

Browser Logs

INVOX Medical SDK incorporates a logging system for the Browser side.

All the recorded log is sent to the Dictation Service, which is in charge of creating a file with all the information collected.

File Location

The log file is located on the computer where the Dictation Service is installed. In the following path:

`C:\ProgramData\Vocali\EasyDict\INVOXFront.log`

How it works

It is totally independent of the session. The information is stored in Local Storage in an item called `INVOX_LOG-TEMP`. When a user logs in, the temporary information is sent to the Server and removed from Local Storage because it can already identify who the log belongs to. The new Log named `INVOX_LOG-<USER_LOGIN>` belongs to the session user.

Logging Possibilities

You can choose to use Local Storage or send directly to the Dictation Server. At the same time you can show log messages in the Browser Console.

To modify the logging target, check the `ChangeLogTarget` function from the API.

You can choose the target that best suits your needs. In any case, the Server is in charge of collecting the records and creating its corresponding log file.

Local Storage

INVOX Logger uses a maximum of **1MB** of memory in Local Storage.

In this mode, the Logger records all the logs in the Browser Local Storage until reaching the maximum size set (1MB) or until it detects that there is no more space in the Local Storage.

INVOX Logger is in charge of sending the logs to the Server. This can happen:

- When the user starts the session (Login).
- When the user ends the session (Logout).
- When the maximum size established in the LocalStorage is reached.

Only Server

This logger target takes precedence over the Local Storage target.

In this mode, the Logger sends each log to the Server directly, without storing anything locally.

Browser Console

This target can be used at the same time with another one.

In this mode, the Logger only displays the information in the Browser Console.

Installation of certificates in Remote Dictation Service environments

In order to be able to use the audio sending functionality, the dictation server must have a valid certificate for the client.

When the dictation server is not in the VÓCALI cloud network, it does not have a certificate validated by a certification authority (CA), so it is necessary to include one.

If a certificate validated by a trusted CA is available for the client machines, it must be included in the dictation server.

If a certificate validated by a trusted CA is not available, it is possible to use one generated by a own-CA, in which case it is necessary that the own CA is installed on the client machines in order to be valid.

You need to have *OpenSSL 1.1.0g* or higher installed. *OpenSSL* is installed on most *Linux* distributions, in the case of *Windows* it can be downloaded from any of these websites:

- <https://wiki.openssl.org/index.php/Binaries>
- <https://slproweb.com/products/Win32OpenSSL.html>

Install on the dictation server

To include a certificate in the dictation server, the following steps must be followed:

1. Access the folder `C:\Program Files\Vocali\INVOX Medical Dictation Server` on the machine where the server is located.
2. In that folder edit the **ServerWS.exe.config** file to indicate the information relevant to the certificate to be used.

```
<certificate filePath="name-of-certificate.pfx" password="its-password" isEnabled="true" />
```

or

```
<certificate storeName="Root" thumbprint="available-in-certificates-in-certlm.msc" storeLocation="LocalMachine" />
```

3. After this modification you will need to restart the Invox Medical Dictation Server.

Create certification authority

1. Private key generation.

```
openssl genrsa -des3 -out myCA.key 2048
```

It will ask for a password, which it is advisable to enter so that a possible attacker does not generate certificates without our consent.

2. Generation of the CA root certificate.

```
openssl req -x509 -new -nodes -key myCA.key -sha256 -days 1825 -out myCA.pem
openssl x509 -outform der -in myCA.pem -out myCA.crt
```

It will ask for the password used in the previous step and a series of data. The most interesting are the **Organisation Name** (ON) and the **Common Name** (CN) with which it is easy to identify the generated certificate.

After these two steps you will have three files:

- myCA.key (private key)
- myCA.pem (root certificates for macOS)
- myCA.crt (root certificates for Windows)

Create certificate

To create the certificate for the dictation server, the following steps must be followed:

1. Generation of the private key.

```
openssl genrsa -out server.key 2048
```

2. Certificate solicitation.

```
openssl req -new -key server.key -out server.csr
```

It will ask for the password used in the previous step and a series of data. The most interesting are the **Organisation Name** (ON) and the **Common Name** (CN) with which it is easy to identify the generated certificate.

3. Configuration. A plain text file named *config.ext* must be created with the following content.

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
```

```
[alt_names]
DNS.1 = computer-name
DNS.2 = computer-name
```

Where computer-name is the DNS of the dictation server, **it is not possible to indicate the IP as the computer name.**

4. Creation of the certificate with the above configuration.

```
openssl x509 -req -in server.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial -out server.crt -days 1825 -sha256 -extfile config.ext

openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
```

Install on Windows

In order for browsers to trust the dictation server's certificate, the CA certificate must be installed in the Windows certificate store:

1. Double click on the `myCA.crt` file and select Install certificate.
2. Select Local computer and place the certificate in the Trusted Root Certification Authorities store.

Install in Firefox

1. Open Firefox.
2. Go to Options > Privacy & security.
3. Click the “View certificates...” button.
4. Open the “Authorities” tab.
5. Click on the “Import...” button.
6. Select the `myCA.pem` or `myCA.crt` file.

Install on macOS

1. Open the keychain application.
2. Go to File > Import items...
3. Select the `myCA.pem` file.
4. Search for the certificate by the Common Name.
5. Double click on it.
6. Expand the Trust section.
7. Change the “When using this certificate” combo box to “Always trust”.
8. Close all windows of the Keychain Access application.

Deploying website in IIS

This tutorial will guide you through setting up a new website in Internet Information Services (IIS). These steps are shown for IIS 10 on Windows 10, but the same basic procedures apply to IIS 7 and 8.

Open the IIS Manager

Open *Internet Information Services Manager (IIS)*. You can quickly find it by typing “IIS” in the search field.

Add website

On the root of the site, right click and select the option *Add Website...*

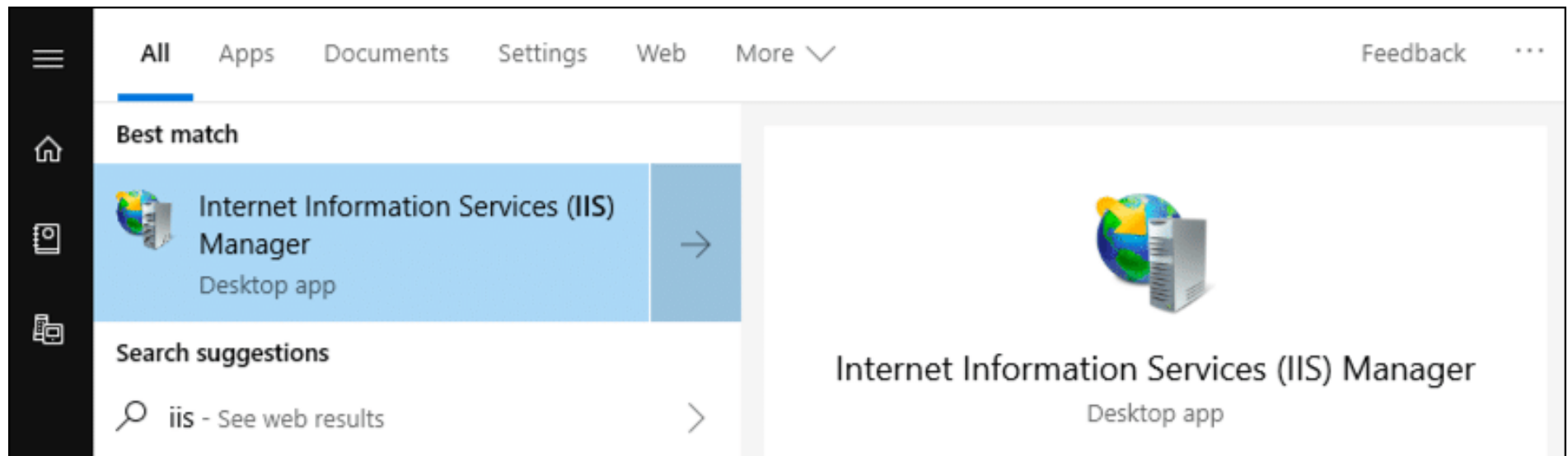


Figure 1: Search

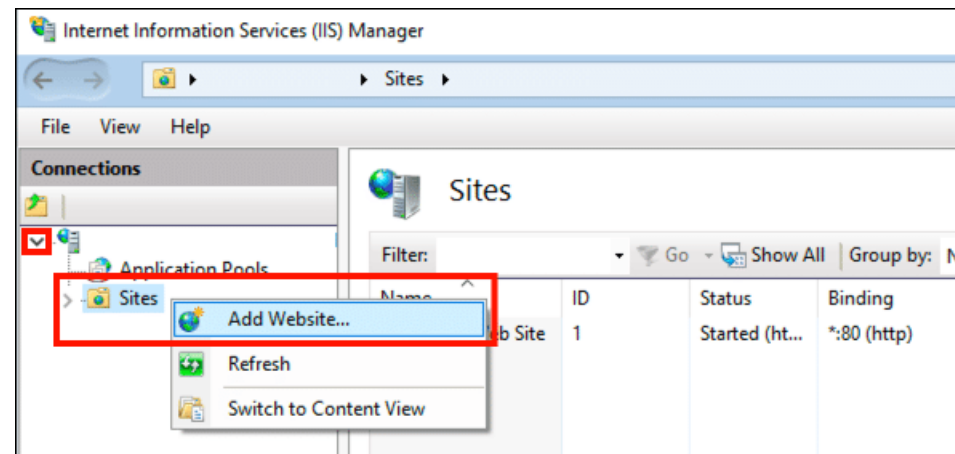


Figure 2: Add website

Create site name

The site creation window will open. First, add an easy-to-remember name for the website in the *Site Name* field.

Add physical path

In the *Content Directory* section, enter the physical path to the directory where you are going to place the content of the SDK examples package. To do this, click on the *...* button and navigate to the directory containing the files of your website.

The .zip package of the content must be extracted in its entirety into a directory, so that we can indicate in the physical path of the website, the root directory.

Set the bindings

In the *Bindings* section, click on the drop-down *Type* and select one of the available options (HTTP or HTTPS). After that, enter the IP address (or leave the default value in case you don't have a specific IP) and do the same with *port* and *hostname*.

Decide whether or not to launch the website

If you want to start the website immediately, make sure *Start Website immediately* is checked. If not, disable it.

Accept changes

Click the accept button to finish creating your new website.

Add Website

Site name: My Website

Application pool: My Website Select...

Content Directory

Physical path: ...

Pass-through authentication

Connect as... Test Settings...

Binding

Type: http IP address: All Unassigned Port: 80

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

OK Cancel

Figure 3: Add Web Site Name

Add Website ? X

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

Figure 4: Add physical path

Add Website

Site name: My Website Application pool: My Website Select...

Content Directory

Physical path: C:\inetpub\test-website ...

Pass-through authentication

Connect as... Test Settings...

Binding

Type:	IP address:	Port:
http	All Unassigned	80

Host name: www.example.com

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

OK Cancel

Figure 5: Set the bindings

Add Website ? X

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

Figure 6: Launch Website

Add Website ? X

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

Figure 7: Accept changes