Version 5 of OpenLM Server comes with some changes. Here's what you need to know.

Component Compatibility

Installing OpenLM Server version 5 means that you will also have to upgrade any of the components that interact with Server.

The minimum component versions compatible with v5 are:

- OpenLM Broker v4.9.0
- OpenLM Agent v5.0.0
- OpenLM Applications Manager v2.3
- OpenLM Reports Scheduler v1.9.8
- OpenLM Router v2.1

Application Ports

The default communication port for OpenLM Server is now 5015. There are no more different ports for each application: Broker, Agent, Router, etc… All communication is done on 5015.

What if I'm upgrading from v4, do I need to change any settings?

If upgrading from v4, the installer will detect previous port configurations and keep the old port numbers only for the Broker port (7016) and the Agent port (7012) unchanged. This way, if you have any version 5 compatible Brokers or Agents pointing to an existing v4 OpenLM Server that you plan to upgrade, no changes will be necessary. These settings are automatically written in the OpenLM Server/bin/**appsettings.json** file.

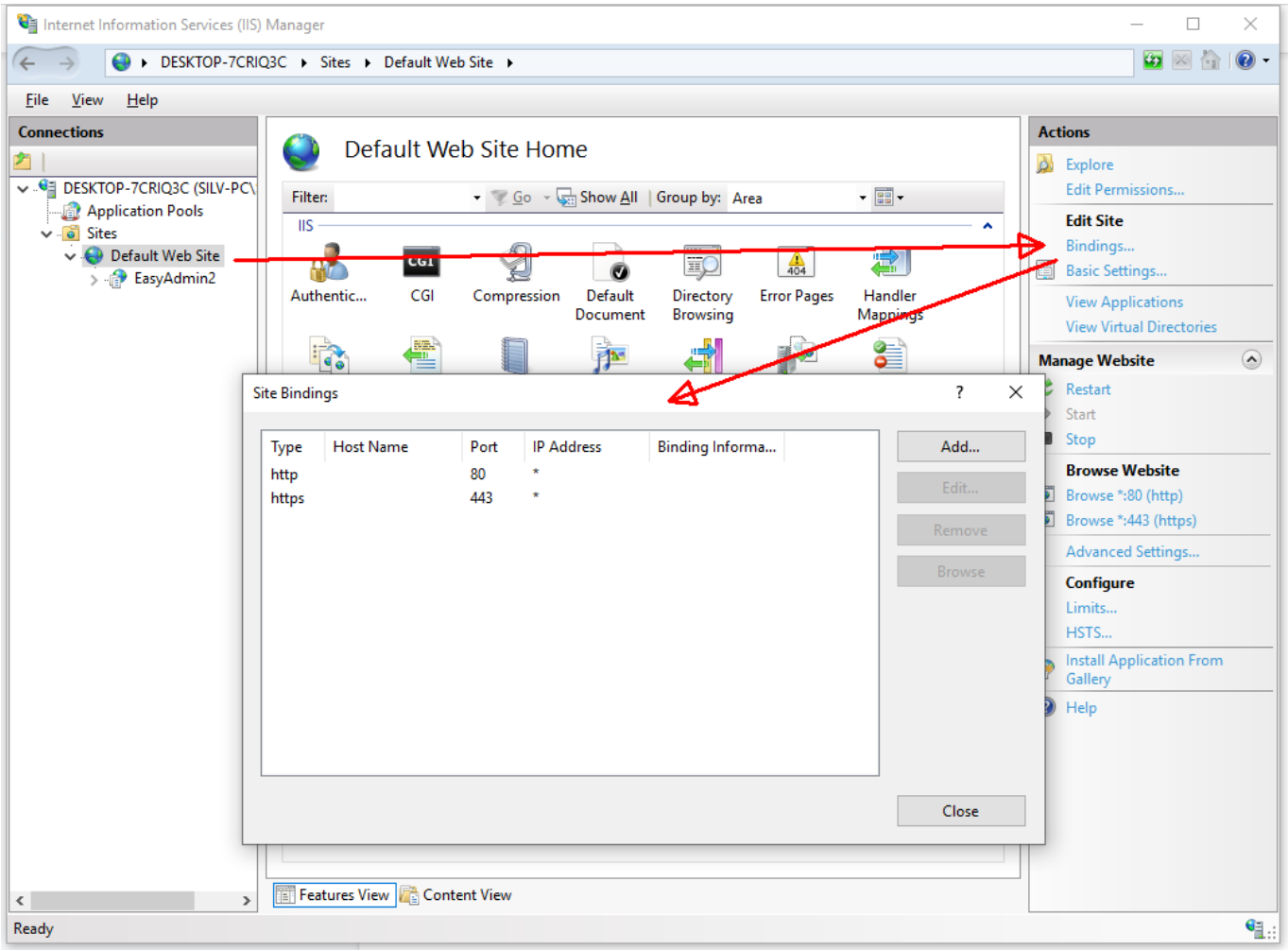
If you're **installing v5 from scratch**, the main port will be 5015. If you already have Brokers or other components pointing to the same hostname or IP address, you have two options:

1. Change each component configuration to point to the new Server port. This can be a hassle if you have many installations (e.g. hundreds of Brokers).
2. Add an “alias” port configuration in the OpenLM Server/bin/**appsettings.json** file. The alias port can be any free port number (e.g. 7016), and still act as the “old” port configuration, requiring a change only on the OpenLM Server machine.

What if I had previously configured Server ports to use HTTPS/SSL?

If you have previously configured SSL for OpenLM’s ports to be served via IIS, you will have to remove the IIS bindings as they will conflict with the ports specified in appsettings.json and the Server process will fail to start. A manual change to use SSL will also be required.

1. Go to IIS → Sites → Default Web Site → on the right panel, click on Bindings and remove any conflicting ports except those used to serve EasyAdmin:



2. Open the **C:\Program Files (x86)\OpenLM\OpenLM Server\WebApps\EasyAdmin2\params.js** file in a text editor with administrator privileges and edit the protocols to use http**s.** Make sure the FQDN name is exactly as it's written on the SSL certificate (e.g. hostname.com, etc.).

```
var _operationMode = "";
var _enableDemoMode = false;
var _debug = false;
var _useProxy = true;
var _sampleMode = false;
var _schedulingTaskURL = 'http://127.0.0.1:8888/report_scheduler/job';
var _SAASLoginURL = 'https://saas.openlm.com/SaasClient/Home/Login';
var SoapProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';
var WebProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';
var WebProxySaasPath = 'https://SILV-PC:8084/SaasService/service.svc';
var OpenLMServer = 'https://SILV-PC:5015/api/easyadminapi/postmessage';
var EasyadminRoot  = 'https://SILV-PC/easyadmin_trunk/';
var _angularURL = "";
var Locales = [["en_US", "English US", "UTF-8"],
    ["es_ES", "Español - España", "ISO-8859-1"],
    ["de_DE", "Deutsch - Deutschland", "ISO-8859-1"],
    ["fr_FR", "Française - France", "ISO-8859-1"],
    ["nl_NL", "Dutch - Nederland", "ISO-8859-1"],
    ["pt_BR", "Português - Brazil", "ISO-8859-1"],
    ["ja_JP", "日本語 - 日本", "UTF-8"],
    ["zh_CN", "汉语 - 中国", "UTF-8"]];
```

3. Open **C:\Program Files (x86)\OpenLM\OpenLM Server\bin\appsettings.json** in a text editor with administrator privileges.

4. At the end of the file, edit as follows:

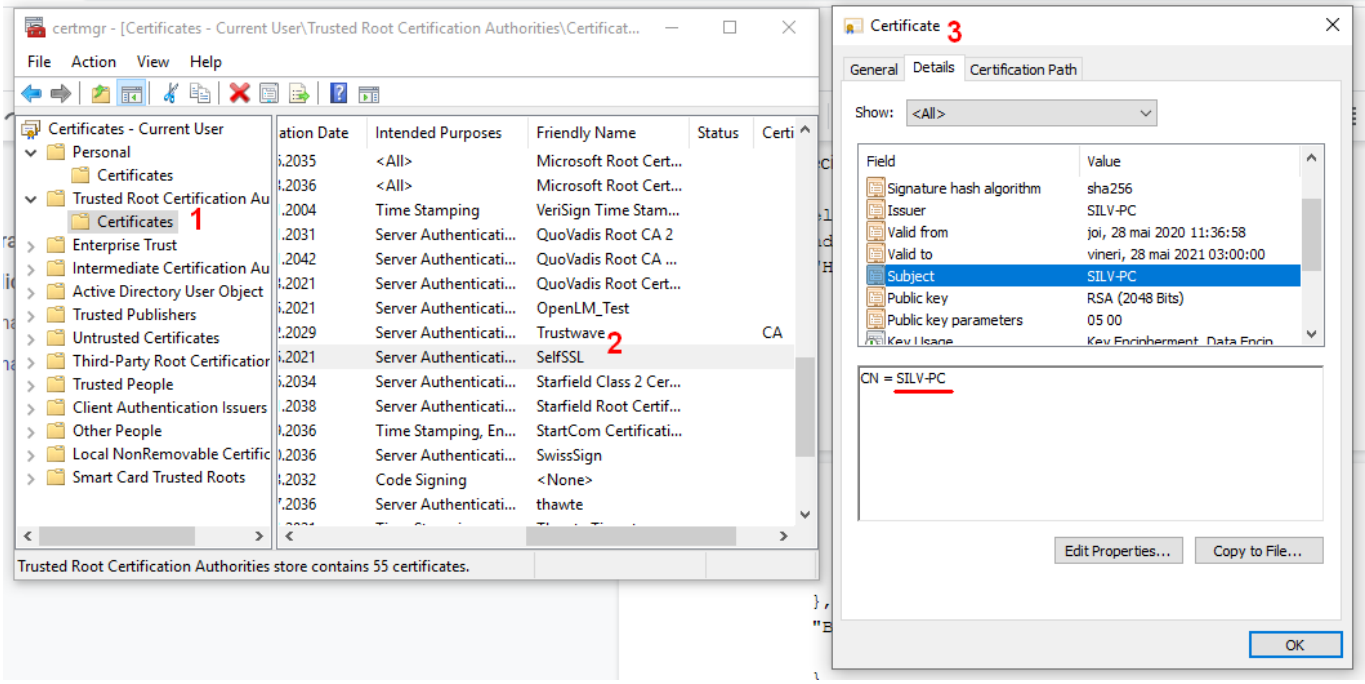
- Edit the “Url” variables to point to http**s.**
- Edit the “Kestrel” node depending on whether you want to use a certificate store or a specific path to a certificate.
- If needed, you can add extra ports that will act as an alias to the main one. The name between the quotes (e.g. “Broker”) is purely descriptive and can hold any value.

a) to use a certificate from the Windows store

```
"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"
    }
  }
}
```

Where "**Subject**" is the owner of the certificate, whom it has been issued to. This can be found by going to Run → certmgr.msc → select the certificate store where your certificate resides → double-click on it → click the Details tab → locate the Subject



"**Store**" indicates the certificate store. The "Personal" store is referred to as "My" and the

“Trusted Root Certification Authorities” as “Root”. For the names of other certificate stores, consult this article.

“**Location**” can be either LocalMachine or CurrentUser.

Set “**AllowInvalid**” to true to permit the use of invalid certificates (for example, self-signed certificates).

b) to use a certificate with a specific path

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

- **Path** is the path to the certificate file. Make sure the Windows paths use double backslashes instead of forward slashes.
- **Password** is the password for the private key of the certificate.
- Make sure the curly braces are properly closed.

5. Save the file.

6. Restart the “OpenLM Server” service.

> **Important:** for both options a) and b) it is mandatory that the certificate is also installed and present in the certificate store of the machine connecting to OpenLM Server (e.g. Agent).

If configuring SSL on a new install of OpenLM Server v5, check out this guide instead.

License file

Your version 4 license file will not be compatible with OpenLM Server v5. Please request a new license file from **sales@openlm.com**

LDAP Synchronization

LDAP Synchronization has been split from v5 and is now provided as a separate component called Directory Synchronization. You will need to install the Directory Synchronization Service (DSS) and Directory Synchronization Agent (DSA) to continue having your users synchronized with a domain directory.

Does this mean that if I upgrade without DSS & DSA I will lose my current syncs?

No.

If you upgrade without installing DSS & DSA, your sync definitions and all associated data will be kept, however they will not be active. Once you install DSS & DSA, you will be able to migrate all your current sync definitions to the DSS and continue to use LDAP synchronization as previously.