



Tech20210929-1-0

Installing Microsoft IIS & Setting up HTTPS Proxy with a self-signed certificate

Pre-Requisites:

- Cellwatch iBMU with Windows 10 Image
- Internet Connection (For installing IIS extensions and updates) •

Install Internet Information Services (IIS)

Turn on IIS

Windows 10 allows installing version 10 of IIS. This has been tested on iBMU image version 6.0.7 only.



PC name cellwatch-17565

Rename PC

Organization WORKGROUP

Connect to work or school

Edition Windows 10 Enterprise 2016 LTSB 1607

Version





To install IIS, search for "Turn Windows Features on or off".







Go to Internet Information Services and check the boxes for:

Web Management Tools > IIS Management Console

World Wide Web Services.

📷 Windows Features	_		\times
Turn Windows features on or off			?
To turn a feature on, select its check box. To turn a feature off, cle means that only part of the feature is turned on.	ear its check bo	x. A filled I	box
Device Lockdown Hyper-V Internet Explorer 11			^
Internet Information Services FTP Server Web Management Tools			
World Wide Web Services Application Development Features			
Performance Features E Security Internet Information Services Hostable Web Core			
 			
Microsoft Message Queue (MSMQ) Server			~
	OK	Canc	el

Download and install IIS extensions

URL rewrite	https://www.iis.net/downloads/microsoft/url-rewrite
Advanced Request Routing	https://www.iis.net/downloads/microsoft/application-request-
(ARR)	routing





From the Windows Start Button, navigate to "Windows Administrative Tools" and open "Internet Information Services (IIS)"







Click on the name of the server in the **Connections** column on the left. Double click the **Server Certificates** icon.







In the Actions column on the right-hand side, click on Create Self Signed Certificate.

V]	Internet Information Services (IIS) Manager	_ D X
€		🐱 🛛 🟠 🔞 🗸
File View Help		
Connections Start Page Application Pools 	Server Certificates Use this feature to request and manage certificates that the Web server can use with websites configured for SSL. Filte:	Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate View Export Remove Disable Automatic Rebind of Renewed Certificate Rehove Help
Ready		™ ⊒.:





Enter the friendly name you wish to use to identify the certificate, and then click **OK**.

Create Self-Signed Certificate			
Specify Friendly Name			
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:			
Specify a friendly name for the certificate:			
SSL2019			
Select a certificate store for the new certificate: Personal v			
ОК С	ancel		





You now have an IIS Self Signed Certificate, valid for one year, which will be listed under Server Certificates. The common name is the server's name.







How to Bind the Self Signed Certificate

1. Browse to the connections column on the left-hand side, expand the sites folder and click on the website you wish to bind the SSL certificate to. Once you have done that, on the right-hand side, click on **Bindings** in the Actions column.



2. Click the Add. button.

			Site	Bindings	? X
Type http	Host Name	Port 80	IP Address *	Binding Informa	Add Edit Remove Browse
					Close





Add Site Binding	? ×
Type: https V All Unassigned Host name: Require Server Name Indication	Port: ✓ 443
SSL certificate: SSL2019 v	Select View OK Cancel

4. You should now see the bindings for port 443. You can now on click **Close**.

			Site	Bindings	? X
Type http https	Host Name	Port 80 443	IP Address *	Binding Informa	Add Edit Remove Browse
					Close





Configure HTTPS Redirect & Reverse Proxy Rules

HTTPS Redirect

From **Default Website Home**, select the URL Rewrite Extension

NOTE: If this extension is not visible, verify you installed it during the IIS Extension installation section in the first steps of these instructions.

Image: CallWATCH-9270 + Site + Default Web Site + Image: CallWATCH-9270 (CLUART) Image: CallWATCH-9270 (CLUART) <	Sinternet Information Services (IIS) Manager	- 🗆 ×
File View Help Connections Image: Default Web Site Home Image: Default Web Site	← → ● ◆ CELLWATCH-9270 → Sites → Default Web Site →	📴 🐼 🚱 •
Connections Image: Configure: Status: Image: Configure: Image: Configure: <t< td=""><td>File View Help</td><td></td></t<>	File View Help	
neauy 1	Configuration Config	sctions Staplore Edit Strice Bindings Basic Settings View Applications View Applications View Applications Start Start Browse Website Browse Vebsite Browse 7:443 (https) Advanced Settings Configure Limits Pleip

Under the Actions side-bar, choose to "Add Rule(s)..."

Internet Information Services (IIS) Ma	nager	-		\times
← → € · CELLWATCH-17565	→ Sites → Default Web Site →		2 🔤 🟠	10-
File View Help				
Connections	URL Rewrite	Actions Add Rule(s)		
Application Pools Sites See Default Web Site	Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response. Inbound rules that are applied to the requested URL address:	Revert to Pan Manage Serv View Server V	ent ver Variabl /ariables	les

Select a rule template: Under the "Inbound rules" section choose to create a "Blank rule





The rule settings for the HTTPS Redirect should be as follows:

- Name "HTTPS Redirect"
- Match URL
 - Requested URL Matches the Pattern
 - Using Regular Expressions
 - Pattern: (.*)
 - Ignore Case Box should be checked
- Conditions
 - o Logical Grouping: Match All
 - Add a condition
 - Condition Input: {HTTPS}
 - Check if input string: Matches he Pattern
 - Pattern: ^OFF\$
 - Ignore case Box should be checked
- Track capture groups across conditions Box should be blank
- Server Variables None
- Action
 - Action Type: Redirect
 - Action Properties
 - Redirect URL: <u>https://{HTTP_HOST}{REQUEST_URL}</u>
 - Append query string Box should be blank
 - Redirect type: Permanent (301)

Once you have completed the rule it should look like the following in the URL Rewrite list:

URL Rewrite						
Provides rewriting capabilities	Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.					
	a to the requested one address.					
Name	Input	Match	Pattern			
🗆 💕 HTTPS Redirect	URL path after '/'	Matches	(.*)			
	{HTTPS}	Matches the Pattern	^OFF\$			
1 _				1		





Reverse Proxy Rule

Under the Action menu, add another rule.

This time under the "Inbound and Outbound Rules" section, pick "Reverse Proxy"

Add Rule(s)		? ×
Select a rule template:		
Inbound rules Blank rule Request blocking	滤 Rule with rewrite map	
User-friendly URL	👰 Reverse Proxy	

- Inbound Rules
 - Enter Server name or the IP address where the HTTP requests will be forwarded:
 /localhost:8080/
 - Enable SSL Offloading Box should be checked

Add Reverse Proxy Rules	?	×
Inbound Rules Enter the server name or the IP address where HTTP requests will be forwarded: /localhost:8080/		
Example: contentserver1		
☑ Enable SSL Offloading		
Selecting this option will forward all HTTPS requests over HTTP.		
Outbound Rules		
Rewrite the domain names of the links in HTTP responses		
Responses that are generated by applications that are behind a reverse proxy HTTP links that use internal domain names. These links must be updated to u domain names. From:	can have ise external	
Example: contentserver1		
То:		
Example: www.contoso.com	~	
ОК	Cancel	





Changing the Cellwatch Port

IIS uses Port 80 by default for HTTP and Port 443 for HTTPS. Cellwatch communicates on Port 80 by default as well, to avoid conflicts we will change

Stopping the Cellwatch Service

Search the Windows Start Menu for "Services"



From the list of services, locate the Cellwatch Service. (Sort names alphabetically if this is not done already)

Right click on the Cellwatch service to choose to "Stop" the service

Do not close the Services windows, as you will need to restart the service once changes have been made to the .ini file.





Modifying the .INI File

Once the service has stopped, go to the Desktop and locate the "Shortcut to Cellwatch" folder. Double-Click to open.

Open the "cellwatch.ini' file. This should open in Notepad.

Scroll down to the [HTTP] section to the "Port" entry. Change the port number to 8080

cellwatch.ini - Notepad File Edit Format View Help [Program settings] Language=1 Auto start=1 Minutes into day for scan=0 Audible alarm=0 Resistance sensitivity=0 Voltage sensitivity=5 Minimum length of discharge (in Secs.)=5 Interval to check on voltage alarmed cells (in Mins.)=10 Time limit to check on voltage alarmed cells (in Mins.)=60 Number of temperatures to average=10 Degrees for temperature alarm Hysteresis (x0.1, e.g. Enter 7 for 0. Display Temperature in C=1 Ripple hysteresis(V)=0.000 Days of daily data to keep=30 [Modbus] Enabled=0 System Unit ID=1 WriteEnabled=0 [HTTP] Enabled=1 Authorization needed=0 System page refresh period=10 Battery page refresh period=10 String page refresh period=60 Info page refresh period=10 Maximum log file count=0 Maximum discharge file count=50 Port=8080 [Scan frequency settings] Voltage=1 Resistance=24 [AppServer] Host=localhost Port=211 Enabled=1 Prefix=CW

Save the close the cellwatch.ini file.

Re-open the Services windows and Start the Cellwatch Service.





Testing

Once all settings have been modified, open the Cellwatch GUI and verify that it is connected to the Cellwatch Service. (You do not need to have Cellwatch scanning, but it does need to be connected the service)

Open Internet Explorer from the IBMU Desktop.

You will be prompted with a security message from Internet Explorer due to the Self-signed Certificate.

Click "Continue to this website (not recommended)" to proceed to the Cellwatch webpage interface.



If everything was done correctly, the webpage URL should be: <u>https://localhost/</u>. Internet Explorer will report a Certificate Error, as this is a self-signed certificate not one issued by a certificate authority (CA).







If the solution does not work, it may be due to the Server or the Default Website itself not being enabled. They can be enabled by following the below steps in the pictures:



File View Help				
Connections		CEL	LWATCH	I-6313 Hor
CELLWATCH-6313	(CELLWATC	~		
- Applicatio	Refresh			• 🦉 Go - 🐙
✓ - i Sites Of the second	Add Website	e		A
> 🗊 Server Far 🕨	Start			¥2
	Stop		uthentic	Compression
	Rename		2	-
	Switch to Co	ontent View		
		Caching	Request Filtering	Server l Certificates
		Managemen	t	
				ý=
		Configurat	Feature	Shared
		Editor	Delegation	Configurat

Default Website - Start

Connections		😜 De	fault W	eb Si	te Hor	ne
CELLWATCH-631	3 (CEL ools	LWATC Filter:	<u>_</u>	• 9	<u>G</u> o - (Show All
Server Farms	à	Explore Edit Permissions		ion D	on Default Directo	Directory
		Add Application Add Virtual Directory		ttings URL Rewrite		
		Edit Bindings				
		Manage Website	• 2	Resta	art	
	-	<u>R</u> efresh Remove Rename		Start		
	×			Stop		
				Brow	se	
		Switch to Content View		Advanced Sett		ings