

OpenLM Server v5のSSL設定 – KB501

- OpenLM Server v5のSSL設定 – KB501

このドキュメントはOpenLM Serverバージョン5と関係するコンポーネント用のSSL設定を説明します。証明書機関（CA）からのデジタル署名付き証明書が目標のマシンに既に存在する事を想定しています。

Contents:

1. OpenLM ServerのSSL設定

オプションA – Windowsストア用証明書付きSSL

オプションB – 特定証明書ファイル付きSSL

2. SSL使用中OpenLM Serverへの接続

OpenLM Broker

OpenLM Agent

OpenLM Applications Manager

OpenLM Router

OpenLM Reports Scheduler

3. EasyAdminユーザー接続用SSLの使用

4. SSL設定のアップグレードServer v4.xからv5

1. OpenLM ServerのSSL設定

1. アドミンアカウントでテキストエディターでC:\Program Files (x86)\OpenLM\OpenLM Server\bin\appsettings.jsonを開く。

ファイルの最後で、次を検索して編集する:

- “Url”変数 – httpsを指定
- “Kestrel”ノード – 証明書ストアか証明書への特定パスの使用かによって下記a)か b)を参照。
- (オプション) 必要なら、エイリアスとして行動するようにポートを追加できます。(7016と7012参照)。 “ ”間の名前



(例 ; “Broker”) は単純に説明でどの値でも構いません。

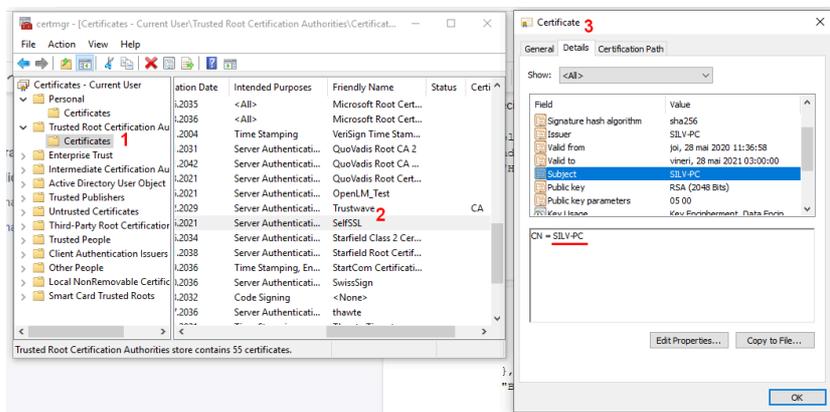
オプション A – Windowsストアの証明書付きSSL

証明書ノードを追加する:

```
"Kestrel": {
  "Endpoints": {
    "Http": {
      "Url": "https://*:5015"
    },
    "Broker": {
      "Url": "https://*:7016"
    },
    "Agent": {
      "Url": "https://*:7012"
    }
  },
  "Certificates": {
    "Default": {
      "Subject": "SILV-PC",
      "Store": "Root",
      "Location": "LocalMachine",
      "AllowInvalid": "true"
    }
  }
}
```

- **Subject (対象)** – 誰に証明書が発行されたか。Windows Run → certmgr.msc → 証明書がある証明書ストアを選択 → ダブルクリック → 詳細タブをクリック → 対象を検索 (下記図参照)
- **Store (ストア)** – 証明書ストア。“Personal” (個別) ストアは“My” (私の) で参照され、“Trusted Root Certification Authorities” (信頼ルート証明機関) は“Root” (ルート) として参照される。他の証明書ストアの名前については、[こちらの記事を参照してください](#)。
- **Location (場所)** – LocalMachineローカルマシンか CurrentUser現行ユーザーのどちらでも構いません。
- **AllowInvalid (無効許可)** – 必要なら無効証明書の使用許可を Trueに設定してください(例 ; 自己署名証明書)





証明書の対象を検索

オプション B – 特定証明書ファイル付きSSL

証明書ノードを追加する:

```
"Kestrel": {
  "Endpoints": {
    "Http": {
      "Url": "https://*:5015"
    },
    "Broker": {
      "Url": "https://*:7016"
    },
    "Agent": {
      "Url": "https://*:7012"
    }
  },
  "Certificates": {
    "Default": {
      "Path": "C:\\Users\\borisi\\Desktop\\"
      "Password": "ZXzx12!@"
    }
  }
}
```

- **Path (パス)** – 証明書ファイルへのパス。スラッシュの代わりに2重バックスラッシュを必ず使用してください。
- **Password (パスワード)** – 証明書のプライベートキーのパスワード。



注意: 必ず `{ }` が適切にとじられているか確認してください。

2. ファイルを保存する。

3. アドミンアカウントでテキストエディターで `C:\Program Files (x86)\OpenLM\OpenLM`

`Server\WebApps\EasyAdmin2\params.js` ファイルを開く。

4. 変数(`SoapProxyPath`, `WebProxyPath`, `WebProxySaasPath`, `OpenLMServer`, `EasyadminRoot`)を編集してURLを`https`にする。ホスト名は必ずSSL証明書に記載されているものと正確に一致するようにする(例 ; ホスト名.com)。

```
6 var _schedulingTaskURL = 'http://127.0.0.1:8888/report_scheduler/job';
7 var _SAASLoginURL = 'https://saas.openlm.com/SaaSClient/Home/Login';
8 var SoapProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';
9 var WebProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';
10 var WebProxySaasPath = 'https://SILV-PC:8084/SaaSService/service.svc';
11 var OpenLMServer = 'https://SILV-PC:5015/api/easyadminapi/postmessage';
12 var EasyadminRoot = 'https://SILV-PC/easyadmin_trunk/';
13 var _angularURL = '';
14 var Locales = [
15   ["en_US", "English US", "UTF-8"],
16   ["es_ES", "Español - España", "ISO-8859-1"],
17   ["de_DE", "Deutsch - Deutschland", "ISO-8859-1"],
18   ["fr_FR", "Française - France", "ISO-8859-1"],
19   ["nl_NL", "Dutch - Nederland", "ISO-8859-1"],
20   ["pt_BR", "Português - Brazil", "ISO-8859-1"],
21   ["ja_JP", "日本語 - 日本", "UTF-8"],
22   ["zh_CN", "汉语 - 中国", "UTF-8"]];
```

5. ファイルを保存する。

6. “OpenLM Server”サービスをリスタートする。

2. SSL使用中OpenLM Serverへの接続

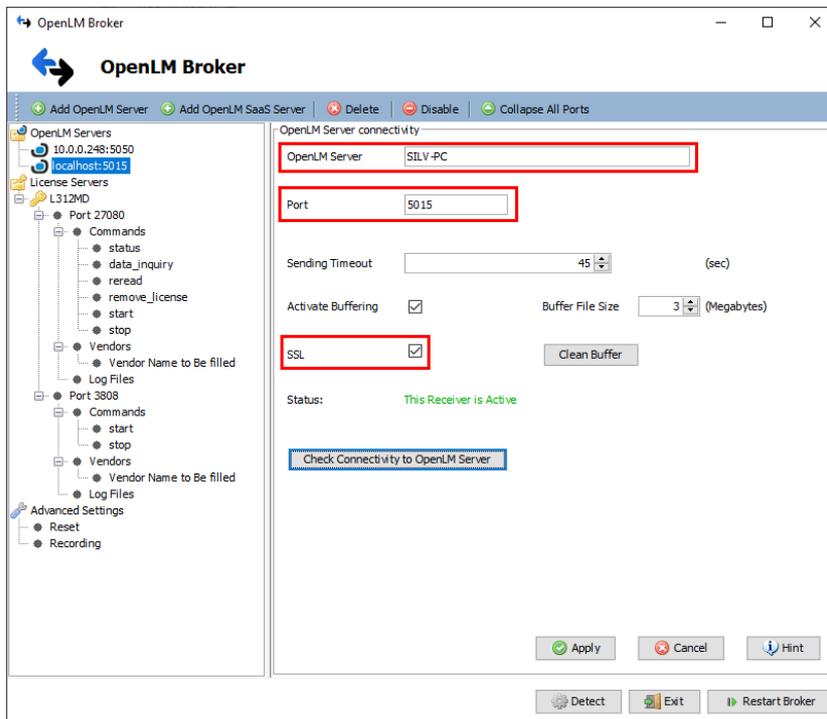
重要: サーバーに使用されており、サーバーにインストールされたマシンの信頼証明書ストアに提供されている自己署名証明書は、OpenLM Serverに接続しているコンポーネント（例：Agent, Broker, Router）のマシンにも必要です。Linuxの場合、JAVAベースのコンポーネント（Broker、Applications Manager、Router、Reports Scheduler)では、自己署名証明書はローカルのJDKキーストンに追加しなければなりません。JAVA提供の`keytool`ユーティリティを使用して実行してください。

ServerにSSLが一旦設定された場合、`httpS`プロトコールを使用して接続している全てのコンポーネントのホスト名/IPを更新する必要があります。サーバーの自己署名証明書の設定どおり、ホストを指定する時は正確なFQDN名を使用するようにしましょう。



OpenLM Broker

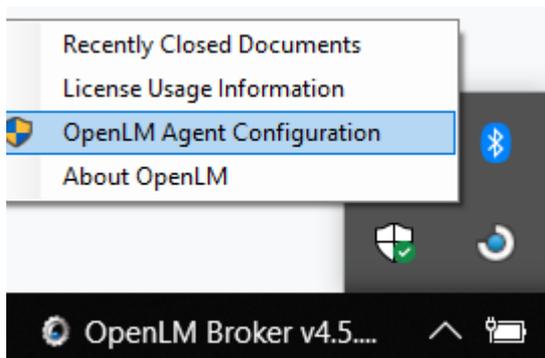
1. OpenLM Brokerコンフィグツールを開始してください。
(Windows Start (スタート) → OpenLM → OpenLM Broker設定ツール)
2. 右側パネルでSSL接続を設定したサーバーを選択する。
3. “OpenLM Server”フィールドはSSL証明書で記載されている**完全に有効なドメイン名**を入力してください。ポート番号を入力し、**SSLボックスがチェックされているのを確認**してください。
4. “Check Connectivity to OpenLM Server” (OpenLM Serverへの接続をチェック) をクリックしてください。SSLの設定に成功している場合、成功ダイアログがポップアップします。
5. “Apply” (適用) をクリックし、新しい設定を保存し、“Restart Broker” (リスタート) をクリックしてください。



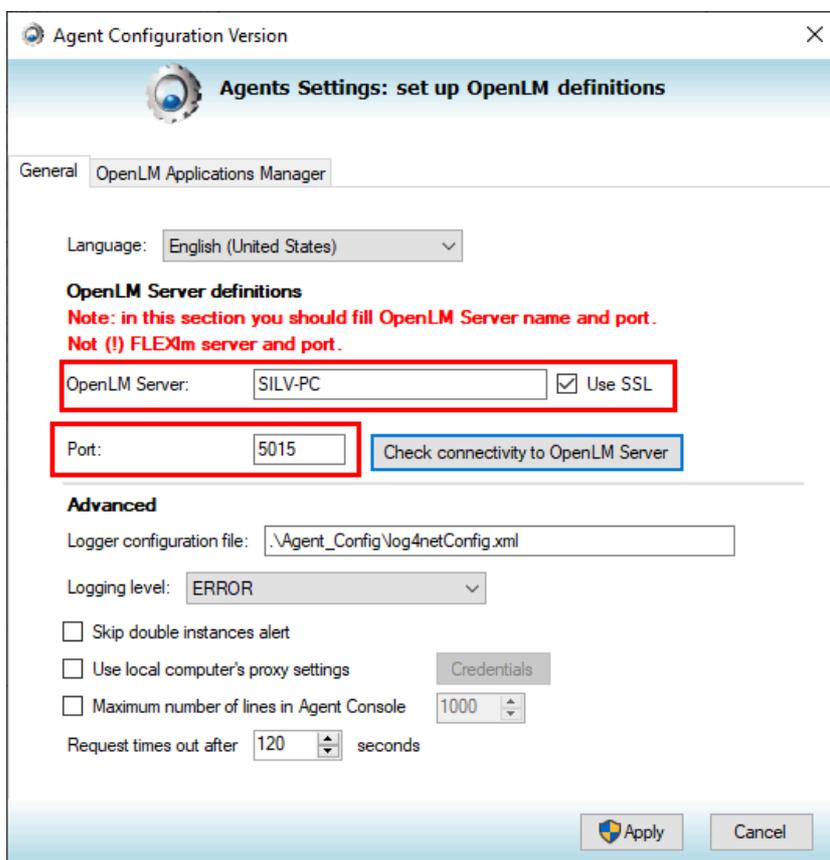
OpenLM Agent

1. Agentトレイアイコンを右クリックし、“OpenLM Agent Configuration” (Agentコンフィグ) をクリックしてください。





2. OpenLM ServerフィールドにSSL証明書で記載された完全に有効なドメイン名を入力してください。“**Use SSL**”（SSL使用）ボックスをチェックし、ポートのフィールドがOpenLM Serverのappsettings.jsonで設定されたメインポートである事を確認してください。(例：5015)



3. “**Check connectivity to OpenLM Server**”（OpenLM Serverへの接続チェック）をクリックし、接続が確立されているか確認してください。

4. “**Apply**”（適用）をクリックして設定を保存し、Agentコンフィグウィンドウを閉じてください。

OpenLM Applications Manager



次のステップでは、OpenLM Applications ManagerがSSL有効のOpenLM Serverへの接続設定の仕方を学びます。OpenLM Applications Manager自体をSSL通信にするには (例 ; Agents へ)、代わりにこの文書を参考にしてください。

1. Applications Managerフォルダーを探し、openlm-app-manager.propertiesファイルをテキストエディターで開いてください。(デフォルト ; C:\Program Files\OpenLM\OpenLM App Manager)
2. 次の変数を変更してください ;

```
openlm.server.protocol = https
```

```
openlm.server.host =
```

```
openlm.server.port = <デフォルトのポートを変更した場合はここでも変更>
```

```
52 #database.username=db_load
53 #database.password=db_load_1234
54
55 # --MS SQL Server 2017 DB configuration--
56 #database.type=MSSQLSERVER2017
57 #database.location=jdbc:sqlserver://openlm_load_mssql:databaseName=openlm-app-manager
58 #database.username=db_load
59 #database.password=db_load_1234
60
61 #https://github.com/brettwooldridge/HikariCP/wiki/About-Pool-Sizing
62 database.pool.max.active=50
63 database.pool.max.idle=-1
64 database.pool.max.wait=-1
65
66 # OpenLM Server connection protocol http or https
67 openlm.server.protocol=https
68 # OpenLM Server connection host name or IP address
69 openlm.server.host=windows2019dev2.openlm.com
70 # Primary connection port to retrieve other ports and auth details
71 openlm.server.port=5015
72 # OpenLM server admin user
73 openlm.server.user=
74 # OpenLM Server admin password
75 openlm.server.password=
76 openlm.server.session.filtering.period.hours=72
```

3. ファイルの変更を保存する。
4. Windows Servicesを開き、“OpenLM App Manager”サービスをリスタートする。

OpenLM Router

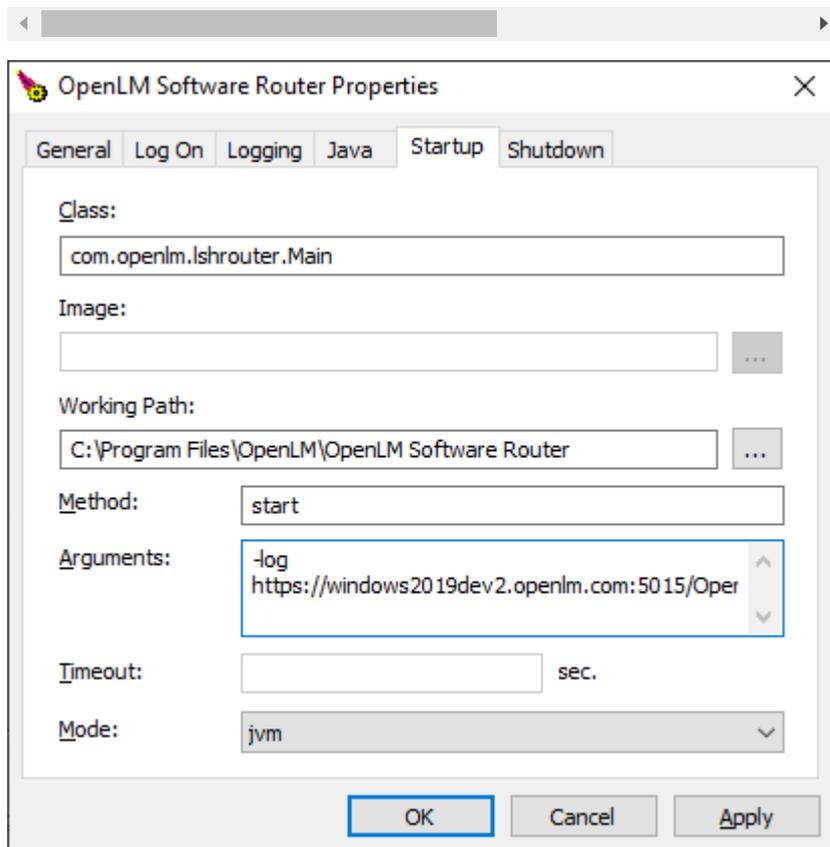
Windowsの場合

1. “OpenLM Software Router.exe” を実行する (デフォルト ; C:\Program Files\OpenLM\OpenLM Software Router\bin)
2. Routerプロパティツールが開きます。“Startup” (スタートアップ) タブをクリックしてください。



3. SSL証明書で記載されたOpenLM Serverのアドレスをアーギュメントに反映するように編集してください。例:

```
-log https://windows2019dev2.openlm.com:5015/
```



4. “Apply”（適用）をクリックしOKでツールを閉じてください。
5. Windowsサービスを開き“OpenLM Software Router”サービスをリスタート。

Linux/Unixの場合

1. OpenLM Routerをインストールしたフォルダーで**router.sh** スクリプトを編集してください。
2. SSL証明書で記載されたOpenLM Serverのアドレスを-logの後のアーギュメントに反映するように編集してください。例:

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

```
java -Dlog4j.configuration=file:log4j.properties
```

3. OpenLM Routerサービスをリスタートしてください。



OpenLM Reports Scheduler

1. OpenLM Report Schedulerフォルダーに行き **report_scheduler.properties** ファイルをテキストエディターで開く(デフォルトC:\Program Files (x86)\OpenLM\OpenLM Report Scheduler)

2. 次の変数を変更:

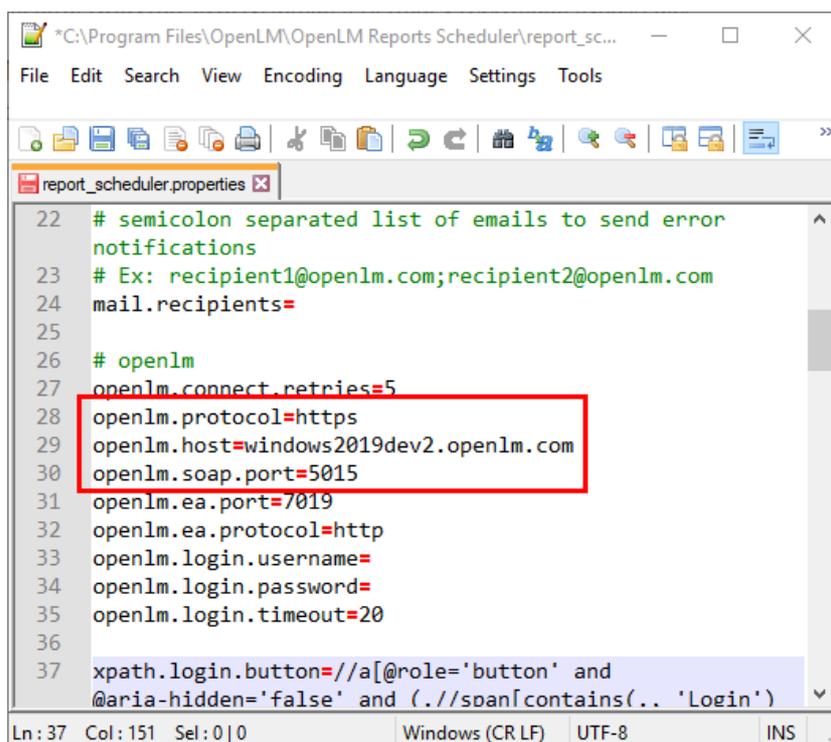
```
openlm.protocol=https
```

```
openlm.host=
```

```
openlm.soap.port=<デフォルト5015を変更した場合に変更>
```

3. 変更を保存する

4. Windowsサービスを開き“OpenLM Report Scheduler”サービスをリスタート



```
*C:\Program Files\OpenLM\OpenLM Reports Scheduler\report_sc...
File Edit Search View Encoding Language Settings Tools

report_scheduler.properties
22 # semicolon separated list of emails to send error
    notifications
23 # Ex: recipient1@openlm.com;recipient2@openlm.com
24 mail.recipients=
25
26 # openlm
27 openlm.connect.retries=5
28 openlm.protocol=https
29 openlm.host=windows2019dev2.openlm.com
30 openlm.soap.port=5015
31 openlm.ea.port=7019
32 openlm.ea.protocol=http
33 openlm.login.username=
34 openlm.login.password=
35 openlm.login.timeout=20
36
37 xpath.login.button=//a[@role='button' and
    @aria-hidden='false' and (..//span[contains(.. 'Login')]
```

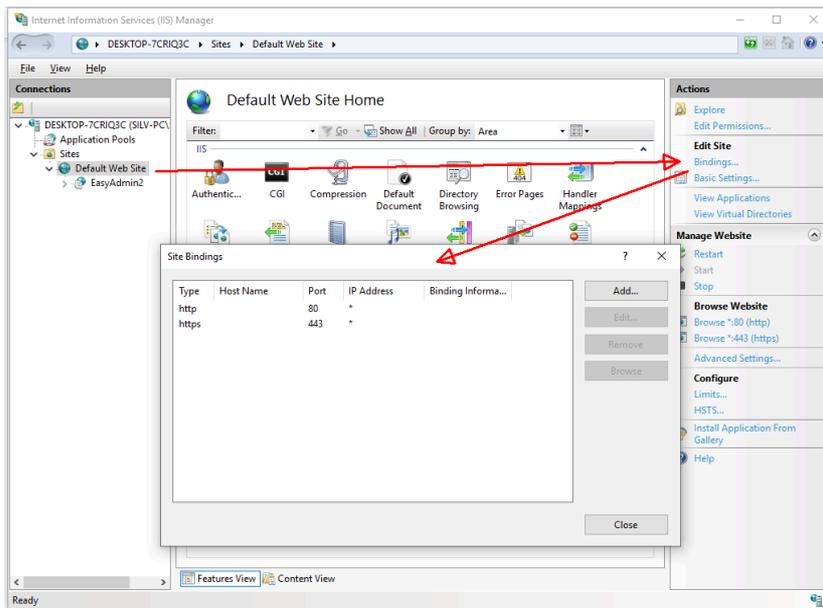
3. EasyAdminユーザー接続にSSLを有効化

EasyAdminをIISで運用している場合、EasyAdmin<->ユーザー接続でSSL通信を有効化できます。EasyAdminをSSLで設定する事は、セクション1に頼らないです。OpenLM Server ポート



(5015) でSSLが有効化されているかどうかには依らず有効化できます。有効化のステップは単純に以下の通りです。

1. IISマネジャーを開く
2. Sites (サイト) に移動し → Default Web Site (デフォルトウェブサイト)
3. 右のパネルで、Bindings (バインディング) をクリックしデフォルトの443 HTTPSポートを追加し、SSL証明書を指定します。



4. ウィンドウを閉じ、ウェブサイトのリスタートします。
5. 次のURLでEasyAdminを開けるかどうか検証。

<https://EasyAdmin2/index.html>

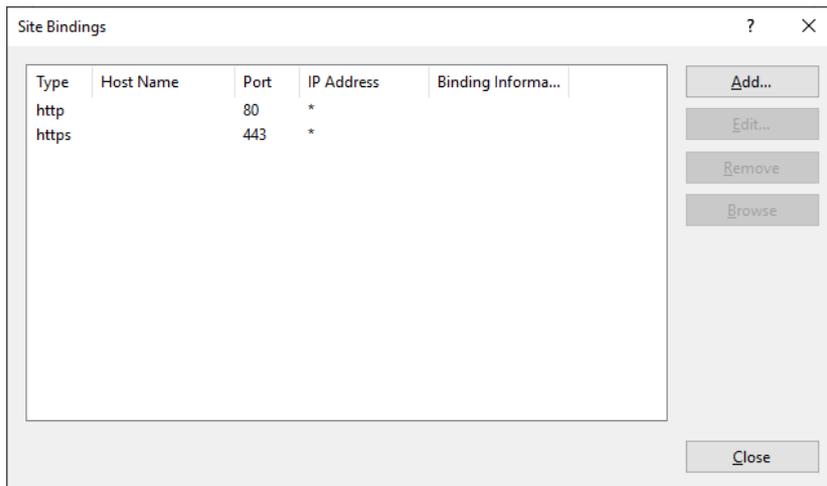
4. SSL有効のOpenLM Serverバージョン4.xから5.xにアップグレード

IISを通してOpenLMバージョン4.xポートでSSLを以前設定していた場合、最初に**appsettings.json** で指定されたポートとコンフリクトするIISバインディングを取り除かなければ、OpenLM Serverのプロセスは開始に失敗します。SSLを使用するには手動の変更が必要です。

1. IISマネジャー → Sites (サイト) → Default Web Site (デフォルトウェブサイト) (EasyAdminをホストするように設定したサイト)



- 右パネルで、**Bindings (バインディング)** をクリックし、EasyAdminに使用するポート以外の以前設定した全てのSSL設定ポートを取り除く (7012, 7016, 7014等)



- Default Web Site (デフォルトウェブサイト) をリスタート。
- 本書のセクション 1 のSSL設定手順に従ってください。

+81 (0)50 5893 6263

sales@openlm.com

