Dragon® Medical 360 network edition

Service Pack 3

Configuring LDAP and Single Sign-On

Table of Contents

Copyright

2012. Dragon Medical Enterprise Network Edition, Service Pack 3.

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

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

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

Nuance, 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 non-infringement.

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 Enterprise Network Edition DMENE with EditChoice for Third Party Transcription 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.

Visit Nuance Healthcare on the Web at www.nuance.com/healthcare.

Creating Single Sign-On user accounts

Dragon Medical supports two types of single sign-on accounts:

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

The following section describes how to configure EHR Single Sign-On, which is new in Service Pack 3.

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

Note: If you upgrade your Active Directory Single Sign-On from a pre-SP3 implementation to the SP3 implementation, your Nuance Management Console (NMC) logins will change from being authenticated by the LDAP system to being authenticated by the NMC. This means that users must log in to the NMC using their NMC credentials, not their LDAP credentials.

If you plan to upgrade from pre-SP3 SSO to one of the SP3 SSO implementations, see "*L-3475 Technical Note: Upgrading Pre-SP3 LDAP and SSO to an SP3 Implementation*", found on the https://isupport.nuance.com website.

Implementing EHR Single Sign-On

When you implement EHR Single Sign-On, you create Dragon log in/log out code and configure your EHR to call that code, allowing providers to log in to and out of Dragon from the EHR's user interface.

While the steps for configuring this in the EHR differ depending on which EHR your providers use, the steps on the Dragon 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 her Dragon credentials
- Write Dragon log in/log out code
- Configure your EHR to call the log in/log out code
- Install the Dragon Clients with EHR Single Sign-On enabled

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

If your EHR is running on Citrix, EHR Single Sign-On requires that vSync be installed on the Citrix server and Dragon Citrix Support components be installed on the client. 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 Console

Complete the following steps for each site that you want to use EHR Single Sign-on:

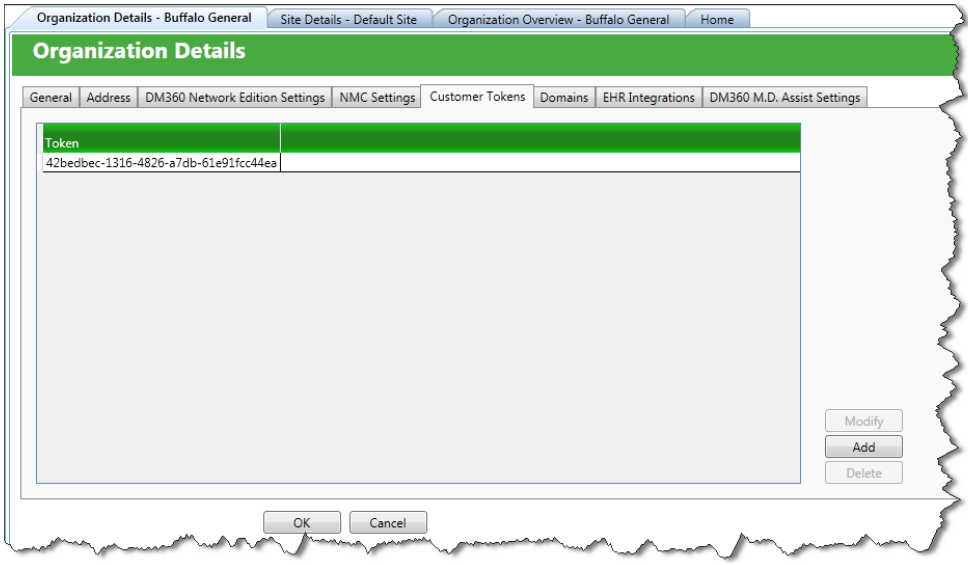
1. Open the site in the Nuance Management Console.
2. Click the **DM360 Network Edition Settings** tab.
3. Check the **Enable SSO Authentication** checkbox to enable EHR Single Sign-on for that site.
4. Click **Save** to save your changes.

Generate a Client ID

A Client ID is also known as a Customer Token.

Complete the following steps to create a customer token:

1. In the Nuance Management Console, go to **Sites > Organization Overview**.
2. Select the organization that you want to create a token for, and click the **Organization Details** icon. The Organization Details tab appears.
3. On the **Customer Tokens** tab, click **Add** to generate a new customer token:


Organization Details - Buffalo General
Site Details - Default Site
Organization Overview - Buffalo General
Home
Organization Details
General
Address
DM360 Network Edition Settings
NMC Settings
Customer Tokens
Domains
EHR Integrations
DM360 M.D. Assist Settings
Modify
Add
Delete
OK
Cancel

Token	
42bedbec-1316-4826-a7db-61e91fcc44ea	

4. The new token appears in the **Token** table. Copy or make a note of this value; you will need it to configure EHR Single Sign-On.

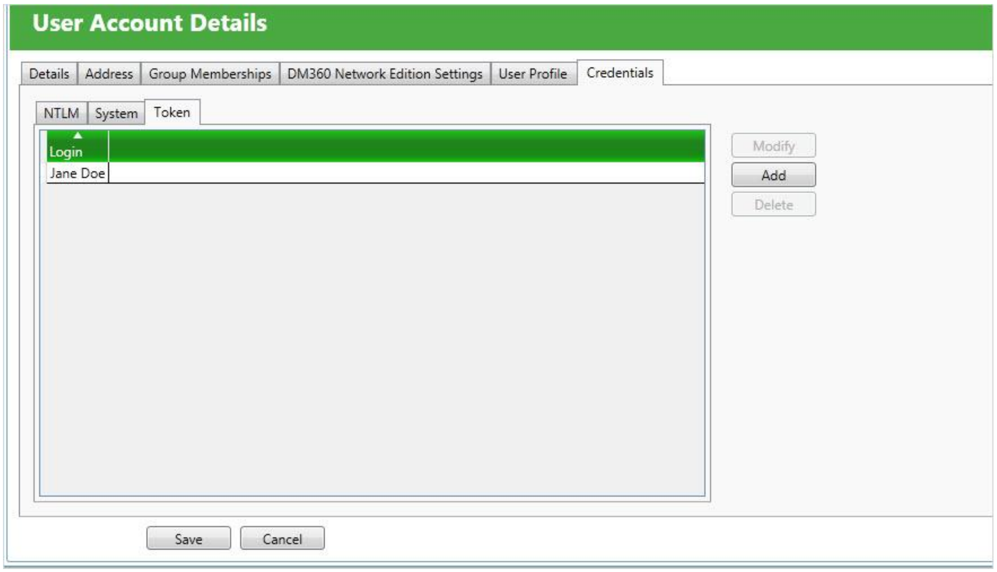
You will use this ID as one of the parameters for the Dragon log in script.

(Optional) Map the EHR User Names to the Dragon Credentials

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

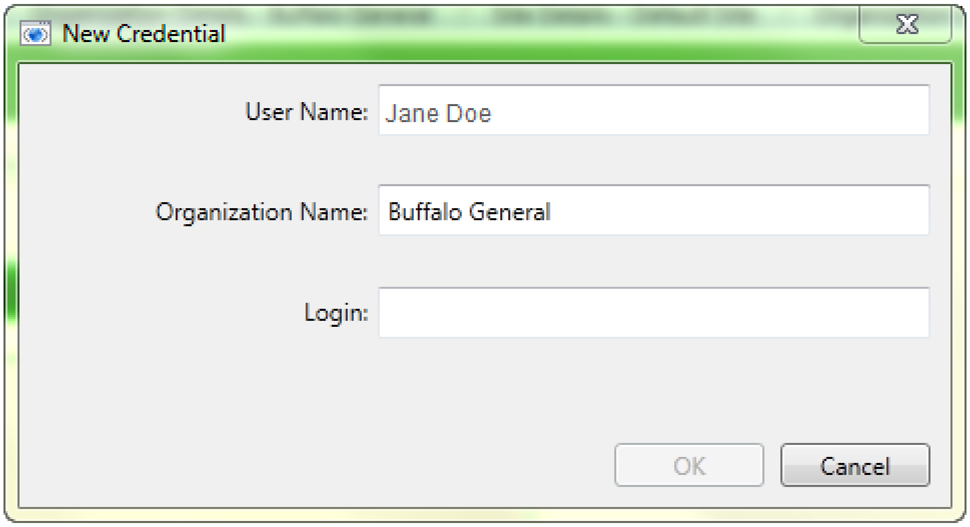
If your users' EHR usernames and Dragon usernames are **not** the same, complete the following steps to map the EHR user name to the Dragon credentials:

1. Open the user you want to configure.
2. Go to **User Account Details > Credentials > Token**:



Login
Jane Doe

3. Click **Add**. The New Credential dialog box appears:



User Name: Jane Doe

Organization Name: Buffalo General

Login:

4. Enter the user's EHR user name in the **Login** field.
5. Click **OK** to save your changes.

Write Dragon log in/log out commands

To log in or out of Dragon with EHR Single Sign-on, you use Dragon's command line parameters. 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, or using an external scripting language.

Logging in when Dragon is local

If you are going to run the log in command on the same machine where Dragon is installed, use the following syntax to log a user in:

```
<Path to Dragon executable>\natspeak.exe /SSOUser <Username> <Client ID>
```

where:

`<Path to Dragon executable>` is the path to the directory that contains the `natspeak.exe` file.

`<Username>` is an EHR username.

`<Client ID>` is the ID that you created in *Creating Customer Tokens* on page **Error! Bookmark not defined.**.

For example:

```
C:\Program Files\Nuance\NaturallySpeaking10\Program\natspeak.exe
/SSOUser jdoe eacd17e4-f0fb-4a2b-9b20-03a80231e9a0
```

Logging out when Dragon is local

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

```
<Path to Dragon executable>/natspeak.exe /Logout
```

where:

`<Path to Dragon executable>` is the path to the directory that contains the `natspeak.exe` file.

For example:

```
C:\Program Files\Nuance\NaturallySpeaking10\Program\natspeak.exe /Logout
```

Logging in when you are running Dragon on a Citrix server

If you are running Dragon on a Citrix server use the following command to log users in to Dragon:

```
<Path to Dragon executable>\natspeakSSO.exe /SSOUser <Username> <Customer Token>
```

where:

`<Path to Dragon executable>` is the path to the directory that contains the `natspeakSSO.exe` file.

`<Username>` is a EHR username.

`<Customer Token>` is the token that you created in *Creating Customer Tokens* on page **Error! Bookmark not defined.**.

For example:

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

Logging out when you are running Dragon on a Citrix server

If you are running Dragon on a Citrix server use the following command to log the currently loaded user out of Dragon:

```
<Path to Dragon executable>\natspeakSSO.exe /Logout
```

where:

`<Path to Dragon executable>` is the path to the directory that contains the `natspeakSSO.exe` file.

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 with your EHR to configure it to call the log in and log out code that you created in *Creating Single Sign-On user accounts* on page 6.

Install Dragon Client Software with EHR SSO Enabled

Use the MSI installer to install the Dragon Client 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 *Dragon Medical Enterprise Network Edition Installation Guide* for more information about the MSI installer and MSI command line options.

Note: Be sure that EHR Single-Sign On is enabled or disabled in **both** the Nuance Management Console **and** the Dragon clients. If these settings are out of synch—for example, EHR Single Sign-On is enabled in the NMC but not on the clients—unpredictable log in behavior results.

Setting up the Nuance Management Server to run Active Directory Services

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

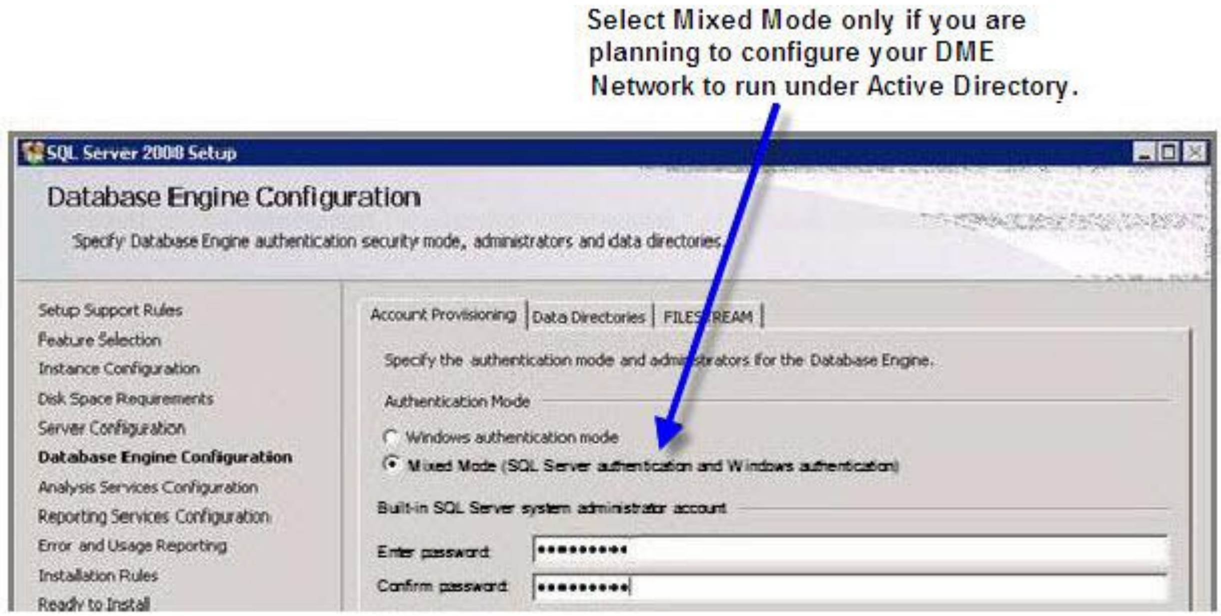
Enabling Active Directory Services

1. Install SQL Server 2008.
    - Select **Mixed Mode** authentication for accessing database.
2. Creating NMC Administrator Account in NMS Server for Active Directory Administrator: After you install the *NMS Server*:
    - Install the Nuance Certificates on any workstation where you want to log in through the *NMC Console*. (Refer to the *Dragon Medical Enterprise Network Edition Installation Guide*.)
    - 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 an **NMC 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 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 4. 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.

Selecting Mixed Mode authentication during SQL Server installation

During the SQL Server installation, on the **Database Engine Configuration** page of the wizard, when you choose the type of authentication required to access the database, select **Mixed Mode**.

Selecting **Mixed Mode** ensures that you can later attach to the database using an Active Directory account.



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

SQL Server 2008 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Built-in SQL Server system administrator account

Enter password: •••••••••

Confirm password: •••••••••

Creating an NMC Administrator account for Active Directory

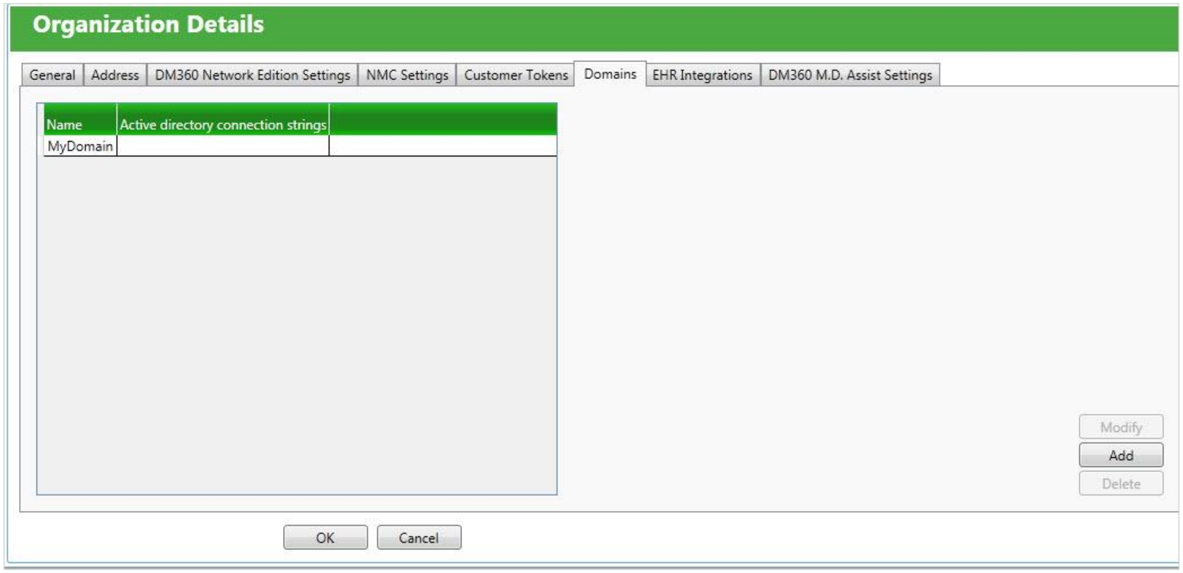
To create the **NMC Administrator** account for the Active Directory administrator:

1. Install the *NMS Server* following the instructions in this manual.
2. Log in to the *NMS Server* through the *NMC Console*.
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 DME*
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

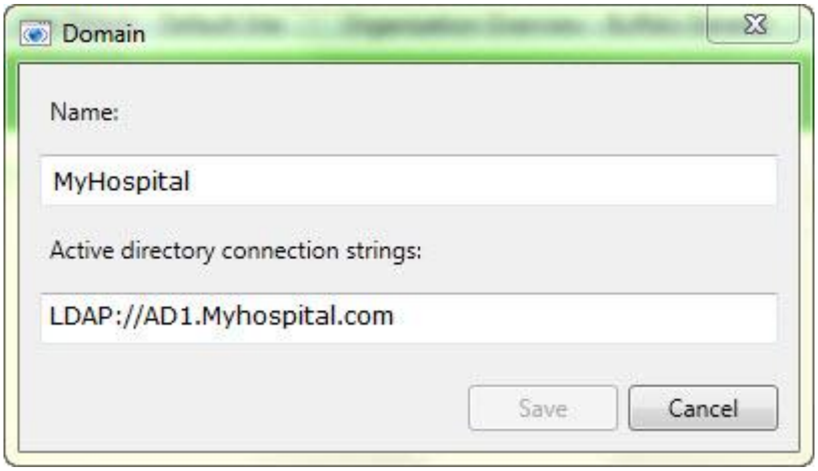
Complete the following steps to add an Active Directory connection string:

1. Click the **Organization Details** icon for the site that you want to configure, then click the **Domains** tab:



Name	Active directory connection strings
MyDomain	

2. Click **Add**. The **Domain** dialog box appears.
3. Enter the domain name in the **Name** field, and the Active Directory connection string for that domain in the **Active directory connection strings:** field:



Name: MyHospital

Active directory connection strings: LDAP://AD1.Myhospital.com

4. Click **Save** to save your changes.
5. Repeat steps 2-4 for every domain that you want to set up.

Once Active Directory is on, the *NMS Server* sends all authentication requests to the server you specified in the connection string value. You can then take actions to set up and manage your network using Active Directory Services. For information on using Active Directory Services, refer to the documentation Microsoft provides.

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 4.
5. To continue to configure the *NMS Server* as Active Directory administrator account by following the remaining instructions in this book.

Configuring LDAP

Configuring LDAP involves both Dragon Client and Nuance Management Console tasks. Complete the following steps to configure LDAP.

Note: If you upgrade your LDAP from a pre-SP3 implementation to the SP3 implementation, your Nuance Management Console (NMC) logins will change from being authenticated by the LDAP system to being authenticated by the NMC. This means that users must log in to the NMC using their NMC credentials, not their LDAP credentials.

For the most current information on how to configure LDAP, see the https://isupport.nuance.com website.

Configure LDAP in the Nuance Management Console

Complete the following steps to configure LDAP in the NMC.

Note: If you are upgrading from an earlier version of Dragon and already have single-domain LDAP configured and working, do **not** follow these steps—pre Service Pack 3 single-domain LDAP will work for you.

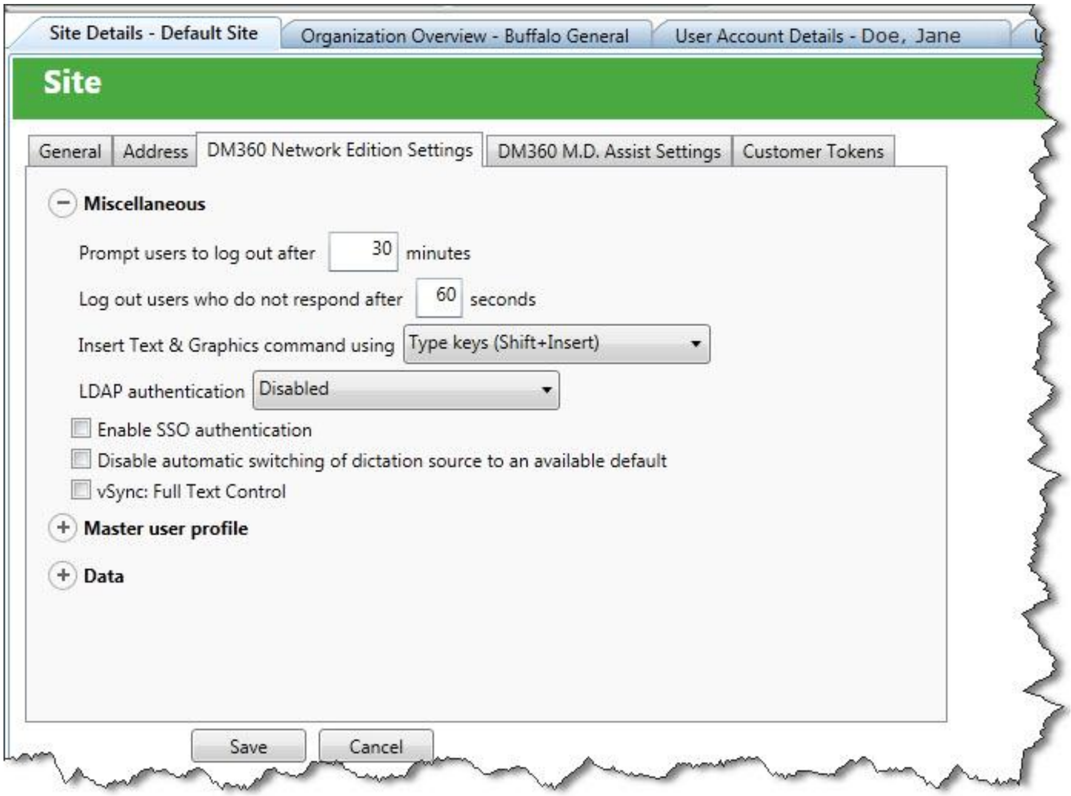
If you plan to upgrade from pre-SP3 single domain LDAP to multiple-domain LDAP, see "*L-3475 Technical Note: Upgrading Pre-SP3 LDAP and SSO to an SP3 Implementation*", found on the https://isupport.nuance.com website.

Configure the Site

Note: Nuance does not recommend having workstations where users log in with credentials for more than one site, where those sites' LDAP settings are different. Imagine, for example, that your system is configured with two sites, Site One and Site Two. Site One has single domain LDAP enabled and Site Two has multiple domain LDAP enabled. A user who has login credentials for both Site One and Site Two should only log in to a given workstation with credentials for one of the sites—she cannot log in to Site One and Site Two on the same workstation.

For each site you are configuring to use LDAP:

1. Select the site that you want to configure for LDAP and click on the **DM360 Network Edition Settings** tab.
2. Click the **+** to expand the **Miscellaneous** section of the tab:


Site Details - Default Site
Organization Overview - Buffalo General
User Account Details - Doe, Jane
Site
General
Address
DM360 Network Edition Settings
DM360 M.D. Assist Settings
Customer Tokens
Miscellaneous
Master user profile
Data
Save
Cancel

Prompt users to log out after 30 minutes

Log out users who do not respond after 60 seconds

Insert Text & Graphics command using: Type keys (Shift+Insert)

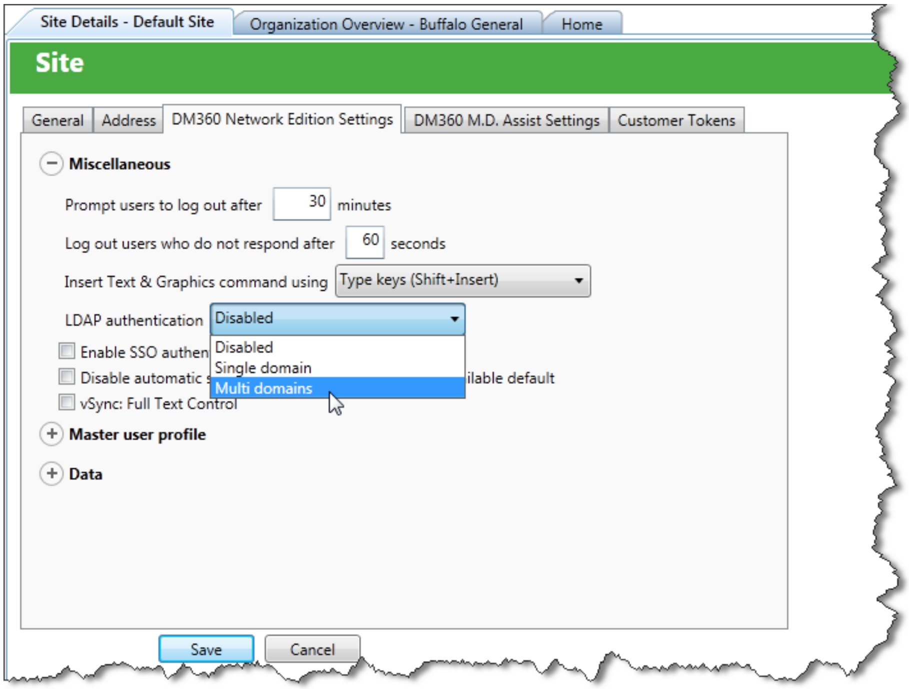
LDAP authentication: Disabled

□ Enable SSO authentication

□ Disable automatic switching of dictation source to an available default

□ vSync: Full Text Control

3. In the **LDAP authentication** drop down, select **Single Domain** or **Multi Domains**.


Site Details - Default Site
Organization Overview - Buffalo General
Home
Site
General
Address
DM360 Network Edition Settings
DM360 M.D. Assist Settings
Customer Tokens
Miscellaneous
Disabled
Single domain
Multi domains
Master user profile
Data
Save
Cancel

Prompt users to log out after 30 minutes

Log out users who do not respond after 60 seconds

Insert Text & Graphics command using: Type keys (Shift+Insert)

LDAP authentication: Disabled

□ Enable SSO authen

□ Disable automatic ilable default

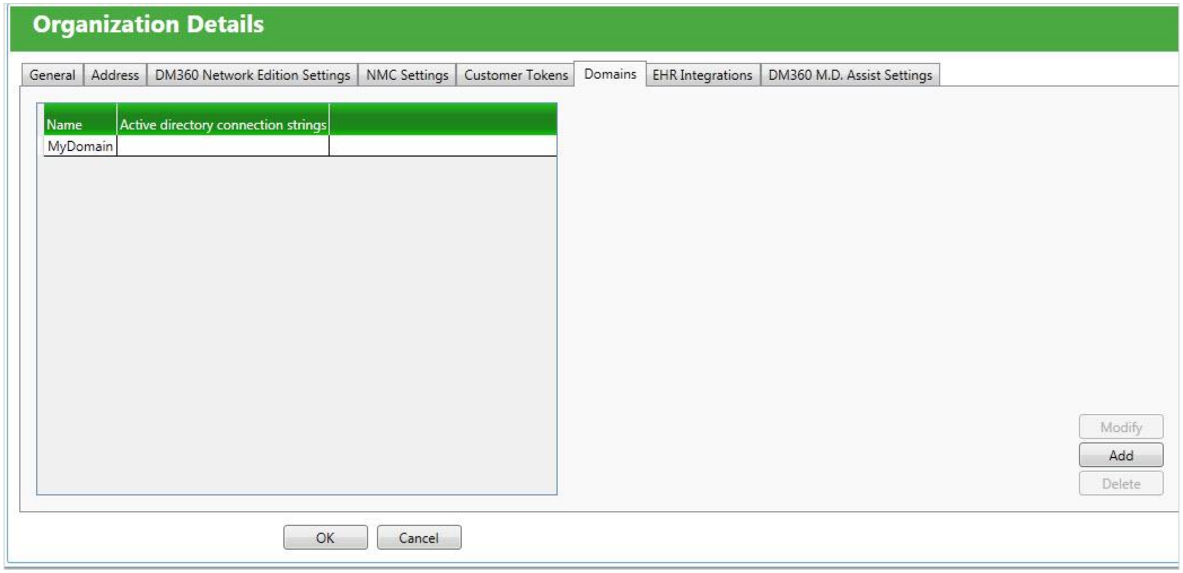
□ vSync: Full Text Control

4. Click **Save** to save your changes.

Configure the Domain(s)

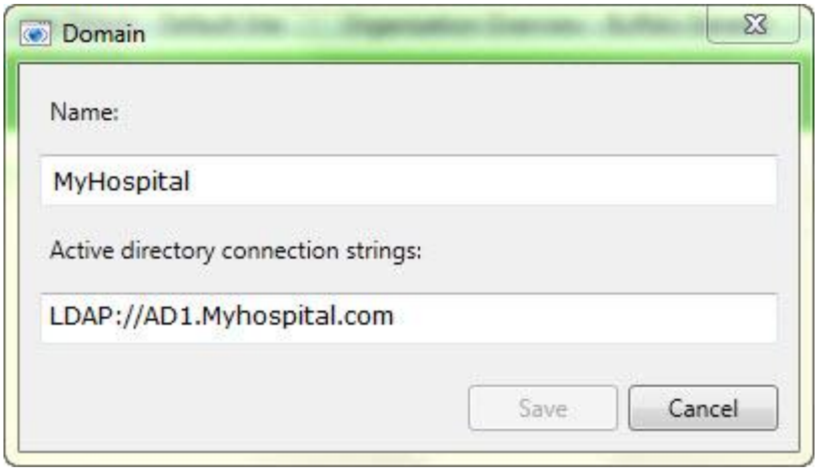
Complete the following steps to add domains to your organization:

1. Click the **Organization Details** icon for the site that you want to configure, then click the **Domains** tab:



Name	Active directory connection strings
MyDomain	

2. Click **Add**. The **Domain** dialog box appears.
3. Enter the domain name in the **Name** field, and the Active Directory connection string for that domain in the **Active directory connection strings:** field:



Name: MyHospital

Active directory connection strings: LDAP://AD1.Myhospital.com

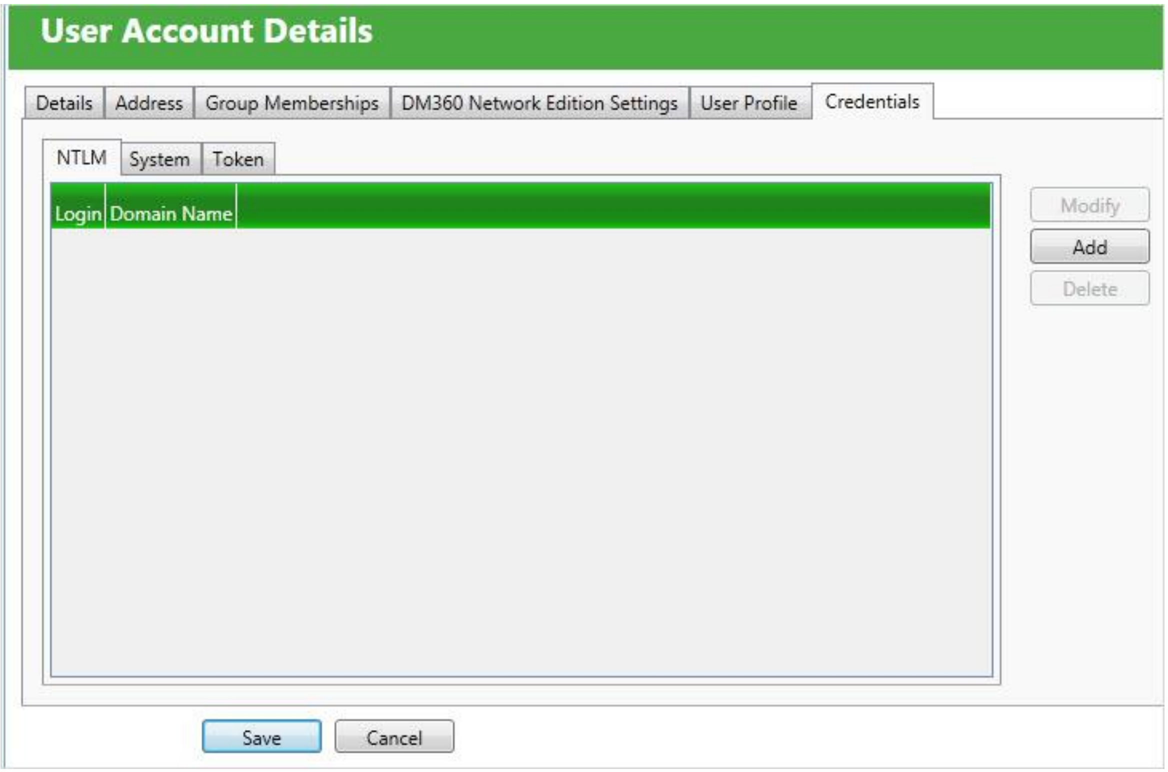
4. Click **Save** to save your changes.
5. Repeat steps 2-4 for every domain that you want to set up.

Configure the User

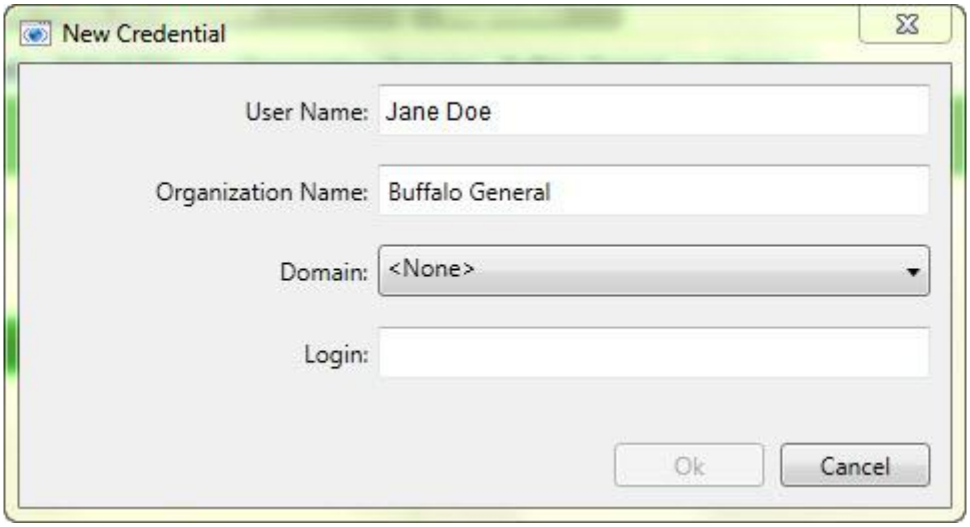
Complete the following steps for each user you want to configure for LDAP.

Note: You can also import users and their LDAP domains and usernames in bulk. See *Import multiple users into the NMS server* on page 18 for more information

1. Open **User Account Details** and select the **Credentials** tab:



2. On the **NTLM** tab, click **Add** to add a new domain mapping. The New Credential dialog appears:



User Name: Jane Doe

Organization Name: Buffalo General

Domain: <None>

Login:

3. The Dragon user name and organization name are already filled out. Use the **Domain** drop down to choose the user's domain, and enter her LDAP login for that domain in the **Login** field.
4. Click **OK** to save your changes.
5. If you have enabled multi-domain LDAP, repeat steps 5-7 for each additional domain you want to configure for this user.

Note: If you are using multi-domain LDAP, be sure to provide your users with their usernames, domain(s) and the appropriate login syntax: `<Domain Name>\<User Name>`.

Install Dragon Client Software with LDAP Enabled

Use the MSI installer to install the Dragon Client with LDAP enabled. Be sure to set the MSI command line option to enable the type of LDAP that you are configuring; `NAS_LDAP_SIGN_ON=1` for single-domain LDAP, and `NAS_LDAP_SIGN_ON=2` for multi-domain LDAP. See the *Dragon Medical Enterprise Network Edition Installation Guide* for more information about the MSI installer and MSI command line options.

Note: Be sure that LDAP is enabled or disabled with the same setting in **both** the Nuance Management Console **and** the Dragon clients. If these settings are out of synch—for example, multi-domain LDAP is enabled in the NMC, but single domain LDAP is enabled on the clients—unpredictable log in behavior results.

Import multiple users into the NMS server

In Dragon Medical Enterprise Network Edition, Service Pack 2, you can use the *Import Users* wizard to import multiple users at one time into the system. You can also assign user account types and licenses to the users and assign the users to specific Groups.

To perform a mass import of users, you must perform the following two main tasks:

1. Create a comma-delimited text file or an XML file that contains information about the users, including user names and passwords.
2. Use the file to import users into the Nuance Management Server.

Creating a file with information about users to import

To import multiple users into the Nuance Management Server (NMS) , you must create either a comma-delimited text file or an XML file that contains user information. The Import Users wizard supports both file types. However, each file must conform to specific formatting standards.

Creating a comma-delimited text file for importing users

The comma-delimited text file can contain the following fields for each user:

- First name (50 characters maximum)
- Last name (50 characters maximum)
- Login id (30 characters maximum)
- Password (30 characters maximum)

The fields must be separated by commas. The First name, Last name, and Login id fields must contain characters. The Password field can be blank.

Example: A comma-delimited text file with user information

The following is an example of a valid text file containing user information.

Notice there is no password in the second example. When importing a comma-delimited file, if the password is blank, you must still place a comma after the login id field and leave the password field blank. The NMS expects four fields in the text file.

```
 Jack, Degnan, jdegnan, pwd124

Tim, Roberts, troberts,

Frank, Fiddler, ffiddler, fflr2
```

Creating an XML file for importing users

The XML file must begin with the XML version declaration processing instruction, <?xml version="1.0"... ?>.

The XML file can contain the following fields for each user. The fields can contain commas.

- First name (required: 1 character minimum, 50 characters maximum)

- Last name (required: 1 character minimum, 50 characters maximum)
- Middle name (50 characters maximum)
- Prefix (10 characters maximum)
- Login id (required: 3 characters minimum, 30 characters maximum)
- Password (required: 30 characters maximum)
- Location (50 characters maximum)
- Department (50 characters maximum)
- Email address (50 characters maximum)
- Street 1 (60 characters maximum)
- Street 2 (60 characters maximum)
- Street 3 (60 characters maximum)
- City (40 characters maximum)
- State (5 characters maximum)
- ZipCode (20 characters maximum)
- NTLMCredential (160 characters maximum) Syntax: `NTLMCredential="<DomainName>\<UserName>"`

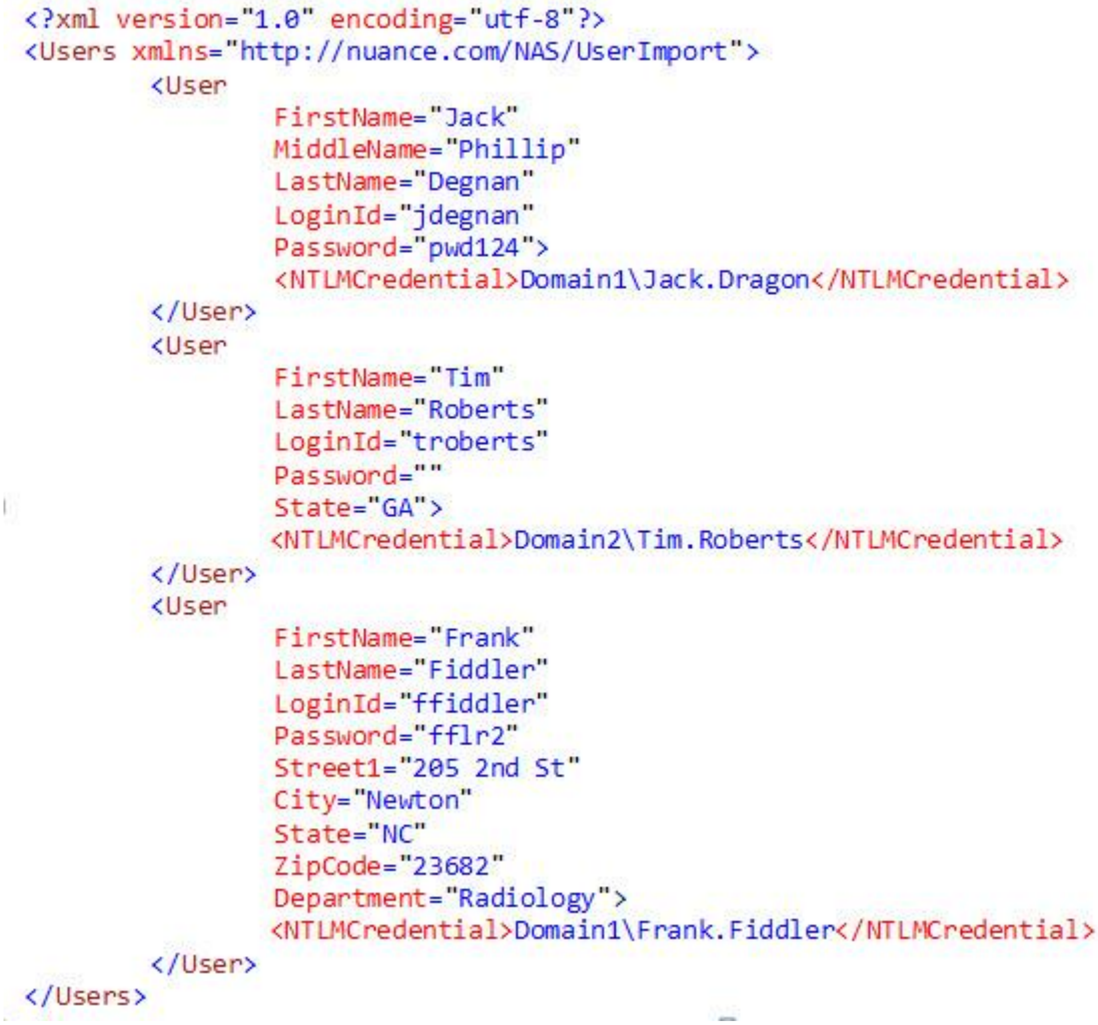
Note: The NTLM Credential element allows you to import a user's domain and user name pair for multi-domain LDAP. For this import to work, you must create an Active Directory connection string entry for each unique `DomainName` that you specify in the NTLMCredential element **before** you run the import. For example if you support two domains, Domain1 and Domain2, you must create an Active Directory connection string entry for each of these domains before you can do a bulk import of users on either domain. See the "Configure the Organization" section of the *Configuring LDAP* on page 13 for instructions on setting the Active Directory connection string.

XML file format

To view the XML schema that defines the file format for the user XML file, see XML schema for the user XML file.

Example: An XML file with user information

The following is an example of a valid XML file containing user information:



```
<?xml version="1.0" encoding="utf-8"?>
<Users xmlns="http://nuance.com/NAS/UserImport">
        <User
                FirstName="Jack"
                MiddleName="Phillip"
                LastName="Degnan"
                LoginId="jdegnan"
                Password="pwd124">
                <NTLMCredential>Domain1\Jack.Dragon</NTLMCredential>
        </User>
        <User
                FirstName="Tim"
                LastName="Roberts"
                LoginId="troberts"
                Password=""
                State="GA">
                <NTLMCredential>Domain2\Tim.Roberts</NTLMCredential>
        </User>
        <User
                FirstName="Frank"
                LastName="Fiddler"
                LoginId="ffiddler"
                Password="fflr2"
                Street1="205 2nd St"
                City="Newton"
                State="NC"
                ZipCode="23682"
                Department="Radiology">
                <NTLMCredential>Domain1\Frank.Fiddler</NTLMCredential>
        </User>
</Users>
```

If the user import field is not required, you can omit the attribute. The attributes can be placed in any order in the XML file. The Users and User elements are in the following default XML name space:

`http://nuance.com/NAS/UserImport`

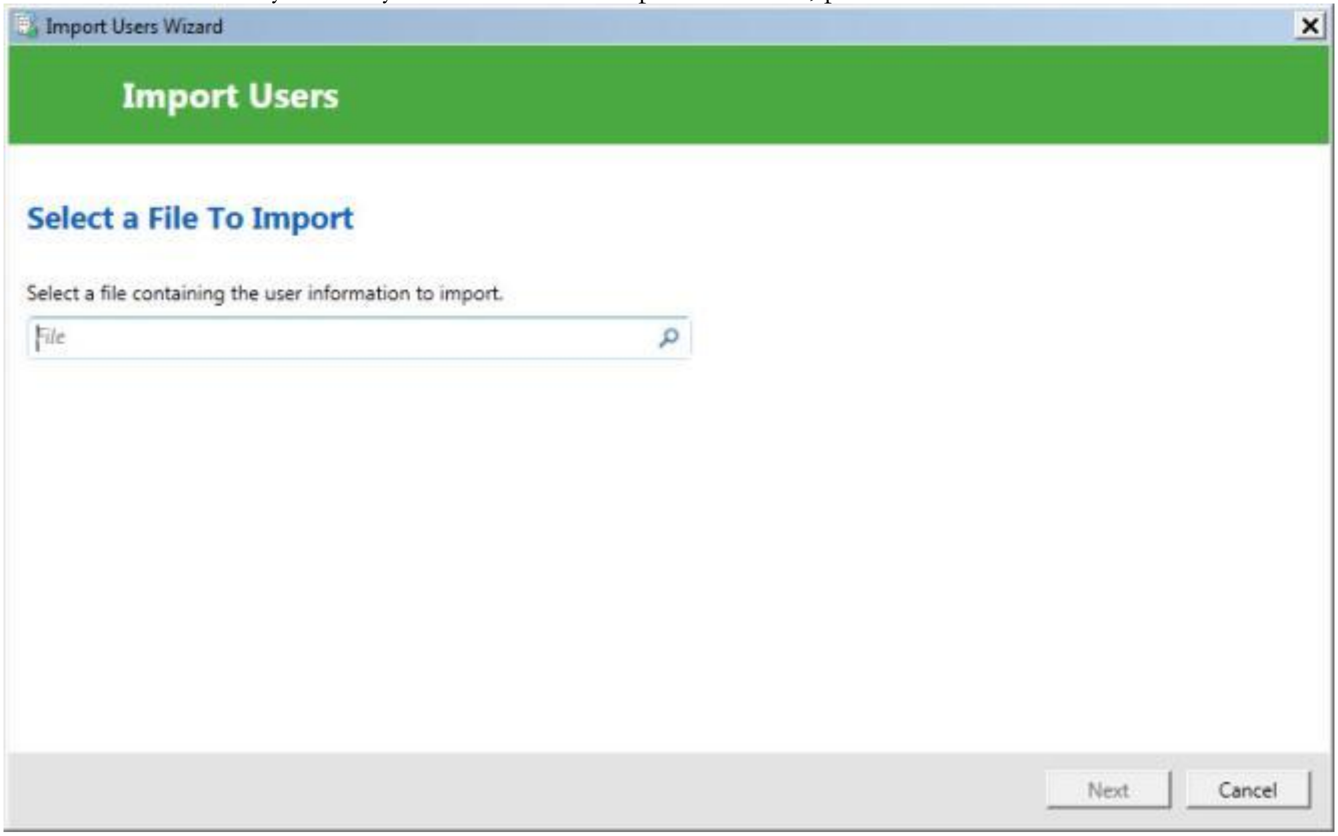
Importing users into the Nuance Management Server

After you create a comma-delimited text file or an XML file that contains user information, you must use the file and the Nuance Management Console to import users into the system.

At any time in the following steps, you can press **Cancel** to exit a step and stop the import process. You can also press **Back** to return to the previous screen in the *Import Users* wizard.

1. In the NMC, select the **User Accounts** tab.
2. Select **Import User Accounts**. The *Import Users* wizard appears.

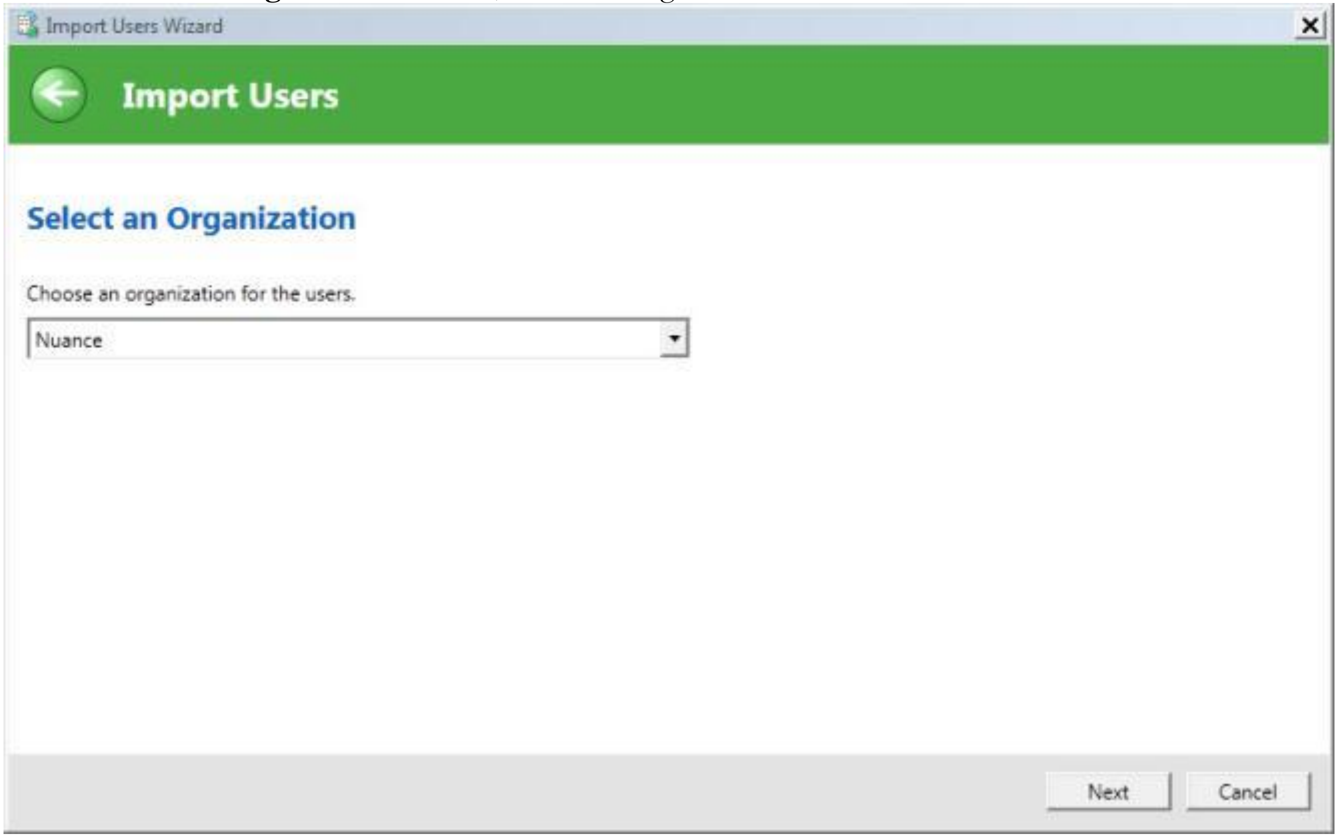
3. In the **Select a File To Import** screen, enter the path and name of the file that contains the user information. If for any reason you decide to not import the users, press **Cancel**.



4. If the path and name of the text file are valid, the **Next** button is enabled. Press **Next**. If the *Import Users* wizard has trouble parsing the data from the text file or simply cannot find any users in the text file, the wizard displays a message that tells you no users were found. Press **OK** to close the message. You may now re-enter the name of the text file or make changes to the existing text file and retry this step.
5. The **Users to Import** screen displays information about the users from the text file.
6. Review the list of users to import. Press **Next** to continue. If you wish to cancel the import of users, press **Cancel**. To return to the previous page, press **Back**.

   If the *Import Users* wizard encounters errors when importing the user data, the NMC displays a message. Press **Close** on the dialog to leave this step.

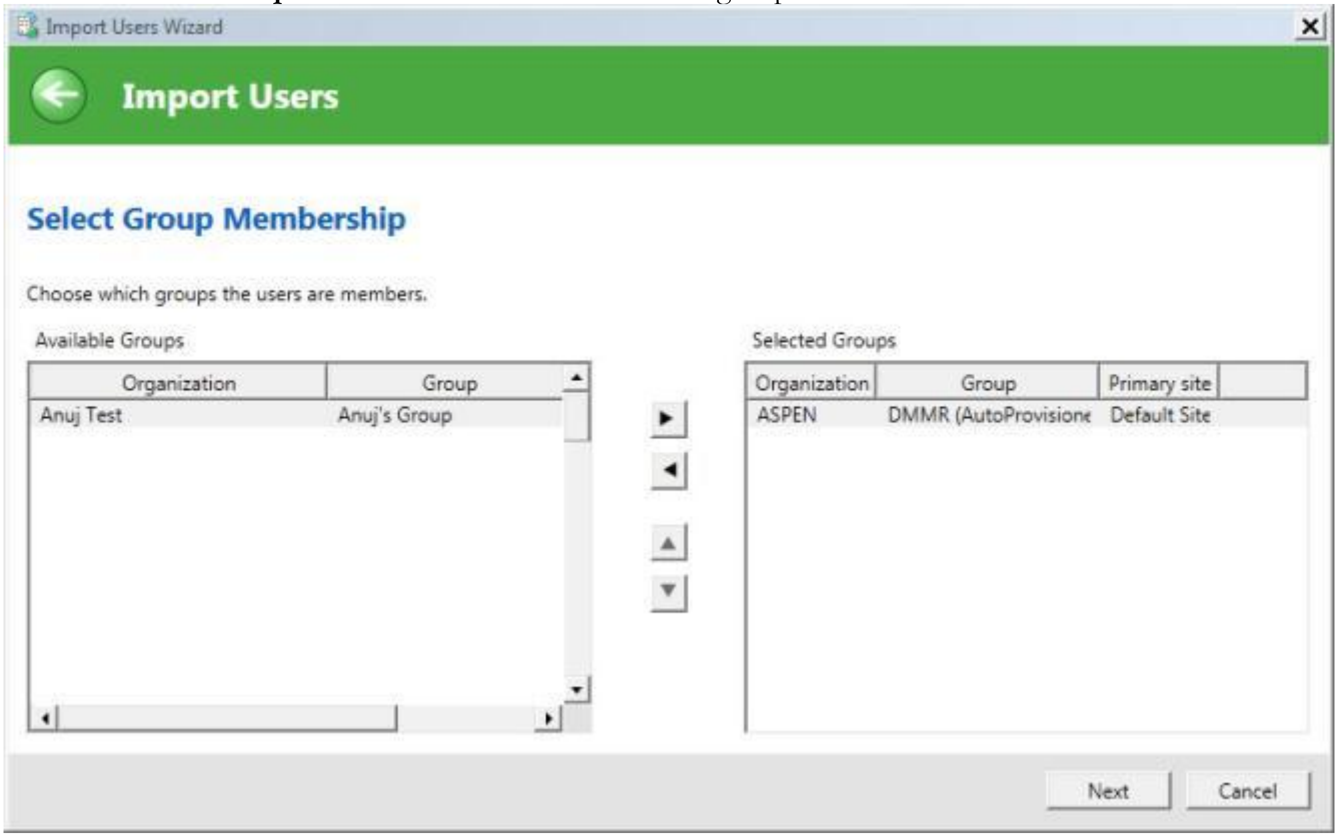
7. On the **Select an Organization** screen, select the organization to associate with the users.



8. Press **Next**.

9. The **Select Group Membership** screen displays a list of groups that you can associate with the users. In **Available Groups**, select one or more groups. User the arrows to move the selected groups

to the **Selected Groups** list. You must select at least one group.



Select Group Membership

Choose which groups the users are members.

Available Groups

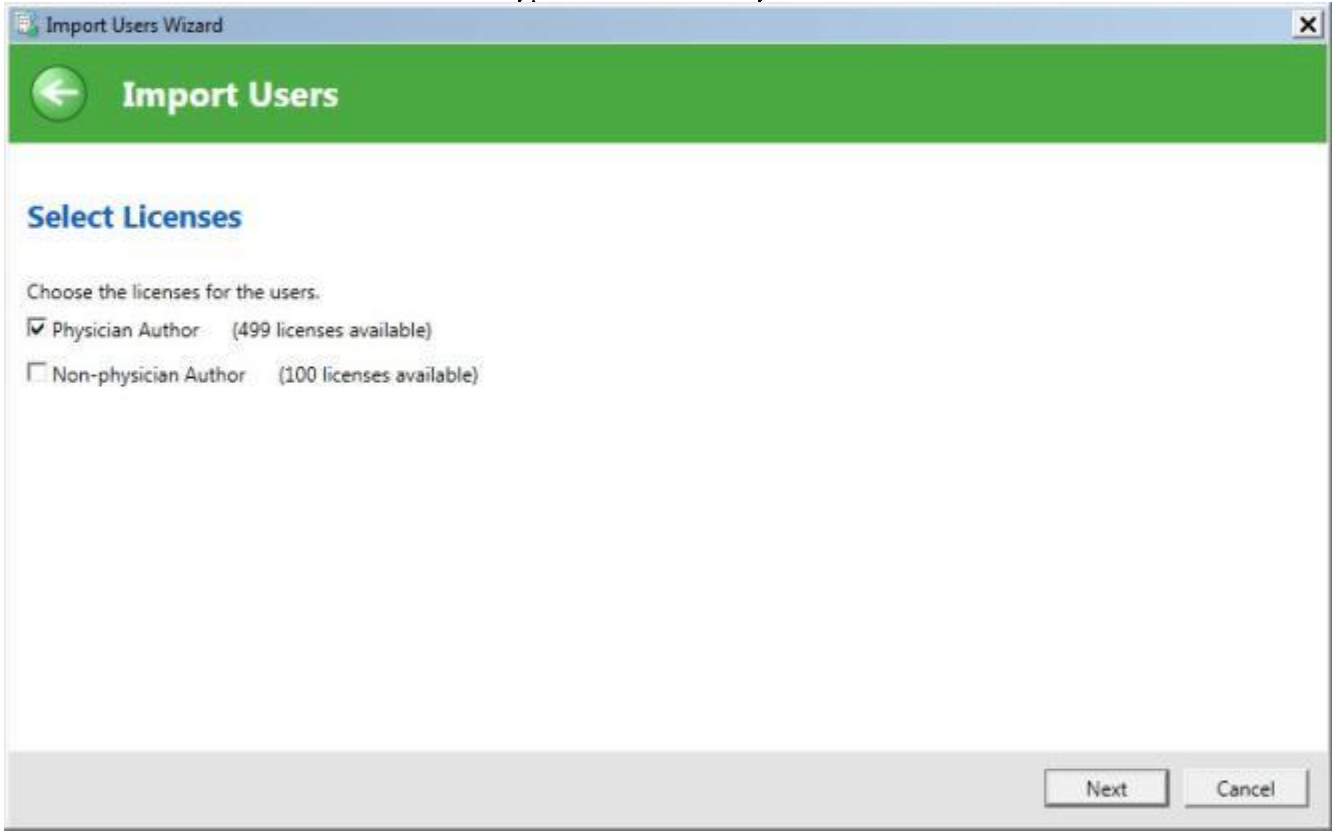
Organization	Group
Anuj Test	Anuj's Group

Selected Groups

Organization	Group	Primary site
ASPEN	DMMR (AutoProvisione	Default Site

10. Press **Next**. If you do not have the administrative rights to grant licenses to users, proceed to step .
11. If you have the administrative rights to grant licenses to users, the *Import Users* wizard displays the **Select Licenses** screen. The screen lists all the licenses that you can grant to the users. The list displays the license type and the number of available licenses for each license type.
    You cannot apply a license type to the users if the number of available licenses is less than the

number of users In this case, the license type is disabled and you cannot select it in the screen.



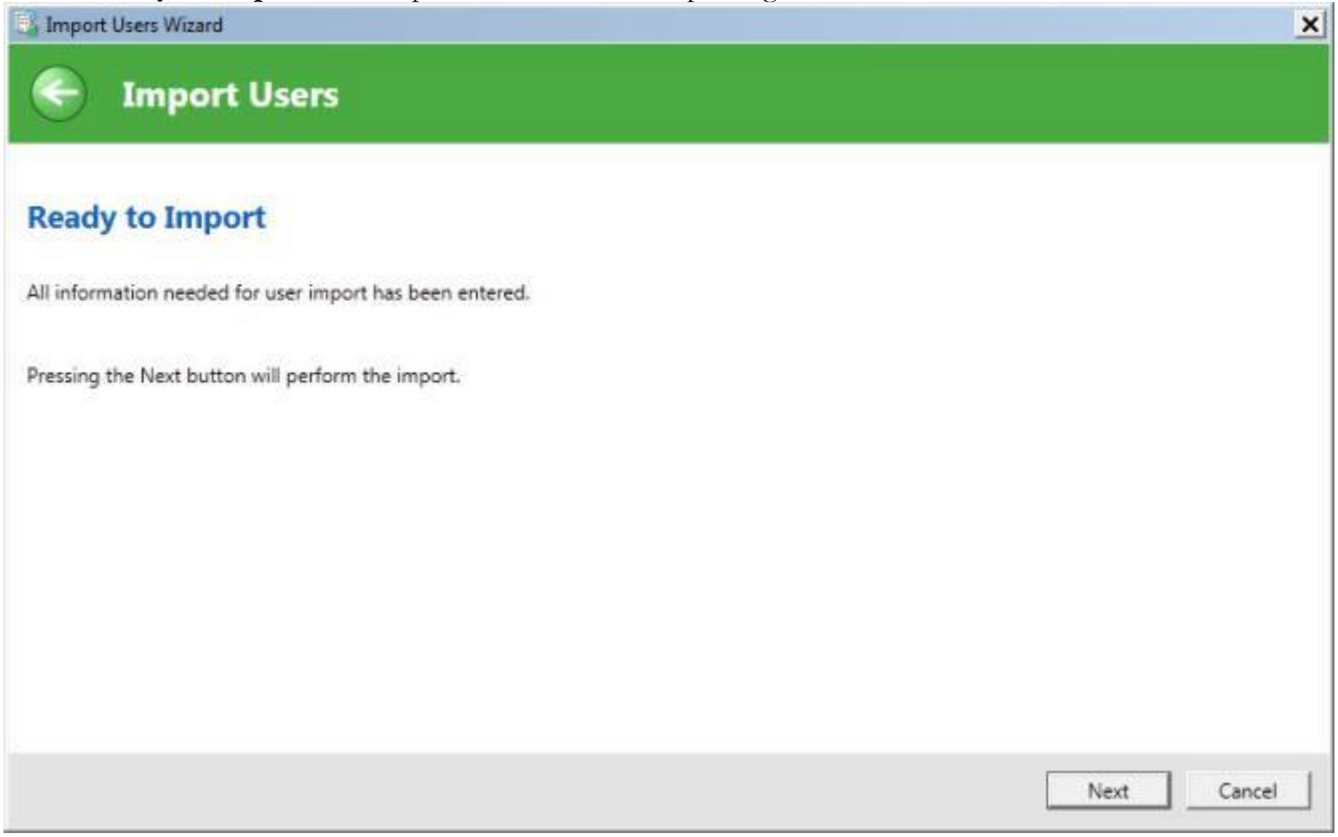
Select Licenses

Choose the licenses for the users.

☑ Physician Author (499 licenses available)

□ Non-physician Author (100 licenses available)

12. Optional: Select the licenses to apply to the users. Press **Next**.
13. In the **Ready to Import** screen, press **Next** to start importing the users.

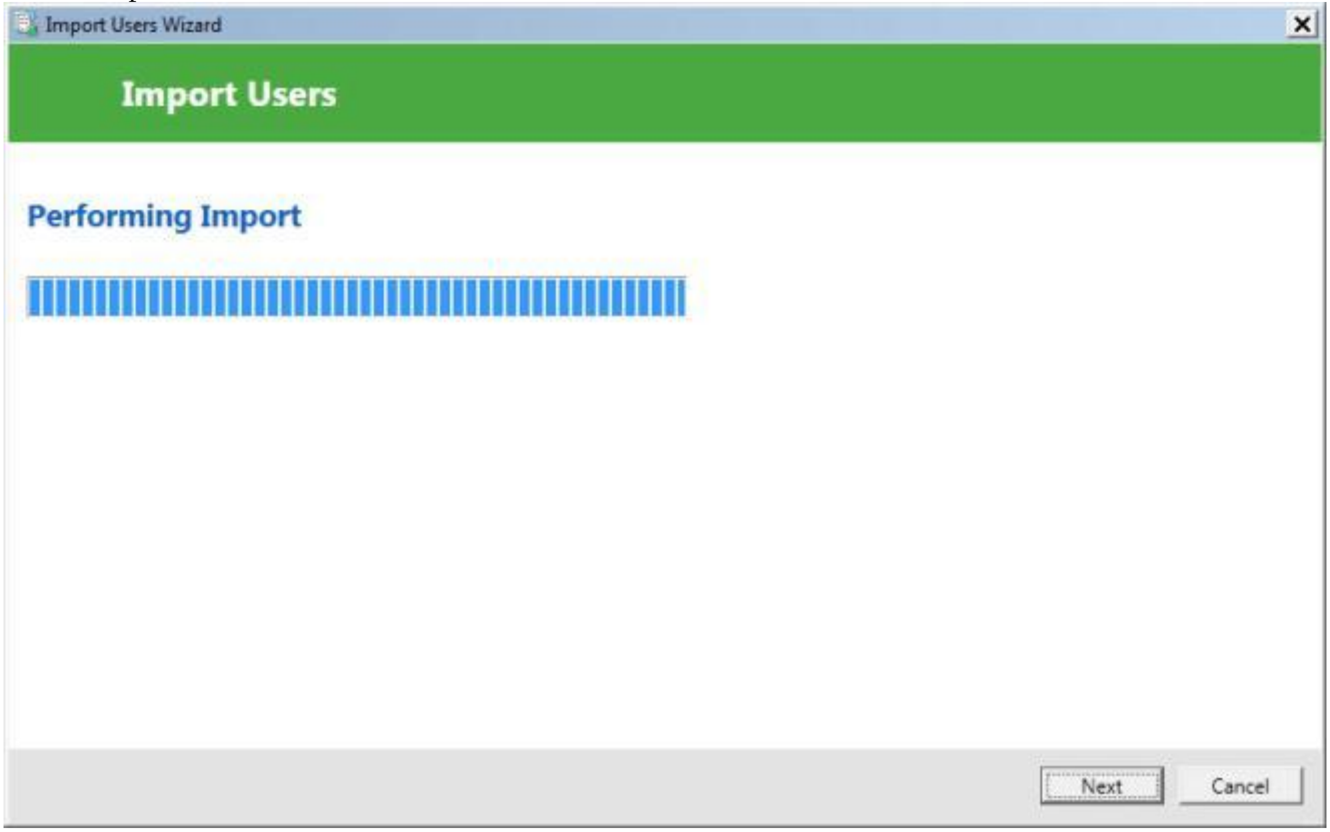


Ready to Import

All information needed for user import has been entered.

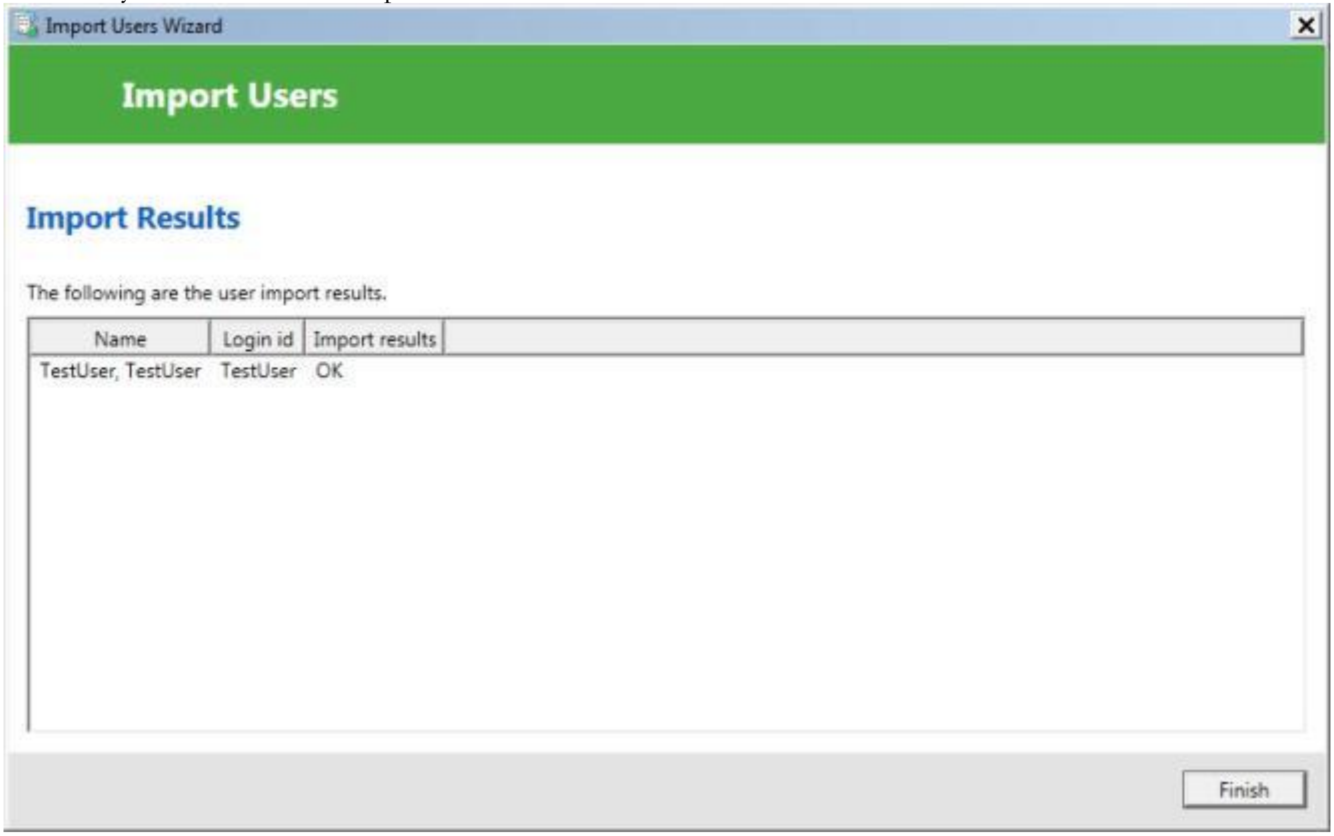
Pressing the Next button will perform the import.

14. The *Import Users* wizard displays the **Performing Import** screen and starts to import the users. A progress indicator displays the status of the import process. When the wizard finishes importing all the users, press **Next**.



15. The **Import Results** screen displays a list of all the users that the *Import Users* wizard imported into the system. If the wizard could not import a user, the Import Results screen displays information

about why the user was not imported.



Import Users

Import Results

The following are the user import results.

Name	Login id	Import results
TestUser, TestUser	TestUser	OK

16. Press **Finish**.

XML schema for the user XML import file

The following schema defines the file format for any XML file that contains user information for importing users into the system.

```
<?xmlversion="1.0"encoding="utf-8"?>      <xs:schema
    id="UserImportSchema"
    targetNamespace="http://nuance.com/NAS/UserImport"
    elementFormDefault="qualified"
    xmlns="http://nuance.com/NAS/UserImport"
    xmlns:mstns="http://nuance.com/NAS/UserImport"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" >

    <!-- Users element -->
    <xs:elementname="Users"type="Users">
        <xs:annotation>
            <xs:documentation>A collection of users to import</xs:documentation>
        </xs:annotation>
    </xs:element>

    <!-- Users type definition -->
    <xs:complexTypename="Users">
        <xs:annotation>
            <xs:documentation>This types defines the user
collection</xs:documentation>
        </xs:annotation>
        <xs:sequence>
            <xs:elementname="User"type="User"minOccurs="1"maxOccurs="unbounded">
                <xs:annotation>
                    <xs:documentation>One of more users to import</xs:documentation>
                </xs:annotation>
            </xs:element>
        </xs:sequence>
    </xs:complexType>

    <!-- User type definition -->
    <xs:complexTypename="User">
```

```
        <xs:annotation>
            <xs:documentation>This type defines the basic user information that can be
imported</xs:documentation>
        </xs:annotation>
        <xs:attributename="LastName"type="NameString"use="required"/>
        <xs:attributename="FirstName"type="NameString"use="required"/>
        <xs:attributename="MiddleName"type="NameString" />
        <xs:attributename="Prefix"type="PrefixString"/>
        <xs:attributename="LoginId"type="LoginIdString"use="required"/>
        <xs:attributename="Password"type="PasswordString"use="required"/>
        <xs:attributename="Location"type="GeneralInfoString" />
        <xs:attributename="Department"type="GeneralInfoString"/>
        <xs:attributename="EmailAddress"type="GeneralInfoString"/>
        <xs:attributename="Street1"type="StreetAddressString"/>
        <xs:attributename="Street2"type="StreetAddressString"/>
        <xs:attributename="Street3"type="StreetAddressString"/>
        <xs:attributename="City"type="CityString"/>
        <xs:attributename="State"type="StateString"/>
        <xs:attributename="ZipCode"type="ZipString"/>
    </xs:complexType>

    <!-- Name String -->
    <xs:simpleTypename="NameString">
        <xs:annotation>
            <xs:documentation>A general string from names (50 characters
maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:minLengthvalue="1"/>
            <xs:maxLengthvalue="50"/>
        </xs:restriction>
    </xs:simpleType>

    <!-- Login Id String -->
    <xs:simpleTypename="LoginIdString">
        <xs:annotation>
```

```
            <xs:documentation>A string that contains the user's login id (30 
characters maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:minLengthvalue="3"/>
            <xs:maxLengthvalue="30"/>
        </xs:restriction>
    </xs:simpleType>

    <!--  Password String -->
    <xs:simpleTypename="PasswordString">
        <xs:annotation>
        <    xs:documentation>A string for the user's login password (30 characters 
maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:maxLengthvalue="30"/>
       </xs:restriction>
    </xs:simpleType>

    <!-- Prefix String -->
    <xs:simpleTypename="PrefixString">
        <xs:annotation>
            <xs:documentation>A user name prefix (10 characters 
maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:maxLengthvalue="10"/>
        </xs:restriction>
    </xs:simpleType>

    <!-- General Info String -->
    <xs:simpleTypename="GeneralInfoString">
        <xs:annotation>
            <xs:documentation>A general information string (50 characters 
maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:maxLengthvalue="50" />
        </xs:restriction>
    </xs:simpleType>

    <!-- Street Address String -->
    <xs:simpleTypename="StreetAddressString">
        <xs:annotation>
            <xs:documentation>A street address string (60 characters
maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:maxLengthvalue="60"/>
        </xs:restriction>
    </xs:simpleType>

    <!-- City String -->
    <xs:simpleTypename="CityString">
        <xs:annotation>
            <xs:documentation>A city string (40 characters maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:maxLengthvalue="40"/>
        </xs:restriction>
    </xs:simpleType>

    <!-- State String -->
    <xs:simpleTypename="StateString">
        <xs:annotation>
            <xs:documentation>A state string (5 characters maximum)</xs:documentation>
        </xs:annotation>
        <xs:restrictionbase="xs:string">
            <xs:maxLengthvalue="5"/>
        </xs:restriction>
    </xs:simpleType>
    <!-- Zip String -->

    <xs:simpleTypename="ZipString">

        <xs:annotation>

            <xs:documentation>A zip code string (20 characters
maximum)</xs:documentation>

        </xs:annotation>

        <xs:restrictionbase="xs:string">

            <xs:maxLengthvalue="20"/>

        </xs:restriction>

    </xs:simpleType>

    <!— -NTLM Credential String -->

    <xs:simpleType name="NTLMCredentialString">

        <xs:annotation>

            <xs:documentation>A NTLM Credential string (160 characters
max)</xs:documentation>

        </xs:annotation>

        <xs:restriction base="xs:string">

            <xs:maxLength value="160"/>

        </xs:restriction>

    </xs:simpleType>

</xs:schema>
```