How to Secure on-premise Relays

By: Sanja Muench



Last Revision: February 2, 2018

Table of Contents

Introduc	ction	3
Chapter 1	Requirements	4
1.1	A certificate valid for the full DNS name of the PC	4
1.2	The GUID of your relay application host	4
Chapter 2	Prep your PC	5
2.1	Ensure DNS and Certificate name match	5
2.1.1	Ensure successful ping with the DNS name	5
2.2	Install the Certificate on your PC	5
2.2.1	Locate and copy certificate's own hash	6
2.2.2	Assign the Certificate to the GUID of the Host app and then to your STATIONPORT (443 is the	
stand	lard SSL/TLS port but we support any other port as well)	10
2.2.3	Ensure file was added successfully	10
Chapter 3	Update App.config	11
3.1	Update App.Config	11
3.1.1	Update App.config with new URL	11
Chapter 4	Summary	12

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
 - \circ ~ 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

19 COMpDocdarepitritist - Microsoft Visual Statio						🔨 🖉 🖓 🖓 🖓 🖓 🕄 🖓 🕄 🖉
File Edit View Project Build Debug Team Tools Architecture Test Assister Window Help						🔺 Sania Frita 🔹 🎫
0 • 0 8 • 0 9 4 9 • 0 • 0 • 0 • 0 • 0 • 0 • • • 5 • • • 8 • • 8 • 5 • 5 • 1 • • • • 9 • 1 • 0 • 0 • 0						-
						Souton Dipoer
10 United and the full section in the full section in the full section in the full section in the full section is the full section in the full section is the full section in the full section is the full sec						○○☆☆ · `○ · ≒ Č # Ø · ፆ -
2 using System Bartime CompilerServices:						Search Solution Explorer (Chri+;) P +
a using System. Runtime. InteropServices;						Solution TCMyDocuSampleHost (3 projects)
4						A E CDMyDocuSampleHost
5 // General Information about an assembly is controlled through the following						🖌 🎜 hoperties
6 // set of attributes. Change these attribute values to modify the information						(* Amerablykitucs
7 // associated with an assembly.						P *# References
8 [assembly: AssemblyTitle("CDPyOccaSampleHost")]						» e* program.ci
9 [assembly: AssemblyDescription(**)]						P E CMpanian
10 (assessive assessive and granting ("))						 W neseonenyole
12 [assembly: assembly@roduct("CDMonora@ampleinst")]						
13 [accently: accently/myright/"Convright 0, 2018")]						
14 [assembly: AssemblyTrademark(")]						
15 [assembly: AssemblyCulture(")]						
16						
17 // Setting CowVisible to false makes the types in this assembly not visible						
18 // to COM components. If you need to access a type in this assembly from						
19 // COM, set the ComVisible attribute to true on that type.						
20 [assembly: ConVisible(false)]						
21 statistical and the statistical stat						
23 [accesh]y: [6:6]("46a75c74:1611-680-382-5019766577")]						
25 // Version information to an approach consists of the following four values:						
26 //						
27 // Hajor Version						
28 // Plinor Version						
29 // Build Number						Solution Explorer Team Facilities Notifications
30 // Revision						
						Properties • • • •
32 // Tou can specify all the values or you can default the build and nevision numbers						
14 // by using the ** as shown below: 14 // Issueshirt Assessibility (as \$*1)						10 P /
35 [assembly: assembly/environ[1, a, a, and						
36 [assembly: AssemblyfileVersion("1.0.0.0")]						
1						
107.00						
Error List - Current Project (CDMyOocuSampleriost)					• • • ×	
Carrent Project - 😨 0 Errors 🔺 0 Warnings 🚺 0 Mossages 🦎 Build + IntelliGence -				Search Error List	, P -	
¹⁵ Code Description	Project	File		Line Suppression 5	- Y	
Error List Output Find Symbol Results						
C Ready		14.1	Col 1	0.1	PIS .	 Add to Source Control +

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

Administrator: Command Prompt
C:\WINDOWS\system32>ping mypc.c-labs.com
Pinging mypc.c-labs.com [192.168.3.111] with 32 bytes of data: Reply from 192.168.3.111: bytes=32 time<1ms TTL=128 Reply from 192.168.3.111: bytes=32 time<1ms TTL=128 Reply from 192.168.3.111: bytes=32 time<1ms TTL=128 Paply from 192.168.3.111: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.3.111: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\WINDOWS\system32>

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

\overline certlm - [Certificates - Local Computer\Personal]		×
File Action View Help		
🗢 🔿 🙍 📋 🙆 😹 🛛 🖬		
Certificates - Local Computer Computer Certificates Certificates Certificates		
Certificates		
> 🛅 Enterprise Trust		
Intermediate Certification		
Intrusted Publishers Untrusted Certificates		
> 🧮 Third-Party Root Certificat		
> 🧾 Trusted People		
Client Authentication Issue		
Preview Build Roots		
eSIM Certification Authorit		
Homegroup Machine Cert		
Remote Desktop		
Smart Card Trusted Roots		
Trusted Devices		
Mindows Live ID Tokon Ise		>
Personal store contains 1 certificate.		

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

	Select Local Machine
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location © Current User © Local Machine	
To continue, dick Next.	
_	
Next Cancel	
Figure 4: Certificate Import Wizard 1	
 File to Import 	Specify the file you want to import:
Specify the file you want to import.	
File name: WA(CodeStm2015), CLABS, COM(CLabsStm2018);pfx Browse Browse	a file ending
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (PFX, P12) Cryptographic Message Syntax 11 \quarktering (Squark PKCS #7 Certificates (P78) Microsoft Senalzed Certificate Store (LSST)	with .pfx will be installed.
Net Cancel Figure 5: Certificate Import Wizard 2	
← 🐉 Certificate Import Wizard	Enter Password
Private key protection To maintain security, the private key was protected with a password.	
Type the password for the private key.	
Password:	
Display Password	
Import options:	
_ chanse strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
keys at a later time.	
Protect private key using virtualized-based security(Non-exportable) Include all extended properties.	
Next Cancel	
Figure 6: Certificate Import Wizard 3	

 Exertificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept. 	Specify location where certificate is to be stored:
Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Browse	
Nex Cancel	
igure 7: Certificate Import Wizard 4 ← ₽ Certificate Import Wizard	Click on the Finish button.
igure 7: Certificate Import Wizard 4 ←	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.

Certificate	×	Click on Details
General Details Certification P	ath	tab and scroll
Show: <all></all>	~	down to
		Thumborint
Field	Value ^	manisprint
Serial number	00d07cc7379f9427090dbe945	
Signature algorithm	sha256RSA	
Signature hash algorithm	sha256	
Valid from	Sunday, November 12, 2017 5	
Valid to	Wednesday, January 30, 201	
	Edit Properties Copy to File	
	ОК	
Certificate	×	Click on the
Seneral Details Certification	Path	Thumbprint to
Show: <all></all>	~	expose the
Field	Value	hash.
CRL Distribution Points	[1]CRL Distribution Point: Distr	
Authority Information Acc	ess [1]Authority Info Access: Acc	
3 Subject Alternative Name	DNS Name=*.c-labs.com, DNS Digital Signature, Key Encipher	
Basic Constraints	Subject Type=End Entity, Pat	
Thumbprint	da93ddb406bb7f139e42eef30	
Friendly name	CLabsStar v	
1-02111 (0(1) 7(100-	12 (202) (1) ((00-(12/2-	
da93ddb406bb/1139e	42eer307441r696a6d363C	
	I	
	Edit Properties Copy to File	
	ок	
	ОК	
gure 10: Certificate	ок hash exposed	
gure 10: Certificate	hash exposed	
gure 10: Certificate	hash exposed be used in your app.	
gure 10: Certificate opy the hash to ecause some ce	hash exposed be used in your app. rtificates come with blan	nk spaces and
gure 10: Certificate opy the hash to ecause some ce pecial characters	hash exposed be used in your app. rtificates come with blan s, it is recommended:	nk spaces and
gure 10: Certificate opy the hash to ecause some ce pecial characters 1. Paste this	hash exposed be used in your app. rtificates come with blan s, it is recommended: s hash into the Notepad	nk spaces and app,
gure 10: Certificate opy the hash to ecause some ce pecial characters 1. Paste this 2. Remove	hash exposed be used in your app. rtificates come with blan s, it is recommended: s hash into the Notepad all empty spaces and app	nk spaces and app, v special

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