Dragon® Medical 360 network edition

Installation Guide

2.7

NUANCE®

Copyright

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 Medical Network Edition 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.

L-3930

Contents

Document Versions

Version Number	Date
Initial version for DM Network Edition 2.7	6/3/2017

Introduction to installing Dragon Medical Network Edition

For information about installing or upgrading to Dragon Medical Network Edition, 2.7, please see chapter 1.

Dragon Medical Network Edition provides a central server (the *NMC server*) along with multiple local or remote speech recognition client machines where healthcare providers dictate. DM Network Edition takes advantage of distributed processing across servers and workstations for greater efficiency.

The *Installation Guide* takes you through the process of installing the various server and client components of DM Network Edition, connecting them to a database that stores your organization's data, and installing/setting up Dragon Medical Clients that work with both the *NMC server* and the other servers and components of the network.

Before you use this manual to install Dragon Medical Client, you should determine your network needs and be sure you have the required software by reading the *Planning and Deployment Guide*. That guide takes you through the process of planning deployment of a Dragon Medical Network Edition network, showing you how to determine the number of servers and other equipment you will need and how to prepare that equipment for installation of *Dragon Medical Enterprise*.

Note:

Some product features might have changed since this manual was printed. A current version of this book is always available on Nuance's documentation portal, in PDF format. Contact your Nuance representative about accessing that portal to retrieve the latest copy.

What's new in Dragon Medical Network Edition

What's new in Dragon Medical Network Edition, 2.7

Dragon Medical Network Edition, 2.7 includes the features, enhancements, and bug fixes from all previous service packs and hot fixes, plus new features.

For details about what's new in Dragon Medical Network Edition, 2.7 for administrators, see the following topics in the DM Network Edition Administrator Guide:

- What's new in NMC server - All products
- What's new in NMC server - DM Network Edition

Data objects are stored in the (NMC server) in the cloud (in the Nuance data center) instead of an on-premise NMC server. These objects include:

- User accounts
- Text and Graphics/auto-texts
- Custom words
- Custom command sets

To learn more about NMC server in the cloud, see the 'Introducing NMC server in the cloud' section in the DM Network Edition Administrator Guide or the Dragon Medical Network Edition, 2.7 release notes.

Installing or Upgrading an On-Premise Installation vs a Cloud Based Installation

Installing an On-Premise System

Use the instructions in the Dragon Medical Network Edition Installation Guide, starting with *Preparing to install Dragon Medical Network Edition* on page 5 and continuing to the end of the guide. Skip any sections or chapters about installing or upgrading the cloud based system.

Upgrading an On-Premise System

Use the instructions in *Upgrading an On-Premise Installation* on page 1. Skip any sections or chapters about installing or upgrading the cloud based system

Installing a Cloud Based System

Use the instructions in the Dragon Medical Network Edition Installation Guide, starting with *Overview of NMC server in the cloud* on page 1 of Dragon Medical Network Edition and continuing to *Installing and Configuring NMC server in the Cloud* on page 1. Skip any sections or chapters that do not mention the cloud based system.

Upgrading a Cloud Based System

Use the instructions in the Dragon Medical Network Edition Installation Guide, *Upgrade to NMC server in the cloud* on page 1 and continuing to the end of the cloud upgrade section. Skip any sections or chapters that do not mention the cloud based system.

.

Chapter 1: Preparing to install Dragon Medical Network Edition

System Requirements for Dragon Medical Network Edition

Hardware Recommendations

See the *DM Network Edition Planning Guide* for additional information on hardware and sizing.

Dragon Client Hardware Recommendations

CPU: 2.4 GHz Intel Dual Core or equivalent AMD processor. (IMPORTANT: SSE2 instruction set required) **Processor Cache**: 2 MB

DVD-ROM: drive required for installation

Sound Card: Creative® Labs Sound Blaster® 16 or equivalent sound card supporting 16-bit recording.

Free hard disk space: 5 GB required, 8 GB recommended

RAM:

- 4 GB for:
  - Microsoft® Windows® 10, 32-bit and 64-bit
  - Microsoft® Windows® 8 and 8.1, 32-bit and 64-bit
  - Microsoft® Windows® 7, 32-bit and 64-bit
  - Microsoft® Windows Vista®, 32-bit and 64-bit
  - Windows Server 2016
  - Windows Server 2012
  - Windows Server 2012
  - Windows Server 2008 R2

Microphone: Nuance-approved microphone (included in purchase)

For details on Bluetooth microphones, recorders, Tablet PCs, and other hardware, please go to http://support.nuance.com/compatibility/.

You can also use an iOS or Android device as a microphone using the Dragon Remote Microphone app.

Bluetooth (Optional): For Bluetooth wireless microphone support, visit http://support.nuance.com/compatibility/

Software Requirements

Software Requirements for the Dragon Client

The Dragon Client installer checks your system for minimum requirements. If the minimum requirements are not met, the installer will not install the client.

Operating system:

- Microsoft® Windows® 10 (including Professional and Enterprise), 32 bit and 64 bit
- Microsoft®Windows® 8.1, 32 bit and 64 bit
- Microsoft® Windows® 8 (including Professional and Enterprise), 32 bit and 64 bit
- Microsoft® Windows® 7, 32-bit and 64-bit
- Microsoft® Windows Vista® Service Pack 2, 32-bit and 64-bit
- 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
- Microsoft® Windows Server 2016

Software Requirements for the NMC server

Operating system:

Choose one of the following:

- 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

Whichever operating system you choose, you should have all service packs installed, up to the

most current one.

Microsoft .NET:

- Microsoft .NET Framework 4.5.2

Web Server

- Internet Information Services (IIS). Version 7.0, 7.5, 8.0, 8.5, or 10.0

Internet Browser: Microsoft Internet Explorer 9, 10, 11, Microsoft Edge (free download at www.microsoft.com)

SQL Server

- SQL Server 2008
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016

Software Requirements for the Profile Optimizer Nodes

Operating system:

Choose one of the following:

- Microsoft® Windows Server 2008 R2, 32-bit and 64-bit
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2016

Whichever operating system you choose, you should have all service packs installed, up to the most current one.

Microsoft .NET:

- Microsoft .NET Framework 4.5.2

Windows Installer 4.5 and 5.0 If you are installing a *Speech Node* on a machine with any supported operating system other than Windows Server 2008, the installer requires that the machine have Windows Installer 4.5 or greater on it. (Windows Server 2008 automatically installs a later version of Windows Installer.) For information on operating systems that support *Speech Nodes* refer to *Dragon Medical Enterprise Planning and Deployment Guide*.

Dragon Medical SDK Client You must install the latest version of the Dragon Medical SDK Client software on workstations where you plan to install *Speech Nodes*. This software is included on the *NMC server Software and Documentation* DVD.

Supported Virtual Desktop Infrastructure Applications and Terminal Emulators

- XenDesktop 7.11, and XenDesktop 7.13
- Wyse terminals

Supported non-EHR Applications

Once you have installed Dragon Medical, you can use it to control the following applications using your voice:

- WordPad
- NotePad
- Microsoft® Word 2010 (32 & 64 bit), 2013 (32 & 64 bit), 2016 (32 & 64 bit)
- Microsoft® Outlook® 2010, 2013, 2016
- Microsoft® Excel® 2010, 2013, 2016
- WordPerfect® x5, x6
- Apache OpenOffice Writer 3.4
- Open Office Writer v3.1, 3.2
- Internet Explorer 10, 11 (11 supported when Enhanced Protective Mode is disabled)
- Rich Internet Application IE10, IE11
- Rich Internet Application Google Chrome 16+
- Windows Live Mail v15 & v16
- Mozilla® Thunderbird™ x3 and up
- Lotus Notes 8.5

Configuring support for Windows Presentation Framework controls

In DM Network Edition, you can enable Full text Control support for Windows Presentation Foundation (WPF) based edit controls in either local applications (running on the same computer as Dragon) or in applications published from a Citrix server (and accessed through vSync (minidragon)).

By default, the Dragon installer, the Patch Installer, and the vSync (minidragon) installer will install but will not register Dragon WPF support libraries; disabling support for WPF edit controls in local and Citrix published applications.

You can enable support for WPF edit controls in local applications, published applications, or both. When you enable WPF support, the setting applies to all users of a Dragon installation.

On a command prompt, when you run the Dragon installer or the Patch installer on a workstation, or run the minidragon installer on a Citrix XenApp server, pass the "`TEXT_SERVICE_SUPPORT=1`" flag.

The flag causes the installer to install and register the WPF support libraries. Full Text Control support for WPF controls is enabled.

Notes:

- If you enable WPF support in local applications, but disable WPF support in published applications, WPF support is only available in local applications.
- If you disable WPF support by installing, re-installing, or upgrading Dragon, and enable WPF support by upgrading vSync on the server, WPF native support is disabled in both local and published applications.

Disable support for WPF controls in local and published applications

1. On the workstation where you will install or upgrade Dragon, open a command prompt.
2. Navigate to the location of the Dragon installer or the patch installer exe file.

3. Run the installer exe file, passing the "TEXT_SERVICE_SUPPORT=0" command flag as a parameter. For example:
   ```
   DMNE2DOT6.exe /V"/l* C:\Temp\dmnesetup.log TEXT_SERVICE_
   SUPPORT=0"
   ```
   Make sure there is no space between /V and the double quote (") character.

Disable support for WPF controls only in an application published from a Citrix server

1. On the Citrix server, open a command prompt.
2. Navigate to the location of the mindragon installer exe file.
3. Run the installer exe file, passing the "TEXT_SERVICE_SUPPORT=0" command flag as a parameter. For example:
   ```
   MiniTracker.exe /V"/l* C:\Temp\dmnesetup.log TEXT_SERVICE_
   SUPPORT=0"
   ```

Make sure there is no space between /V and the double quote (") character.

Enable support for WPF controls in local and published applications

Note: This requires WPF support libraries to be registered on the Citrix server.

1. On the workstation where you will install or upgrade Dragon, open a command prompt.
2. Navigate to the location of the Dragon installer (for Installing/Re-installing Dragon) or the patch installer exe file (for upgrading Dragon).
3. Run the installer exe file, and either pass the "TEXT_SERVICE_SUPPORT=1" command flag as a parameter or do not use the "TEXT_SERVICE_SUPPORT" flag.

   Example: Using the patch installer:
   ```
   DMNE2DOT6.exe /V"/l* C:\Temp\dmnesetup.log TEXT_SERVICE_
   SUPPORT=1"
   ```
   Make sure there is no space between /V and the double quote (") character.

   Example: Using the Full client installer:
   ```
   setup.exe /V"/l* C:\Temp\dmnesetup.log TEXT_SERVICE_
   SUPPORT=1"
   ```
   Make sure there is no space between /V and the double quote (") character.

Creating Accounts

Before you begin the installation, you create two user accounts, one for *Dragon Medical Network Edition* services to run under (see next immediate *Caution*) and one to install the software (see next section).

Caution:

Before you carry out this procedure, you must create ***a single Windows administrator account*** to run all services under (named something like **nmcapps**) that meets the following requirements:

- Is an administrator account in the domain or, for a single server configuration, the workgroup.
- Never expires.
- Has a password that never expires (does not have to be changed at regular intervals).
- Has rights to install software and Windows services on the server.
- Has rights to create and start a Windows service on the server.

VERY IMPORTANT:

- Has full read/write access rights to all other servers within the network.
- Has full read/write access to the database server (if it is on a separate server).
- Has full read/write/modify permissions to access the directory hosting the master user profiles.

You must set up this account with **Log on as Service** rights so that it can launch the services when the installation is complete.

Creating/selecting user account to install all services

Caution:

Before you carry out this procedure, you must create ***a single Windows administrator account*** to install all DM Network Edition services. That account must meet these requirements:

- Has rights to install software and Windows services on the server.
- Has rights to create and start a Windows service on the server.
- Has full read/write access to the database server.

VERY IMPORTANT:

You must use this account to install the database software and all servers in the product.

Installing Dragon Medical Network Edition

Before you begin the installation, you should evaluate your own system installation skill set. To select the appropriate hardware and install the *Dragon Medical Network Edition* server and client software, you should have adequate skills and experience to:

- Create a network domain/user account with full read/write access rights across all servers
- Create databases with SQL Server
- Set up backup plans for SQL Server
- Create and securely administer a Windows share
- Set Windows user rights and directory permissions
- Set up and configure Internet Information Services (IIS)
- Securely administer IIS (if using web server for master user profiles)
- Order, receive, and install SSL certificates in IIS (if using secure web server for master user profiles)
- Edit XML configuration files
- Manage Windows Services

Checklists for installing the NMC server and other servers

Installing Operating System software

On each physical server where you plan to install *NMC server* components:

❒ Install Windows Server. See *System Requirements for Dragon Medical Network Edition* on page 6 for the supported version.

❒ Install all available Windows Updates and service packs.

Decide to work in Active Directory

❒ Decide if you are going to be using *NMC server* in the Active Directory Services interface.

Creating required account

❒ Create single Windows administrator level account to run all *Dragon Medical Network Edition* services

Call it something like **nmcapps** and provide full access across all DM Network Edition servers and the master user profiles directory. Use this account to run all services, including SQL Server services, so that all servers run under the same account. You can also use this account to install all software on the network, but you can also make a separate
account that meets less stringent requirements.

Refer to *Creating Accounts* on page 12 and *Creating/selecting user account to install all services* on the same page.

Installing database software

❒ Install SQL Server. See *System Requirements for Dragon Medical Network Edition* on page 6 for the supported version.

❒ If you are using Active Directory Services, be sure to select **Mixed Mode** authentication.

Otherwise, Nuance recommends you select **Windows** authentication.

Refer to *Installing SQL Server* on page 33.

Refer to *Setting up the NMC server to run Active Directory Services* on page 164.

Installing NMC server, NMC console, and Database

Gather information you need:

- ❒ Name or IP address of machine for this server: _____
- ❒ Name or IP address of database server: _____
- ❒ Name or IP address of machine to host master user profiles or URL to web server or SSL web server to host master user profiles: _____
- ❒ Your customer ID _____

Install prerequisite software:

❒ Install .NET Framework and all available updates. See *System Requirements for Dragon Medical Network Edition* on page 6 for the supported versions.

Refer to *Installing prerequisite software for NMC server* on page 1.

❒ Install Internet Information Services. See *System Requirements for Dragon Medical Network Edition* on page 6 for the supported version.

Refer to *Installing prerequisite software for NMC server* on page 1.

- ❒ Enter server name or IP address of *NMC server SQL Database*.
- ❒ Enter SQL Server Login (sa) and password.
- ❒ Enter information about the user account that will run all DM Network Edition servers.

  Refer to *Installing NMC server and NMC console* on page 1.

Open required ports on NMC server and hardware firewalls:

See 'Ports to open for clients, servers, and hardware firewalls' in the Dragon Medical Network Edition Planning guide.

Installing Speech Nodes

Gather information you need:

❒ Name or IP address of machine for this server: _____

❒ Name or IP address of database server: _____

_____

❒ Name or IP address of machine to host master user profiles or URL to web server or SSL web server to host master user profiles: _____

❒ Path to where you want *Dragon* logs written (if not the default):

_____

To install Profile Optimizer Speech Node alone on machine or virtual machine:

Install prerequisite software for Profile Optimizer Speech Node:

❒ Install .NET Framework 4.5 and all available updates.

❒ Install Windows Installer 4.5 or greater on machine.

❒ Install *Dragon Medical SDK Client* on machine.

Refer to *Installing prerequisite software for speech nodes* on page 83

Checklists for Setting up Active Directory Services

To set up your *NMC server* to run in Active Directory Services you should take particular actions during each step of the *Dragon Medical Network Edition* installation and *NMC server* setup process. The steps that require you take action are named in the headings below.

For details on each step, refer to *Setting up the NMC server to run Active Directory Services* on page 164.

Installing SQL Server 2008, 2012, 2014, and 2016

❒ For SQL Server 2008, select **Mixed Mode** authentication for accessing database.

Creating NMC Administrator Account for Active Directory Administrator

To create an **NMC Administrator** user account for the Active Directory Administrator:

❒ If you have not already done so, install the *NMC server*.

❒ Log in through the *NMC console* using the login and password that Nuance provides.

❒ Create a user account for the Active Directory administrator (see the *NMC server Administrator Guide* for details on setting up user accounts). You can add this account to the default **NMC Administration** group that comes with the product.

❒ (Optional, as you can create them later) Create all other user accounts, adding some to the default **NMC Administration** group that comes with the product and others to the default **DM Network Edition** group that comes with the product.

Logging Out and logging back in

❒ Log out of the *NMC server*.

❒ Stop and restart the Nuance Management Service.

❒ Log back in through the *NMC console* as Active Directory administrator.

❒ Revoke the **NMC Administrator** license of the original admin user account, as it does not work in Active Directory.

Creating Active Directory Single Sign-On user accounts (optional)

You need to create these accounts before you can associate a user account with an already existing upgraded master user profile.

❒ Create Active Directory user accounts/logins.

❒ Create Single Sign-On user accounts with same login name as their Active Directory accounts.

Continue to Configure NMC server as Active Directory Administrator

❒ Follow instructions in *NMC server Administrator Guide*.

Checklists for Starting the NMC server and other servers

Services should start as soon as the servers are installed. To verify that the *NMC server* is running and ensure it can talk to the *Speech Nodes*:

❒ Verify that you can log in to the *NMC console* using the supplied login and password.

❒ Ensure that the *NMC server* can communicate with *Profile Optimizer Speech Nodes*.

Refer to:

Logging in to the NMC server through the NMC console on page 1

Verifying server services are running

❒ Check for the status of each of the following services in the **Services** dialog box on corresponding physical servers:

- ❒ Nuance Management Service
- ❒ Profile Optimizer Speech Node

❒ If any service is not running, start that service.

Refer to *Starting the NMC server* on page 90.

If you are planning to use Active Directory Services

❒ Proceed to *Checklists for Setting up Active Directory Services* on page 17.

Checklists for Setting up a file server for master user profiles

❒ Select a machine to host the master user profiles.

❒ Be sure that the machine is a Windows server or workstation with .NET Framework installed (See *System Requirements for Dragon Medical Network Edition* on page 6 for the supported version.) and that the machine is in the same Windows domain as your *Dragon Medical Network Edition* servers.

❒ If you are using a RAID array or other storage device, be sure that it is connected to a server or workstation running Windows with .NET installed (See *System Requirements for Dragon Medical Network Edition* on page 6 for the supported version.) and that the machine is in the same Windows domain as your DM Network Edition servers.

❒ Create top level master user profile directory on the host.

❒ For each site, create a subdirectory under the master user profile directory.

  ❒ Share the top level master user profiles directory in Windows and give **Everyone** full read/write/modify control over the directory.

On each *Dragon Medical Client* workstation:

  ❒ If workstations will access the profiles over a mapped network drive, map a drive to the master user profiles location.

  ❒ If workstations will access the profiles through a UNC path, ensure the workstations have access to that path.

Refer to *Choosing a master user profiles location for a site* on page 96 and *Setting up a computer to host master user profiles* on page 98.

In the *NMC console*, in the **Master User Profiles Directory Settings** dialog for each site:

❒ Set **Location** to path each workstation later uses to access the master user profiles.

❒ Set **NMC UNC Path** to path the *NMC server* later uses to find the master user profiles.

Refer to *Setting up a computer to host master user profiles* on page 98.

Checklists — Setting up web server to host master user profiles

❒ Be sure that the web server machine is a Windows server or workstation with .NET Framework installed (see *System Requirements for Dragon Medical Network Edition* on page 6 for the supported version) and that the machine is in the same Windows domain as your DM Network Edition servers.

❒ Install the web server or secure web server.

Refer to *Installing software for storing master user profiles on a web server* on page 101.

❒ Create top level master user profile directory on the web server.

❒ Share the top level master user profiles directory in Windows and give **Everyone** full read/write/modify control over the directory.

On each *Dragon Medical Client* workstation:

- ❒ If workstations will access the profiles through an **https** connection, install the required certificate on each workstation.
- ❒ If master user profiles are on an **http** web server, see the Planning guide about the port to open.
- ❒ If master user profiles are on an **https** web server, see the Planning guide about the port to open.

Refer to: *Choosing a master user profiles location for a site* on page 96 and *Setting up a computer to host master user profiles* on page 98.

In the *NMC console* , in the **Master User Profiles Directory Settings** dialog for each site:

❒ Set **Location** to path each workstation later uses to access the master user profiles.

❒ Set **NMC UNC Path** to path the *NMC server* later uses to find the master user profiles.

Refer to *Setting up a computer to host master user profiles* on page 98.

In the *NMC console*, in the **HTTP Settings** or **SSL Settings** dialog for each site:

❒ Set **HTTP Settings** for an **http** web server.

Refer to *Setting HTTP connection settings for web server* on page 105

❒ Set **SSL Settings** for an **https** web server.

Refer to *Setting SSL connection settings for secure web server* on page 108

Checklist for upgrading roaming user profiles

To upgrade each directory of roaming users from Version 10.x of *Dragon Medical*, be sure to take ***all steps below*** in the order presented, starting with *Before you upgrade*, proceeding to *Upgrading*, and then to *Associating user accounts with newly upgraded master user profiles*. (You do not have to upgrade roaming users from Version 12 or later of *Dragon Medical*.)

❒ Be sure that all user profiles for a single site are in their own subdirectory of the master user profiles directory.

❒ Schedule the upgrade process during hours when dictation is not occurring.

Before you upgrade

❒ Back up your Version 10.x user profiles.

❒ Install *Dragon Medical SDK Client* on the machine where you are upgrading the profiles.

❒ Create lists of the different source directories of roaming user profiles you are upgrading.

❒ Copy profiles from a single directory to their folder on the upgrade machine.

❒ On the upgrade machine, create a directory for the newly upgraded profiles to be stored in.

❒ In *NMC console*, create user accounts for all providers whose profiles you are upgrading.

❒ Be sure that providers whose profiles you are upgrading are not dictating with *Dragon Medical*.

Refer to *Creating user accounts for healthcare providers* on page 117 and

Before upgrading Dragon roaming user profiles on page 1

Upgrading

For each directory of roaming users being upgraded to master user profiles:

❒ On the upgrade machine, start the **upgrade.exe** utility.

❒ In the **User Upgrade Wizard**, add the existing user profiles.

❒ Execute the upgrade and choose the directory to store the newly upgraded profiles.

❒ (Optional) In **Advanced Options** dialog, modify user information, such as the vocabulary.

❒ Start the actual upgrade process by clicking **Begin** and click **Finish** when it completes.

❒ Copy the new master user profiles to the master user profiles host on the network.

Refer to *Upgrading Dragon roaming user profiles to master user profiles* on page 1.

Associating user accounts with newly upgraded master user profiles

Note: Be sure you have already upgraded the profiles or you will not see them in the **Profiles** list.

Refer to *Associating new user accounts with upgraded user profiles* on page 130.

Checklists — Converting local users

Schedule the conversion process during hours when dictation is not occurring.

Before you convert

❒ Back up your Version 10 local user profiles.

❒ Be sure that providers whose profiles you are upgrading are not dictating with *Dragon Medical*.

(If applicable) Combine multiple Dragon Medical Client profiles for a single provider, keeping only one

❒ Export custom words from extra profiles.

❒ Export custom commands from extra profiles.

❒ Export vocabularies from extra profiles.

❒ Import the exported custom commands into the profile you are retaining.

❒ Import the exported vocabularies into the profile you are retaining.

❒ Import the exported words into the profile you are retaining.

Exporting local user profiles

In Dragon Medical Network Edition, 2.7, you use the Dragon client to export and import user profiles. For details, see the Dragon Help.

❒ Create temporary location for local user profiles that exist.

❒ Create temporary location for roaming user profiles you will create as part of conversion.

❒ In *Dragon Medical Practice Edition*, export local user profiles to the roaming user profiles location you created.

Enabling roaming feature on workstation

❒ In *Dragon Medical Practice Edition* , enable the **Roaming** feature in **Administrative settings**.

❒ Save the local users to the roaming user location you created.

Associating user accounts with newly converted master user profiles

Note: Be sure you have already converted the profiles or you will not see them in the **Existing Profiles** list.

❒ In *NMC console*, create a user account for each provider.

❒ In *NMC console*, open the **User Profile Association** tool.

❒ Select a user account from the list of **User Accounts**.

❒ Select an upgraded profile for the user account from the list of **Existing Profiles**.

❒ Click the **Associate** button.

❒ Repeat the process for each user profile.

Refer to *Associating new user accounts with upgraded user profiles* on page 130.

Migrating roaming users to *Dragon Medical Network Edition*

❒ In *NMC console*, create user accounts for all providers whose profiles you are converting.

❒ Copy the temporary roaming users you just created to a subdirectory of the master user profiles directory on the network.

❒ In *NMC console*, associate new user accounts with the newly converted user profiles.

❒ On the workstation install the Dragon Medical Client.

❒ Log in using the new user account login and password.

Refer to *Migrating Non-Network Dragon User Profiles to the NMC server* on page 117.

Checklist for installing Dragon Medical Clients

There are several approaches to installing *Dragon Medical Client* and this checklist includes first pre-requisite steps, then steps for each type of installation.

Before removing earlier version of Dragon Medical

❒ Be sure you have converted any local user profiles from an earlier version of *Dragon Medical* to roaming user profiles before you remove the already existing installation of *Dragon Medical*. For instructions on how to convert the users, refer to *Migrating Non-Network Dragon User Profiles to the NMC server* on page 117.

Before beginning any client installation to a workstation

❒ Be sure workstations meet the requirements for installing *Dragon Medical Client*.

❒ Be sure that the account that each *Dragon Medical Client* workstation runs under has full read/write/modify access to the master user profiles directory.

❒ Be sure you have the *Dragon Medical Client* serial number on hand.

Downloading Dragon Medical Client MSI installer through the NMC console

❒ On the client workstation, log in as a Windows administrator.

❒ Log in to the NMC console.

❒ Set the location of the Dragon MSI install file on the *NMC server* in the **System Settings > DM Network Edition.**.

❒ Download the MSI installer for the *Dragon Medical Client* from the *NMC console*.

❒ Log in to the client using a user account and enter the name of the *NMC server*.

Refer to *Associating Dragon with the NMC server or the Local Authenticator* on page 138.

Installing Dragon client manually

❒ Insert the *Dragon Medical Enterprise client* software DVD into the DVD reader of the workstation.

❒ Browse the DVD and double click the **setup.exe** file.

❒ Follow the wizard instructions.

❒ Log in to the client using a user account and enter the name of the *NMC server*.

Refer to *Installing Dragon manually outside of the NMC console* on page 137 and *Associating Dragon with the NMC server or the Local Authenticator* on page 138.

Pushing Dragon MSI installation to multiple workstations: administrative installation

❒ Copy and modify the **admininstall.bat** file provided on the *Dragon Medical Enterprise client* software DVD.

❒ Use any of the options or variables in the tables provided:

General options for installing Dragon

MSI options for installing Dragon features/advanced options

Pushing Dragon MSI installation to multiple workstations: using SCCM

❒ Create MSI installer to use with SCCM to install *Dragon Medical Client* on several workstations.

Refer to *Pushing the Dragon MSI installation to workstations* for more information.

Pushing Dragon MSI installation to multiple workstations: creating custom installer for Active Directory

❒ Create the custom installer for *Dragon Medical Client* following the instructions provided.

Refer to *Creating a custom installer for the client in Active Directory* on page 148

Chapter 2: Installing the NMC server and components

To install the *NMC server* and its components for the Dragon Medical Network Edition network, you carry out the procedures in these sections:

Prerequisites for installing the NMC Servers and NMC console

Before you actually install the *NMC server* and *NMC console*, you should gather the information indicated below and make modification to your machine's security policy.

Creating an account to run all services

Note:

Before you carry out this procedure, be sure you have a Windows administrator account for running the server under, (named something like **nmcapps**) that meets the following requirements:

- Is an administrator account in the domain or, for a single server configuration, in the workgroup.
- Never expires.
- Has a password that never expires (does not have to be changed at regular intervals).
- Has rights to install software and Windows services on the server.
- Has rights to create and start a Windows service on the server.
- Has full read/write access rights to all servers within the same network.
- Has full read/write access to the database server (if it is on a separate server).
- Has full read/write/modify permissions to access the directory housing the master user profiles.

During the installation, the wizard prompts you to enter the name of this user account and the password to it.

Important: You should run all of the services of the product using this same account.

If you are creating the account for someone else to log in and install the software, the account only need to be able to run *NMC server* services and does not require **Log into workstation** rights.

Information requirements for installing the NMC server and NMC console

Before you begin, you need to have the following information:

Name or IP Address of NMC server Machine—You need the name or address of the machine where you intend to install the *NMC server* . If your network uses dynamic addresses, you should use the computer name to identify it, just in case the dynamic address changes in the future.

Name or Address of Database Machine—You need the name or address for the server machine where you either have installed or plan to install the *NMC server SQL Database*. If your network uses dynamic addresses, you should use the computer name to identify it, just in case the dynamic address changes in the future.

Installing SQL Server

Before you install the *NMC server* , you must install the database server first.

Before you begin database software installation

Before you begin installing the database software, have the following information on hand:

- Machine name or IP address of the database's physical server.
- Windows user account name and password you want the database server to run under.

Caution:

Nuance recommends that you run all server DM Network Edition services and even all database services under the same Windows user account.

Installing SQL Server

You can also install SQL Server 2014 and 2016 on Windows Server 2012 and Windows Server 2016.

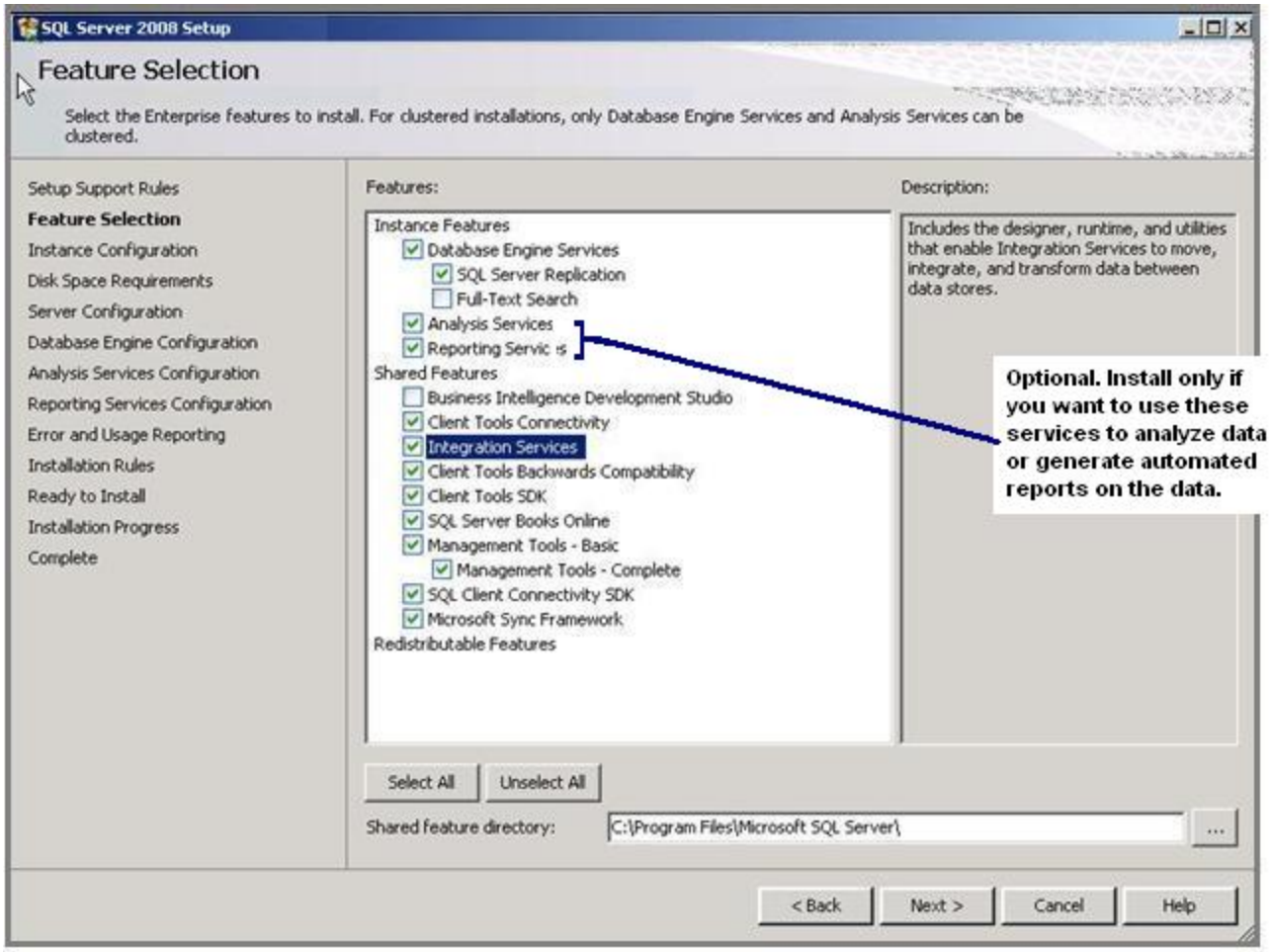
The following information is about installing SQL Server 2008.

To install SQL Server 2008 from the *NMC server MS SQL 2008* DVD provided in the DM Network Edition software package you received from Nuance:

1. Log on to Windows as an Administrator or as a domain user who has local administrative rights. If you do not have that type of Windows account, create one first.
2. Using Windows Explorer, find and note which of the non-operating system hard drives has the most unused space on it.
3. Insert the *NMC server MS SQL 2008* DVD into the slot on your physical server.
4. If the install installation does not start automatically, find the **setup.exe** file on the DVD and double click on it to start the installation.
5. When the **SQL Server Installation Center** dialog box appears, select **New SQL Server stand-alone installation or add features to an existing installation** option.

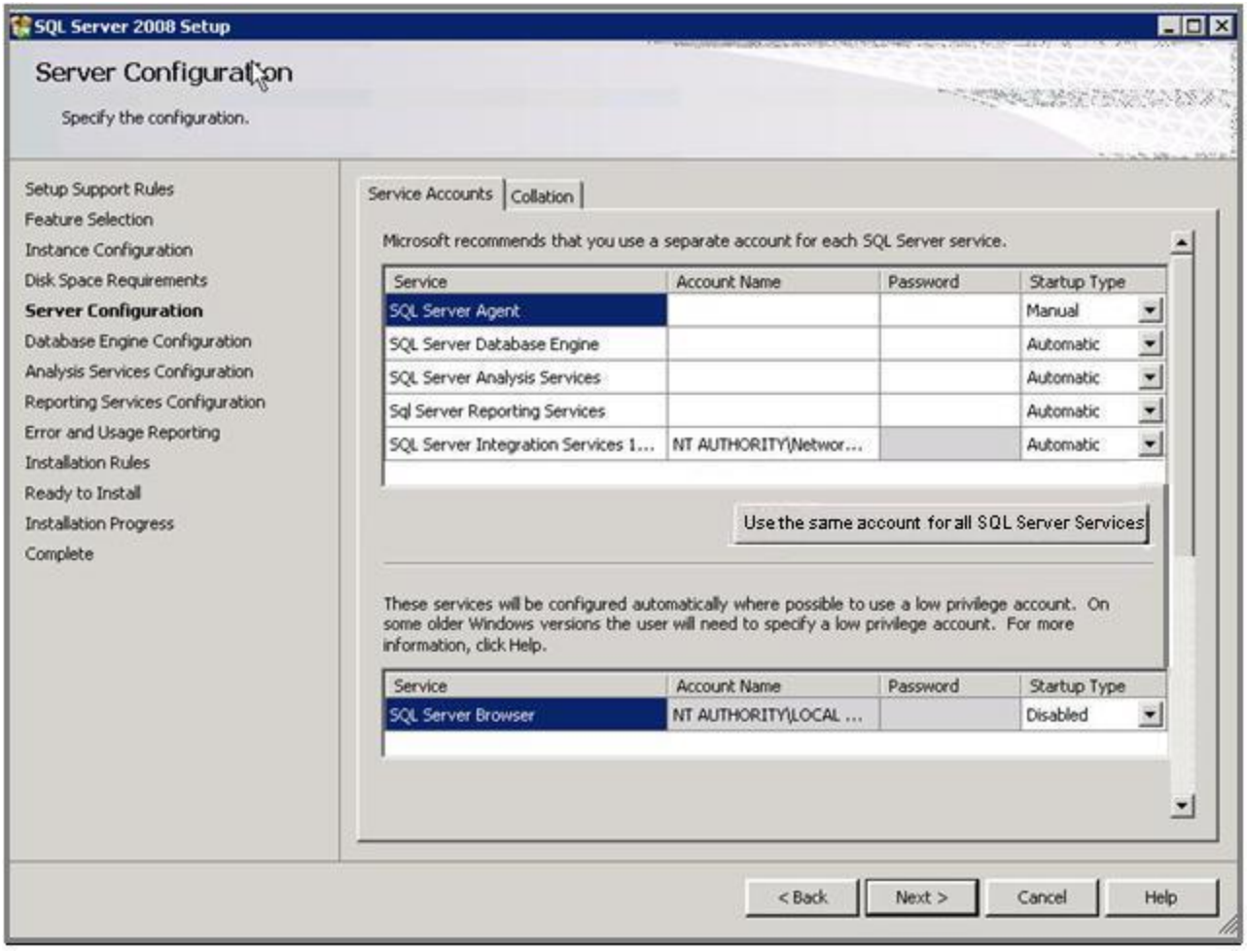
6. When the **Setup Support Rules** dialog box displays, click **Install**.
7. When the **Product Key** page is displayed, the SQL product key is automatically entered as it is embedded within the Nuance-provided SQL software DVD. The product key will not have to be entered manually. Click **Next**.
8. When the **License Terms** page of the wizard appears, check the box next to **I accept the license terms** and click **Next**.

9. If you are asked to create a local user with Administrative privileges and you do not have such an account, create one now and click **Next** to continue.
10. In the **Feature Selection** page, under **Instance Features**, you only need to select **Database Engine Services**. Under **Shared Features** > **Management Tools**, only **Basic** and **Complete** are required. All other features are optional. Click **Next** to continue.
    Note: **Analysis Services** and **Reporting Services** are not required by the *NMC server*; however, if any problems occur with your installation or later with your databases, these services can help Nuance technical support troubleshoot the problem, so you might choose to install them as a proactive measure.



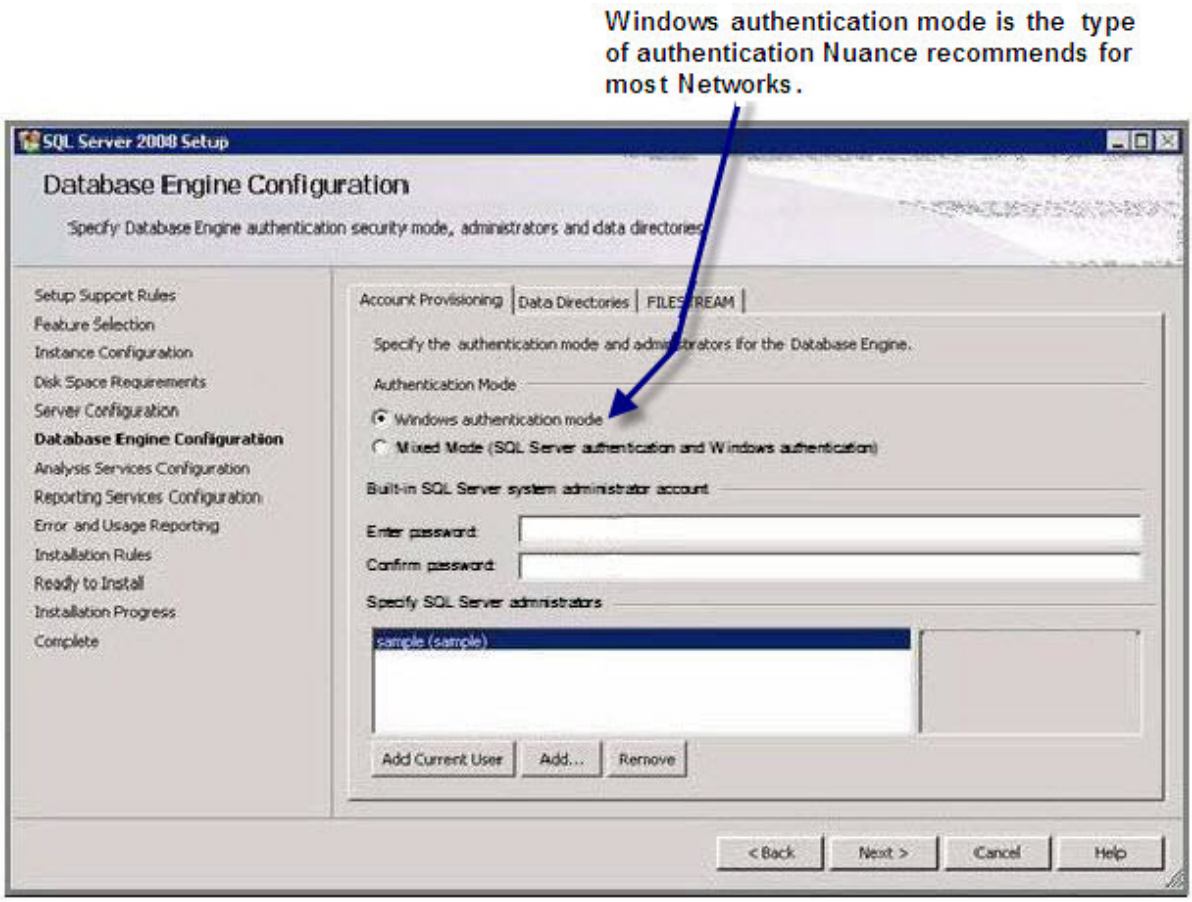
12. When the **Instance Configuration** page of the wizard displays, leave the **Default instance** option selected and click **Next**.

13. When the **Disk Space Requirements** page of the wizard displays, verify that you have adequate storage space on the server and click **Next**.
14. When the **Server Configuration** page of the wizard displays, click the **Use the same account for all SQL Server services** button.

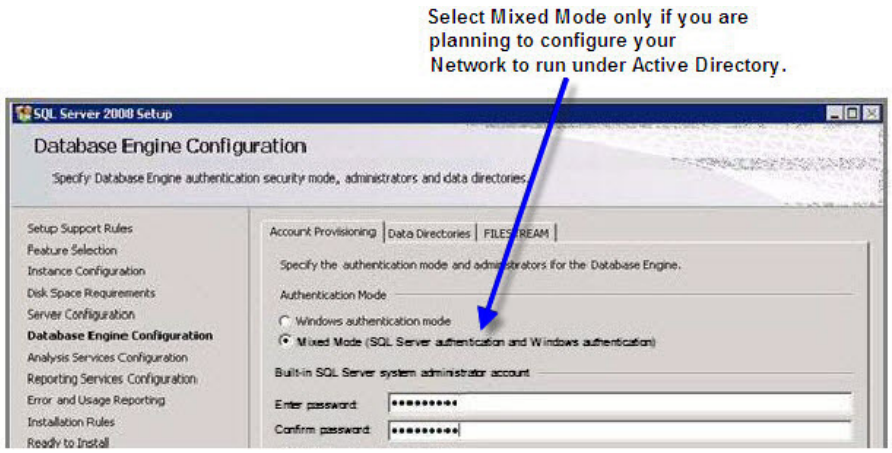


15. When the **Use the same account for all SQL Server 2008 services** popup appears, enter the username and password of the Windows user account that the SQL Server services should all run under and click **OK**. You should use the same account that the product services will run under. That account can be in a workgroup instead of a domain and Nuance recommends that you use an account in a workgroup if you are planning to install all DM Network Edition servers along with the database on a single machine.

    Enter the name of the domain where the server resides followed by a backslash and then the user name for the account. Enter the password other servers and clients on the Dragon Medical Network Edition network will use to access the database.



16. When you return to the wizard, click **Next**.
17. When the **Database Engine Configuration** page of the wizard appears, you choose the type of authentication you want to use when allowing access to the SQL Server database.
    - Under **Authentication Mode**, Nuance recommends that you select **Windows Authentication Mode** (see illustration above). You would select **Mixed Mode** only if you plan to later attach to the database using an Active Directory account or an SQL Server account. Keep in mind that SQL Server accounts have full access to the database.

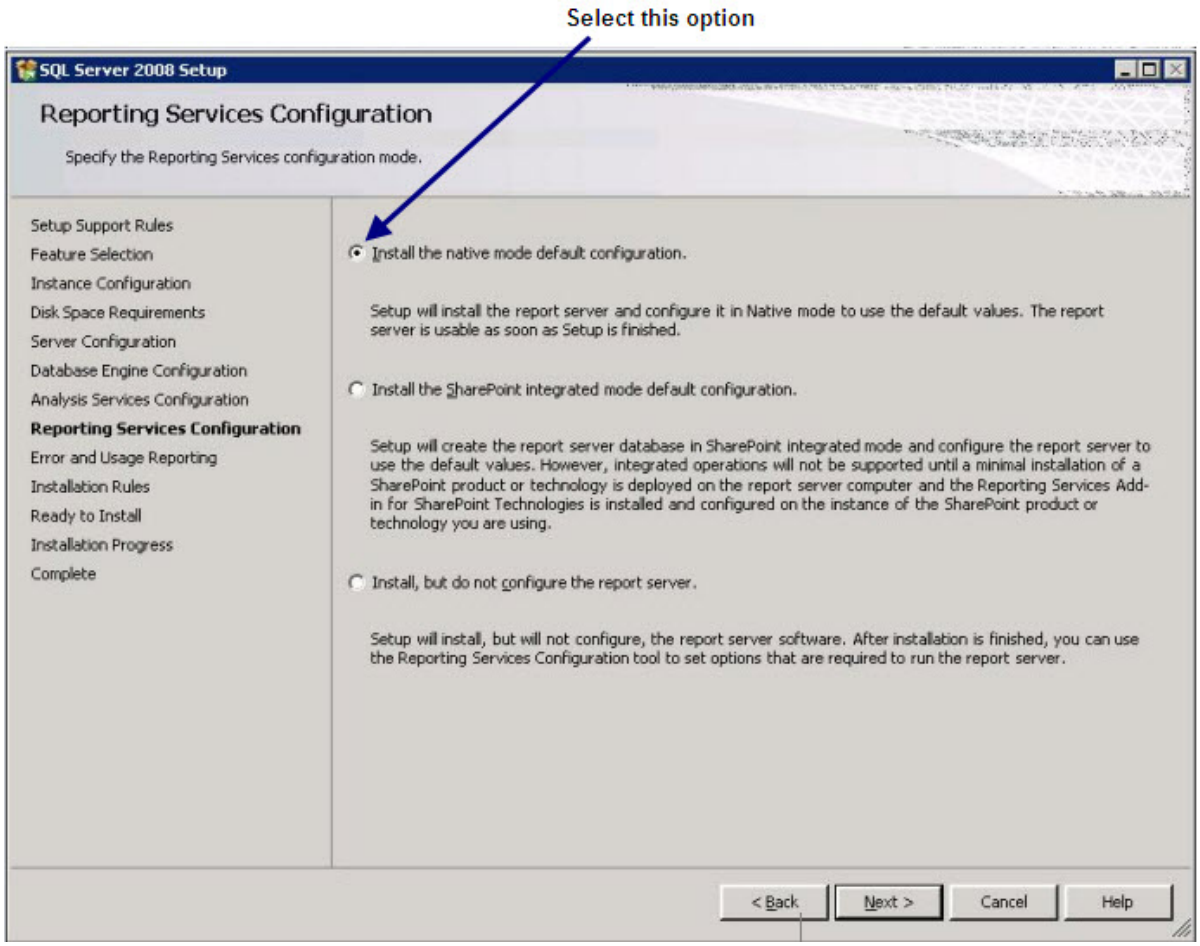


- If you select **Mixed Mode**, then under **Built-in SQL Server system administrator account**, enter the password in **Enter password** and type the password a second time in **Confirm password**.
- Regardless of the type of authentication you choose, under **Specify SQL Server administrators**, click **Add...** and add the account you are installing under to make that account an SQL Server administrator will full access to the database, as you will need that access later in the installation process.

18. Still on the **Database Services Configuration** page of the wizard, to add the user account for the person is carrying out the installation to the list of users who can administer the database, click **Add Current User...** The user's name then appears in the list under **Specify SQL Server administrators**.
19. Click **Add** and add the account you created for all services to run under, to ensure it not only has access to the database, but can also administer the database.
20. Finally, click **Add** again and add at least one other user to the list to ensure that if either of the first two accounts is accidentally locked out of the database, you have one more account with the ability to administer the database.

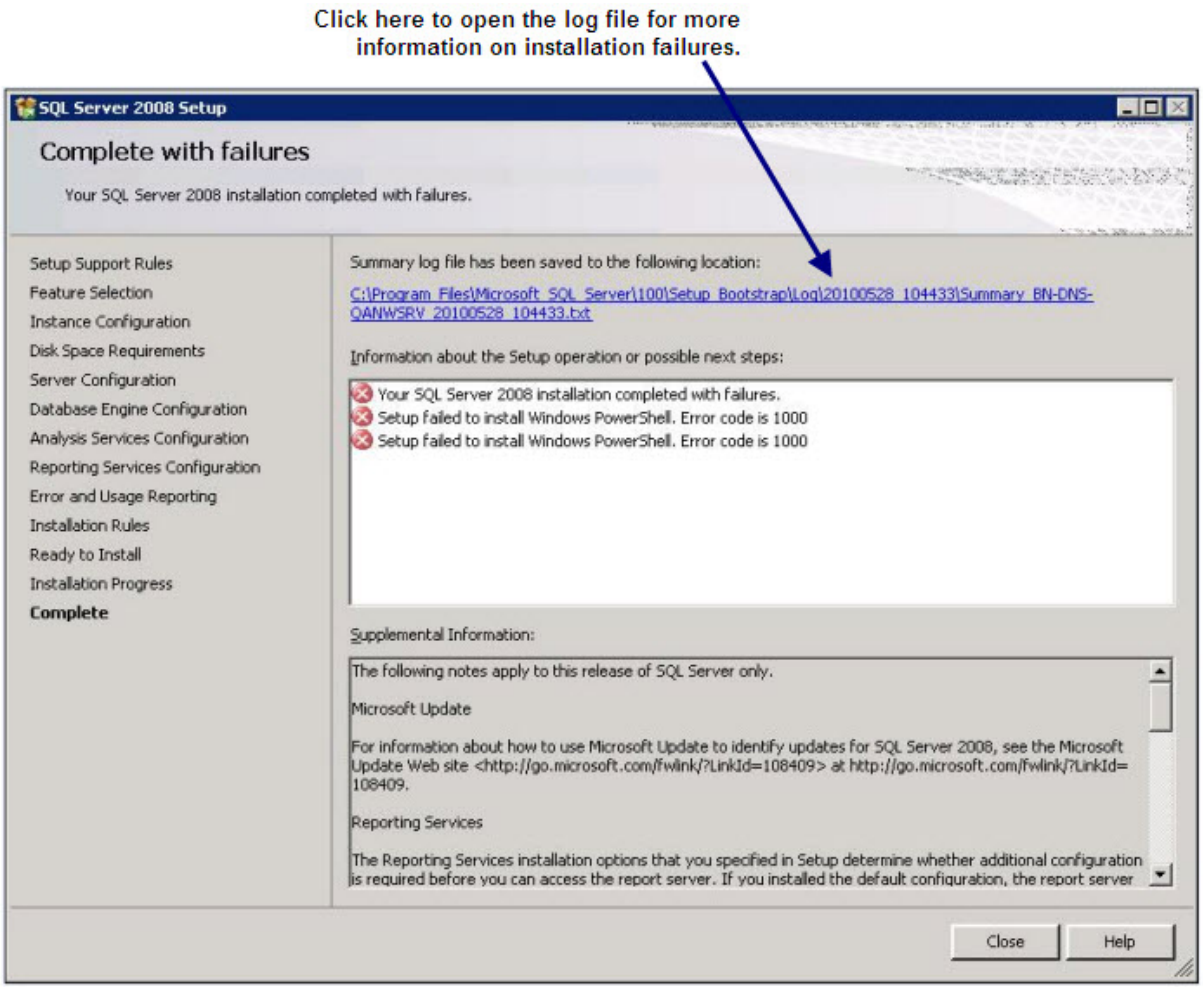
When you have added all these users to the database administrator list, click **Next**.

21. When the **Analysis Services Configuration** page of the wizard displays, under the **Account Provisioning** tab, click the **Add Current User** button to add the installer's user account to the list of users who can have access to the Analysis Services.
22. Click the **Add** button and add the **nmcapps** user account to give that account access to the Analysis Services.
23. Click the **Add** button again and add the database administrator account to give that account access to the Analysis Services; then click **Next**.
24. When the **Reporting Services Configuration** page appears, select **Install the native mode default configuration** and click **Next**.



25. Skip the **Error and Usage Reporting** page and click **Next**
26. Click **Next** until you reach the **Ready to Install** page of the wizard.
27. Click **Install** and wait for the installation to complete.

28. If you experienced any failures while running the wizard, the **Complete with failures** page appears.



If you receive this page, click on the link near the top of the page under **Summary log file has been saved to the following location** and save the log in a location where you can retrieve it. If you later have any network issues, you can provide this log file to the Nuance support team.

29. After the installation is complete, to verify that all SQL Server database services are running before you begin to install the DM Network Edition servers, select **Start > Administrative Tools > Services** and check the **Services** window.

Ensuring all required ports are open

See 'Ports to open for clients, servers, and hardware firewalls' in the Dragon Medical Network Edition Planning guide.

Configuring the network traffic switch to ping NMC servers for load balancing

If you have a large network with multiple *NMC servers*, you can include a network traffic switch in your network to balance the load on the *NMC servers*. The network traffic switch can be an F5 or similar switch.

To configure the network traffic switch to send a message to the *NMC server* to see if the server is operational, you would have the network traffic switch send the following message in the URL line of the browser:

```
https://<yourserver>/NMS/Platform/ConfigurationSvc/v1/Status
```

The *NMC server* delivers the following XML-formatted response to the network traffic switch:

```
<<PlatformStatus xmlns=
"http://schemas.datacontract.org/2004/07/NMS.Platform.Objects" xmlns:i-
i="http://www.w3.org/2001/XMLSchema-instance">
<Status>Running</Status>
<ServerDateTimeUTC>2017-01-05T21:48:47.7895755Z</ServerDateTimeUTC>
<NMSVersion>5.6.98.0</NMSVersion>
<Products>...</Products>
</PlatformStatus>
```

If the *NMC server* is down, the switch receives an error. If the network traffic switch makes this call and the *NMC server* sends anything other than the expected response, the switch can tag that server as down and reroute the traffic accordingly.

About SSL certificates

Using SSL requires that you obtain an SSL certificate. Nuance Management Center supports both signed certificates from a certificate authority, and unsigned (or internally generated) certificates. However, Nuance strongly recommends that you use a signed certificate, as self-signed certificates are not always easily recognized by the client the same way signed certificates are.

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.

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.

For more detailed information on installing SSL certificates, see:

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

Install an SSL certificate on a load balancing switch

Nuance uses this mode in the Nuance data center 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. In the NMC Platform installation folder, find and open the Nuance.NMS.Server.exe.config file.
2. In the file, find the line near the top that contains the key="UseSSL" tag.
3. Change the value to false:
   ```
   <add key="UseSSL" value="false"/>
   ```
4. Restart the NMC server to allow the configuration changes to take effect.

Install an SSL certificate on the NMC server or the Local Authenticator

In this configuration, messages are sent over HTTPS. The messages are not encrypted. However, the HTTPS channel is encrypted.

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. Note 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. Bind the SSL port (443) used by the services to the certificate.
   Windows Server 2008, 2012, or 2016:
   Using the netsh utility, run the following command to bind port 443 to the certificate :
   netsh http add sslcert ipport=0.0.0.0:443 certhash=<thumbprint>
   appid={00000000-0000-0000-0000-000000000000}
5. 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"/>
6. 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.

7. Restart the NMS Platform server or Local Authenticator 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.

Note: If you are testing "Install an SSL certificate on a load balancing switch", you cannot run these tests from inside the firewall.

Use the NMS Port Checker Tool

Run the port checking tool, and see if it can access the NMS server properly.

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?

   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 NMC server is configured and working properly.

Check the Bindings

If the NMC console is not working, make sure that the ports are properly bound to the SSL certificate. You can do this by using the "httpcfg help" (Windows 2003) or "netsh http show sslcert" (Windows 2008) commands to display the current configuration. Be sure that port 443 is bound to the certificate.

Remove SSL Certificate support from the NMC server or the Local Authenticator

1. In the NMC server configuration file, find the line that contains the 'key-y=SeviceDeploymentMode' tag.
2. Change the value= section to "wsHttpMessage".

   When completed, the line should appear as below.

   `<add key="SeviceDeploymentMode" value="wsHttpMessage "/>`.
3. In the NMC server configuration file, find the line that contains the 'key=UseSSLForRest' tag.
4. Change the value= section to "false". When completed, the line should appear as below.

   `<add key="UseSSLForRest" value="false"/>`.

Chapter 3: Install or Upgrade to NMC server 5.x

To install or upgrade to NMC server 5.x, you carry out the procedures in these sections:

Install NMC server 5.x for a single-node or multiple-node configuration

This topic is for customers that do not have an existing NMC server installation and that are installing the Dragon Medical Network Edition 2.7 client.

Notes:

- All installations of NMC server 5.x and later require an SSL certificate from a certified authority (CA).
- Supported versions of SQL Server:
  - SQL 2008 R2 - See Installing SQL Server.
  - SQL 2012
  - SQL 2014
  - SQL 2016
- Supported versions of Windows:
  - Windows 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- .NET Framework 4.5.2 is required for the NMC server , the PO Speech Nodes, and the Dragon clients.

Prerequisites

- An SQL Server to install the NMC server database on (supported version) - See Installing SQL Server.
- One or more computers or virtual machines or the appropriate specification for your installation needs.
- An SSL certificate, purchased from a certified authority (CA), and the information necessary to install and bind the certificate.
- The NMC server installation: "NMC server Suite Installer - Full.exe".

- The Profile Optimizer Speech Node installation "PO.SpeechNode.exe".
- The Dragon Medical SDK installation.

Install the SSL certificate for a single-node configuration

1. Procure an SSL certificate from a trusted certificate authority (CA).
2. Install the certificate on the server, binding the certificate to the standard SSL port (443).

Install the SSL certificate for a multiple-node configuration

1. Procure an SSL certificate from a trusted certificate authority (CA).
2. Install the certificate on your load balancing switch.
3. Forward decrypted traffic to port 80 on the NMC servers.

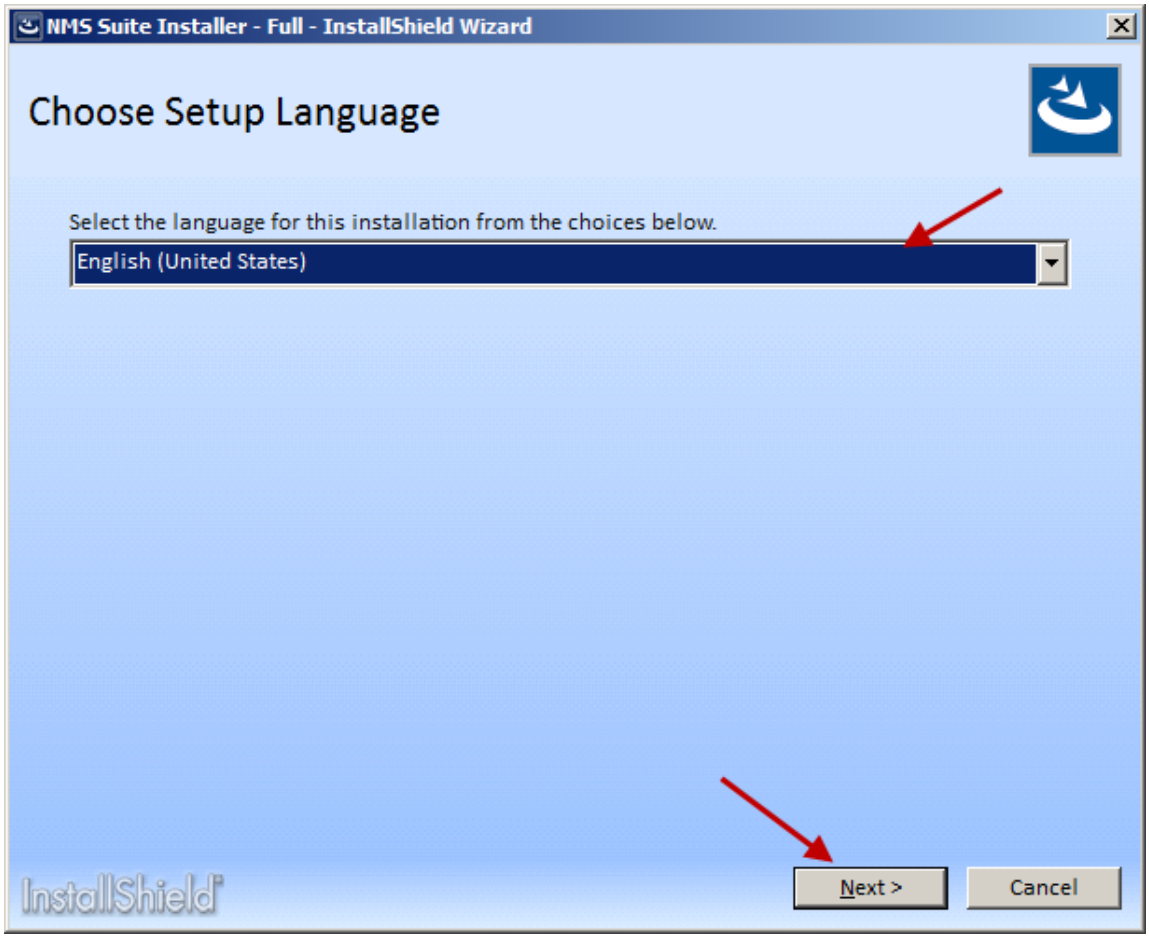
Install the NMC server software

1. If your system uses multiple NMC servers, configure the FileStore location.
2. (Single-node only) On the NMC server, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.

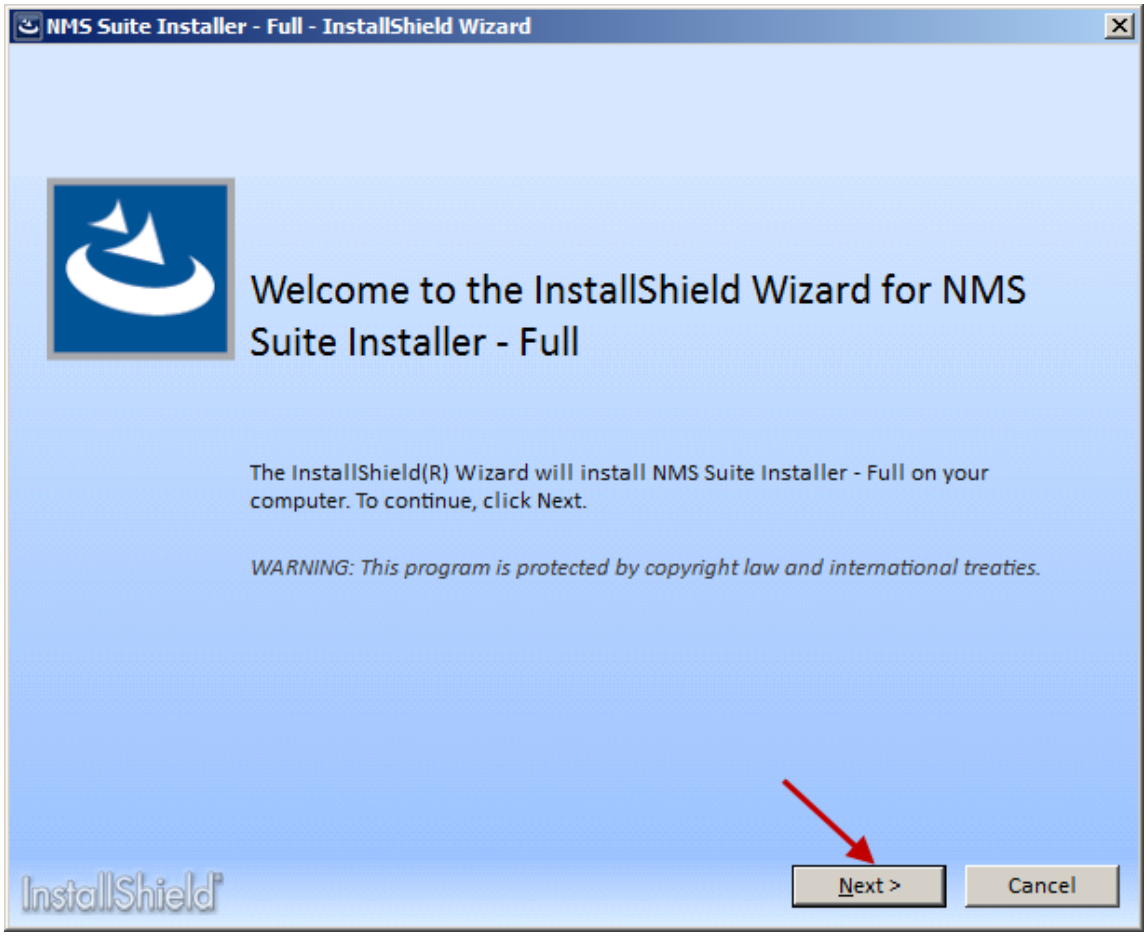
   or

   (Multiple-node only) On each NMC server node, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.

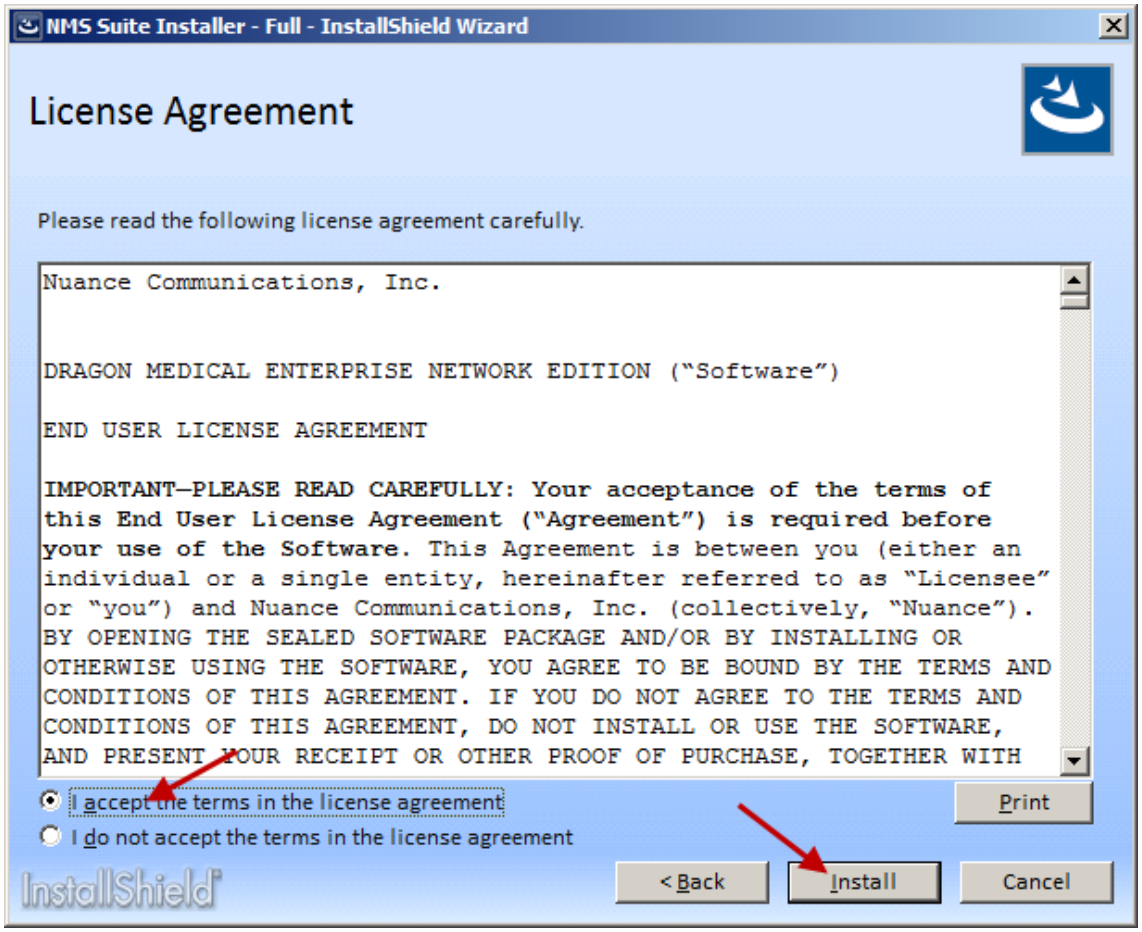
3. On the **Choose Setup Language** screen, select a language, and click **Next**.



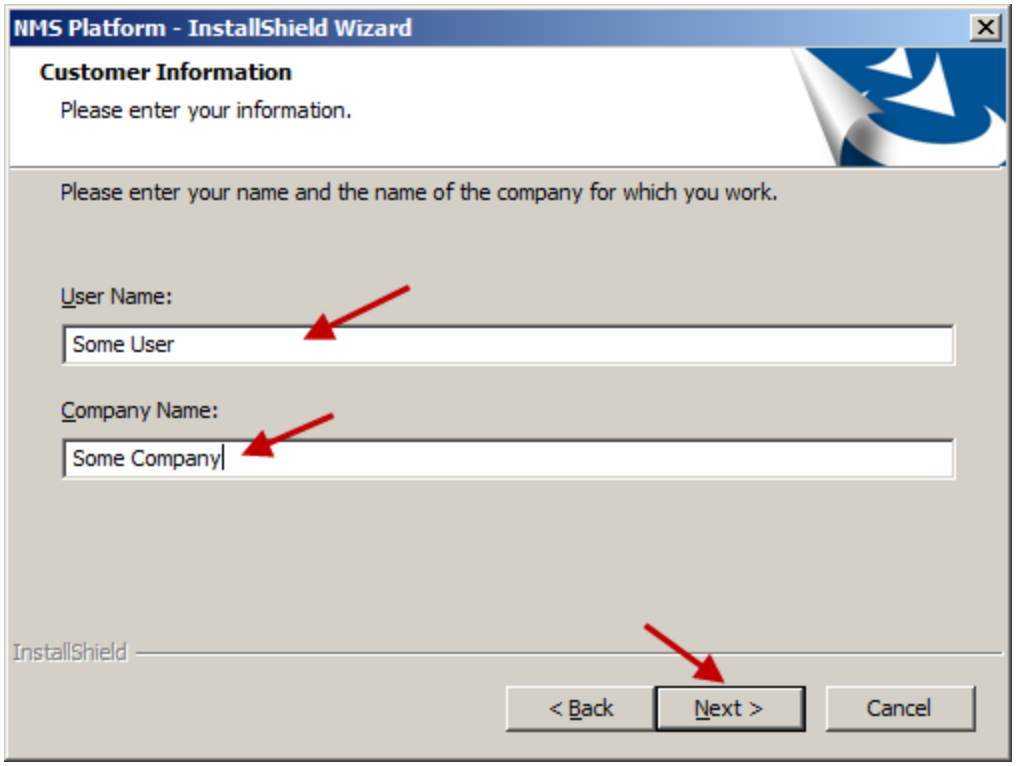
4. On the **Welcome** screen, click **Next**.



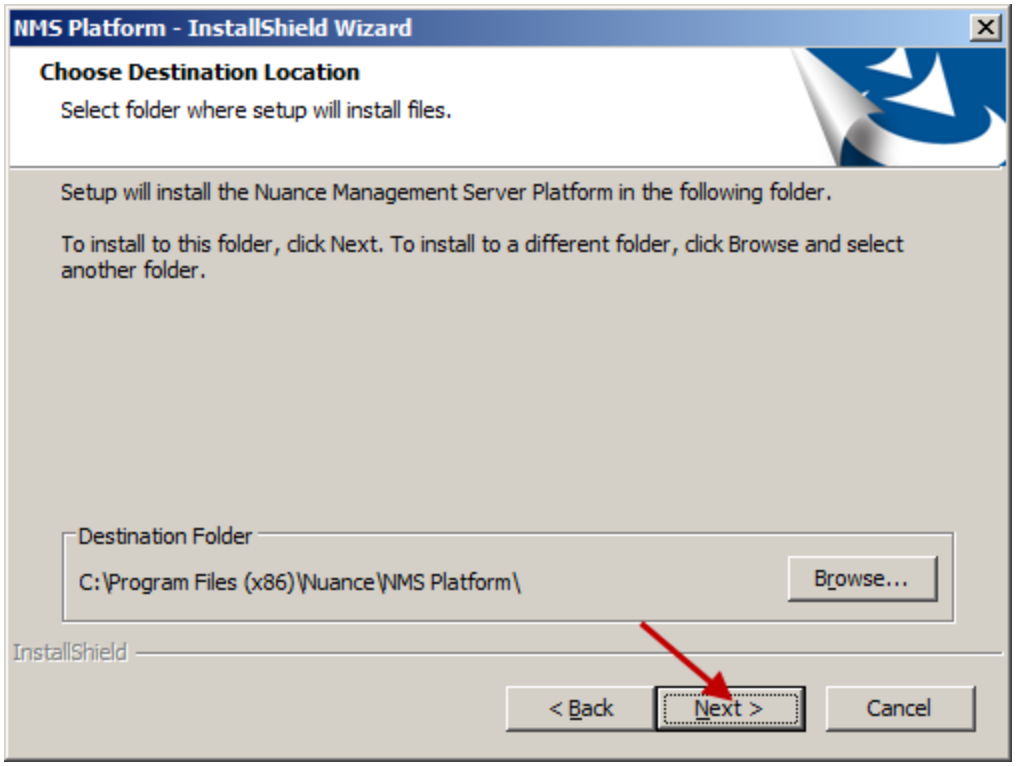
5. On the **License Agreement** screen, accept the agreement, and click **Install**.



6. On the **Customer Information** screen, enter a user name and company name, and click **Next**.

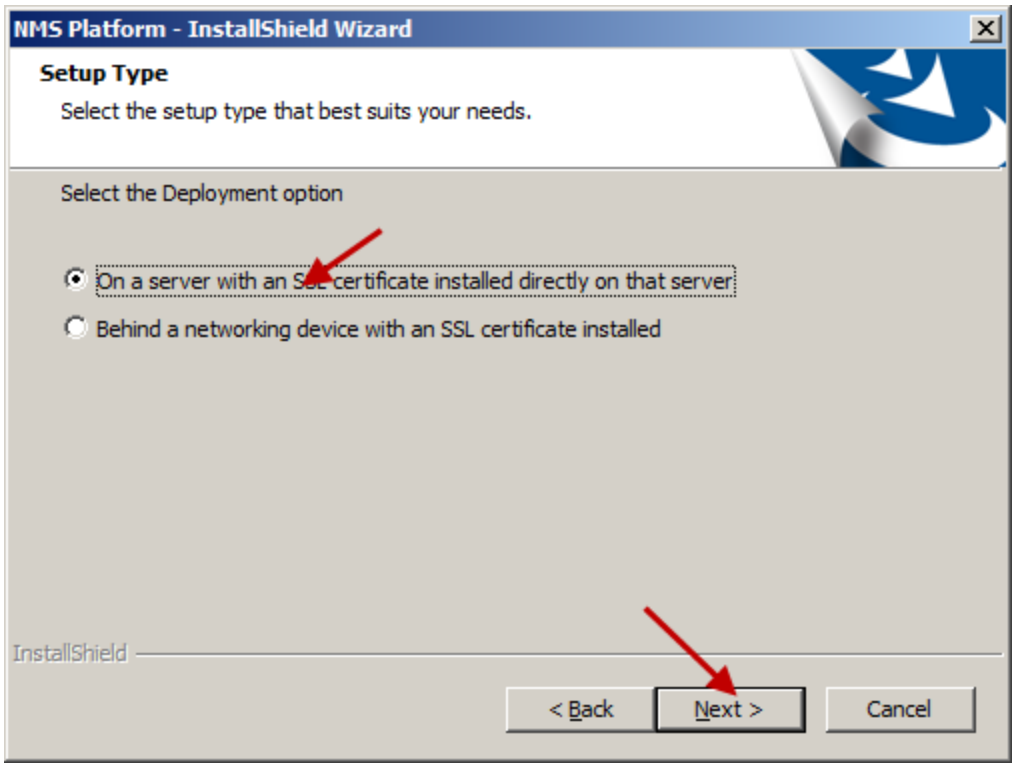


7. On the **Choose Destination Location** screen, accept the default or use the **Browse** button to select a location, and click **Next**.

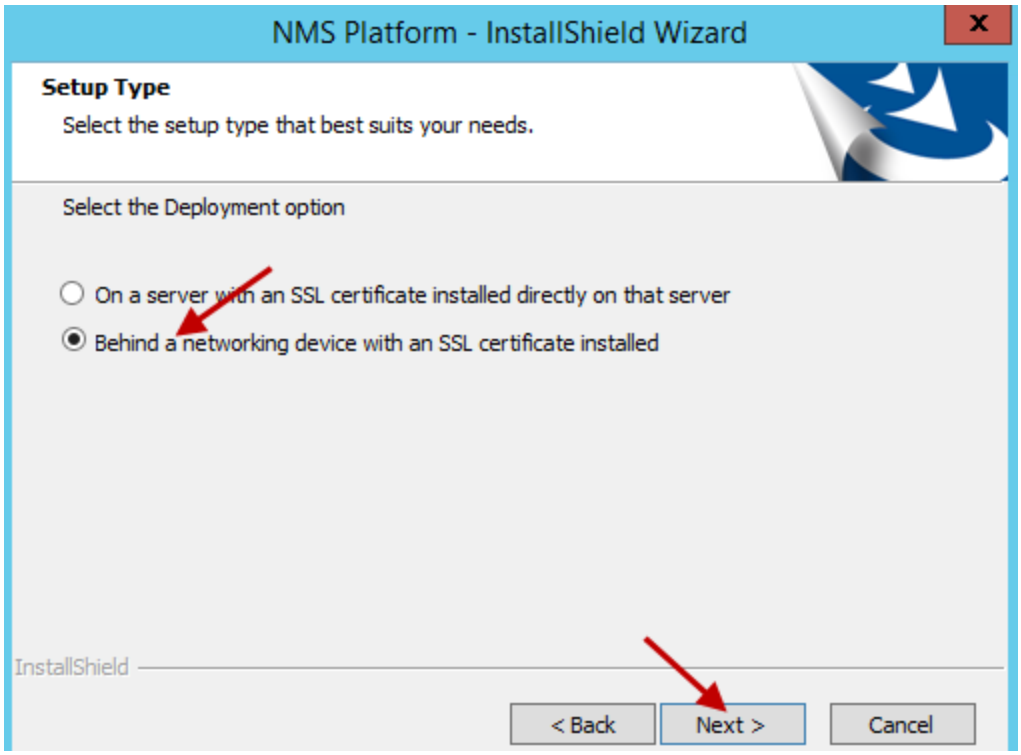


8. On the **Setup Type** screen, select an option:

- (Single-node only) **On a server with an SSL certificate installed directly on that server**, and click **Next**.



- (Multiple-node only) **Behind a networking device with an SSL certificate installed**, and click **Next**.



11. On the **Database Server** screen, enter the machine name or IP address of the physical server where you have installed the SQL Database Server software. The wizard automatically creates the database and its backup directory in default locations on that server.

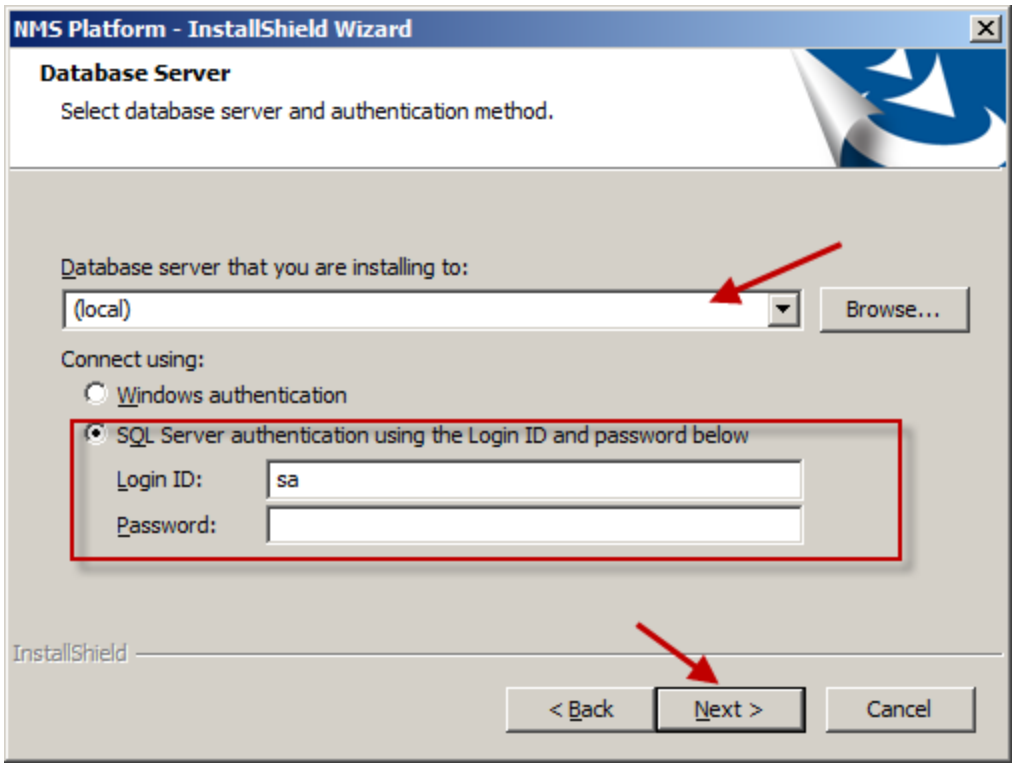
    Under **Connect using**, you see from two ways for the server to access the database—using a Windows login and password to authorize access, as indicated by **Windows authentication** or an SQL Server login and password, as indicated by **SQL Server authentication**.

    You should choose the same type of authentication for access to the database that you chose when you installed the SQL Server.

    Nuance recommends **Windows authentication**. If you choose this type of authentication, the **Login ID** and **Password** text boxes become unavailable, as they are not required.

    If you choose **SQL Server authentication using the Login ID and password below**, you then enter the database system administrator login name and password that you set up in SQL Server earlier into the **Login ID** and **Password** text boxes provided.

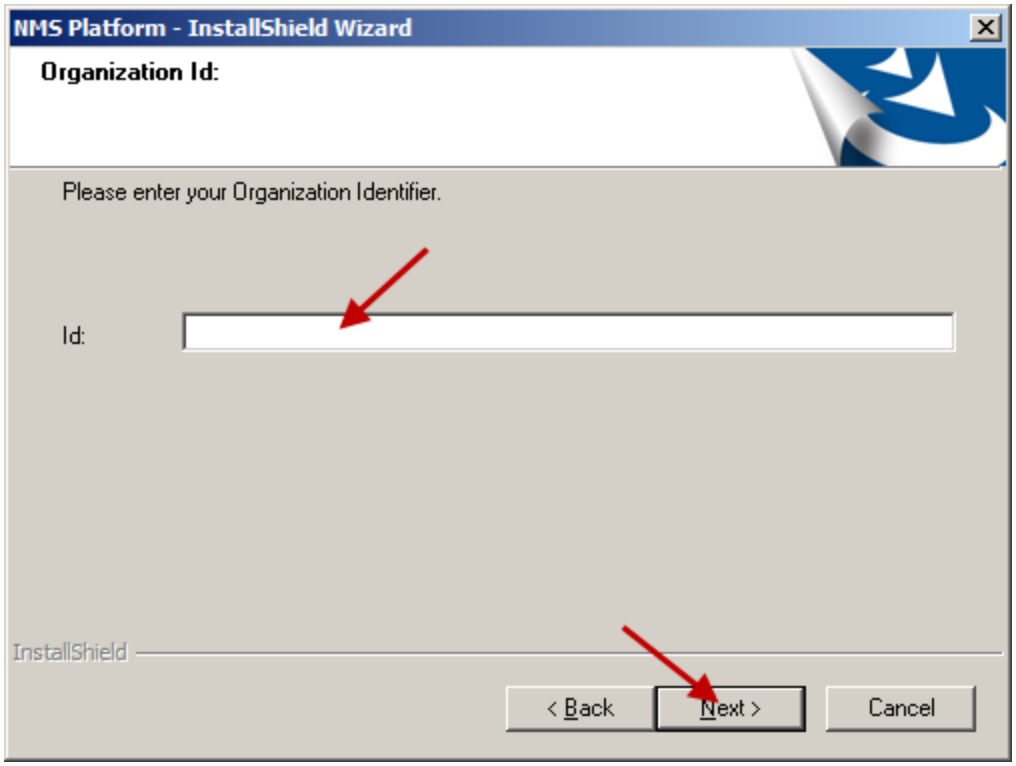
    Click **Next**.



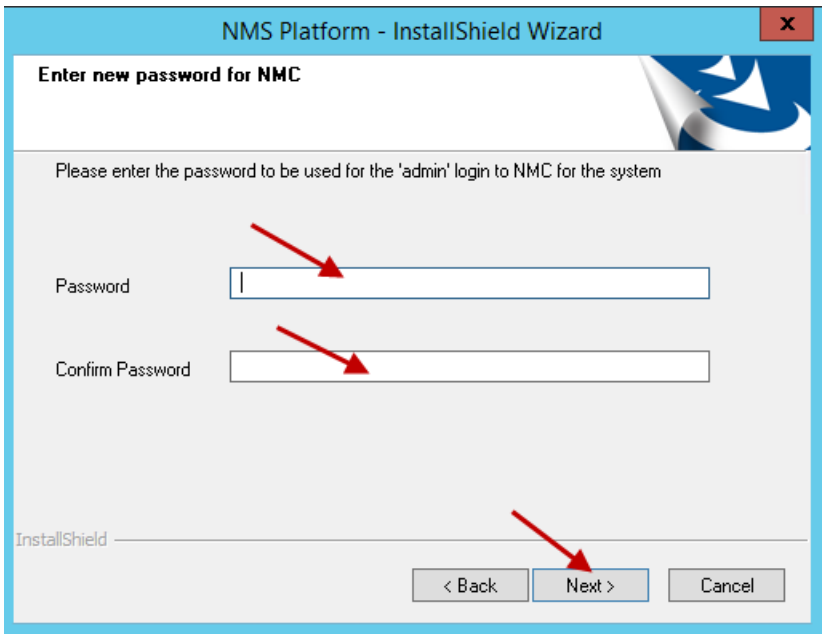
12. In the **Organization Id** screen, enter the unique ID that Nuance has assigned you. You should receive this ID on a slip of paper inserted with your *Dragon Medical Network Edition* software package. Carefully enter the ID into the **ID** text box here. You do not have to write it down or keep track of it on paper after you enter it here, as you will later be able to find the ID any time you need it through the *NMC console*.

    Click **Next**. For more information about organization IDs, see the Dragon Medical Network

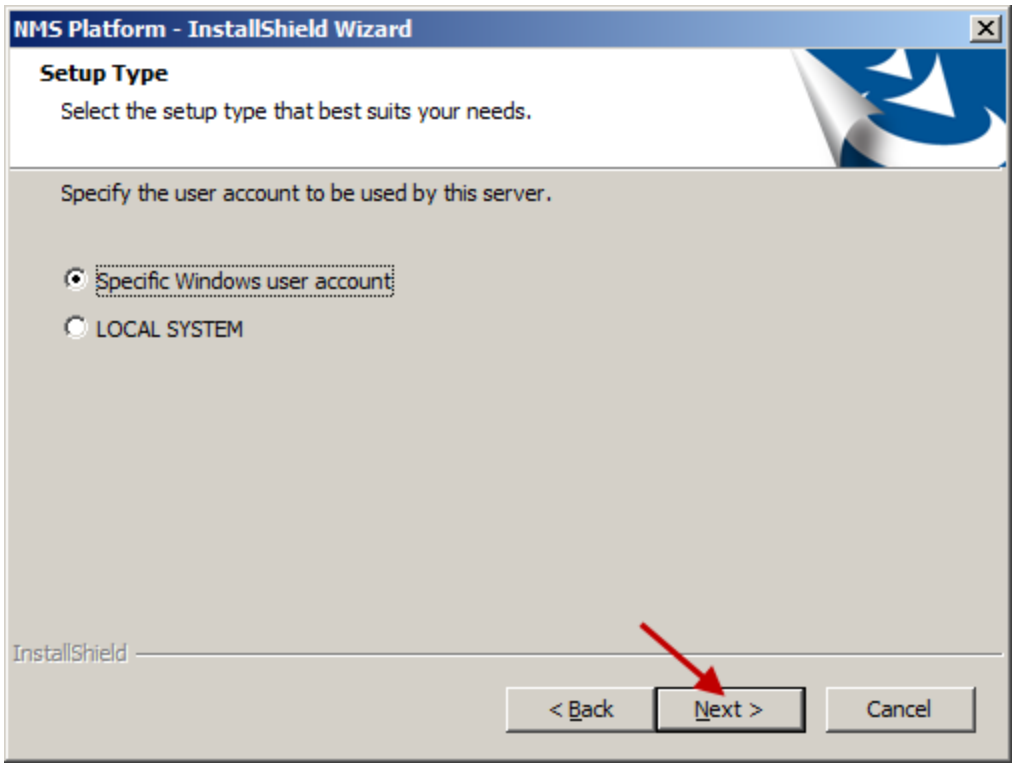
Edition Administrator guide.



13. On the **Enter new password for NMC** screen, enter the password for the default administrator account, and click **Next**. Note: When an administrator logs into the NMC console for the first time, the administrator uses the "admin" login ID and the password you enter in the **Enter new password for NMC** screen.

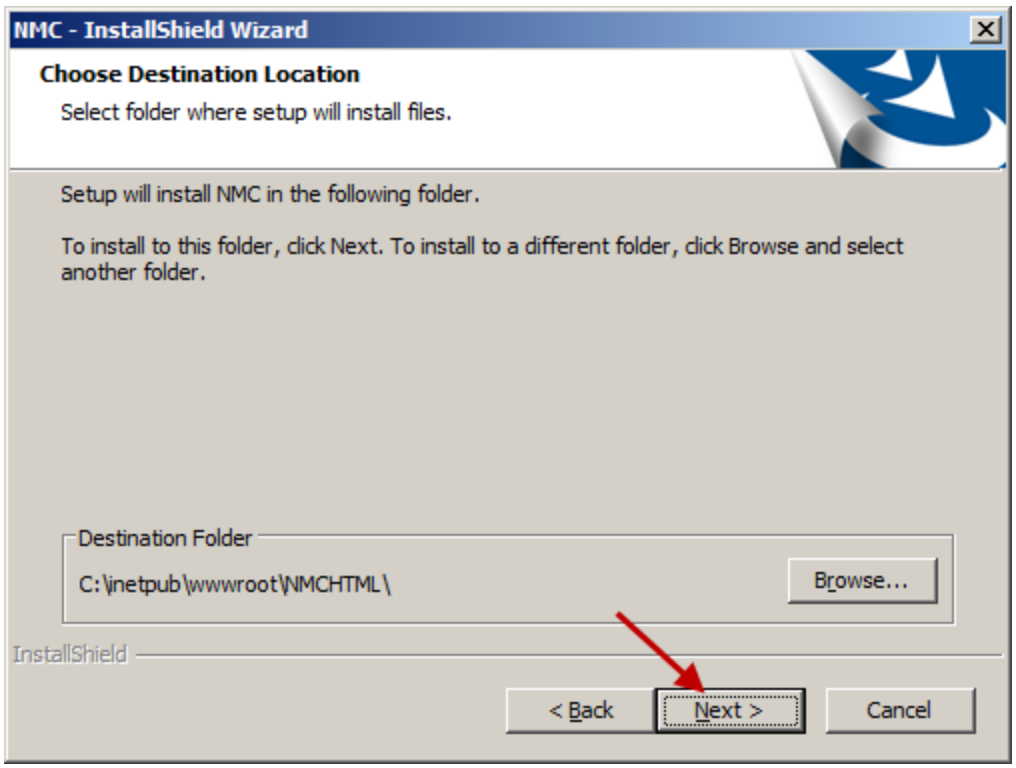


14. On the **Setup Type** screen, select the account that the NMC server windows service runs under, and click **Next**. The install wizard installs several components.

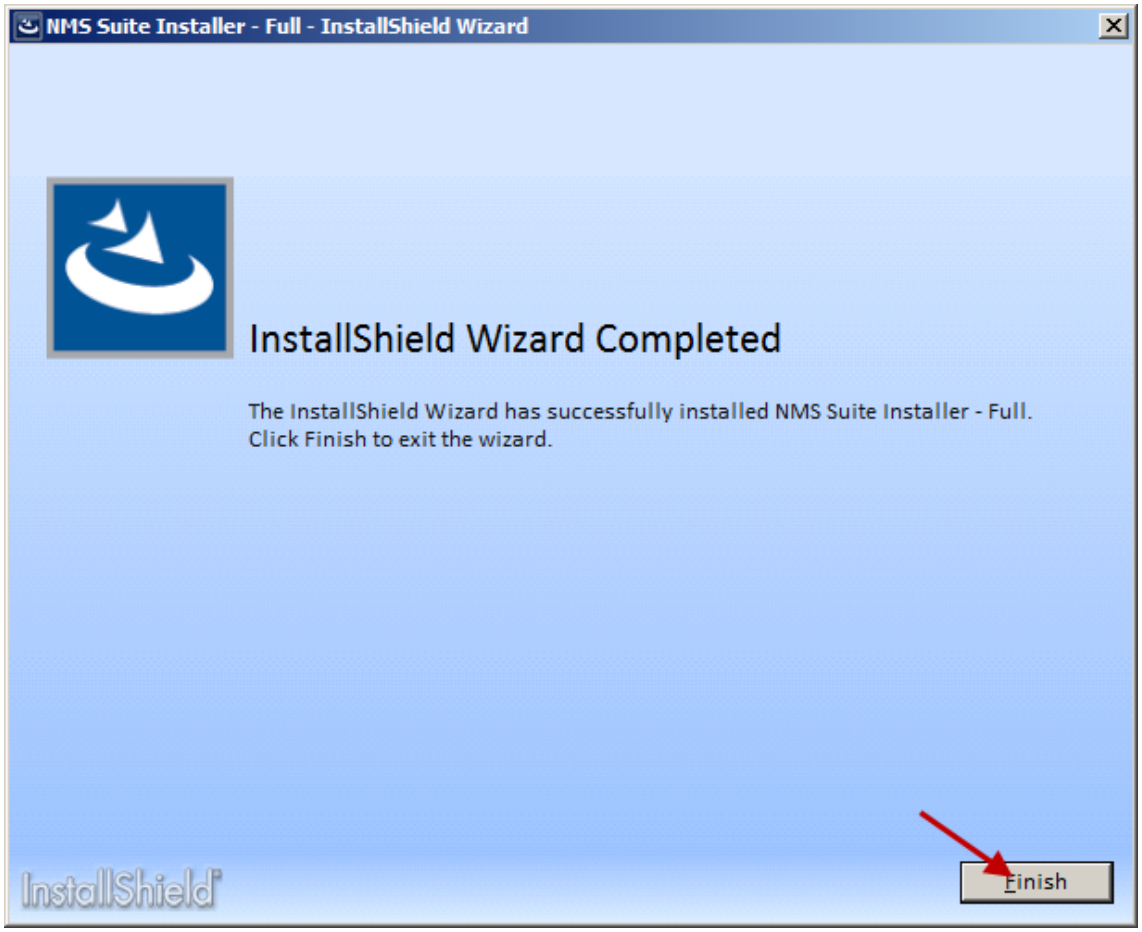


15. On the **NMC - InstallShield Wizard - Choose Destination Location** screen, select the location where the install wizard installs the NMC console (default recommended), and click

Next.


NMC - InstallShield Wizard
Choose Destination Location
Select folder where setup will install files.
Setup will install NMC in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\inetpub\wwwroot\NMCHTML\
Browse...
InstallShield
< Back
Next >
Cancel

16. On the **InstallShield Wizard Completed** screen, click **Finish**.



If you installed the *NMC server* and *NMC console* with the Windows Server 2008, 2012, 2012 R2, or Windows Server 2016 firewall turned on during the installation, you must now open Port 443 so that the *NMC console* can communicate with the *NMC server*.

17. In a supported browser, go to https://servername/nmchtml.
18. Log into the NMC console using the "administrator" ID and the password you entered in the setup process.
19. Import your license key. For more information about license keys, see the Dragon Medical Network Edition Administrator guide.

Install one or more Profile Optimizer Speech Nodes

1. On the computers you select to host speech nodes (and that do not host the NMC server):
   ii. Install the Dragon Medical Client SDK.
   iii. Run the PO SpeechNode installation. See Installing prerequisite software for speech nodes and Installing the speech nodes.

2. After you install the speech nodes, use the NMC console to configure your Profile Optimizer Speech Node Collections. For more information about managing speech node collections, see the Dragon Medical Network Edition Administrator guide.

Upgrade a single-node or multiple-node configuration to NMC server 5.x

This topic is for customers that are running an NMC server 4.x installation, are running 2.4 or earlier Dragon Medical Network Edition clients, and will be installing or upgrading to the Dragon Medical Network Edition 2.7 client.

Notes:

- All installations of NMC server 5.0 and later require an SSL certificate from a certified authority (CA).
- Supported versions of SQL Server:
  - SQL 2008 R2 - See Installing SQL Server.
  - SQL 2012
  - SQL 2014
  - SQL 2016
- Supported versions of Windows:
  - Windows 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
- .NET Framework 4.5.2 is required on both the NMC server and PO Speech Nodes.

Prerequisites

- A SQL Server to install the NMC server database on (supported version) - See Installing SQL Server.
- One or more computers or virtual machines or the appropriate specification for your installation needs.
- An SSL certificate, purchased from a certified authority (CA), and the information necessary to install and bind the certificate. If you previously installed your 4.x system with SSL, you can use the same certificate for NMC server 5 and later.

- The NMC server installation: "NMC server Suite Installer - Full.exe".
- The Profile Optimizer Speech Node installation "PO.SpeechNode.exe".
- The Profile Optimizer Migration Tool installation "PO.ServerMigrationTool.exe".
- The Dragon Medical SDK installation.

Install the SSL certificate for a single-node configuration

1. Bind the SSL certificate to the standard SSL port (443). If you have installed your 4.x system with SSL previously, you can use the same certificate for NMC server 5 and later.

Install the SSL certificate for a multiple-node configuration

1. Install (or configure) the certificate on your load balancing switch.
2. If you have installed your 4.x system with SSL previously, the same certificate can be used for NMC server 5 and later.
3. Forward decrypted traffic to port 443 on the NMC servers.

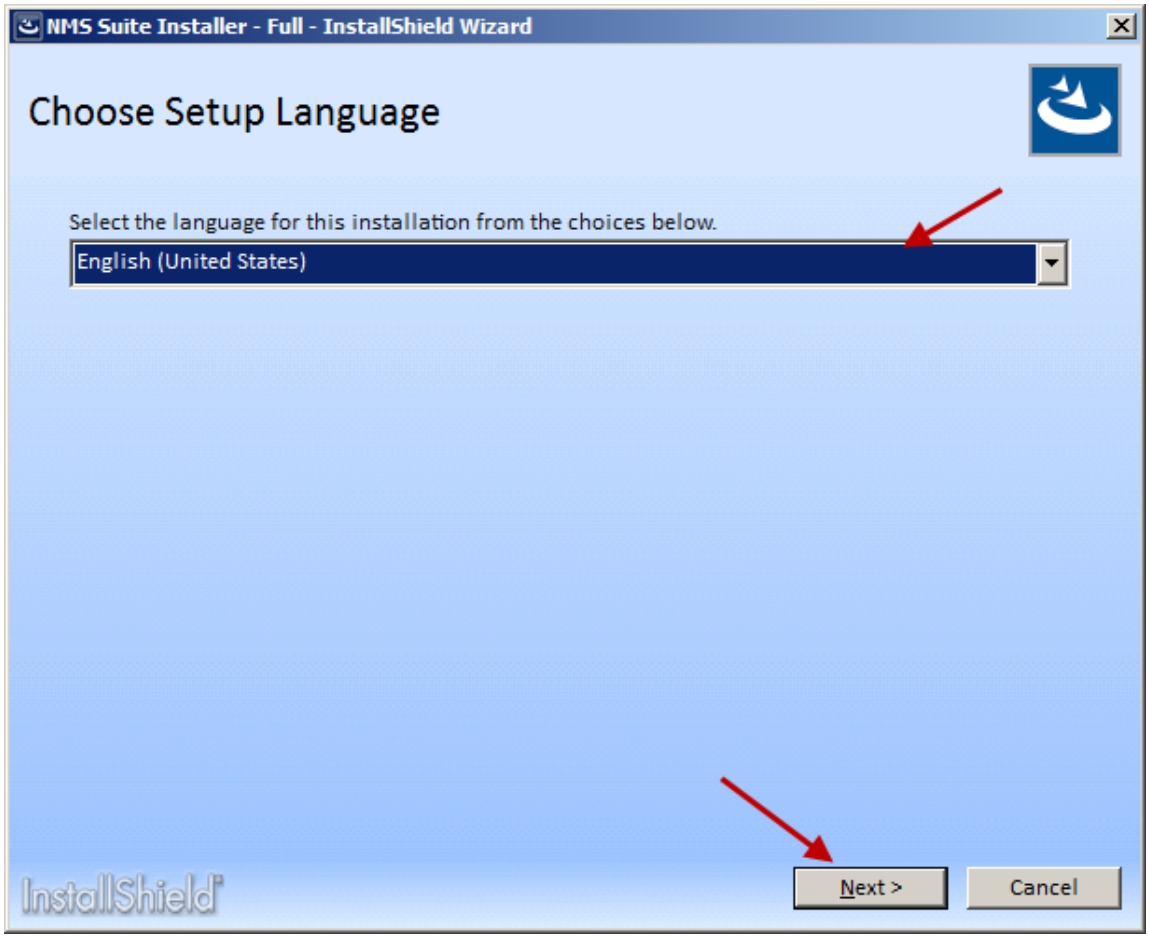
Install the NMC server software

1. (Single-node only) On the NMC server, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.

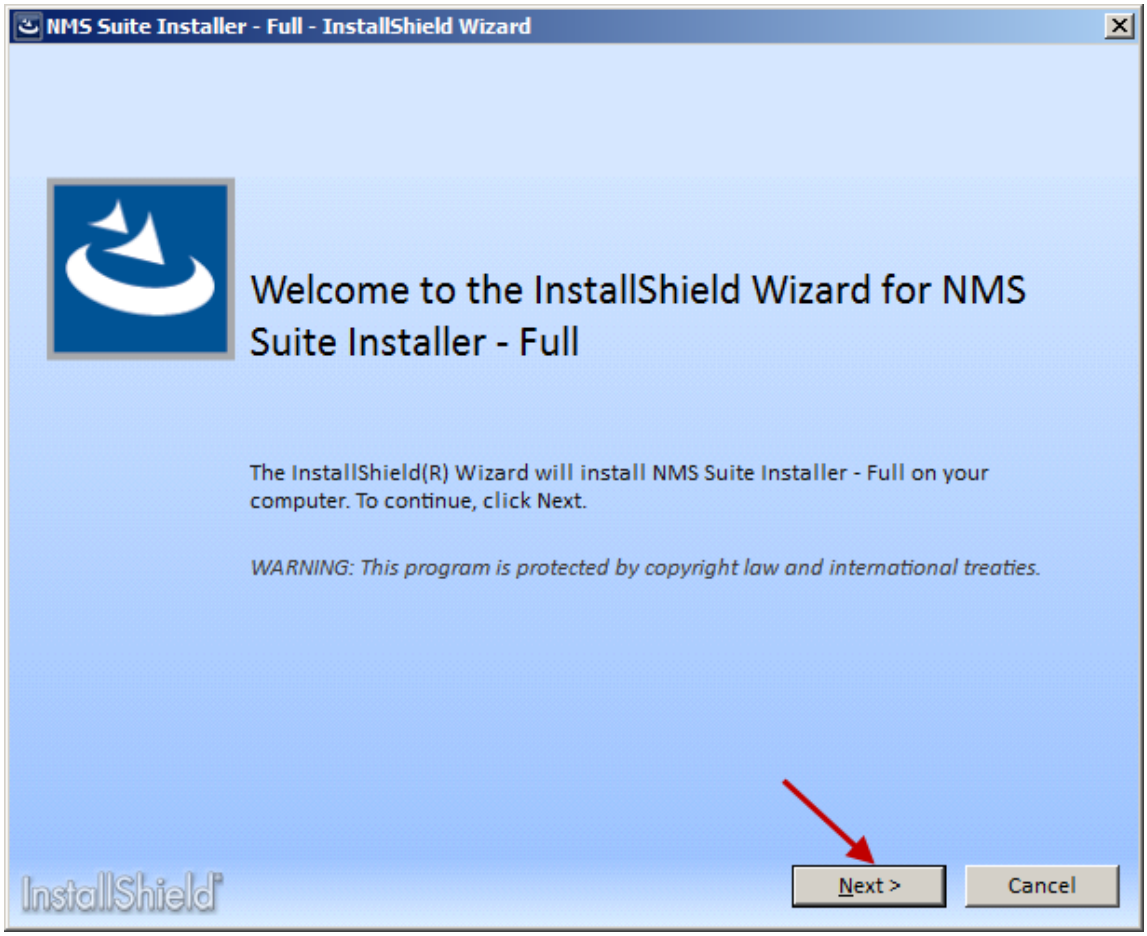
   or

   (Mutli-node only) On each NMC server node, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.

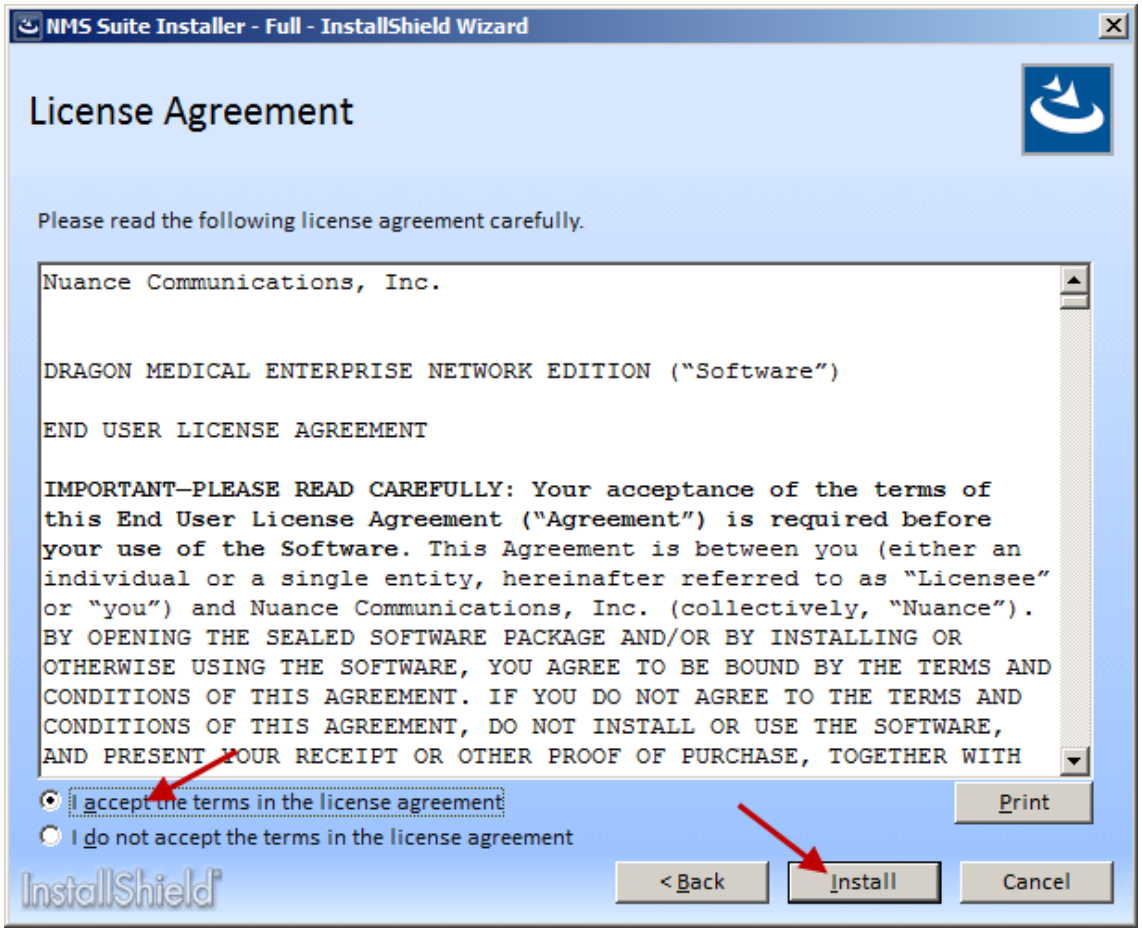
2. On the **Choose Setup Language** screen, select a language, and click **Next**.



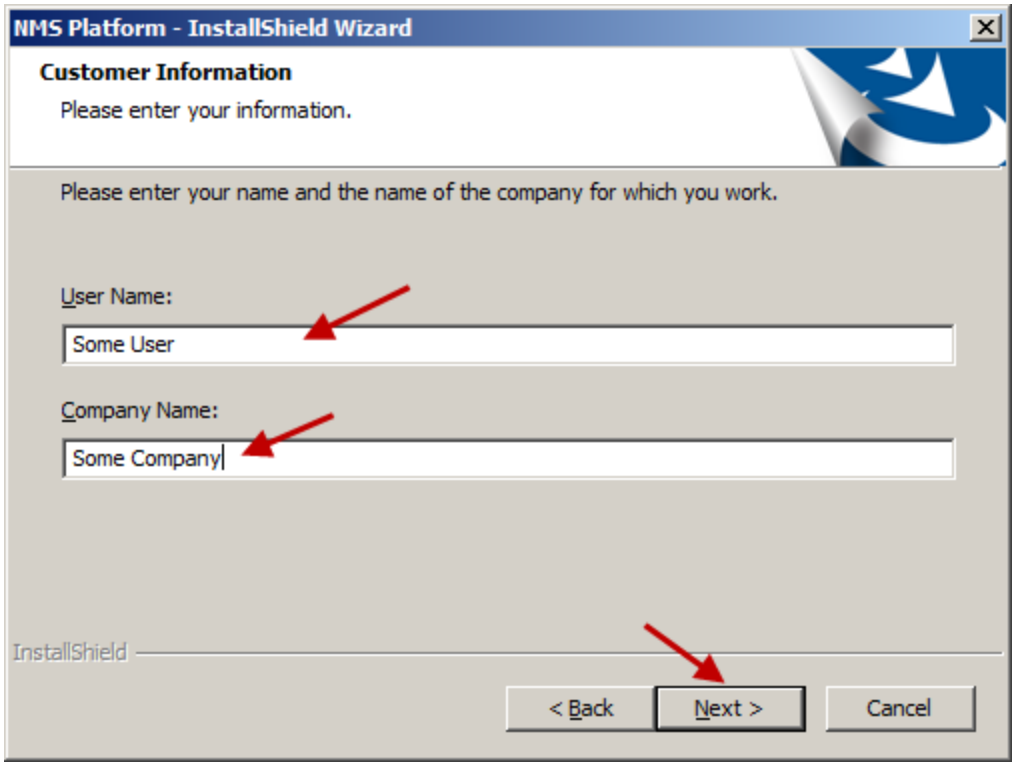
3. On the **Welcome** screen, click **Next**.



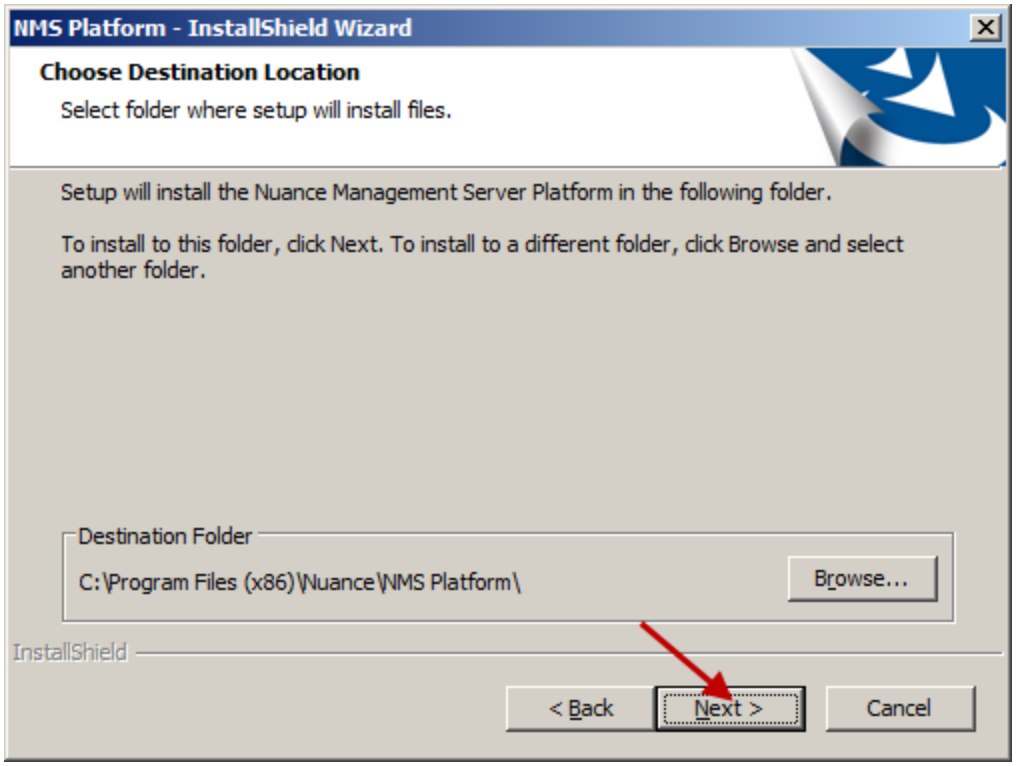
4. On the **License Agreement** screen, accept the agreement, and click **Install**.



5. On the **Customer Information** screen, enter a user name and company name, and click **Next**.

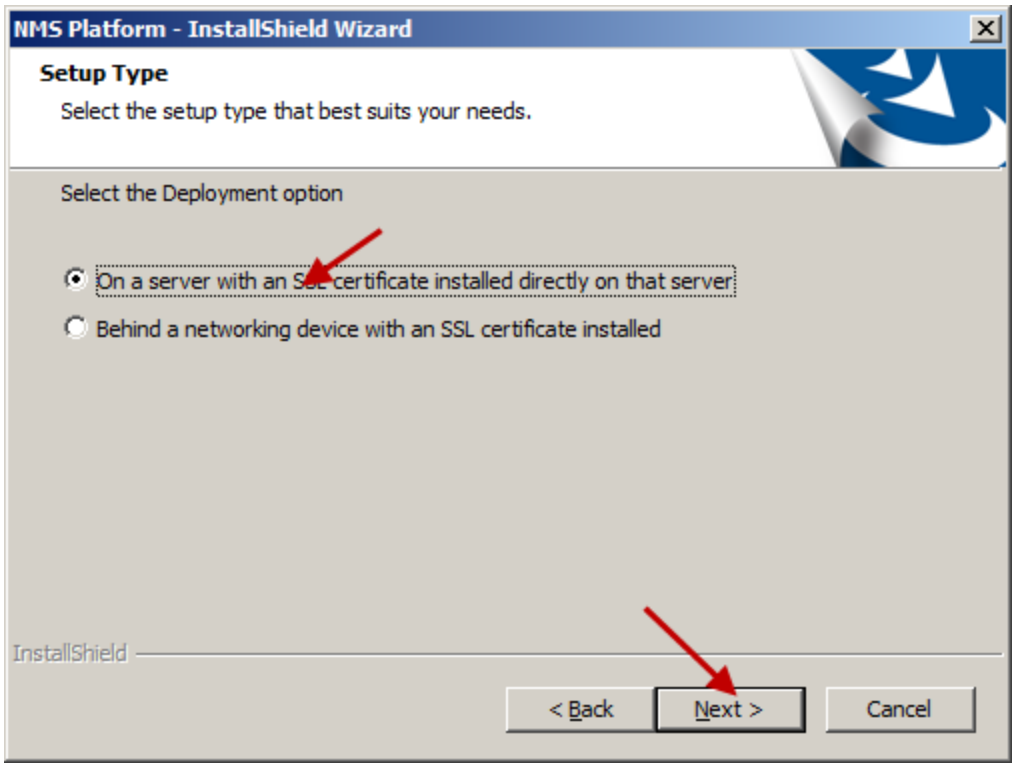


6. On the **Choose Destination Location** screen, accept the default or use the **Browse** button to select a location, and click **Next**.

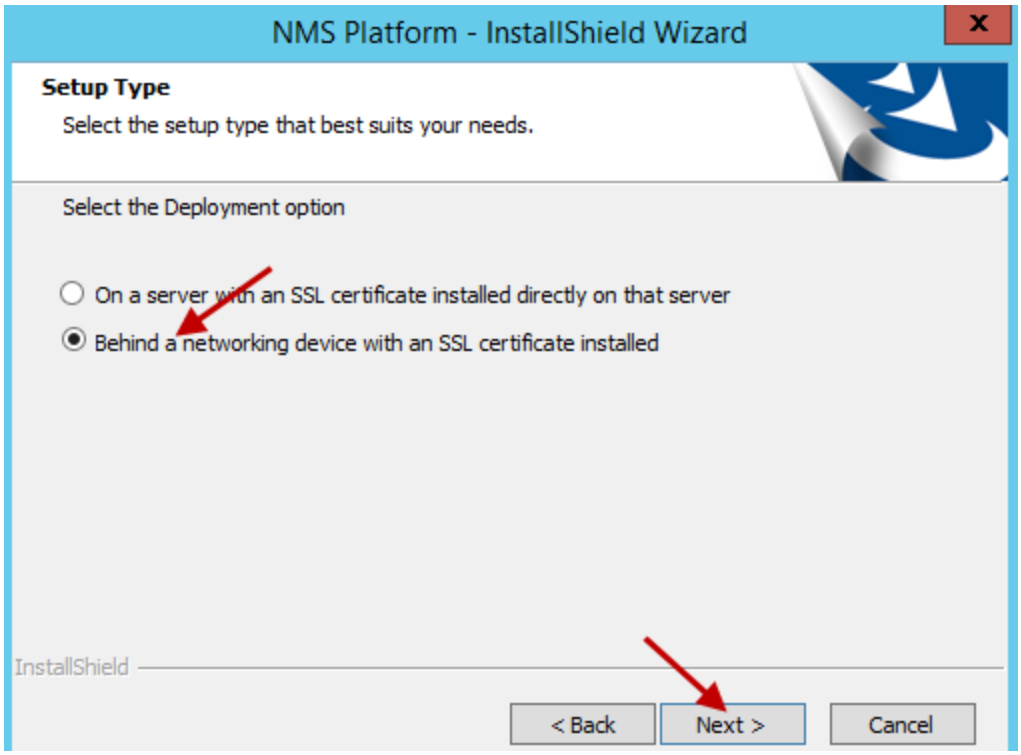


7. On the **Setup Type** screen, select an option:

- (Single-node only) **On a server with an SSL certificate installed directly on that server**, and click **Next**.



- (Mutli-node only) **Behind a networking device with an SSL certificate installed**, and click **Next**.



8. On the **Database Server** screen, enter the machine name or IP address of the physical server where you have installed the SQL Database Server software. The wizard automatically creates the database and its backup directory in default locations on that server.

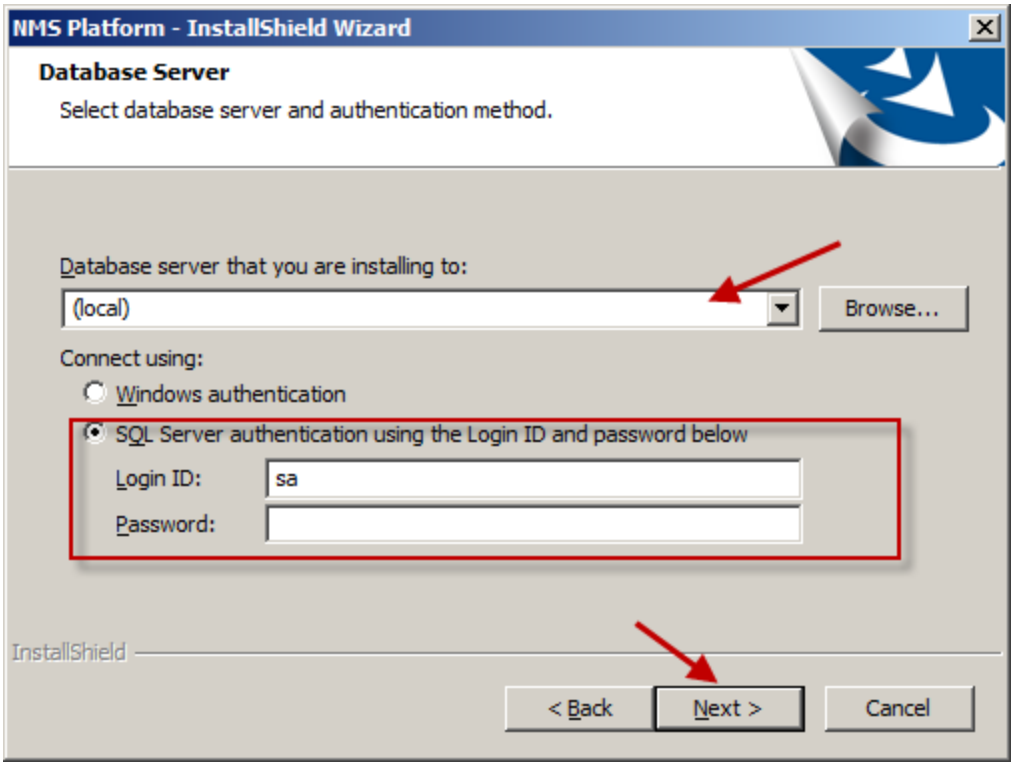
   Under **Connect using**, you see from two ways for the server to access the database—using a Windows login and password to authorize access, as indicated by **Windows authentication** or an SQL Server login and password, as indicated by **SQL Server authentication**.

   You should choose the same type of authentication for access to the database that you chose when you installed the SQL Server.

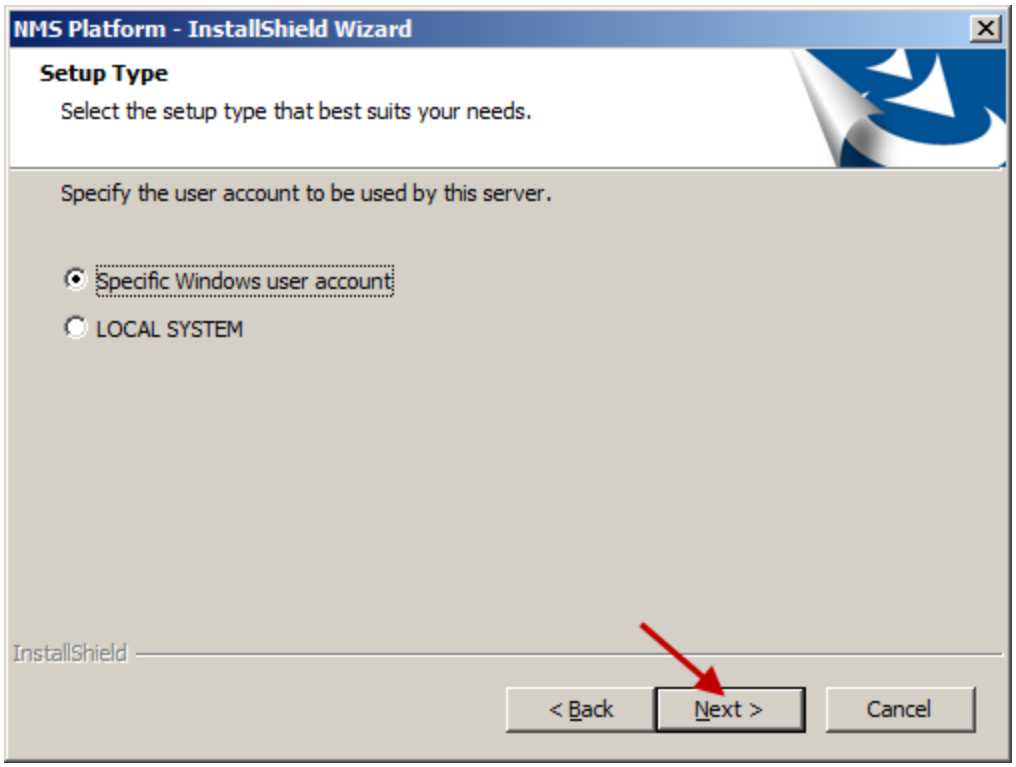
   Nuance recommends **Windows authentication**. If you choose this type of authentication, the **Login ID** and **Password** text boxes become unavailable, as they are not required.

   If you choose **SQL Server authentication using the Login ID and password below**, you then enter the database system administrator login name and password that you set up in SQL Server earlier into the **Login ID** and **Password** text boxes provided.

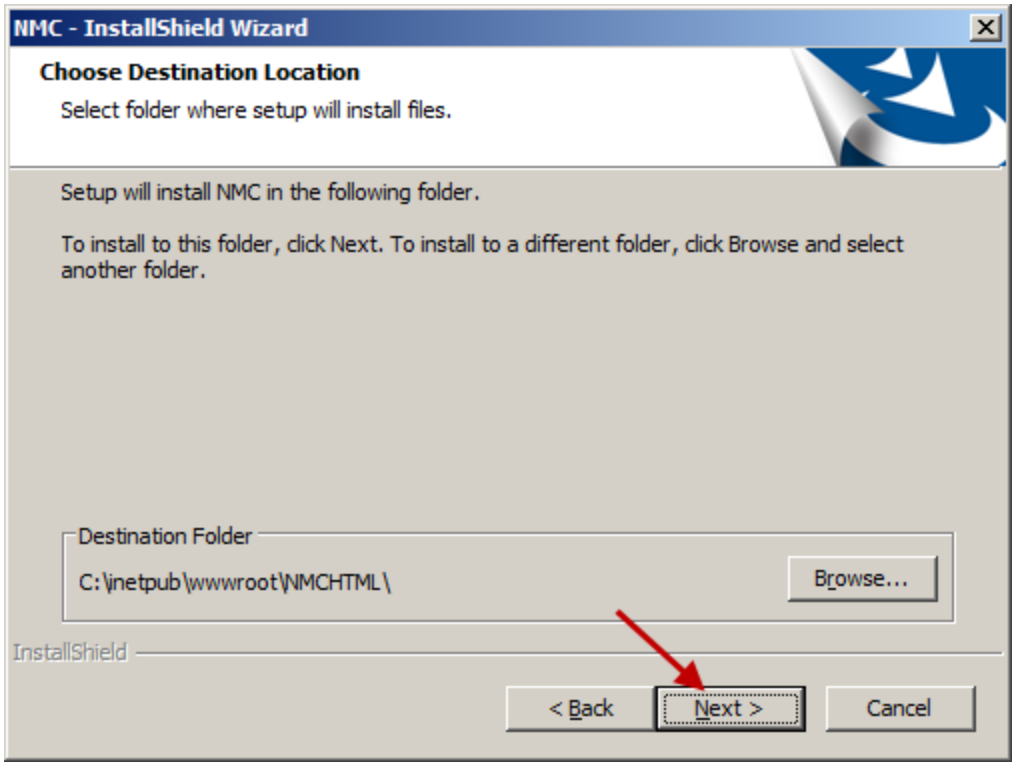
   Click **Next**.



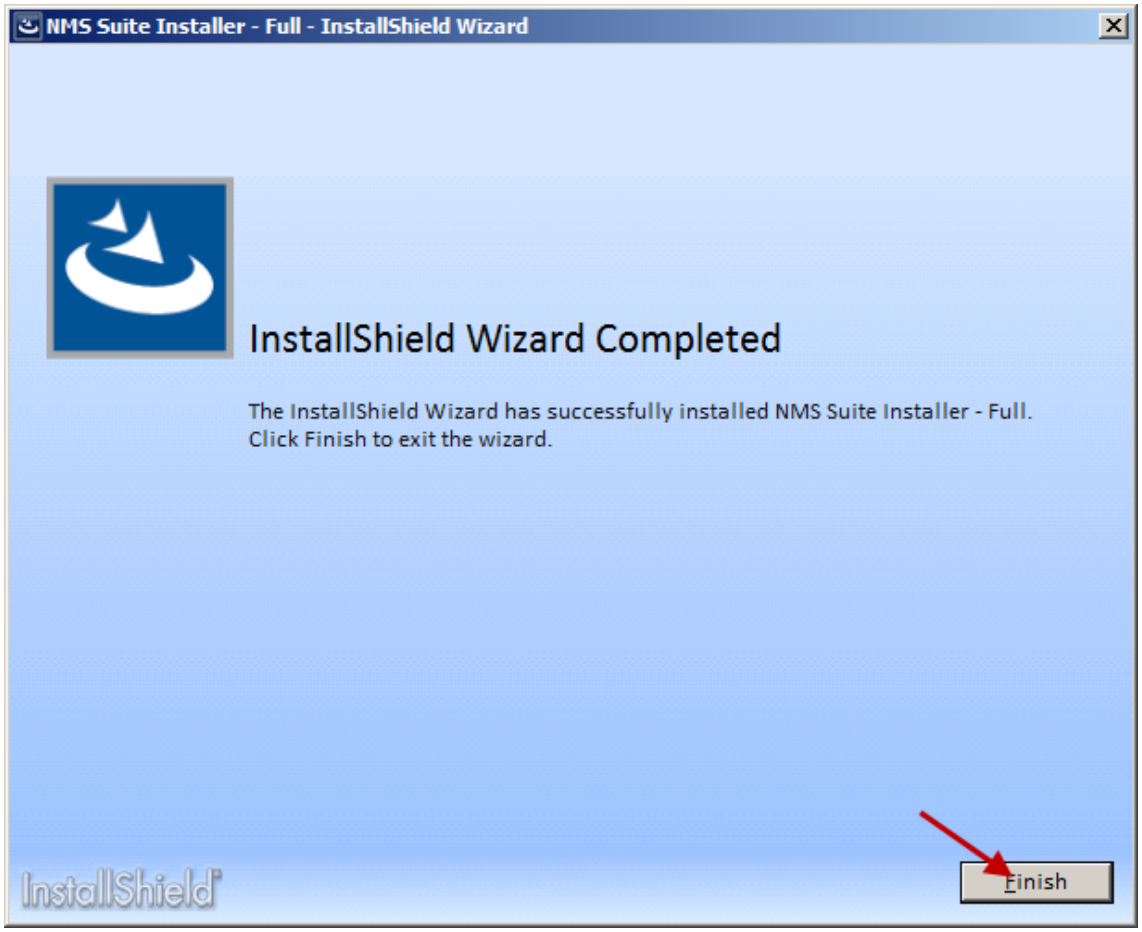
9. On the **Setup Type** screen, select the account that the NMC server windows service runs under, and click **Next**. The install wizard installs several components.



10. On the **NMC - InstallShield Wizard - Choose Destination Location** screen, select the location where the install wizard installs the NMC console (default recommended), and click **Next**.



11. On the **InstallShield Wizard Completed** screen, click **Finish**.



If you installed the *NMC server* and *NMC console* with the Windows Server 2008, 2012, 2012 R2, or Windows Server 2016 firewall turned on during the installation, you must now open Port 443 so that the *NMC console* can communicate with the *NMC server*.

12. Log into the NMC console with your existing administrator account.
13. On your existing Profile Optimizer Server:
    i. On all Profile Optimizer speech nodes, stop the Profile Optimizer Speech Node service.
    ii. On the Profile Optimizer server, stop the Profile Optimizer Speech Node service.
    iii. On the Profile Optimizer server, run the Profile Optimizer Server Migration Tool.
14. On each Profile Optimizer speech node, run the Profile Optimizer Speech Node installation. See Installing prerequisite software for speech nodes and Installing the speech nodes.
    The NMC server now only communicates with the new Profile Optimizer speech node. The Profile Optimizer server is no longer required.

Run the Profile Optimizer Server Migration Tool

Use the PO Server Migration Tool to migrate data from the Profile Optimizer server database to the NMC server 2.7 database.

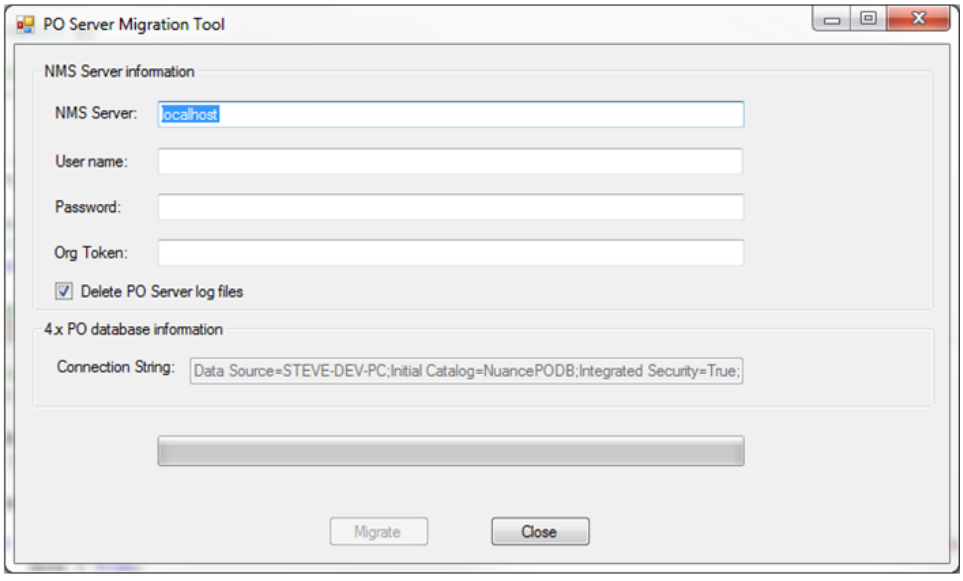
Requirements

- The Profile Optimizer Server Migration Tool runs on the Profile Optimizer server you are migrating from.
- The person running the tool is a user that is an administrator and a member of the organization with the data to be migrated. The person that runs the tool enters their user credentials in the **PO Server Migration Tool** screen.
- The version of the NMC server database is 5.1 or greater.

Steps for migrating Profile Optimizer server data

1. On the 4.x Profile Optimizer server, run the Profile Optimizer Server Migration Tool (PO_Server-MigrationTool.exe).

2. On the **PO Server Migration Tool** screen, enter information in the following fields:

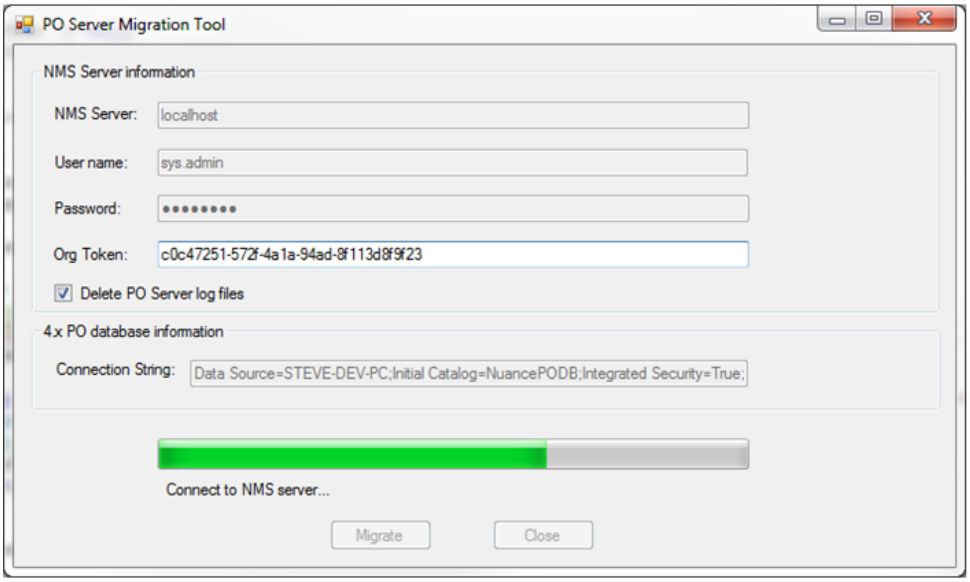


- **NMC server**: The name of the NMC server server.
- **User name**: The user login of the person running the tool.

- **Password**: The user password of the person running the tool.
- **Org Token**: Organization Token for the organization. For more details about organization tokens, see 'Creating Organization Tokens' in the Administrator guide.

3. To remove all log files from the 4.x Profile Optimizer server, select **Delete PO Server log files**.

4. Click **Migrate**. On the **PO Server Migration Tool** screen, a status bar displays the progress of the Tool, and when the migration process is complete.



36Using and configuring the FileStore location for multiple NMC servers

Note: You only need to modify the FileStore location if your system uses multiple NMC servers.

You can ignore this topic if your system uses only one NMC server.

The NMC server FileStore is a common location for files that need to be shared between multiple NMC servers. If your system uses only one NMC server, you can use the default FileStore location (the local system). If your system uses multiple NMC servers, you must create a common location for the servers to use as a FileShare.

You must configure each NMC server to use the common location. It is recommended that you do not use one of the NMC servers as the common location. If the server were to fail, the other servers will not be able to access the FileShare location.

In DM Network Edition, the NMC server uses the FileStore to store temporary files that upload and download to the NMC console. For example, log files from various client applications.

Space requirements for the FileStore depend on your system configuration.

Change the FileStorePath for the NMC server

1. Determine where you want to put the FileStorePath.
2. Shutdown the NMC server Service. You can't move an existing FileStorePath while the service is running.
3. Create the FileStorePatch folder that you chose in step 1.
4. Copy the current ClientLogs, Completed, Download, and Upload folders (The default location is %ALLUSERSPROFILE%\xnms\FileStore) to the folder you created in step 3.
   The value of the %ALLUSERSPROFILE% environmental variable depends on the operating system.
   The following is a list of default locations for the environmental variable %ALLUSERSPROFILE% based on Operating Systems:
   - Windows 7, 8.x, and 10: C:\ProgramData
   - Windows 2008: C:\ProgramData

5. Delete the current FileStore folder (%ALLUSERSPROFILE%\xnms\FileStore).
6. Modify the FileStorePath key value for NMC server version 5.x and 4.5 to use the folder location you set earlier.

Modify the FileStorePath key value for NMC server version 5.x and 4.5

Step 1: Modify the FileStorePath key value for NMC server 5.x

1. In the NMC Platform installation folder, find and open the Nuance.NMS.Server.exe.config file.
2. Find the key in the "appSettings" section called FileStorePath that controls the location of the NMC server FileStore.
3. Look for the following line:

   ```
   <add key="FileStorePath" value="" />
   ```

4. Assign a location to the right side of the value paramater.

   A empty string ("") means to use the default. The default location is

   %ALLUSERSPROFILE%\xnms\FileStore

   where %ALLUSERSPROFILE% is an environmental variable.

   Windows 2008 Example:

   - If you set the value parameter to "", the NMC server uses `c:\ProgramData\xnms\FileStore` as the FileStore location.
   - If you set the value parameter to "D:\xnms\FileStore", the NMC server uses `D:\xnms\FileStore` as the FileStore location.

5. Save the config file.

Step 2: Modify the FileStorePath key value for NMC server 4.x

When you install NMC server 5.X and above, you are also installing NMC server 4.5.

To change the FileStore path for NMC server 5.x, you must also change the FileStore path for NMC server 4.5.

1. In the NMS server folder, find and open the Nuance.NAS.Server.exe.config file.
2. Perform the rest of the steps in Modify the FileStorePath key value for NMC server 5.x.
3. Restart the NMC server Service.

Chapter 4: Installing Profile Optimizer speech node components

To install the *Profile Optimizer* components of the Dragon Medical Network Edition network, you carry out the procedures in these sections:

Prerequisites for Installing Profile Optimizer speech nodes

Installing software to support Profile Optimizer Speech Nodes installation

You install two extra packages on machines where you are planning to install *Profile Optimizer Speech Nodes*:

Windows Installer 5.0 If you are installing a *Speech Node* on a machine with any supported operating system other than Windows Server 2008, the installer requires that the machine have Windows Installer 5.0 or greater on it. Windows Server 2008, Windows Server 2012, and Windows Server 2016 automatically install a later version of the Windows Installer. For information on operating systems that support *Speech Nodes* refer to *Dragon Medical Enterprise Planning and Deployment Guide*.

Dragon Medical SDK Client You must install the latest version of the Dragon Medical SDK Client software on workstations where you plan to install *Speech Nodes*. This software is included on the *NMC server Software and Documentation* DVD.

Installing prerequisite software for speech nodes

Required software for Speech Nodes

- See *System Requirements for Dragon Medical Network Edition* on page 6 for a list of required software.
    - Windows Server 2016
    - Windows Server 2012 R2
    - Windows Server 2012

More information on installing these prerequisites is in the corresponding section below.

Installing Windows Installer for Speech Nodes not on Windows Server

Every machine where you use install a *Profile Optimizer Speech Node*, Windows Installer must be on the machine.

Caution:

If you are installing on a Windows Server 2008, 2012 R2, or 2016 machine, you installed the Windows Installer when you installed the operating system, so you can skip this section.

To obtain:

Windows Server 2008: Get the Windows installer 4.5 download here: https://support.microsoft.com/en-us/kb/942288.

Windows Server 2012: Windows Installer 5.0 is part of Windows Server 2012. There is no redistributable for Windows Installer 5.0.

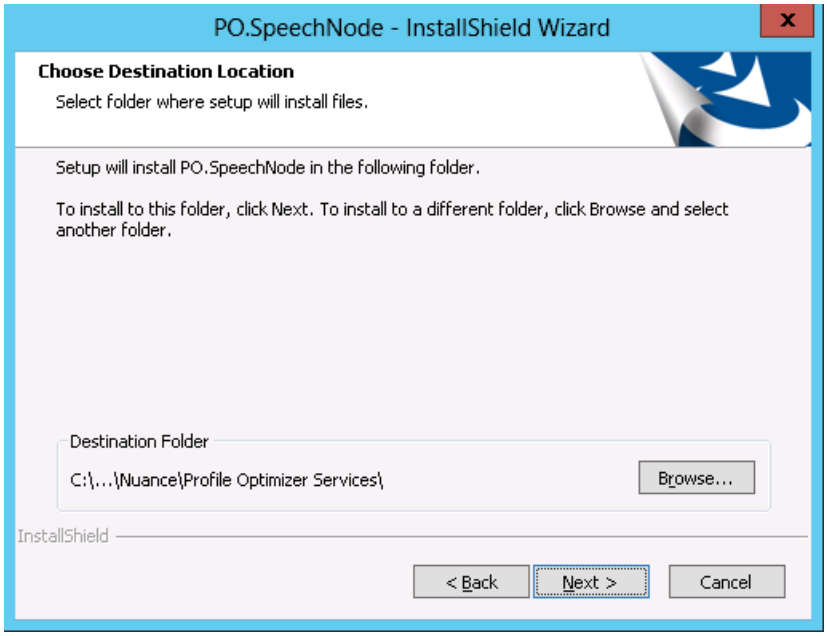
Installing Dragon Medical SDK Client Edition

You can find the *Dragon Medical SDK Client* software on the *NMC server Software and Documentation* DVD. You must install this software on every machine or virtual machine where you plan to install a *Profile Optimizer Speech Node*. To install the software:

1. In the **Dragon Medical SDK Client** directory of the *NMC server Software and Documentation* DVD, find the **Dragon SDK Client Edition** msi file and double click it.
2. Click **Next** and, when choosing the type of installation, be sure to select **Typical/ Complete**.
3. Click **Next** until you reach the installation page of the wizard.
4. Click **Install**.
5. When the installation is complete, click **Finish**.

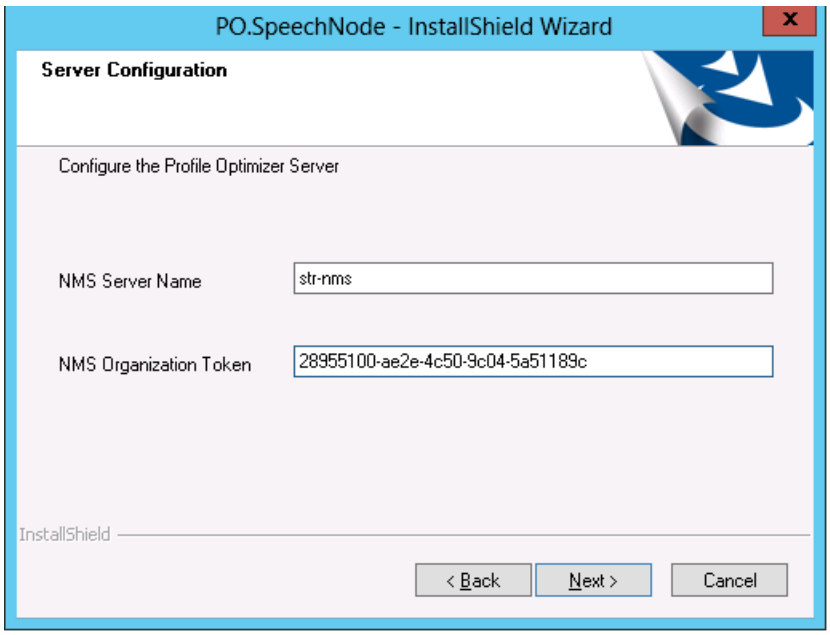
Installing the speech nodes

1. Before you install, you will need an Organization Token. The Organization token is required for both NMC server in the cloud or an on-premise NMC server. If you are using (or migrating to) NMC server in the cloud, Nuance creates the Organization token for your organization and provides it to you. If you are using an on premise NMC server, you must create the Organization Token yourself. To create an Organization Token, see 'Creating Organization Tokens' in the Administrator guide.
2. On the product DVD, right-click the PO.SpeechNode.exe file, and select 'Run as Administrator'.
3. On the **Select the language for the installation from the choices below** screen, click **OK**.
4. On the **Select folder where setup will install files** screen, click **Next**.

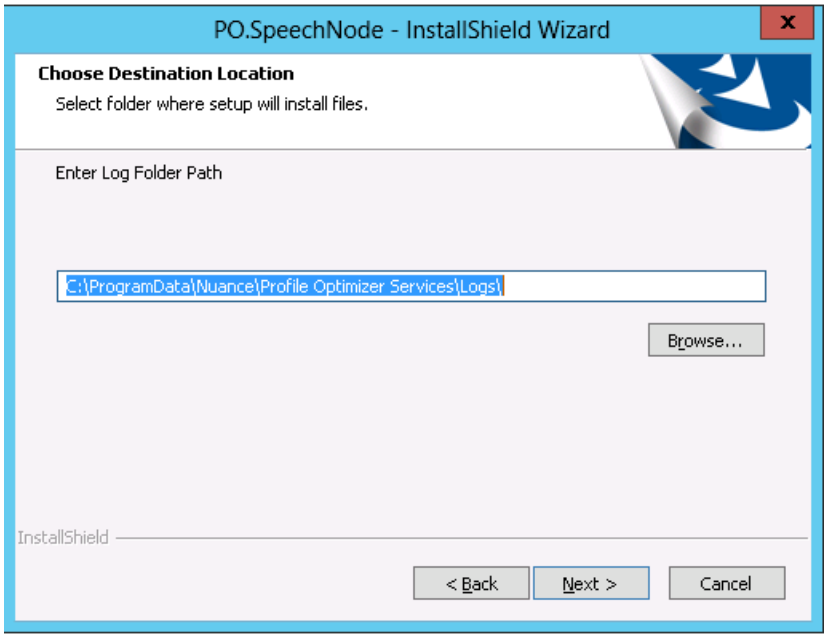


5. On the **Configure the Profile Optimizer Server** screen, enter the NMC server Name and Organization Token. If the system uses multiple NMC servers, enter the name of the load bal-

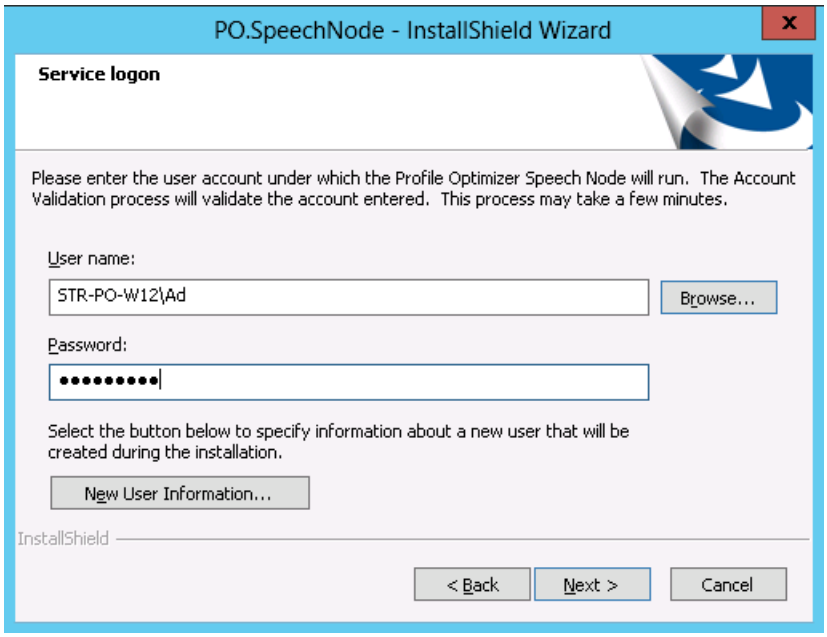
ancer.



6. Click **Next**.
7. On the **Enter Log Folder Path** screen, click **Next** to accept the default path.



8. On the **Service logon** screen, enter the user credentials for the PO Node Service. On this page, you enter the domain and user name of the account to run the services under.



Nuance recommends that you enter the account you created earlier to run all services under, that it be the same account you are running the NMC server under, and that you assign an appropriate name, such as nmcapps, to the account.

9. Click **Next**.
10. On the **Ready to Install the Program** screen, click **Install**.
11. On the **InstallShield Wizard Complete** screen, click **Finish**.

Installing Profile Optimizer Speech Nodes on independent or virtual machines

In large *Dragon Medical Network Edition* configurations, you usually install multiple *Profile Optimizer Speech Nodes* on their own independent machines or on virtual machines.

Installing Profile Optimizer Speech Nodes

To install *Profile Optimizer Speech Nodes* on their own machines or virtual machines, see Installing the speech nodes.

Chapter 5: Starting servers and logging in to the NMC console

Starting the NMC server

After the *NMC server* is installed, if the services do not start on their own, be sure that the account the servers are running under has Windows administrator level privileges, has rights to start a service, and that the same account is the one all entities are running on all servers and (if Windows-based) file servers of the entire Dragon Medical Network Edition network, including *NMC server*, and all *Speech Nodes* and the machine hosting the master user profiles directory.

Caution:

The account running the services for the *NMC server* and *Speech Nodes* must have full access rights on all those machines and on the machine that hosts the master user profiles.

Changing the account running NMC server

If you had no trouble entering the user account the server should run under during the *NMC server* installation, skip to the next subsection, *Starting NMC server service* on page 91.

If during the installation you were forced to change the account that the *NMC server* runs under to the local administrator or local system account, you need to change that account to the same one that the other servers are running under (such as **nmcapps**):

1. Click **Start > Control Panel** and double click **Administrative Tools**, then double click **Services**.
2. In the **Services** list, find the **Nuance Management Service**.
3. Right click on the service name and select **Properties** to open its **Nuance Management Service Properties** dialog box.
4. Click the **LogOn** tab and in the **This Account** text box enter the domain and user name of the account that all *Dragon Medical Network Edition* services should run under, separating them with a backslash:
   <DOMAIN>\<user name>
5. Enter the password in the **Password** and **Confirm Password** text boxes.
6. Click **Apply** to change the account and then click **OK** to close the dialog box.
7. Now you are ready to start any DM Network Edition services that do not automatically start.

Starting NMC server service

After you are sure you have all the necessary privileges, to start *NMC server* service:

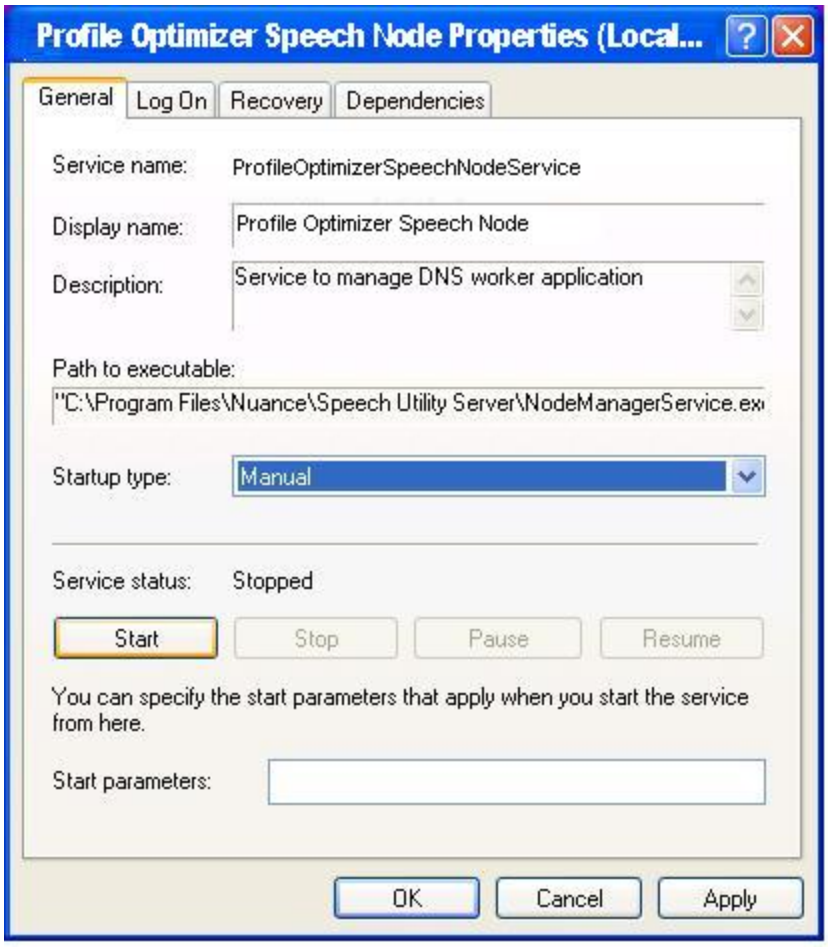
1. Click **Start > Control Panel** and double click **Administrative Tools**, then double click **Services**.
2. In the **Services** list, find the **Nuance Management Service**.
3. To start the service, right click on the service name to open its **Nuance Management Service Properties** dialog box.
4. If the **Startup type** is not set to **Automatic** select **Automatic** from the drop-down list.
5. Click the **Start** button in the lower third of the dialog box.
6. Click **OK** to close the dialog box.

Starting Profile Optimizer Speech Nodes

Running Profile Optimizer Speech Node service

Once you have installed *Profile Optimizer Speech Nodes*, to be sure the *Speech Nodes* are running and to start them if they are not:

1. Click **Start > Control** panel and double click **Administrative Tools** to open the **Administrative Tools** dialog box.
2. Find and double click **Services**. The **Services** dialog box opens, displaying a list of services installed on the machine.
3. Look in the **Name** column for the **Profile Optimizer Speech Node** service. Double click on the service name to open its **Properties** dialog box.



4. In the **Startup type** drop-down list, if the service is not already set to start automatically, select **Automatic**.
5. Under **Service status**, click the **Start** button to the left.
6. After the **Service status** says **Started**, you can click **OK** and close the dialog box.

Troubleshooting: If the Speech Node Will Not Start - Giving Yourself Rights to Start the Service

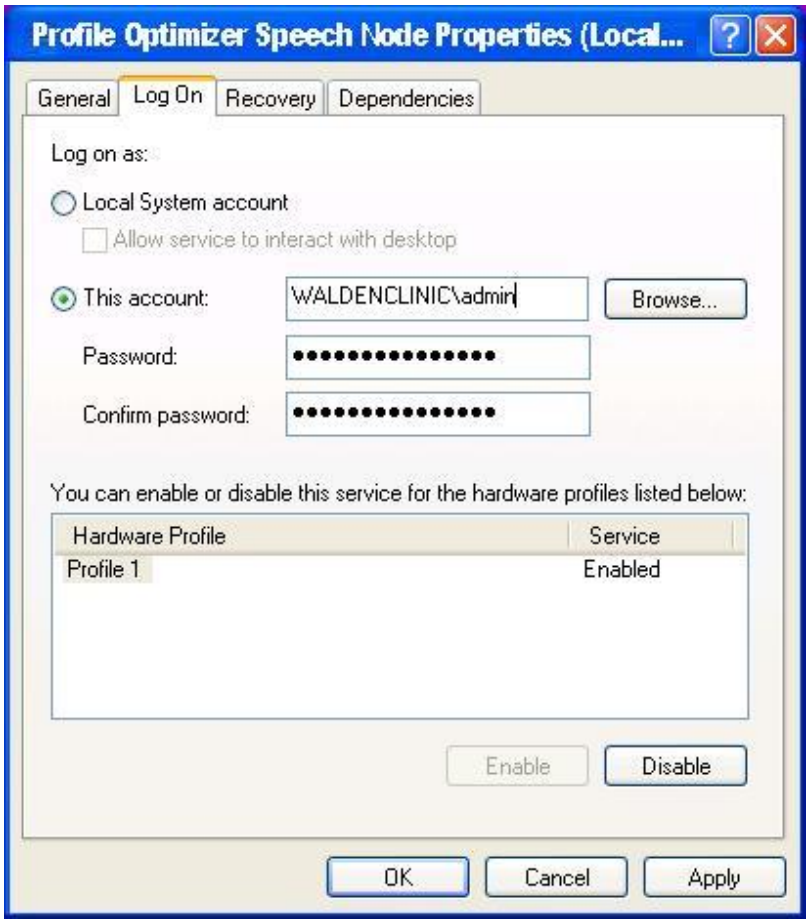
If you cannot start the *Profile Optimizer Speech Node*, you might have only had privileges to install the Speech Node; that means you might not have privileges to run the service that launches the node.

By default, the installation grants you **Log on as Service** level privileges.

If you do not have that privilege, you might receive the error shown below:

A quick way to correct this problem is to enter your credentials in the **Service Control Manager** by taking these steps:

1. Click **Start > Control** panel and double click **Administrative Tools** to open the **Administrative Tools** dialog box.
2. Find and double click **Services**. The **Services** dialog box opens, displaying a list of services installed on the machine.
3. Look in the **Name** column for the **Profile Optimizer Speech Node** service. Double click on the service name to open its **Properties** dialog box.



4. Click the **Log On** tab, then to enter a network domain level user's login and password, click **This account** and enter the domain and user name of the individual who should have access and enter it in the format of <*DOMAIN*>\<*username*> with a backslash between them. The user must be a Windows administrator level user.

   To allow a local machine user to have access, click **This account** and enter <*machineName*>\<*username*> with a backslash between them or **.**<*username*>, where **.** precedes the login name.

Chapter 6: Setting up the Master User Profiles machine

Choosing a master user profiles location for a site

For each site on your *Dragon Medical Network Edition* network, you must determine where on the network the master user profiles should be located. In fact, a site is, by definition, a facility location or group of facility locations in your organization that use the same server location for their user profiles. If all of your user profiles are stored in a single server location, your organization needs only one site.

All user profiles for a single site should be in their own subdirectory of the master user profiles directory.

The *NMC server* lets you store you master user profiles on a Windows server, a networked Windows workstation (a server is not required), or a web server with or without SSL—this last option allowing you to access your master user profiles over the Internet. (The machine storing the master user profiles must be Windows-based.)

If you choose to use a networked Windows server or workstation, you should determine the path to where the master user profiles will reside and be able to access it any of these ways:

- Mapped Drives—Connects to a shared network folder that has a drive letter assigned to it.
- UNC Paths—Connects to a shared network folder using the Universal Naming Convention (UNC) to locate a user. The UNC is a way to identify a shared file on a computer or network without having to know the storage device it is on. Format is: \\<*servername*>\<*sharename*>\<*path*>\<*filename*>.
- HTTP (**http:**)—Connects to machine on the Internet or your local intranet running a web server. Format is: **http://**<*myserver.com*>**/<webdav>**
- HTTP with SSL (**https:**)—Connects to machine on the Internet or your local intranet running a secure socket layer (SSL) web server. Format is: **https://<***myserver.com*>/<*webdav*>

The location(s) you select must be accessible to all computers where healthcare providers dictate. Each location must have adequate storage space for the master user profiles.

Caution:

- If the master user profiles directory is on a separate server or workstation, you must share the top level master user profiles directory in Windows and give **Everyone** full read/write/modify control over the directory, so that the *Dragon Medical Client* can write to those directories when it creates the master user profile for each healthcare provider.
- Be sure that when you set up the master user profiles directory, you locate it either on a Windows machine or on a device connected to a Windows machine with .NET Framework installed on it and that the machine is in the same Windows domain as your DM Network Edition servers. See *System Requirements for Dragon Medical Network Edition* on page 6

If you choose to use server, choose one of the supported web servers. See *System Requirements for Dragon Medical Network Edition* on page 6

Information required for setting up Web Server

If you have chosen to store the master user profiles on a web server or secure web server, you should determine the following information so that you can tell **Dragon** how to connect to the HTTP server:

- **The network location**—You need to know the URL address of your HTTP server.
- **HTTP settings**—For your **http** (or **https**) connection you need to know authentication, firewall, and proxy server information.
- **SSL settings**—For your **https** connection you need to know Certificate store information, and the type(s) of SSL protocols used.
- If you are using **Open SSL**, you need the locations of the cipher list, certificate authority file, and certificate authority directory.

Setting up a computer to host master user profiles

Caution:

If you have proxy servers in your network, they must all point to the machine hosting the master user profiles.

Any time after you have installed the *NMC server* and started its service , you can set up the machine that hosts your master user profiles by taking these actions:

- *Creating the master user profile directory* on page 98
- *Mapping the disk drive on the client workstation* on page 99
- *Setting up access to the master user profile directory* on page 100

Creating the master user profile directory

On the machine that you selected to host the master user profiles for the *Dragon Medical Network Edition* network:

Caution:

Be sure the machine is a Windows server or workstation with the .NET Framework installed (see *System Requirements for Dragon Medical Network Edition* on page 6 for the appropriate version) and that the machine is in your Windows domain. If you are using a RAID array, be sure to attach the device to a Windows machine meeting these requirements. The requirements that machine be a Windows machine with specific software installed differ from roaming user storage requirements for previous non-network editions of *Dragon Medical*.

1. Create a directory to store the profiles. You can have more than one directory for profiles, but you should store all user profiles from providers at the same site in the same location.
2. Write down the machine name and full path to the directory.

Mapping the disk drive on the client workstation

On the workstations where you have the *Dragon Medical Client* installed or in the Windows user profiles of all providers who will later dictate:

If your workstations uses a mapped drive to access the master user profiles, map a drive letter to the location where the master user profiles are located on every machine running the *Dragon Medical Client*. This mapping must be the same on every workstation and every Windows user profile.

Setting up access to the master user profile directory

Please see 'Setting general site settings for master user profiles' in the DM Network Edition Administrator Guide.

Installing software for storing master user profiles on a web server

Caution:

If you have never set up a web server or secure web server before, do not attempt to do so; these instructions assume you have experience setting up a web server. Appropriate settings vary.

After you install the *NMC server* and *NMC console*, if you choose to store your master user profiles on a web server or secure web server, be sure you have the correct type of server, download the required software, and make the correct selections while installing the web server.

Notes:

- Storing your master user profiles on a web server or secure web server is entirely optional. You can choose to store them on a mapped drive, on any *Dragon Medical Network Edition* network physical server or workstation with adequate storage space, or on their own Windows server or workstation within your network's domain without using a web server at all.
- By default ,IIS can only send files less than 30 MB in size over a WebDAV connection. To increase the size limit, follow the instructions in: https://www.iis.net/configreference/system.webserver/security/requestfiltering/requestlimits.

To store the master user profiles on one of the web servers below, first be sure you have .NET Framework 4.5.2 installed as well as the associated WebDAV software for the server. For more information, visit the software provider's site (some links below are provided for reference):

- Microsoft Internet Information Services (IIS) Version 10 on Windows Server 2016:
  - https://www.iis.net/learn/get-started/whats-new-in-iis-10/wildcard-host-header-support
- Microsoft Internet Information Services (IIS) Version 8.5 on Windows Server 2012 R2:
  - http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2

- Microsoft Internet Information Services (IIS) Version 8.0 on Windows Server 2012:
  - http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012
- Microsoft Internet Information Services (IIS) Version 7.0 or 7.5 0 on Windows Server 2008:
  - 32-bit Version: http://learn.iis.net/page.aspx/350/installing-and-configuring-webdav-on-iis-7/webdav_x86_75.msi
  - 64-bit Version: http://learn.iis.net/page.aspx/350/installing-and-configuring-webdav-on-iis-7/webdav_x64_75.msi
- Apache Server 2.2.32 or higher on Windows Server 2012 and Windows Server 2012 R2:

  This server should run on Windows Server 2008 R2 or Windows Server 2012 R2 and also runs on Windows 7, 8.x, 10, or Vista. For more information see:
  - http://www.markwilson.co.uk/blog/2007/07/apache-http-server-on-windows-server-2008-server-core.htm
  - http://www.thesitewizard.com/apache/install-apache-on-vista.shtml

For more information on installing Apache web server, see: http://www.apache.org/

Configure Internet Information Services 8.x

1. Open the Internet Information Services (IIS) Manager window.
2. On **Server name**, right-click: **Add Website**.
3. In **Site name**, enter the name for the site.
4. In **Physical path**, enter the path to the location of the master user profiles.
5. Leave the other settings and fields as is.
6. In the Internet Information Services (IIS) Manager window, in the left-side panel, under **Sites**, select your site and go to **Directory Browsing**.
7. Click **Enable**.
8. In the Internet Information Services (IIS) Manager window, in the left-side panel, under **Sites**, select your site and go to **Handler Mappings**.
9. Click **Edit Feature Permissions**.
10. Select **Execute**.
11. Click **OK**.
12. In the Internet Information Services (IIS) Manager window, in the left-side panel, under **Sites**, select your site and go to **Authentication**.
13. Right click on Basic **Authentication**.
14. Click **Enable**.
15. Right click on **Anonymous Authentication** .
16. Click **Disable**.
17. Click **OK**.

Configure SSL

1. Open the Internet Information Services (IIS) Manager window.
2. Click on **Server name**.
3. Open **Server Certificates**.
4. Import the certificate.
5. In the Internet Information Services (IIS) Manager window, in the left-side panel, under **Sites**, right-click your site.

6. In the righ-side panel, under **Actions**, click **Bindings**.
7. In the **Site Bindings** window, click **Add**.
8. Under **Type**, choose https.
9. In **IP address**, enter an IP address for the site or leave as is.
10. In the drop-down field under **SSL certificate**, select the SSL certificate.
11. Click **OK**.

Setting HTTP connection settings for web server

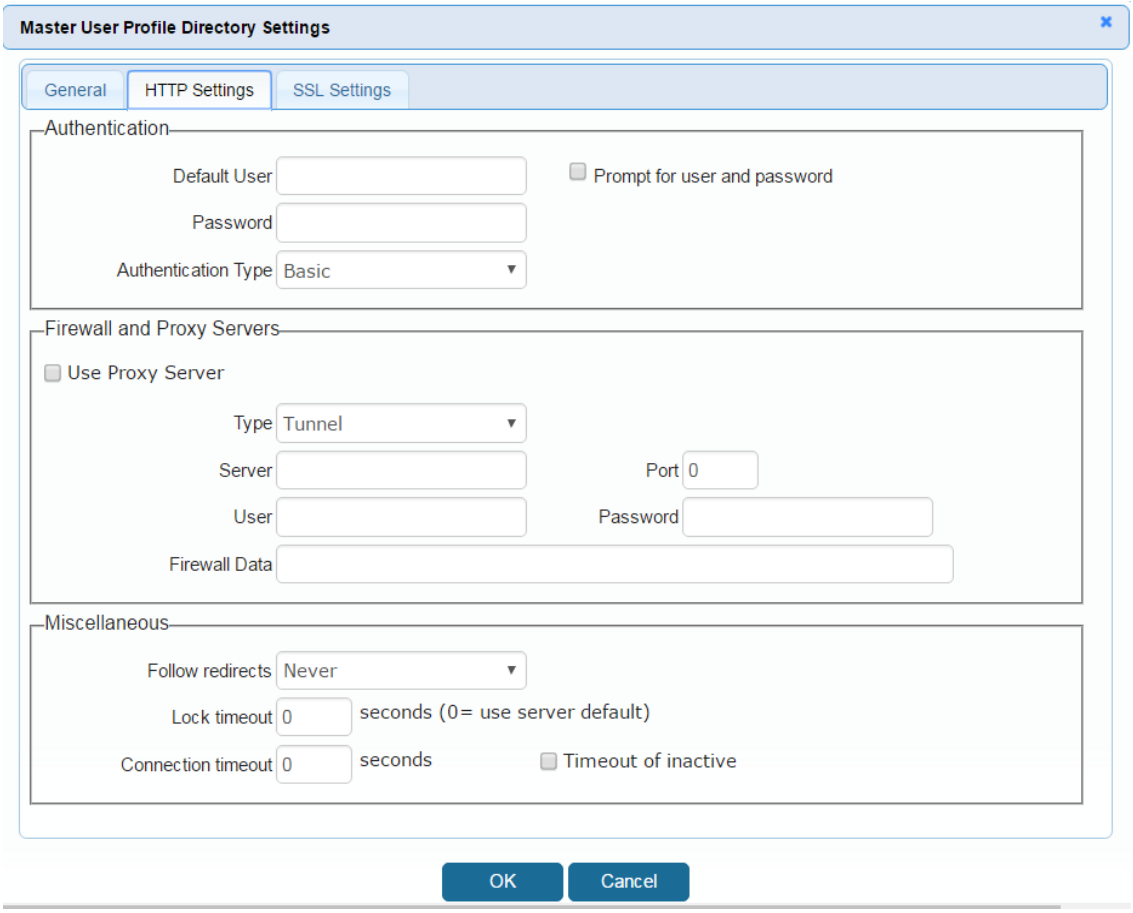
Caution:

If you have never set up a web server before, do not attempt to do so; these instructions assume you have experience setting up a web server, and appropriate settings to use vary.

After you install your web server, you must set HTTP connection settings in the *NMC console*. For details on how to set up a site, refer to the *NMC server Administrator Guide*.

Note:

You set these **HTTP Settings** only to store master user profiles on a web server.



Making selections on HTTP Settings tab

The next table shows the settings you should select for each type of web server (not using SSL).

Recommended HTTP settings for particular web servers

Web Server Type & Version	Default Values for IIS 7.0, 7.5, 8.0, and 8.5	Default Values for Apache 2.0.xx or 2.2.xx	Other Considerations Based on Your Site Configuration
Authentication			
Prompt for user and password	Off		Turn off to prevent prompt for a user-name/password when *Dragon Client* accesses master user profiles.
Default user	Empty		Enter username for the account that the servers run under, such as **nmcapps**.
Password	Empty		Enter password for the account that servers run under.
Authentication type	**Basic**	**Basic** or **Digest**	For IIS, always choose **Basic**. For Apache, choose type you set up on the web server. **Basic authentication** sends transmits as plain text. **Digest authentication** transmits passwords in encrypted form.
Firewall and Proxy Servers			
Use proxy server	Off		Check (On) if you are connecting through a proxy server.
Type	**HTTP**		**HTTP** for web page transactions. **Tunnel** if you are using tunneling software. **Socks4** for SOCKS4 protocol/transparent client access across firewall. **Socks5** for SOCKS5 protocol/transparent access across firewall and SOCKS5 server DNS lookup.
Server	Empty		Enter name of the proxy server.
Port	Empty		Enter number of port for proxy server or firewall.
User	Empty		Enter user name for logging in to proxy server or firewall.
Password	Empty		Enter password for logging in to proxy server or firewall.
Firewall data	Empty		Enter any special authentication string required.
Miscellaneous			
Follow redirects	Off	**Always** or **Same Scheme Only**	Never turn off. Handles redirects of incoming connections.

Web Server Type & Version	Default Values for IIS 7.0, 7.5, 8.0, and 8.5	Default Values for Apache 2.0.xx or 2.2.xx	Other Considerations Based on Your Site Configuration
Keep connection alive	Off		Could be turned on even if turned off for the site. If on, keeps the connection alive after current communication ends, which can be useful if the connection setup process involves multiple message transfers between the web server and the client or server interacting with it. Should be off if you have **Follow Redirects** set to anything other than **Never**.
Lock timeout	**120** seconds		Never set this value to **0**. Setting the value to 0 causes the web server to choose a timeout which may be excessively long, and can result in users being locked out of their user profiles.
Connection timeout	**60**		Must be **60**.
Timeout of inactive	Off		Must be On.

Setting SSL connection settings for secure web server

Caution:

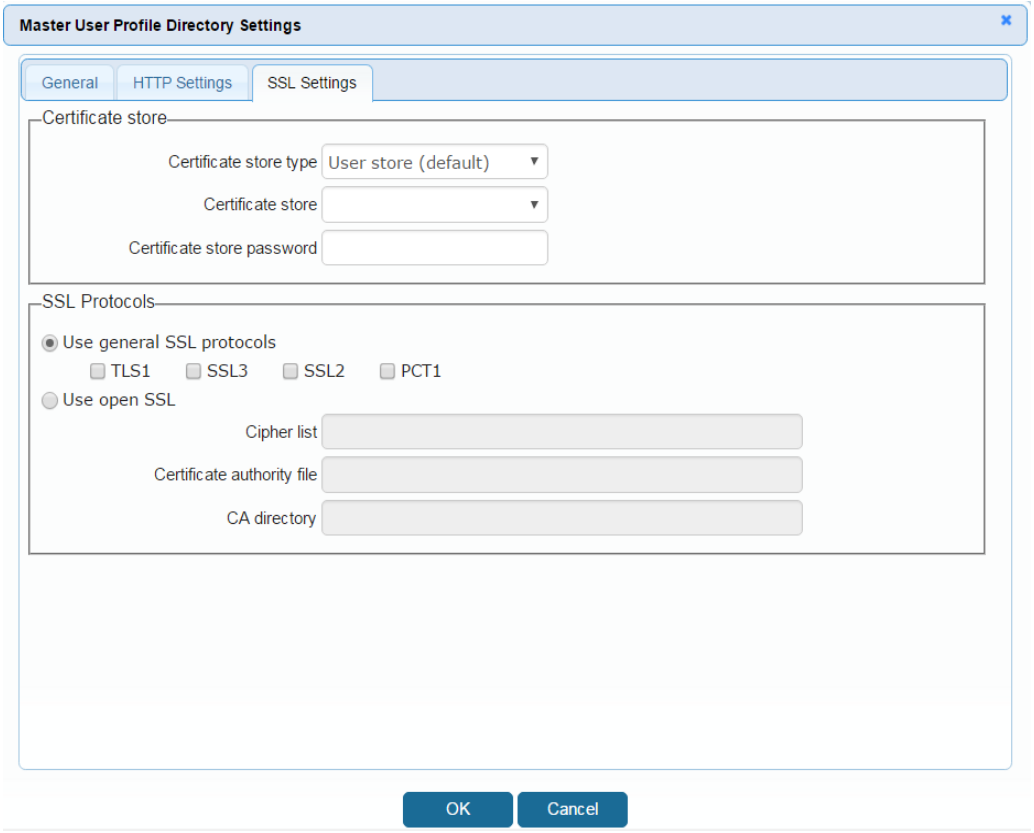
If you have never set up a secure web server before, do not attempt to do so; these instructions assume you have experience setting up a secure web server. Appropriate settings vary. Be sure that you install an SSL certificate that is trusted for directory on every workstation. You should push install the SSL certificate as Trusted Root Certificate Author.

After you install your secure web server, you must set SSL connection settings in the *NMC console*. For details on how to set up a site, refer to the *NMC server Administrator Guide* .

Note:

You set these SSL Settings only to store your master user profiles on a secure web server.

Settings on SSL Settings tab



Recommended settings for SSL web servers

The table below shows the settings you should select for various versions of each type of secure web server. In general, you have flexibility in selecting these settings and should select those appropriate for your installation.

Recommended settings for particular secure web servers

Web Server Type & Version	IIS 7.0, or 7.5	Apache 2.0.xx or 2..xx	Other Considerations Based on Your Site Configuration
Certificate store			
Certificate store type	User Store	User Store	
Certificate store	My	My	
Certificate store password	Empty	Empty	
SSL Protocols			
Use general SSL	On	On	Check all protocols your server might receive legit-

Web Server Type & Version	IIS 7.0, or 7.5	Apache 2.0.xx or 2..xx	Other Considerations Based on Your Site Configuration
protocols			imate input from: **TLS1**, **SSL3**, **SSL2**, and **PCT1**.
Use Open SSL	On	On	
Cipher List	String of ciphers if applicable.		These options apply only if you are using **OpenSSL** as a Certificate Authority. Refer to the *NMC server Administrator Guide* for details.
Certificate authority file	Name of file containing list of certificate authorities to trust.		
CA directory	Path to the directory where certificate authority certificates reside.		

Assigning access to folders and master user profiles across the network

Caution:

To ensure that your *Dragon Medical Clients* can communicate with the master user profiles server and the other servers, you must assign correct permissions to all appropriate directories and access rights to particular keys in the registry, as indicated in the tables in *Assigning access to servers, clients, and master user profiles across network* on page 1. Do not skip this step, as it is important!

Turning off Automatic Updates

On each machine you plan to use in the network, be sure to turn off Windows Automatic Updates. You should, instead, qualify each update Windows sends by installing it first on a single test machine of the network and then updating other machines on the network only after you determine that it clearly will not disrupt the network.

Once you are sure an update does not have any negative effects, you should install the update during off-hours and, if required, reboot each machine during those hours to ensure that requests to reboot do not disrupt the servers or workstations during peak hours of dictation.

Chapter 7: Upgrading roaming and local User Profiles

Preparing to upgrade non-network edition Dragon Medical Clients

If you are planning to install the *Dragon Medical Network Edition* on a computer where *Dragon Medical Client* is already installed, you do not have to uninstall the non-*Network Edition* first. However, Nuance recommends you uninstall *Dragon Medical* first if doing so would not disrupt the operation of your medical facility.

Before you upgrade Dragon Medical non-network edition

If you choose to uninstall the non-*Network Edition* of *Dragon Medical*, you should be sure to take these steps first:

- Save and back up all user profiles.
- If you have any local users (not roaming) from *Dragon Medical* 10.x (non-*Network Edition*), prepare to move them to DM Network Edition as explained in *Migrating Non-Network Dragon User Profiles to the NMC server* on page 117
- Save any *Dragon Medical* 10.x roaming user profiles to a location where the *NMC server* can access them.
- Uninstall the previous edition of *Dragon Medical* (optional, but recommended).
- Install the new Dragon client on each client workstation.

Note:

The term ***roaming user profiles*** has been changed for DM Network Edition. Since all users of the DM Network Edition server networks are *roaming* by definition (the master copy of their profiles always resides on a central machine), the profiles stored on a central machine are now called ***master user profiles***. When a provider dictates, the *Dragon Medical Client* retrieves a copy of the master user profile and that copy is called the ***local cache user profile***.

When you upgrade previously existing ***roaming user profiles*** or ***local user profiles*** for use with Dragon Medical Network Edition, these profiles all become ***master user profiles***.

Overview of migrating local users from Dragon Medical Practice Edition

If you have local users from Dragon Medical Practice Edition, to move them to *Dragon Medical Network Edition*, you take these general steps:

1. If any local users have multiple login names, combine all of their profiles under a single login name.
2. Export the local user profiles to a different location, so that the action you take does not affect the user profiles of dictating providers. In Dragon Medical Network Edition, 2.7, you use the Dragon client to export and import user profiles. For details, see the Dragon Help
3. Enable the ***Roaming*** feature on the workstation and save the local users to the roaming user location.
4. Export each roaming user profile to a location where the *NMC server* can access it. In Dragon Medical Network Edition, 2.7, you use the Dragon client to export and import user profiles. For details, see the Dragon Help.
5. Create user accounts in *NMC server* for the healthcare providers dictating with the local user profiles you are converting.
6. Associate the user accounts with the master user profiles for the corresponding healthcare professionals.

For more details, refer to *Migrating Non-Network Dragon User Profiles to the NMC server* on page 117.

After you install the Dragon Medical client, perform the following steps

After you install *Dragon Medical Network Edition*, on the new client:

1. Log in to the *Dragon Medical Enterprise Client* with the *NMC server* user account login and password.
2. Re-import any custom words, commands, and vocabularies as instructed in the Dragon Help.

Creating user accounts for healthcare providers

See 'Creating user accounts' in the Administrator guide.

Migrating Non-Network Dragon User Profiles to the NMC server

If you want to migrate *Dragon Medical* (non-network) user profiles (stored only on *Dragon Medical Client* workstations) to DM Network Edition (where they become master user profiles on the network), complete the following steps:

Before migrating Dragon local user profiles

Caution:

Nuance recommends that you protect your profile data by taking these precautions:

- Migrating profiles can take a long time. Because of this, plan to convert the *Dragon Medical* local user profiles at a time when healthcare providers are not using them to dictate, such as at night or on a weekend. If there is no time when all your user profiles are not in use (because healthcare providers dictate 24/7), you can convert sets of local user profiles from particular workstations at appropriate times.
- Note that once you migrate these user profiles, if you continue using the profiles stored on the workstations (instead of the versions on the NMC server), any additions or changes to those user profiles will not propagate to the copies on the NMC server.
- Make sure that the Dragon workstations that contain profiles you want to convert have .NET Framework Version 4.5.2 installed.

  See Microsoft's documentation for more information on installing the .NET framework.

Migration Paths

Nuance Communications supports migrating from the following products to DM Network Edition, version 2.7:

Patch installer and Full installer

- DMNE 2.x

Full installer

- Service Pack 6
- DMPE 11, DMEE 10.1

Overview of migrating local user profiles

To migrate Dragon Medical Practice Edition and Dragon Medical Enterprise Edition local user profiles to DM Network Edition Version 2.7 user profiles, on each workstation with users to move to DM Network Edition, you take these major steps:

1. Back up local user profiles by exporting them to a different location, so that the actions you take do not affect the user profiles of dictating providers. See *Migrating Non-Network Dragon User Profiles to the NMC server* on page 117
2. If a healthcare provider has multiple user names for logging in, that provider has more than one profile. For efficiency, you should combine multiple user profiles for the same provider, creating a single user profile for that person. See *Migrating Non-Network Dragon User Profiles to the NMC server* on page 117 for more information.
3. If they aren't already there, export the profiles that you want to upgrade to the default location for Dragon user profiles. See *Migrating Non-Network Dragon User Profiles to the NMC server* on page 117 for more information.
4. On the NMC server , set the directory for the user profiles that you are migrating. See *Step 7: Create user accounts for the migrated profiles on the NMC server* on page 124 for more information.
5. Copy the directory containing the User Profile Export Tool to a location on the network that can access all of the DM Network Edition and Dragon Medical Enterprise Edition workstations that you want to upgrade. See *Step 5: Copy the User Profile Export Tool to a network location* on page 123 for more information.

6. Install and run the User Profile Export tool. See *Step 6: Install and Run the User Profile Export Tool* on page 123
7. Create user accounts in *NMC server* for the healthcare providers dictating with the local user profiles you are converting. See *Step 7: Create user accounts for the migrated profiles on the NMC server* on page 124 for more information.
8. Associate the user accounts with the master user profiles for the corresponding healthcare professionals. See *Step 8: Associate the new user accounts with the profiles you migrated in Step 6* on page 124 for more information.
9. Upgrade the master user profiles. See *Step 9: Upgrade the User Profiles* on page 124
10. Install the *Dragon Medical Enterprise Client* on the workstation.
11. Log in to the *Dragon Medical Enterprise Client* with the *NMC server* user account login and password. See *Step 11: Log in* on page 125

Step 1: Back up local user profiles

Before you migrate your local user profiles, you should back them up to ensure that you'll still have them if anything goes wrong. To do this, export the local user(s) from the workstation where Dragon Medical Practice Edition or Dragon Medical Enterprise Edition is installed to a separate directory on the same machine or to a shared location on the network:

1. Create a temporary location for the user profiles (for example, **CpyLocProfiles**).
2. Map a drive to the location for the user profiles (for example, **Z:\CpyLocProfiles**).
3. Start Dragon Medical Practice Edition or Dragon Medical Enterprise Edition.
4. On the DragonBar, select **Profile > Manage user**.
5. When the **Manage Users** dialog box appears, select the name of the user profile you want to make a copy of and then select **Advanced > Export**.
6. Browse the repository where you are storing the copies of local profiles (**Z:\CpyLocProfiles**) and click **OK**.
7. Repeat the above steps for each user profile you want to copy.

Step 2: Combine multiple Dragon Medical profiles for a single provider (DMEE only)

Any healthcare provider who has more than one user name, has more than one user profile. If you have any such providers, you need to reduce their profiles to a single user profile for using with *Dragon Medical Network Edition*. The single profile can have more than one vocabulary and more than one audio input device (dictation source), so it is not any more restrictive than working with multiple profiles.

To combine the multiple profiles, take these steps:

Export custom words from extra profiles

1. In Dragon Medical Enterprise Edition, on the DragonBar, select **Dragon > Open User Profile**.
2. In the list of user profile names, decide which profile you want to merge the others into for the provider. If you are not sure which profile to select, you should find out the one that the provider most recently used and keep that profile. You can click the **Properties** button to find out the date each profile was last saved.
3. Open one of the profiles you do not expect to keep. You see the vocabulary it uses.
4. Select **Vocabulary > Export custom word and phrase list** or **Vocabulary > Export words with customized properties** to export all custom words created with this profile. When the **Export Custom Words** or **Export Customized Words** dialog box opens, browse to the directory where you want to save the file and save the words in a **.txt** file. You can name it whatever you would like—usually a name containing the user name and the vocabulary helps identify the file. For example, you might name it **ConradCardiology.txt**.

Export commands from extra profiles

1. On the DragonBar, select **Tools > Command Browser** and open the **Task Pane**.
2. In the **Task Pane**, click **Manage** (under **Mode**). You then see a list of command types appear in the pane to the right.
3. Select all check boxes for all command types in the pane to the right.
4. In the **Task Pane**, click **Export** (under **Manage**).

5. When the **Export Commands** dialog box opens, browse to the directory where you want to save the file and save the custom commands as a **.dat** file using the same root name as you used for the **.txt** file of words. For example, you might name the file **ConradCardiology.dat**.

Export vocabularies from extra profiles

1. If the provider has multiple vocabularies, go to the DragonBar and select **Vocabulary > Manage Vocabularies...**. Select the vocabulary in the list and click the **Export** button to the right.
2. When the **Save As** dialog box opens, save the vocabulary in a **.Top** file using the same root name as you used for the words and commands. For example, you might name it **ConradCardiology.Top**.

Import commands into the profile you are retaining

1. Open the profile you are retaining and plan to upgrade to DM Network Edition.
2. On the DragonBar, select **Tools > Command Browser**.
3. Open the **Task Pane** and in the **Task Pane** click **Manage** (under **Mode**).
4. In the **Task Pane**, click **Import** (under **Manage**).
5. In the **Import Commands** dialog box, select the **.dat** file you saved earlier and click **Open**.
6. In the **Import Commands** dialog box, click **Import**.
7. If any of the commands would replace a command with the same name, you are prompted to replace the existing command. Click **No** if you are uncertain whether or not to replace the command. Remember, the user profile you are keeping is the newest one, so probably has the newest command by the same name.

Import vocabulary into the profile you are retaining

1. If it is not already open, open the profile you are retaining and plan to upgrade to DM Network Edition.
2. On the DragonBar, select **Vocabulary > Manage Vocabularies...** .
3. In the **Manage Vocabularies** dialog box, click **New** and in the **New Vocabulary** dialog box, name the vocabulary anything you would like and choose a vocabulary to base it on from the pull down list for **Based on**. Then click **OK**.
4. When the **Manage Vocabularies** dialog box reappears, you see the additional vocabulary in the list.

Import words into the profile you are retaining

1. If it is not already open, open the profile you are retaining and plan to upgrade to DM Network Edition.
2. On the DragonBar, select **Vocabulary > Import list of words or phrases**.
3. When the **Import list of words or phrases** Wizard appears, click **Next**.
4. Click **Add File** and when the **Add File** dialog box opens, select the file of words you exported earlier and click **Open**.
5. Click **Next** to advance the wizard until you reach the end.
6. Click **Finish** to complete the process and close the wizard.

Step 3: Export user profiles to the default user profile directory

Your user profiles should be in Dragon's default user profile directory—if they are, you can skip this step. If they aren't—if you have changed the location where the profiles are stored, for example, or you are exporting roaming user profiles—complete the following steps to export them to the default directory:

1. Start Dragon Medical Practice Edition or Dragon Medical Enterprise Edition.
2. In Dragon (non-Network Edition), on the DragonBar, select **Dragon > Manage User**.
3. When the **Manage Users** dialog box appears, select the name of the user profile you want to make a copy of and then select **Advanced > Export**.
4. Browse to the default location for Dragon user profiles.

   If you are running Dragon on Windows XP, this is the path:

   C:\Documents and Settings\All Users\Application Data\Nuance\NaturallySpeaking<VersionNumber>\Users

   where <VersionNumber> is the version number of your Dragon installation.

   If you are running Dragon on Windows 7, 8.x, or 10, this is the path:

   C:\Program Data\Nuance\NaturallySpeaking<VersionNumber>\Users

   where <VersionNumber> is the version number of your Dragon installation.

5. Click **OK**.
6. Repeat the preceding steps for each user profile you want to copy.

(missing or bad snippet)

Step 4: Set Up a Directory for the User Profiles via the NMC console

Set up the directory for the migrated profiles using the NMC console by entering the path to your chosen directory in the **DMNE Version 2.0 (or higher) Speech Profile Location** field of the Master User Profile Directory Settings dialog.

See *Configuring the location of user profiles* on page 128 for instructions.

Step 5: Copy the User Profile Export Tool to a network location

The DM Network Edition client installation DVD includes a profile export tool. You must copy the directory containing the export tool to a location on your network where you can do a push install via .msi to all the Dragon workstations containing profiles that you want to export.

1. Open the DM Network Edition Client installation DVD and locate the following directory:

   ```
   DNS12_DVD1/Dragon Profile Export
   ```

2. Copy the Dragon Profile Export directory to a location on the network where you can run an .msi install to all Dragon workstations containing profiles that you want to export.

Step 6: Install and Run the User Profile Export Tool

1. Use the following command to install the User Profile Export Tool:

   ```
   msiexec.exe /i DgnProfileExport.msi NETWORKLOCATION=<location>
   [NETWORKCREDENTIALS=PROMPT] /qn
   ```

Parameter	Description
NETWORKLOCATION (Required)	A path—either a UNC path or a path to a mapped drive—to the network location of the DM Network Edition Version 2.7 User Profiles. See the *Configuring the location of user profiles* section of the DM Network Edition Administrator's Guide for more information.
NETWORKCREDENTIALS (Required)	Set this value to PROMPT. This insures that if a network connection isn't established prior to the running the User Profile Export Tool, the tool prompts for Windows user credentials and

Parameter	Description
	establishes a network connection before your profiles are exported.

MSI command line example

```
msiexec.exe /i "DgnProfileExport.msi" NETWORKLOCATION-
N=\\myserver\DragonUsers\Exported NETWORKCREDENTIALS-
S=PROMPT /qn
```

2. Reboot the Dragon Medical Client workstation where the tool is installed. The User Profile Export Tool is invoked on reboot.

   The exported profiles appear in the specified user profile directory with the following naming convention:

   username.workstation

   For example, a profile with username `John_Doe` on the `DoeWorkstation` will be named:

   `John_Doe.DoeWorkstation`

Step 7: Create user accounts for the migrated profiles on the NMC server

Log on to the NMC console and create user accounts in *NMC server* for the healthcare providers who dictate with the local user profiles you are migrating. For more information on creating users, refer to *Creating user accounts for healthcare providers* on page 117.

Step 8: Associate the new user accounts with the profiles you migrated in Step 6

Associate the user accounts with the master user profiles for the corresponding healthcare professionals. For more information, see *Associating new user accounts with upgraded user profiles* on page 130.

Step 9: Upgrade the User Profiles

Upgrade your user profiles to the latest version by following the instructions in *Upgrading a user profile to DM Network Edition Version 2.7* on page 129.

Step 10: Install/Upgrade the Dragon Client on the workstations

Install/Upgrade the Dragon Medical Client on the workstation.

Step 11: Log in

Log in to the Dragon Medical Client with the *NMC server* user account login and password. For more information, see *Logging in to the NMC server through the NMC console* on page 1.

Upgrading User Profiles from DM Network Edition Version 10.x to Version 2.0 or Higher

After you have upgraded the NMC server , you must upgrade your DM Network Edition Version 10.5 user profiles to DM Network Edition 2.7 or higher.

Before upgrading Dragon user profiles

Caution:

Nuance recommends that you plan to upgrade the *Dragon Medical* user profiles at a time when healthcare providers are not using them to dictate, such as at night or on a weekend. If there is no time when all your user profiles are not in use (because healthcare providers dictate 24/7), you can convert sets of local user profiles from particular workstations at appropriate times.

Note:

- If you are upgrading from a version of DM Network Edition that is not Service Pack 3 or higher, you must first upgrade to Service Pack 3. See the *DM Network Edition SP 3 Installation Guide* for more information.
- Nuance recommends upgrading user profiles on multi-core machines for better throughput. Profiles upgraded on machines with a number of cores that is different than the number of cores on the speech nodes that run the profiles generates a warning message about recognition accuracy. For example, if you upgrade your profiles on a dual core machine but run them on a single core speech node, the warning message appears when the profile is opened.

  To prevent the warning message from appearing, use machines with the same number of cores to upgrade speech profiles and for the speech nodes. For example, if you upgrade the profiles on a dual core machine, run those profiles on dual core speech nodes.

Complete the following tasks before you upgrade your user profiles:

- Configure the Master User Profile directory for the DM Network Edition Version 2.0 (and higher) user profiles by entering the path to your chosen directory in the **DMNE Version 2.0 (or higher) Speech Profile Location** field of the Master User Profile Directory Settings dialog.

  See *Configuring the location of user profiles* on page 128 for instructions.

- Share the Master User Profile directory and grant the Nuance service account (for instance `nmcapps`) at least Modify permissions to the folder structure. This share should mirror the same access permissions as the DM Network Edition 10.x Master Profile directory share.

- For each speech node, set the user profile directory for DMENE 2.0 and higher to the same location as your Master User Profile Directory.

  See *Configuring the location of user profiles* on page 128 for instructions.

Upgrade the User Profiles

Complete the following steps to upgrade your DM Network Edition user profiles:

1. Log in to the NMC console.
2. Go to the site that contains the user profiles that you want to upgrade and click the **DM Network Edition** tab. The DM Network Edition settings interface appears.
3. Click the **+** icon next to **Master user profile** to expand the Master user profile options.
4. Click the **Initiate Speech Profile Upgrade to DMNE Version 2.0** button. A dialog appears asking if you want to upgrade speech profiles to DM Network Edition Version 2.0. Click **YES** to start the upgrade.
5. When the profile upgrade is complete, the NMC console sends a confirmation message to the Administrator.
6. Install/Upgrade the Dragon Medical Client on the workstation. .
7. Log in to the Dragon Medical Client with a DM Network Edition user name and password.

Configuring the location of user profiles

Each version has its own user profile location.

When an end user logs into Dragon through the NMC server, the NMC server sends the location of the user's profile to Dragon. This allows Dragon to find and access the user profile.

For details about how an administrator can configure these locations in the NMC console, see 'Configuring the location of user profiles' in the Administrator guide.

Upgrading a user profile to DM Network Edition Version 2.7

See 'Upgrading a user profile to DM Network Edition Version 2.7' in the Administrator guide.

Associating new user accounts with upgraded user profiles

If you have not already done so, you should upgrade any user profiles from *Dragon Medical* Versions as described elsewhere in this chapter.

For information about how to associate new user accounts with upgraded user profiles, see 'Associating new user accounts with existing user profiles' in the Administrator guide.

Chapter 8: Installing the Dragon Medical Client

Overview of installing the Dragon Medical Client

Caution:

The account that each *Dragon Medical Client* workstation runs under must have full read/write/-modify access to the master user profiles directory so that *Dragon* can create and modify the master user profile for each healthcare provider.

When you install the client, you usually perform a *typical Dragon* installation.

However, if you want to set up *Dragon* so that the *DragonBar* always comes up in, for instance, Floating mode on every single client workstation in your network, you can still set some options in advance of the installation by using the *Dragon Medical SDK Client*, available on the *NMC server Software and Documentation* DVD. After you set the options, you can retrieve the **nsdefaults.ini** file and pass it as an argument to **msiexec.exe** (the MSI installer from Microsoft).

Opening ports to access user profiles on web server or secure web server

Caution:

It is critical that if they are not already open, you open the ports required for the *Dragon Medical Client* to access the master user profiles on a web server or secure web serve

For details about the ports to open to access user profiles on a web server or secure web server, see 'Ports to open for clients, servers, and hardware firewalls' in the Planning guide.

Approaches to installing the Dragon Medical Client

You can install the *Dragon Medical Client* in any of these ways:

- *Installing Dragon manually outside of the NMC console* on page 137
- *Pushing the Dragon MSI installation to workstations* on page 140

- *Carrying out administrative installation of Dragon with .bat file* on page 1
- *Creating a custom installer for the client in Active Directory* on page 148

Pushing the Dragon MSI installation to workstations

An overview of the options for installing multiple *Dragon Medical Client* workstations at once is provided below.

The Dragon Medical Network Edition DVD includes a Microsoft Windows Installer (MSI) file. You can use this MSI file to install *Dragon* from a server to client workstations across a network or to install several client workstations at once using either an SMS or SCCM installation or an ActiveDirectory Services installation.

Caution: Whenever you carry out an MSI installation of DM Network Edition, Nuance recommends that you uninstall any *Dragon Medical* software already on the machine before it proceeds to install the new client software. You can do this via the MSI installer using the **/x**<*Product.msi*> command, where <*Product.msi*> is the name of the .msi file of the version of DM Network Edition that you are uninstalling. For more information on command line options you can use to install Dragon, refer to *Understanding Dragon MSI command line options* on page 143.

Note:

When you create an MSI installer for the *Dragon Medical Client* included with the *NMC server*, you are not required to have the installer set any user or administrative options that you would prefer to set in the *NMC server* later.

DVD name	MSI file name
Dragon Medical Enterprise Network Edition Client Software DVD	Dragon NaturallySpeaking 12.msi
NMC server Software and Documentation DVD	Dragon SDK Client Edition 12.msi

The command line you use to install *Dragon* using the **.MSI** file is:

```
msiexec.exe /i "Dragon NaturallySpeaking 12.msi"
```

- General options for installing *Dragon*
- MSI options for installing *Dragon* features/advanced options
- Feature variables to set through the ADDLOCAL or ADVERTISE properties

Options for pushing MSI installation of Dragon to one or more workstations on a network

You can use a server application to push an MSI installation of *Dragon* to client workstations without having to install *Dragon* separately on each computer. The server administrator creates an image of the *Dragon* installation program. The administrator then places the image on a server and configures the server to automatically push the application to client workstations.

There are several server applications that you can use to push a *Dragon* installation. See *System Requirements for Dragon Medical Network Edition* on page 6 for supported versions:

- Windows Server
- System Center Configuration Manager (SCCM)
- Active Directory Services

Support for the Windows System Center Configuration Manager

You can use the System Center Configuration Manager (SCCM) to push an MSI installation of *Dragon Medical Client* across a network to multiple client workstations at once. SCCM provides a mechanism for pushing the *Dragon Medical Client* installation from a server to several client workstations, using a Windows Installer (MSI) file to push the installation to workstations that run a compatible Windows operating system. See *System Requirements for Dragon Medical Network Edition* on page 6 for supported operating systems.

For information about Windows Installer technology, you can download the article *Software Distribution in Configuration Manager*, available at this link: http://technet.microsoft.com/en-us/library/bb632640.aspx

Support for the Windows System Management Server

You can use the System Management Server (SMS) to push an MSI installation of *Dragon Medical Client* across a network to multiple client workstations at once. SMS provides a mechanisms for pushing the *Dragon Medical Client* installation from a server to several client workstations, using a Windows Installer (MSI) file to push the installation to workstations that run a compatible Windows operating system. See *System Requirements for Dragon Medical Network Edition* on page 6

Support for Windows Server with Active Directory Services

You can use Windows Active Directory Service to push an MSI installation of *Dragon* across a network to multiple client workstations at once.

Active Directory Services is a feature of Windows Server. The Group Policy component of Active Directory Services includes a Software Installation snap-in that lets an administrator create a network installation. Administrators can use this feature to install *Dragon Medical Client* to workstation computers that run Windows XP or Windows Vista.

Dragon supports the **Active Directory Services Assign to Computers installation** option. This option requires that you reboot the computer to complete a *Dragon Medical Client* installation.

You can delay the installation of *Dragon Medical Client* on a workstation that runs Windows Vista by enabling logon optimization for group policy. You can view a log entry for this type of installation in the event log after the client computer reboots for the first time. The *Dragon* installation application then installs *Dragon* and reboots the computer for a second time. The installation is a silent installation and does not display a GUI.

1. If necessary, create a custom MSI installation of *Dragon Medical Client* to push to several client workstations.
2. Verify that each computer meets the system requirements for *Dragon Medical Client* installation. See *System Requirements for Dragon Medical Network Edition* on page 6 for more information.
3. Push the custom MSI installation of *Dragon* to the client workstations.

Installing Dragon manually outside of the NMC console

Be sure your computer meets the system requirements for installing and running *Dragon Medical*. For additional steps you might need to take if you are upgrading, see *Preparing to upgrade non-network edition Dragon Medical Clients* on page 114.

1. Insert the installation DVD into the DVD drive of the computer. If the installation does not start on its own, browse on the DVD for the **setup.exe** file and double click it.
2. The InstallShield window might display and ask you to install software that *Dragon Medical* requires on the computer. The software might include Microsoft .NET Framework .
3. If a message displays asking you to restart your computer, restart the workstation and follow the instructions.
4. On the **Welcome** screen, click **Next**.
5. On the **License Agreement** screen, read the license agreement information. Select **I accept the terms in the license agreement** and click **Next**.
6. On the **Customer Information** screen, type your name, the name of your organization and the serial number from Nuance, then click **Next**.
7. On the **Setup Type** screen, select **Typical/Complete**. Click **Next**.
8. On the **Ready to Install the Program** page, click **Install**. The installation process begins to copy files to your computer.
9. When the wizard displays the **InstallShield Wizard Completed** screen, click **Finish**.

Now, proceed to Associating Dragon with the NMC server to associate the Dragon client with the *NMC server*.

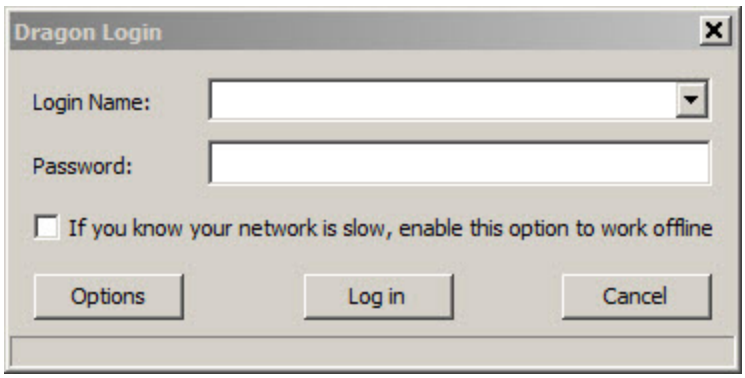
Associating Dragon with the NMC server or the Local Authenticator

After you have completed installation of the *Dragon Medical Client* on one or more workstations, you must be sure to open all required ports (see 'Ports to open for clients, servers, and hardware firewalls' in the Planning guide) and then let the client know the name of the particular *NMC server* to communicate with.

Associating Dragon with an NMC server or Local Authenticator

Once the appropriate ports are open (see 'Ports to open for clients, servers, and hardware firewalls' in the Planning guide), when a healthcare provider logs in to the client, that provider indicates the particular machine where the server is running:

1. When the healthcare provider logs in to the *Dragon Medical Client*, first the splash screen displays.
2. When the **Dragon Login** dialog box appears, the provider should click the **Options** button:



3. When the **Options** dialog box appears, the provider must then enter the name of the machine that houses the *NMC server* or Local Authenticator:
   For information on using the check boxes in this dialog box, refer to the *Dragon Medical Client* Help. If you have a network traffic switch managing multiple *NMC servers*, see *Ensuring clients can contact an NMC server with a load balancing traffic switch in the network* at the end of this section for more information on what to enter for the address.
4. The provider then logs in using the user account that an **NMC Administrator** has created in the *NMC server*.

5. If this is the very first time the provider has ever logged in to the *Dragon Medical Client* (the user has no previously existing profile of his or her voice), the **New User Wizard** appears. The **New User Wizard** does not appear if the provider has a user profile you upgraded from an earlier version of *Dragon Medical*.
6. The provider should click the check box indicating **I have read and agree to the License Agreement** and proceed through the **New User Wizard** as instructed.
7. When the provider finishes completing every page of the wizard, the **DragonBar** then becomes available, and the provider can begin dictating.

Ensuring clients can contact an NMC server with a load balancing traffic switch in the network

When you install clients using a push installation, if you have a load balancing traffic switch managing multiple *NMC servers* on your network, you should set **NAS_ADDRESS** to the address of the traffic switch, rather than the address of any particular *NMC server*.

Note: If the user already entered a value for this option, your value will overwrite that.

When providers first log in to *Dragon Medical Client*, when they click the **Advanced** button, instead of entering the IP address or name of an *NMC server*, they should enter the IP address or name of the ***traffic switch appliance*** in the **Address** text box of the **Server Location** dialog box.

If your workstations have desktop shortcuts for *Dragon Medical Client*, those shortcuts should also point to the traffic switch's address, rather than the address of any particular *NMC server*.

For more information on using the *Dragon Medical Client*, refer to the *Dragon* Help.

Pushing the Dragon MSI installation to workstations

An overview of the options for installing multiple *Dragon Medical Client* workstations at once is provided below.

The Dragon Medical Network Edition DVD includes a Microsoft Windows Installer (MSI) file. You can use this MSI file to install *Dragon* from a server to client workstations across a network or to install several client workstations at once using either an SMS or SCCM installation or an ActiveDirectory Services installation.

Caution: Whenever you carry out an MSI installation of DM Network Edition, Nuance recommends that you uninstall any *Dragon Medical* software already on the machine before it proceeds to install the new client software. You can do this via the MSI installer using the **/x**<*Product.msi*> command, where <*Product.msi*> is the name of the .msi file of the version of DM Network Edition that you are uninstalling. For more information on command line options you can use to install Dragon, refer to *Understanding Dragon MSI command line options* on page 143.

Note:

When you create an MSI installer for the *Dragon Medical Client* included with the *NMC server*, you are not required to have the installer set any user or administrative options that you would prefer to set in the *NMC server* later.

DVD name	MSI file name
Dragon Medical Enterprise Network Edition Client Software DVD	Dragon NaturallySpeaking 12.msi
NMC server Software and Documentation DVD	Dragon SDK Client Edition 12.msi

The command line you use to install *Dragon* using the **.MSI** file is:

```
msiexec.exe /i "Dragon NaturallySpeaking 12.msi"
```

- General options for installing *Dragon*
- MSI options for installing *Dragon* features/advanced options
- Feature variables to set through the ADDLOCAL or ADVERTISE properties

Options for pushing MSI installation of Dragon to one or more workstations on a network

You can use a server application to push an MSI installation of *Dragon* to client workstations without having to install *Dragon* separately on each computer. The server administrator creates an image of the *Dragon* installation program. The administrator then places the image on a server and configures the server to automatically push the application to client workstations.

There are several server applications that you can use to push a *Dragon* installation. See *System Requirements for Dragon Medical Network Edition* on page 6 for supported versions:

- Windows Server
- System Center Configuration Manager (SCCM)
- Active Directory Services

Support for the Windows System Center Configuration Manager

You can use the System Center Configuration Manager (SCCM) to push an MSI installation of *Dragon Medical Client* across a network to multiple client workstations at once. SCCM provides a mechanism for pushing the *Dragon Medical Client* installation from a server to several client workstations, using a Windows Installer (MSI) file to push the installation to workstations that run a compatible Windows operating system. See *System Requirements for Dragon Medical Network Edition* on page 6 for supported operating systems.

For information about Windows Installer technology, you can download the article *Software Distribution in Configuration Manager*, available at this link: http://technet.microsoft.com/en-us/library/bb632640.aspx

Support for the Windows System Management Server

You can use the System Management Server (SMS) to push an MSI installation of *Dragon Medical Client* across a network to multiple client workstations at once. SMS provides a mechanisms for pushing the *Dragon Medical Client* installation from a server to several client workstations, using a Windows Installer (MSI) file to push the installation to workstations that run a compatible Windows operating system. See *System Requirements for Dragon Medical Network Edition* on page 6

Support for Windows Server with Active Directory Services

You can use Windows Active Directory Service to push an MSI installation of *Dragon* across a network to multiple client workstations at once.

Active Directory Services is a feature of Windows Server. The Group Policy component of Active Directory Services includes a Software Installation snap-in that lets an administrator create a network installation. Administrators can use this feature to install *Dragon Medical Client* to workstation computers that run Windows XP or Windows Vista.

Dragon supports the **Active Directory Services Assign to Computers installation** option. This option requires that you reboot the computer to complete a *Dragon Medical Client* installation.

You can delay the installation of *Dragon Medical Client* on a workstation that runs Windows Vista by enabling logon optimization for group policy. You can view a log entry for this type of installation in the event log after the client computer reboots for the first time. The *Dragon* installation application then installs *Dragon* and reboots the computer for a second time. The installation is a silent installation and does not display a GUI.

1. If necessary, create a custom MSI installation of *Dragon Medical Client* to push to several client workstations.
2. Verify that each computer meets the system requirements for *Dragon Medical Client* installation. See *System Requirements for Dragon Medical Network Edition* on page 6 for more information.
3. Push the custom MSI installation of *Dragon* to the client workstations.

Understanding Dragon MSI command line options

Modifying the admininstall.bat file

To make changes to the **admininstall.bat** file, you can use any of the following options.

Note: Be sure that the values that you pass in to the MSI are valid. Entering an invalid value can cause the installer to crash.

General options for installing Dragon

Options	Description
USE_VSYNC_FOR_ CITRIX_BASIC_ DICTATION=0 (or 1)	Enable Dragon to insert text into published applications through vSync. Text insertion through vSync is available when Dragon switches to Basic dictation mode during a timeout that occurs when dictating text. **Prerequisites for enabling text insertion through vSync** • vSync is enabled and running on a Citrix XenApp server. • The Dragon client is updated to build DM Network Edition 2.4.4 or higher. • vSync is updated to build 2.4.4 or higher. • The Dragon user is dictating into a published application window supported by vSync. • The user dictates at least once into the application. **Steps for enabling text insertion through vSync** On the Dragon workstation, upgrade the Dragon client. 1. Open a command prompt with administrative privileges. 2. Ensure that the C:\temp directory exists. If the directory does not exist, create it. 3. Run the following command: setup.exe /v"USE_VSYNC_FOR_CITRIX_ BASIC_DICTATION=1 /Liwmo!e C:\temp\setup.log" **Text insertion through vSync is not available when**: • Dictating into an edit control or window that is not supported by vSync. • Using voice or keyboard commands such as "Copy x" and "Paste y". • Inserting Text & Graphics commands and templates. • Transferring text from the Dictation Box. • vSync is not enabled. • The 'Insertion through vSync' feature is disabled. Notes: • By default, this feature is disabled (Set to 0). • To enable text insertion through vSync, set USE_VSYNC_FOR_CITRIX_ BASIC_DICTATION to 1. • To disable text insertion through vSync, set USE_VSYNC_FOR_CITRIX_ BASIC_DICTATION to 0.
SERIALNUMBER=abcde-fgh-ijkl-mnop-qr	The serial number for the *Dragon* product. All *Dragon* installations require that you provide a serial (license) number for the product. The *Dragon*

	installation process checks for a serial number even if you run the process from a command line.
NAS_ADDRESS="DNS|<IP_address>"	Indicates the IP address of the *NMC server* that the *Dragon Medical Client* connects to when the healthcare provider logs on. If you set this option during the installation, then the provider does not need to enter the server machine name when logging in to *Dragon Medical Client* for the first time. If you do not set this option during the installation, each provider should click the **Advanced** button when logging in to the client for the first time and enter either the IP address or the machine name (with no prefix for instance, no **www** or **http://**) in the **Server Location** text box. If your network has multiple *NMC servers* being managed by a load balancing traffic switch in the network, you should set this option to the address of the switch rather than the address of any particular *NMC server*. **Note:** *If you define this option when installing an upgrade to* Dragon Medical Network Edition, version 2.7*, you will overwrite any value the user already entered.*
NAS_LDAP_SIGN_ON=0 (or 1 or 2)	**Note:** Before you enable LDAP, you must make additional configuration changes in order for the feature to work. See the "DM Network Edition Administrator Guide" *Configuring LDAP* section for more information. Set the option to **0** to disable LDAP login. Set the option to **1** to enable LDAP login for a single domain LDAP. In this case, Dragon retrieves the domain name from the user's workstation. Set the option to **2** to enable LDAP login for multiple domains. In this case, the user must supply credentials in the "domain name\user name" format. The default value is **0**. Be sure that the value you set here is the same as the type of LDAP that is enabled in the NMC server. See the "DM Network Edition Administrator Guide" *Configuring LDAP* section for more information. **Note:***If you define this option when installing an upgrade to* Dragon Medical Network Edition, version 2.7*, you will overwrite any value the user already entered.*
NAS_SINGLE_SIGN_ON=0 (or 1)	**Note:** Before you enable EHR single sign on, you must make additional configuration changes in order for the feature to work. See the "DM Network Edition Administrator Guide" *Implementing EHR Single Sign-On* section for more information. Set the option to **0** to disable single sign on from an EHR. Set the option to **1** to enable single sign on from an EHR. The default value is **0**. Be sure that the value you set here —enabled or disabled—that is set in the NMC console. See the "DM Network Edition Administrator Guide" *Implementing EHR Single Sign-On* section for more information. **Note:** *If you define this option when installing an upgrade to* Dragon Medical Network Edition, version 2.7*, you will overwrite any value the user already entered.*

MSI options for installing Dragon features/advanced options

Options	Description
ADDLOCAL=Feature1,Feature2,... or ADDLOCAL=ALL	Set the ADDLOCAL option to a comma delimited list of features to install locally. To install all features locally (including speech files), set the ADDLOCAL option to **ALL**. See General Options for Installing Dragon for a list of the features that you can make available or install locally using the ADDLOCAL option or the ADVERTISE option.
ADVERTISE-E=Feature1,Feature2,Feature3,...	Set the ADVERTISE option to a comma delimited list of features to make available but not install locally. To install all features as advertised, set the ADVERTISE option to **ALL**. The ADVERTISE option overrides the ADDLOCAL option. The best method for installing a particular set of features is to set the ADDLOCAL option to **ALL** and then set the ADVERTISE option to the features you do not want to install locally. See General Options for Installing Dragon for a list of the features that you can make available or install locally using the ADDLOCAL option or the ADVERTISE option.
REINSTALL=Feature1,Feature2,... (or ALL)	Set the REINSTALL option to a comma delimited list of features to reinstall. To reinstall all features, set the REINSTALL option to **ALL**. If you set the REINSTALL option, you should also set the REINSTALLMODE option to set the type of reinstall to perform. If you do not set the REINSTALLMODE option, the installation process only reinstalls a file if it is an earlier version of the file that is presently installed or if the a file is not present on the system. By default, no registry entries are rewritten. Even if you set the REINSTALL option to **ALL**, the installation process only reinstalls features that are already installed. Thus, if you use the REINSTALL option for a product that is not yet to installed, product installation does not occur. For more information, see: http://msdn.microsoft.com/en-us/library/windows/desktop/aa371175
REINSTALLMODE={type of reinstallation to perform}	Set the REINSTALLMODE option to a string that indicates the type of reinstall to perform. Options are case-insensitive and order-independent. You should use this option when you use the REINSTALL option. You can also use this option during an installation of *Dragon Medical Client*, not just during a reinstallation.

<table>
<tr><td></td><td>
<table>
<tr><th>Opt</th><th>Purpose</th></tr>
<tr><td>p</td><td>Only reinstall a file if the file is missing.</td></tr>
<tr><td>o</td><td>Only reinstall a file if the file is missing or is an older version.</td></tr>
<tr><td>e</td><td>Only reinstall a file if the file is missing or is an equal or older version.</td></tr>
<tr><td>d</td><td>Only reinstall a file if the file is missing or a different version is present.</td></tr>
<tr><td>c</td><td>Only reinstall a file or files whose checksums are missing or corrupt.</td></tr>
<tr><td>a</td><td>Force a reinstall of all files, regardless of checksum or version.</td></tr>
<tr><td>u</td><td>Rewrite all required registry entries from the Registry Table that go under HKEY_CURRENT_USER or HKEY_USERS.</td></tr>
<tr><td>m</td><td>Rewrite all required registry entries from the Registry Table that go under HKEY_LOCAL_MACHINE or HKEY_CLASSES_ROOT. Regardless of machine or user assignment.

Rewrite all data from the following tables: Class, Verb, PublishComponent, ProgID, MIME, Icon, Extension, and AppID .

Reinstall all qualified components. When reinstalling an application, run the RegisterTypeLibraries and InstallODBC actions.</td></tr>
<tr><td>s</td><td>Reinstall all shortcuts and re-cache all icons, overwriting existing shortcuts and icons.</td></tr>
<tr><td>v</td><td>Run from the source package, re-cache the local package. Does not apply to a new installation of a product or feature.</td></tr>
</table>
</td></tr>
<tr><td>REMOVEOLDPROD=1</td><td>Set the REMOVEOLDPROD option to remove an older version of Dragon before installing the newer version. You should only use this option for major upgrades.</td></tr>
<tr><td>/x<Product.msi|ProductCode></td><td>Set the installation process to uninstall the current installed version of Dragon. You must perform this action during an upgrade. However, you should be familiar with the entire upgrade procedure before you use this option.</td></tr>
</table>

Feature variables to set through the ADDLOCAL or ADVERTISE properties

Feature/Sub-feature	Sub-feature
NatSpeak ***Note:*** *Required in ADDLOCAL; if not included, installation fails*	None

Samples *(Sample Commands files)*	None	
TTS *(Text-to-Speech)*	TTSENU *(US English Text-to-Speech)* TTSENG (*British English Text-to-Speech*)	
Tutorial	TutENX *(English Tutorial)*	
Speech ENX *(English)* /ENU *(US English)*	**Dragon NaturallySpeaking and Dragon Medical:Sub-features for ENU (US English):** ENULegal *(US English Legal Large)* ENUGeneral *(US English General Medium, US English Empty Dictation, US English Commands Only)* ENUGenSvc *(US English Large General)*	**Note:** The ENU sub-feature includes support for the following accents: General: Use if your accent is not covered by the another choice or you are not sure which to select. Australian accented English British accented English Indian accented English Inland Northern US (Great Lakes area): Covers Upstate New York through the Chicago area. SEAsian accented English: South East Asian Southern US: Covers most of the Southern United States, including Texas. Spanish Accented English
Speech ENX *(English)* /ENU *(US English)* (continued)	**Dragon Medical Only Sub-features for ENU (US English):** ENUCardiology *(US English Medical Large Cardiology, Pediatric Cardiology)* ENUEmergency *(US English Emergency Medicine Large)* ENUGastroenterology *(US English Medical Large Gastroenterology, Pediatric Gastroenterology)* ENUGeneralPractice *(US English Large Family Medicine, Allergy and Immunology, Dermatology, Epidemiology, Geriatric, Hematology, Infectious Disease, Internal Medicine, Medical Education and Writing, Nephrology, Nursing, Osteopathy, Pulmonary Disease, Rheumatology, Sleep Lab)* ENUMedical *(US English General Medical Large No Specialty)* ENUMentalHealth *(US English*	ENUObGyn *(US English Medical Large ENT, Fetal Medicine, Midwifery, Obstetrics and Gynecology, Ophthalmology)* ENUOncology *(US English Medical Large Oncology, Radiation Therapy)* ENUOrthopaedic *(US English Medical Large Dentistry, Large Hand Surgery, Neurosurgery, Orthopaedics, Oral and Facial Surgery, Orthopaedic Surgery, Plastic Surgery, Podiatry)* ENUPathology *(US English Medical Large Pathology)* ENUPediatrics *(US English Medical Large Pediatrics, Neonatal and Perinatal Medicine, Pediatric Dentistry)* ENURadiology *(US English Medical Large Nuclear Medicine or Radiology)* ENURehabilitation (*Neurology, Physical Medicine, Rehabilitation and Speech and Language Pathology*)

	Large Medical Addiction Psychiatry; Endocrinology, Diabetes, and Metabolism; Psychiatry, Psychology) ENGNeurology *(US English Anesthesiology, Neurology, Pain Medicine, Physical Medicine and Rehabilitation, Vascular and Interventional Radiology)*	ENUSurgery *(US English Medical Large Cardiac Surgery, Colon and Rectal Surgery, Surgery, Thoracic Surgery, Urology, Vascular Surgery)*

Creating a custom installer for the client in Active Directory

If you are installing Dragon on a network using Active Directory Services, you can create a custom installation program using a set of tools available from Microsoft.

- Download and install the tools
- Run the wizard

You are then ready to use the custom installer to install the *Dragon Medical Client* from Active Directory Services.

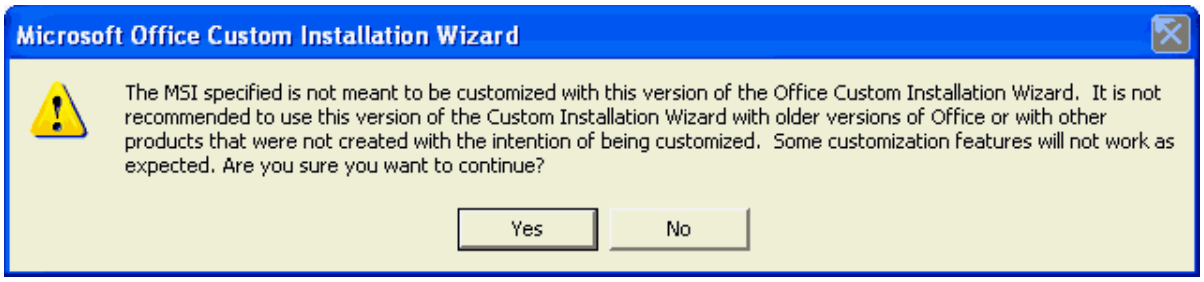
Modifying setup Properties for Custom Installation

The following explains how to modify setup properties for a custom installation of *Dragon Medical Client*. This example shows how to add to the installer configuration one of the many MSI options you can set for installing *Dragon Medical Client*, the SERIALNUMBER property. (You can add any options available to MSI on the command line.)

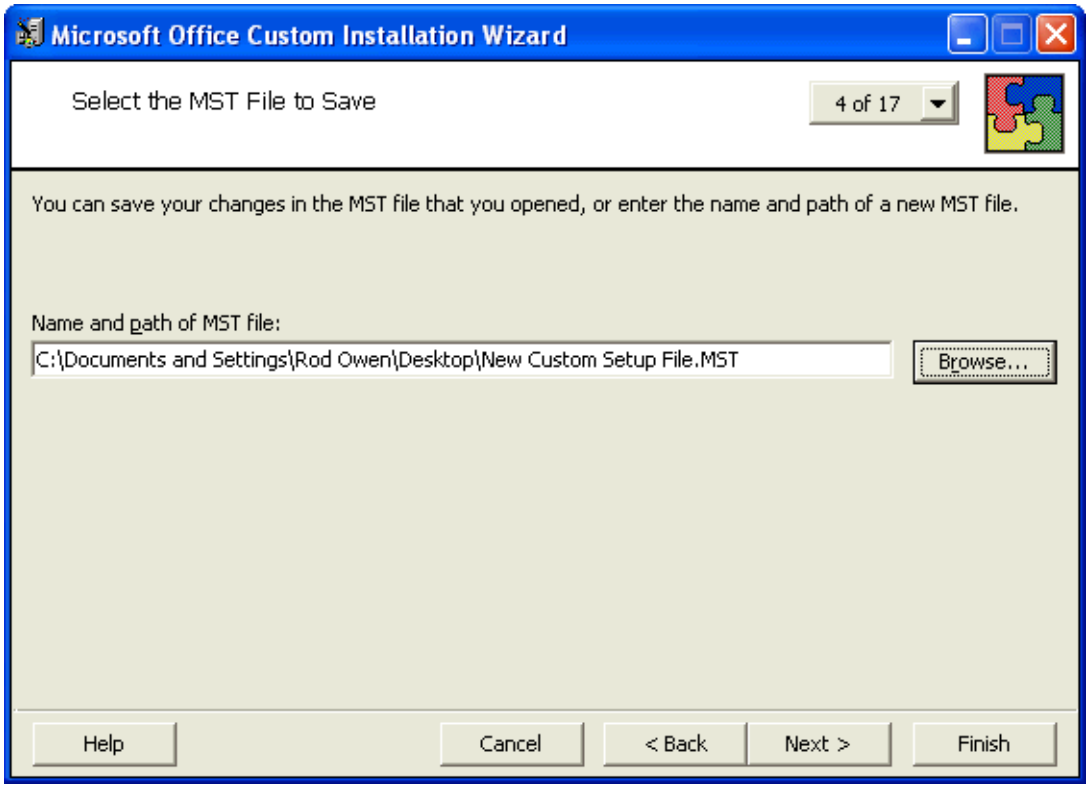
1. Start the Microsoft Custom Installation Wizard by choosing **Start > Programs > Microsoft Office Tools > Microsoft Office XP Resource Kit Tools**, and then click **Custom Installation Wizard**. The **Custom Installation Wizard** screen displays:

2. Click **Next**.
3. On the Open the MSI File page of the wizard, shown below, select the .MSI file you want to use to create a custom installation. The compiled .MSI file is located on your installation CD. The file you should select is named *Dragon Medical*: **Dragon NaturallySpeaking 12.msi**.
4. Click **Next**.

5. Click **Yes** when you see the following message:



6. On the **Open the MST File** page of the wizard, select **Create a new MST file**.
7. Click **Next** to continue.
8. On the **Select MST File to Save** page of the wizard, select a file name and path for the MST file you are creating:



9. Click **Next**.

10. On the **Specify a Default Path and Organization** page, select the default path for the installation. By default, *Dragon Medical Client* installs in:

    On a 32 Bit machine:

    `\Program Files\Nuance\NaturallySpeaking12.`

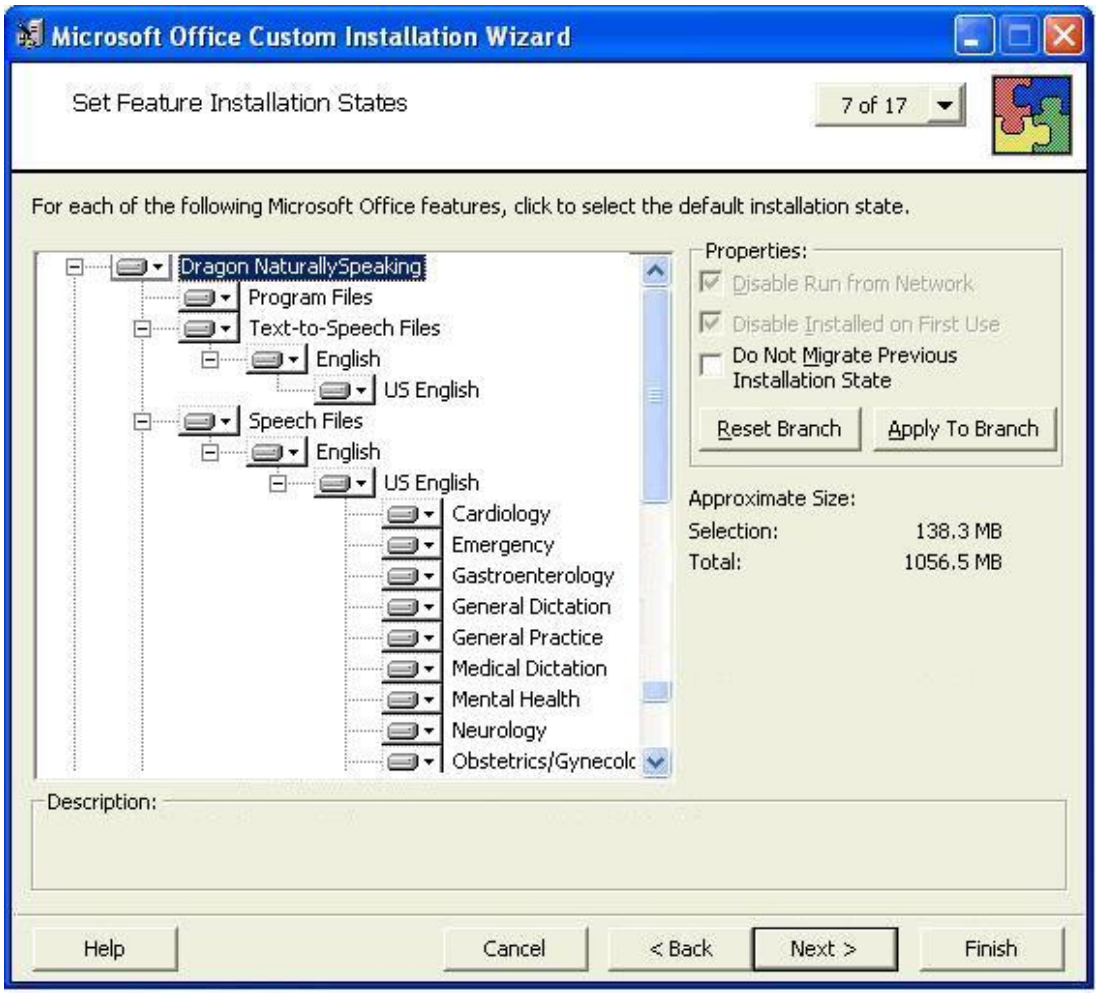
    On a 64 Bit machine:

    `\Program Files (x86)\Nuance\NaturallySpeaking12.`

11. Click **Next**.

12. On the **Remove Previous Versions** page, keep the default selections and click **Next**. This page applies only to Microsoft Office and does not affect the *Dragon Medical Client* installation.

13. Click **Next** to keep all the defaults when you come to **the Set Features Installation States** page, where you select particular components to install. The illustration here shows some of the Medical vocabularies you might choose:



14. On the next several pages of the wizard, click **Next** on each, and proceed until you reach the **Modify Setup Properties** page. All the pages in between apply only to Microsoft Office or do not affect the *Dragon Medical Client* installation.

    Customize Default Application Settings page

    Change Office User Settings page

    Add/Remove Files page

    Add/Remove Registry Entries page

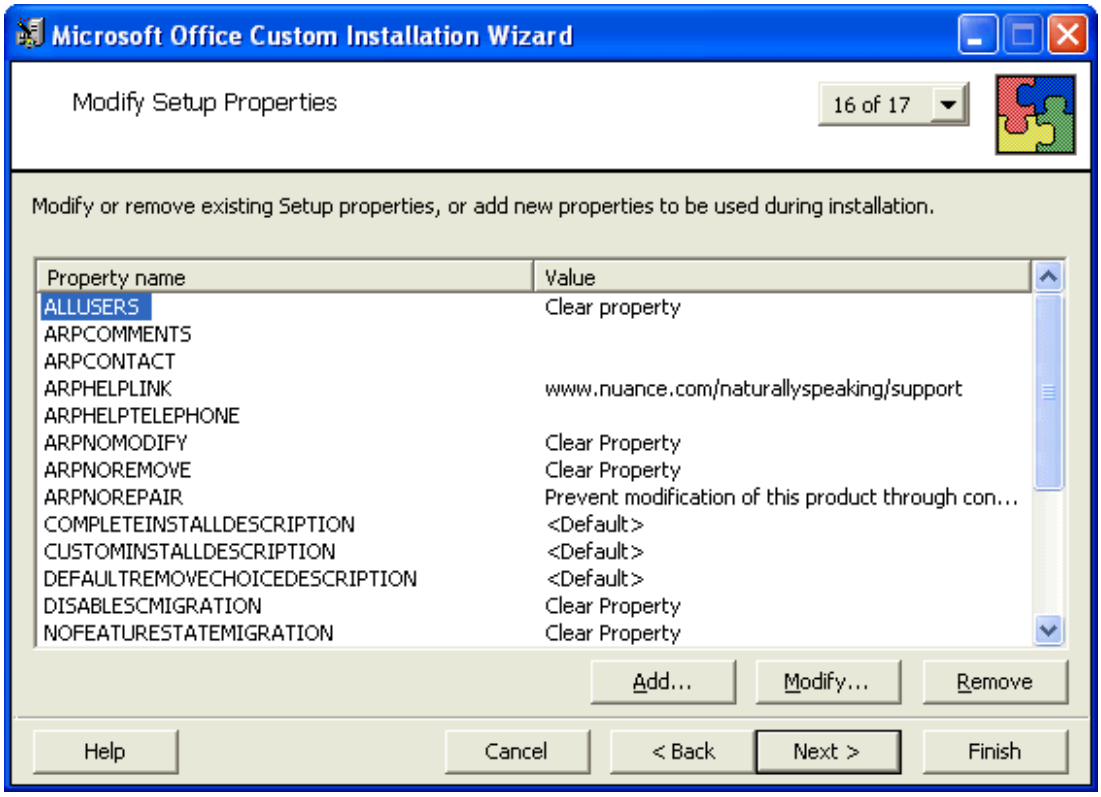
    Add, Modify, or Remove Shortcuts page

    Identify Additional Servers page

    Specify Office Security Settings page

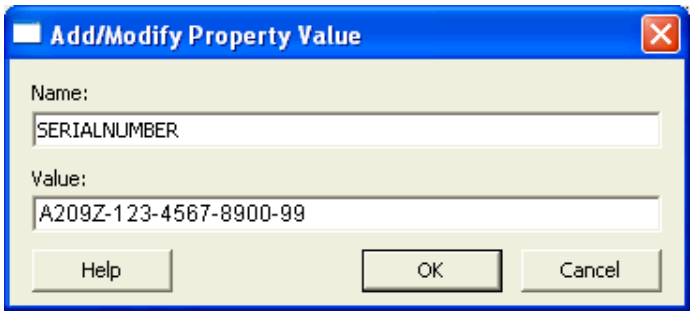
    Add Installations and Run Programs page

15. Use the **Modify Setup Properties** page, shown below, to add, modify, and set the MSI options of your custom installation.

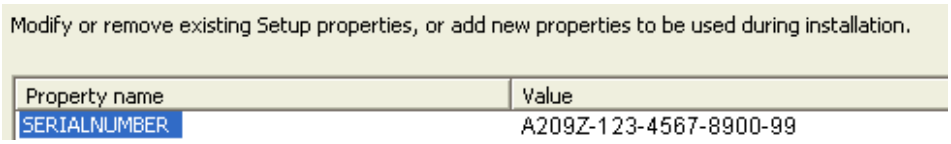


16. Click the **Add...** button to display the **Add/Modify Property Value** dialog box, where you modify the MSI installation options. In this example, we add and set the SERIALNUMBER option.

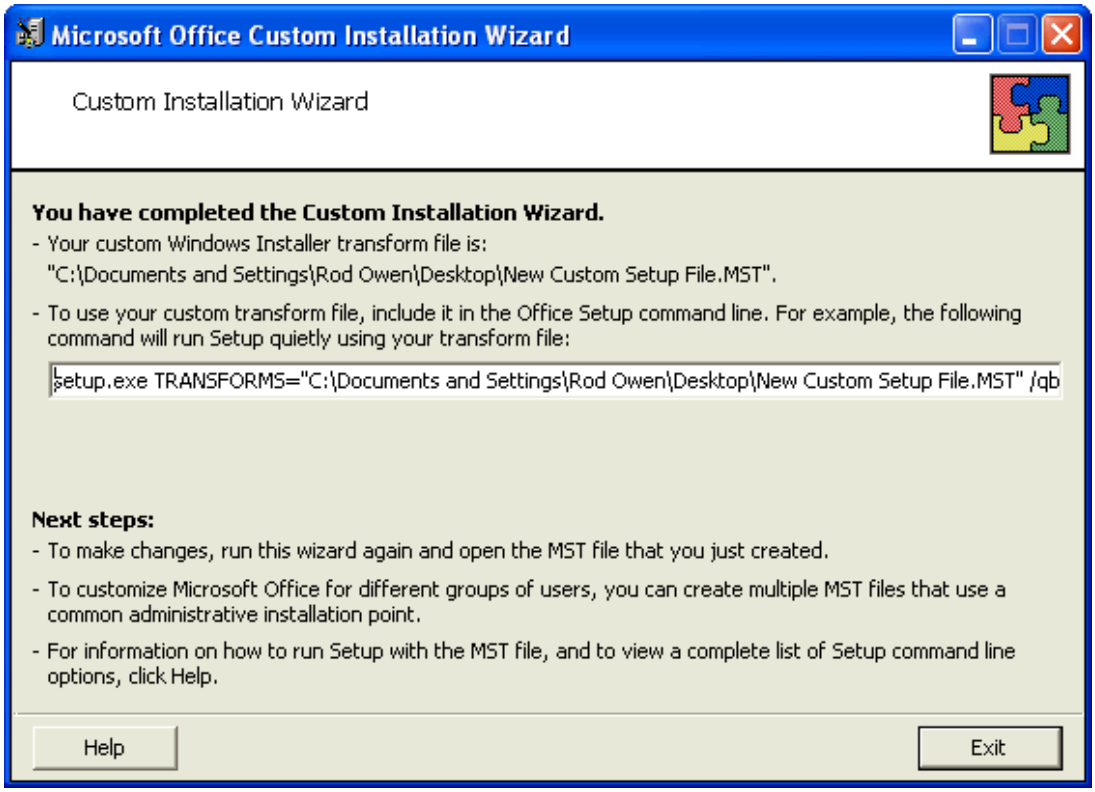
17. In the following **Add/Modify Property Value** page, enter the new property name SERIALNUMBER and a valid serial number, then click **OK**:



18. Note that the **Modify Setup Properties** page re-displays with the updated information. For example:



19. Continue adding or modifying other MSI options that apply for your environment. Once you are done, click **Next**.
20. On the **Save Changes** page, click **Finish**.
21. When the **Custom Installation Wizard** page appears, click **Exit**. This screen displays the location of *Windows Installer transform* (.MST file) that you created.



After you save changes, you can use the resulting .MST file to manage an installation through a Group Policy in Active Directory Services.

You are now ready to use the custom installer you created to install the product.

Command line interface

You can use command line options to modify the way in which Dragon starts up. These switches are used in the following syntax:

natspeak */switch*

Where */switch* is the switch from the following table:

Switch	Function
/diagnose	Runs Dragon in diagnostic mode. Outputs information into the Dragon.log file and exits.
/FindCustom	Brings up the custom directory
/finddragonlog	Brings up a Windows Explorer window with the dragon.log high-lighted
/findsetuplog	Brings up a Windows Explorer window with the dgnsetup.log high-lighted
/findappdataallusers	Brings up a Windows Explorer window in our "all users" application data directory (nssystem.ini, nsapps.ini, models.ini, Users\ dir-ectory, etc.)
/findappdata	Brings up a Windows Explorer window in our "this user" application data directory (dragon.log, upgrade.log, nsuser.ini, etc.)
/findupgradelog	Brings up a Windows Explorer window with the upgrade.log high-lighted
/user <*username*> <*password*>	Automatically loads the user profile for the user with the specified username and password.
/ssouser <*EHR username*> <*cli-entID*>	Automatically logs in to the Dragon Medical Client with the specified user account. The switch expects you to supply the EHR username and a Client ID. You must have set up EHR single-sign-on using the NMC console in order for this flag to work. See the Dragon Medical Network Edition Administrator Guide for more information.
/trusted	Automatically logs in to the Dragon Medical Client with the user account of the logged in Windows user (also known as Active Directory Single Sign-On). The user account must be set up in Active Directory and have a cor-responding user account in the NMC server. See the Administrator Guide for more information. The `/trusted` command line option works on the server as well as the client.
/trustedOffline	Use this option to perform a trusted login in offline mode. Example command line instruction: `/natspeak.exe /trustedOffline`
/trustedDeleteCache	Use this option to perform a trusted login and delete the local cache.

	Example command line instruction: `/natspeak.exe /trustedDeleteCache`
/trustedDeleteProfile	Use this option to perform a trusted login and delete a user's profile. Example command line instruction: `/natspeak.exe /trustedDeleteProfile`
/logout	Logs the current user out. If a user is logging out of Dragon, any command line `/login` request received during that log out goes into a queue and is executed once the log out is complete.
/save	Saves the current user's profile. You can specify a time out value for the `/save` command with `natspeak.exe` and `natspeaksso.exe`. If you call `natspeak.exe /save <timeout>` using a script, the script will not continue processing until the `save` command is completed, or the timeout value elapses, whichever comes first. Valid values for the timeout parameter are between 30 and 120 seconds and use the following syntax: `natspeak.exe /save <timeout>` where `<timeout>` is the time out in seconds. The default timeout—which Dragon uses when given a value less than 30 or greater than 120—is 60 seconds. If you supply a non-numeric value or a value of zero, the time out feature is disabled for the current run.
/shutdown	Closes Dragon without saving user profile changes. This command works even if the Automatically save user files on close option is enabled in the Dragon Client.
/saveandshutdown	Closes Dragon after saving user profile changes. This command works even if the Automatically save user files on close option is disabled in the Dragon Client. You can specify a time out value for the `/saveandshutdown` commands with `natspeak.exe` and `natspeaksso.exe`. If you call `natspeaksso.exe /saveandshutdown <timeout>` using a script, the script will not continue processing until the `save` command is completed, or the timeout value elapses, whichever comes first. Valid values for the timeout parameter are between 30 and 120 seconds and use the following syntax: `natspeak.exe /saveandshutdown <timeout>` where `<timeout>` is the time out in seconds. The default timeout—which Dragon uses when given a value less than 30 or greater than 120—is 60 seconds. If you supply a non-numeric value or a value of zero, the time out feature is disabled for the current run.
/topic <*topic*>	Automatically loads the topic specified by <*topic*> *(Professional edition only)*

/quick	Runs Dragon in quick mode. QuickStart mode starts Dragon without loading a user profile or any speech models when you start your computer. Only the Dragon tray icon is visible. When you click on the Dragon desktop icon, the Open Profile dialog box immediately appears. When you exit Dragon the program returns to the QuickStart mode and remains in memory with a reduced footprint (approximately 10 MB).
/SetDefaultOptions	Displays the Options dialog box at the end of the installation. The Options dialog box lets you change Dragon's standard behavior, including specifying hot keys, customizing how text is formatted, initial microphone settings.
/SetDefaultAdministrativeOptions	Displays the Administrative settings dialog box at the end of the installation.
/SetDefaultFormattingOptions	Brings up the default Auto-Formatting options dialog

Ensuring Dragon Medical Client anti-virus recommendations are met

Nuance recommends anti-virus software on all DM Network Edition servers and clients to protect the system from potential downtime due to viruses. However, on *Dragon Medical Clients*, be sure to exclude from the anti-virus scan any files found in the folders indicated below or with the extensions listed below (on Windows workstations):

- **C:\ProgramData\Nuance** folder and all sub-folders
- **C:\users\<windows user_ID>\Appdata\Roaming\Nuance** folder and all sub-folders
- **C:\Users\All Users\Application Data\Nuance** folder and all sub-folders
- **C:\Users***Windows user_ID***\Local Settings\Temp** folder
- Files with these extensions: **BD, BIN, DAT, DVC, ENH, GSB, GRM, GRX, INI, LCK, NWV, SIG, SVC, USR, VER, VOC, WAV, XML, LOG**

Assigning access to folders and master user profiles across the network

Caution:

To ensure that your *Dragon Medical Clients* can communicate with the master user profiles server and the other servers, you must assign correct permissions to all appropriate directories and access rights to particular keys in the registry, as indicated in the tables in *Assigning access to servers, clients, and master user profiles across network* on page 1. Do not skip this step, as it is important!

Turning off Automatic Updates

On each machine you plan to use in the network, be sure to turn off Windows Automatic Updates. You should, instead, qualify each update Windows sends by installing it first on a single test machine of the network and then updating other machines on the network only after you determine that it clearly will not disrupt the network.

Once you are sure an update does not have any negative effects, you should install the update during off-hours and, if required, reboot each machine during those hours to ensure that requests to reboot do not disrupt the servers or workstations during peak hours of dictation.

Chapter 9: Moving Databases

Moving NMC server SQL database

To move the *NMC server SQL Database*, you first move it to the new location, then test the new database to be sure it is operational. Finally, you remove the database from the original location.

Moving the database to a new location

To move the *NMC server SQL Database*, take these steps:

1. Back up the *NMC server SQL Database* and then close all network connections.
2. Remove the *NMC server SQL Database* from the existing server. This step exports a copy of the database but does not remove it from the original server. For more details, see the SQL Server dump/export documentation from Microsoft.
3. Install the SQL Server software on the new physical server.
4. Restore the database on the new server. For more details, see the SQL Server restore documentation from Microsoft.
5. Uninstall the *NMC server* following the steps in *Moving NMC server SQL database* on page 161. The old database remains intact.
6. Reopen all network connections.
7. Reinstall the *NMC server* to its original location, being sure to give the new location of the database when you are prompted for it during the installation process.
8. Once you are sure that the new database is operational, remove the old database from the original server (see steps below).

Removing the old database from the original location

To remove the old *NMC server SQL Database*, take these steps:

1. Close all network connections on the original database server.
2. Click **Start** > **Programs** and look for **SQL Server Management Studio**.
3. When the **Microsoft SQL Server Management Studio** dialog box appears, expand **Databases** in the Object Explorer (to the left) and find the database named **NuanceMC**. That is

your *NMC server* database.

4. Right click on **NuanceMC** and select **Delete** from the drop-down menu.

Chapter 10: Setting up Active Directory Services

Setting up the NMC server to run Active Directory Services

You can use ActiveDirectory Services to manage your DM Network Edition network. Ideally, you should decide to use Active Directory Services before you install the DM Network Edition network. Enabling Active Directory Services requires specific steps during the DM Network Edition installation process. However, you can enable Active Directory Services before or after you have installed the DM Network Edition network.

Enabling Active Directory Services

1. Install SQL Server 2008 , 2012, or 2016.
2. Creating NMC console Administrator Account in NMC server for Active Directory Administrator: After you install the *NMC server*:
   - Log in to *NMC server* using the admin login Nuance provides.
   - Prepare to create user accounts by changing the name of the organization/site Nuance provides to match your organization and site.
   - Create a **NMC console Administrator** user account for the Active Directory administrator.
   - If you would like, create all other user accounts now; or you can create user accounts later.
   - **Create Active Directory Single Sign-On User Accounts:** If you want to set providers up to log in only once, you can set up Active Directory Single Sign-On user accounts (they are optional); see *Creating Single Sign-On user accounts* on page 1. You need to create these accounts before you can associate a user account with an already existing upgraded master user profile.
3. Continue to configure the NMC server as Active Directory Administrator
   - Follow instructions in NMC server Administrator Guide.

Creating an NMC Administrator account for Active Directory

To create the **NMC Administrator** account for the Active Directory administrator:

1. Install the *NMC server* following the instructions in this manual.
2. Log in to the *NMC server* through the *NMC console*.
3. To prepare to set up user accounts required for Active Directory in *NMC server*, you need to first:
   - Change the name of the default organization to your organization's name. See details on modifying the organization information in the *NMC server Administrator Guide* under *Accessing and adding to your organization data.*
   - Change the name of the default site in that organization to your site's name. See details on how to create a site in the *NMC server Administrator Guide* under *Configuring sites in DM Network Edition*
4. Create an **NMC Administrator** user account for the Active Directory administrator to use when logging in to the *NMC server*. Make sure the login you assign in *NMC server* matches an existing login in Active Directory.
5. Assign an **NMC Administrator** license to the new account for the Active Directory administrator.
6. You can create other user accounts at this time, but if you are not ready to create them, you can create them later, as long as every *NMC server* user account login you assign matches an existing login in Active Directory.
7. Proceed to the next subsection.

Restarting the Nuance Management Service

1. Restart the *NMC server* by restarting the service: In the **Control Panel,** double click **Administrative Tools**. Then double click **Services**. In the **Services** window, find the **Nuance Management Service** and restart it.
2. Log in to the *NMC server* using the new **NMC administrator** user account you created for the Active Directory administrator.
3. Revoke the **NMC administrator** license of the original **admin** user account that Nuance provided, since that account does not work within Active Directory. You might want to grant that license to another user account.

4. If you would like dictating healthcare providers to be able to log in to Windows and then automatically be logged in to the *Dragon Medical Client* on the same workstation without having to enter separate login credentials for *Dragon*, see *Creating Single Sign-On user accounts* on page 1.
5. To continue to configure the *NMC server* as Active Directory administrator account by following the remaining instructions in this book.

Index

R

S

U

W