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 http**s**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)

₩ Cer ~ 📫 ~ 📫	rtificates - Current User Personal Certificates	ation Date i.2035	Intended Purposes	Friendly Name	Status	Certi ^			
	Certificates	.2036 .2004	<all> Time Stamping</all>	Microsoft Root Cert Microsoft Root Cert VeriSign Time Stam			1	Field Signature hash algorithm Signature	Value sha256 SILV-PC
> > > > >	Enterprise Trust Intermediate Certification Au Active Directory User Object Trusted Publishers Untrusted Certificates	.2031 .2042 1.2021 i.2021 1.2029	Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati	QuoVadis Root CA 2 QuoVadis Root CA QuoVadis Root Cert OpenLM_Test Trustwave		CA	d H	Valid from Valid to Subject Public key Public key parameters	jol, 28 mai 2020 11:36:58 vineri, 28 mai 2021 03:00:00 SILV-PC RSA (2048 Bits) 05 00 Key Encideement, Data Encid
> 11 > 11 > 11 > 11 > 11 > 11	Third-Party Root Certification Trusted People Client Authentication Issuers Other People Local NonRemovable Certific	i.2021 i.2034 .2038 i.2036 i.2036	Server Authenticati Server Authenticati Server Authenticati Time Stamping, En Server Authenticati	SelfSSL Starfield Class 2 Cer Starfield Root Certif Starfield Root Certificati SwisSign			6	CN = <u>SILV-PC</u>	
>	>	1.2032 1.2036	Code Signing Server Authenticati	<none> thawte</none>		`	Ľ	1	Edit Properties Copy to File

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http**s**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)。



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、http**S**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

 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 Broker		- 🗆 ×							
OpenLM Broker									
🔾 Add OpenLM Server 🕓 Add OpenLM SaaS Server 😵 Delete 🤤 Disable 👄 Collapse All Ports									
OpenLM Servers	OpenLM Server connectivity								
localhost: 5015	OpenLM Server SILV-PC								
Cicense Servers	Port S015								
 Commands status data_inquiry reread 	Sending Timeout 45 束	(sec)							
• remove_license • • start	Activate Buffering 🗹 Buffer File Size	3 🔹 (Megabytes)							
 Vendors Vendor Name to Be filled 	SSL Clean Buffer								
• Log Files • Port 3808 • Commands	Status: This Receiver is Active								
• start • start • start • start • vendors • Vendors • Log Files # Advanced Settings	Check Connectivity to OpenLM Server								
 Reset Recording 									
	🖉 Apply) Cancel 😲 Hint							
	🔅 Detect 🛃	Exit III Restart Broker							

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)

Agent Configuration Version	×							
Agents Settings: set up OpenLM definitions								
General OpenLM Applications Manager								
Language: English (United States)								
OpenLM Server definitions Note: in this section you should fill OpenLM Server name and port								
Note: In this section you should fill OpenLM Server name and port. Not (!) FLEXIm server and port.								
OpenLM Server: SILV-PC 🔽 Use SSL								
Port: 5015 Check connectivity to OpenLM Server								
Advanced								
Logger configuration file: .VAgent_ConfigVog4netConfig.xml								
Logging level: ERROR ~								
Skip double instances alert								
Use local computer's proxy settings Credentials								
Maximum number of lines in Agent Console								
Request times out after 120 🖕 seconds								
September 2017 Cancel C	el							

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 グウインドウを閉じてください。

OpenLM Applications Manager

OpenLM Server v5のSSL設定 – KB501 - OpenLM Japan

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、openIm-appmanager.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;

openIm.server.protocol = https

openIm.server.host =

openIm.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>

🔚 param	is jis 🔀 🔚 openim-app-manager properties 🔀	
52	#database.username=db load	^
53	#database.password=db load 1234	
54		
55	#MS SQL Server 2017 DB configuration	
56	#database.type=MSSQLSERVER2017	
57	<pre>#database.location=jdbc:sqlserver://openlm_load_mssql;databaseName=openlm-app-manager</pre>	
58	#database.username=db_load	
59	<pre>#database.password=db_load_1234</pre>	
60		
61	<pre>#https://github.com/brettwooldridge/HikariCP/wiki/About-Pool-Sizing</pre>	
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. <u>openlm</u> .com	
70	# primary connection port to retrieve other po rts and <u>auth</u> details	
71	openlm.server.port= 5015	
72	# openim server aomin user	
73	openlm.server.user=	
74	# OpenLM Server admin password	
75	openlm.server.password=	
76	openlm.server.session.filtering.period.hours=72	~
<		>
Proper I	ength: 2,825 lines: 76 Ln: 65 Col: 1 Sel: 0 0 Windows (CR LF) UTF-8 IN	s

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/

	ware Router Properties
eneral Log On	Logging Java Startup Shutdown
<u>C</u> lass:	
com.openIm.ls	hrouter.Main
Image:	
Working Path:	
C:\Program Fil	les\OpenLM\OpenLM Software Router
Method:	start
<u>M</u> ethod: <u>A</u> rguments:	-log https://windows2019dev2.openlm.com:5015/Oper
<u>M</u> ethod: <u>A</u> rguments: <u>T</u> imeout:	start -log https://windows2019dev2.openlm.com:5015/Oper sec.

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** s 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.propert

.

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:

openIm.protocol=https

openIm.host=

openIm.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



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 オルトの443 HTTPSポートを追加し、SSL証明書を指定します。

 Internet Information Services (IS) Manager RIQ3C → Sites → Default Web Site →	×
<u>F</u> ile <u>V</u> iew <u>H</u> elp		
Connections	Default Web Site Home	Actions Actions Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories
	Site Bindings ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?	Manage Website (*) K Restart Start Start Stop Browse Website Browse Website Browse Website Denvose %43 (https) Advanced Settings Configure Limits HSTS Install Application From Galley Help
¢	Close	

4. ウインドウを閉じ、ウェブサイトをリスタートします。

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) 2. 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

<u>ポートを取り除く</u>(7012, 7016, 7014等)

e Bindiı	ngs				? ×
Type http https	Host Name	Port 80 443	IP Address * *	Binding Informa	<u>A</u> dd Edit <u>R</u> emove <u>B</u> rowse
					Close

3. Default Web Site (デフォルトウェブサイト) をリスタート。

4. 本書のセクション1のSSL設定手順に従ってください。

