



Installation Guide

2.5.1



Copyright

2016 Dragon Medical Network Edition, 2.5.1.

To view and download the latest version of this document, visit:

<http://www.nuance.com/for-healthcare/dragon-medical-360/user-guides/index.htm>

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

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

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

Copyright © 2002-2016 Nuance Communications, Inc. All rights reserved.

Nuance, ScanSoft, the Nuance logo, the Dragon logo, Dragon, DragonBar, NaturallySpeaking, NaturallyMobile, RealSpeak, Nothing But Speech (NBS), Natural Language Technology, Select-and-Say, MouseGrid, and Vocabulary Editor are registered trademarks or trademarks of Nuance Communications, Inc. in the United States or other countries. All other names and trademarks referenced herein are trademarks of Nuance Communications or their respective owners. Designations used by third-party manufacturers and sellers to distinguish their products may be claimed as trademarks by those third-parties.

Disclaimer

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

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

Notice

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

Nuance believes that data security is best maintained by limiting access to various types of information to authorized users only. Although no software product can completely guarantee against security failure, Dragon 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-3867

Contents

Disclaimer	ii
Notice	ii
Document Versions	x
Introduction to installing Dragon Medical Network Edition	1
What's new in Dragon Medical Network Edition	2
What's new in Dragon Medical Network Edition, 2.5.1	2
Installing or Upgrading an On-Premise Installation vs a Cloud Based Installation	3
Installing an On-Premise System	3
Upgrading an On-Premise System	3
Installing a Cloud Based System	3
Upgrading a Cloud Based System	3
Chapter 1: Preparing to install Dragon Medical Network Edition	5
System Requirements for Dragon Medical Network Edition	7
Hardware Recommendations	7
Software Requirements	8
Supported Virtual Desktop Infrastructure Applications and Terminal Emulators	10
Supported non-EHR Applications	10
Accessing the Nuance Management Center	11
Pre-requisites for accessing the Nuance Management Center	11
Steps for accessing the Nuance Management Center	11
Adding the Nuance Management Center URL as a trusted site	12
Configuring support for Windows Presentation Framework controls	14
Disable support for WPF controls in local and published applications	14
Disable support for WPF controls only in an application published from a Citrix server ...	15
Enable support for WPF controls in local and published applications	15
Creating Accounts	16
Creating/selecting user account to install all services	16
Installing Dragon Medical Network Edition	17
Assigning access to servers, clients, and master user profile locations	18
Assigning permissions to the NMS, clients, and master user profiles	20
Privacy of patient data	20
Ensuring appropriate ports are open	20

Turning off Automatic Updates	21
Anti-Virus recommendations	21
On NMS Servers, Profile Optimization Server, and SQL Database Server	21
Recommended virtual memory settings	22
Server Virtual Memory:	22
Dragon Medical Client Workstation Virtual Memory:	22
Allocating disk space for logs	23
Checklists for installing the Nuance Management Server and other servers	24
Installing Operating System software	24
Decide to work in Active Directory	24
Creating required account	24
Installing database software	24
Installing NMS Server, Nuance Management Center, and Database	25
Installing Speech Nodes, and Database	25
Checklists for Setting up Active Directory Services	26
Installing SQL Server 2008, 2012, and 2014	26
Creating NMC Administrator Account for Active Directory Administrator	26
Enabling Active Directory and setting connection string	27
Logging Out and logging back in	27
Creating Active Directory Single Sign-On user accounts (optional)	27
Continue to Configure NMS Server as Active Directory Administrator	27
Checklists for Starting the Nuance Management and other servers	28
Verifying server services are running	28
If you are planning to use Active Directory Services	28
Checklists for Setting up a file server for master user profiles	29
Checklists – Setting up web server to host master user profiles	30
Checklist for upgrading roaming user profiles	31
Before you upgrade	31
Upgrading	32
Associating user accounts with newly upgraded master user profiles	32
Checklists – Converting local users	32
Before you convert	32
(If applicable) Combine multiple Dragon Medical Client profiles for a single provider, keeping only one	32
Exporting local user profiles	33
Enabling roaming feature on workstation	33
Associating user accounts with newly converted master user profiles	33
Migrating roaming users to Dragon Medical Network Edition	35
Checklist for installing Dragon Medical Clients	35

Before removing earlier version of Dragon Medical	35
Before beginning any client installation to a workstation	35
Downloading Dragon Medical Client MSI installer through the Nuance Management Center	36
Installing Dragon client manually	36
Pushing Dragon MSI installation to multiple workstations: administrative installation	36
Pushing Dragon MSI installation to multiple workstations: using SCCM	37
Pushing Dragon MSI installation to multiple workstations: creating custom installer for Active Directory	37
Chapter 2: Installing the Nuance Management Server and components ...	39
Prerequisites for installing the Nuance Management Server and Nuance Management Center	40
Creating an account to run all services	40
Information requirements for installing the NMS server and Nuance Management Center	41
Installing prerequisite software for the Nuance Management Server	42
Installing Windows Server and .NET Framework	42
Internet Information Services Support	42
Installing SQL Server	45
Before you begin database software installation	46
Installing SQL Server	46
Ensuring all required ports are open	53
Installing the Nuance Management Server and Nuance Management Center	54
Creating an account to run all services	54
Installing the NMS—Server, Nuance Management Center, and Database	55
Anti-virus recommendations and requirements	56
On NMS Servers and the SQL Database Server:	56
Configuring the network traffic switch to ping NMS Servers for load balancing	57
Ensuring clients can contact an NMS Server with a load balancing traffic switch in the network ..	57
Accessing the Nuance Management Center when load balancing traffic switch chooses among multiple NMS Servers on your network	58
Verifying all necessary ports are open	58
Test access to NMS ports from a site client machine	58
Chapter 3: Install or Upgrade to Nuance Management Server 5.1	61
Install NMS 5.1 for a single-node or multiple-node configuration	62
Prerequisites	62
Install the SSL certificate for a single-node configuration	62
Install the SSL certificate for a multiple-node configuration	63
Install the NMS software	63
Install one or more Profile Optimizer Speech Nodes	71

Upgrade a single-node or multiple-node configuration to NMS 5.1	73
Prerequisites	73
Install the SSL certificate for a single-node configuration	73
Install the SSL certificate for a multiple-node configuration	74
Install the NMS software	74
Run the Profile Optimizer Server Migration Tool	82
Requirements	82
Steps for migrating Profile Optimizer server data	82
Chapter 4: Installing Profile Optimizer speech node components	85
Prerequisites for Installing Profile Optimizer speech nodes	86
Installing software to support Profile Optimizer Speech Nodes installation	86
Installing prerequisite software for speech nodes	87
Installing Windows Installer for Speech Nodes not on Windows Server	87
Installing Dragon Medical SDK Client Edition	88
Installing the speech nodes	89
Installing Profile Optimizer Speech Nodes on independent or virtual machines	92
Installing Profile Optimizer Speech Nodes	92
Anti-virus recommendations and requirements	92
On NMS Servers and the SQL Database Server:	92
Chapter 5: Starting servers and logging in to the Nuance Management Center	93
Logging in to the Nuance Management Server through the Nuance Management Center	94
Starting the Nuance Management Server	95
Changing the account running NMS Server	95
Starting NMS Server service	95
Starting Profile Optimizer Speech Nodes	96
Running Profile Optimizer Speech Node service	96
Troubleshooting: If the Speech Node Will Not Start - Giving Yourself Rights to Start the Service	97
Anti-virus recommendations and requirements	99
On NMS Servers and the SQL Database Server:	99
Chapter 6: Setting up the Master User Profiles machine	101
Choosing a master user profiles location for a site	102
Information required for setting up Web Server	104
Setting up a computer to host master user profiles	105
Creating the master user profile directory	105
Mapping the disk drive on the client workstation	105
Setting up access to the master user profile directory	107
Installing software for storing master user profiles on a web server	108

Entering settings under Virtual Directory or Home Directory tab	110
Configuring HTTP or SSL settings in Nuance Management Center	114
Example: Installing SSL certificates for IIS 6.0	116
Setting HTTP connection settings for web server	119
Making selections on HTTP Settings tab	120
Setting SSL connection settings for secure web server	122
Settings on SSL Settings tab	123
Recommended settings for SSL web servers	123
Assigning access to folders and master user profiles across the network	125
Turning off Automatic Updates	125
Chapter 7: Upgrading roaming and local User Profiles	127
Preparing to upgrade non-network edition Dragon Medical Clients	128
Before you upgrade Dragon Medical non-network edition	128
Overview of migrating local users from Dragon Medical Practice Edition	129
After you install the Dragon Medical client, perform the following steps	130
Creating user accounts for healthcare providers	131
Migrating Non-Network Dragon User Profiles to the Nuance Management Server	131
Before migrating Dragon local user profiles	131
Migration Paths	132
Overview of migrating local user profiles	132
Step 1: Back up local user profiles	133
Step 2: Combine multiple Dragon Medical profiles for a single provider (DMEE only)	133
Step 3: Export user profiles to the default user profile directory	135
Step 4: Set Up a Directory for the User Profiles via the Nuance Management Center	136
Step 5: Copy the User Profile Export Tool to a network location	136
Step 6: Install and Run the User Profile Export Tool	136
Step 7: Create user accounts for the migrated profiles on the NMS	137
Step 8: Associate the new user accounts with the profiles you migrated in Step 6	137
Step 9: Upgrade the User Profiles	138
Step 10: Install/Upgrade the Dragon Client on the workstations	138
Step 11: Log in	138
Upgrading User Profiles from DM Network Edition Version 10.x to Version 2.0 or Higher	139
Before upgrading Dragon user profiles	139
Upgrade the User Profiles	140
Configuring the location of user profiles	141
Upgrading a user profile to DM Network Edition Version 2.5.1	142
Associating new user accounts with upgraded user profiles	143
Chapter 8: Installing the Dragon Medical Client	145

Overview of installing the Dragon Medical Client	146
Opening ports to access user profiles on web server or secure web server	146
Approaches to installing the Dragon Medical Client	146
Pushing the Dragon MSI installation to workstations	147
Options for pushing MSI installation of Dragon to one or more workstations on a network	148
Support for the Windows System Center Configuration Manager	148
Support for the Windows System Management Server	149
Support for Windows Server with Active Directory Services	149
Installing Dragon manually outside of the Nuance Management Center	150
Associating Dragon with the Nuance Management Server or the Local Authenticator	151
Associating Dragon with an NMS Server or Local Authenticator	151
Ensuring clients can contact an NMS Server with a load balancing traffic switch in the network	152
Pushing the Dragon MSI installation to workstations	153
Options for pushing MSI installation of Dragon to one or more workstations on a network	154
Support for the Windows System Center Configuration Manager	154
Support for the Windows System Management Server	155
Support for Windows Server with Active Directory Services	155
Understanding Dragon MSI command line options	156
Modifying the admininstall.bat file	156
Creating a custom installer for the client in Active Directory	161
Installing the Microsoft Custom Installation Wizard	161
Modifying setup Properties for Custom Installation	161
Starting Dragon Medical Clients from Command Line	168
Creating Organization Tokens	170
Creating Single Sign-On user accounts	170
Implementing Active Directory Single Sign-On	170
Implementing EHR Single Sign-On	171
Closing the Dragon Medical client from a command line	176
Command line interface	177
Ensuring Dragon Medical Client anti-virus recommendations are met	180
Assigning access to folders and master user profiles across the network	181
Turning off Automatic Updates	181
Chapter 9: Migrating from the Data Distribution Tool to Command Sets and Command Sharing	182
Migrating from Data Distribution Tool to Command Sets	183
About Command Sets	183
Choosing a Migration Strategy	183
Migrating Custom Words from Data Distribution Tool to Word Sharing	186
Chapter 10: Backing up server systems	187

NMS SQL Server backup system	188
Scheduled NMS transaction log and database backups	188
Disabling scheduled backups of the NMS database	188
Database Backup File Names	189
Master user profiles backups	190
Removing a master user profile folder for a deleted user account	190
Servers and Dragon client logs	192
Dragon and Profile Optimizer Speech Node logs	192
NMS Server logs	192
View log files for a variety of products and product components	193
Nuance Management Center logs	194
Upload the Nuance Management Center log file to the NMS	194
Chapter 11: Moving Databases	195
Moving NMS Server SQL database	196
Moving the database to a new location	196
Removing the old database from the original location	196
Chapter 12: Setting up Active Directory Services	197
Setting up the Nuance Management Server to run Active Directory Services	198
Enabling Active Directory Services	198
Creating an NMC Administrator account for Active Directory	198
Set the Active Directory Connection String	199
Restarting the Nuance Management Service	199
Index	201

Document Versions

Version Number	Date
Initial version for DM Network Edition 2.5.1	5/6/2016

Introduction to installing Dragon Medical Network Edition

For information about installing or upgrading to Dragon Medical Network Edition, 2.5.1, please see chapter 1.

Dragon Medical Network Edition provides a central server (the *Nuance Management 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 *NMS 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, 2.5.1

Dragon Medical Network Edition, 2.5.1 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, 2.5.1 for administrators, see the following topics in the DM Network Edition Administrator Guide:

- What's new in Nuance Management Server - All products
- What's new in Nuance Management Server - DM Network Edition

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

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

To learn more about NMS in the cloud, see the 'Introducing NMS in the cloud' section in the DM Network Edition Administrator Guide or the Dragon Medical Network Edition, 2.5.1 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 NMS in the cloud* on page 1 of Dragon Medical Network Edition and continuing to *Installing and Configuring NMS 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 NMS 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	7
Accessing the Nuance Management Center	11
Configuring support for Windows Presentation Framework controls	14
Creating Accounts	16
Creating/selecting user account to install all services	16
Installing Dragon Medical Network Edition	17
Assigning access to servers, clients, and master user profile locations	18
Ensuring appropriate ports are open	20
Turning off Automatic Updates	21
Anti-Virus recommendations	21
Recommended virtual memory settings	22
Allocating disk space for logs	23
Checklists for installing the Nuance Management Server and other servers	24
Checklists for Setting up Active Directory Services	26
Checklists for Starting the Nuance Management and other servers	28
Checklists for Setting up a file server for master user profiles	29
Checklists — Setting up web server to host master user profiles	30
Checklist for upgrading roaming user profiles	31

Checklists — Converting local users	32
Checklist for installing Dragon Medical Clients	35

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:

- 2 GB RAM for Microsoft® Windows XP®*.
- 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 2012, 64-bit
 - Windows Server 2012, 64-bit R2.
 - Windows Server 2008, 64-bit

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/>

Web Connection: A web connection is required for activation during installation.

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 XP® Service Pack 3, 32-bit only*
- Microsoft® Windows Server 2008, Service Pack 1, Service Pack 2
- Microsoft® Windows Server 2008, R2, 32-bit and 64-bit
- Microsoft® Windows Server 2008, R2 64 bit Service Pack 2
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 R2

Software Requirements for the Nuance Management Server (NMS) Server

Operating system:

Choose one of the following:

- Microsoft® Windows Server 2008, Service Pack 1, Service Pack 2
- Microsoft® Windows Server 2008 R2, 32-bit and 64-bit
- Microsoft® Windows Server 2008 R2 64 bit Service Pack 2
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 R2 (64 bit)

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

Web Server

- Internet Information Services (IIS). Version 6.0, 7.0, or 7.5.

Internet Browser: Microsoft Internet Explorer 8, 9, 10, and 11 (free download at www.microsoft.com)

SQL Server

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

Software Requirements for the Profile Optimizer Nodes

Operating system:

Choose one of the following:

- Microsoft® Windows XP SP3
- Microsoft® Windows 7
- Microsoft® Windows Server 2008, Service Pack 1, Service Pack 2
- Microsoft® Windows Server 2008 R2, 32-bit and 64-bit
- Microsoft® Windows Server 2012

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

Microsoft .NET:

- Microsoft .NET Framework 4.0

SQL Server

Choose one of the following:

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

Windows Installer 3.1 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 3.1 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 *Nuance Management Server Software and Documentation DVD*.

Supported Virtual Desktop Infrastructure Applications and Terminal Emulators

- XenDesktop 7.1, and XenDesktop 7.6
- 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 2007, 2010 (32 & 64 bit), 2013 (32 & 64 bit), 2016 (32 & 64 bit)
- Microsoft® Outlook® 2007, 2010, 2013, 2016
- Microsoft® Excel® 2007, 2010, 2013, 2016
- WordPerfect® x5, x6
- Apache OpenOffice Writer 3.4
- Open Office Writer v3.1, 3.2
- Internet Explorer 8, 9, 10, 11 (11 supported when Enhanced Protective Mode is disabled)
- Rich Internet Application IE8, IE9, IE10, IE11
- Mozilla® Firefox® 8+
- Rich Internet Application Firefox® 12+
- Rich Internet Application Google Chrome 16+
- Windows Live Mail v15 & v16
- Mozilla® Thunderbird™ x3 and up
- Lotus Notes 8.5

* The 2.x versions of DM Network Edition will be the last versions of the product to support Windows XP. DM Network Edition 2.1 continues to support Windows XP.

Accessing the Nuance Management Center

The Nuance Management Center (NMC) is a web-browser based application that is part of the overall Nuance Management Server (NMS) system. The NMC supports many functions for Nuance Healthcare applications, including reporting for iChart/DESS, and eScription.

When you install the NMS, a default user account, called the admin account, is created automatically. The admin account has a license type of 'NMC Administrator'. The admin account includes elevated access to NMS features and services, including DM Mobile Recorder configuration.

Pre-requisites for accessing the Nuance Management Center

On the computer that will access the Nuance Management Center, make sure the following items are installed:

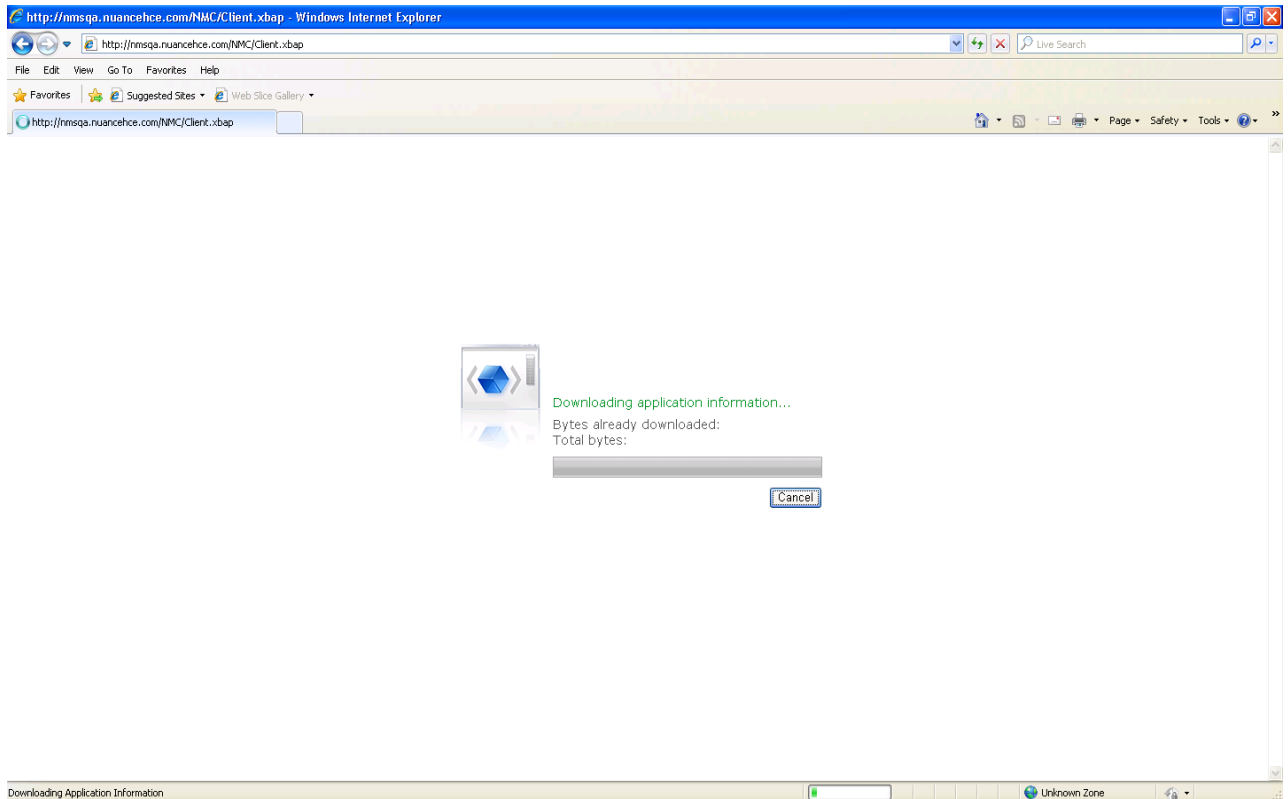
- Microsoft .NET framework. See *System Requirements for Dragon Medical Network Edition* on page 7 for supported versions.
- Full trust privileges.
- Intranet or Trusted Web Site.
- Internet Explorer. Microsoft .NET framework. See *System Requirements for Dragon Medical Network Edition* on page 7 for supported versions.

To allow the computer to communicate with the Nuance Management Server, open the following port 443. All communication from clients occurs on SSL-encrypted REST endpoints on port 443.

Steps for accessing the Nuance Management Center

1. Open Internet Explorer and type in the following address in the address bar: <http://nms.nuancehdp.com/NMCHTML>

The following screen appears: "Downloading application information" as required files are downloaded to the local computer.

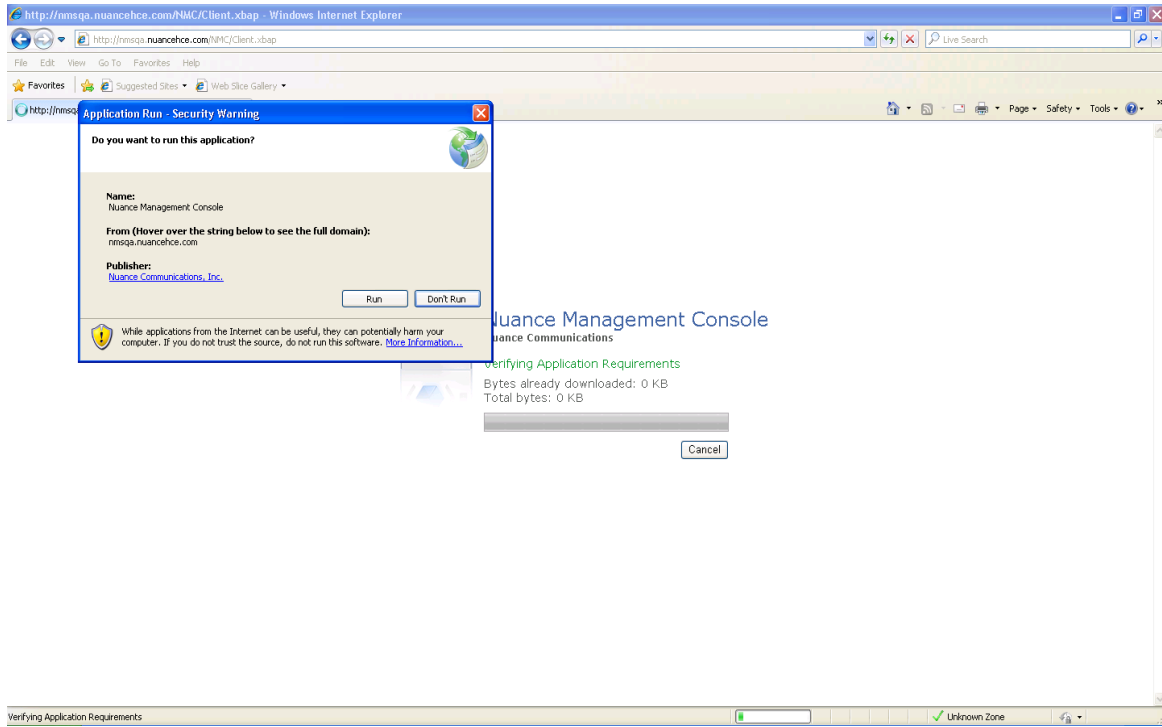


2. While files are downloading, if you see the message "Trust Not Granted", [add the NMC URL as a 'Trusted site'](#).

Adding the Nuance Management Center URL as a trusted site

1. In Internet explorer, Select **Tools** -> **Internet options** -> **Security Tab** -> **Click on Trusted sites icon** -> **Sites**.
2. Enter the Nuance Management Center URL
3. Click **Add**.
4. Uncheck the checkbox **Require Server verification (https:)** for all sites in this zone.

5. If you see the following security warning, click **Run**.



6. When the file downloads are complete, you will see the login screen. Enter your **User Login** and **Password** and click **Log in**.

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:

```
C:\Temp\DMNE2DOT5.exe /V"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:

```
C:\Temp\MiniTracker.exe /V"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:

```
C:\Temp\DMNE2DOT5.exe /V"TEXT_SERVICE_SUPPORT=1"
```

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

Example: Using the Full client installer:

```
C:\Temp\setup.exe /V"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 **NMSapps**) 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

Assigning access to servers, clients, and master user profile locations

Caution:

To ensure that your Dragon Medical Network Edition network components can communicate with each other and that the network can function properly, you must assign permissions to all appropriate directories and access rights to administrator and user accounts on servers and clients as indicated in the tables that follow this note.

Locations Servers Need Access To			
Location	Permissions level or Type of user access rights	Users affected	Equipment given access
Directories where server components are installed.	Full read/write/modify permissions	On servers: Windows admin account that all server services run under.	Server Components: <i>NMS Server</i> <i>Nuance Management Center</i> <i>NMS Database</i> Each <i>Profile Optimizer Speech Node</i> SQL Server
Master User Profiles folder	Full read/write/modify permissions	Windows admin accounts that all server services run under & user accounts for all providers dictating on <i>Dragon Medical Clients</i> .	Server Components: <i>NMS Server</i> <i>Nuance Management Center</i> <i>NMS Database</i> Each <i>Profile Optimizer Speech Node</i> Client Components: Each dictating healthcare provider

Locations Clients Need Access To			
Location or Registry Key	Permissions level or Type of access rights	Users affected	Equipment given access
Master User Profiles folder	Full read/write/modify permissions	Windows user accounts for all providers dictating on <i>Dragon Medical Clients</i> .	Client Components: Each dictating health-care provider
Locations on all physical servers that house <i>NMS Servers</i>			
<drive letter> : \Users\All Users\Application Data\Nuance folder and all sub-folders	Full read/write/modify permissions	Windows user accounts for all providers dictating on <i>Dragon Medical Clients</i> .	Client Components: Each dictating health-care provider
<drive letter> : \Program Data\Application Data\Nuance folder and all sub-folders	Full read/write/modify permissions		
<drive letter> : \Program Files\Nuance folder and all sub-folders	Read permissions		
Locations on the client workstation where the provider dictates with <i>Dragon Medical Client</i>			
<drive letter> : \Program Data\Nuance folder and all sub-folders	Full read/write/modify permissions	Windows user accounts for all providers dictating on <i>Dragon Medical Clients</i> .	Client Components: Each dictating health-care provider
<drive letter> : \<Windows User ID>\AppData\ folder and all sub-folders	Full read/write/modify permissions		
<drive letter> : \Documents and Settings\All Users\Application Data\Nuance folder and all sub-folders	Full read/write/modify permissions		
Locations in Registry of the client workstation where the provider dictates with <i>Dragon Medical Client</i>			
HKEY_LOCAL_MACHINE\SOFTWARE\Nuance	Rights to update the registry to read/write to these keys.	Windows accounts that workstations running <i>Dragon Medical Client</i> run under.	Client Components: Each dictating health-care provider
HKEY_CURRENT_USER\SOFTWARE\Nuance			

Assigning permissions to the NMS, clients, and master user profiles

Caution: Servers: To ensure all *NMS* and processes can interact with one another, you run all the software under a single administrator account. These components must have complete read/write/modify access to the **master user profiles directory**. If the servers and *Speech Nodes* cannot access the master user profiles, *Dragon Medical Network Edition* cannot function properly.

Clients: To ensure every dictating healthcare provider has appropriate access to his or her user profile, you must give full read/write/modify permissions to all files and directories housing the master user profiles, even to access them through an **http** or **https** connection. This level of permission/access ensures that when the provider dictates, *Dragon* can interact with the master user profiles effectively.

Each windows user account that logs in to the Dragon Medical Client workstation should also have access to the master user profiles that allows reading/writing/modifying the profiles, actions that the Dragon Medical Client takes frequently to keep profiles current.

Master User Profiles: 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 4.0 installed on it, and that the machine is in the same Windows domain as your DM Network Edition servers.

Privacy of patient data

To protect the privacy of patient data and the integrity of the master user profiles, you should **not** give Windows user accounts of *Dragon Medical Clients* rights to log in to the master user profiles machine; the *Dragon* software writes to and modifies the profiles in the background.

Ensuring appropriate ports are open

On the *Dragon Medical Network Edition* network, you must open particular ports to ensure the free flow of data between the various servers and clients.

A complete list of all the ports that should be open is given in the Planning guide.

You must open all ports listed in the table on any hardware firewalls to ensure that no firewall blocks transmission of data and brings the network to a halt.

Turning off Automatic Updates

After you set up each physical server or workstation you plan to use in the network, be sure to turn off Windows Automatic Updates. You should be qualifying each update Windows sends by installing it first on a single test machine of the network and updating other machines on the network only after you determine that it clearly will not disrupt the network.

Even if you have determined an update is not going to negatively affect the network, you still 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.

Anti-Virus recommendations

Nuance recommends anti-virus software on all DM Network Edition servers and clients to protect the system from potential downtime due to viruses. However, be aware of the recommended restrictions.

You should exclude from the anti-virus scan any files found in the folders indicated below or with the extensions listed below.

On NMS Servers, Profile Optimization Server, and SQL Database Server

- Nuance folder and all sub-folders
- Files with these extensions:
DAT, DRA, ENH, INI, LCK, LOG, NWV, SIG, TXT, USR, VER, VOC, WAV

Dragon Medical Client Workstations (Windows 7, 8.x, 10, XP, and Vista):

- **C:\Program Files\Nuance**folder and all sub-folders
- **C:\Program Data\Nuance** folder and all sub-folders
- **C:\<Windows user_ID>\AppData** folder and all sub-folders
- **C:\Documents and Settings\All Users\Application Data\Nuance** folder and all sub-folders
- **C:\Documents and Settings\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

Recommended virtual memory settings

Nuance recommends that you set virtual memory to particular levels on servers and workstations in the Dragon Medical Network Edition network.

Server Virtual Memory:

Nuance recommends that the virtual memory for all servers be set to three times the physically installed RAM.

Dragon Medical Client Workstation Virtual Memory:

Set Virtual Memory to 4092 on Windows Server 2008, or to the maximum possible setting on workstations that have 4 GB of RAM.

Allocating disk space for logs

The *Profile Optimizer Speech Node* generates two log files for each ACO and LMO task it carries out:

- *Dragon* log file—*Dragon Medical SDK Client* writes this file.
- *Speech Node* service log file—Profile Optimizer services write these files.

(You can view both the *Dragon* log files and the *Speech Node* service log files through the *Nuance Management Center*.)

The *NMS Server* generates one log file for each user:

- Windows communication foundation service log files

The *NMS Server* stores up to the last 10 MB of logs generated, a maximum of 50 log files for the entire server, before purging the oldest files and replacing them with newer ones as it generates them.

The *Dragon* log and *Speech Node* service log files are generally between 3 and 5 KB each. The *Profile Optimizer Server* stores them for 30 days. Although the log files could be larger, they are stored in a zipped format and compress very well. If you run an optimization process for every provider every day and have 500 providers, if every log were as large as 5 KB, all of those logs would still use only 2.5 MB of storage space and in 30 days that would become 75 MB of storage space.

Storage space for all of these logs is relatively inconsequential; however, if you expand the number of providers in your organization, it is always best to take into account storage requirements for all generated files.

If you call Technical Support, you might be asked to provide any of these logs to help Nuance engineers work on any issues with your network.

To access your *Dragon* log files, refer to the *Nuance Management Server Administrator Guide*.

Checklists for installing the Nuance Management Server and other servers

Installing Operating System software

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

- Install Windows Server. See *System Requirements for Dragon Medical Network Edition* on page 7 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 *NMS 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 **NMSapps** 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 16 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 7 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 45.

Refer to *Setting up the Nuance Management Server to run Active Directory Services* on page 198.

Installing NMS Server, Nuance Management Center, 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 7 for the supported versions.

Refer to *Installing prerequisite software for the Nuance Management Server* on page 42.

- Install Internet Information Services. See *System Requirements for Dragon Medical Network Edition* on page 7 for the supported version.

Refer to *Installing prerequisite software for the Nuance Management Server* on page 42.

- Enter server name or IP address of *NMS 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 the Nuance Management Server and Nuance Management Center* on page 54.

Open required ports on NMS 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, and Database

Gather information you need:

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

- Name or IP address of database server: _____
or Database connection string for SQL server authentication:

- 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 3.1 or greater on machine.
- Install *Dragon Medical SDK Client* on machine.

Refer to *Installing prerequisite software for speech nodes* on page 87

Checklists for Setting up Active Directory Services

To set up your *NMS Server* to run in Active Directory Services you should take particular actions during each step of the *Dragon Medical Network Edition* installation and *NMS 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 Nuance Management Server to run Active Directory Services* on page 198.

Installing SQL Server 2008, 2012, and 2014

- 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 *NMS Server*.

- Log in through the *Nuance Management Center* using the login and password that Nuance provides.
- Create a user account for the Active Directory administrator (see the *Nuance Management 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.

Enabling Active Directory and setting connection string

- Configure *NMS Server* for Active Directory in **Nuance.NAS.Server.exe.config** file.

Logging Out and logging back in

- Log out of the *NMS Server*.
- Stop and restart the Nuance Management Service.
- Log back in through the *Nuance Management Center* 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 NMS Server as Active Directory Administrator

- Follow instructions in *Nuance Management Server Administrator Guide*.

Checklists for Starting the Nuance Management and other servers

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

- Verify that you can log in to the *Nuance Management Center* using the supplied login and password.
- Ensure that the *NMS Server* can communicate with *Profile Optimizer Speech Nodes*.

Refer to:

Logging in to the Nuance Management Server through the Nuance Management Center on page 94

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 Nuance Management Server* on page 95.

If you are planning to use Active Directory Services

Proceed to *Checklists for Setting up Active Directory Services* on page 26.

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 7 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 7 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 102 and *Setting up a computer to host master user profiles* on page 105.

In the *Nuance Management Center*, 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 *NMS Server* later uses to find the master user profiles.

Refer to *Setting up a computer to host master user profiles* on page 105.

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 7 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 108.

- 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 102 and *Setting up a computer to host master user profiles* on page 105.

In the *Nuance Management Center*, 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 *NMS Server* later uses to find the master user profiles.

Refer to *Setting up a computer to host master user profiles* on page 105.

In the *Nuance Management Center*, 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 119

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

Refer to *Setting SSL connection settings for secure web server* on page 122

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 *Nuance Management Center*, 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 131 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 143.

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, 2.5.1, 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 *Nuance Management Center*, create a user account for each provider.
- In *Nuance Management Center*, 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 143.

Migrating roaming users to *Dragon Medical Network Edition*

- In *Nuance Management Center*, 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 *Nuance Management Center*, 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 Nuance Management Server* on page 131.

Checklist for installing Dragon Medical Clients

There are several approaches to installing *Dragon Medical Client* and this checklist includes first prerequisite 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 Nuance Management Server* on page 131.

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 Nuance Management Center

- On the client workstation, log in as a Windows administrator.
- Log in to the Nuance Management Center.
- Set the location of the Dragon MSI install file on the *NMS Server* in the **System Settings > DM Network Edition..**
- Download the MSI installer for the *Dragon Medical Client* from the *Nuance Management Center*.
- Log in to the client using a user account and enter the name of the *NMS Server*.

Refer to *Associating Dragon with the Nuance Management Server or the Local Authenticator* on page 151.

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 *NMS Server*.

Refer to *Installing Dragon manually outside of the Nuance Management Center* on page 150 and *Associating Dragon with the Nuance Management Server or the Local Authenticator* on page 151.

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 161

Chapter 2: Installing the Nuance Management Server and components

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

Prerequisites for installing the Nuance Management Server and Nuance Management Center ..	40
Installing prerequisite software for the Nuance Management Server	42
Installing SQL Server	45
Ensuring all required ports are open	53
Installing the Nuance Management Server and Nuance Management Center	54
Anti-virus recommendations and requirements	56
Configuring the network traffic switch to ping NMS Servers for load balancing	57
Verifying all necessary ports are open	58

Prerequisites for installing the Nuance Management Server and Nuance Management Center

Before you actually install the *Nuance Management Server* and *Nuance Management Center*, 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 **NMSapps**) 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 *NMS* services and does not require **Log into workstation** rights.

Information requirements for installing the NMS server and Nuance Management Center

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

Name or IP Address of NMS Server Machine—You need the name or address of the machine where you intend to install the *Nuance Administration Server (NMS)*. 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 *NMS 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 prerequisite software for the Nuance Management Server

Before you install the *Nuance Management Server (NMS)*, you must install Windows Server and other prerequisite software on the same machine. See *System Requirements for Dragon Medical Network Edition* on page 7 for a list.

Although you do not have to install it on the same machine as the *NMS Server*, you should also install the SQL Server database software before you install the *NMS Server*. For details, refer to *Installing SQL Server* on page 45.

Installing Windows Server and .NET Framework

Follow these steps:

1. If you have not already done so, install Windows Server.
2. After you install the server software, you should download any Windows updates to be sure you have all updates available. Then, once you have all updates available, turn off automatic updates.
3. Install .Microsoft .NET Framework 4.5 full version. If you do not have this version of .NET Framework already installed, visit <https://www.microsoft.com/en-us/download/details.aspx?id=30653>
4. Once you have saved the `dotNetFx45_Full_setup.exe` file, double click on the file to initiate the .NET Framework installation.
5. When the .NET Framework installation is complete, you should also retrieve any updates available for the program.

Internet Information Services Support

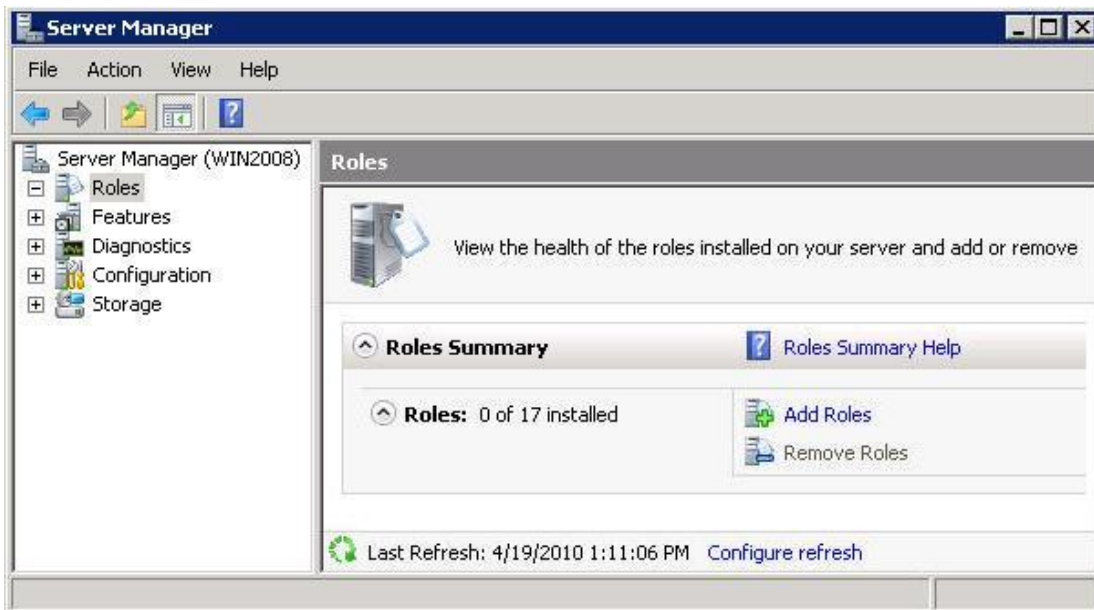
You can install and use the following versions of Internet Information Services (IIS):

Operating system	IIS version	Installation instructions
Windows Server 2012 R2	IIS 8.5	Installing IIS 8.5 on Windows Server 2012 R2: http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2
Windows Server 2012	IIS 8.0	Installing IIS 8 on Windows Server 2012: http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012

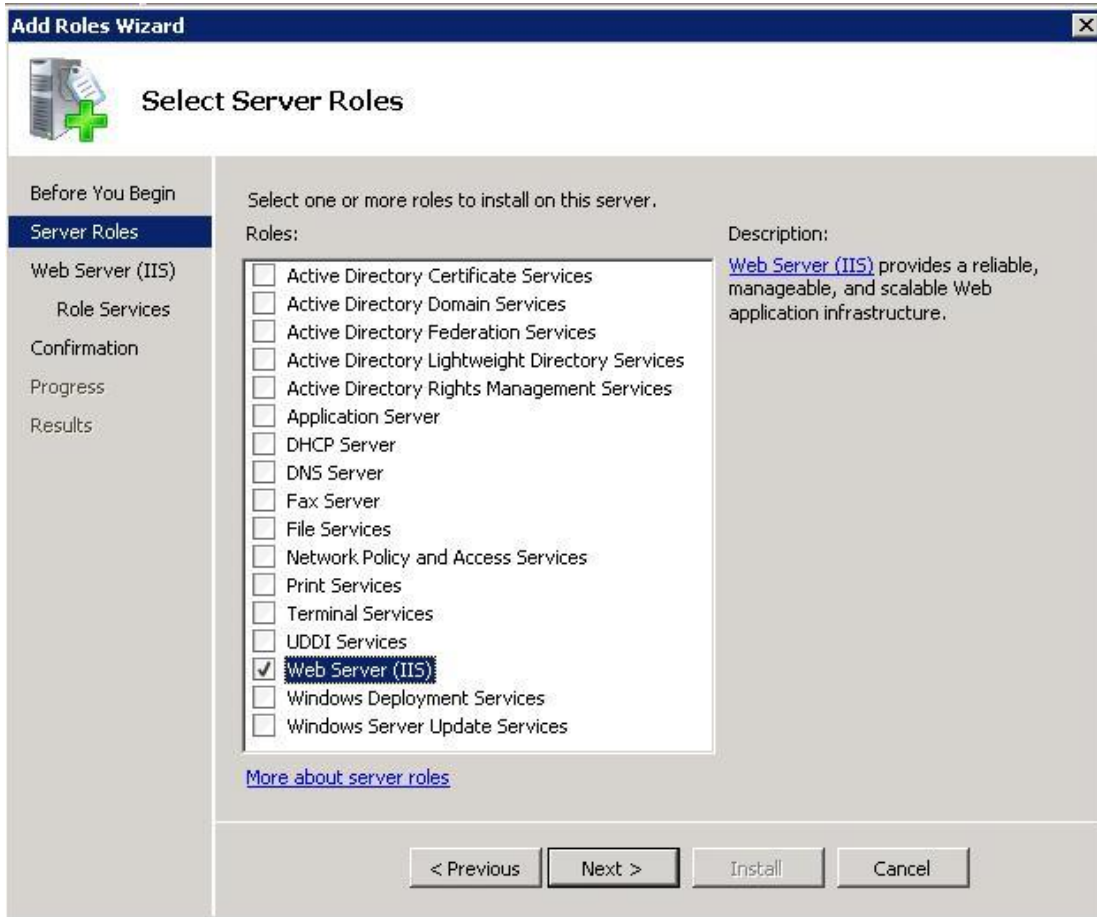
Operating system	IIS version	Installation instructions
Windows Server 2008 R2	IIS 7.5	Installing IIS 7.5 on Windows Server 2008 R2: https://technet.microsoft.com/en-us/library/cc771209.aspx
Windows 7		Installing IIS 7.5 on Windows 7 Professional, Enterprise, or Ultimate: https://technet.microsoft.com/en-us/library/cc725762.aspx
Windows Server 2008	IIS 7.0	Installing IIS 7 on Windows Server 2008 or Windows Server 2008 R2: http://www.iis.net/learn/install/installing-iis-7/installing-iis-7-and-above-on-windows-server-2008-or-windows-server-2008-r2
Windows Vista		Installing IIS 7 on Windows Vista and Windows 7: http://www.iis.net/learn/install/installing-iis-7/installing-iis-on-windows-vista-and-windows-7

Example: Installing Internet Information Services 7 and automatic updates on Windows Server 2008:

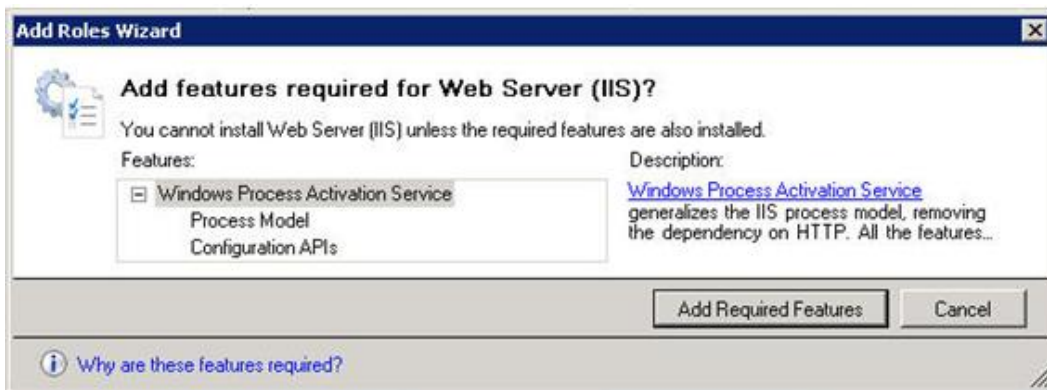
1. Go to your server desktop and click **Start > Programs > Administrative Tools** , then click on **Server Manager**.
2. To see if it is installed, under **Server Manager**, expand **Roles** and look for IIS in the list. If you do not see IIS, you need to install it.



3. Click on **Add Roles** and when the **Add Roles Wizard** opens, click **Next**.
4. Check the **Web Server (IIS)** check box in the **Roles** list.

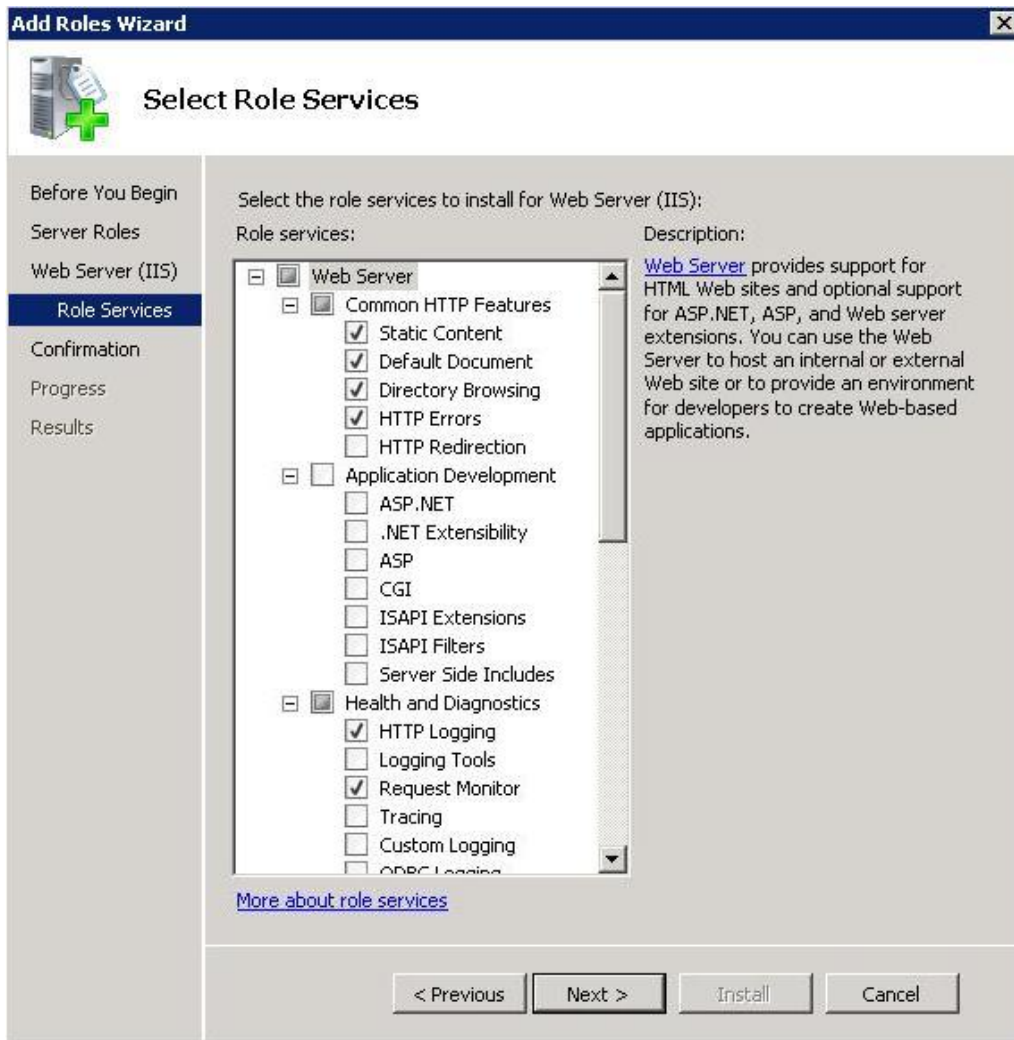


5. When the **Add features required for Web Server (IIS)**, click the **Add Required Features** button.



6. When the installation wizard displays again, click **Next** to proceed to the **Web Server (IIS)** page of the wizard.

- Click **Next** to proceed to the **Select Role Services** page of the wizard and accept the services selected by default (shown in the next illustration).



- Click **Next** to proceed to the **Confirm Installation Selections** page and verify your selections under **Web Server (IIS)**.
- Click **Install**. The **Installation Progress** page displays during installation.
- When the **Installation Results** page appears, it should say **Installation succeeded**.
- Click **Close** to exit the wizard.
- Return to the **Server Manager** and click **Roles** in the **Server Manager** explorer. Under **Role Services** verify that the list of IIS features that you installed is complete.

Installing SQL Server

Before you install the *Nuance Management Server (NMS)*, 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

The following information is about installing SQL Server 2008.

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

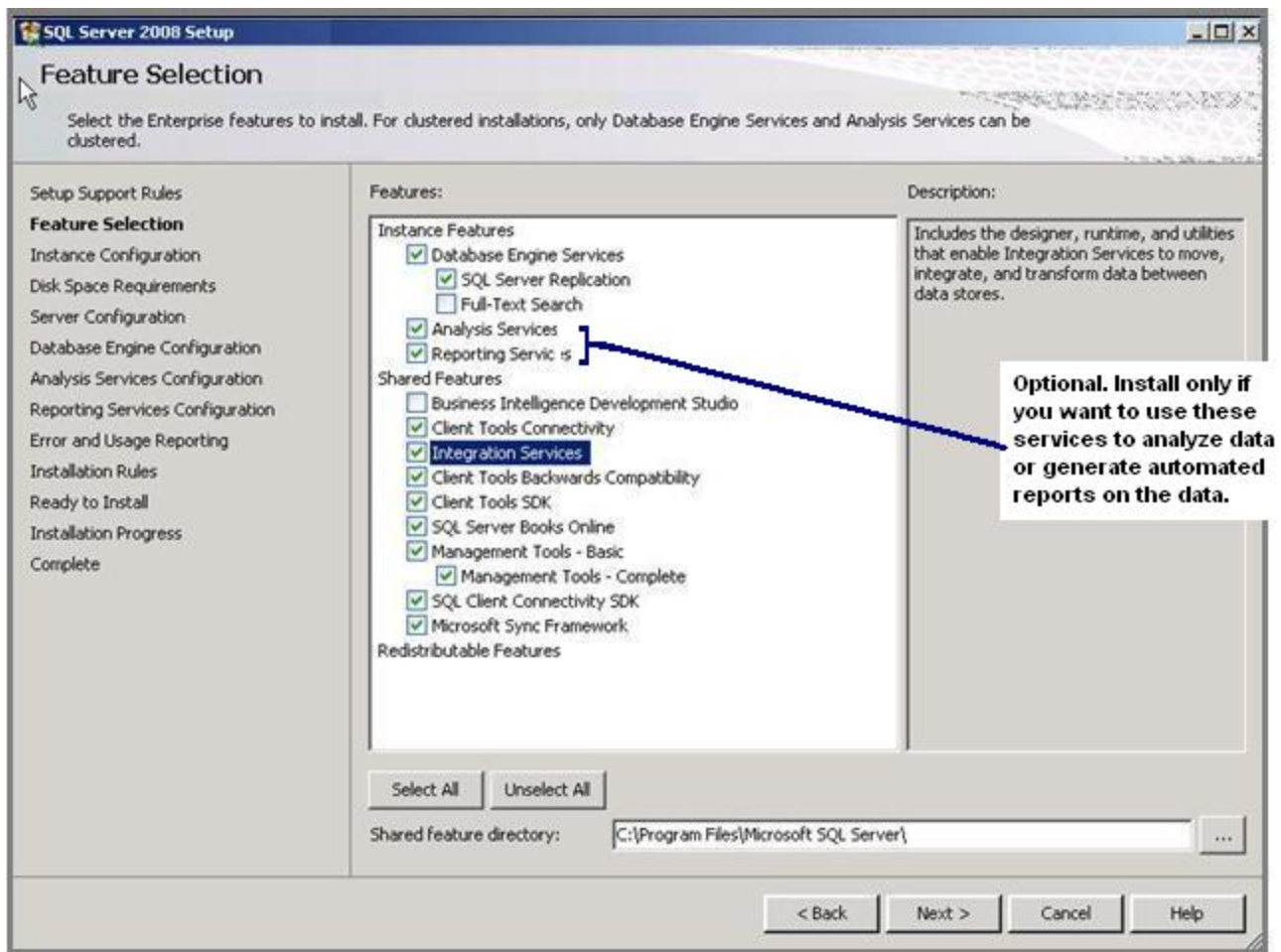
To install SQL Server 2008 from the *Nuance Management Server MS SQL 2008* DVD provided in the DM Network Edition software package you received from Nuance:

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 *Nuance Management 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.

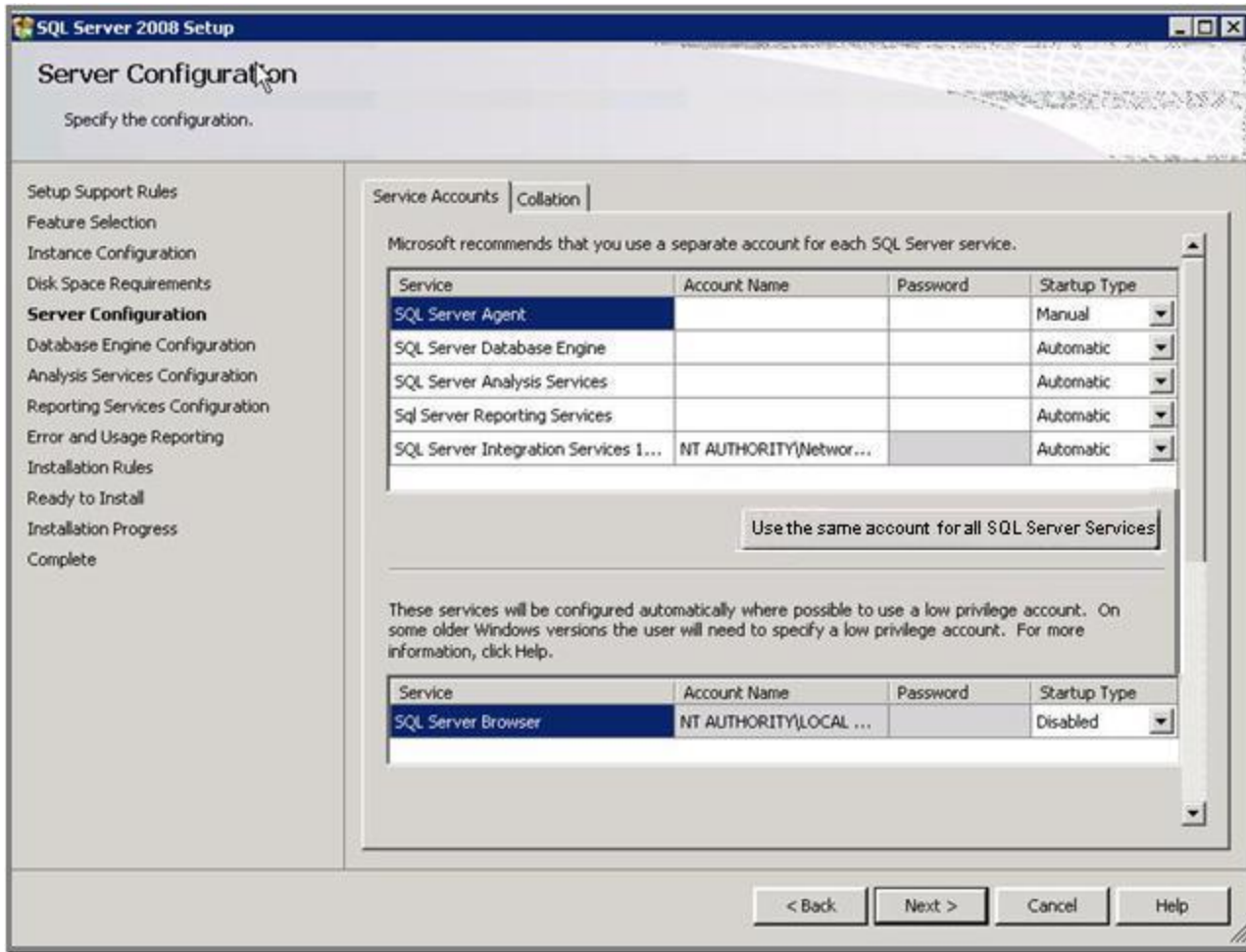


6. When the **Setup Support Rules** dialog box displays, click **Install**.
7. When the **Product Key** page is displayed, the SQL product key is automatically entered as it is embedded within the Nuance-provided SQL software DVD. The product key will not have to be entered manually. Click **Next**.
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 *NMS 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.



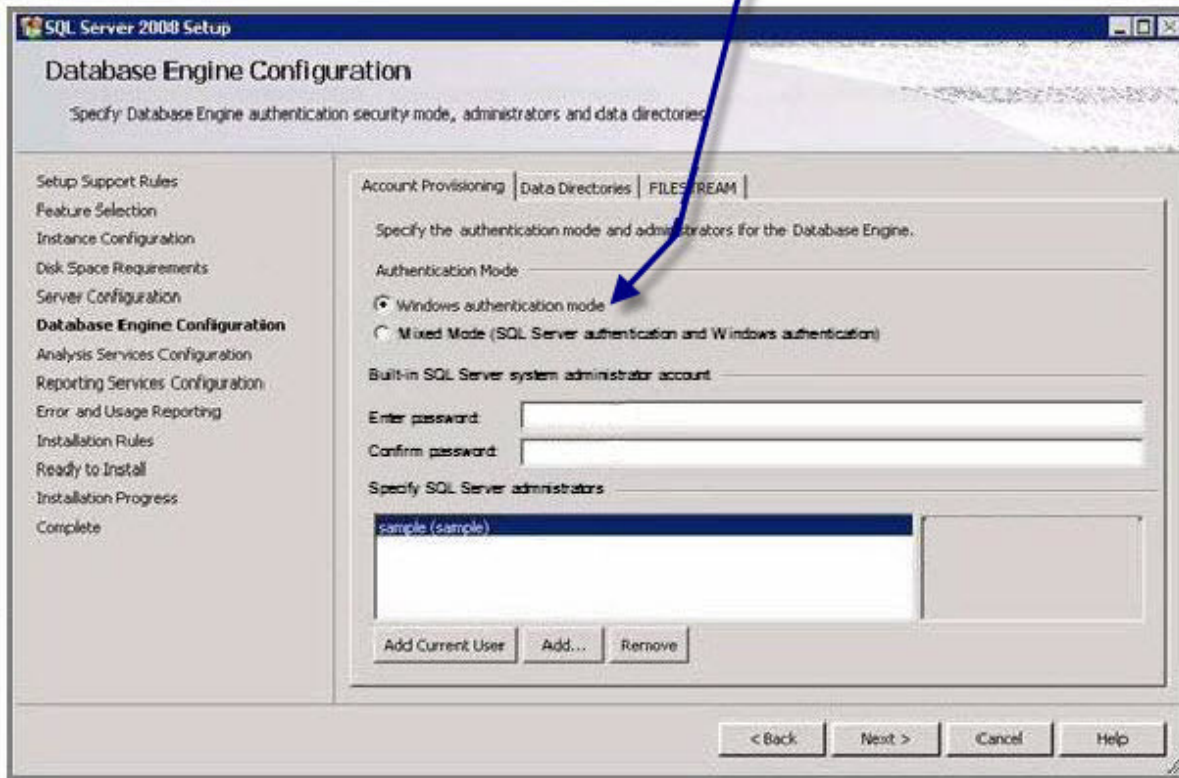
12. When the **Instance Configuration** page of the wizard displays, leave the **Default instance** option selected and click **Next**.
13. When the **Disk Space Requirements** page of the wizard displays, verify that you have adequate storage space on the server and click **Next**.
14. When the **Server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



- 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.

Windows authentication mode is the type of authentication Nuance recommends for most Networks.

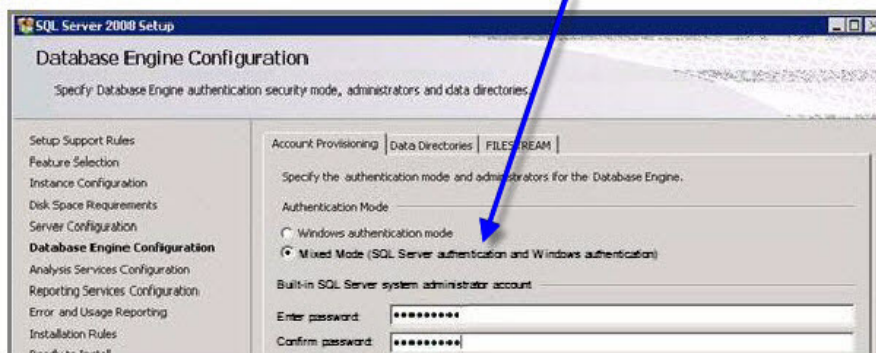


16. When you return to the wizard, click **Next**.

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.

Select Mixed Mode only if you are planning to configure your Network to run under Active Directory.



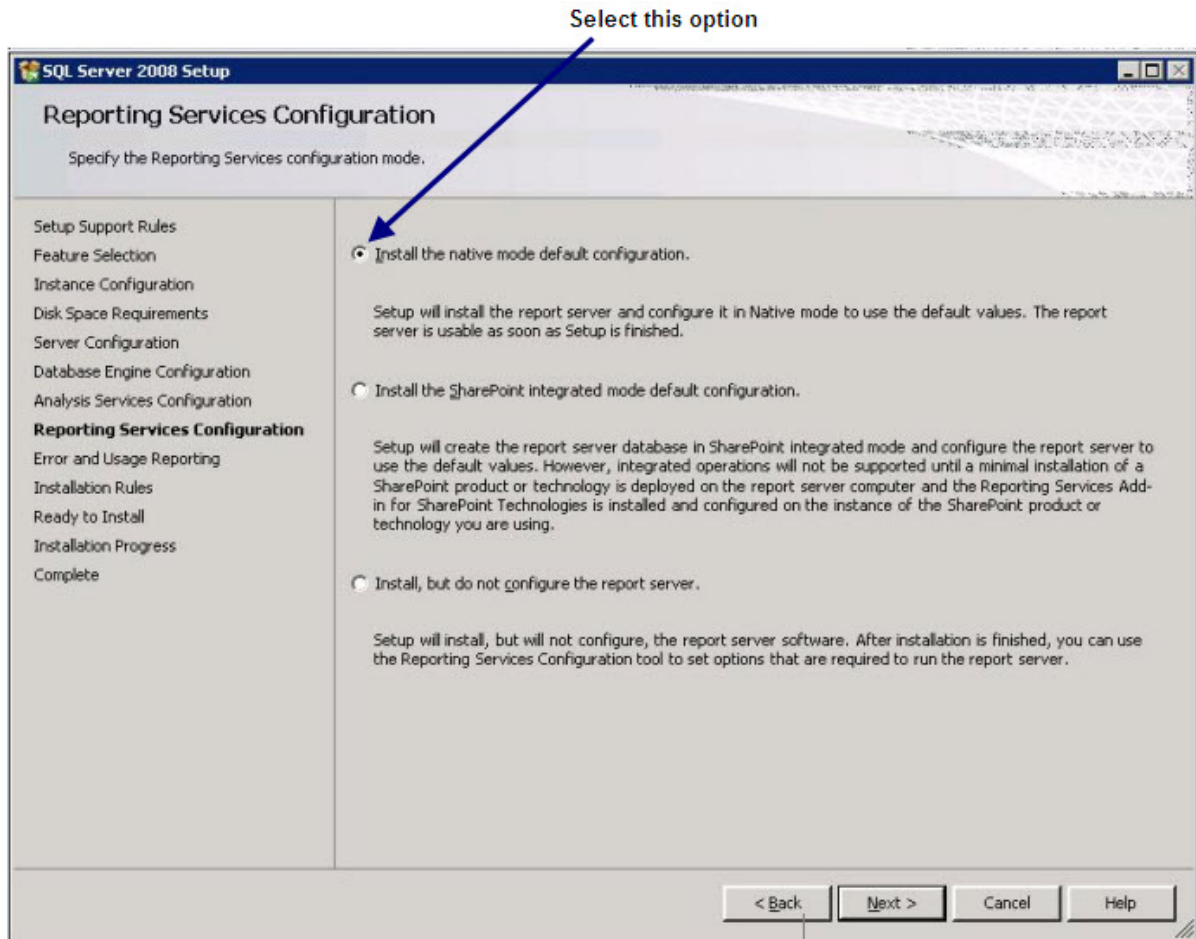
- If you select **Mixed Mode**, then under **Built-in SQL Server system administrator account**, enter the password in **Enter password** and type the password a second time in **Confirm password**.
 - Regardless of the type of authentication you choose, under **Specify SQL Server administrators**, click **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.



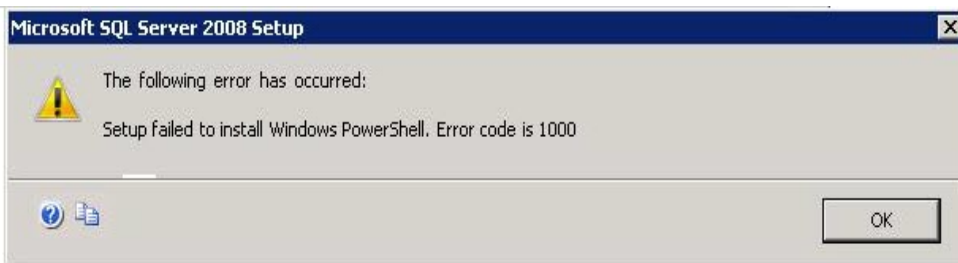
When you have added all these users to the database administrator list, click **Next**.

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 **NMSapps** 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**.

- When the **Reporting Services Configuration** page appears, select **Install the native mode default configuration** and click **Next**.

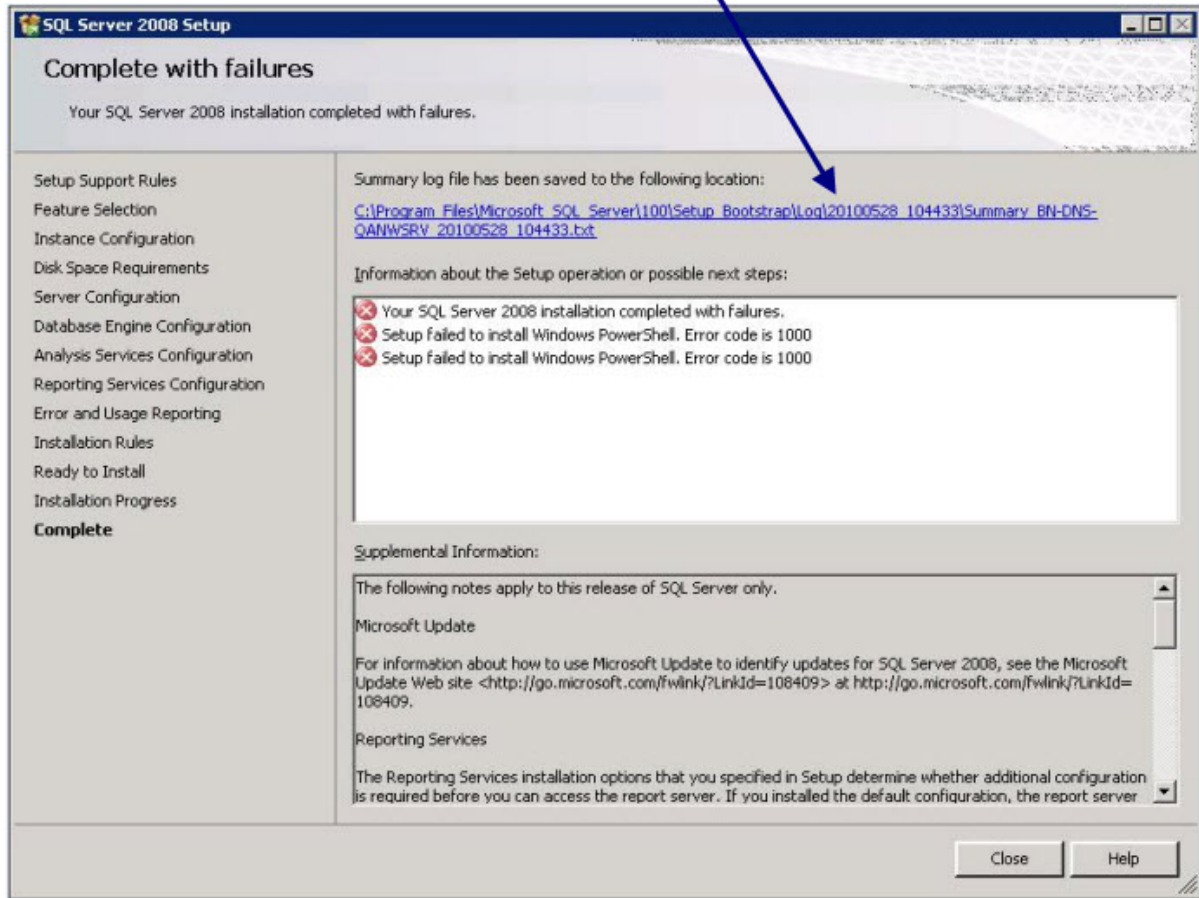


- Skip the **Error and Usage Reporting** page and click **Next**
- Click **Next** until you reach the **Ready to Install** page of the wizard.
- Click **Install** and wait for the installation to complete.



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

Click here to open the log file for more information on installation failures.



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.

Installing the Nuance Management Server and Nuance Management Center

This procedure covers installing all components of the *Nuance Management Server (NMS)*, including the server, the Nuance Management Center, and the database.

Creating an account to run all services

Note:

Before you carry out this procedure, be sure you have created a Windows administrator account to run this server and all other servers under (name it something like **NMSapps**). That server should meet the following requirements:

- Is in the organization's domain.
- 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 *Profile Optimizer Speech Nodes* server(s) within the same network.
- 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 and password of this user account.

Be sure you have the organization identifier Nuance assigned you, delivered to you via email, in a readily accessible file on a stick or on the Windows Server itself.

Installing the NMS—Server, Nuance Management Center, and Database

You are now ready to install all of the components of *Nuance Management Center*. You install them on the same machine using a single installation wizard. (After the installation is complete, you then use the Nuance Management Center to configure the server.)

Caution:

If you do **not** want to store the *NMS Server*'s data files in SQL Server's default location, you can let the installer create the database, its transaction log, and its dump device in the default location, then move the database and its files to the location you would prefer.

FOR ADVANCED INSTALLERS ONLY:

If you are installing the database in any location other than the SQL default, you can create the **NuanceMC.mdf** database, the **NuanceMC_log.LDF** transaction log, and the **NuanceMCDump.bak** dump device in SQL Server **before installing** the *NMS Server*; otherwise, the *NMS Server* installation ends up placing these files in the SQL default location.

-
1. Install .Microsoft .NET Framework. See *System Requirements for Dragon Medical Network Edition* on page 7 the required version.
 2. The *Nuance Management Center* software is code signed by Nuance to allow Nuance Support access to the client computer's resources. However, to ensure Nuance has access, if your hospital or medical facility's network requires a security policy on the computer where you install the client, you should set up that security policy to allow any code signed by Nuance to run on the machine with full trust credentials.
 3. Before you begin the installation, you might want to turn off the Windows Server Firewall.

This step applies whether you are installing the *NMS Server* on the same machine as the SQL Server or on a separate/possibly remote machine. If you instead plan to store data files in another location, you can move the database and its associated files after you let the installer create them for you.

(Alternatively, you can create the **NuanceMC.mdf** database, the **NuanceMC_log.LDF** transaction log, and the **NuanceMCDump.bak** device inside SQL Server first and specify where you want these files to reside, but Nuance recommends that you be an advanced user to create your own database.)

4. See the steps in [Chapter 3: Install or Upgrade to Nuance Management Server 5.1](#).

Anti-virus recommendations and requirements

Nuance recommends anti-virus software on all *Dragon Medical Network Edition* servers and clients to protect the system from potential downtime due to viruses. However, be aware of the recommended restrictions.

After you have installed the servers, be sure to exclude from the anti-virus scan any files found in the folders indicated below or with the extensions listed below.

On NMS Servers and the SQL Database Server:

- **Nuance** folder and all sub-folders
- Files with these extensions:
DAT, DRA, ENH, INI, LCK, LOG, NWV, SIG, TXT, USR, VER, VOC, WAV

Configuring the network traffic switch to ping NMS Servers for load balancing

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

To configure the network traffic switch to send a message to the *NMS 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:

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

The *NMS Server* delivers the following XML-formatted response to the network traffic switch:

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

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

Ensuring clients can contact an NMS 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 *NMS Servers* on your network, you should set **NAS_ADDRESS** to the address of the traffic switch, rather than the address of any particular *NMS 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 *NMS 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 *NMS Server*.

Accessing the Nuance Management Center when load balancing traffic switch chooses among multiple NMS Servers on your network

When you have multiple *NMS Servers* and a load balancing traffic switch in your network, you should be sure that when you open the *Nuance Management Center*, you substitute the name or address of the switch for the name or address of the *NMS Server*. For instance, for a load balancing switch named **NMS_Switch** at IP address **10.1.1.2**, here are two possible URLs you would use to run the Nuance Management Center:

http://NMS_Switch/NMCHTML/

or

http://10.1.1.2/NMCHTML/

Verifying all necessary ports are open

Be sure that all of the following ports are open on the *NMS Server*.

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

Test access to NMS ports from a site client machine

You can test the ability of a client machine to communicate with the NMS (cloud or on-premise).

You access a web page where you can test access to all ports required for connecting to the NMS, including:

- Port 443: To determine access to SSL-encrypted Representational State Transfer (REST) endpoints.

Steps for determining access to NMS ports

The web page tests the connection between a client machine and a server (the one in the URL when they access the web page).

If access to a port is available, the Accessibility column contains "Yes". Otherwise, the column contains "No" and may contain other information useful for troubleshooting.

- If the NMS is installed on-premise, the server URL is

<http://<yourlocalservername>/nmc/portscan.html>.

- If the NMS is in the cloud, the server URL is <http://nms.nuancehdp.com/nmc/portscan.html>.
1. Open a supported web browser and navigate to <http://nms-dev.nuancehce.com/nmc/portscan.html>.
 2. Select the check box beside the product(s) to test:
 - Nuance Management Center: Tests access to port 443.
 - DM Network Edition: Tests access to port 443.
 - Dragon Medical Recorders: Tests access to port 443.
 - Dragon Medical Direct:
 - Tests access to port 443.
 - If the NMS Server URL used to access the web page contains “nms.nuancehdp.com”, this indicates that we are accessing the production instance of the NMS. The web page tests the response of the following URL: <https://nsa.nuancehdp.com/SpeechAnywhereServices/IsAlive>
 - If the NMS Server URL used to access the page contains “nuancehce.com”, this indicates that we are accessing a QA/HCE instance of the NMS. The web page tests the response of the following URL: <https://nsa-qa.nuancehce.com/SpeechAnywhereServices/IsAlive>
 - If the NMS server URL used to access the page does not contain “nms.nuancehdp.com” or “nuancehce.com”, the installation process displays an edit box where you can enter the full Dragon Medical Direct URL for the web page to test.
 3. Press **Test**. The web page displays the test results for each of the products you selected. If a port cannot be accessed, the web page displays the host, port number, and the related protocol. The web page also displays details about the error to help you troubleshoot the issue.

Chapter 3: Install or Upgrade to Nuance Management Server 5.1

To install or upgrade to NMS 5.1, you carry out the procedures in these sections:

Install NMS 5.1 for a single-node or multiple-node configuration	62
Upgrade a single-node or multiple-node configuration to NMS 5.1	73
Run the Profile Optimizer Server Migration Tool	82

Install NMS 5.1 for a single-node or multiple-node configuration

This topic is for customers that do not have an existing NMS installation and that are installing the Dragon Medical Network Edition 2.5 client.

Notes:

- All installations of NMS 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
- Supported versions of Windows:
 - Windows 2008 R2
 - Windows Server 2012
- .NET Framework 4.5 is required on both the NMS server and PO Speech Nodes.

Prerequisites

- An SQL Server to install the NMS 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 Nuance Management Server installation: "NMS 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

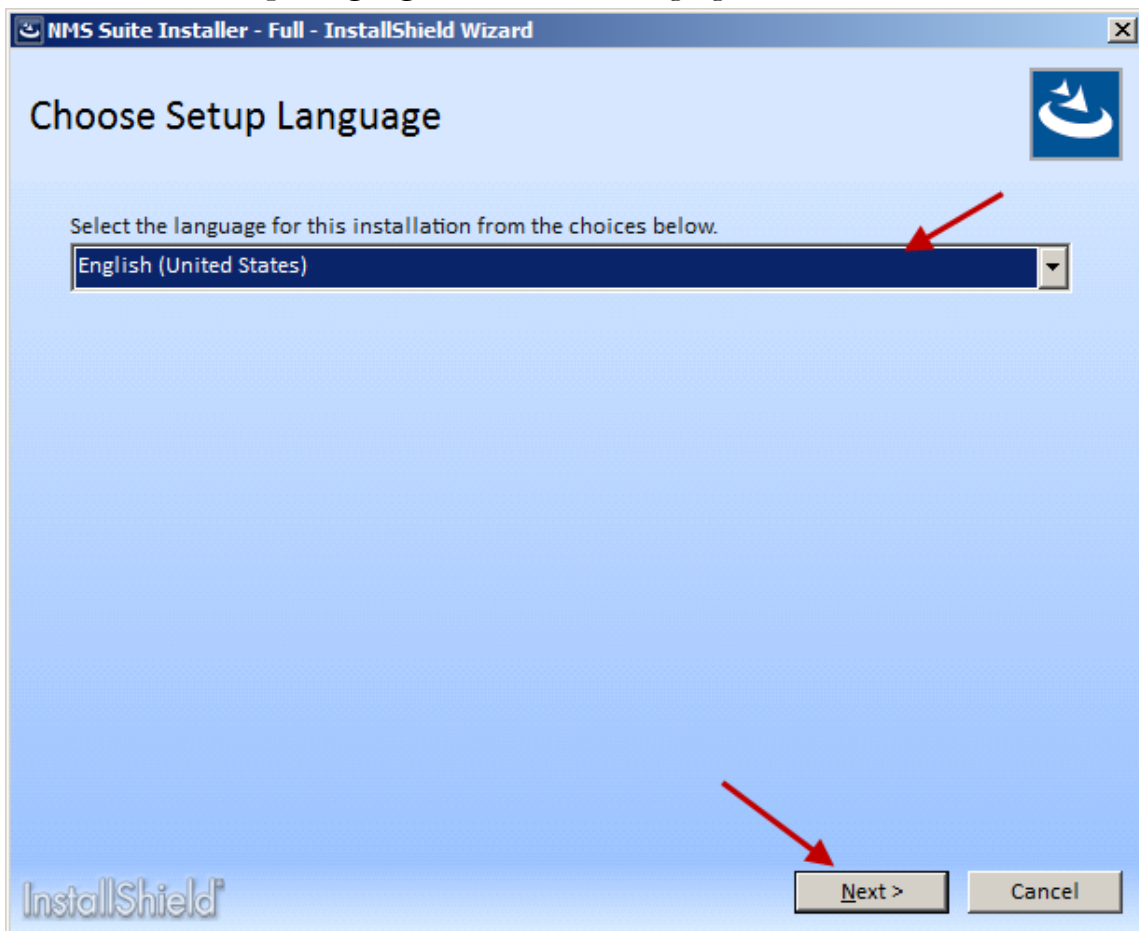
1. Procure an SSL certificate from a trusted certificate authority (CA).
2. Install the certificate on the NMS server, binding the certificate to the standard SSL port (443).

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 NMS servers.

Install the NMS software

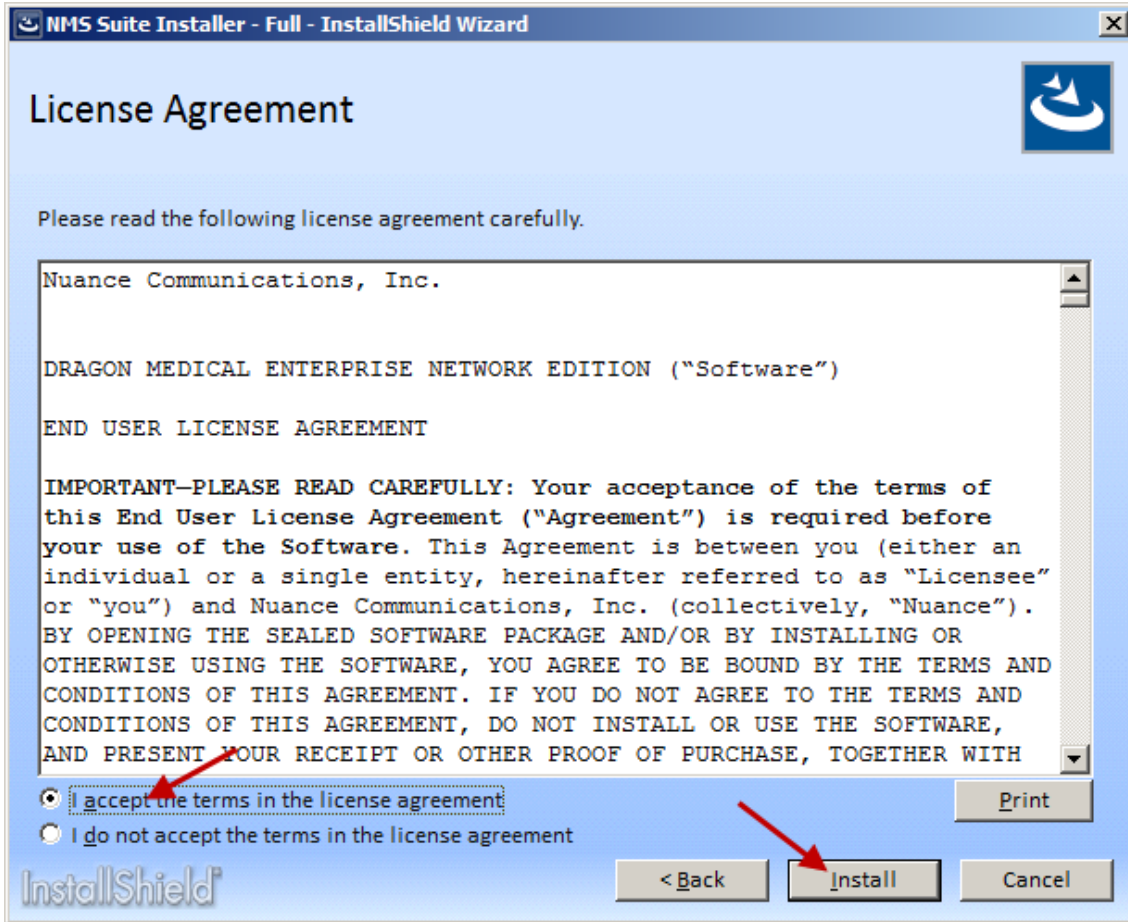
1. (Single-node only) On the NMS server, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.
or
(Multiple-node only) On each NMS node, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.
2. On the **Choose Setup Language** screen, select a language, and click **Next**.



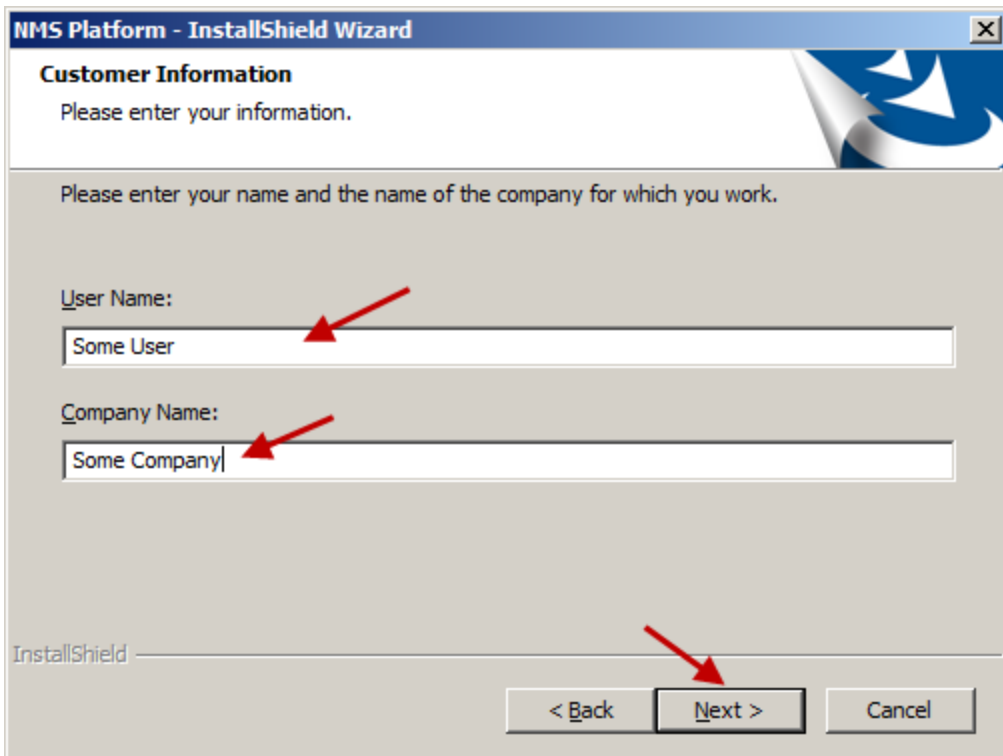
3. On the **Welcome** screen, click **Next**.



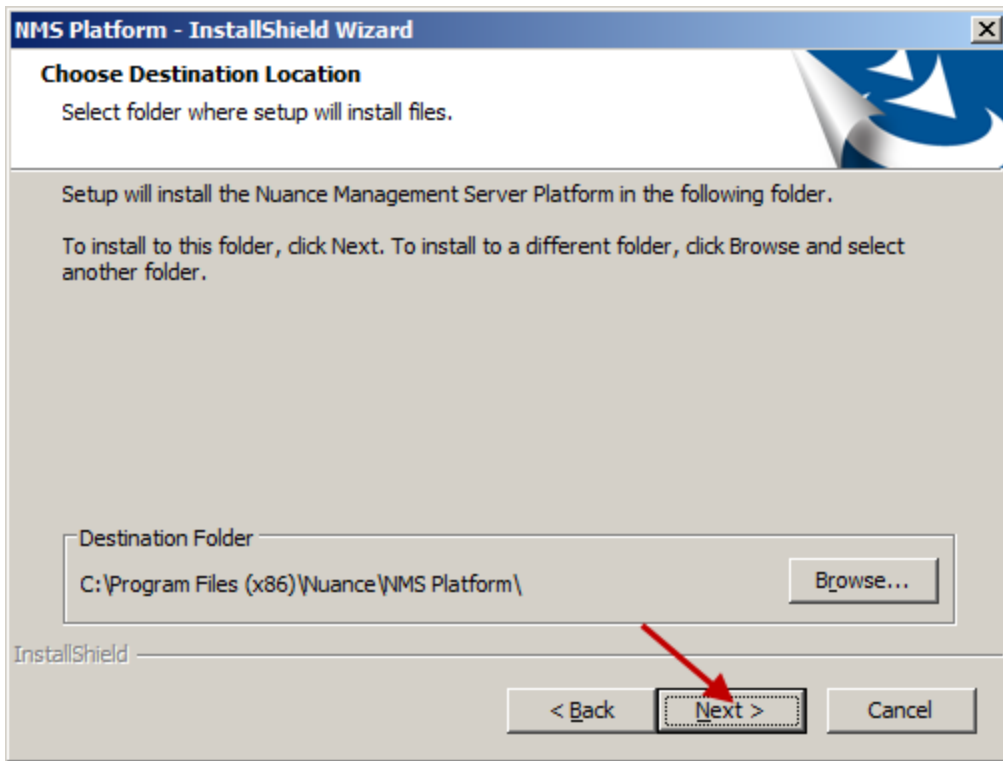
4. On the **License Agreement** screen, accept the agreement, and click **Install**.



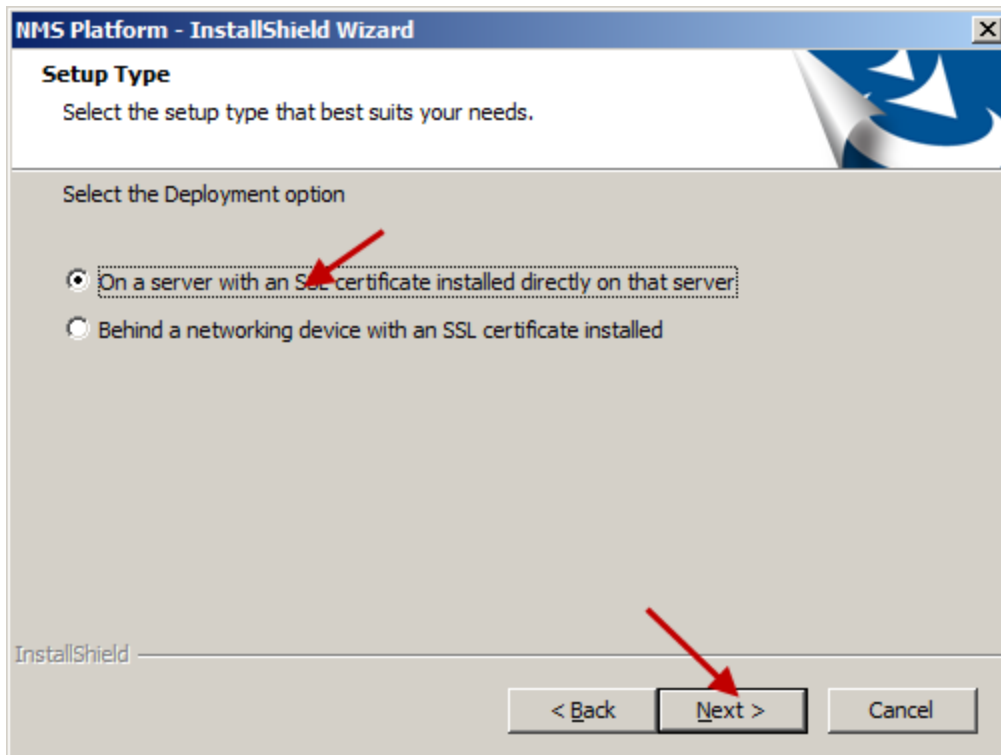
5. On the **Customer Information** screen, enter a user name and company name, and click **Next**.



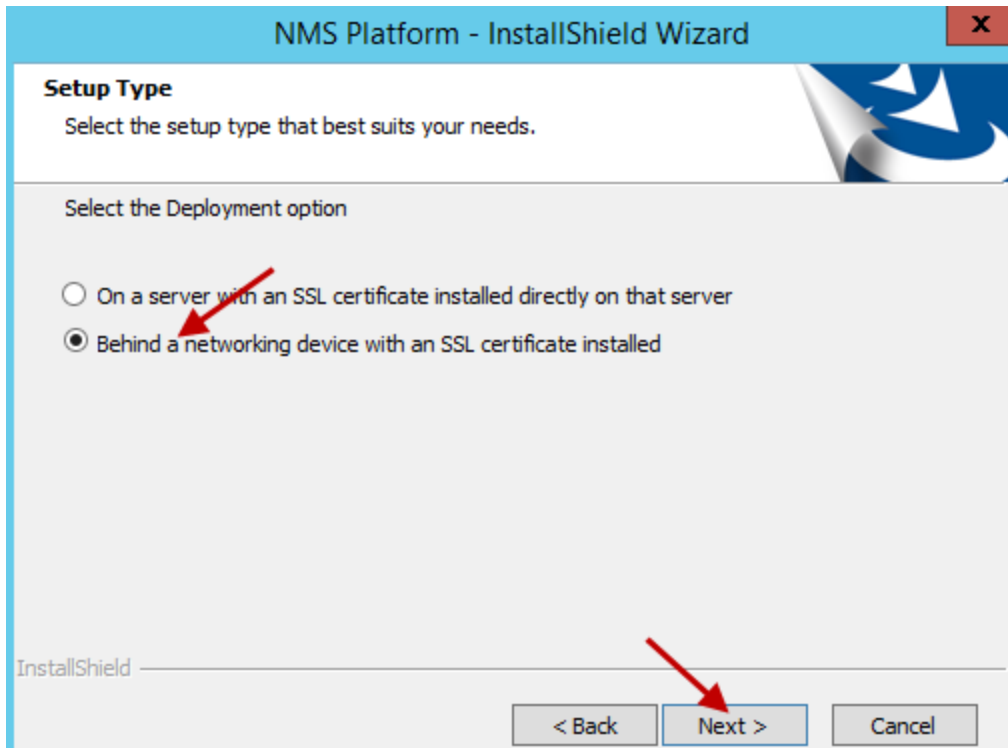
6. On the **Choose Destination Location** screen, accept the default or use the **Browse** button to select a location, and click **Next**.



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**.



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



10. 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.

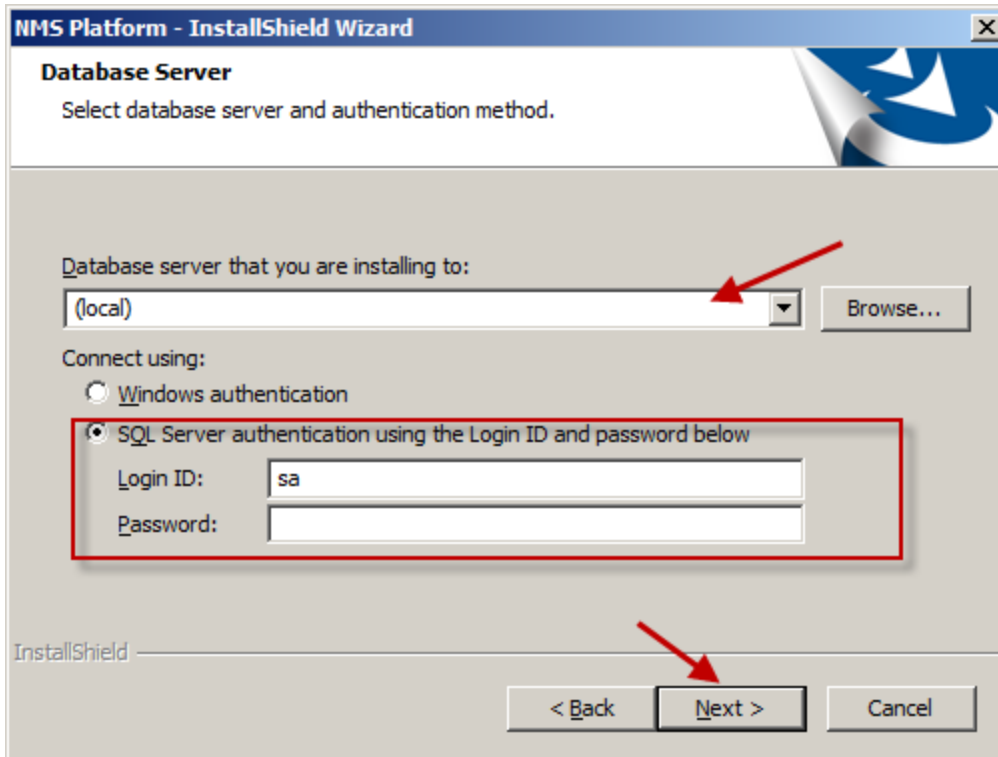
Under **Connect using**, you see from two ways for the server to access the database—using a Windows login and password to authorize access, as indicated by **Windows authentication** or an SQL Server login and password, as indicated by **SQL Server authentication**.

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.

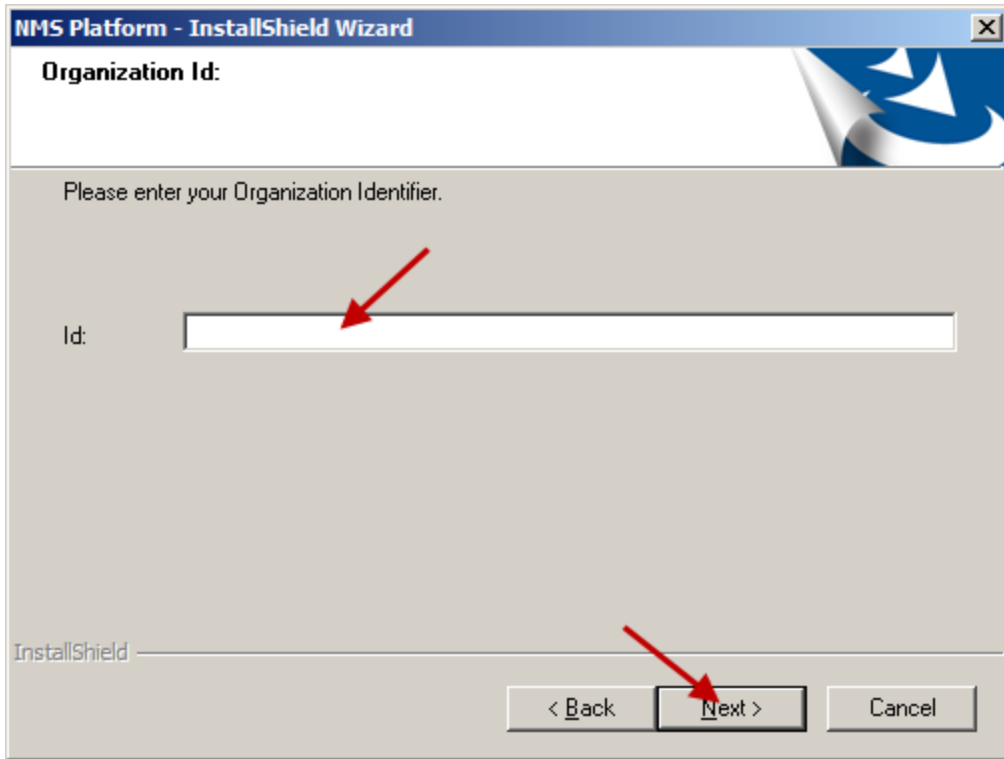
Click **Next**.



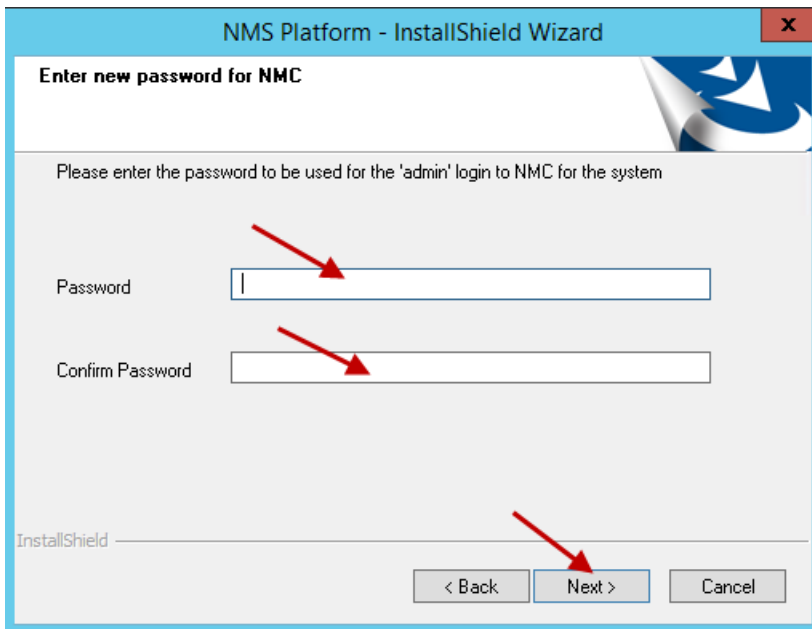
11. In the **Organization Id** screen, enter the unique ID that Nuance has assigned you. You should receive this ID on a slip of paper inserted with your *Dragon Medical Network Edition* software package. Carefully enter the ID into the **ID** text box here. You do not have to write it down or keep track 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 *Nuance Management Center*.

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

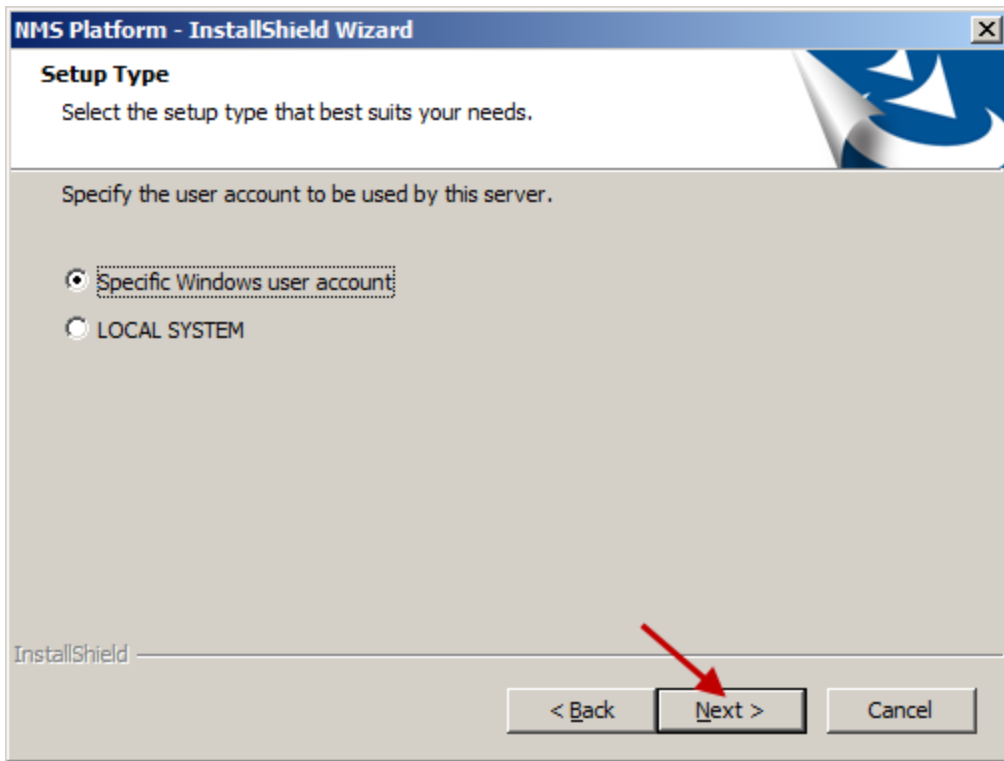
tion Administrator guide.



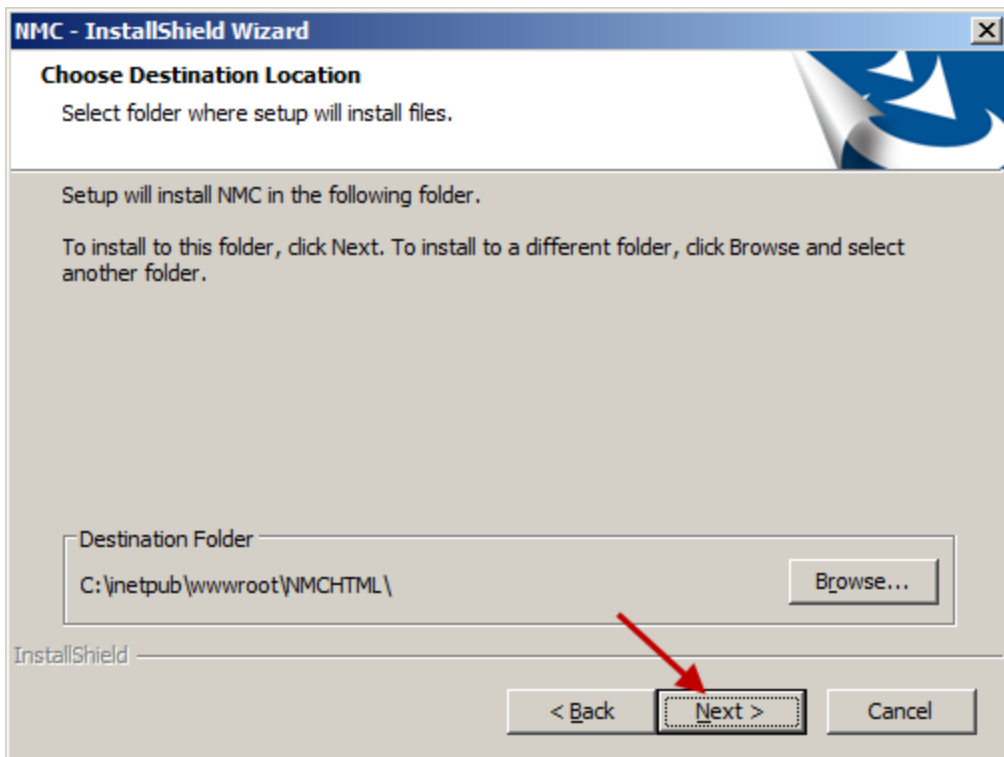
12. On the **Enter new password for NMC** screen, enter the password for the default administrator account, and click **Next**. Note: When an administrator logs into the Nuance Management Center for the first time, the administrator uses the "admin" login ID and the password you enter in the **Enter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



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



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



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



If you installed the *NMS Server* and *Nuance Management Center* with the Windows Server 2008, 2012, or 2012 R2 firewall turned on during the installation, you must now open Port 443 so that the *Nuance Management Center* can communicate with the *NMS Server*.

16. In a supported browser, go to <https://servername/nmhtml>.
17. Log into the Nuance Management Center using the "administrator" ID and the password you entered in the setup process.
18. 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 Nuance Management 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 Nuance Management Center 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 NMS 5.1

This topic is for customers that are running an NMS 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 2.5 client.

Notes:

- All installations of NMS 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
- Supported versions of Windows:
 - Windows 2008 R2
 - Windows Server 2012
- .NET Framework 4.5 is required on both the NMS server and PO Speech Nodes.

Prerequisites

- A SQL Server to install the NMS 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 NMS 5 and later.
- The Nuance Management Server installation: "NMS 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

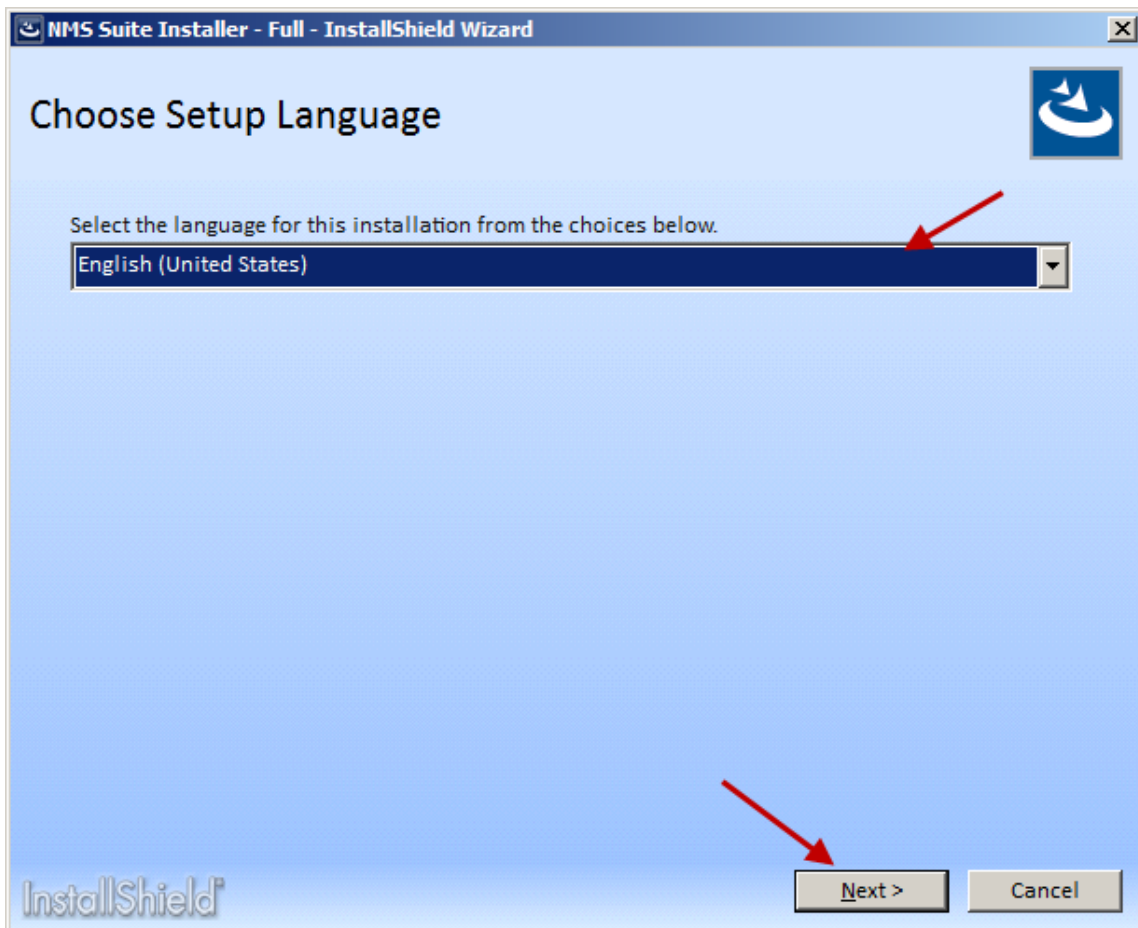
1. Bind the SSL certificate to the standard SSL port (443). If you have installed your 4.x system with SSL previously, you can use the same certificate for NMS 5 and later.

Install the SSL certificate for a multiple-node configuration

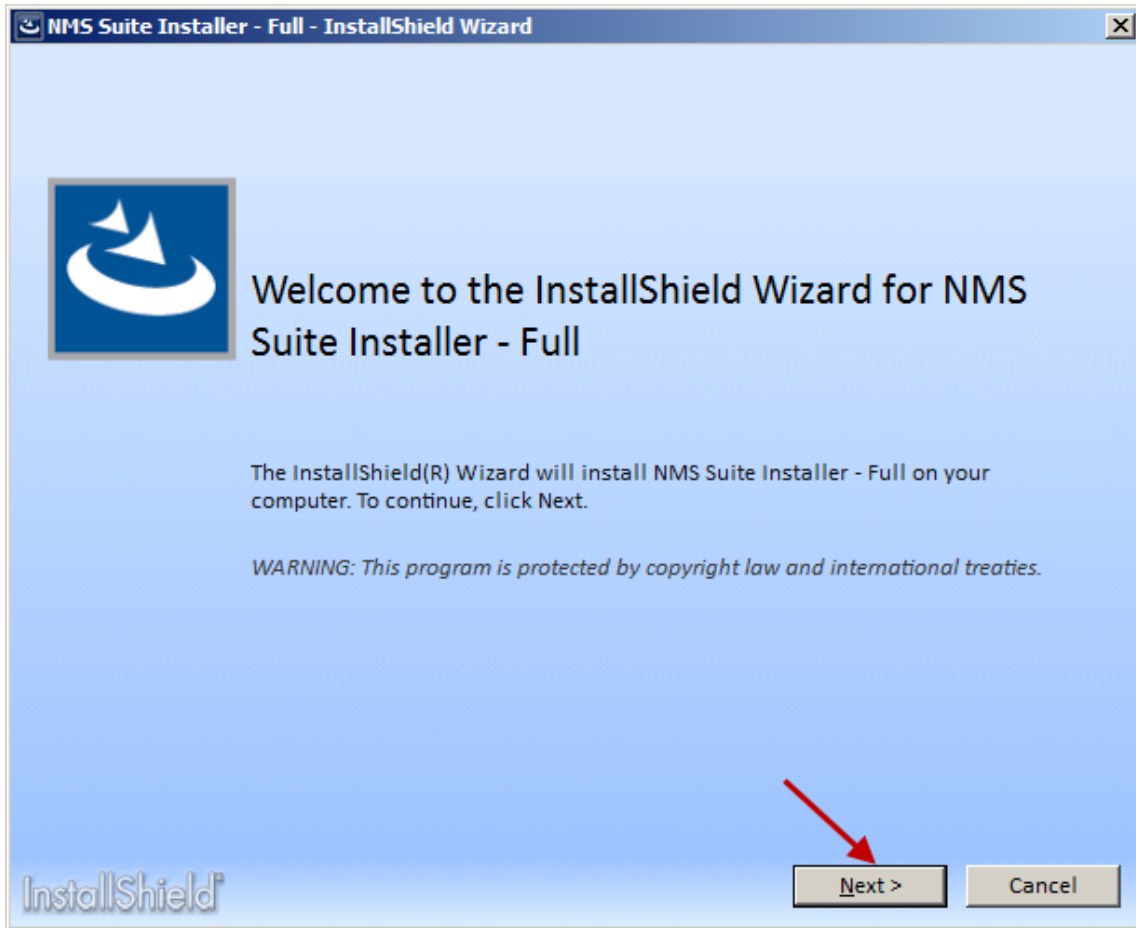
1. Install (or configure) the certificate on your load balancing switch.
2. If you have installed your 4.x system with SSL previously, the same certificate can be used for NMS 5 and later.
3. Forward decrypted traffic to port 80 on the NMS servers.

Install the NMS software

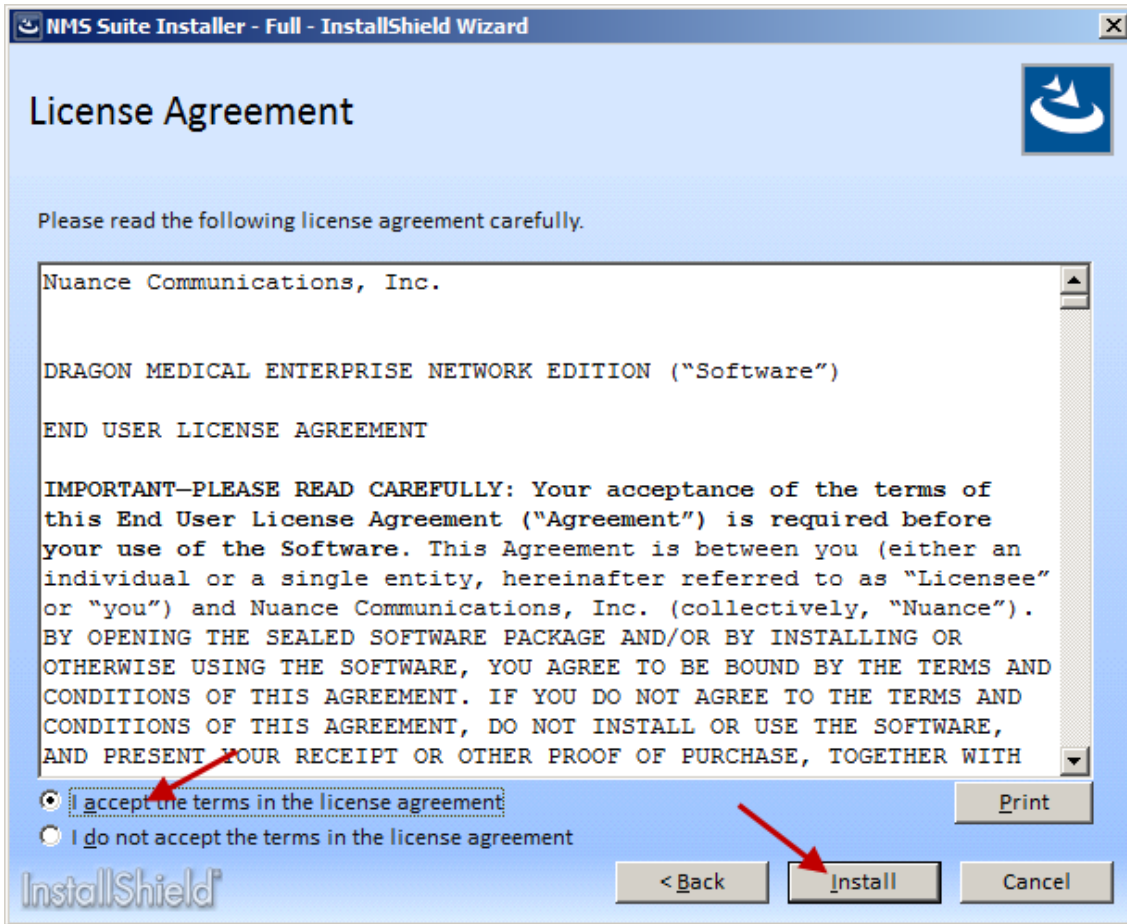
1. (Single-node only) On the NMS server, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.
or
(Mutli-node only) On each NMS node, run the "NMS Suite Installer - Full" installation - NMS_SuiteInstaller.exe.
2. On the **Choose Setup Language** screen, select a language, and click **Next**.



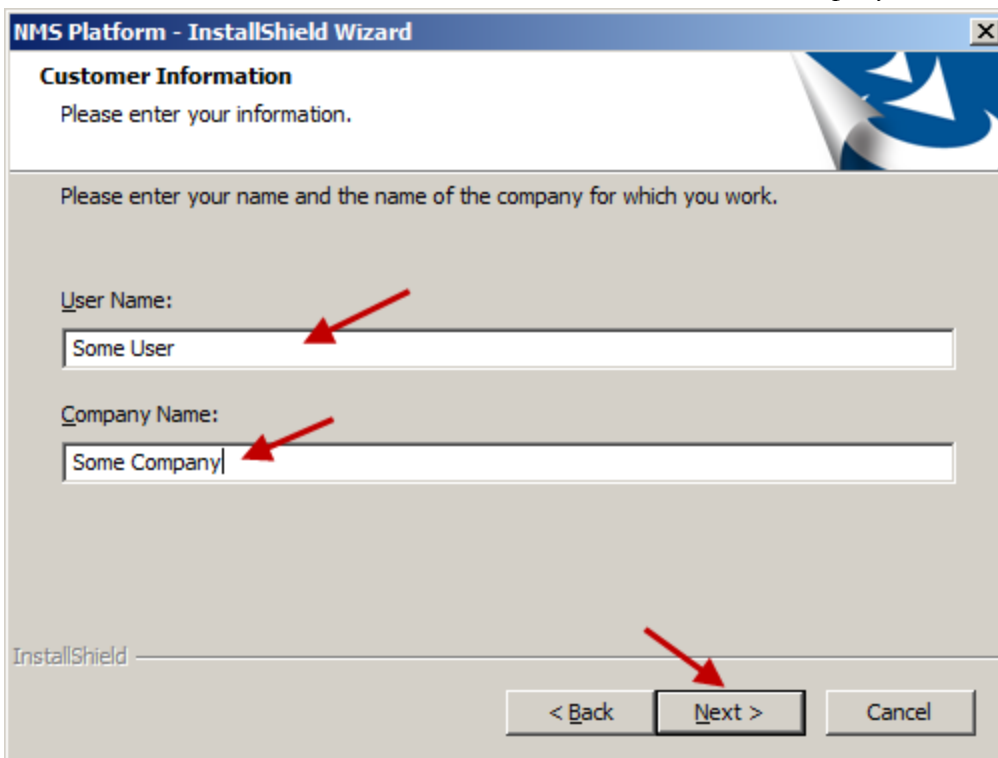
3. On the **Welcome** screen, click **Next**.



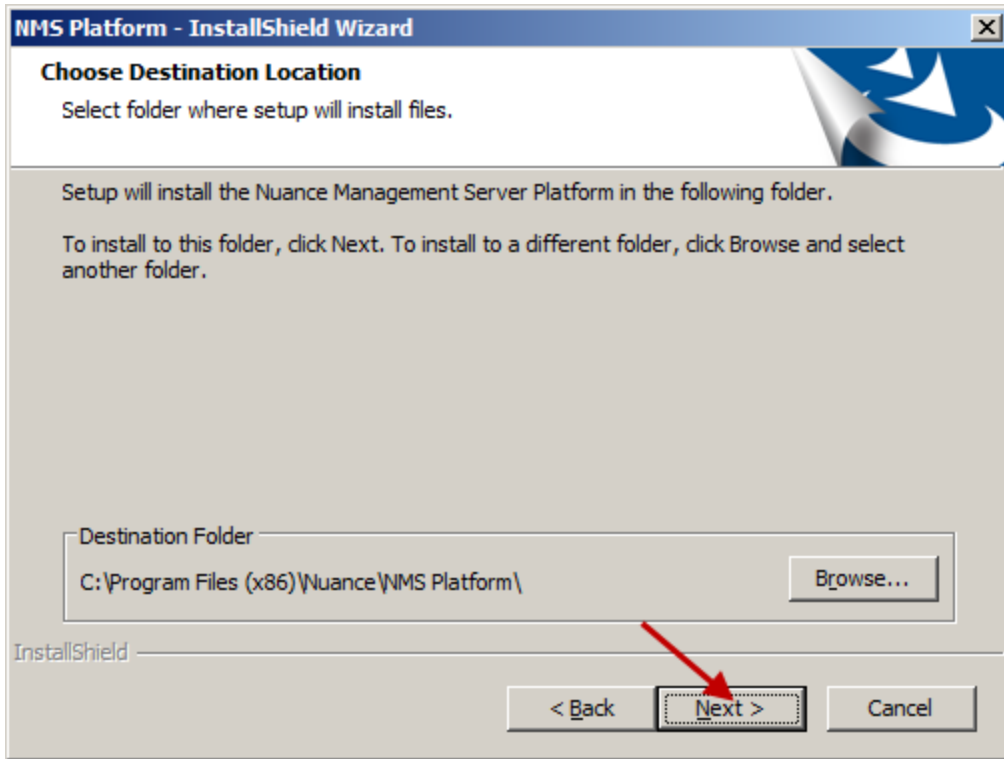
4. On the **License Agreement** screen, accept the agreement, and click **Install**.



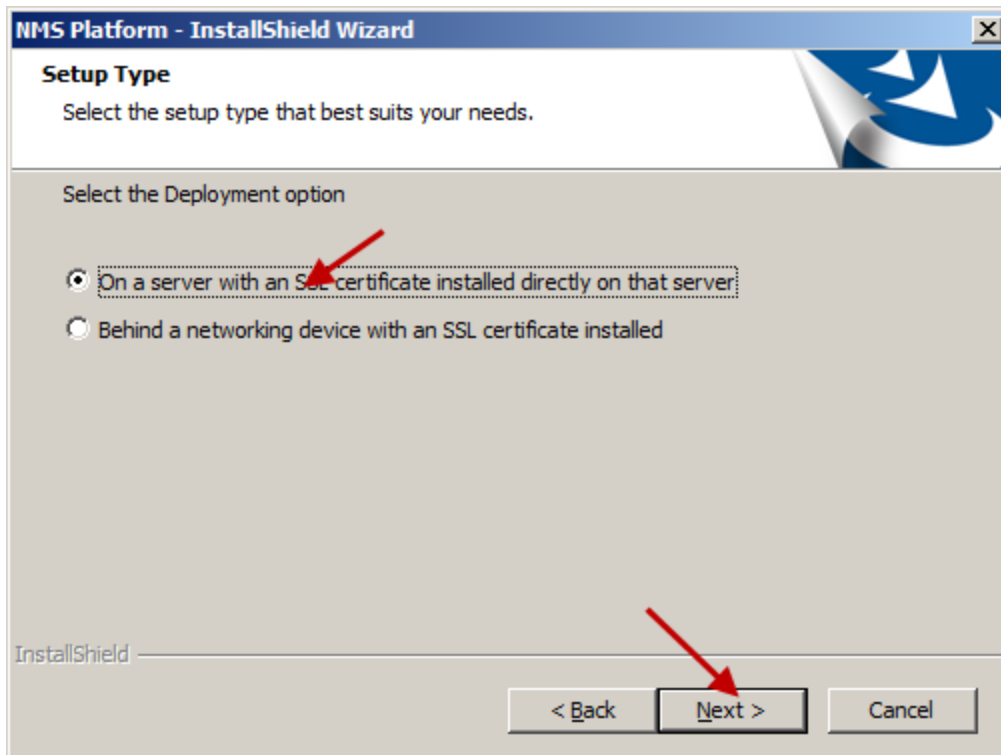
5. On the **Customer Information** screen, enter a user name and company name, and click **Next**.



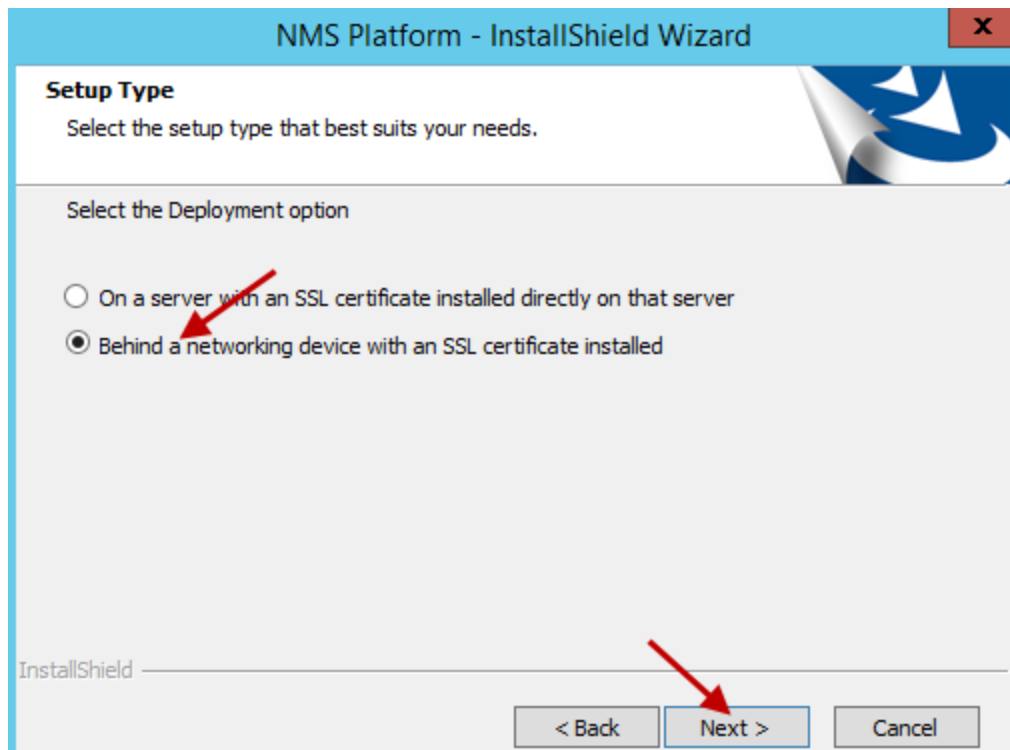
6. On the **Choose Destination Location** screen, accept the default or use the **Browse** button to select a location, and click **Next**.



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.

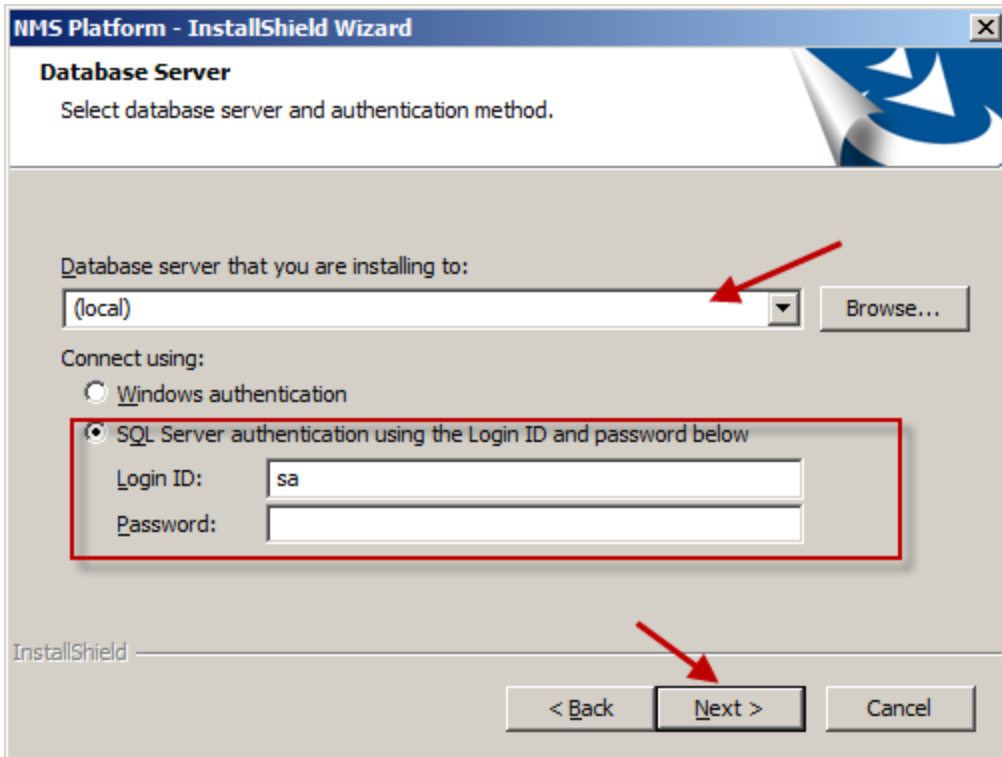
Under **Connect using**, you see from two ways for the server to access the database—using a Windows login and password to authorize access, as indicated by **Windows authentication** or an SQL Server login and password, as indicated by **SQL Server authentication**.

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

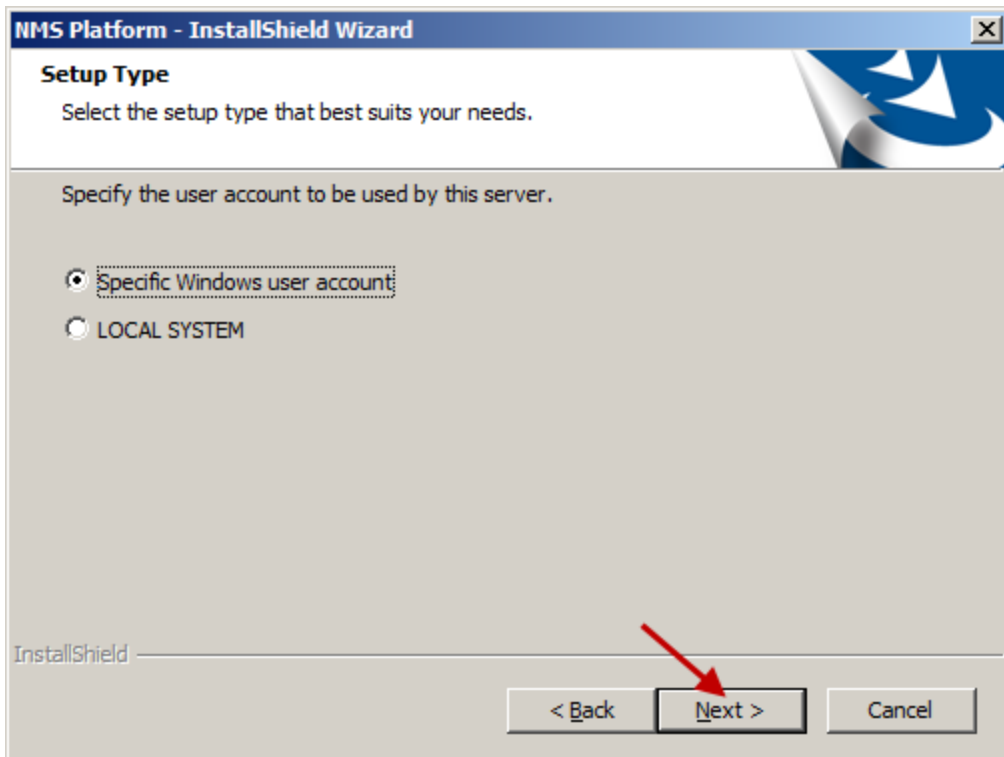
Nuance recommends **Windows authentication**. If you choose this type of authentication, the **Login ID** and **Password** text boxes become unavailable, as they are not required.

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**.

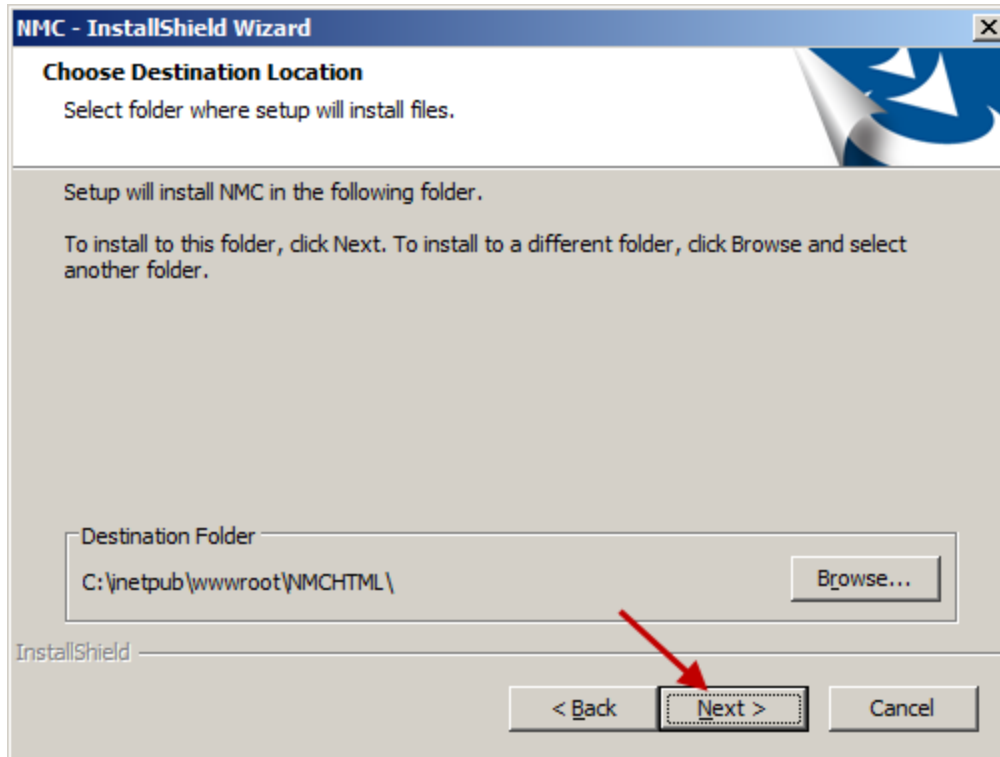


9. On the **Setup Type** screen, select the account that the NMS windows service runs under, and click **Next**. The install wizard installs several components.



10. On the **NMC - InstallShield Wizard - Choose Destination Location** screen, select the location where the install wizard installs the Nuance Management Center (default recommended),

and click **Next**.



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



If you installed the *NMS Server* and *Nuance Management Center* with the Windows Server 2008, 2012, or 2012 R2 firewall turned on during the installation, you must now open Port 443 so that the *Nuance Management Center* can communicate with the *NMS Server*.

12. Log into the Nuance Management Center with your existing administrator account.
13. On your existing Profile Optimizer Server:
 - i. On all Profile Optimizer 4.x speech nodes, stop the Profile Optimizer Speech Node service.
 - ii. On the Profile Optimizer 4.x server, stop the Profile Optimizer Speech Node service.
 - iii. On the Profile Optimizer 4.x server, run the [Profile Optimizer Server Migration Tool](#).
14. On each Profile Optimizer 4.x speech node, run the Profile Optimizer Speech Node installation. See [Installing prerequisite software for speech nodes](#) and [Installing the speech nodes](#).
The NMS now only communicates with the new Profile Optimizer speech node. The 4.x Profile Optimizer server is no longer required.

Run the Profile Optimizer Server Migration Tool

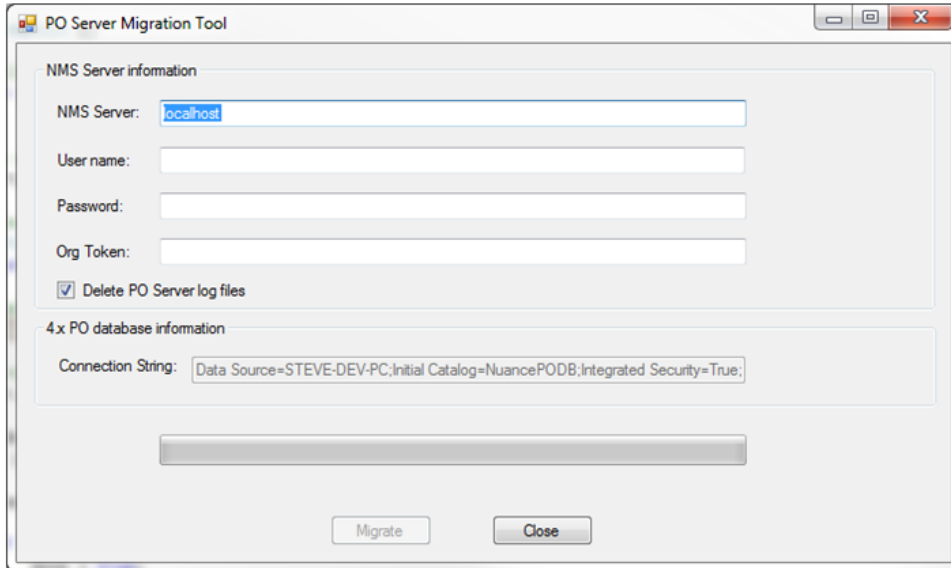
Use the PO Server Migration Tool to migrate data from the Profile Optimizer server database to the Nuance Management Server 5.1 database.

Requirements

- The Profile Optimizer Server Migration Tool runs on the 4.x Profile Optimizer server.
- 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 Nuance Management 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:



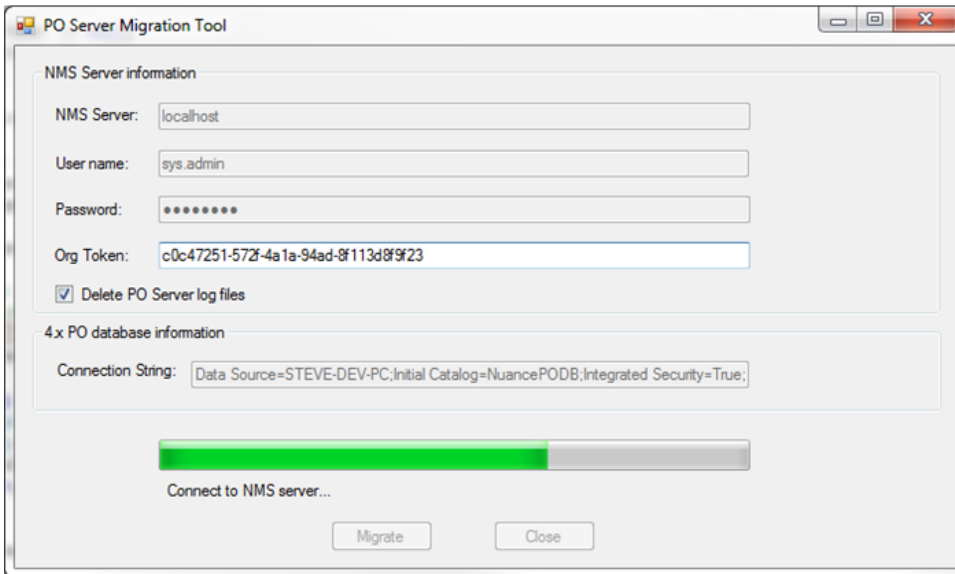
The screenshot shows a window titled "PO Server Migration Tool". It contains two main sections for data entry:

- NMS Server information:** Includes text boxes for "NMS Server" (pre-filled with "localhost"), "User name", "Password", and "Org Token". A checkbox labeled "Delete PO Server log files" is checked.
- 4x PO database information:** Includes a text box for "Connection String" with the value "Data Source=STEVE-DEV-PC;Initial Catalog=NuancePODB;Integrated Security=True;".

At the bottom of the window, there are two buttons: "Migrate" and "Close".

- **NMS Server:** The name of the NMS 5.1 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.



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	86
Installing prerequisite software for speech nodes	87
Installing the speech nodes	89
Installing Profile Optimizer Speech Nodes on independent or virtual machines	92
Anti-virus recommendations and requirements	92

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 3.1 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 3.1 or greater on it. (Windows Server 2008 and Windows Server 2012 automatically install 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 *Nuance Management 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 7 for a list of required software.
 - Windows Server 2012 R2
 - Windows Server 2008 R2: On all machines where Speech Nodes will run on Windows Server 2008 R2 (with or without Service Pack 1), download and apply the following patch:
http://hotfixv4.microsoft.com/Windows%207/Windows%20Server2008%20R2%20SP1/sp2/Fix392120/7600/free/445413_intl_x64_zip.exe

Please see the following Microsoft Support articles for information about why this hot fix is necessary for reliable operation of a Speech Node on Windows Server 2008 R2:

<http://support.microsoft.com/kb/2687753>
<http://support.microsoft.com/kb/2624677>
<http://support.microsoft.com/kb/2584874>

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 or 2012 R2 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.

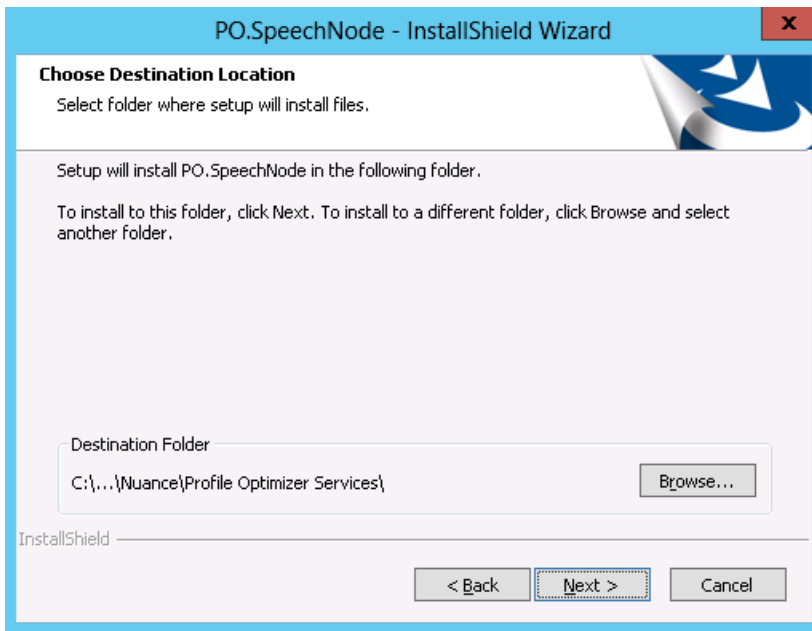
Installing Dragon Medical SDK Client Edition

You can find the *Dragon Medical SDK Client* software on the *Nuance Management 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:

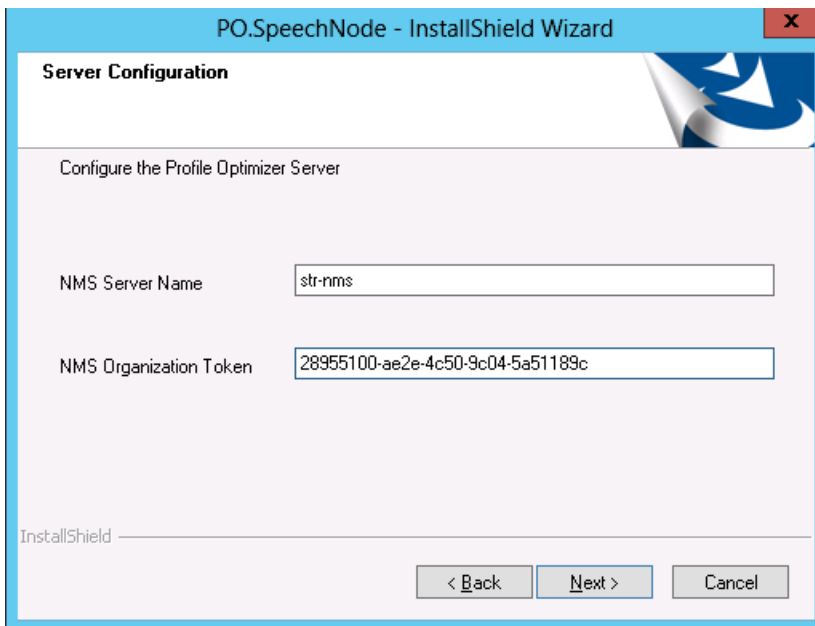
1. In the **Dragon Medical SDK Client** directory of the *Nuance Management Server Software and Documentation* DVD, find the **Dragon SDK Client Edition 14.msi** file and double click it.
2. Click **Next** and, when choosing the type of installation, be sure to select **Typical/Complete**.
3. Click **Next** until you reach the installation page of the wizard.
4. Click **Install**.
5. When the installation is complete, click **Finish**.

Installing the speech nodes

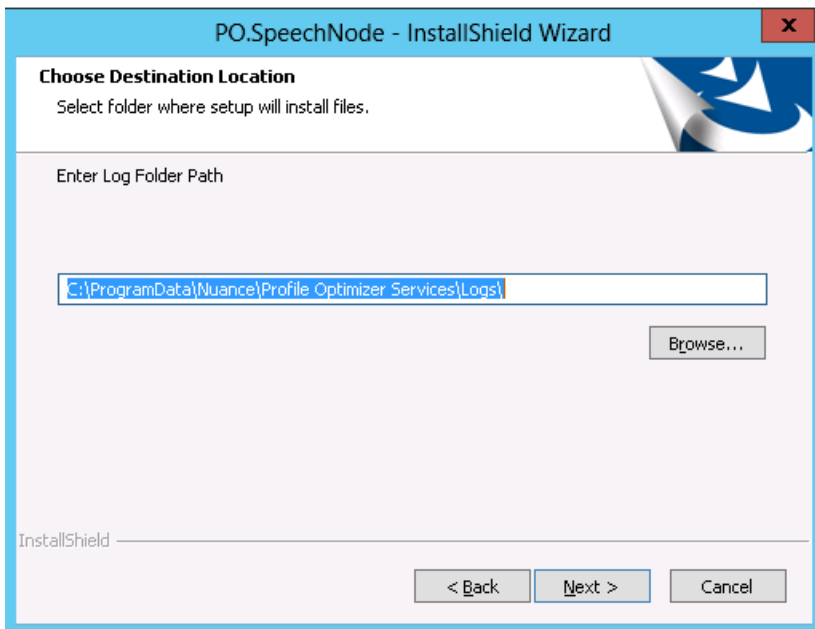
1. Before you install, you will need an Organization Token. The Organization token is required for both NMS in the cloud or an on-premise NMS. If you are using (or migrating to) NMS in the cloud, Nuance creates the Organization token for your organization and provides it to you. If you are using an on premise NMS, 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**.



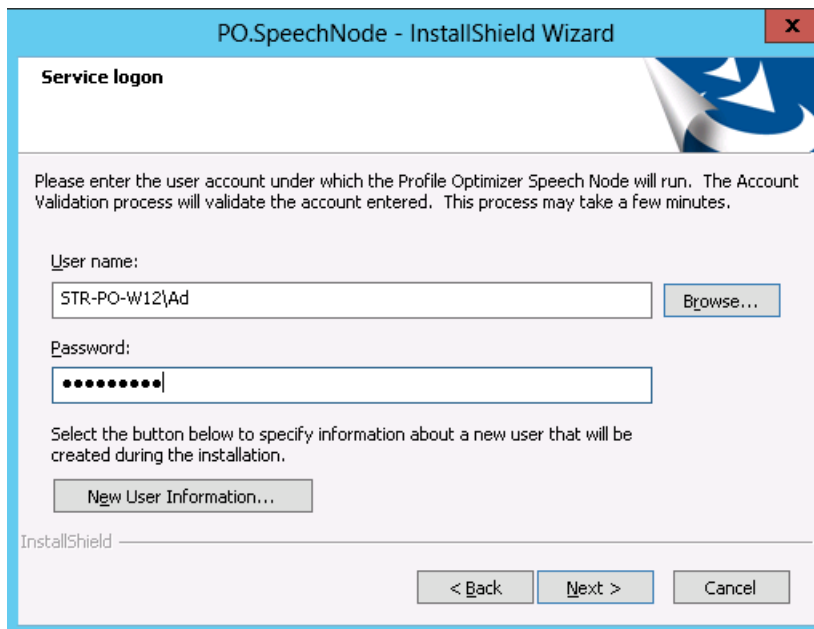
5. On the **Configure the Profile Optimizer Server** screen, enter the NMS Server Name and Organization Token.



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 NMS Server under, and that you assign an appropriate name, such as NMSapps, 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](#).

Anti-virus recommendations and requirements

Nuance recommends anti-virus software on all *Dragon Medical Network Edition* servers and clients to protect the system from potential downtime due to viruses. However, be aware of the recommended restrictions.

After you have installed the servers, be sure to exclude from the anti-virus scan any files found in the folders indicated below or with the extensions listed below.

On NMS Servers and the SQL Database Server:

- **Nuance** folder and all sub-folders
- Files with these extensions:
DAT, DRA, ENH, INI, LCK, LOG, NWV, SIG, TXT, USR, VER, VOC, WAV

Chapter 5: Starting servers and logging in to the Nuance Management Center

Logging in to the Nuance Management Server through the Nuance Management Center	94
Starting the Nuance Management Server	95
Starting Profile Optimizer Speech Nodes	96
Anti-virus recommendations and requirements	99

Logging in to the Nuance Management Server through the Nuance Management Center

See 'Accessing the Nuance Management Center' in the Administrator guide.

Starting the Nuance Management Server

After the *NMS* 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 *NMS Server*, and all *Speech Nodes* and the machine hosting the master user profiles directory.

Caution:

The account running the services for the *NMS 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 NMS Server

If you had no trouble entering the user account the server should run under during the *NMS Server* installation, skip to the next subsection, *Starting NMS Server service* on page 95.

If during the installation you were forced to change the account that the *NMS 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 **NMSapps**):

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 NMS Server service

After you are sure you have all the necessary privileges, to start *NMS Server* service:

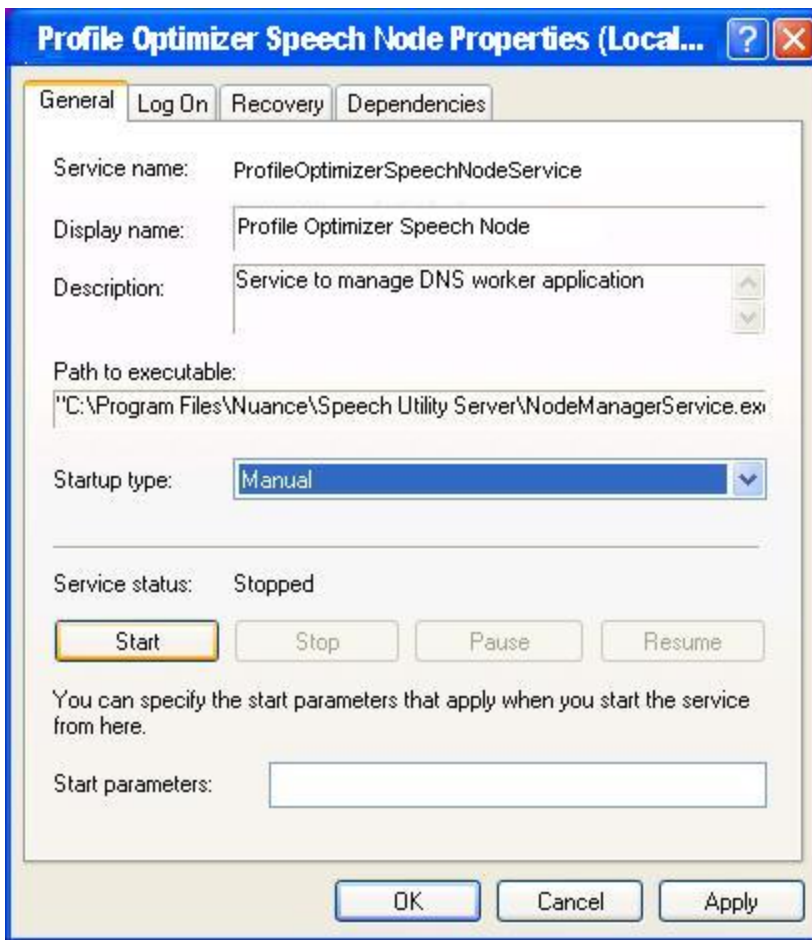
1. Click **Start > Control Panel** and double click **Administrative Tools**, then double click **Services**.
2. In the **Services** list, find the **Nuance Management Service**.
3. To start the service, right click on the service name to open its **Nuance Management Service Properties** dialog box.
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.



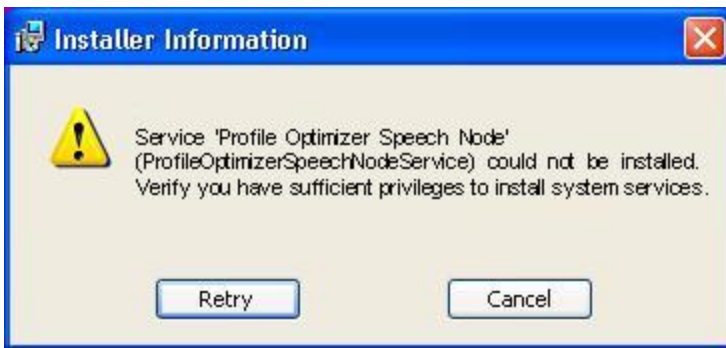
4. In the **Startup type** drop-down list, if the service is not already set to start automatically, select **Automatic**.
5. Under **Service status**, click the **Start** button to the left.
6. After the **Service status** says **Started**, you can click **OK** and close the dialog box.

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.

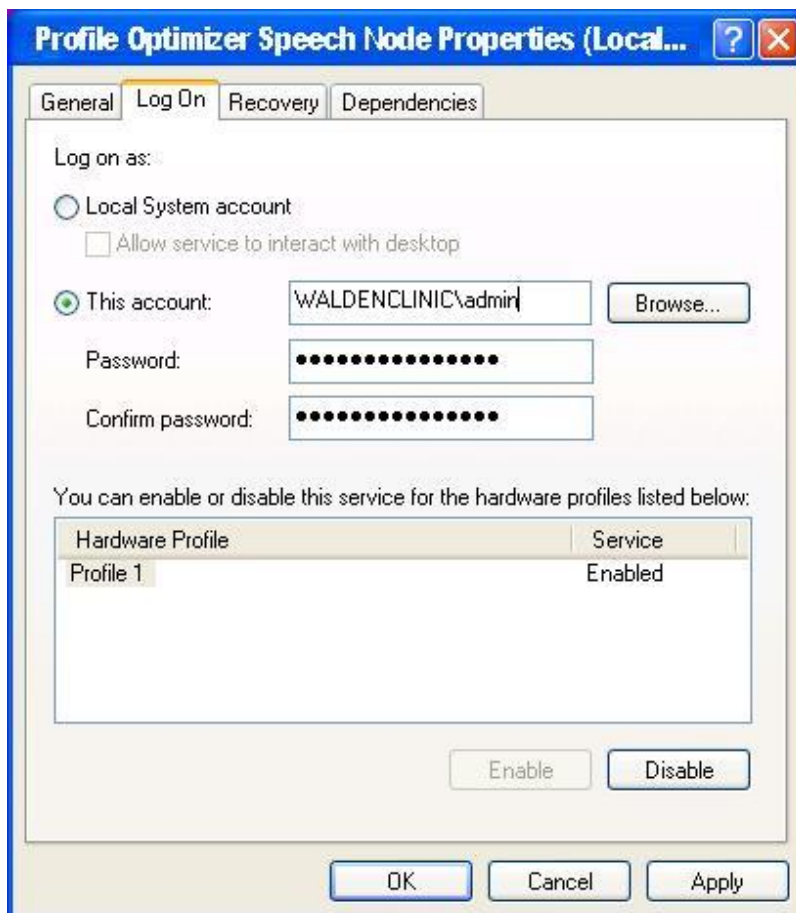
By default, the installation grants you **Log on as Service** level privileges.

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.

Anti-virus recommendations and requirements

Nuance recommends anti-virus software on all *Dragon Medical Network Edition* servers and clients to protect the system from potential downtime due to viruses. However, be aware of the recommended restrictions.

After you have installed the servers, be sure to exclude from the anti-virus scan any files found in the folders indicated below or with the extensions listed below.

On NMS Servers and the SQL Database Server:

- **Nuance** folder and all sub-folders
- Files with these extensions:
DAT, DRA, ENH, INI, LCK, LOG, NWV, SIG, TXT, USR, VER, VOC, WAV

Chapter 6: Setting up the Master User Profiles machine

Choosing a master user profiles location for a site	102
Setting up a computer to host master user profiles	105
Installing software for storing master user profiles on a web server	108
Setting HTTP connection settings for web server	119
Setting SSL connection settings for secure web server	122
Assigning access to folders and master user profiles across the network	125
Turning off Automatic Updates	125

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 *NMS Server* lets you store your 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.

Caution:

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 7

If you choose to use server, choose one of the supported web servers. See *System Requirements for Dragon Medical Network Edition* on page 7

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 *NMS 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 105
- *Mapping the disk drive on the client workstation* on page 105
- *Setting up access to the master user profile directory* on page 107

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 7 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 *NMS Server* and *Nuance Management Center*, 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.

Note:

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.

To store the master user profiles on one of the web servers below, first be sure you have .NET Framework 4.5 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 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 2.2.16 or higher on Windows Server 2008 and Windows Server 2012:

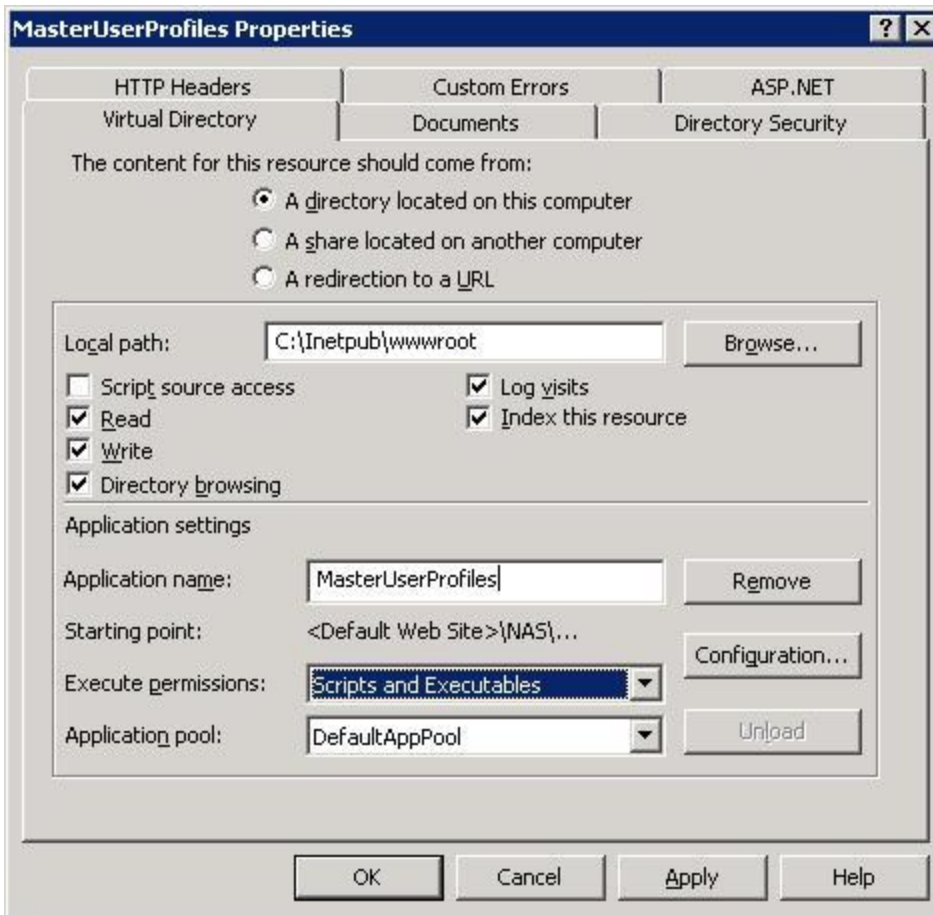
This server should run on Windows Server 2008 Core or Windows Server 2012 R2 and also runs

on Windows 7, 8.x, 10, Vista, or XP. 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/>

Entering settings under Virtual Directory or Home Directory tab



You should enter these settings under the **Virtual Directory** or **Home Directory** tab:

1. **The content for this resource should come from**—Select **A directory located on this computer**.
2. **Local path**—Enter the full path to the web site folder. If you use the default folder, the path is C:\Inetpub\wwwroot.
3. Check off the following check boxes under the local path to indicate the kind of access to the master user profiles you want to grant to the user accounts running the other services of the *Dragon Medical Network Edition* network:
 - **Read**
 - **Write**
 - **Directory Browsing**

- Log visits
 - Index this resource
4. **Application name**—You should see the name you gave to your virtual directory, in this case **MasterUserProfiles**.
 5. **Execute permissions**—Select **Scripts and executables** from the drop-down list. You need the option of running executables on the master user profiles so that the acoustic and language model optimization results can be integrated into the profiles. When you choose this selection, the **IIS Manager** warns you that you could be exposing the site, so be sure your firewall and other security precautions are adequate to protect the site from malicious attack.
To avoid giving permission to run scripts on the entire machine, be sure that you set the permissions to **Scripts and executables** only on the virtual directory, not on its parent directory.
 6. **Application pool**—Select **DefaultAppPool** from the drop-down list.
 7. Click **Apply** to apply the changes.

Entering settings under Directory Security tab

Under the **Directory Security** tab, you select **Basic authentication** for the virtual directory you created for your web server. You also view and verify certificate information that ensures the identity of the computer if you are installing the software on a remote computer, rather than locally.

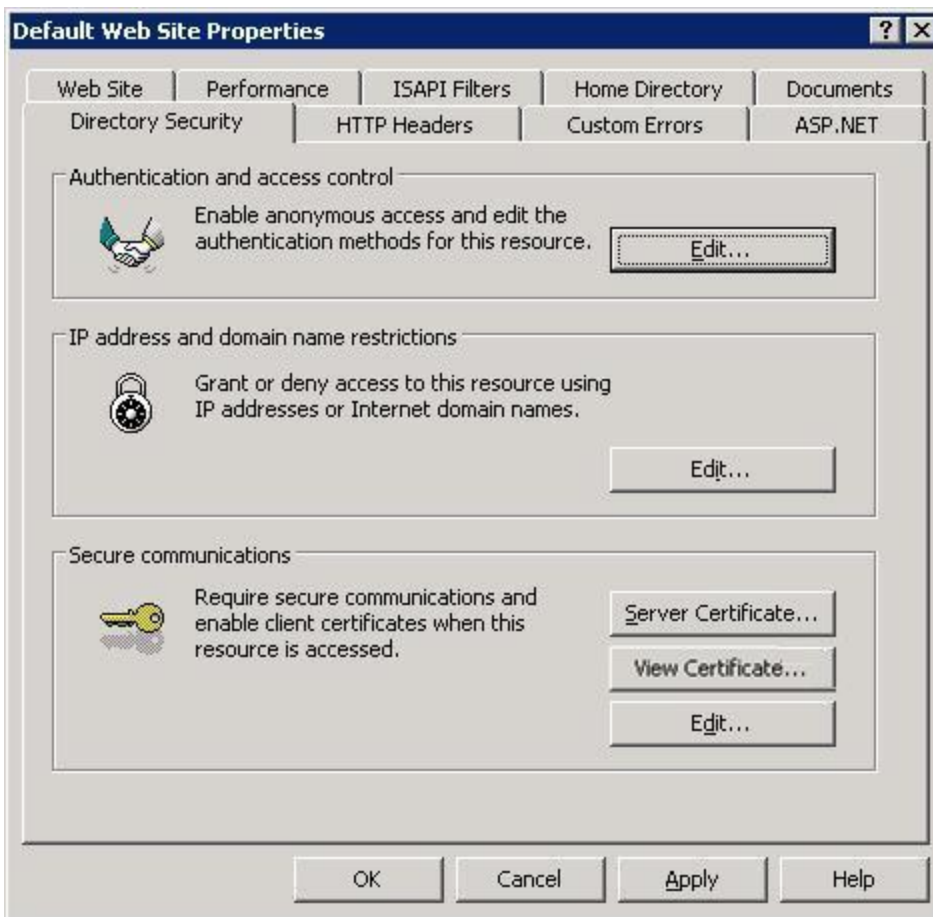
Caution:

Basic authentication transmits user names and passwords across the network in an unencrypted form. You must use your web server's encryption features to ensure the security of login information.

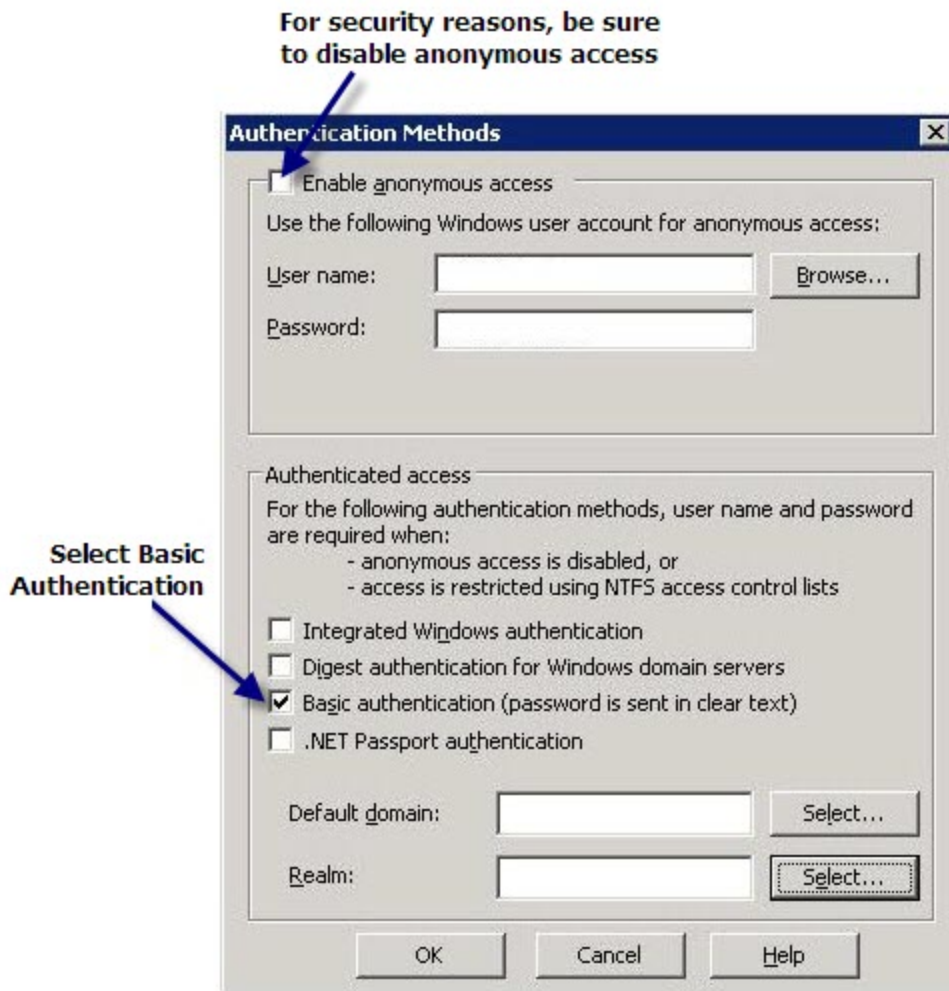
To use **Basic authentication** to control access to your web server, you grant each Windows administrator account that needs access the right to log on locally. (You can add each administrator to a group and then give the group access to the necessary files.)

Caution:

You should not give the right to log on locally to healthcare providers dictating with *Dragon Medical Client*. Only administrator level users should have log on rights to the web server hosting the master user profiles.



1. To enable **Basic Authentication**:
 - i. In the **Authentication and access control** section, click the **Edit...** button.
 - ii. When the **Authentication Methods** dialog box pops up, check off **Basic authentication**.



- iii. When you are warned that this type of authentication passes unencrypted passwords over the network, click **Yes** to proceed.
 - iv. Be sure that if you see a check mark in the check box for **Enable anonymous access** you click it to remove the check mark. For security reasons, you should not allow anonymous access.
 - v. Leave the **Default domain** text box empty to have the domain name be the name of the machine itself when a party accessing this web server does not provide the domain name.
 - vi. Click **OK** to save the changes and return to the **Directory Security** tab. If you are setting up a secure (SSL) web server, proceed to the next step. Otherwise, skip to step 5.
2. If you are setting up a secure (SSL) web server, for the web server to selectively allow only *Dragon Medical Client* machines access to the master user profiles, you need to require that the web server enable security certificates on any client that tries to access the web server. Take these steps:

- i. In the **Secure communications** section, click the **View Certificate...** button.
 - ii. When the **Certificate** dialog box pops up, under the **General** tab you should see **Certificate Information** indicating that this certificate's purpose is to ensure the identity of the remote system seeking access.
 - iii. Under the **Certification Path** tab, click the **View Certificate** button and again under the **General** tab you should see root **Certificate Information** that ensures the validity of all issuance and application policies.
3. If the **View Certificate...** button is not available, you can purchase an SSL certificates on the web and install it. The button should then become available. For more information on purchasing and installing an SSL certificate, you can visit http://www.rapidssl.com/index_ssl.htm or a similar site.
 4. For instructions on installing an SSL certificate, visit http://www.rapidssl.com/resources/install/chainedssl/MS_IIS5.html.
 5. Click **Apply** to apply all changes in the **Directory Security** tab and then click **OK** to close the dialog box.

Now that you have finished entering all of the settings for the web server, restart the World Wide Web Publishing Service or wait for the process to recycle for the changes to take effect.

Caution:

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.

Configuring HTTP or SSL settings in Nuance Management Center

Later, when you set up sites in the *NMS Server*, to set up access to the master user profiles, you enter HTTP settings for interacting with a non-secure web site or SSL settings for interacting with a secure web site. For details, refer to the related topics in the *Nuance Management Center Help* or the *Nuance Management Server Administrator Guide*.

For specific HTTP settings that you should enter in the **HTTP Settings** tab in the *Nuance Management Center* for this type of web server, refer to *Setting HTTP connection settings for web server* on page 119.

For specific SSL settings that you should enter in the **SSL Settings** tab in the *Nuance Management Center* for this type of web server, refer to *Setting SSL connection settings for secure web server* on page 122.

Example: Installing SSL certificates for IIS 6.0

1. After you have downloaded an SSL certificate for IIS, the **View Certificate...** button becomes available under the **Directory Security** tab.
2. Click the **View Certificate...** button to see the certificate and verify that it is valid. It should look something like the one shown below.



Note:

All certificates should be valid, not expired, free of errors, and properly signed.

3. Keep the certificate open and click the **Certification Path** tab to display the path to the certificate that *Dragon Medical Client* workstations will need to follow.
4. In the **Certification Path** tab, expand the path in the **Certification path** box. The **Certificate Status** text box near the bottom of the dialog box should say **This certificate is OK.**(See the next illustration.)



5. Click the next **View Certificate** button and view the certificate for **All Issuance and Application Policies** to be sure it was issued to the correct organization and is valid for the expected time period.
6. Install the **Root Certificate for All Issuance and Application Policies** (see previous illustration) on every *Dragon Medical Client* workstation and install it to **Trusted Root Certification Authorities**.

Caution:

If you do not install the above certificate on every *Dragon Medical Client* workstation, when the workstation attempts to access a master user profile on the web server, the provider will receive this error: **This Certificate cannot be verified up to a trusted certification authority.**

When you save the certificate, be sure to save it to *<PC-name>/<Site-name>* where the *PC-name* matches the name of the computer and the *Site-name* matches the name of the site you created in **IIS Manager**. Or you can save it to a name that matches the Active Directory host name.

Setting HTTP connection settings for web server

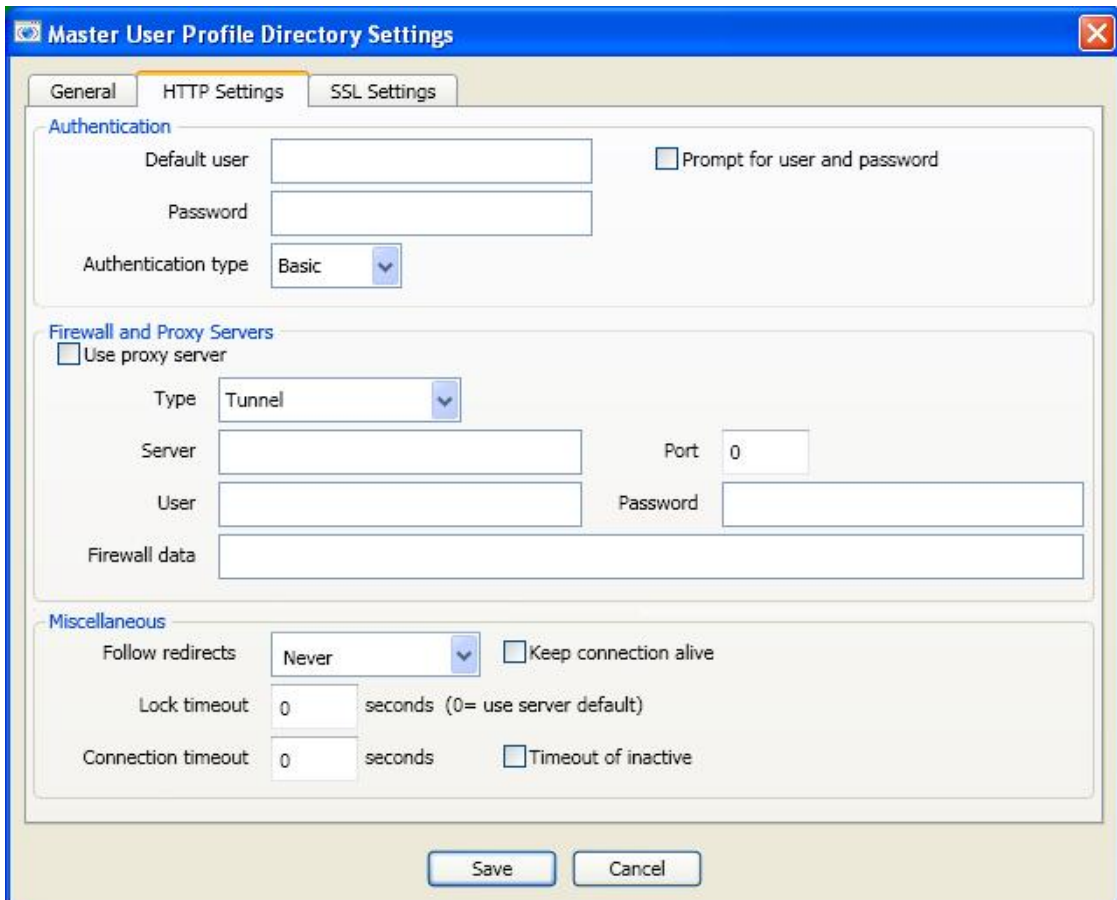
Caution:

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 *Nuance Management Center*. For details on how to set up a site, refer to the *Nuance Management Server Administrator Guide*.

Note:

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



The screenshot shows the "Master User Profile Directory Settings" dialog box with the "HTTP Settings" tab selected. The dialog is divided into three sections: Authentication, Firewall and Proxy Servers, and Miscellaneous.

- Authentication:** Includes fields for "Default user" and "Password", a "Prompt for user and password" checkbox (unchecked), and a dropdown menu for "Authentication type" set to "Basic".
- Firewall and Proxy Servers:** Includes a "Use proxy server" checkbox (unchecked), a "Type" dropdown menu set to "Tunnel", and fields for "Server", "Port" (set to 0), "User", and "Password". There is also a "Firewall data" field.
- Miscellaneous:** Includes a "Follow redirects" dropdown menu set to "Never", a "Keep connection alive" checkbox (unchecked), "Lock timeout" and "Connection timeout" fields both set to 0 seconds (with a note "(0= use server default)"), and a "Timeout of inactive" checkbox (unchecked).

At the bottom of the dialog are "Save" and "Cancel" buttons.

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 6.0, 7.0, or 7.5	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 <i>Dragon Client</i> accesses master user profiles.
Default user	Empty		Enter username for the account that the servers run under, such as NMSapps .
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.
Keep connection	Off		Could be turned on even if turned off for the site. If

Web Server Type & Version	Default Values for IIS 6.0, 7.0, or 7.5	Default Values for Apache 2.0.xx or 2.2.xx	Other Considerations Based on Your Site Configuration
alive			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:

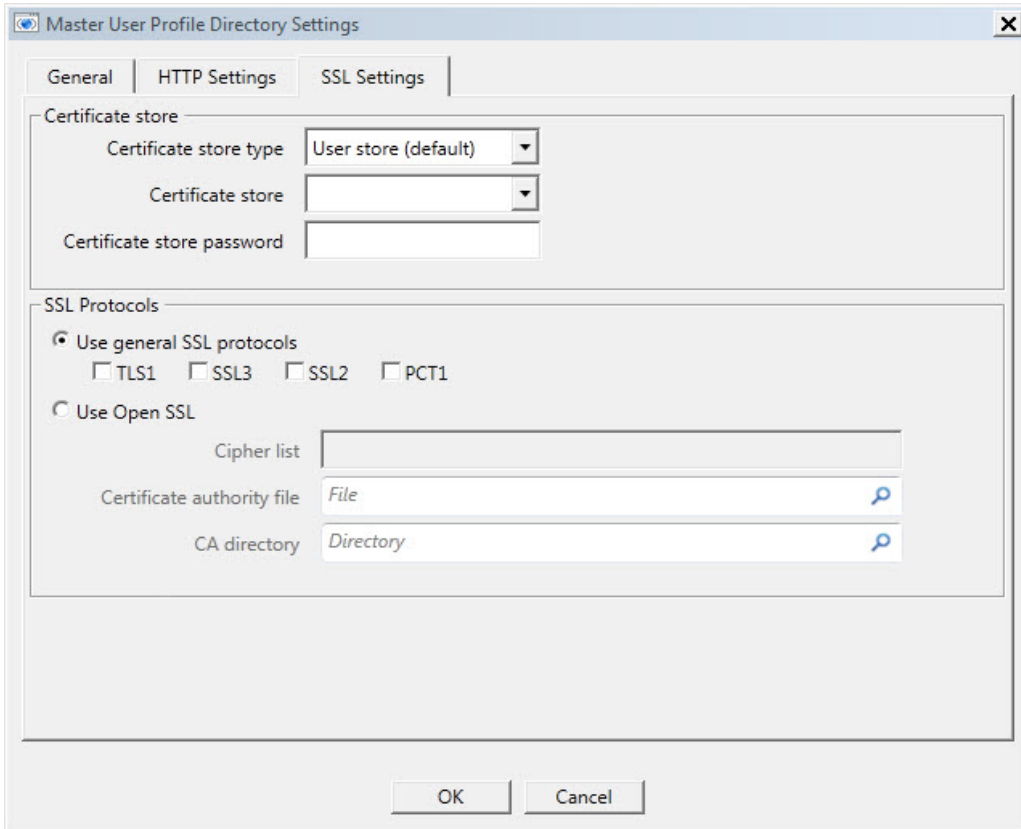
If you have never set up a secure web server before, do not attempt to do so; these instructions assume you have experience setting up a secure web server. Appropriate settings vary. Be sure that you install an SSL certificate that is trusted for directory on every workstation. You should push install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

After you install your secure web server, you must set SSL connection settings in the *Nuance Management Center*. For details on how to set up a site, refer to the *Nuance Management 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 6.0, 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 protocols	On	On	Check all protocols your server might receive legitimate input from: TLS1 , SSL3 , SSL2 , and

Web Server Type & Version	IIS 6.0, 7.0, or 7.5	Apache 2.0.xx or 2..xx	Other Considerations Based on Your Site Configuration
			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 <i>Nuance Management Server Administrator Guide</i> 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 profile locations* on page 18. 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	128
Creating user accounts for healthcare providers	131
Migrating Non-Network Dragon User Profiles to the Nuance Management Server	131
Upgrading User Profiles from DM Network Edition Version 10.x to Version 2.0 or Higher	139
Configuring the location of user profiles	141
Upgrading a user profile to DM Network Edition Version 2.5.1	142
Associating new user accounts with upgraded user profiles	143

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 Nuance Management Server* on page 131
- Save any *Dragon Medical 10.x* roaming user profiles to a location where the *NMS 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, 2.5.1, 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 *NMS Server* can access it. In Dragon Medical Network Edition, 2.5.1, you use the Dragon client to export and import user profiles. For details, see the Dragon Help.
5. Create user accounts in *NMS 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 Nuance Management Server* on page 131.

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 *NMS 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 Nuance Management 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 NMS), any additions or changes to those user profiles will not propagate to the copies on the NMS.
- Make sure that the Dragon workstations that contain profiles you want to convert have .NET Framework Version 4.5 installed. Y

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 2.5.1:

- Dragon Medical Enterprise Edition, version 10.1
- Dragon Medical Practice Edition, version 11

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 2.5.1 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 Nuance Management Server* on page 131
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 Nuance Management Server* on page 131 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 Nuance Management Server* on page 131 for more information.
4. On the Nuance Management Server (NMS), set the directory for the user profiles that you are migrating. See *Step 7: Create user accounts for the migrated profiles on the NMS* on page 137 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 136 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 136
7. Create user accounts in *NMS 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 NMS* on page 137 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 137 for more information.
9. Upgrade the master user profiles. See *Step 9: Upgrade the User Profiles* on page 138
10. Install the *Dragon Medical Enterprise Client* on the workstation.
11. Log in to the *Dragon Medical Enterprise Client* with the *NMS Server* user account login and password. See *Step 11: Log in* on page 138

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 Nuance Management Center

Set up the directory for the migrated profiles using the NMC 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 141 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 2.5.1 User Profiles. See the <i>Configuring the location of user profiles</i> 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 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 NMS

Log on to the Nuance Management Center and create user accounts in *NMS 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 131.

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 143.

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 2.5.1* on page 142.

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 *NMS* user account login and password. For more information, see *Logging in to the Nuance Management Server through the Nuance Management Center* on page 94

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

After you have upgraded the Nuance Management Server (NMS), you must upgrade your DM Network Edition Version 10.5 user profiles to DM Network Edition 2.5.1 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 141 for instructions.

- Share the Master User Profile directory and grant the Nuance service account (for instance nmsapps) 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 141 for instructions.

Upgrade the User Profiles

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

1. Log in to the Nuance Management Center.
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 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 *Logging in to the Nuance Management Server through the Nuance Management Center* on page 94

Configuring the location of user profiles

Each version has its own user profile location.

When an end user logs into Dragon through the NMS server, the NMS 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 Nuance Management Center, see 'Configuring the location of user profiles' in the Administrator guide.

Upgrading a user profile to DM Network Edition Version 2.5.1

See 'Upgrading a user profile to DM Network Edition Version 2.5.1' 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	146
Pushing the Dragon MSI installation to workstations	147
Installing Dragon manually outside of the Nuance Management Center	150
Associating Dragon with the Nuance Management Server or the Local Authenticator	151
Pushing the Dragon MSI installation to workstations	153
Understanding Dragon MSI command line options	156
Creating a custom installer for the client in Active Directory	161
Starting Dragon Medical Clients from Command Line	168
Creating Organization Tokens	170
Creating Single Sign-On user accounts	170
Closing the Dragon Medical client from a command line	176
Command line interface	177
Ensuring Dragon Medical Client anti-virus recommendations are met	180
Assigning access to folders and master user profiles across the network	181
Turning off Automatic Updates	181

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 *Nuance Management 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 Nuance Management Center* on page 150
- *Pushing the Dragon MSI installation to workstations* on page 153
 - *Carrying out administrative installation of Dragon with .bat file* on page 1
 - *Creating a custom installer for the client in Active Directory* on page 161

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 156.

Note:

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

DVD name	MSI file name
Dragon Medical Enterprise Network Edition Client Software DVD	Dragon NaturallySpeaking 12.msi
Nuance Management 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 7 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 7 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 7

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 XP or 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 7 for more information.
3. Push the custom MSI installation of *Dragon* to the client workstations.

Installing Dragon manually outside of the Nuance Management Center

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 128.

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 Nuance Management Server](#) to associate the Dragon client with the *NMS Server*.

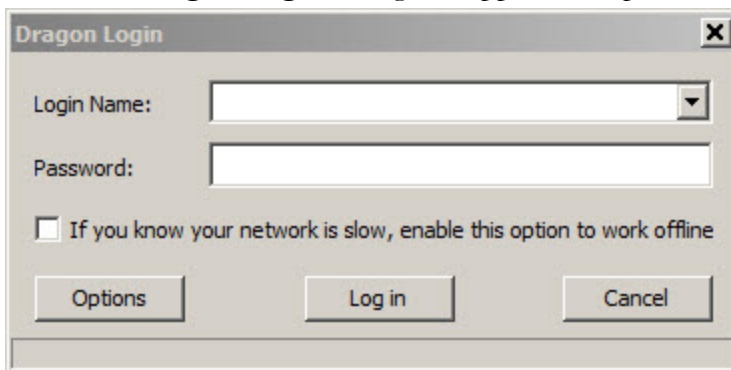
Associating Dragon with the Nuance Management Server or the Local Authenticator

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 *NMS Server* to communicate with.

Associating Dragon with an NMS 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 *Nuance Management 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 *NMS Servers*, see *Ensuring clients can contact an NMS 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 **NMS Administrator** has created in the *Nuance Management 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 NMS 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 *NMS Servers* on your network, you should set **NAS_ADDRESS** to the address of the traffic switch, rather than the address of any particular *NMS 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 *NMS 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 *NMS 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 156.

Note:

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

DVD name	MSI file name
Dragon Medical Enterprise Network Edition Client Software DVD	Dragon NaturallySpeaking 12.msi
Nuance Management 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 7 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 7 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 7

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 XP or 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 7 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
<p>USE_VSYNC_FOR_CITRIX_BASIC_DICTATION=0 (or 1)</p>	<p>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.</p> <p>Prerequisites for enabling text insertion through vSync</p> <ul style="list-style-type: none"> • 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. <p>Steps for enabling text insertion through vSync</p> <p>On the Dragon workstation, upgrade the Dragon client.</p> <ol style="list-style-type: none"> 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: <code>setup.exe /v"USE_VSYNC_FOR_CITRIX_BASIC_DICTATION=1 /Liwmo!e C:\temp\setup.log"</code> <p>Text insertion through vSync is not available when:</p> <ul style="list-style-type: none"> • 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. <p>Notes:</p> <ul style="list-style-type: none"> • 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.
<p>SERIALNUMBER=abcde-fgh-ijkl-mnop-qr</p>	<p>The serial number for the <i>Dragon</i> product. All <i>Dragon</i> installations require that you provide a serial (license) number for the product. The <i>Dragon</i> installation process checks for a serial number even if you run the process</p>

	<p>from a command line.</p>
<p>NAS_ADDRESS="DNS <IP_address>"</p>	<p>Indicates the IP address of the <i>NMS Server</i> that the <i>Dragon Medical Client</i> 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 <i>Dragon Medical Client</i> 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.</p> <p>If your network has multiple <i>NMS Servers</i> 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 <i>NMS Server</i>.</p> <p>Note: <i>If you define this option when installing an upgrade to Dragon Medical Network Edition, version 2.5.1, you will overwrite any value the user already entered.</i></p>
<p>NAS_LDAP_SIGN_ON=0 (or 1 or 2)</p>	<p>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" <i>Configuring LDAP</i> section for more information.</p> <p>Set the option to 0 to disable LDAP login.</p> <p>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.</p> <p>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.</p> <p>The default value is 0.</p> <p>Be sure that the value you set here is the same as the type of LDAP that is enabled in the Nuance Management Server. See the "DM Network Edition Administrator Guide" <i>Configuring LDAP</i> section for more information.</p> <p>Note: <i>If you define this option when installing an upgrade to Dragon Medical Network Edition, version 2.5.1, you will overwrite any value the user already entered.</i></p>
<p>NAS_SINGLE_SIGN_ON=0 (or 1)</p>	<p>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" <i>Implementing EHR Single Sign-On</i> section for more information.</p> <p>Set the option to 0 to disable single sign on from an EHR.</p> <p>Set the option to 1 to enable single sign on from an EHR.</p> <p>The default value is 0.</p> <p>Be sure that the value you set here —enabled or disabled—that is set in the Nuance Management Center. See the "DM Network Edition Administrator Guide" <i>Implementing EHR Single Sign-On</i> section for more information.</p> <p>Note: <i>If you define this option when installing an upgrade to Dragon Medical Network Edition, version 2.5.1, you will overwrite any value the user already entered.</i></p>

MSI options for installing Dragon features/advanced options

Options	Description
<p>ADDLOCAL=Feature1,Feature2,... or ADDLOCAL=ALL</p>	<p>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.</p> <p>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.</p>
<p>ADVERTISE- E=Feature1,Feature2,Feature3,...</p>	<p>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.</p> <p>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.</p> <p>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.</p>
<p>REINSTALL=Feature1,Feature2,... (or ALL)</p>	<p>Set the REINSTALL option to a comma delimited list of features to reinstall. To reinstall all features, set the REINSTALL option to ALL.</p> <p>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.</p> <p>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.</p> <p>For more information, see: http://msdn.microsoft.com/en-us/library/windows/desktop/aa371175</p>
<p>REINSTALLMODE={type of reinstallation to perform}</p>	<p>Set the REINSTALLMODE option to a string that indicates the type of reinstall to perform. Options are case-insensitive and order-independent.</p> <p>You should use this option when you use the REINSTALL option. You can also use this option during an installation of <i>Dragon Medical Client</i>, not just during a reinstallation.</p>

	Opt	Purpose
	p	Only reinstall a file if the file is missing.
	o	Only reinstall a file if the file is missing or is an older version.
	e	Only reinstall a file if the file is missing or is an equal or older version.
	d	Only reinstall a file if the file is missing or a different version is present.
	c	Only reinstall a file or files whose checksums are missing or corrupt.
	a	Force a reinstall of all files, regardless of checksum or version.
	u	Rewrite all required registry entries from the Registry Table that go under HKEY_CURRENT_USER or HKEY_USERS.
	m	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.
	s	Reinstall all shortcuts and re-cache all icons, overwriting existing shortcuts and icons.
	v	Run from the source package, re-cache the local package. Does not apply to a new installation of a product or feature.
REMOVEOLDPROD=1		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.
/x<Product.msi ProductCode>		Set the installation process to uninstall the current installed version of <i>Dragon</i> . You must perform this action during an upgrade. However, you should be familiar with the entire upgrade procedure before you use this option.

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

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

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.

Installing the Microsoft Custom Installation Wizard

The Microsoft Custom Installation Wizard is part of the Microsoft Office Resource Kit Tools. To install the Custom Installation Wizard:

1. Download the Office Resource Kit Tools (**OrkTools.exe**) from: <http://www.microsoft.com/office/orkarchive/xpddl.htm>. The **OrkTools.exe** self-extracting executable (EXE) file installs the core Office XP Resource Kit tools on your computer through a single Setup program.
2. After downloading **OrkTools.exe**, to install the tools, you either double-click the executable or select **Start > Programs > Microsoft Office Tools > Microsoft Office XP Resource Kit Tools**.

After you install the tool, you use its **Custom Installation Wizard** to create your custom installation. For details on using the wizard, continue with the next subsection.

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

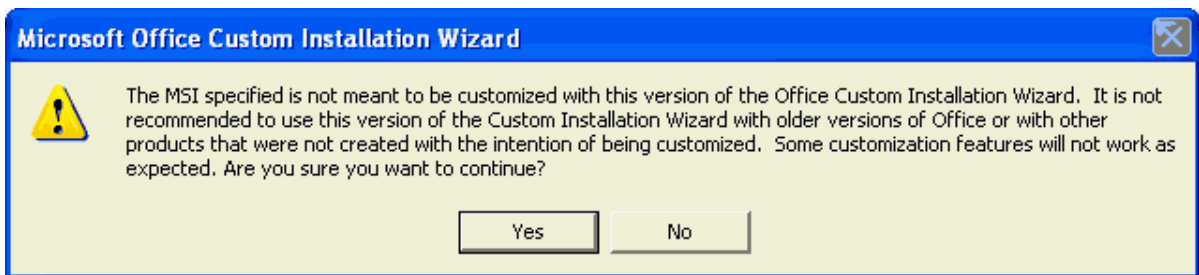
you can set for installing *Dragon Medical Client*, the SERIALNUMBER property. (You can add any options available to MSI on the command line.)

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:

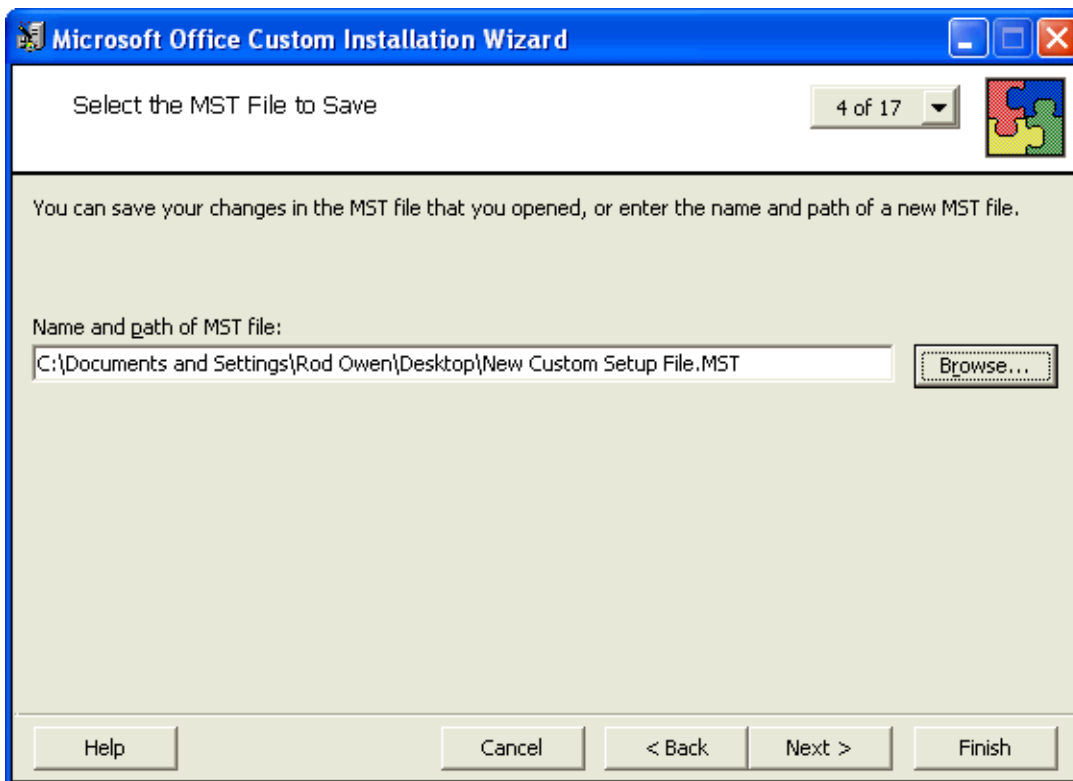


2. Click **Next**.
3. On the Open the MSI File page of the wizard, shown below, select the .MSI file you want to use to create a custom installation. The compiled .MSI file is located on your installation CD. The file you should select is named *Dragon Medical: Dragon NaturallySpeaking 12.msi*.
4. Click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

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

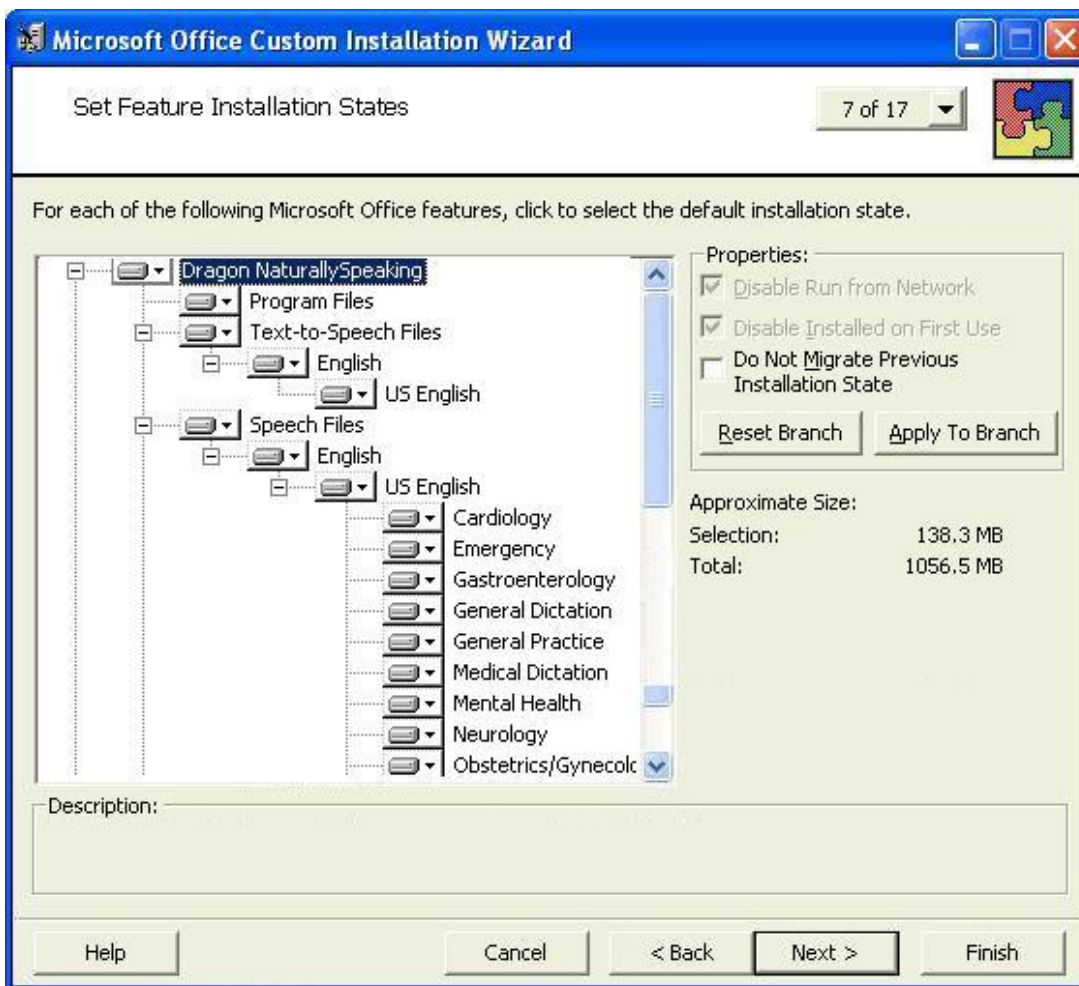


6. On the **Open the MST File** page of the wizard, select **Create a new MST file**.
7. Click **Next** to continue.
8. On the **Select MST File to Save** page of the wizard, select a file name and path for the MST file you are creating:



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 \Program Files\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

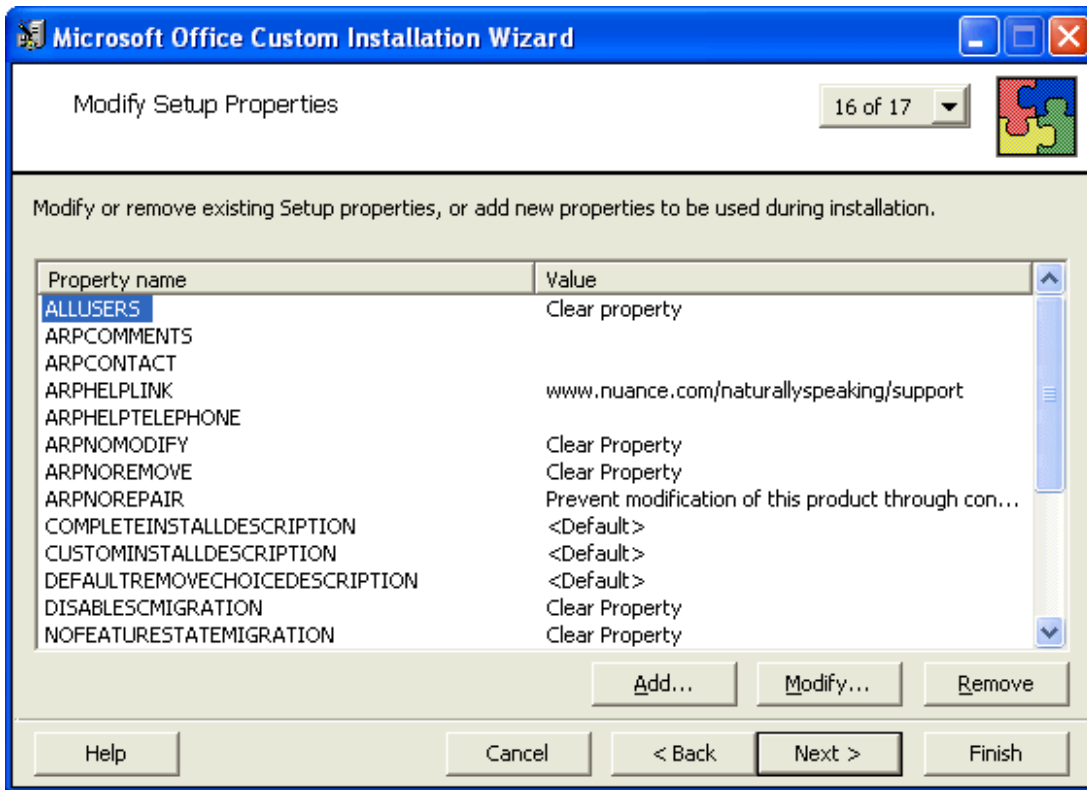
Add, Modify, or Remove Shortcuts page

Identify Additional Servers page

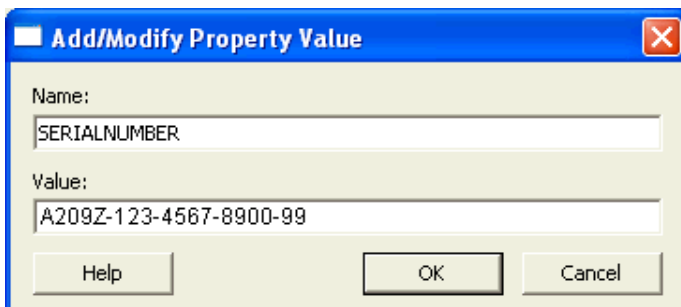
Specify Office Security Settings page

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**:

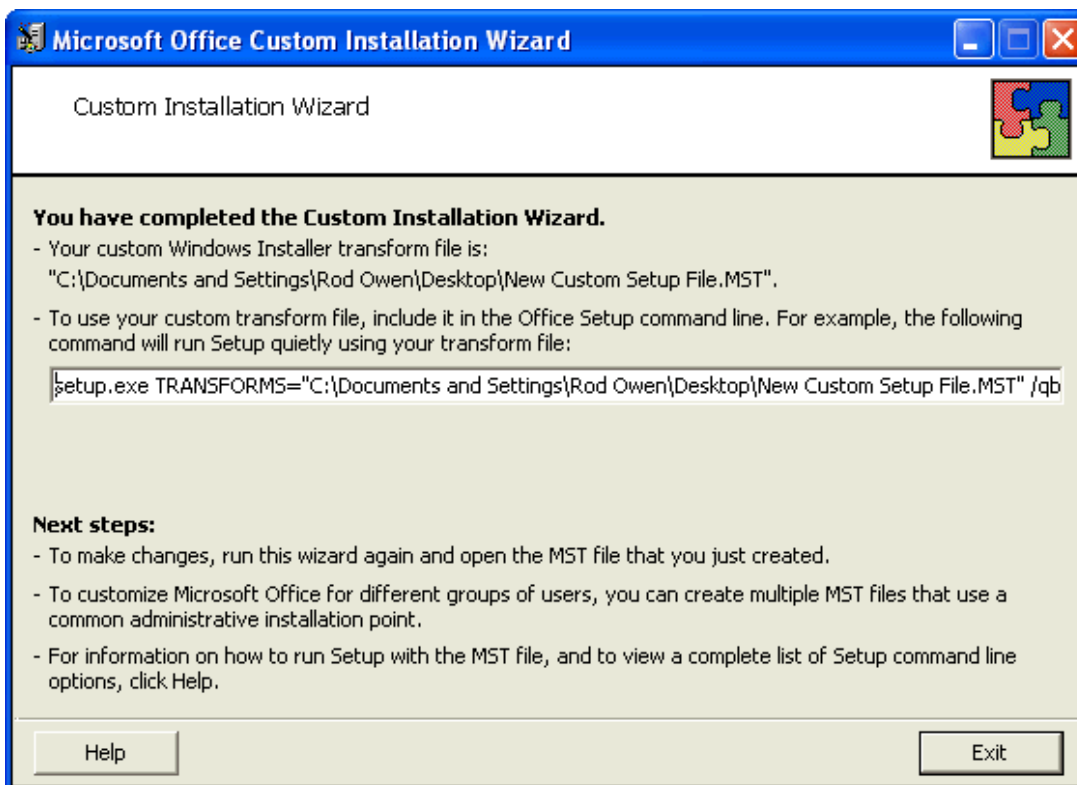


18. Note that the **Modify Setup Properties** page re-displays with the updated information. For example:

Modify or remove existing Setup properties, or add new properties to be used during installation.

Property name	Value
SERIALNUMBER	A209Z-123-4567-8900-99

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.

Starting Dragon Medical Clients from Command Line

On any workstation where you installed the client, you can start the *Dragon Medical Client* from the command line and login/connect to the *NMS Server*, as long as you know the login name and password of the user account on the server:

1. Select **Start > Run...** and enter **cmd** in the **Run** dialog box that pops up.
2. Switch directories to the following path:

```
<drive>:\Program Files\Nuance\NaturallySpeaking12\Program
```

3. Enter the command line shown below, passing either the **-user** option or the **/user** option followed by the user name and password, in that order. The user name and password must be from a user account created on the *NMS Server*:

```
natspeak.exe /user <username> <password>
```

4. The password is optional if a provider does not have a password, but Nuance recommends that you assign all providers using *Dragon Medical* a password.
5. To log in using an Active Directory single sign-on user account (when the *NMS Server* has been set up to run in Active Directory and the user accounts correspond to Windows user accounts), once the provider has logged in to Windows, he or she can use the **/trusted** switch on the command line:

```
natspeak.exe /trusted
```

6. To log in using an EHR single sign-on user account use the **/SSOUser** switch on the command line.

Use either of the following syntaxes:

```
natspeak.exe /SSOUser <username> <ClientID>
```

or

```
natspeakSSO.exe /SSOUser <username> <ClientID>
```

Where **<username>** is an EHR username, and **<Client ID>** is the token that you created in *Creating Organization Tokens* on page 170.

The user account must be set up in the NMS Server, as described in *Creating Single Sign-On user accounts* on page 170.

You can specify a time out value for the `/saveandshutdown` commands with `natspeak.exe` and `natspeakssso.exe`.

If you call `natspeakssso.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.

7. You can also use **natspeak** to install the client from the command line. To receive diagnostic messages about the *Dragon Medical Client* installation process, you can use the diagnostic option shown below:

```
natspeak.exe /diagnose
```

When you use the `/diagnose` option, *Dragon Medical* sends any information about errors that occur during the installation into the **Dragon.log** file.

Creating Organization Tokens

See 'Creating Organization Tokens' in the Administrator guide.

See 'Creating Single Sign-On user accounts' in the Administrator guide for information on using the tokens to configure EHR Single Sign-On.

Creating Single Sign-On user accounts

DM Network Edition supports two types of single sign-on accounts:

- Active Directory Single Sign-On, which allows users to log in using their Windows credentials.
- EHR Single Sign-On, which allows users to log in from their EHR.

The following sections describe how to configure both types of Single Sign-On accounts.

Note: For the most current information on how to configure Single Sign-On accounts, see the <https://isupport.nuance.com> website.

Implementing Active Directory Single Sign-On

When you implement Active Directory Single Sign-On, you set up providers to automatically log in when they have logged in to Windows. In this type of setup, providers avoid having to enter their login and password multiple times.

Steps

- You must configure your *NMS Server* to use Windows Active Directory Services. For more information see [Setting up the Nuance Management Server to run Active Directory Services](#) in the Dragon Medical Network Edition Administrators Guide.
- You must set up Windows Domain user names and user account login names that are identical. For more information, see [To configure Active Directory Single Sign-On](#) in the Dragon Medical Network Edition Administrators Guide.

If the login credentials for an existing user account do not match the user's Windows login, you must delete the user account and create a new one. Make sure the login credentials for the new account match the user's Windows login credentials. See the Enabling Active Directory Single Sign-On for Dragon users after you install DM Network Edition tech note, found at the <https://isupport.nuance.com> website, for details.

Note: For DM Network Edition, if you upgrade your Active Directory Single Sign-On from a pre-SP3 implementation to an SP3 or newer implementation, your Nuance Management Center logins will change from being authenticated by the LDAP system to being authenticated by the Nuance Management Center. This means that users must log in to the Nuance Management Center using their NMS credentials, not their LDAP credentials.

To configure Active Directory Single Sign-On

1. During the process of creating provider user accounts in the *NMS Server*, be sure to assign a login name that matches the user name of the provider's Windows Domain login name.

In the **Login** field, enter the user name of the provider's Windows Domain login name. The logins for DM Network Edition and Windows must be identical.

For example, if a provider's Windows Domain login name is one of the following:

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

You enter "John_Doe" in the **Login** field.

For DM Network Edition, for each Dragon client, perform the steps in Enabling Dragon client computers for Active Directory Single Sign-On.

Implementing EHR Single Sign-On

To implement EHR Single Sign-On, you create the log in and log out code for DM Network Edition. You then configure your EHR to call that code; allowing providers to log in and out of DM Network Edition from the EHR.

While the steps for configuring this in the EHR differ depending on which EHR your providers use, the steps on the DM Network Edition side are the same regardless of the EHR.

Steps

- (Optional) Ensure that vSync is installed on both the Citrix client and server
- Enable EHR Single Sign-On
- Generate a Client ID
- (Optional) Map the User's EHR log in to their DM Network Edition log in credentials
- Write the log in/log out code
- Configure your EHR to call the log in/log out code
- For DM Network Edition, install the Dragon Clients with EHR Single Sign-On enabled

(Optional) Ensure that vSync is installed on the Citrix server

For DM Network Edition, if your EHR is running on Citrix, EHR Single Sign-On requires that vSync be installed on the Citrix server and Citrix Support components be installed on the client machine. Visit <https://isupport.nuance.com> and view "L-3431 - Using Dragon with Citrix clients and servers Administrator Guide" for more information about vSync.

Enable EHR Single Sign-On in the Nuance Management Center

See the steps in 'Enable EHR Single Sign-on in the Nuance Management Center' in the Administrator guide.

Generate a Client ID

Generate a client ID for each site that you want to use EHR Single Sign-on. For information about how to generate a Client ID, see [Creating Organization Tokens](#). Your log in script for DM Network Edition will use this ID as a parameter .

(Optional) Map the EHR User Names to the log in credentials for DM Network Edition

If your users' EHR usernames and user account usernames are the same, you can skip this step.

If your users' EHR usernames and user account usernames are **not** the same, complete the following steps:

1. Open the user you want to configure.
2. Go to **User Account Details > Credentials > Token:**
Go to **User Account Details > Credentials > Token:**
3. Click **Add**. The **New Credential** dialog box appears.
4. Enter the user's EHR user name in the **Login** field.
5. Click **OK** to save your changes.

Write commands for logging in and out of DM Network Edition

You use command line parameters to log in and out of DM Network Edition using EHR Single Sign-on. You can integrate these commands with your EHR in a number of ways including:

- using a third party product
- using functionality that is built in to your EHR
- using an external scripting language.

Logging into the local machine

If you are going to run the log in command on the same machine where DM Network Edition are installed, use the following syntax to login a user:

```
<Path to the product executable>\<product exe file>/SSOUser <Username> <Client ID>
```

where:

- <Path to the product executable> is the path to the directory that contains the product exe file.
- <product exe file> is the name of the exe file that launches the product.
 - For DM Network Edition, the exe file is called natspeak.exe.
- <Username> is an EHR username.
- <Client ID> is the ID that you created. See [Creating Organization Tokens](#).

For example:

```
C:\Program Files\Nuance\NaturallySpeaking12\Program\natspeak.exe  
/SSOUser jdoe eacd17e4-f0fb-4a2b-9b20-03a80231e9a0
```

Logging out of the local machine

If you are going to run the log out command on the same machine where DM Network Edition are installed, use the following syntax to log out the currently loaded user:

```
<Path to the product executable>\<product exe file>/SSOUser <Username> <Client ID>
```

where:

- <Path to the product executable> is the path to the directory that contains the product exe file.
- <product exe file> is the name of the exe file that launches the product.
 - For DM Network Edition, the exe file is called natspeak.exe.
- <Username> is an EHR username.
- <Client ID> is the ID that you created. See [Creating Organization Tokens](#).

For example:

```
C:\Program Files\Nuance\NaturallySpeaking12\Program\natspeak.exe  
/Logout
```

Logging in when running DM Network Edition on a Citrix server

Use the following command to log users into DM Network Edition:

```
<Path to the product SSO executable>\<product SSO exe file>/SSOUser <Username> <Customer Token>
```

where:

- <Path to the product SSO executable> is the path to the directory that contains the product SSO exe file.
- <product SSO exe file> is the name of the SSO exe file for the product.
 - For DM Network Edition, the exe file is called natspeakSSO.exe.
- <Username> is an EHR username.
- <Customer Token> is the organization token that you created. For details, see [Creating Organization Tokens](#).

For example:

```
C:\Program Files\Nuance\EHR Synchronizer\Program\natspeakSSO.exe /SSOUser jdoe eacd17e4-f0fb-4a2b-9b20-03a80231e9a0
```

Logging out when running DM Network Edition on a Citrix server

Use the following command to log out the currently loaded user:

```
<Path to the product SSO executable>\<product SSO exe file> /Logout
```

where:

- <Path to the product SSO executable> is the path to the directory that contains the product SSO exe file.
- <product SSO exe file> is the name of the SSO exe file for the product.
 - For DM Network Edition, the exe file is called natspeakSSO.exe.

For example:

```
C:\Program Files\Nuance\EHR Synchronizer\Program\natspeakSSO.exe /Logout
```

Configure your EHR to call the log in/log out code

Follow the instructions provided in your EHR documentation to configure the EHR to call the log in and log out code that you created in the *Write Dragon log in/log out commands* topic in the Nuance Management Center Help.

Install the client software with EHR SSO Enabled

Use the MSI installer to install the DM Network Edition client software - with EHR Single Sign-On enabled Set the MSI command line option to enable EHR Single Sign-On by passing in `NAS_SINGLE_SIGN_ON=1`. See the Nuance Management Center Help for more information about the MSI installer and MSI command line options.

Notes:

Be sure that EHR Single-Sign On is enabled or disabled in **both** the Nuance Management Center

and the client software for DM Network Edition. If these settings are out of synch—for example, EHR Single Sign-On is enabled in the Nuance Management Center but not on the clients—unpredictable log in behavior results.

When installing an upgrade for DM Network Edition on a client machine, you can enter values in the command line for the Active Directory and EHR single sign-on settings. However, be aware that your values will overwrite any the user already entered for these settings.

Closing the Dragon Medical client from a command line

In Dragon Medical Network Edition, version 2.5.1, on any workstation where Dragon is installed, end-users can logout of Dragon and close the Dragon from the command line.

Closing Dragon from a command line is the same as closing Dragon from the Dragonbar menu and closes all Dragon related processes.

This feature is useful for customers that use Dragon in a virtual environment as it allows administrators to close Dragon without using the Task Manager.

1. Select **Start > Run...** and enter **cmd** in the **Run** dialog box that pops up.
2. Switch directories to the following path:

```
<drive>:\Program Files\Nuance\NaturallySpeaking<VersionNumber>\Program
```

3. To close Dragon without saving user profile changes, enter the command line shown below. This command works even if the **Automatically save user files on close** option is enabled in the Nuance Management Center.

```
natspeak.exe /ShutDown
```

4. To close Dragon and save user profile changes, enter the command line shown below. This command works even if the **Automatically save user files on close** option is enabled in the Nuance Management Center.

```
natspeak.exe /SaveandShutDown
```

Notes:

- If Dragon is running and a user profile is not open, running `natspeak.exe /ShutDown` or `natspeak.exe /SaveandShutDown` simply closes Dragon and all related processes.
- If Dragon is running and a user profile is open, running `natspeak.exe /ShutDown` closes Dragon and all related processes and **does not** save user profile changes.
- If Dragon is running and a user profile is open, running `natspeak.exe /SaveandShutDown` closes Dragon and all related processes and **saves** user profile changes.

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 highlighted
/findsetuplog	Brings up a Windows Explorer window with the dgnsetup.log highlighted
/findappdataallusers	Brings up a Windows Explorer window in our "all users" application data directory (nssystem.ini, nsapps.ini, models.ini, Users\ directory, 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 highlighted
/user <username> <password>	Automatically loads the user profile for the user with the specified username and password.
/ssouser <EHR username> <clientID>	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 Nuance Management Center 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 corresponding user account in the NMS Server. See the Administrator Guide for more information. The /trusted command line option works on the server as well as the client.
/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.

	<p>You can specify a time out value for the <code>/save</code> command with <code>natspeak.exe</code> and <code>natspeakssso.exe</code>.</p> <p>If you call <code>natspeak.exe /save <timeout></code> using a script, the script will not continue processing until the <code>save</code> command is completed, or the timeout value elapses, whichever comes first.</p> <p>Valid values for the timeout parameter are between 30 and 120 seconds and use the following syntax:</p> <pre>natspeak.exe /save <timeout></pre> <p>where <code><timeout></code> is the time out in seconds.</p> <p>The default timeout—which Dragon uses when given a value less than 30 or greater than 120—is 60 seconds.</p> <p>If you supply a non-numeric value or a value of zero, the time out feature is disabled for the current run.</p>
<p><code>/shutdown</code></p>	<p>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.</p>
<p><code>/saveandshutdown</code></p>	<p>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.</p> <p>You can specify a time out value for the <code>/saveandshutdown</code> commands with <code>natspeak.exe</code> and <code>natspeakssso.exe</code>.</p> <p>If you call <code>natspeakssso.exe /saveandshutdown <timeout></code> using a script, the script will not continue processing until the <code>save</code> command is completed, or the timeout value elapses, whichever comes first.</p> <p>Valid values for the timeout parameter are between 30 and 120 seconds and use the following syntax:</p> <pre>natspeak.exe /saveandshutdown <timeout></pre> <p>where <code><timeout></code> is the time out in seconds.</p> <p>The default timeout—which Dragon uses when given a value less than 30 or greater than 120—is 60 seconds.</p> <p>If you supply a non-numeric value or a value of zero, the time out feature is disabled for the current run.</p>
<p><code>/topic <topic></code></p>	<p>Automatically loads the topic specified by <code><topic></code> (<i>Professional edition only</i>)</p>
<p><code>/quick</code></p>	<p>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).</p>
<p><code>/SetDefaultOptions</code></p>	<p>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.</p>
<p><code>/SetDefaultAdministrativeOptions</code></p>	<p>Displays the Administrative settings dialog box at the end of the</p>

	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:\<Windows user_ID>\AppData\Roaming folder and all sub-folders
- C:\Documents and Settings\All Users\Application Data\Nuance folder and all sub-folders
- C:\Documents and Settings\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 profile locations* on page 18. 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: Migrating from the Data Distribution Tool to Command Sets and Command Sharing

Migrating from Data Distribution Tool to Command Sets	183
Migrating Custom Words from Data Distribution Tool to Word Sharing	186

Migrating from Data Distribution Tool to Command Sets

The Command Sets feature replaces distributing custom commands via the Data Distribution Tool (DDT). This section discusses the factors that you will need to consider before migrating, and tells you how to migrate to the Command Sets feature.

About Command Sets

Command Sets are a collection of related commands that are managed on and distributed from the Nuance Management Server (NMS). Once a Command Set is created, the Administrator uses the Nuance Management Center (NMC) to assign it to specific sites and groups, and can add, update, or remove the Command Set from the NMS.

An Administrator generates a Command Set by:

- Exporting custom commands from the Dragon Client's Command Browser to a .dat or .xml file (Nuance recommends using a .dat file whenever possible).
- Creating a Command Set in the NMC. This involves uploading the exported command file to the NMS, where it becomes the basis of the Command Set.

See the DM Network Edition Administrator's Guide for details on how to create a Command Set.

When a user logs in to the Dragon Client, the most recent Command Set files are downloaded and placed in her profile. The downloaded Command Set files are kept separate from custom commands, allowing the Administrator to make changes to the Command Sets without affecting a user's custom commands.

If the name and availability of a command within a Command Set exactly matches the name and availability of a command in a user's MyCommands, the local version overrides the version of the command in the Command Set, and the Command Set version will be inactive. You will have to remove the local version of the command using the "Purge Identical MyCommands" feature in order for the Command Set version to become active.

Choosing a Migration Strategy

There are multiple ways to migrate from DDT-distributed commands to Command Sets. The following section outlines the pros and cons of each strategy, allowing you to choose the best one for your organization.

Creating Command Sets that Replicate Existing DDT-Distributed Commands

You can migrate to distributing commands via Command Sets by creating new Command Sets that exactly replicate your existing DDT-distributed commands.

The advantage of this strategy is that running the "Purge Identical MyCommands" feature is likely to find and delete any custom commands created on the Dragon Client that are causing conflicts.

However, to be sure that your new Command Sets contain all of the commands that your organization needs, you may need to wait until the Purge feature has been run for all of your users, assess the new Command Sets, update them, and redeploy them.

If you choose this migration strategy, you'll use the following workflow to migrate:

1. Create Command Set files that replicate the existing commands that were distributed via DDT. This can be as simple as using the existing .dat or .xml files that comprised your DDT commands as the data files for your new Command Sets. See the DM Network Edition Administrator Guide for details on how to create a Command Set.
2. For each user that you want to migrate over to Command Sets, log in to the Dragon Client as that user and run the "Purge Identical MyCommands" feature. This will delete any custom commands that duplicate commands in your Command Sets. See the DM Network Edition Administrator Guide for details on how to run the "Purge Identical MyCommands" feature.
3. Save the user profile to save these changes.
4. Repeat steps 2 and 3 until all of the user profiles have been purged of identical commands.
5. Update and redeploy the Command Sets as needed.

Creating Command Sets that are Different from Existing DDT-Distributed Commands

You can also create Command Sets that don't exactly replicate your existing DDT-distributed commands. This migration strategy makes conflicts between old and new commands and between old and new lists within those commands less likely, as you can name the commands and lists in your new Command Sets specifically to reduce these sorts of problems.

However, this strategy also means that running the "Purge Identical MyCommands" feature may not find all identical commands, and you may have to delete those duplicates manually.

If you choose this strategy, you'll use the following workflow to migrate:

1. Create new Command Sets with new command and list names, chosen to prevent current and future conflicts. See the DM Network Edition Administrator Guide for naming guidelines.

Assign those Command Sets to the appropriate sites and groups. See the DM Network Edition Administrator Guide for instructions on how to create new command sets and assign them to sites and groups.

2. Temporarily deploy Command Set versions of the DDT commands, but prefix the Command Sets with a low-sorting and easily identifiable name, such as 'z z zTEMP_<DDTCommandSetName>', where <DDTCommandSetName> is the name of the original DDT .dat or .xml file. This allows any new Command Set commands that conflict to be loaded first and be active.
3. For each user in the affected sites and groups, log in to the Dragon Client as that user and run the "Purge Identical MyCommands" feature. This will delete any custom commands that duplicate commands in your Command Sets. See the DM Network Edition Administrator Guide for details on how to run the "Purge Identical MyCommands" feature.
4. Save the user profile to save these changes.
5. Repeat steps 3 and 4 until all of the user profiles have been purged of identical commands.
6. Once the 'Purge' process is complete across the user profiles, delete the temporary Command Set files from the NMS. This results in these files being removed from the Command Set files on the Dragon Clients. See the DM Network Edition Administrator Guide for instructions on how to delete Command Sets.
7. Review the existing MyCommands and delete any that are no longer relevant.

Migrating Custom Words from Data Distribution Tool to Word Sharing

In DM Network Edition Network Edition version 2.1 and newer, the Word Sharing feature replaces using the Data Distribution Tool (DDT) to share custom words across your organization.

Take the following steps to migrate from distributing custom words via DDT to distributing them via the Word Sharing feature:

- Import the custom words that you used to distribute via DDT to the Nuance Management Server (NMS). See the *Working with Text and Graphics auto-texts and custom words* chapter of the DM Network Edition Administrator Guide for instructions.
- When users log into the client for the first time after a large number of words have been added or deleted from the NMS, the vocabulary may take a bit longer than usual to load, as the custom words download from the server are added and deleted from the users' vocabulary.

Users **must** save their profiles after this to avoid the vocabulary loading slowly in the future.

Chapter 10: Backing up server systems

NMS SQL Server backup system	188
Master user profiles backups	190
Removing a master user profile folder for a deleted user account	190
Servers and Dragon client logs	192
View log files for a variety of products and product components	193
Nuance Management Center logs	194

NMS SQL Server backup system

When you look in the SQL Server explorer, to find the *NMS SQL Database* database, look for a database named **NuanceMC** by default. If you name the database differently during the installation process, *NMS Server* retrieves the database name from SQL Server and uses its name as the root for the backup files.

During the installation process, the *NMS Server* creates the backup folder in the location you indicate or, by default, in the **C:\NMSDDBBACKUP** folder.

The *NMS Server* automatically backs up the data you have entered into it on sites, users, groups, and other objects into the backup folder. It also backs up all Windows communication foundation service logs that it creates.

(For more information on logs that the clients and servers create, refer to *Servers and Dragon client logs* on page 192.)

Scheduled NMS transaction log and database backups

The *NMS Server* schedules these backups:

- Transaction log backups—Scheduled hourly
- Differential database backups—Scheduled daily
- Full database backups—Scheduled weekly

By default, full and differential backups run at 2 AM.

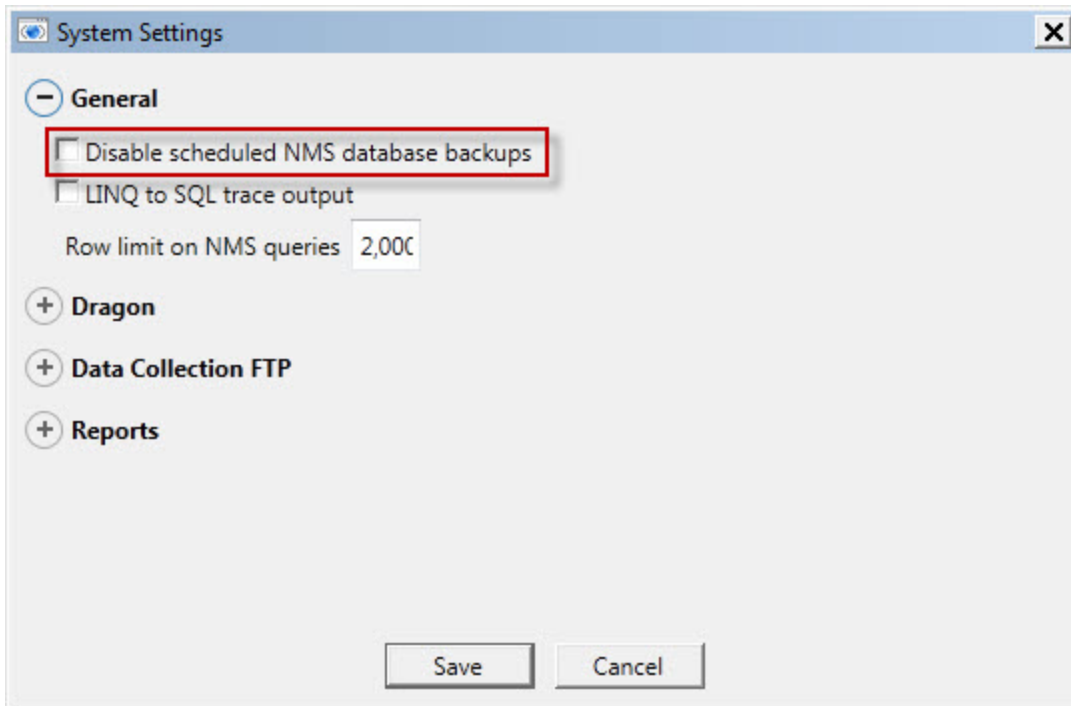
The *NMS Server* stores up to one month of backups on its hard disk.

To retain more than one month of backups, you must copy the data before the month is over.

Disabling scheduled backups of the NMS database

You can set an option to turn off scheduled backups of the NMS database. This is useful for sites that want to manage their own backups of the NMS database. When you set the option, the scheduled backups still run but do not do anything. To disable scheduled backups of the NMS database:

1. In the Nuance Management Center, in **System Settings**, check **Disable scheduled NMS database backups**.



2. Click **Save**.

Database Backup File Names

Database backup files use the following naming convention:

NuancePOBBDump X .BAK where X is a number between 1 and 5.

Each time it carries out a full database backup, the *NMS Server* takes the following steps:

1. Deletes database files older than 1 month.
2. Names the new database backup file NuancePOBBDump $X+1$.BAK. So if the previous week's file was named NuancePOBBDump1.BAK, the new database backup file will be named NuancePOBBDump2.BAK. If the previous week's file was named NuancePOBBDump5.BAK, then the new database backup file will be named NuancePOBBDump1.BAK.

Master user profiles backups

The master user profiles file structure follows a particular pattern. Understanding this structure can help you better plan to back up the master user profiles.

Caution:

Nuance recommends that you back up all master user profiles weekly. You should retain these backups for several weeks in case you need them.

Each DM Network Edition master user profile is stored in its own subdirectory of the *Master User Profiles Server* (or directory on the *NMS Server*, or database server) as shown below:

```
\\<ServerName>\<ProfilesDir>\<NMS_userLoginName>\last known good\  
profile1
```

The first profile for the provider is under **profile1**. If the provider has more than one profile, the next is under **profile2**.

If a profile becomes corrupted, you receive a notification about it in the **Messages** box on the *NMS Server*; the *NMS Server* moves the profile to the following location:

```
\\<ServerName>\<ProfilesDir>\<NMS_userLoginName>\BAD\profile1
```

The next time the provider starts to dictate, the *Dragon Medical Client* automatically creates a new profile for that provider.

The corrupted profile remains on the *Master User Profiles Server* until you remove it. When you have any corrupted profiles, you should contact Nuance, as these profiles are not automatically uploaded to the Nuance data collection site. Avoid removing these profiles until Nuance subsequently notifies you that it has retrieved the profiles for analysis.

Removing a master user profile folder for a deleted user account

In Dragon Medical Network Edition, 2.5.1, you use the Dragon client to export and import user profiles. For details, see the Dragon Help.

Before you delete a user account, you should be sure to export the user profile for the account first. Exporting the user profile saves the information accrued about that particular provider's voice and speech patterns. Should you ever need that user profile again, you can then import the exported user profile to bring the provider back up to speed more quickly.

For details on how to export a user profile and delete its associated user account, refer to the Dragon Help.

Servers and Dragon client logs

Note:

The servers regularly purge all of these logs and do not automatically back them up, so you might want to back them up to another location if you want to save them for longer periods.

Dragon and Profile Optimizer Speech Node logs

The *Profile Optimizer Speech Node* generates two log files for each ACO/LMO task it carries out:

- *Dragon* log files—*Dragon Medical SDK Client* creates **dragon.log** and **dgnsetup.log**. In Service Pack 4, you cannot view Dragon log files from the Nuance Management Center.
- *Speech Node* service log file—*Profile Optimizer* services write these files

Viewing Speech Node service logs

You can view the *Dragon* log files and *Speech Node* service log files in the *Nuance Management Center*.

Upload Speech Node service logs

You must upload the logs before you can view them in the Nuance Management Center.

See 'Upload Speech Node service logs' in the Administrator guide.

View Speech Node service logs

You can view the *Dragon* log files and *Speech Node* service log files in the Nuance Management Center.

See 'View Speech Node service logs' in the Administrator guide.

Viewing Dragon logs

To view the *Dragon* log files, see the 'Viewing Dragon log files' in the Administrator guide.

NMS Server logs

See 'NMS Server logs' in the Administrator guide.

View log files for a variety of products and product components

Please see 'View log files for a variety of products and product components' in the DM Network Edition Administrator Guide.

Nuance Management Center logs

The Nuance Management Center stores user session data in a Nuance Management Center log file.

The log file includes data that could be useful for troubleshooting Nuance Management Center exceptions or issues.

If an administrator performs an action that causes a Nuance Management Center error or crash, the next time the Nuance Management Center starts, it sends the Nuance Management Center Log file to the NMC server. Technical support can then analyze the log file. An administrator can also manually upload the Nuance Management Center log file to the NMS.

An Nuance Management Center log file is kept until it becomes larger than 10 MB in size. At that time, the Nuance Management Center discards the log file and creates a new one. The Nuance Management Center also creates a new log file after it uploads the current one to the NMS.

Upload the Nuance Management Center log file to the NMS

1. In the Nuance Management Center, click the Nuance icon (top left of the screen).
2. Select **Upload NMC Log File**.

Chapter 11: Moving Databases

Moving NMS Server SQL database	196
--------------------------------------	-----

Moving NMS Server SQL database

To move the *NMS 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 *NMS SQL Database*, take these steps:

1. Back up the *NMS SQL Database* and then close all network connections.
2. Remove the *NMS 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 *NMS Server* following the steps in *Moving NMS Server SQL database* on page 196. The old database remains intact.
6. Reopen all network connections.
7. Reinstall the *NMS 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 *NMS 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 *NMS Server* database.
4. Right click on **NuanceMC** and select **Delete** from the drop-down menu.

Chapter 12: Setting up Active Directory Services

Setting up the Nuance Management Server to run Active Directory Services	198
--	-----

Setting up the Nuance Management 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 or SQL Server 2012.
2. Creating Nuance Management Center Administrator Account in NMS Server for Active Directory Administrator: After you install the *NMS Server*:
 - Log in to *NMS 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 **Nuance Management Center 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 170. You need to create these accounts before you can associate a user account with an already existing upgraded master user profile.
3. Set the Active Directory connection string.
4. Continue to configure the NMS Server as Active Directory Administrator
 - Follow instructions in Nuance Management 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 *NMS Server* following the instructions in this manual.
2. Log in to the *NMS Server* through the *Nuance Management Center*.

3. To prepare to set up user accounts required for Active Directory in *NMS 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 *Nuance Management 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 *Nuance Management 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 *NMS Server*. Make sure the login you assign in *NMS 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 *NMS Server* user account login you assign matches an existing login in Active Directory.
7. Proceed to the next subsection.

Set the Active Directory Connection String

Complete the steps in 'Set the Active Directory Connection String' in the Administrator guide.

Restarting the Nuance Management Service

1. Restart the *NMS 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 *NMS 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 170.
5. To continue to configure the *NMS Server* as Active Directory administrator account by following the remaining instructions in this book.

Index

A

access rights	18, 125, 181
required for account to run services	16
access rights to master user profiles	125, 181
access rights to Speech Nodes	125, 181
access to master user profiles	18
Active Directory	
creating custom client installer	161
support for client install	149, 155
Active Directory Services	198
enabling	198
administrative install of clients	156
advanced options	
command line for client	158
Anti-virus recommendations	
Dragon Medical Clients	180
servers	56, 92, 99
assigning rights to start services	97
associating profiles with user accounts	143
associating user accounts with profiles	143
Automatic Updates	
managing Windows	21, 125, 181

B

backups	
master user profiles	190
NMS database	188
NMS transaction logs	188
batch file provided for admin install	156
Bluetooth wireless microphone support	7

C

checklists	
converting local users	32
installing Dragon Medical clients	35
installing servers	24
setting up Active Directory Services	26
setting up master user profiles	29

SQL Server 2008	24
starting servers	28
upgrading roaming users	31
verifying servers are running	28
clients	
access rights to	18, 125, 181
command line	
starting clients on	168
command line interface	177
command line options	
client installation	156, 158-159
custom installer	
Active Directory	161

D

database	
moving NMS Server	196
database software	
installation checklist	24
installing required	45
deleting master user profiles	190
Dragon	
upgrading	142
versions 8.x and 9.x	142
Dragon client	
administrative install	156
overview of installing	146
Dragon clients	
see Dragon Medical Clients	146
Dragon logs	192
Dragon Medical Clients	
administrative install	156
anti-virus recommendations	180
installing outside the NMC	150
logging in to	151
opening ports to access profiles	146
overview of installing	146
pushing MSI install to	147, 153

setting NMS Server for	151
starting on command line	168
system requirements for	7, 128
Dragon Medical Enterprise Clients	
see Dragon Medical Clients	146
Dragon Medical SDK Client	
installing for Speech Nodes	88
dragon.log file	
sending data to	169
DVD	
installing client software from	150
F	
features	
command line options for client	158
firewall in Windows Server 2008	55
H	
hardware/software requirements	
clients	7, 128
http settings for web server	119
https settings for web server	122
I	
installation checklists	
see Checklists	24
IPswitch	
see Load balancing	57
L	
load balancing	
NMS Servers, configuring switch	57
local users	
migrating to this product	131
location of master user profiles	
choosing	102
logging in to clients	151
logging in to NMS Server	94
logs	
client and server	192
Dragon	192
finding Dragon	192
finding NMS service	192
NMS Server	192
Profile Optimizer Speech Node	192

sending install diagnostics to	169
viewing Dragon	192
viewing NMS service	192
viewing Speech Node service	192

M

mapping disk for mastser user profiles	105, 107
master user profile backups	190
master user profile directory	
creating	105
master user profiles	
access rights to	18, 125, 181
choosing location	102
http settings	119
https settings	122
mapping disk	105
permissions	18, 125, 181
removing folder	190
restoring deleted	190
setting up access	107
setting up directory	105
setting up machine	105
SSL settings	122
Windows software	104
master user profiles directory	
see master user profiles	107
migrating local cache user profiles	131
MSI installation	
Active Directory support	149, 155
Dragon ADDLOCAL options	159
Dragon advanced options	158
Dragon ADVERTISE properties	159
Dragon feature options	158
Dragon options	156
options for pushing client	148, 154
pushing to workstations	147, 153
SCCM support	148, 154
SMS support	149, 155
MSI installer	
downloading to workstation	150
N	
natspeak	
options for starting client	168

network traffic switch
 configuring for load balancing 57

NMC
 access rights18, 125, 181
 before installing40
 logging in to server through 94
 see also installing NMS Server 54

NMS database
 access rights18, 125, 181

NMS database backups188

NMS Server
 access rights18, 125, 181
 anti-virus recommendations 56, 92, 99
 before installing40
 installing .NET Framework 42
 installing prerequisite software42
 installing required database software45
 installing required IIS features/roles42
 installing server, NMS, database54-55
 load balancing 57
 logging in to 94
 moving database196
 setup client to find 151

NMS Server logs
 see NMS service logs 192

NMS service logs192

NMS SQL database
 see NMS database18, 125, 181

NMS transaction log backups 188

NMSapps account
 requirements 16

Nuance folder permissions18, 125, 181

Nuance Management Center
 see NMC 40

Nuance Management Server
 see NMS Server40

P

password
 required for account to run services 16

permissions
 Nuance folder18, 125, 181
 required for account to install services16
 required for account to run services 16

setting on master user profiles18, 125, 181
 setting on servers, clients18, 125, 181

ports
 opening on client146

prerequisite software for NMS Server
 installing 42

prerequisite software for Speech Nodes
 installing 87

Profile Optimizer
 installing Speech Nodes only 92
 starting Speech Nodes 96

properties
 Active Directory client installer161
 ADDLOCAL for MSI install159
 ADVERTISE for MSI install 159

R

rights
 requirements for account to install services16
 rights to start services 97

S

SCCM support148, 154

servers
 access rights to18, 125, 181

service logs
 finding NMS192
 NMS service192
 Speech Node192
 viewing NMS 192

services
 giving rights to start97
 Windows user account to install16
 Windows user account to run under 16

sites
 master user profiles locations102

SMS support149, 155

software options for installing clients148, 154

Speech Node service logs 192

Speech Nodes
 access rights18, 125, 181
 Dragon Medical SDK Client 88
 installing on separate machine 92
 installing on virtual machine 92

installing prerequisite software	87
permissions to access	18
starting	96
Windows Installer 3.1	87
SQL Server	
database anti-virus recommendations	56, 92, 99
SQL Server 2008	
installing	45
SSL settings for web server	122
switches	
network traffic for load balancing	57
system requirements for clients	7, 128
U	
upgrading DME	142
user account	
Windows to install product services	16
Windows to run product services	16
user accounts	
associating with user profiles	143
migrating local to current product	131
user profiles	
associating with product users	143
W	
web servers	
http settings	119
https settings	122
information for setup	104
installing software	108
SSL settings	122
Windows Automatic Updates	
managing	21, 125, 181
Windows Installer 3.1	
installing for Speech Nodes	87
Windows Server 2008 firewall	55
Windows software required	104
workstations	
installing clients on multiple	147, 153