Nuance Management Center
Server installation and configuration guide

For:

Nuance®
Dragon® Professional
Group

Nuance®
Dragon® Legal
Group

Nuance®
**Dragon®
Law Enforcement**

Cloud version 2022.3.3

NUANCE

Copyright

Nuance ® Management Center

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

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

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

© Nuance Communications Inc. 2022

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

Disclaimer

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

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

Notice

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

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

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

Contents

About this guide

Guide overview

This guide contains configuration instructions for single-sign-on authentication using Nuance's cloud-hosted NMC server.

Audience

This guide is intended for administrators whose responsibility is to perform the following:

- Set up and manage single sign-on user authentication.

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

Additional resources

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

Documentation

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

Training

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

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

Support

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

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

Chapter 1: Introduction

About Nuance Management Center

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

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

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

Physical architecture

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

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

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

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

Chapter 2: Preparing for your installation

Security considerations

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

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

General security principles

- Require strong, complex user account passwords.

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

- Keep passwords secure.

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

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

- Keep software up-to-date.

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

- Implement the principle of Least Privilege.

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

- Monitor system activity.

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

- Promote policy awareness.

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

Installing and configuring Nuance Management Center securely

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

- Establish best practices for downloading report data.

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

Nuance Management Center security features

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

Authentication

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

Authentication methods

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

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

Password settings

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

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

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

Auditing

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

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

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

User Access Control

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

Assigning privileges

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

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

Assigning grants

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

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

Disabling inactive users

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

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

Installing and configuring IIS securely

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

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

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

For more information, see the following Microsoft article:

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

Opening required ports

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

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

Chapter 3: Post-installation tasks

Configuring the Dragon client for use with Nuance Management Center

Applies to: Dragon desktop products only

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

For more information on configuring Dragon clients for use with Nuance Management Center, see the "Associating Dragon clients with the Nuance Management Center server or Local Authenticator" chapter in the *Dragon Client Installation Guide*.

Chapter 4: Preparing for your Active Directory single sign-on configuration

Single sign-on overview

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

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

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

Before you begin

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

Software requirements

Cloud NMC server

- Local Authenticator service

  You download the Local Authenticator installation file from your NMC console. For more information, see "About the Local Authenticator" on page 20.

- Server on which to install the Local Authenticator with the following:

  - Latest version of the Microsoft .NET Framework installed

  - One of the following operating systems:

    - Microsoft® Windows Server 2012

    - Microsoft® Windows Server 2012 R2 (64 bit)

    - Microsoft® Windows Server 2016

    - Microsoft® Windows Server 2019

- SSL certificate, issued by a certificate authority (CA)

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

On-premise NMC server

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

Other requirements

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

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

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

  SetSPN.exe is included with Microsoft's Windows Support Tools. If this package is not already installed on a computer in your domain, you can download it. For more information, see "Running the SetSPN.exe Windows utility" on page 18.

Checklist—Planning the single sign-on setup

	Task	Reference
☐	Review software requirements	"Software requirements" on page 13
☐	Open port 389 TCP.	"Opening required ports" on page 1
☐	Create an NMC console	"Creating an NMC console Administrator user for Active

	Task	Reference
	administrator account for Active Directory	Directory" on page 15
☐	Set the Active Directory connection string	"Setting the Active Directory connection string" on page 16
☐	Create and configure user accounts in the NMC console	"Creating and configuring user accounts for single sign-on" on page 17
☐	Run the SetSPN.exe Windows utility (Kerberos authentication only)	"Running the SetSPN.exe Windows utility" on page 18
☐	Download the Local Authenticator	"Downloading the Local Authenticator" on page 23
☐	Create an organization token	"Creating organization tokens" on page 24
☐	Install the Local Authenticator	"Installing the Local Authenticator" on page 25
☐	Install and bind the SSL certificate on the Local Authenticator server	"Installing and binding the SSL certificate" on page 29
☐	Edit the Local Authenticator configuration file	"Editing the configuration file" on page 33
☐	Start the Local Authenticator service	"Starting the Local Authenticator service" on page 34
☐	Associate Dragon clients with the Local Authenticator **Applies to:** Dragon desktop products only	See the "Configuring the Dragon Client for Nuance Management Center" chapter in the *Dragon Client Installation Guide*. This step assumes you have already installed Dragon clients.

Creating an NMC console Administrator user for Active Directory

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

1. Log in to the NMC console.

2. From the Menu bar, select **User Accounts**.

3. In the **User Accounts** ribbon, click the **Add** icon.

   The **User Account Details** window opens.

4. Configure the following minimum settings:

   - **Details tab**—First Name, Last Name, and Login.

   - **Group Memberships tab**—Add the administrator to a group.

   - **Messaging tab**—Configure email settings to allow the administrator to receive messages from the NMC console.

5. Click **Save**.

Setting the Active Directory connection string

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

   The **Organization Details** screen appears.

2. Click the **Domains** tab.

3. Click **Add**.

   The **Domain** dialog box appears.

4. Enter the following:

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

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

   Ask your Active Directory domain administrator for the correct connection string. When Active Directory is enabled, Nuance Management Center sends all authentication requests to this server.

5. Click **Save**.

6. Repeat steps 3-5 as needed for each domain.

Creating and configuring user accounts for single sign-on

Creating user accounts

If you have not already created user accounts in the NMC console, you must create them before enabling single sign-on. You can create user accounts manually in the NMC console, or you can batch-create them by importing an XML file. You can include each user's NTLM credentials in the XML file. When you create user accounts, each user's login must match that user's Windows domain login exactly.

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

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

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

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

Configuring user accounts

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

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

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

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

Running the SetSPN.exe Windows utility

About SetSPN.exe

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

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

You run the utility only when you're using Kerberos authentication instead of NTLM. You run the SetSPN.exe utility only once at any time before, during, or after your Nuance Management Center installation, regardless of whether you're using the Nuance cloud-hosted NMC server or your own on-premise NMC server.

Downloading SetSPN.exe

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

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

Executing SetSPN.exe

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

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

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

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

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

Chapter 5: Installing the Local Authenticator

About the Local Authenticator

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

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

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

Supported authentication types

The Local Authenticator supports the following authentication types:

- Windows integrated authentication
- HTTPS authentication with TLS 1.2 support

In HTTPS authentication mode, credentials are validated against a local LDAP store. When credentials are validated locally, the local authenticator validates with the Nuance cloud-hosted server using token credentials.

Local Authenticator logs

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

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

Local Authenticator requirements

- Local Authenticator service

  You download the Local Authenticator installation file from your NMC console.

- Server on which to install the Local Authenticator with the following:

  - Quad-Core server

    - 2 GHz CPU

    - 8GB minimum RAM

    - 4.0GB disk storage

  - Latest version of the Microsoft .NET Framework installed

  - One of the following operating systems:

    - Microsoft® Windows Server 2012

    - Microsoft® Windows Server 2012 R2 (64 bit)

    - Microsoft® Windows Server 2016

    - Microsoft® Windows Server 2019

- SSL certificate, issued by a certificate authority (CA)

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

Local Authenticator best practices

- Nuance does not provide or maintain SSL certificates for the Local Authenticator. SSL certificate management is the responsibility of the customer. Nuance recommends adding the SSL certificate utilized by the Local Authenticator to any existing monitoring/alerting tools used by your organization to monitor SSL certificate expiration. This helps prevent unintended service interruption related to an expired certificate.

- Nuance recommends adding the Local Authenticator service to any existing service monitoring tools currently utilized by your organization. This helps ensure the service is always running and automatically restarted if not in a running state. Doing so helps prevent unintended service interruptions related to a non-running Local Authenticator service.

Downloading the Local Authenticator

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

To download the Local Authenticator:

1. Log in to your NMC console as an administrator.

2. In the Utilities ribbon, click **Tools**.

   The Tools page appears.

3. Click **Install local authenticator**.

   A message appears, prompting you to save or run the Local Authenticator executable.

4. Click **Save**.

   The `LocalAuthenticator.exe` file is saved to your local Downloads folder.

5. Copy the `LocalAuthenticator.exe` file to the local server on which you are installing it.

Creating organization tokens

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

To create an organization token:

1. From the menu bar, select **Sites** > **Organization Overview**.

2. Right-click your organization, and then select **Details**.

   The Organization Details page appears.

3. Click the Organization Token tab.

4. Click **Add** to generate a new organization token.

   The Organization Token Info dialog box appears. The **Organization Token** field is pre-populated with a system-generated token.

5. Enter text in the **Comment** field to describe the token's use. This can help with troubleshooting, if it's necessary.

   For example, **Local Authenticator Token**.

6. Copy the token number, paste it into a new Notepad document, and then save the file for later use.

   You must provide this number during the Local Authenticator installation.

7. Click **Save**.

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

Installing the Local Authenticator

On the server where you are installing the Local Authenticator:

1. Run the `LocalAuthenticator.exe` file.

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

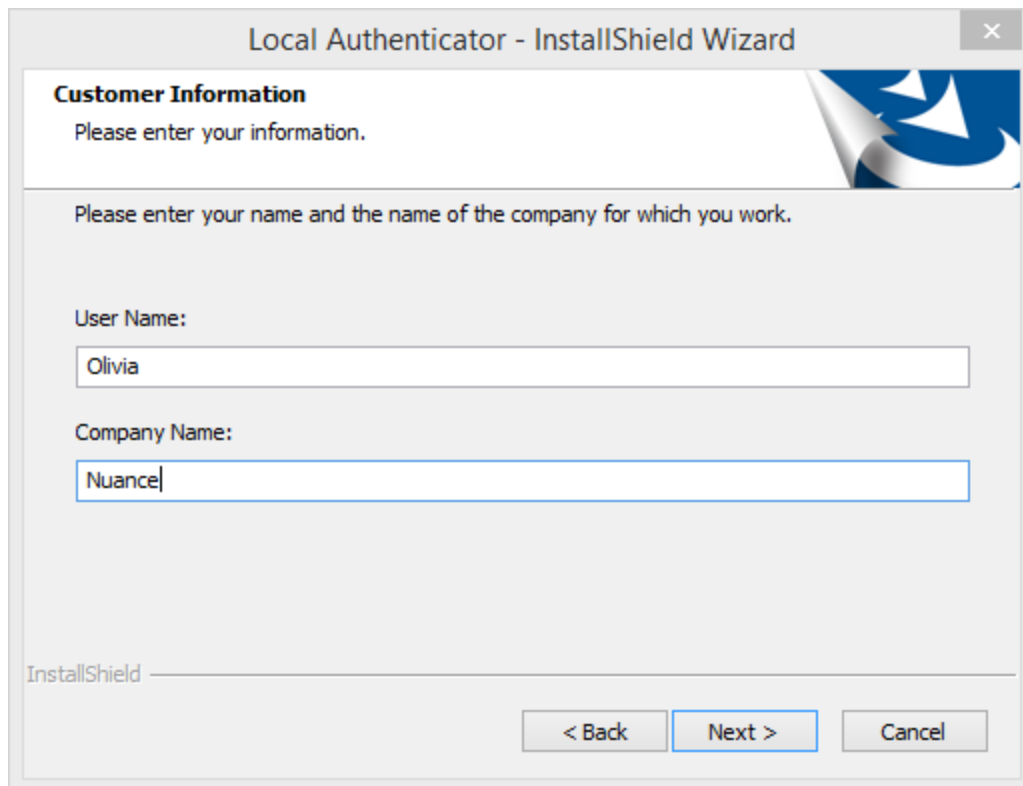2. Select your language from the drop-down list, and then click **OK**.
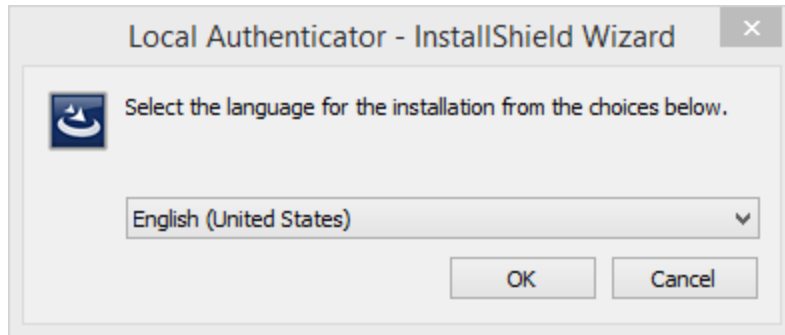
   The InstallShield Wizard opens.
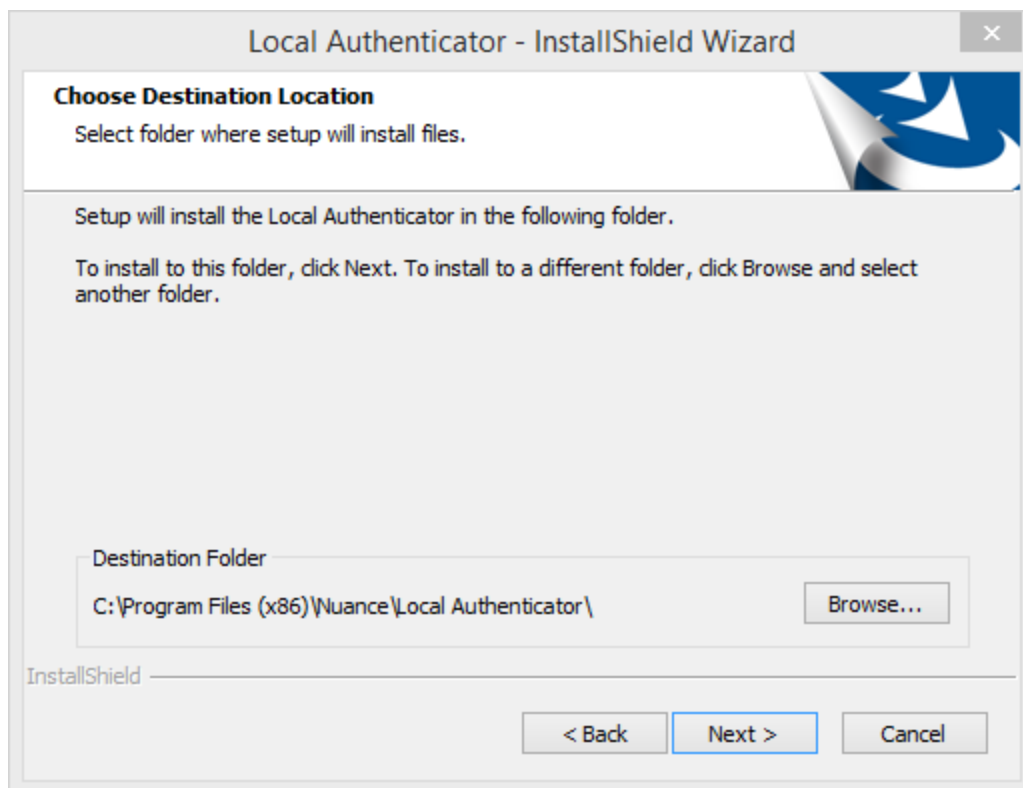
3. Click **Next**.
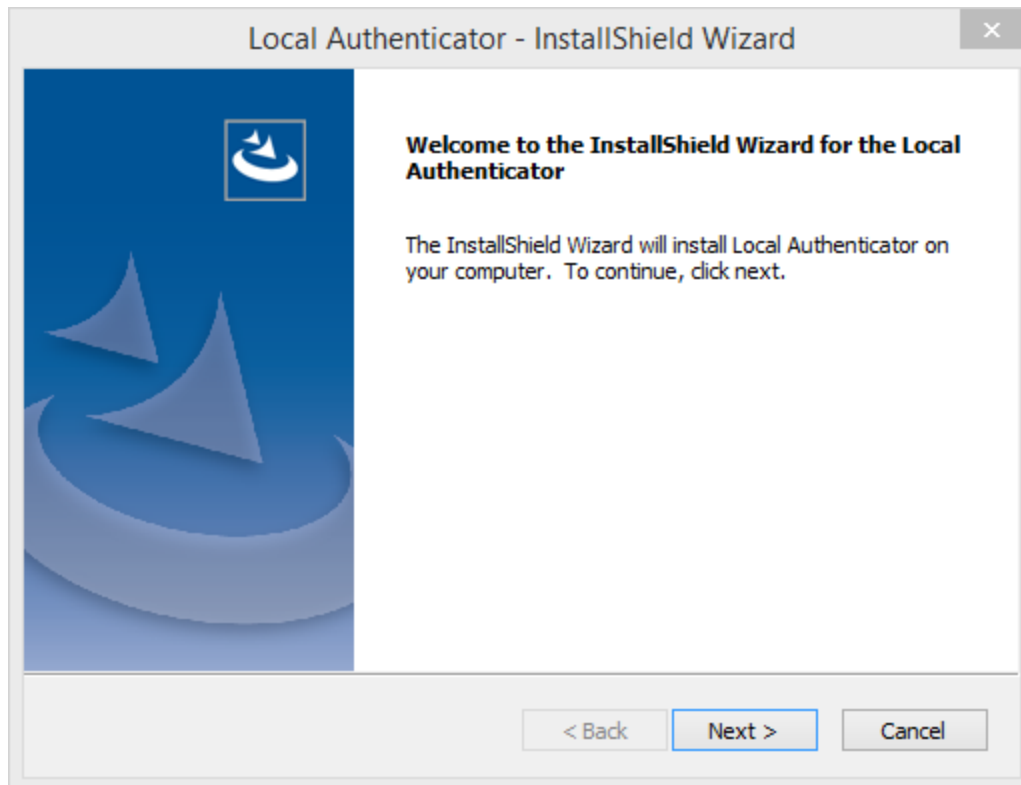
4. Leave the default value in the **User Name** field, and enter your company name in the **Company** field. Then, click **Next**.

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

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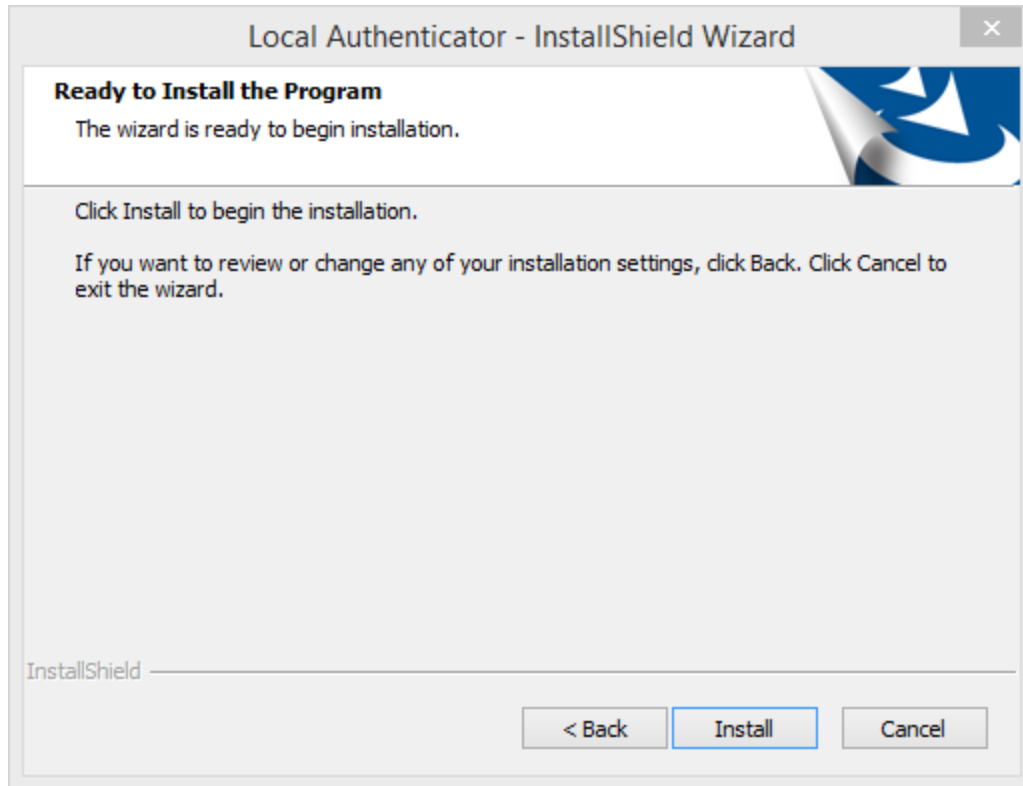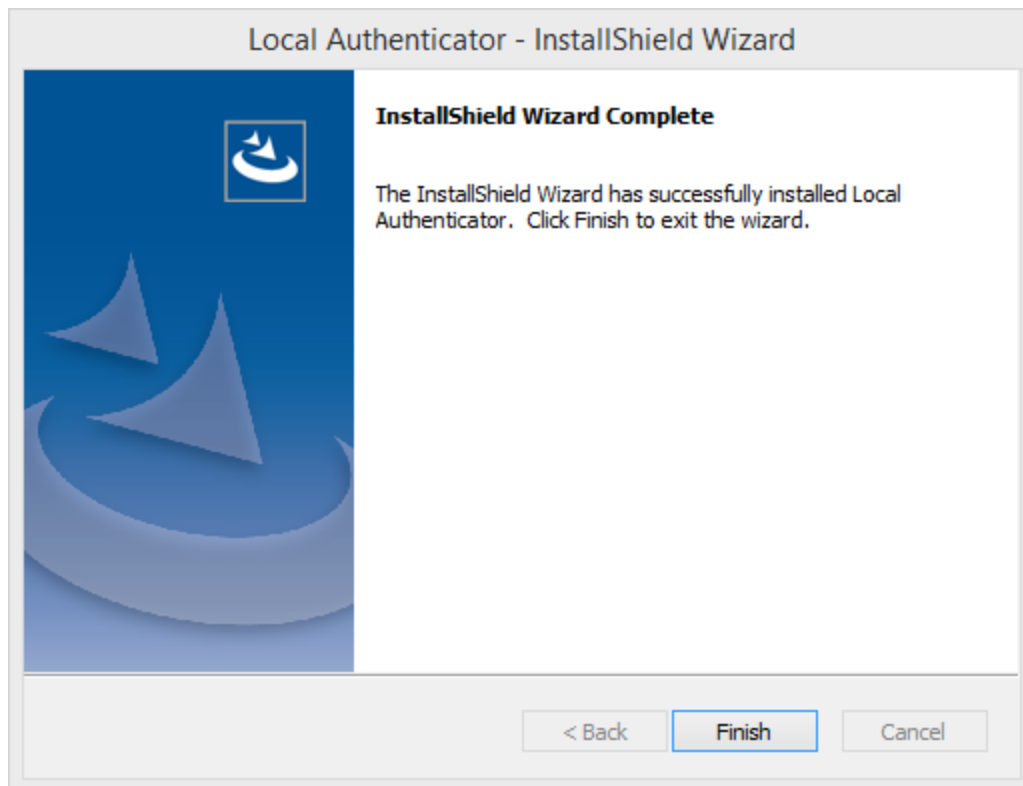
7. Click **Install**.

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

Installing and binding the SSL certificate

About signed certificates

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

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

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

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

For more detailed information on installing SSL certificates, see:

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

Install the SSL certificate

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

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

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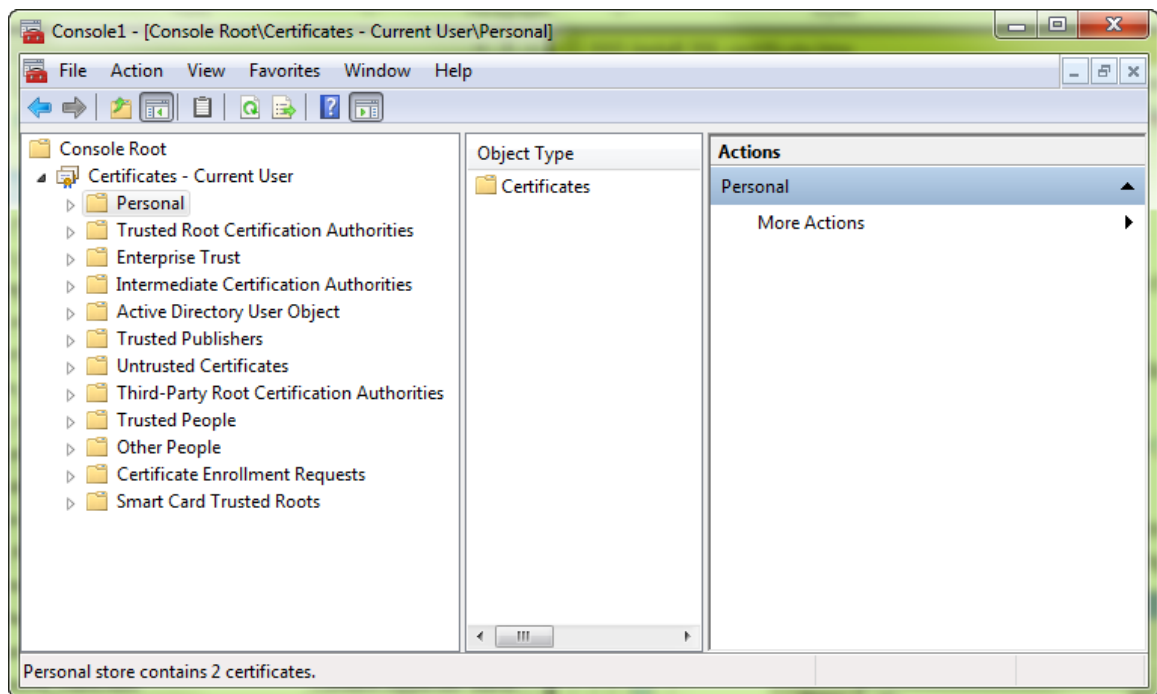
2. Note the subject of the certificate.

    This should match the computer name that the certificate is deployed on, or be a wild card. This must match exactly the host used in the endpoints. For information on viewing the subject, see https://technet.microsoft.com/en-us/library/cc754686(v=ws.10).aspx.
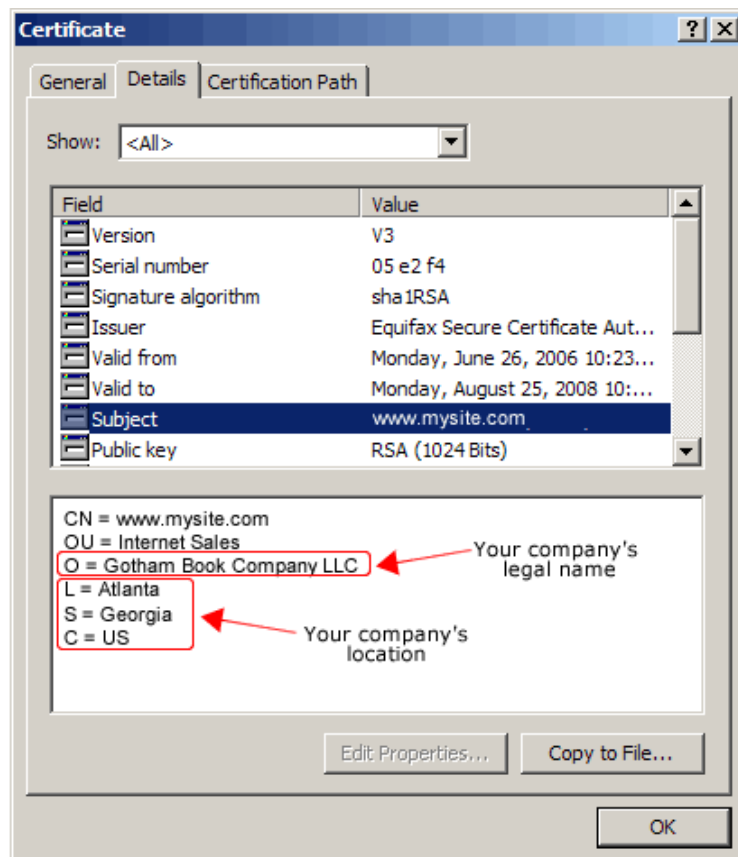
3. Copy the thumbprint of the certificate. You use the thumbprint to bind the certificate to the port used by the primary NMS services in the next step.

   For information on retrieving the thumbprint, see https://msdn.microsoft.com/en-us/library/ms734695.aspx.
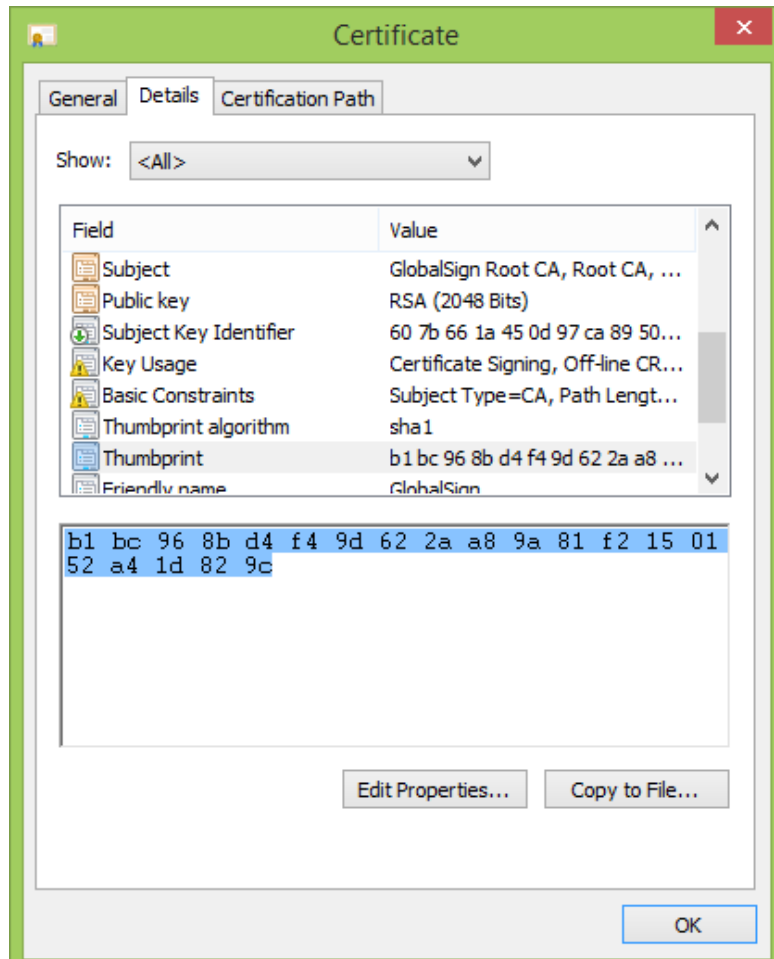
4. Bind the SSL certificate under IIS to port 443.

   a. In the IIS Manager, from the left panel, click **Default Web Site**.

   b. From the right panel, click **Bindings...**

      The Site Bindings dialog box opens.

   c. Click **Add**.

      The Add Site Binding dialog box opens.

   d. From the **Type** drop-down list, select **https**.

   e. From the **SSL certificate** drop-down list, select the certificate that you installed.

   f. Click **OK**.

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

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

Testing and troubleshooting your SSL configuration

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

Use the browser

1. Can you access and log into the NMC console?

   a. Connect to `https://<SERVER_NAME>/NMCHTML/`.

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

   b. Log in to the NMC console. If successful, the console is able to communicate with the server.

2. Can you access the NMC console status interface?

   a. Connect to `https://<SERVER_NAME>/NMS/Platform/ConfigurationSvc/v1/Status`.

   An XML response should appear in the browser.

3. Can you make RESTful web service calls?

   Attempt to create an NMS session using the browser.

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

   A prompt for a login and password appears.

   b. Use any valid NMC console login and password.

   c. If some XML is returned, the NMC console is configured properly and working with SSL.

4. Can you access the NMS API Help pages?

   a. Connect to `https://<SERVER-NAME>/NMS/Platform/UserManagementSvc/v1/help`

   b. Enter any credentials if prompted.

   c. An HTML page with help for one of the NMS API sets should appear. If you see this help, the NMS is configured and working properly.

Check the Bindings

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

`netsh http show sslcert`

Verify that port 443 is bound to the certificate.

Editing the configuration file

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

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

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

2. In any text editor, open `NMS.LocalAuthenticator.Service.exe.config`.

3. Locate the following line and verify that the value is set to the token that you entered during Local Authenticator installation:

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

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

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

5. Save your changes.

Starting the Local Authenticator service

1. Open the Services dialog box.

   a. Click the Windows Start menu.

   b. In the Search field, enter `services.msc`, and then press **Enter**.

   c. Specify your administrator username and password when prompted.

2. Locate the **NMS Local Authenticator Service**.

3. Right-click the service, and then select **Start**.