NexTalk

NexTalk SimpliciTTY
The Most Trusted TTY Call Mangement
Software Solution for Call Centers and Offices

SimpliciTTY® Call Center

SAML Authentication Setup

448 E Winchester Street, Suite 100
Murray, UT 84107
Office: 801-274-6001
Fax: 801-274-6002
www.nextalk.com

SAML Authentication

Security Assertion Markup Language (SAML) is an XML based framework for authentication. It allows the NexTalk server to provide an enhanced authentication method to organizations that support this method. The instructions below outline the steps required to setup and configure the NexTalk Service Provider (SP) to communication with your organization's Identity Provider (IdP).

Prerequisites

Prerequisites:

- Certificates:
  - Self-signed or valid certificate
  - We will need 2 sets of certs. 1 for the Web Server (SP) and the other is the certificate from the IdP.
  - If a valid cert is used, we will need the cert and key files to be used on Apache.
  - We can use a self-signed certificate, but the client will see a warning on the login screen if the self-signed cert is not trusted. The cert can be imported into the trusted certificate store but will need to be pushed out to all agents' workstations.
- Your Consumer Assertion Service URL.
- Using a text editor like Notepad++ is highly recommended. This can be downloaded online or found in the "Patches" folder in the NexTalk Install directory.
- You may run the NexTalk Authentication services on your local machine or on a separate machine. The link below are the latest installers needed to setup either SAML authentication or NexTalk authentication services.
  www.nextalk.com/download/Nauth/Authentication_Services_8.5.6.0.zip

Unpackaging/Install

Once the package is downloaded. Install the below .msi files. There is no need to change any of the installation configurations during the setup. If you are using SAML Authentication, you **do not** need to install Nextalk.Portal.Setup.msi.

Nextalk.Api.Setup.msi
NexTalk.IdSvr.Setup.msi
NexTalk.Portal.Setup.msi (***only if using NexTalk OAuth***)

Apache Configuration

1. **Extract Apache24.zip from the NexTalk Install folder to C:\Apache24**
2. **Place SSL certs files in C:\apache\conf folder. (bundle.crt, .crt, .pfx)**

3. Editing the hppd.conf file. This file is located in C:\Apache24\conf

Httpd.conf File:

Line 222 - ServerAdmin <Email Address>
Line 231 - ServerName <Server Name>

4. Edit C:\Apache24\conf\extra\httpd-vhosts.conf.

httpd-vhosts.conf File:

Line 27 - <VirtualHost *:8080>
Line 28 - ServerName <servername>
Line 29 - ServerAlias *.<domain.com>

Line 31 - SSLEngine On
Line 32 - SSLCertificateFile "${SRVROOT}/conf/<certificate>.crt"
Line 33 - SSLCertificateKeyFile "${SRVROOT}/conf/<privatekey>.key"

Line 60 - <VirtualHost *:8082>
Line 61 - ServerName <FQDN>
Line 62 - ServerAlias *.<domain.com>

Line 64 - SSLEngine On
Line 65 - SSLCertificateFile "${SRVROOT}/conf/<certificate>.crt"
Line 66 - SSLCertificateKeyFile "${SRVROOT}/conf/<privatekey>.key"

5. Edit C:\Apache24\conf\extra\httpd-ssl.conf

httpd-ssl.conf File:

Line 123 - #General setup for the virtual host
Line 124 - DocumentRoot “${SRVROOT}/htdocs
Line 125 - ServerName www.example.com:443
Line 126 - ServerAdmin admin@example.com

Line 144 - SSLCertificateFile "${SRVROOT}/conf/<certificate>.crt"

Line 154- SSLCertificateKeyFile "${SRVROOT}/conf/<privatekey>.key"

If Needed
Line 165 - #SSLCertificateChainFile "${SRVROOT}/conf/server-ca-bundle.crt"

3. **From the command prompt browse to c:\Apache24\Bin**
4. **Type: httpd -k install**
   - **If you get a VCRUNTIME140.dll error, you will need to install the Microsoft Visual C++ 2015 redistributable, vcredist_x64_2015.exe, from the "Patches" folder.**
5. **Type: httpd -k start**
   Leave this window open.

Create Localhost Certificates

Create self-signed localhost certificate

1. Copy the ***openssl.cnf*** file from *C:\Apache24\bin* to *C:\Program Files\Common Files\SSL*
   If the SSL folder does not exist, you will need to create it.

2. In the command prompt window copy the command below and hit enter.

   openssl req -x509 -newkey rsa:4096 -subj "/CN=localhost" -keyout localhostkey.pem -out localhostcert.pem -days 7300

   Enter PEM Pass Phrase: <create a pass phrase>

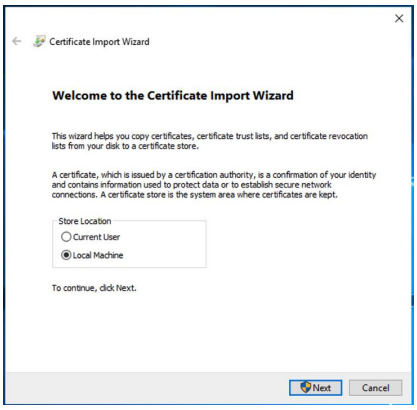
3. In the command prompt copy the command below.

   openssl pkcs12 -name "NexTalk localhost cert" -inkey localhostkey.pem -in localhostcert.pem -export -out localhostcert.pfx

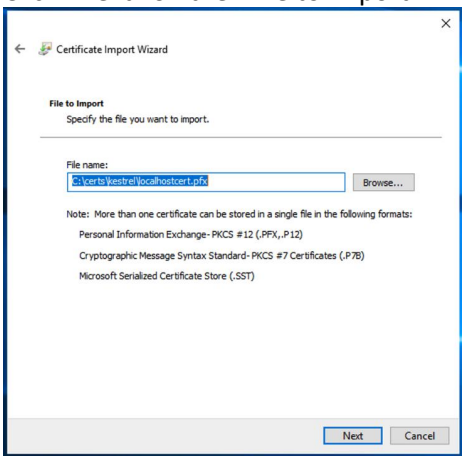
   Enter Pass Passphrase from step 2.
   Enter Export Passphrase: You can use the same Pass Phrase if you want.

   2. Create c:\certs\kestrel and copy localhostcert.pfx into the folder

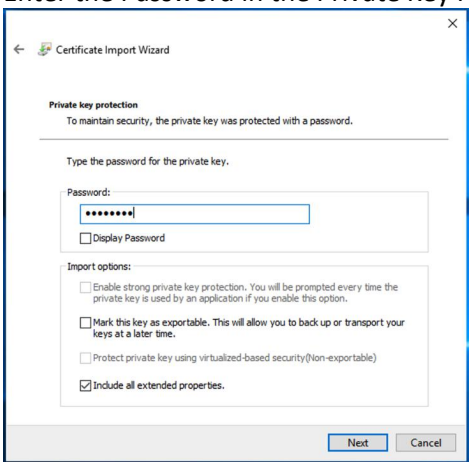
   3. Double click the localhostcert.pfx file to import the cert. Select Local Machine and click "Next".



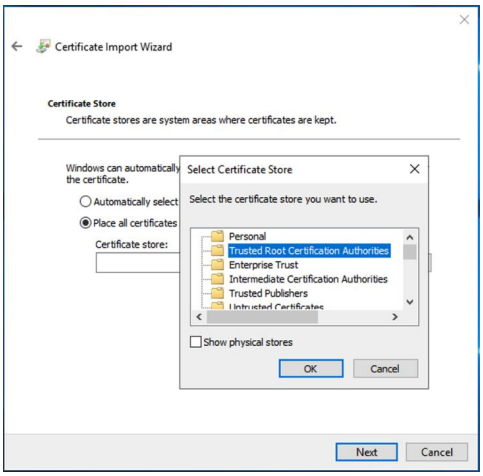
4. Click “Next” on the “File to Import” window.



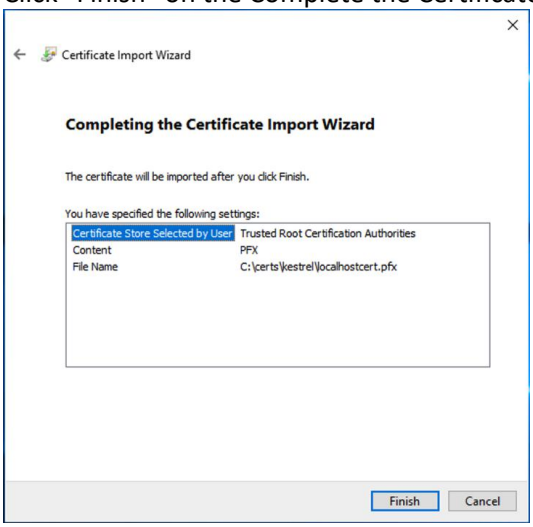
5. Enter the Password in the Private Key Protection window. Then click “Next”

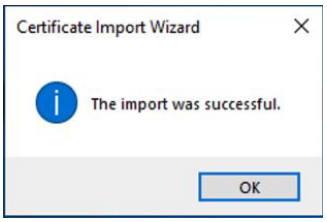


6. In the Certificate Store window, select “Place all certificates in the following store” box then hit “Browse”. In the Select Certificate Store pop up, select Trusted Root Certification Authorities folder and click “OK”. Then click “Next”.



7. Click “Finish” on the Complete the Certificate Import Wizard” window.





Configuring the NexTalk Authentication Configuration Files

1. Browse to C:\Program Files\NexTalk\NexTalk.Api.

2. In a new File Explorer window copy the nlog.production.json file from the Patches\NexTalk APIsrvr folder to the C:\Program Files\NexTalk\NexTalk.Api folder.

3. Open the appsettings.production.json file.

   a. Update “Kestrel” section

```
"Kestrel": {
  "EndPoints": {
    "HttpsInlineCertFile": {
      "Url": "https://localhost:5001",
```

```
      "Certificate": {
        "Path": "C:\\certs\\kestrel\\localhostcert.pfx",
        "Password": "<export passphrase>"
```

a. Update the "Certificates" section

```
"Certificates": {
  "SslCredential": "C:\\certs\\kestrel\\localhostcert.pfx",
  "SslCredentialPassword": "<export passphrase>"
```

b. Update the 'Database" section using the following format:

```
"Database": {
  "ConnectString": "SERVER=<SERVER
NAME>;DATABASE=<DBNAME>;UID=<USERNAME>;PWD=<password>;TRUSTED_CONNECTION=No;
Integrated Security=False;"
 }
```

4. Configure appsettings.production.json file located in C:\Program Files\NexTalk\NexTalk.IdSvr folder:

a. Update 'Kestrel' section

```
"Kestrel": {
  "EndPoints": {
    "HttpsInlineCertFile": {
      "Url": "https://localhost:5000",
      "Certificate": {
        "Path": "C:\\certs\\kestrel\\localhostcert.pfx",
        "Password": "<export passphrase>"
      }
    }
  }
 }
```

c. Update the 'Certificates' section

```
"Certificates": {
  "SslCredential": "C:\\certs\\kestrel\\localhostcert.pfx",
  "SslCredentialPassword": "<export passphrase>"
 }
```

d. Update the 'Database" section using the following format:

```
    "Database": {
      "ConnectString": "SERVER=<SERVER
    NAME>;DATABASE=<DBNAME>;UID=<USERNAME>;PWD=<password>;TRUSTED_CONNECTION
    =No;Integrated Security=False;"
```

e. Update 'Endpoints' section

```
    "Endpoints": {
      "PublicOrigin": "https://IP_ADDRESS:8080",
      "RedirectPublicOrigin": "https://IP_ADDRESS:8082",
```

f. Update NexTalkAccess and SimpliciTTY "DomainName" settings to match what was created for your system:

```
"NexTalkAccess": {
  "CreateOrModifyName": "NtsWeb",
  "DomainName": "DOMAIN",
  "DomainId": 1,
  "ForwardAccountEmail": 1,
  "ForwardPdaEmail": 0,
  "ForwardEmail3": 0,
  "ForwardEmail4": 0,
  "TakeMsgGreeting": null,
  "AnswerGreeting": null,
  "MaxRings": 6,
  "AllowMultiLogins": 0,
  "StartInSystemTray": 1,
  "Groups": {
    "NexTalk Access": "everybody, video",
    "NexTalk Access Pro": "everybody, video, captioned_call"
  }
 },
 "SimpliciTTY": {
  "CreateOrModifyName": "NtsWeb",
     "DomainName": "DOMAIN",
  "DomainId": 1,
  "ForwardAccountEmail": 1,
  "ForwardPdaEmail": 0,
  "ForwardEmail3": 0,
  "ForwardEmail4": 0,
  "TakeMsgGreeting": null,
  "AnswerGreeting": null,
  "MaxRings": 6,
  "AllowMultiLogins": 0,
  "StartInSystemTray": 0,
  "Groups": {
    "SimpliciTTY": "agents"
  }
```

g. Update the GroupMapping section. This section is used in conjunction with the "Group" assertion. We have the ability to automatically assign users to certain groups within NexTalk based on the Group assertion(s) that are sent to our system. This is useful if your organization has users in different groups and require specific role assignments for the users. If your system only has agents, you may skip this section.
Enter your NexTalk domain in the "DOMAIN_NAME" field. Enter the values for "RemoteGroupName" and the "LocalGroupName". The RemoteGroupName is the name of the group your idP would send to us. The "LocalGroupName" is the NexTalk group you want that users to be placed in. The "DefaultGroupPriority" is the priority that you want the groups to be assigned.

```
"GroupMapping": [
 {
  "DOMAIN_NAME": {
   "DefaultGroup": "agents",
   "Groups": [
    {
     "RemoteGroupName": "GROUP_NAME",
     "LocalGroupName": "agents",
     "DefaultGroupPriority": 1
    },
    {
     "RemoteGroupName": "GROUP_NAME",
     "LocalGroupName": "agents",
     "DefaultGroupPriority": 2
    },
    {
     "RemoteGroupName": "GROUP_NAME",
     "LocalGroupName": "agents",
     "DefaultGroupPriority": 3
    },
    {
     "RemoteGroupName": "GROUP_NAME",
     "LocalGroupName": "agents",
     "DefaultGroupPriority": 4
    },
    {
     "RemoteGroupName": "GROUP_NAME",
     "LocalGroupName": "agents",
     "DefaultGroupPriority": 5
```

h. Update the PartnerIdentityProviderConfigurations:

```
    "SingleSignOnServiceUrl": "https://SAML_URL",
    "SingleLogoutServiceUrl": "https://SAML_URL",
    "PartnerCertificates": [ { "FileName": "certificates/idp.cer" } ]
"PartnerName": "SAML_OUTBOUND_FEDERATION_URL"
```

5. Create the System Environment Variable

Variable Name: ASPNETCORE_ENVIRONMENT

Variable Value: Production

NexTalk Assertions/Claims and Metadata Generation

Below are the claims that can support and will need to be setup on the IdP:

FirstName	HomeFaxPhone	PostOfficeBox
LastName	HomeOtherPhone	City
DisplayName		
DomainName	HomeVideoPhone	County
UserCode	AccountEmail	StateProvince
Groups	ForwardAccountEmail	CountryRegion
OneNumber	OfficeEmail	PostalCode
OfficeVoicePhone	ForwardOfficeEmail	AddressType
OfficeTtyPhone	PdaEmail	EmployeeType
OfficeMobilePhone	ForwardPdaEmail	Manager
OfficeFaxPhone	Email3	PreferredLanguage
OfficePagerPhone	ForwardEmail3	DepartmentNumber
OfficeVideoPhone	Email4	RoomNumber
HomeVoicePhone	ForwardEmail4	BusinessCategory
HomeTtyPhone	OfficeName	Location
HomeMobilePhone	StreetAddress	UserName

**The highlighted claims are required.*

Generating SP Metadata:

We will need the metadata from the IdP in order to generate the SP metadata. Once you receive the file;

a. Copy the SAML Utilities folder from the NexTalkAuth folder to C:\Program Files\NexTalk.
b. Open a command promt window in C:\Program Files\NexTalk\SAML Utilities and run "CreateMetadata.exe" to generate the xml file.
c. Send the file to the SAML team to import into their system.

For Technical Assistance:
Phone: 801-274-6001
Email: support@nextalk.com