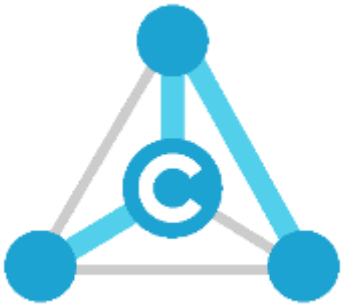
# How to Secure on-premise Relays

By: Sanja Muench



Last Revision: February 2, 2018

# Table of Contents



*IOS is a trademark or registered trademark of Cisco in the U.S. and other countries.*
*Apple, OS X, and iPhone are registered trademarks of Apple, Inc. in the U.S. and other countries.*
*Internet Explorer, Microsoft, Visual Studio, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and other countries.*
*Linux is a registered trademark of Linus Torvold, in the U.S. and other countries.*
*Ubuntu is a registered trademark of Canonical Ltd.*
*Debian is a Registered Trademark of Software in the Public Interest, Inc.*
*Android is a trademark of Google Inc.*
*Mono is a registered trademark of Novell, Inc.*
*Xamarin is a trademark of Xamarin Inc. in the United States and other countries.*
*Raspberry Pi is a trademark of the Raspberry Pi Foundation.*

## Introduction

There are circumstances in which customers want to make sure communication even on their local networks is secure.

To encrypt communication with a local, on-premise relay, the inbound port used by the relay and the NMI must use TLS/SSL.

TLS/SSL requires a certificate for the encryption. This document provides all the necessary steps to enable TLS/SSL for on-premise relays.

# Chapter 1 Requirements

How to create a secure on-premise relay?

- By placing a HTTPS certificate on a local PC
  - used to enable HTTPS on-premise installed relay or gate

Securing a local relay has two requirements:

1. Certificate that is valid for the current PC the relay is to be installed on
2. Get your Relay GUID

## 1.1 A certificate valid for the full DNS name of the PC

- A certificate that is valid for the current PC where installation will take place
- Two choices:
  1. Wildcard certificate: i.e: "*.c-labs.com"
  2. A certificate for a specific machine (DNS name): i.e. "mypc.c-labs.com"

## 1.2 The GUID of your relay application host

- The GUID of AXOOM Gate is: {933D71C0-BAF0-4D40-AAB6-A1B36C5CD8BE}

- For your own app, follow these steps to locate the GUID:
  - Open relay host
  - Under **Properties** Folder locate and open **AssemblyInfo.cs** file
  - In this case, GUID is located in line 23

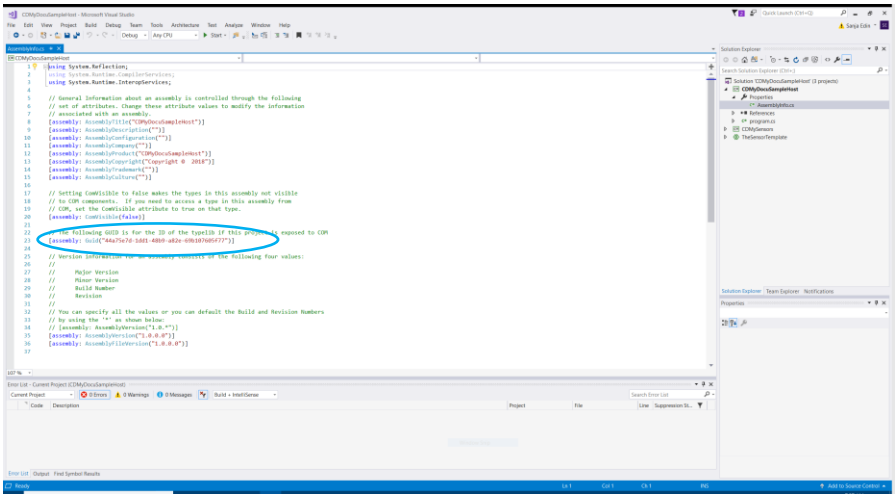


*Figure 1: AssemblyInfo.cs*

It is this GUID that the certificate will be matched to, when somebody goes on your relay on your current machine. This GUID is auto generated when a new host app is created by using template in our SDK.

# Chapter 2 Prep your PC

Here are steps to prep your PC:

## 2.1 Ensure DNS and Certificate name match

For TLS/SSL to work correctly you must ensure that the DNS you assigned in certificate matches to the name of the local machine.

### 2.1.1 Ensure successful ping with the DNS name

While running as an Administrator in **Command Prompt**, enter following command:

```
ping mypc.c-labs.com
```

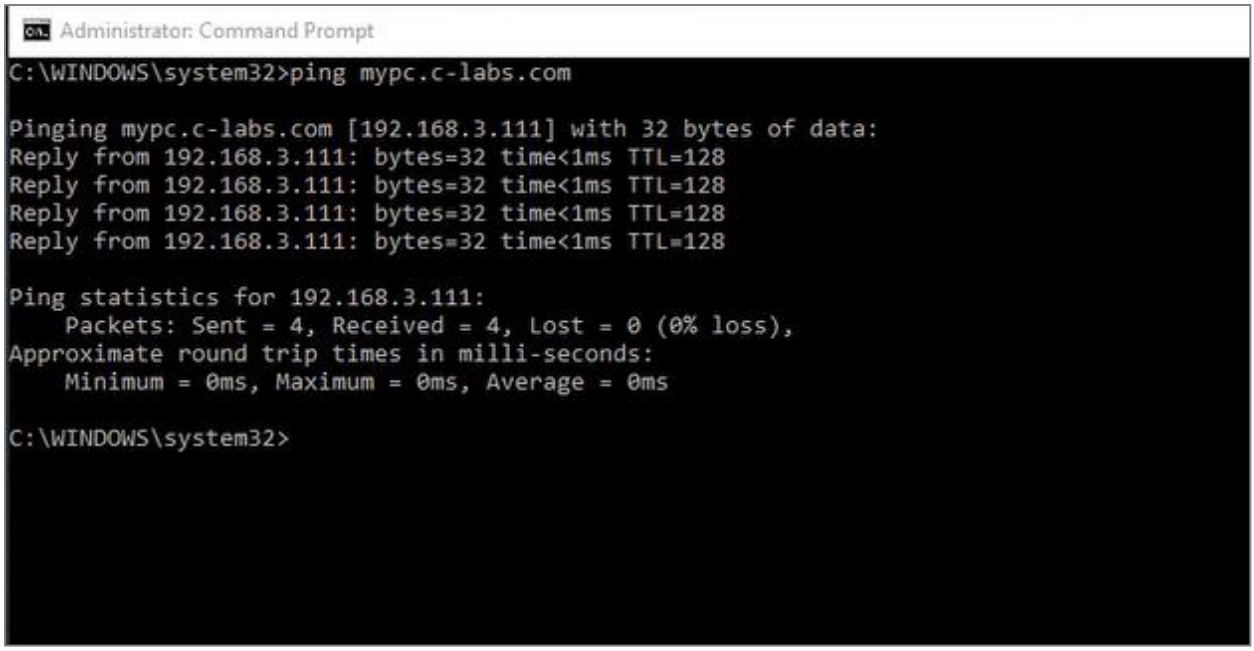



*Figure 2: ping*

NOTE: To run Command Prompt as an Administrator: Locate Command Prompt. Right-click and select to Run as an Administrator. This is not necessary for the ping but for the commands that will follow later.

Make sure that

a) The DNS Names resolve correctly to the PC's IP Address
b) Get a reply from the PC. This might not work if your firewall blocks pings

## 2.2 Install the Certificate on your PC

Certificate installation process includes: getting certificate's own hash/Thumbprint, assigning the GUID of the Host app to port 443 and adding this hash into the command in Administrator Command Prompt.

### 2.2.1 Locate and copy certificate's own hash

1. Open Manage Computer Certificates

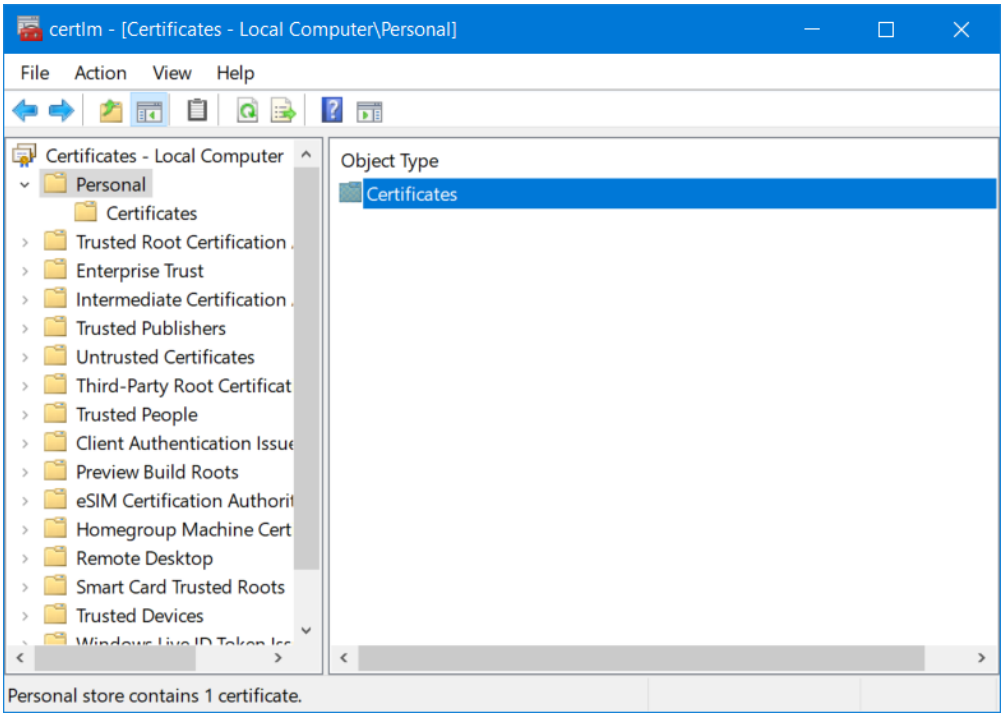



*Figure 3: Manage Computer Certificates*

2. Under Certificates on the left, Open **Personal** folder to see all imported certificates. Ensure the certificate in question is installed, if not do so at this time by following steps described in section : 2.2.1.1 Import the Certificate.

#### *2.2.1.1 Import the Certificate*

1. Open the MMC (Start > Run > MMC).
2. Under **Actions** tab, select **All Tasks**, and **Import…**
3. Use the Certificate Import Wizard to complete this step as described in table below:

| **Using Certificate Import Wizard to install certificate** |
|---|

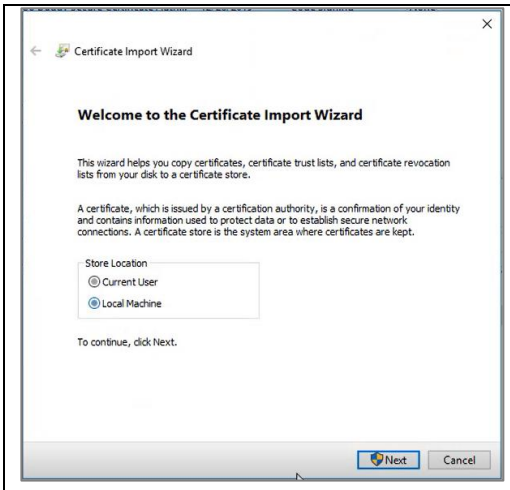



*Figure 4: Certificate Import Wizard 1*

**Select Local Machine**

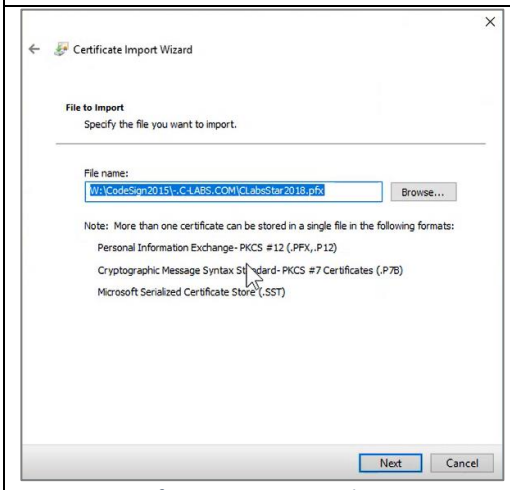



*Figure 5: Certificate Import Wizard 2*

**Specify the file you want to import:**

In this case, a file ending with .pfx will be installed.

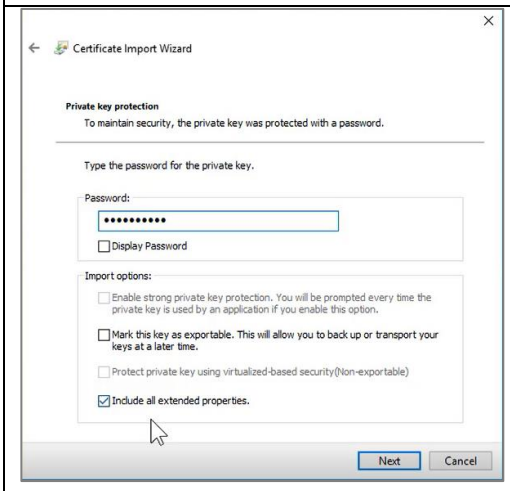
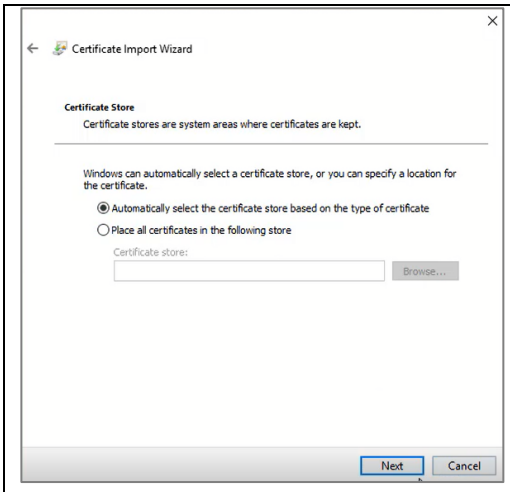
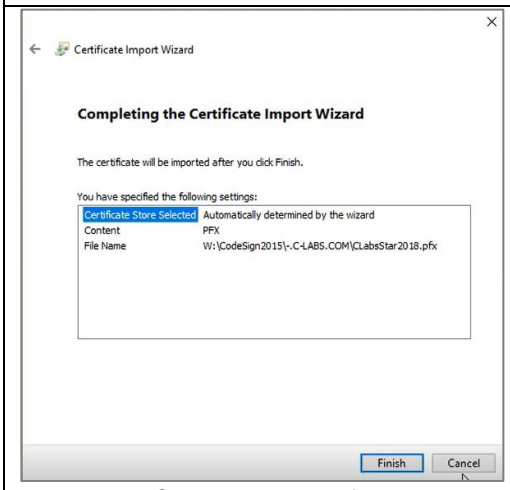



*Figure 6: Certificate Import Wizard 3*

**Enter Password**

| | |
|---|---|
|  <br>*Figure 7: Certificate Import Wizard 4* | **Specify location where certificate is to be stored:** |
|  <br>*Figure 8: Certificate Import Wizard 5* | Click on the **Finish** button. |

3. Once the certificate is installed, locate and copy the hash.
   In the Manage Computer Certificate window, Double-click on the certificate in question.
   Follow steps described in table below, to locate and copy Certificate's hash.

**Locating and copying certificate's hash:**

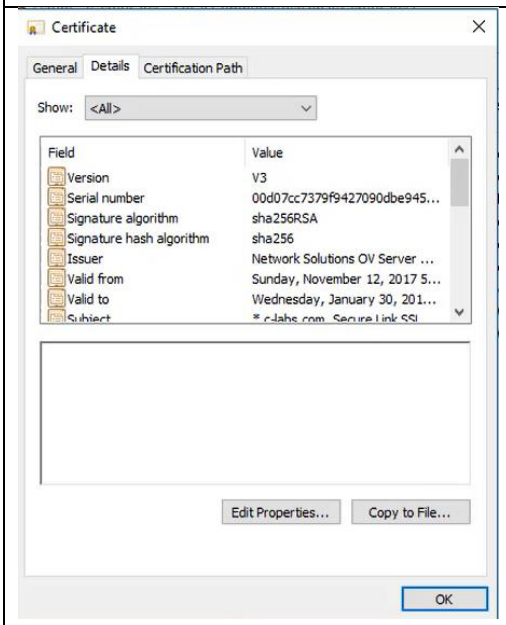



*Figure 9: Certificate Details Page*

Click on **Details** tab and scroll down to **Thumbprint**

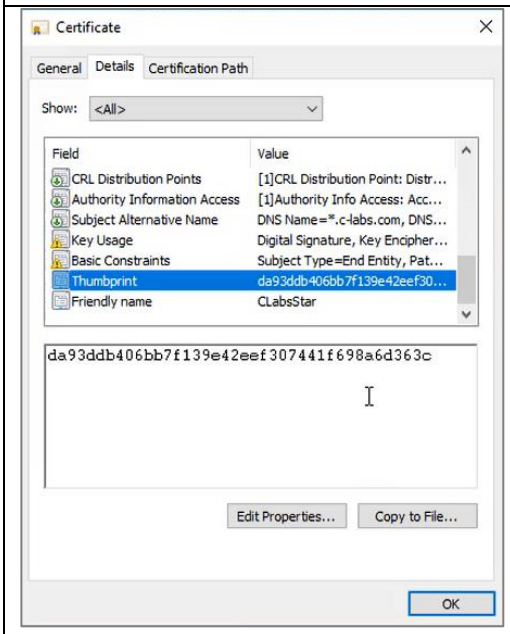



*Figure 10: Certificate hash exposed*

Click on the **Thumbprint** to expose the hash.

Copy the hash to be used in your app.
Because some certificates come with blank spaces and special characters, it is recommended:

1. Paste this hash into the Notepad app,
2. Remove all empty spaces and any special characters

3. Hold on to this window, as you will need to copy this hash out of the Notepad and put it into the command in the next step.

### 2.2.2 Assign the Certificate to the GUID of the Host app and then to your STATIONPORT (443 is the standard SSL/TLS port but we support any other port as well)

NOTE: Only one application id per port is allowed. If you want to add more applications, assign a unique port number.

Add certificate hash within following command into Command Prompt (you had open for the Ping):

```
netsh http add sslcert ipport=0.0.0.0:8080 certhash=<COPY HASH HERE FROM
THE NOTEPAD> appid={2d59d3d9-bbd6-4ab9-bd1a-7210e5c46146}
```

### 2.2.3 Ensure file was added successfully

Upon successful execution, the console will display:

*SSL Certificate successfully added*

# Chapter 3 Update App.config

If you would to go on to the site, you'd see the login screen with the Email and Password prompts but would only be able to get to your portal– this is because not all configurations were made in the C-DEngine. At this point, we're still using HTTP instead of HTTPS.

## 3.1 Update App.Config

In order to fix the App.config file, and prepare it for SSL, in the App.Config file, locate the **MyStationURL** and change its value to:

```
Value="https://mypc.c-labs.com:8080"
```

- Note: here only use the full DNS name here you're using on the browser, that is pinging correctly and corresponds to the Certificate. If you are using https on port 443 you do not explicitly have to specify the port. Most relays are using other ports then 443 then you must specify it here. AXOOM-Gate is using Port: 8701
- Factory-Relay/Machine Monitor is using Port: 8704

### 3.1.1 Update App.config with new URL

At this point we:

- ✓ have the Certificate with mypc.c-labs.com
- ✓ An installed Certificate on port 8080 (netsh command)

Final step: must update App.config to point to this location

In the host test project, open **program.cs** file.
Add following to the **Argument List**(Configuration settings)**:**

```
ArgList.Add("MyStationURL", "https://mypc.c-labs.com:8080");
```

Remember to change http to https in the browser when you run your app, as http will no longer function.

# Chapter 4 Summary

**3 Steps:**

Step 1. Get requirements

- Get Certificate and get the Certificate Hash/Thumbprint
- Get your Relay GUID

Step 2: Prep your PC

- Make sure your DNS name matches the Certificate name
    - *And ping works correctly with the DNS Name*
- Install the Certificate on your PC

Step 3: Update App.Config

- Update your App.Config with new “MyStationURL” matching PC DNS