Want to configure SSL on OpenLM Server v5? Please check out the version 5 guide instead.

The following document describes the setup and configuration of SSL for OpenLM Server and its related components. This document assumes that a certificate with a digital signature from a certificate authority (CA) is already installed on the target machine. Self-signed certificates are supported however there are some particularities regarding their use (see section 4).

Note: We suggest using the latest versions of our Java-based applications (Broker, Applications Manager, Router and Report Scheduler) as they require Java 11 which supports the latest TLS/SSL security protocols. Customers running older versions of these applications which use Java 8 may be limited to older versions of the security protocols.

This documents covers:

1. Setting up SSL for OpenLM

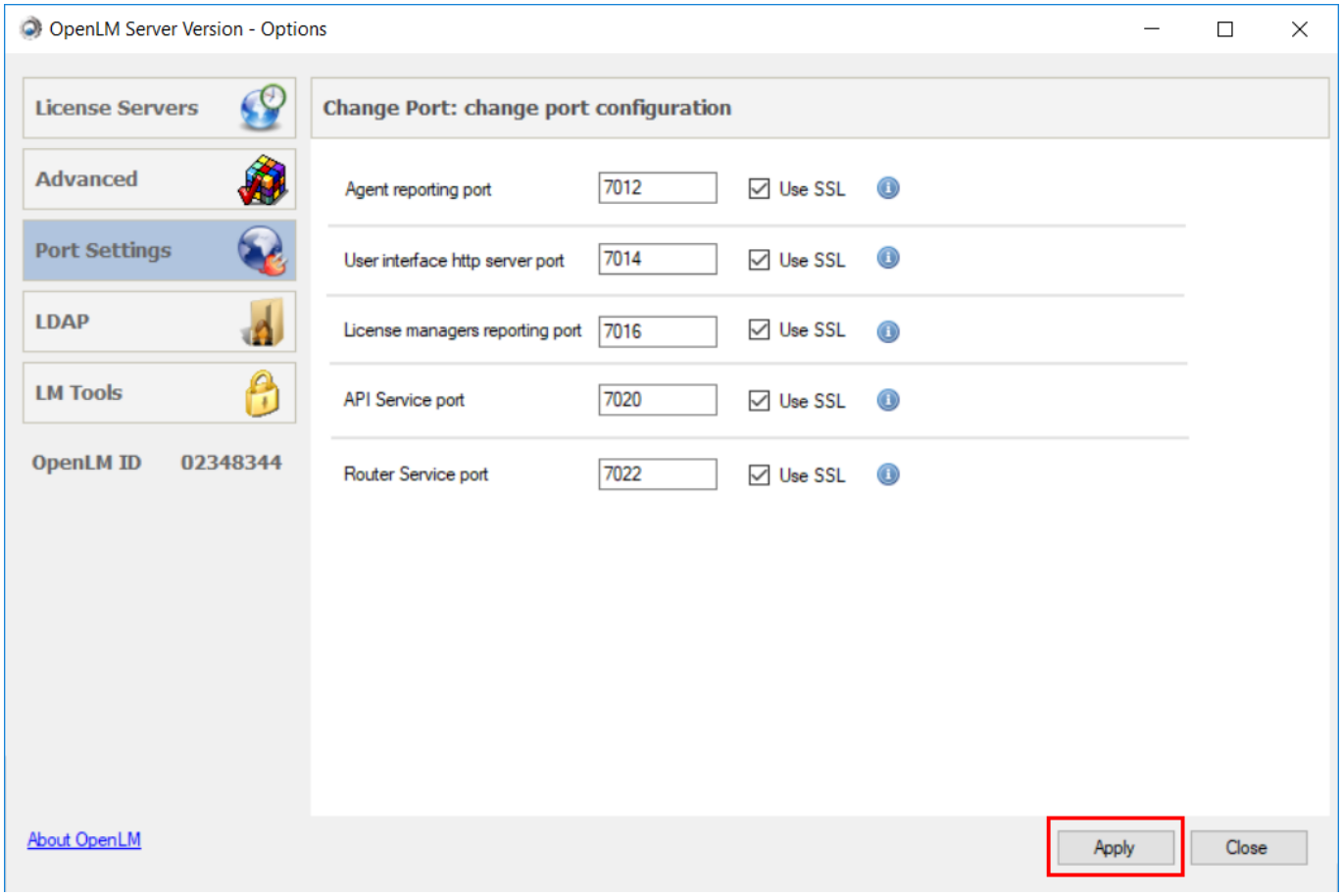
> **NOTE:** If you only want to enable SSL for OpenLM's EasyAdmin interface, you only need to follow steps 6 and 7 with the added port 443 binding

1. Set up Internet Information Services (IIS) with EasyAdmin as described in this document: Configuring OpenLM EasyAdmin with IIS 10 on Windows Server 2016 – KB801

2. Open the OpenLM Server Configuration Tool (*Windows Start → OpenLM → OpenLM Server*)

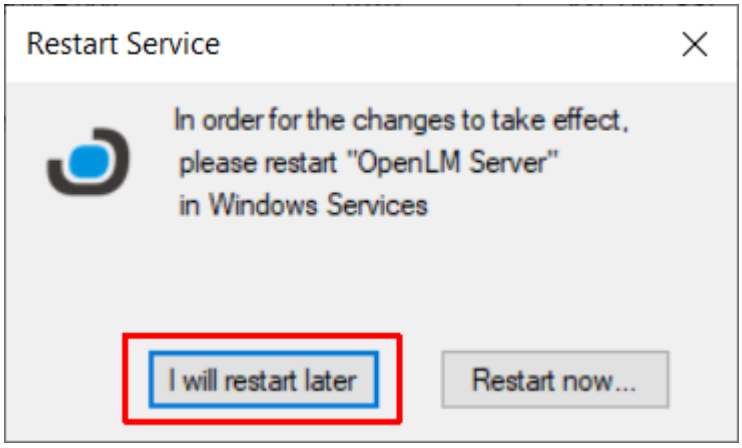
3. Click on the "Port Settings" tab and check each box for each component that you want to enable SSL for. A confirmation dialog will pop-up. Click "Yes" to continue. Consult the table below for a description of what each default port is used for.

Note: If you want to change any of the default ports, note the changes down as they will have to match the IIS bindings which we will configure in step 7.



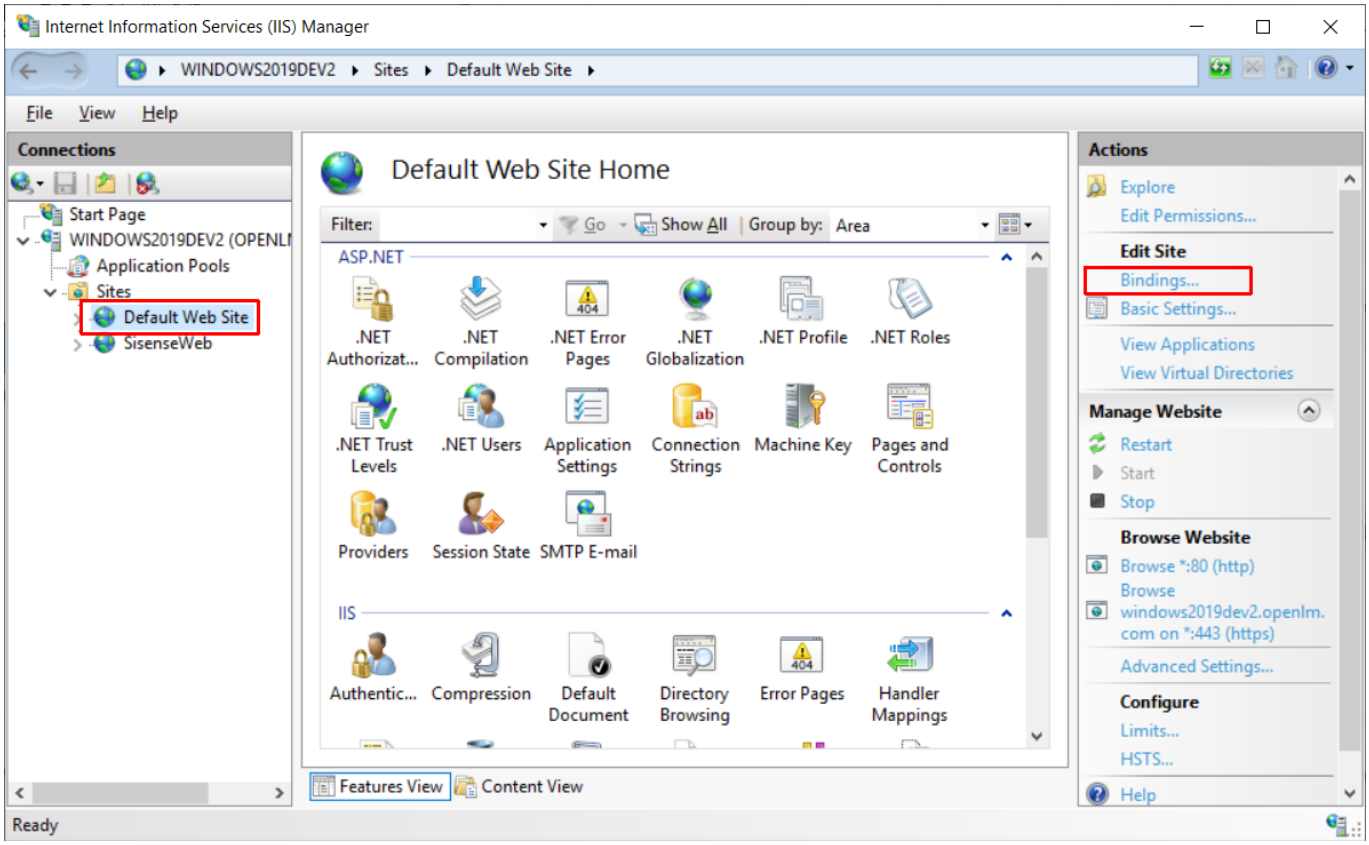
Default Port	Description
7012	The OpenLM Agent reporting port
7014	The primary connection port used by the OpenLM Server Configuration tool as well as OpenLM UI / EasyAdmin to retrieve data
7016	The OpenLM Broker reporting port
7020	OpenLM Admin API Service port, used by OpenLM UI / EasyAdmin (along with 7014) to retrieve and update data
7022	The OpenLM Router reporting port

4. Click on "**Apply**". A dialog will pop-up asking if you want to restart now or later. Choose "**I will restart later**".



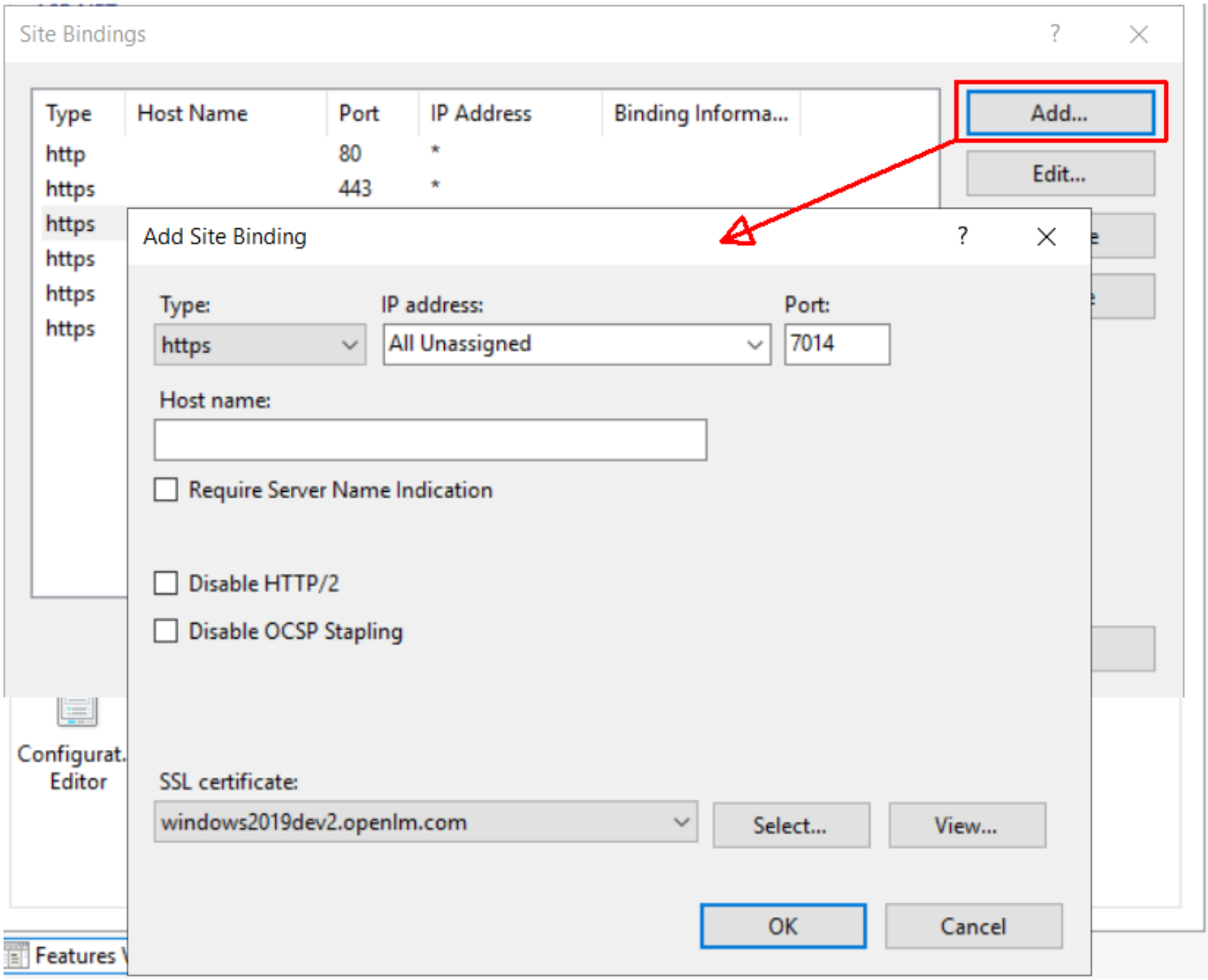
5. Open Windows Services (press Windows + R → type **services.msc** → press Enter) and stop the "OpenLM Server" service.

6. Open Internet Information Services (IIS) Manager. Go to **Default Web Site → Bindings:**



7. Click **"Add"** and individually enter the ports for each of the components you have enabled in step 3 as well as port 443 which is the default https port that will be used to serve

EasyAdmin. Make sure that **https** is selected along with the valid SSL certificate for your domain chosen from the drop-down menu:



8. Open the **params.js** file located in your OpenLM EasyAdmin2 folder in a text editor (typically *C:\Program Files (x86)\OpenLM\OpenLM Server\WebApps\EasyAdmin2\params.js*)

Change the following variables and save the file when finished:

```
var OpenLMServer='https://<full domain name as issued on the SSL certificate>:7014/OpenLMServer'
```

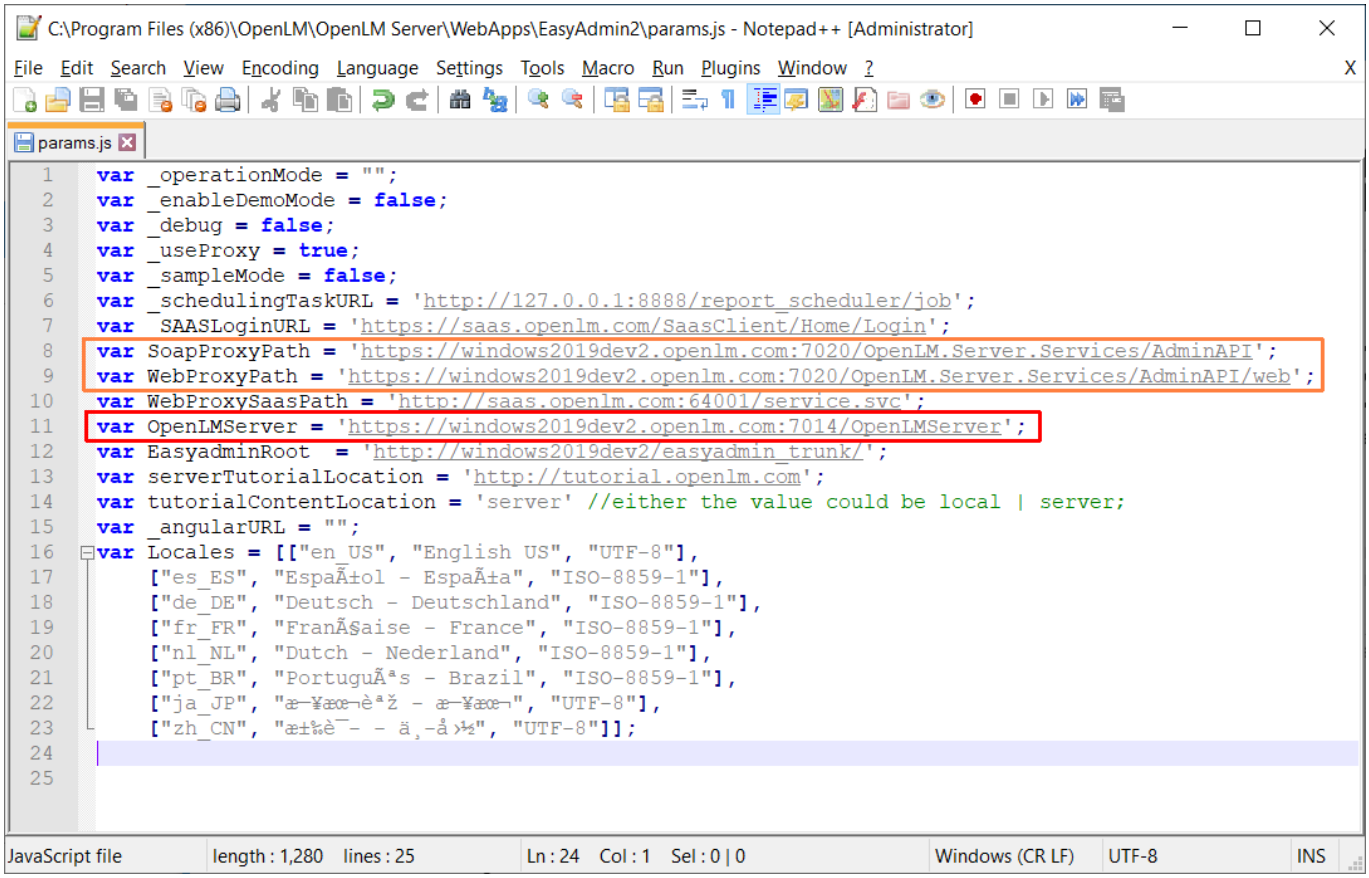
If you have enabled SSL for the "API Service port" in step 3:

```
var SoapProxyPath='https://<full domain name as issued on the SSL certificate>:7020/OpenLM.Server.Services/AdminAPI'

var WebProxyPath='https://<full domain name as issued on the SSL certificate>:7020/OpenLM.Server.Services/AdminAPI/web'
```

Important: make sure that the address is an exact match to the domain name as indicated on your signed certificate (i.e. <hostname>.com, <hostname>.net, etc.)

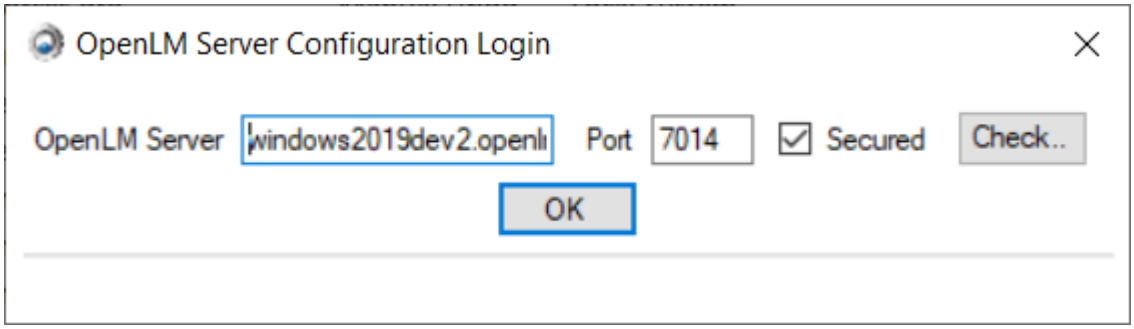
In our example we will be changing the default *http* to *https*, and editing the server hostname to match the domain name of our issued certificate (*.com):

```
var OpenLMServer = 'https://windows2019dev2.openlm.com:7014/OpenLMServer';

var SoapProxyPath = 'https://windows2019dev2.openlm.com:7020/OpenLM.Server.Services/AdminAPI';

var WebProxyPath = 'https://windows2019dev2.openlm.com:7020/OpenLM.Server.Services/AdminAPI/web';
```



9. Open Windows Services (press Windows + R → type **services.msc** → press Enter) and start the "OpenLM Server" service.

10. Open the OpenLM Server Configuration Tool. An error will pop-up saying that a connection cannot be established. In the window that appears, make sure that instead of localhost you **enter the full domain name as indicated on your SSL certificate** along with the User Interface port (by default: 7014) and that the "Secured" box is checked. Click **OK**.

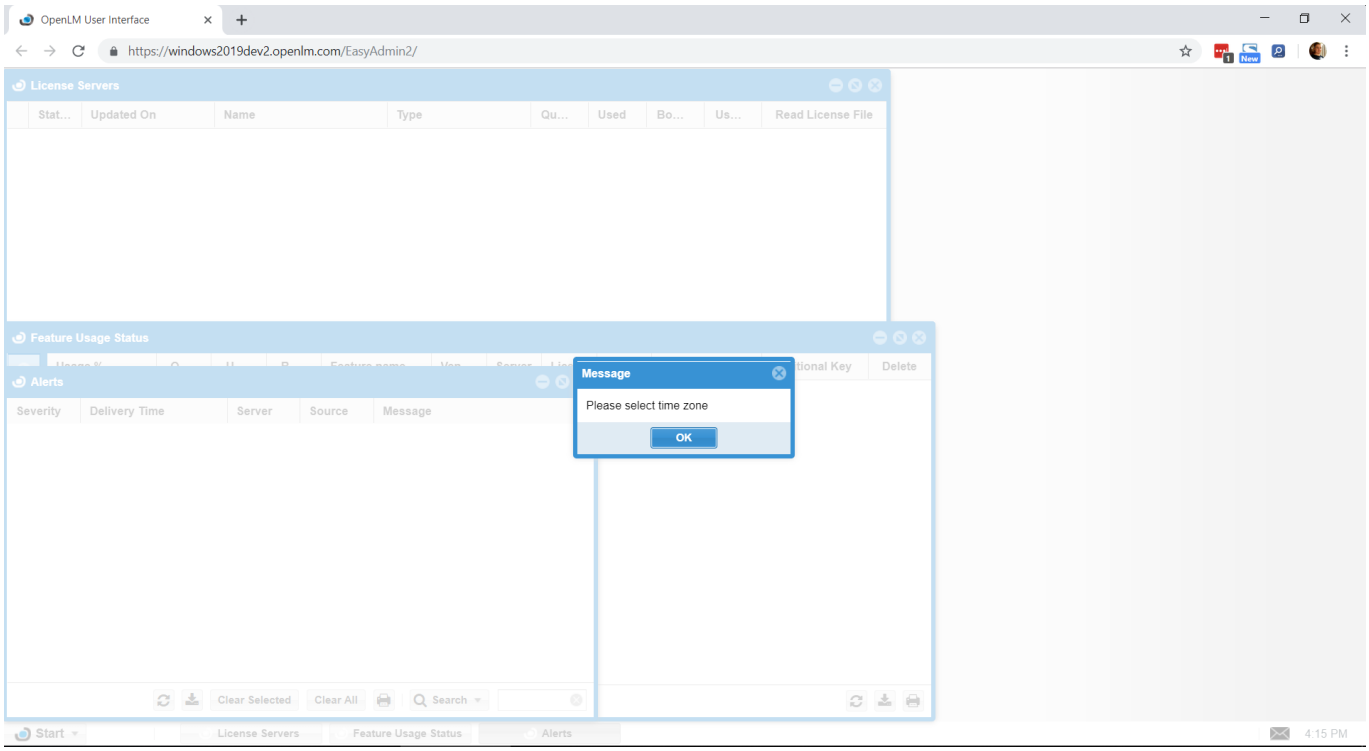


If you have successfully followed the steps above, your OpenLM Server installation should now be communicating to its components using SSL encryption.

2. Checking your EasyAdmin SSL configuration

Open your browser and navigate to the https address of your OpenLM installation (e.g. *https://windows2019dev2.openlm.com/EasyAdmin2/*)

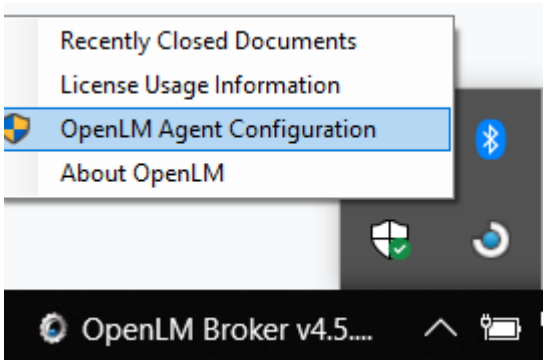
If you've configured everything correctly you should be able to see the default Dashboard screen with the first login configuration window.



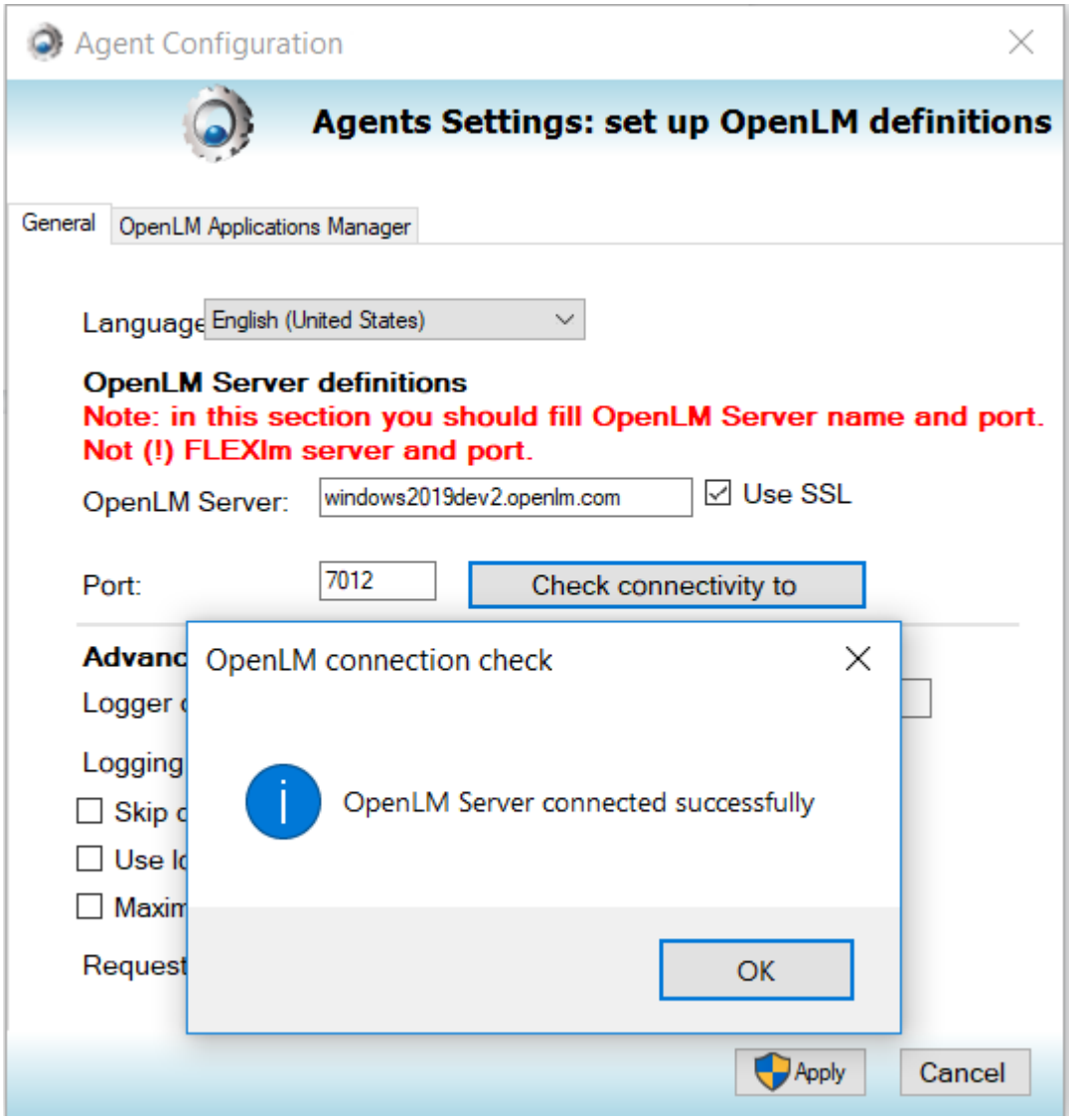
3. Configuring OpenLM components to use SSL

3.1 OpenLM Agent

1. Right click on the Agent tray icon and click on "OpenLM Agent Configuration"



2. In the OpenLM Server field enter the full domain name as issued on the SSL certificate. Check the “Use SSL” box and make sure that the Port field matches the one you have set in the Port Settings tab of the OpenLM Server Configuration Tool.



3. Click “Check connectivity to” to make sure that a connection is established.

4. Click on “Apply” to save the settings and close the Agent configuration window.

3.2 OpenLM Broker

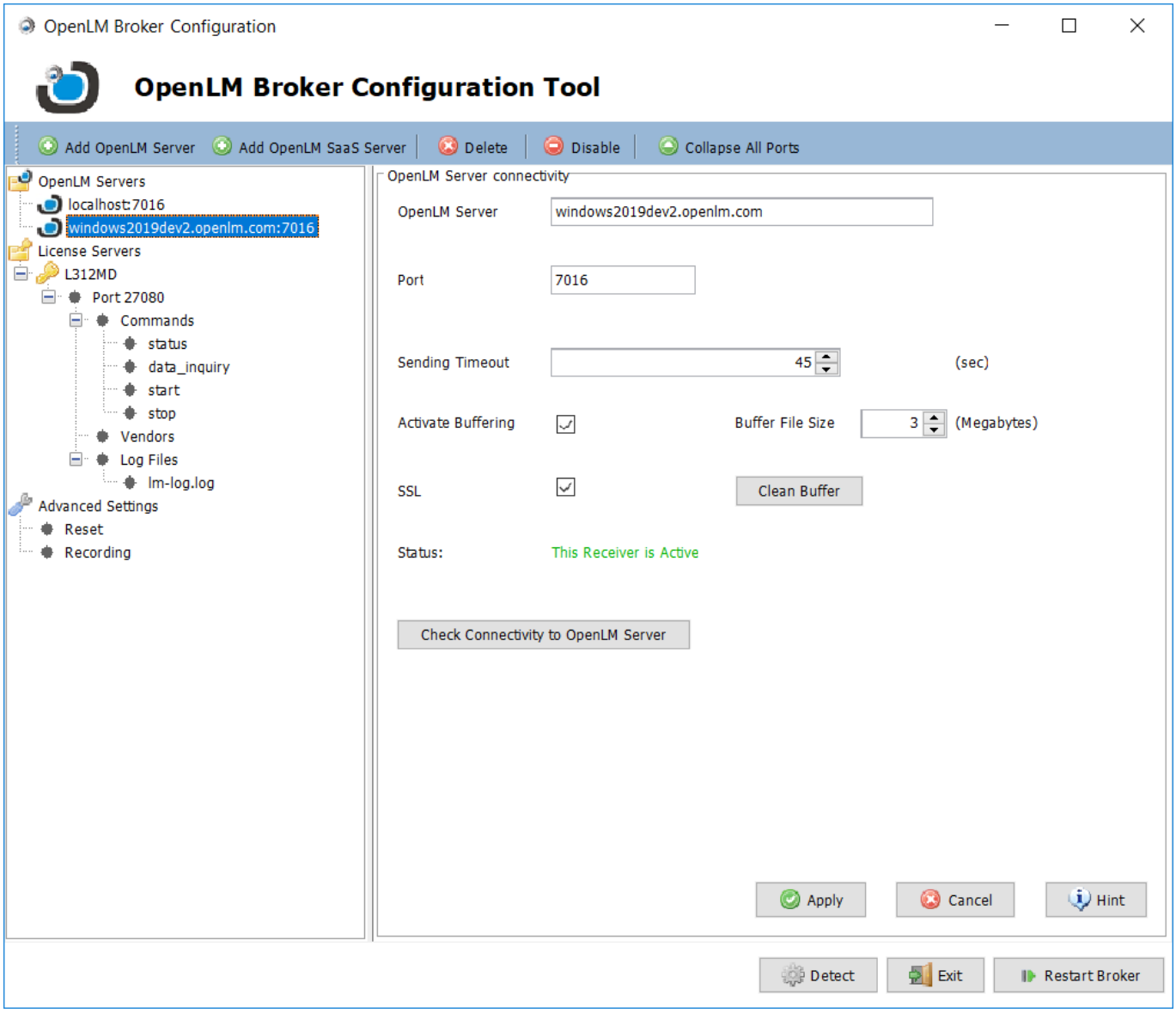
1. Start the OpenLM Broker Configuration Tool (Windows Start → OpenLM → OpenLM Broker Configuration Tool)

2. Select the Server in the right panel for which you have set up a SSL connection.

3. Make sure that the “OpenLM Server” field is the full domain name as issued on the SSL certificate. Check the port number and make sure that the SSL box is checked.

4. Click “Check Connectivity to OpenLM Server”. If you have configured SSL successfully you should see a success dialog.

5. Click “Apply” to save the new settings then click “Restart Broker”.



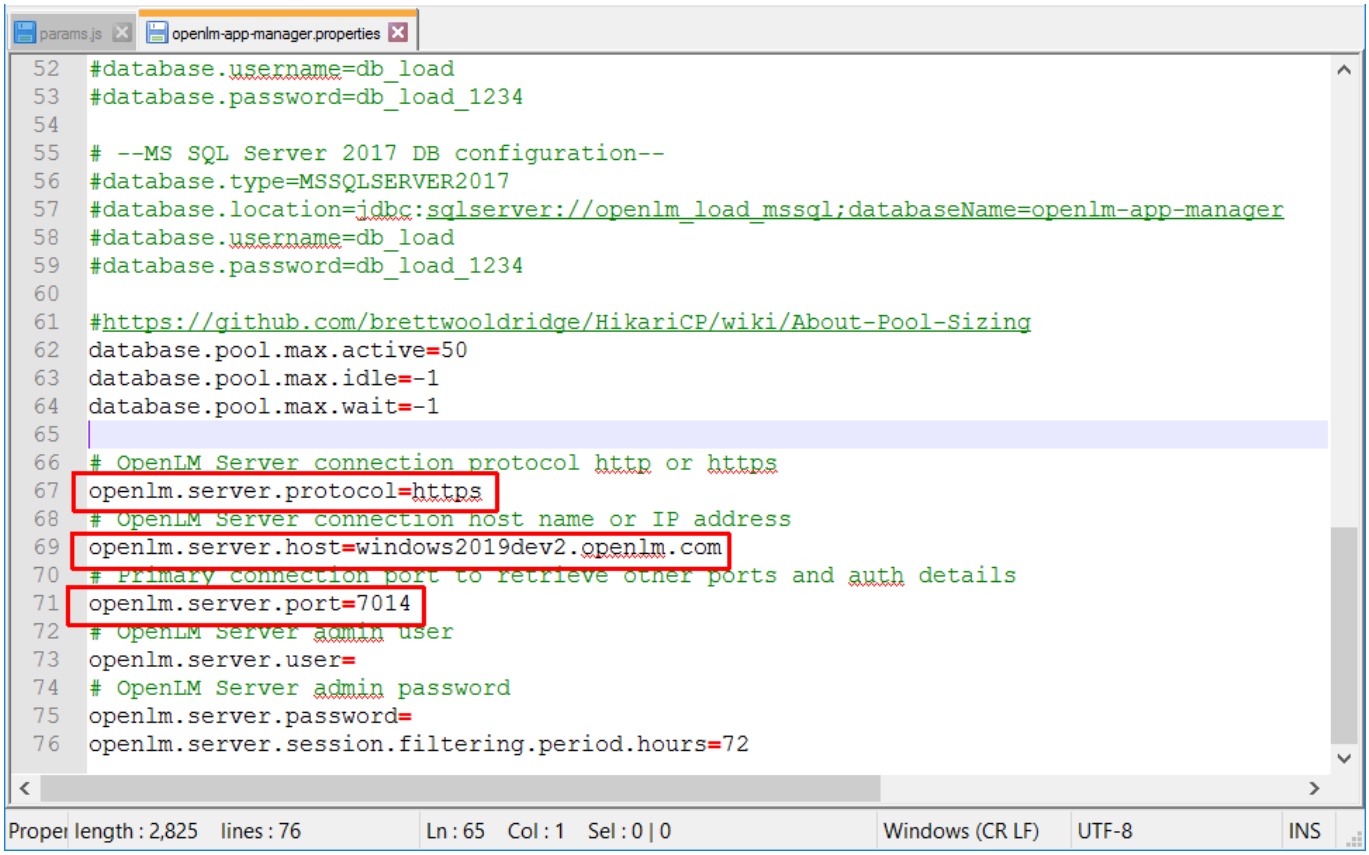
3.3 OpenLM Applications Manager

The following steps describe setting up the OpenLM Applications Manager component only when the OpenLM Server is serving secured connections. To configure the OpenLM Applications Manager to serve SSL connections, please consult this article.

1. Locate the Applications Manager folder and open the **openlm-app-manager.properties** file in a text editor (typically located at C:\Program Files\OpenLM\OpenLM App Manager)

2. Change the following variables:

```
openlm.server.protocol = https

openlm.server.host = <full domain name as reflected on the SSL certificate>

openlm.server.port = <change if you've modified the "User interface http server port" in step 3 of the "Setting Up SSL for OpenLM" section>
```



3. Save changes to file.

4. Open Windows Services and restart the “OpenLM App Manager” service.

3.4 OpenLM Router

For Windows

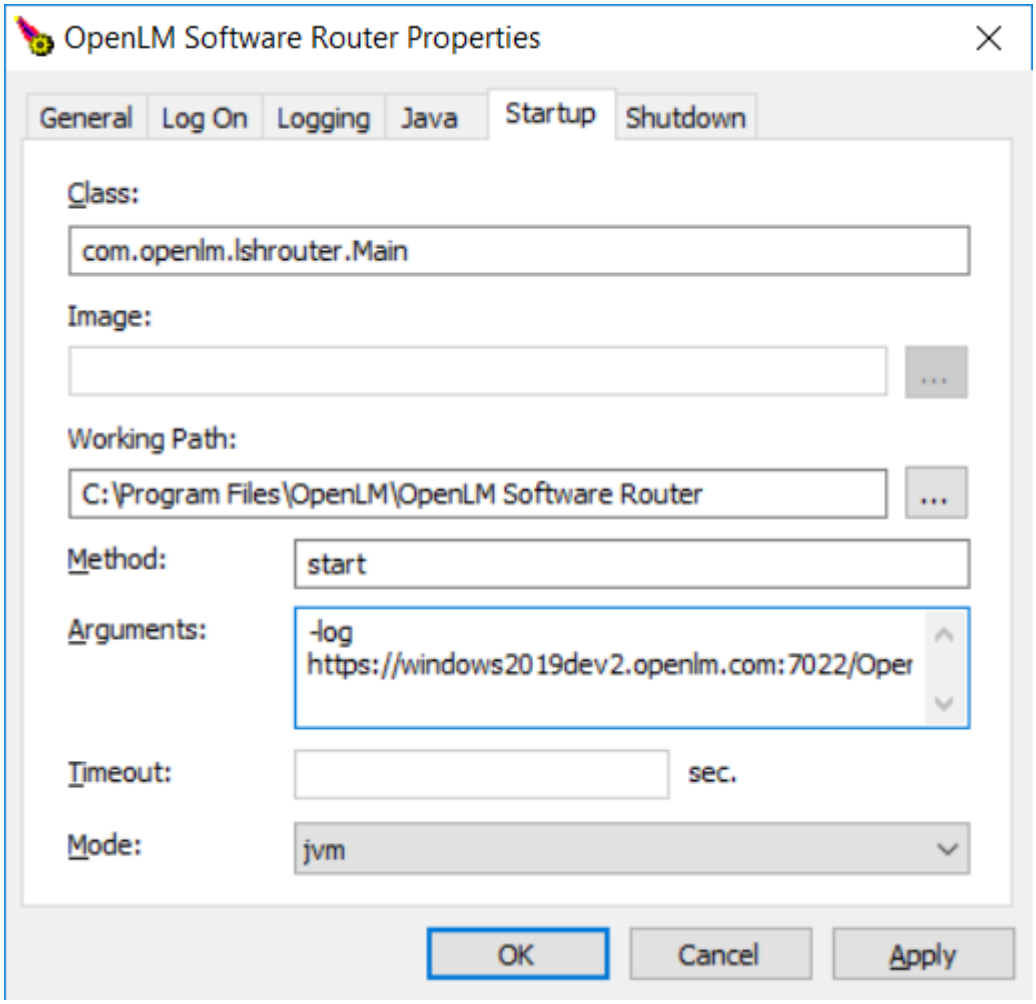
1. Run “**OpenLM Software Router.exe**” located in your OpenLM Software Router\bin folder (typically C:\Program Files\OpenLM\OpenLM Software Router\bin)

2. The Router Properties tool will open. Click on the “Startup” tab.

3. Edit the Arguments field to reflect the address of the OpenLM Server as indicated on the

SSL certificate, e.g:

```
-log
https://windows2019dev2.openlm.com:7022/OpenLM.Server.Services/RouterAPI
```



4. Click “Apply” then “OK” to close the tool.

5. Open Windows Services and restart the “OpenLM Software Router” service.

For Linux/Unix

1. Edit the **router.sh** script located in the folder where you installed OpenLM Router.

2. Change the address after the -log parameter to reflect the address of the OpenLM Server as indicated on the SSL certificate:

```
#!/usr/bin/env bash

java -Dlog4j.configuration=file:log4j.properties -
Djava.net.preferIPv4Stack=true -jar openlm-router-2.0.20.jar -log
https://windows2019dev2.openlm.com:7022/OpenLM.Server.Services/Rout
erAPI
```

3. Restart the OpenLM Router service.

3.5 OpenLM Report Scheduler

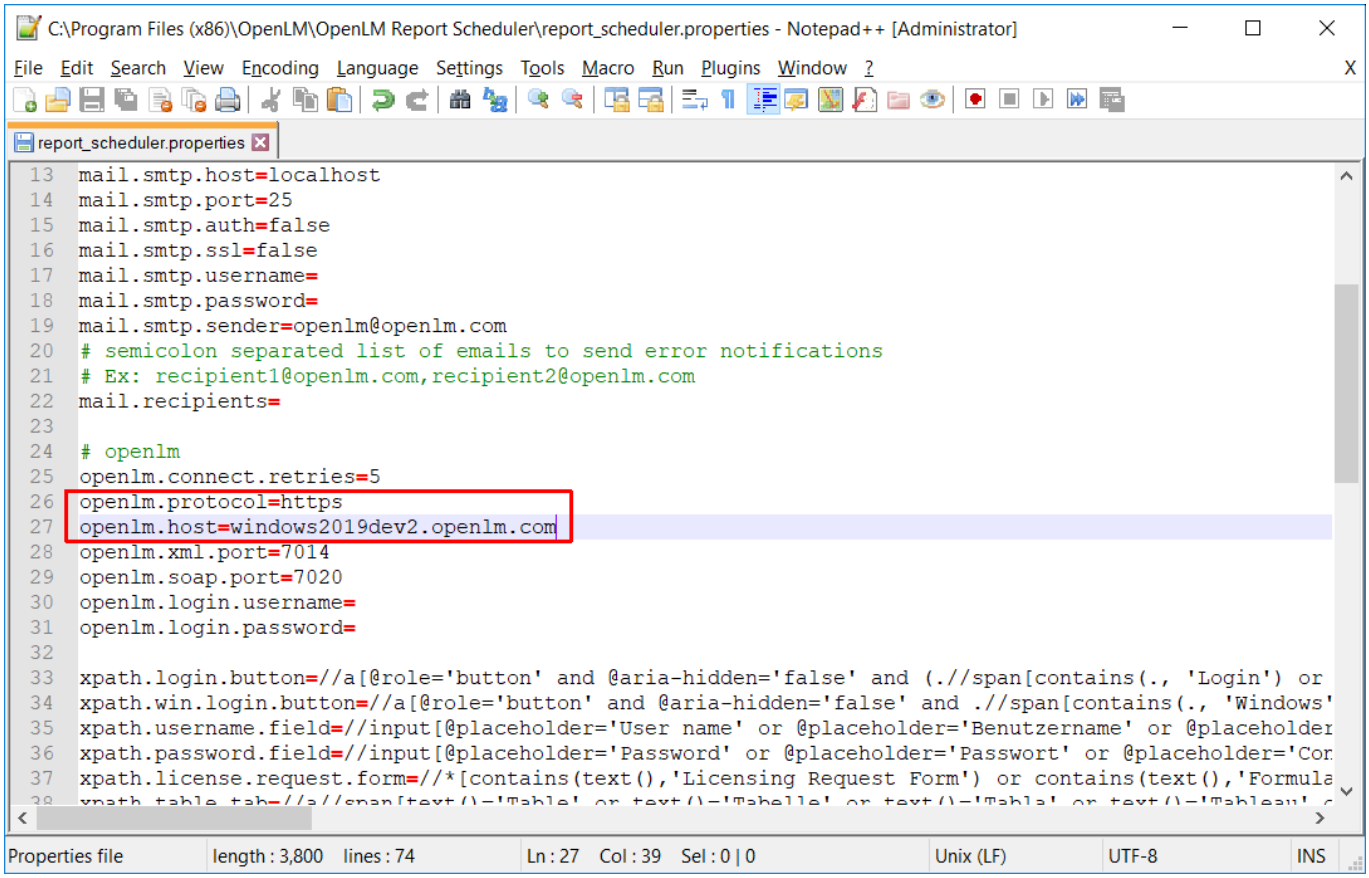
1. Locate the OpenLM Report Scheduler folder and open the **report_scheduler.properties** file in a text editor (typically located at C:\Program Files (x86)\OpenLM\OpenLM Report Scheduler)

2. Change the following variables:

```
openlm.protocol=https

openlm.host=<full domain name as reflected on the SSL certificate>
```

3. Save the changes.

4. Open Windows Services and restart the “OpenLM Report Scheduler” service.



4. Using self-signed certificates with OpenLM

Although it's possible to use self-signed certificates in OpenLM software, we don't advise using them as they can be less secure and require more effort to set up.

Setting up self-signed certificates is outside the scope of this document however here are some general guidelines for doing so:

1. The self-signed certificate must be installed in the "Trusted Root Certification Authorities" folder of the local Computer Account (Microsoft documentation).
2. The self-signed certificate must be installed on the machine where OpenLM Server is running as well as each machine that the Server is interfacing with (for example, OpenLM Agent).
3. On Linux, for the Java-based components (Broker, Applications Manager, Router and Reports Scheduler), the self-signed certificate must be added to the local JDK keystore.

This can be done using the Java-supplied *keytool* utility. On Windows, the latest versions of the Java-based components read the Windows certificate store by default. This includes Broker v4.6.1, Applications Manager v2.2.8, Router 2.0.33, Reports Scheduler 1.7.5. Older versions of these components on Windows must import the certificate into Java KeyStore using the keytool utility.