

Raytec HTTPS Setup Guide $_{_{V1}}$

Raytec Global (excluding Americas)

Tel: +44 (0) 01670 520055 Fax: +44 (0)1670 819760 sales@rayteccctv.com

Raytec Americas:

Tel: +1 613 270 9990 Toll Free: +1 888 505 8335 ussales@rayteccctv.com

www.rayteccctv.com

Contents

Introduction	. 3
Firmware change	.4
DiscoMan Change	.6
Managing Computer Certificates	. 8

Raytec Global (excluding Americas)

Tel: +44 (0) 01670 520055 Fax: +44 (0)1670 819760 sales@rayteccctv.com

Raytec Americas:

Introduction

The latest Raytec lamps now have HTTPS functionality (using encryption algorithm ECDSA with 256bit private keys). It is now possible to upload a security certificate to lamps to enable a secure connection.

This document will show the changes you will see to firmware, software and also how to ensure that your browser doesn't throw warnings when trying to access your lamps over a secure connection.

Raytec Global (excluding Americas)

Tel: +44 (0) 01670 520055 Fax: +44 (0)1670 819760 sales@rayteccctv.com

Raytec Americas:

Firmware change

To benefit from the HTTPS functionality, your lamp needs to be running one of the below firmware versions or newer.

Lamp Type	Firmware revision
Single wavelength lamps – 4,6 and 8 size	v2.7.1 and above
Single wavelength lamps – 16 size	v6.2.0 and above
Hybrid lamps – 4,6 and 8 size	v3.6.9 and above
Hybrid lamps – 16 size	v7.2.0 and above

If you attempt to navigate to a lamp running one of these firmware versions (or newer) prior to uploading a certificate, you will likely be presented with trust errors from your browser like below.

Your connection is not private							
Attackers might be trying to steal your information from 192.168.0.100 (passwords, messages, or credit cards). <u>Learn more</u>	for example,						
NET::ERR_CERT_AUTHORITY_INVALID							
Q To get Chrome's highest level of security, <u>turn on enhanced protection</u>							
Hide advanced	Back to safety						
This server could not prove that it is 192.168.0.100 ; its security certificate your computer's operating system. This may be caused by a misconfigura attacker intercepting your connection.	is not trusted by tion or an						
Proceed to 192.168.0.100 (unsafe)							

The updated firmware has a self-signed certificate which should be changed at the earliest opportunity. The reason for the browser error is that the certificate is generated from within Raytec and there is no chain of trust like with other certificates and as such the browser (rightfully) states that this connection could be problematic.

sales@rayteccctv.com

Raytec Americas:

The updated firmware adds a new web page to the lamp web interface called "Certificate Upload", on clicking this option you will see the following:

raytec"									
Var2-IP-i6 / VARIO2	21P Raytec Vario2 IP Light Controller								
Home	TLS Certificate Upload								
Settings/Groups	This page allows the TLS certificate of the lamp to be updated.								
Adv. Settings	To upload a TLS certificate, choose files below:								
Access	Certificate: Choose File No file chosen								
Network	Private key: Choose File No file chosen								
System Information	Upload New Certificate								
Diagnostics									
Adv. Diagnostics									
Software Update									
Certificate Upload									
Log Off									

To enable secure communications you must upload certificate and private key files in .der format. This format has been chosen to minimise the size of the file to upload.

Warning: Raytec have opted to use ECDSA encryption with 256-bit private keys. Ensure that your files comply with this or you will encounter issues on upload and/or when attempting to access the lamp using HTTPS.

Certificate and private key files will not always be in .der format when you have them therefore some conversion tool will be required to convert the files to .der format to enable you to upload them to the lamp.

Raytec have made changes to DiscoMan to make this whole process a lot easier for users.

Fax: +44 (0)1670 819760

sales@rayteccctv.com

Raytec Americas:

DiscoMan Change (v2)

After the update to the firmware, some questions that came out of the initial testing phase were:

- How do I generate the certificate and private key files?
- How do I convert these files to .der format?
- How do I know when a certificate is due to expire?

All of these questions have been addressed by the latest DiscoMan update. On selecting a lamp in DiscoMan, click the Certificates button.

() Certificate				×
Current Lamp I	nfo			
Name:	VARIO2IP			
IP Address:	192.168.0.100			
MAC Address:	D8:80:39:BD:33:CE			
Certificates				
Certificate Validity (D	ays):		365	\$
 Generate Root Cer 	tificate Authority (CA)			
Generate a root ce certificates for you	ertificate authority to sign ır lamps.	[Generate	
Ensure you export lamp certificate ge	your certificate for future eneration	[Export	
O Import Root Certif	icate Authority (CA)			
Import certificate from an existing r sign certificates fo Ensure your root (and private key (.der format) pot certificate authority to r your lamps. CA uses 256-bit ECDSA		Import	
			OK	Cancel

DiscoMan presents users with two options to secure their lamps:

• Generate Root Certificate Authority (CA)

If the user doesn't have a CA with which they can generate certificates then they can become their own via DiscoMan.

DiscoMan asks the user to select how long certificates should be valid and then the user can generate and export the root CA and private key before clicking OK to upload the certificate and private key to the lamp.

The exported certificate and private key can be re-imported (using the import feature) to create certificates for other lamps.

Raytec Americas:

• Import Root Certificate Authority (CA)

The user can also choose to import a certificate and private key from an existing CA if they wish. The files must be in .der format for upload.

This may be useful in the scenario where the user has a root CA that they use to sign certificates for all network devices and therefore they already have the chain of trust established and the certificate installed in the trusted root certificate store of all machines that require access to the secure devices.

Warning: Raytec have opted to use ECDSA encryption with 256-bit private keys. Ensure that your files comply with this or you will encounter issues on upload and/or when attempting to access the lamp using HTTPS.

If the user selects multiple lamps and clicks "Certificates" then they can update the certificate and private key of multiple lamps at once.

If you imported a CA, the lamp will now be accessible over HTTPS. If you click "Refresh", you will now see an expiry date in the lamp's status message column in DiscoMan.

Status Message
HTTPS Certificate Expires 13/01/2024

If you generated a new CA then you'll need to install the generated certificate in the trusted root certificate store of all machines that will need to access the lamp over HTTPS. See the next section for instructions on how to do this.

Fax: +44 (0)1670 819760

sales@rayteccctv.com

Raytec Americas:

Managing Computer Certificates

After generating your own CA and exporting the resulting certificate and private key files, you need to install the Certificate.der file into the trusted root certificate store on all machines that require secure access the lamp. Follow the steps below for each machine to do this.

1. Double-click the certificate.der file in the directory where you exported it to. You should see the following. Click "Install Certificate..."

8	Certificate	×							
G	eneral Details Certification Path								
	Certificate Information								
	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.								
	Issued to: Raytec Lamp CA								
	Issued by: Raytec Lamp CA								
	Valid from 22/02/2023 to 23/04/2023								
	Install Certificate								
	ОК								

2. You will be presented with the first page of the Certificate Import Wizard, select "Local Machine" and click "Next"

This wizard helps you copy certificates, (certificate trust lists, and certificate revocation
ists nom your disk to a certificate store.	
A certificate, which is issued by a certific and contains information used to protect connections. A certificate store is the sy	cation authority, is a confirmation of your identit t data or to establish secure network rstem area where certificates are kept.
Store Location	
Current User	
To continue, click Next.	

Raytec Global (excluding Americas) Tel: +44 (0) 01670 520055 Fax: +44 (0)1670 819760 sales@rayteccctv.com

Raytec Americas:

3. Select "Place all certificates in the following store", select "Browse..." and select *Trusted Root Certification Authorities.*

←	🐉 Certificate Import Wizard	×
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	\bigcirc Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Certificate store:	
	Browse	
	<u>N</u> ext Can	cel



4. Click "Next" and on the last page click "Finish".

Tel: +44 (0) 01670 520055 Fax: +44 (0)1670 819760

sales@rayteccctv.com

Raytec Americas:

5. You can now communicate with the lamp(s) using HTTPS and DiscoMan will now display the expiry date of the HTTPS certificate in the Status Messages column.

Ģ	Raytec	DiscoMan	ı									- 0	×
	R efr) esh		Addressing	₽ <u>N</u> aming	2	හි Config	Certifie	cates	ି ^{ମ୍ୟୁ} Cr <u>e</u> dentials	Firmware Upload Access	(i) A <u>b</u> out	
	State	On/Off	Access	MAC	IP Address	Name	Group	Firmware	Model	Uptime	Status Message	•	^
	0			D8:80:39:BD:33:F1	192.168.1.74	SHOPF07	Shopfloor	2.7.1	Var2-IP-i6	05:36:21	HTTPS Certificate Expires 13/01/2024		
	0			D8:80:39:2E:0F:F4	192.168.2.90	RAYTEC1	TechnicalDe	2.7.1	Var2-IP-i6	00:13:36	HTTPS Certificate Expires 13/01/2024		
	0		\bigcirc	D8:80:39:BD:12:7F	192.168.1.137	SHOPF10	Shopfloor	2.7.1	Var2-IP-i6	05:36:49	HTTPS Certificate Expires 13/01/2024		
	0			D8:80:39:BD:33:B5	192.168.1.65	SHOPF04	Shopfloor	2.7.1	Var2-IP-i6	05:36:50	HTTPS Certificate Expires 13/01/2024		
	0			D8:80:39:BD:32:E2	192.168.1.127	SHOPF09	Shopfloor	2.7.1	Var2-IP-i6	05:37:18	HTTPS Certificate Expires 13/01/2024		
	0			D8:80:39:BD:33:BB	192.168.2.93	RAYTEC4	TechnicalDe	2.7.1	Var2-IP-i6	01:30:22	HTTPS Certificate Expires 13/01/2024		
	0			D8:80:39:BD:10:7C	192.168.1.75	SHOPF08	Shopfloor	2.7.1	Var2-IP-i6	05:37:03	HTTPS Certificate Expires 13/01/2024		
	0			D8:80:39:BD:10:E7	192.168.1.62	SHOPF03	Shopfloor	2.7.1	Var2-IP-i6	05:36:39	HTTPS Certificate Expires 13/01/2024		
•	0	Θ	0	D8:80:39:BD:10:44	192.168.1.68	SHOPF05	Shopfloor	2.7.1	Var2-IP-i6	05:36:48	HTTPS Certificate Expires 13/01/2024		
	-	-	-										Υ,

Raytec Global (excluding Americas)

Tel: +44 (0) 01670 520055 Fax: +44 (0)1670 819760 sales@rayteccctv.com

Raytec Americas: