, a warning dialog box appears, prompting you to confirm your selection. Click one of the following:

- **Yes**—Disables automatic backups, and the Nuance Management Center installation continues.
- **No**—Closes the dialog box, returning you to the Setup Type screen to change your selection.

The Common File Store Settings screen appears after a few processes complete.

18. Select from the following options, and then click **Next**.

- **Single node deployment**—Select if your deployment is a single-node on-premise installation. Single-node on-premise installations use the AppData folder for file operations by default.
- **Shared drive for multi nodes deployment**—Select if your deployment is a multi-node on-premise installation.
 - **Storage Path**—Shared location to be used as a common file store for all nodes to access.
 - **User name**—User account that has permission to access the common file store.
 - **Password**—Password for the user account that will access the common file store.

- **Azure storage for multi nodes deployment**—Select if your deployment is a Nuance-hosted cloud installation (Nuance employees only).
 - **Storage connection string**—Azure storage connection string.

For more information, see [“Server installation prerequisites” on page 13](#).

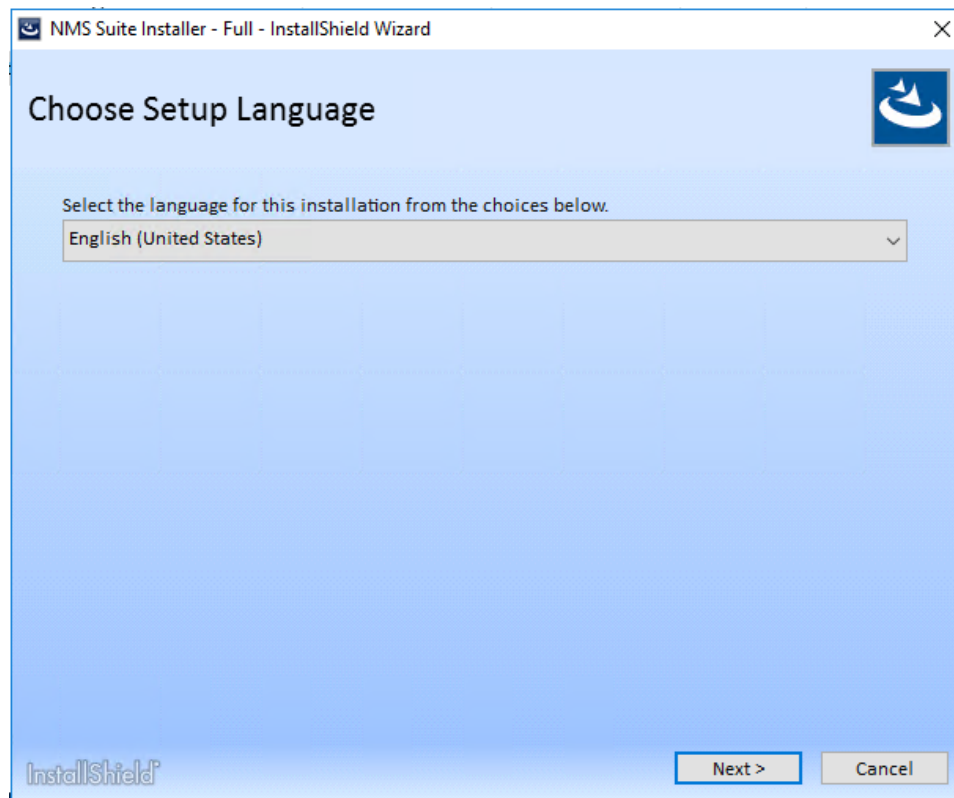
When you click **Next**, the wizard installs the NMS Platform Service.

19. Click **Finish** when the installation is complete.
20. 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.

Installing Nuance Management Center—Multi-node

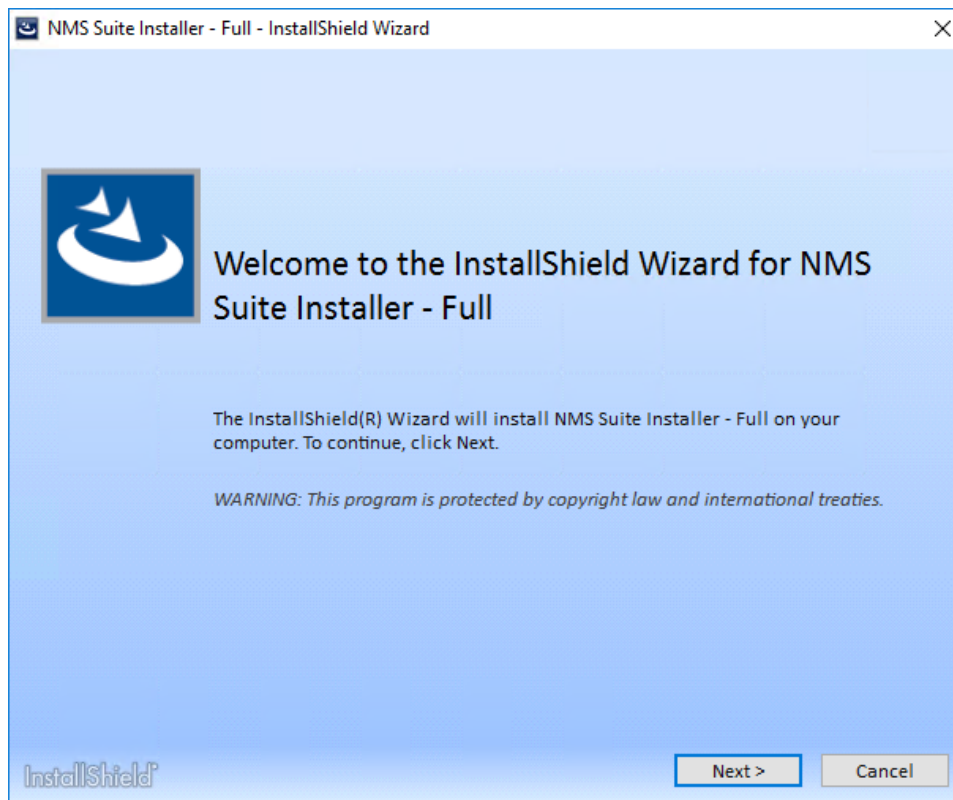
1. On each node, run `NMS Suite Installer - Full.exe`.

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



2. Select a language from the drop-down list, and then click **Next**.

The **Welcome** screen appears.



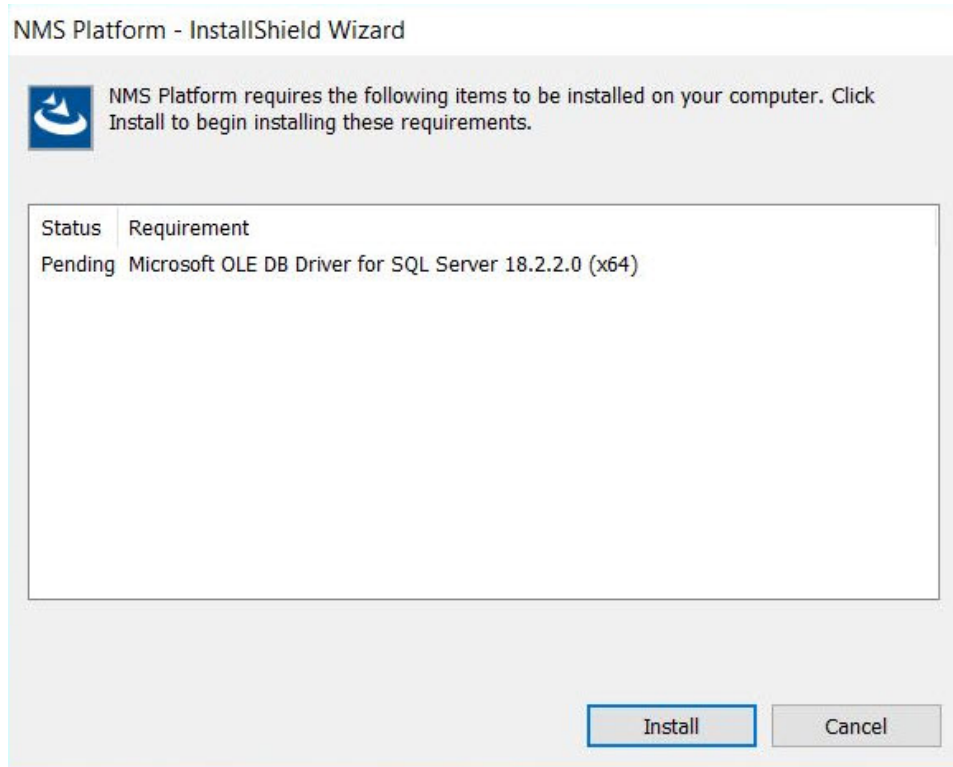
3. Click **Next**.

The **License Agreement** screen appears.



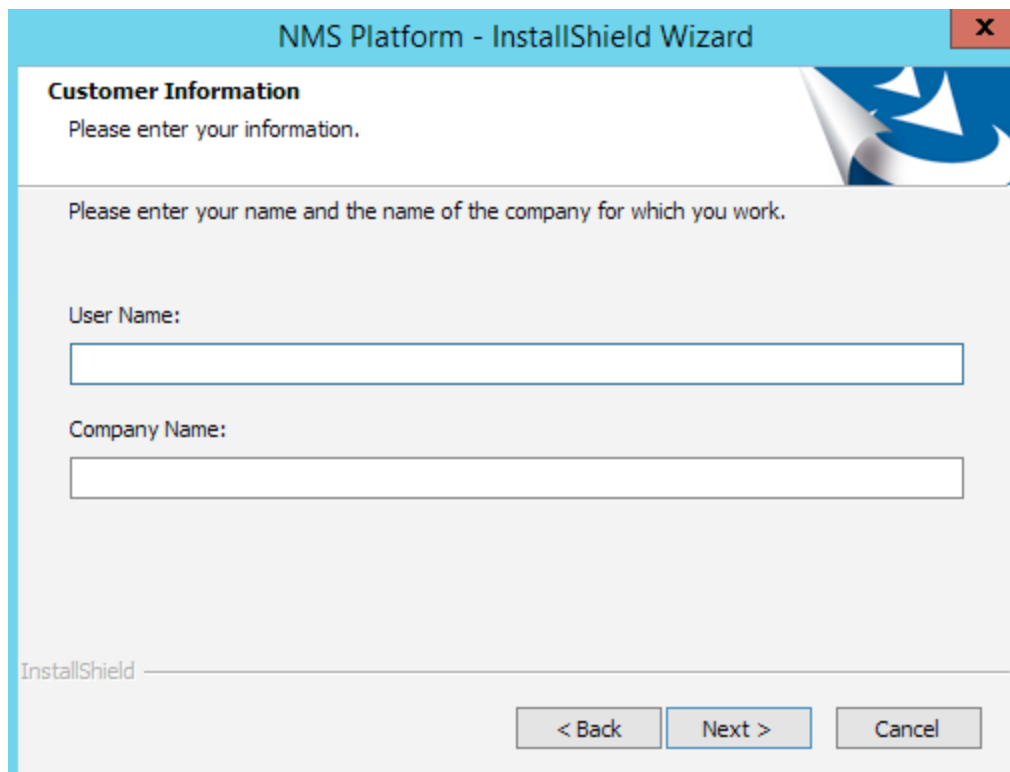
4. Select **I accept the terms in the license agreement**, and then click **Install**.

5. If the Microsoft OLE DB Driver is not already installed on your server, a prompt appears.



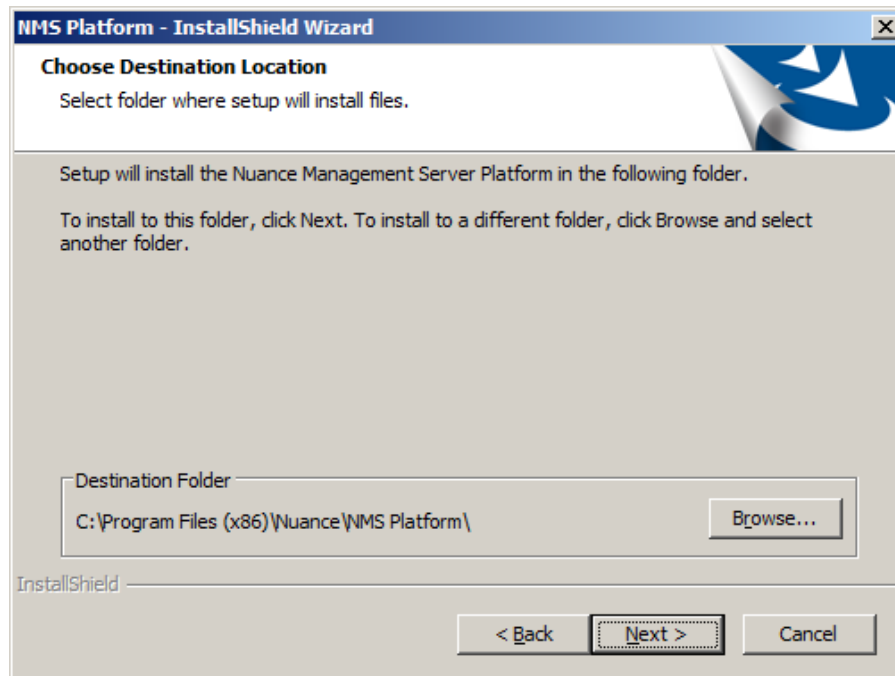
6. Click **Install**.

The client is installed, and the **Customer Information** screen appears.



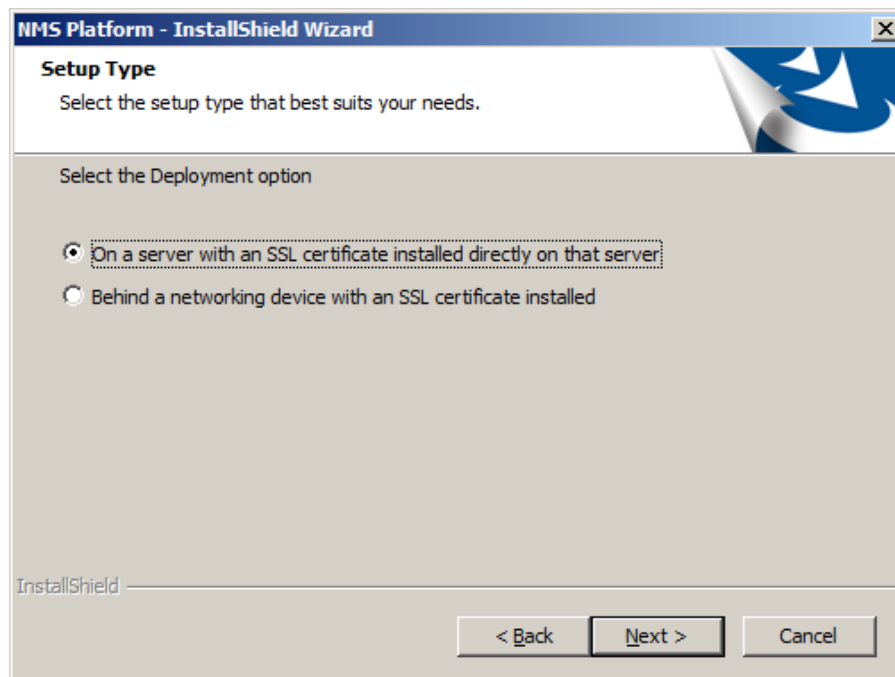
7. Enter a user name and company name, and then click **Next**.

The **Choose Destination Location** screen appears.



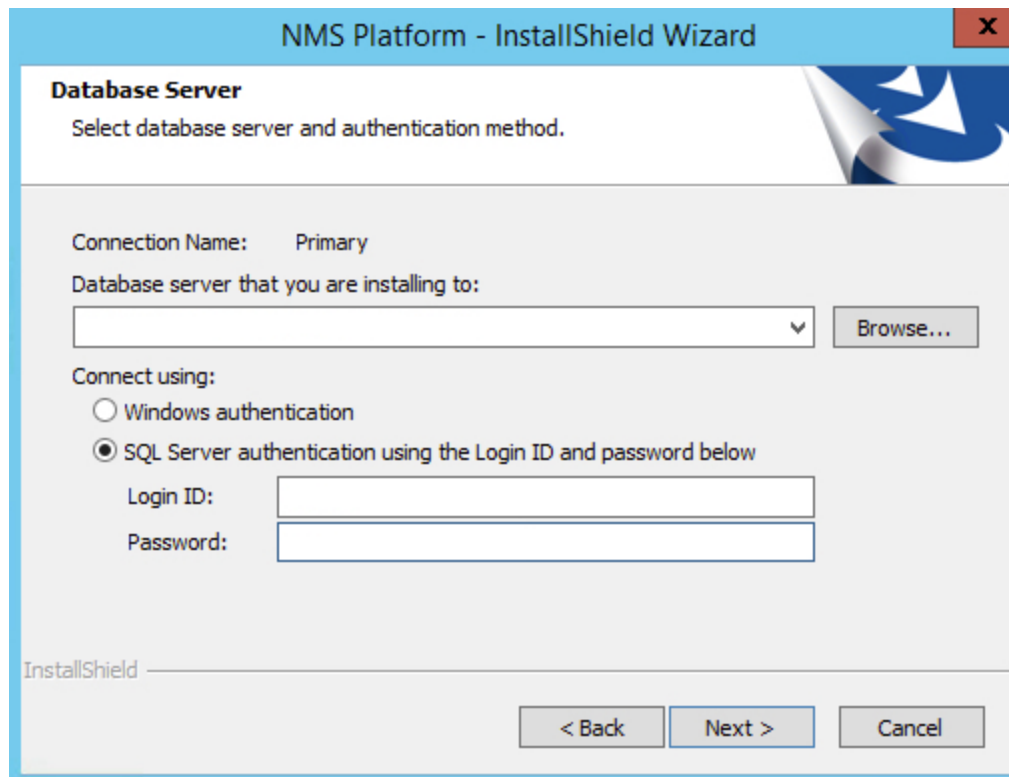
8. Choose where to install the NMS platform (default recommended), and then click **Next**.

The **Setup Type** screen appears.



9. Choose **Behind a networking device with an SSL certificate installed** (for multi-node deployments).

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



10. 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.

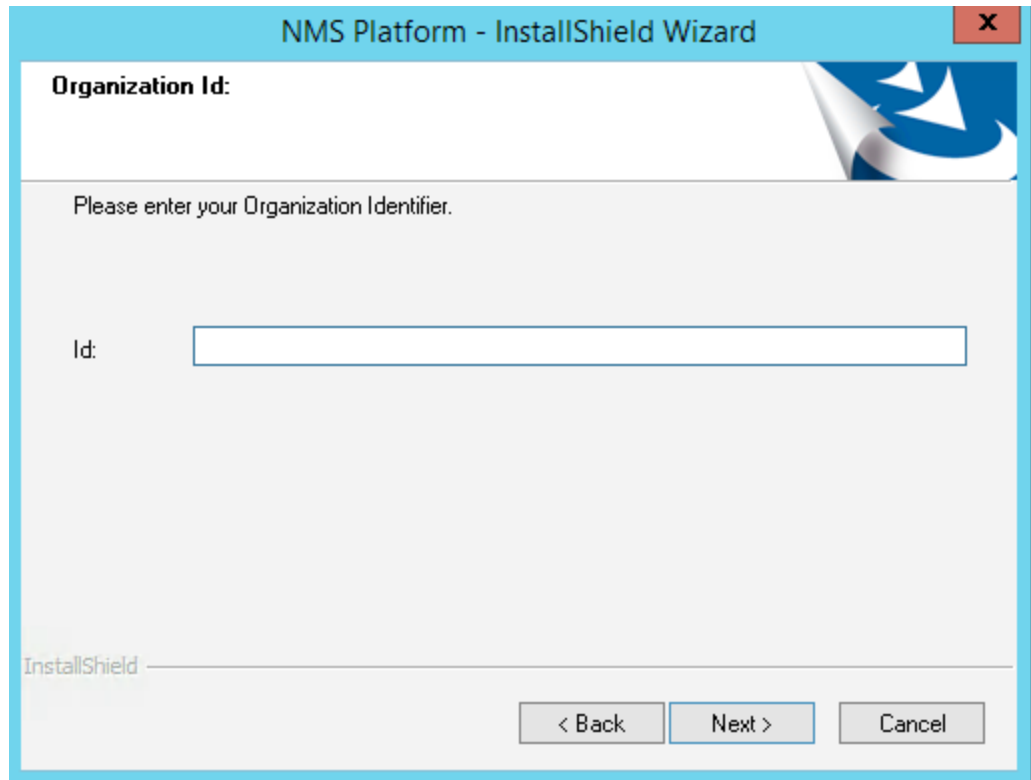
2. Select a method of validating connections to the server:

- **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**.

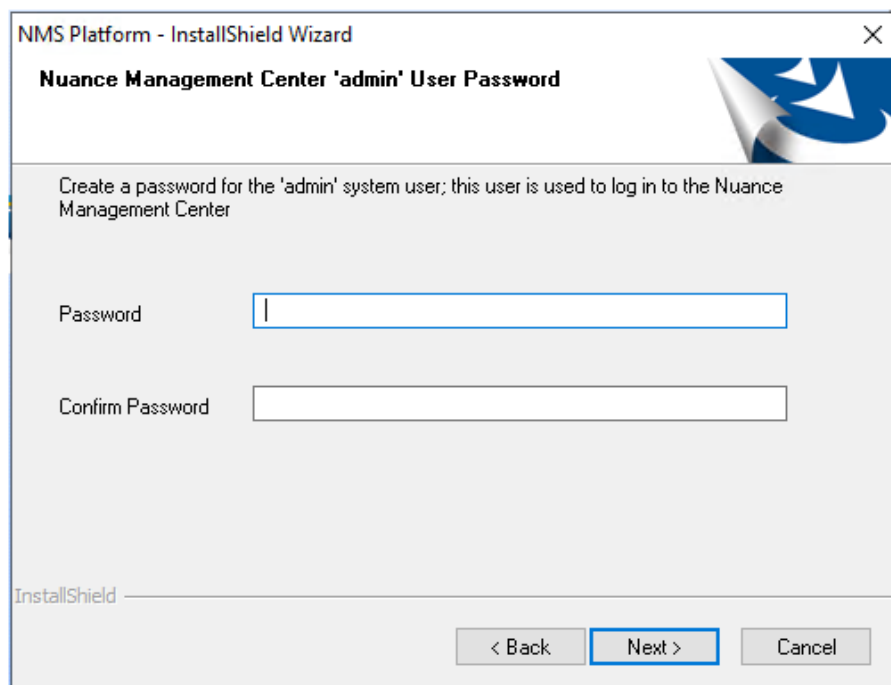
The Organization ID screen appears.



11. 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 **Nuance Management Center 'admin' User Password** screen appears.



12. 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 Dragon Medical Server System User Password screen appears.

13. Specify a password for the default system user created during the installation, and then click **Next**.

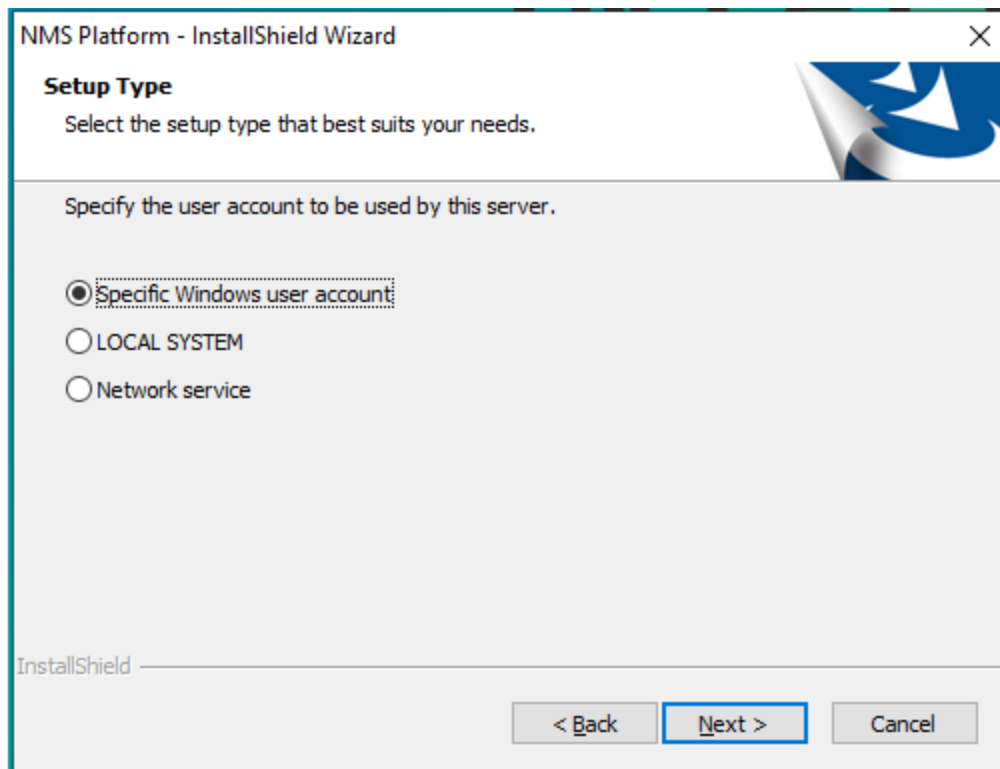
The **NMS File Share** screen appears.

14. Enter the file share location for the NMC server, and then click **Next**.

You must specify a UNC root path. For example, \\had001\nmsfileshare_001. If you do not specify a location, the default location is used (C:\ProgramData\NMS\Filestore).

For more information on the NMS file share, see [“Server installation prerequisites” on page 13](#).

The **Setup Type** screen appears.



15. 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 13](#).
 - **LOCAL SYSTEM**—The predefined local account used by the service control manager.
 - **Network service**—Network service that has access to NMS log file directories.

The **Logon Information** screen appears.

NMS Platform Installation - InstallShield Wizard

Logon Information
Specify a user account and password.

Specify the user account to be used by this server.

User accounts must be in the format DOMAIN\Username.

User Name:

Password:

Select the button below to specify information about a new user that will be created during the installation.

InstallShield

16. Enter the user name and password of the Windows service user account, then click **Next**.
The Setup Type screen appears.

NMS Platform - InstallShield Wizard

Setup Type
Select the setup type that best suits your needs.

Do you want the installation to create a database backup device?

Yes
 No

InstallShield

17. Indicate whether the installation should enable automatic database backups, and then click **Next**.

- **Yes**—Enables automatic database backups. You must be a system administrator to enable this option.
- **No**—Disables automatic database backups. You must manage your database backups outside of Nuance Management Center.

If you select **No**, a warning dialog box appears, prompting you to confirm your selection. Click one of the following:

- **Yes**—Disables automatic backups, and the installation continues.
- **No**—Closes the dialog box, returning you to the Setup Type screen to change your selection.

The Common File Store Settings screen appears after a few processes complete.

18. Select from the following options, and then click **Next**.

- **Single node deployment**—Select if your deployment is a single-node on-premise installation. Single-node on-premise installations use the AppData folder for file operations by default.
- **Shared drive for multi nodes deployment**—Select if your deployment is a multi-node on-premise installation.
 - **Storage Path**—Shared location to be used as a common file store for all nodes to access.
 - **User name**—User account that has permission to access the common file store.
 - **Password**—Password for the user account that will access the common file store.

- **Azure storage for multi nodes deployment**—Select if your deployment is a Nuance-hosted cloud installation (Nuance employees only).
 - **Storage connection string**—Azure storage connection string.

For more information, see [“Server installation prerequisites” on page 13](#).

When you click **Next**, the wizard installs the NMS Platform Service.

19. Click **Finish** when the installation is complete.
20. 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 4: Post-installation tasks

Installing and binding the SSL certificate	45
About certificates	45
Installing the SSL certificate on the server (single-node deployments)	45
Installing the SSL certificate on a load balancer (multi-node deployments)	48
Testing and troubleshooting your SSL configuration	48
Verifying the NMS Platform service is running	50
Starting the NMS Platform service manually	50
Configuring your load balancer	51
Logging in to the NMC console	52
Determining your database backup method	53
Configuring the Dragon client for use with Nuance Management Center	54

Installing and binding the SSL certificate

About certificates

Using SSL requires that you obtain an SSL certificate issued by a certificate authority (CA). You can obtain signed certificates from certificate authorities, such as GoDaddy or Verisign. Nuance Management Center does not support self-signed certificates. 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:

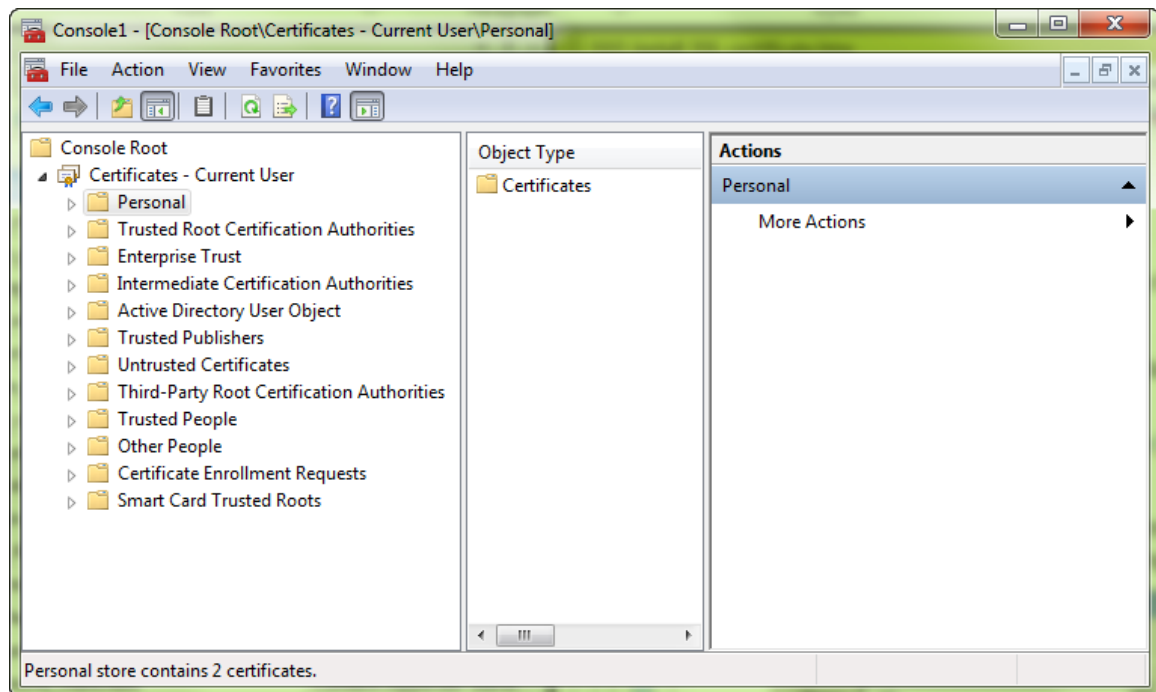
<http://msdn.microsoft.com/en-us/library/ms733791.aspx>

Installing the SSL certificate on the server (single-node deployments)

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

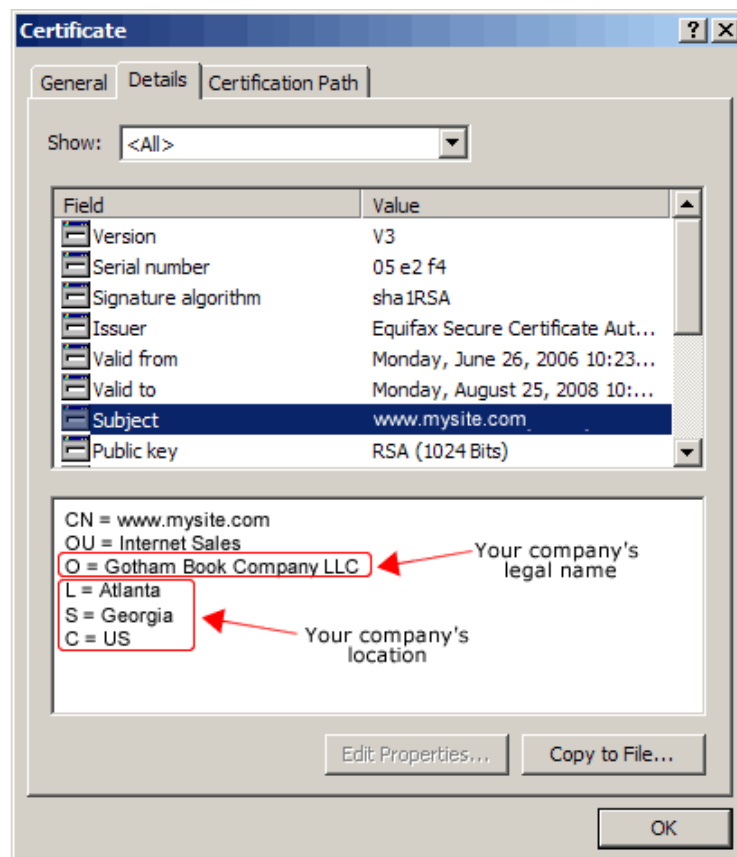
1. Install an SSL certificate in the Personal Store under the Local Computer section for the "logon as" user account under which the NMS service is running.

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](https://technet.microsoft.com/en-us/library/cc754431(v=ws.11).aspx).



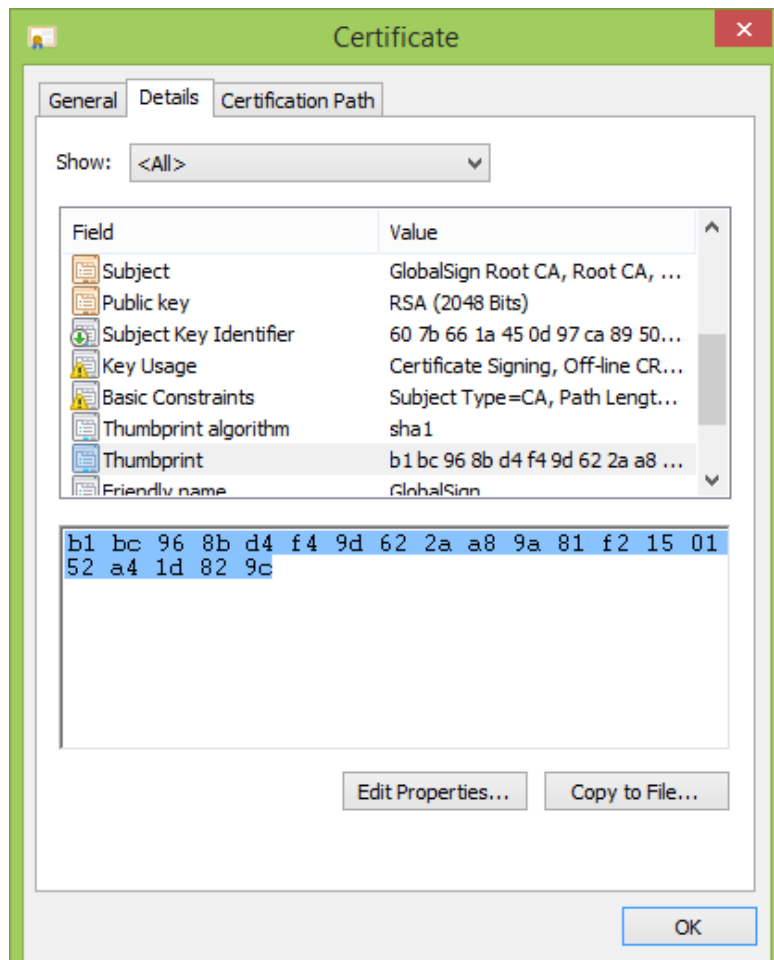
2. Note the subject of the certificate.

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](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 NMSUseSSL 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="NMSUseSSL" tag.
 - b. Change the value to true:


```
<add key="NMSUseSSL" 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.

Installing the SSL certificate on a load balancer (multi-node deployments)

Nuance uses this mode when the NMC server is behind a load balancing switch that also decrypts SSL. In this scenario, the load balancer 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>/NMHTML/`.
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 13](#).

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 load balancer

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

Configure the load balancer 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 load balancer receives an error. If the load balancer receives anything other than the expected response, it 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 load balancer, 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>/nmhtml`

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 69](#).

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 "Associating Dragon clients with the Nuance Management Center server or Local Authenticator" chapter in the *Dragon Client Installation Guide*.

Chapter 5: Upgrading Nuance Management Center

About upgrading Nuance Management Center	56
Upgrading Nuance Management Center 5.x or 6.x	57
Upgrade other software	57
Upgrade Nuance Management Center	57

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 5.x or 6.x

If you are currently on Nuance Management Center version 5.x or 6.x, you can simply run the installation file on each node where Nuance Management Center is installed to upgrade to the latest version.

Upgrade other software

1. If you currently have SQL Server 2008 installed, upgrade to SQL Server version 2016, 2017, or 2019.
SQL Server 2008 is not supported by Nuance Management Center version 5.10 or 6.x.
2. Install Microsoft .NET 4.7.1, if you do not already have it installed.

Upgrade Nuance Management Center

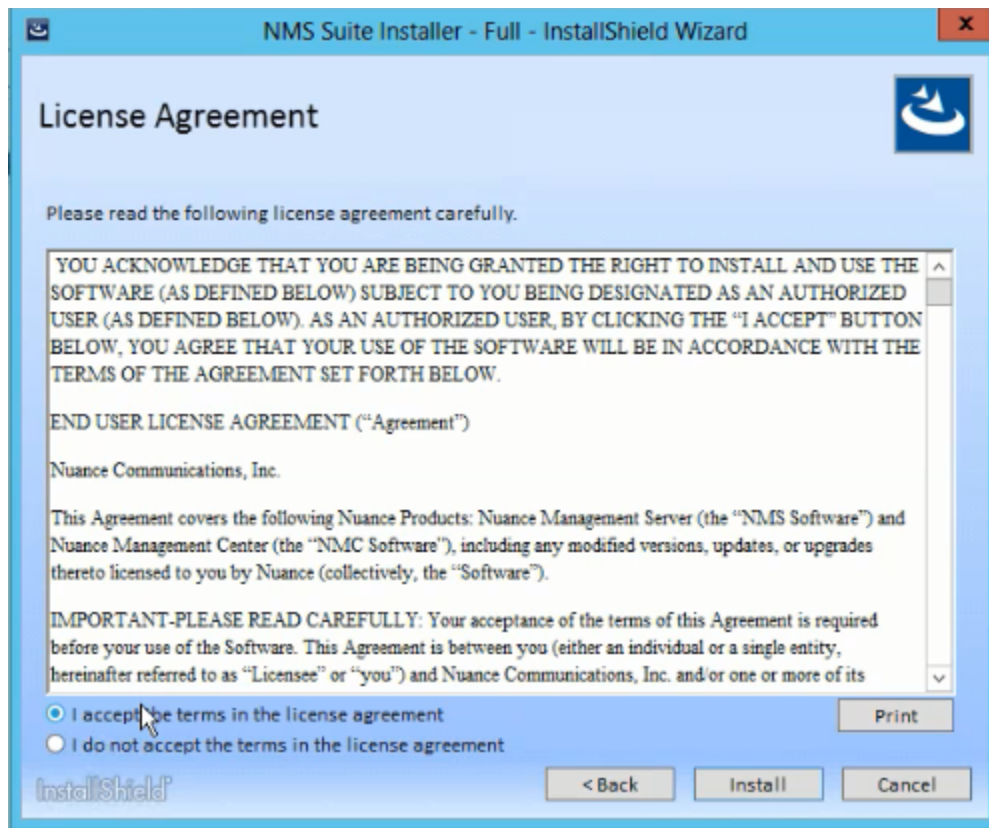
1. On your NMC server, right-click the `NMS Suite Installer - Full.exe` file, and then select **Run as administrator**.

The InstallShield Wizard opens.



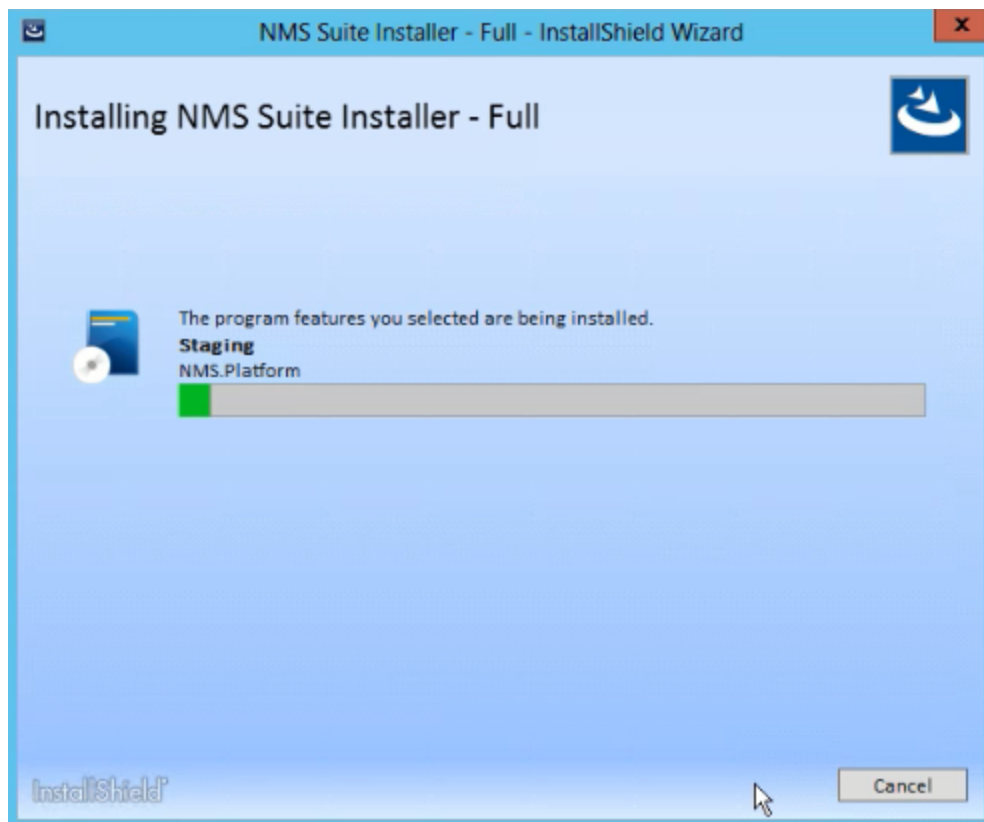
2. Click **Next**.

The License Agreement screen appears.

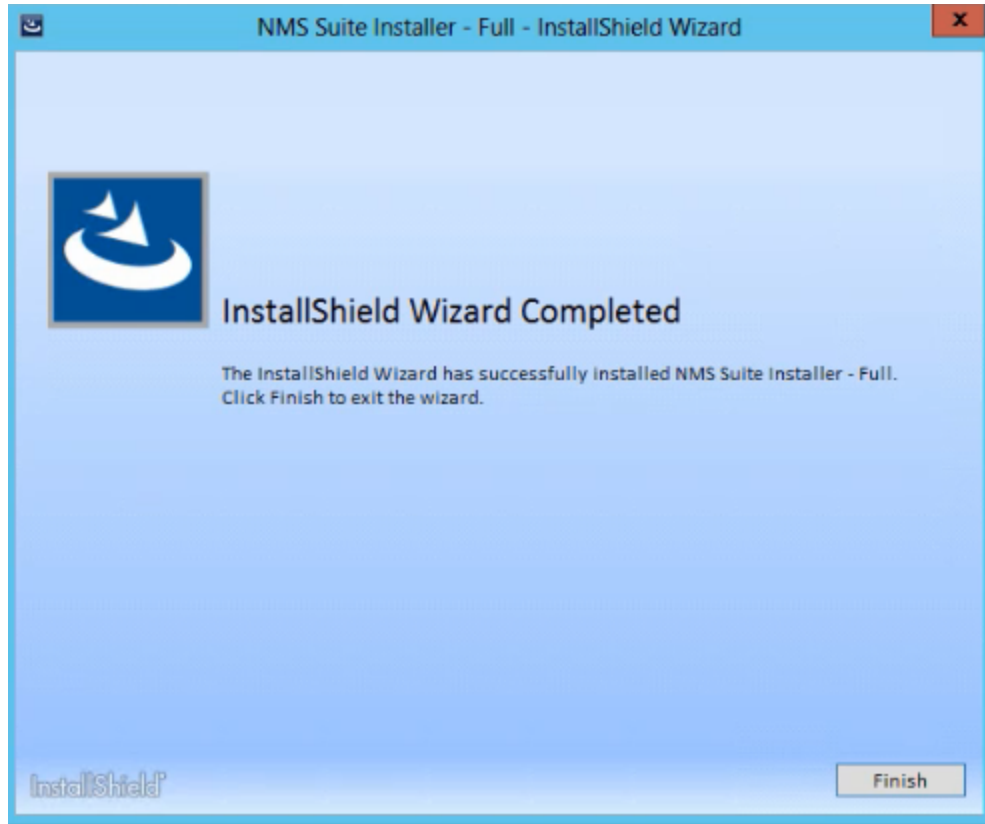


3. Select **I accept the terms in the license agreement**, and then click **Install**.

The upgrade begins.



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



Chapter 6: Preparing for your Active Directory single sign-on configuration

Single sign-on overview	61
Before you begin	62
Software requirements	62
Other requirements	62
Checklist—Planning the single sign-on setup	62
Creating an NMC console Administrator user for Active Directory	64
Setting the Active Directory connection string	65
Creating and configuring user accounts for single sign-on	66
Creating user accounts	66
Configuring user accounts	66
Running the SetSPN.exe Windows utility	67
About SetSPN.exe	67
Downloading SetSPN.exe	67
Executing SetSPN.exe	67

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 1](#).

- 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 2012
 - Microsoft® Windows Server 2012 R2 (64 bit)
 - Microsoft® Windows Server 2016
 - Microsoft® Windows Server 2019
- SSL certificate, issued by a certificate authority (CA)

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*.

- If you're using Kerberos authentication instead of NTLM, you must run the SetSPN.exe Windows utility.

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. For more information, see [“Running the SetSPN.exe Windows utility” on page 67](#).

Checklist—Planning the single sign-on setup

	Task	Reference
<input type="checkbox"/>	Ensure port 389 TCP is open.	“Opening required ports” on page 20
<input type="checkbox"/>	Create an NMC console administrator account for Active Directory	“Creating an NMC console Administrator user for Active Directory” on page 64

	Task	Reference
<input type="checkbox"/>	Set the Active Directory connection string	“Setting the Active Directory connection string” on page 65
<input type="checkbox"/>	Create and configure user accounts in the NMC console	“Creating and configuring user accounts for single sign-on” on page 66
<input type="checkbox"/>	Run the SetSPN.exe Windows utility (Kerberos authentication only)	“Running the SetSPN.exe Windows utility” on page 67
<input type="checkbox"/>	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 <i>Client Installation Guide</i> . 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. You can create user accounts manually in the NMC console, or you can batch-create them by importing an XML file. You can include each user's NTLM credentials in the XML file. 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:

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

For more information on creating user accounts manually or by XML import file, see the *Nuance Management Center Administrator Guide*.

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 NMS Platform Service Principal Name (SPN) with the Windows domain. You run this utility to indicate to the Windows domain that the NMS Platform service is valid and trusted on the domain.

During single sign-on, Dragon clients pass the credentials of authenticated Windows users securely to the NMS Platform service. The credentials are then validated on the NMC server. Dragon clients cannot connect to Nuance Management Center until you register the SPN (nms_spn) for the Nuance Management Center service.

You run the utility only when you're using Kerberos authentication instead of NTLM. You run the SetSPN.exe utility only once at any time before, during, or after your Nuance Management Center installation, 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.

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

```
SETSPN -S http/nms_spn <domain\service account>
```

where <service account> is the Windows user account that runs the NMS Platform service.

Note: There cannot be any other applications that require SPN registration on the Windows domain. If there are other registered applications on the domain and you attempt to register the NMS Platform service, a "Duplicate SPN found" error occurs.

Appendix A: Database backups and data retention

About database backups	69
Disabling automatic database backups	69
About data retention	70

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:\NMSDDBBACKUP 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

If you are a system administrator, you can optionally choose to disable the automatic backups and manage database backups yourself outside Nuance Management Center. You can disable automatic database backups during the installation, or after the installation in the NMC console System Settings. To disable automatic backups in the System Settings:

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 <div data-bbox="711 621 1409 684" style="border: 1px solid black; border-radius: 10px; padding: 5px;">Note: Converted usage data is never purged.</div>
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