# How to configure OpenVPN in Vigor Router using XCA certificate and key management.

#### I. Create local certificate in the Vigor Router.

1.1 Since the certificate has a valid period, please make sure the time settings of the router is correct, by going to **System Maintenance >> Time and Date**.

nformation			
Current System Time	2019 Sep	9 Mon 9 : 58 : 42	Inquire Time
Setup			
Use Browser Time			
Use Internet Time			
Time Server		pool.ntp.org	
Priority		Auto 💌	
Time Zone		(GMT) Greenwich Mean	Time : Dublin 🔹
Enable Daylight Savi	ng	Advanced	
Automatically Update	Interval	30 mins <b>▼</b>	
	rough	Auto	

Cancel

OK

1.2 To generate a new certificate, go to **Certificate Management>>Local Certificate**. Type the information below and select Key size as **2048** *Bit* and Algorithm as **SHA-256** and then click **Generate**.

Certificate Name	openvpn	
Cubbert Alternative News		
Subject Alternative Name	F-Mail V	
E-Mail	support@i-lan.com.au	
L. Hall	supporternation	-
Subject Name		
Country (C)	AU	
State (ST)	NSW	
Location (L)	Sydney	
Organization (O)	i-lan	
Organization Unit (OU)	support	
Common Name (CN)	support@i-lan.com.au	
Email (E)	george@i-lan.com.au	
Кеу Туре	RSA *	
Key Size	2048 Bit 🔻	
Algorithm	SHA-256 🔻	

1.3 After generating, you will see the Certificate Signing Status as *Requesting*, which needs to be signed by a CA. Click *View* and highlight the content inside the **PEM Format Content** and then right-click and select copy.

Certificate Management >> Local Certificate	
Certificate management - Local Certificate	

X509 Local Certificate Configuration

Name	Subject	Status	M	odify
openvpn	/C=AU/ST=NSW/L=Sydney/O=i-la	Requesting	Sign Vie	w Delete
100-000		1000	View	Delete
			View	Delete

REFRESH

Note:

- Please setup the "System Maintenance >> <u>Time and Date</u>" correctly before signing the local certificate.
- 2. The Time Zone MUST be setup correctly!!

GENERATE IMPORT

Certificate Signing Request Informat	tion - Google Chrome				×
) Not secure   192.168.150.1/c	loc/xlocfvi1.htm				
	Certificate Signing Requ	est Information			
Certificate Name :	openvpn				
Issuer :					
Subject :	C=AU, ST=NSW, L=Sydne lan.com.au, emailAddress=	y, O=i-lan, OU=support, CN= support@i-lan.com.au	support@i-		
Subject Alternative Na	me : email:george@i-lan.com.a	iu			
Valid From :					
Valid To :					
PEM Format Content .	Dy fdM77Ngh/EdtfyrMn6EBtyZ( NC MWVrv3vymhALzh0rQs1U// o5 GrmkNid/X1mdsr4kvZTSLy eG IGWm6XQjkDBxoLhf1bR7WP 7e GKrqBfQ/f409cuzYgazKjW END CERTIFICATE R	29w70XPhfcUsFZ2EBTttBoX0G3oJ Emoji Cut Copy Paste	oSNZt713/60		
		Paste as plain text Select all			(
	Close	Search Google for "BEGIN CE Print	RTIFICATE REQ	UEST	"
		Spell check Writing Direction			
		Inspect			

#### II. Create a new CA using XCA.

2.1 Launch XCA, go to File and click New Database.



← → ~ ↑ □ → User → Desktop → Victor-certificate       Organize ▼     New folder       ✓ Quick access     ●       □ Desktop     ✓	ed Type Size	, , (
Organize ▼ New folder	ed Type Size	- (
A Name     Date modifie     Desktop	ed Type Size	
<ul> <li>Documents *</li> <li>Downloads *</li> <li>Pictures *</li> <li>How to configur</li> <li>John.North</li> <li>OpenVPN</li> <li>Video</li> <li>OneDrive</li> <li>This PC</li> </ul>	ems match your search.	
Network Y		
File name: XCA.xdb Save as type: XCA Databases (*.xdb )		

2.2 Name your database as e.g XCA.xdb and click *save*.

2.3 Go to the *Certificates tab*, click *New Certificate*. Select *Create a self-signed Certificate with the serial*. Click *Apply all* to apply the CA Template.

nternal name	commonName	CA Ser	ial Expiry date	CRL Expiration		New Certificate
er x	Certificate and Key ma	nagement		?	×	Export
Cre	ate x509 Certif	cate		J	1	Import
Sou	rce Subject Exten	tions Key usage	Netscape Advance	ed		Show Details
Sig	ning request					Delete
	Sign this Certificate sign	ng request				Import PKCS#12
2	Copy extensions from the	request	5	how regiont		Import PKCS#7
	Modify subject of the req	uest				Plain View
Si	ning					
	Create a self signed certi	ficate with the serial	1			
100	vise any certificate for s	fan di				
Sigr	ature algorithm		SHA 256		2000 175	
Te	mplate for the new certific	ate				
15	lefault] CA			1.4	•	
			Apply extensions	Apply subject Apply	all	
						5

# 2.4 Go to the *Extensions tab* and select type as *Certificate Authority*.

Source Su	biect Extension	s Key usage	Netscape	Advanced		
X509v3 Basic	: Constraints		1 ////////			Key identifier
Type	Certification Autho	rity			•	Subject Key Identifier
Path length					Critical	Authority Key Identifier
					1	
Validity Not before		2019-09-09 00:	26 GMT V	Time range		Years  Apply
Validity Not before Not after		2019-09-09 00: 2020-09-06 04:	26 GMT 🗸	Time range	Local time	Years  Apply No well-defined expiration
Validity Not before Not after 509v3 Subject	:t Alternative Name	2019-09-09 00: 2020-09-06 04:	26 GMT 🗸	Time range	Local time	Years  Apply No well-defined expiration Edit
Validity Not before Not after 509v3 Subjec	t Alternative Name	2019-09-09 00: 2020-09-06 04:	26 GMT ~ 07 GMT ~	Time range	Local time	Years  Apply Apply No well-defined expiration Edit Edit Edit
Validity Not before Not after 509v3 Subject 509v3 Issuer 509v3 CRL Di	t Alternative Name Alternative Name istribution Points	2019-09-09 00: 2020-09-06 04:	26 GMT ~ 07 GMT ~	Time range	Local time	Years Apply No well-defined expiration Edit Edit Edit Edit

2.5 Go to the Subject tab.

- Enter certificate information under *Distinguished name*, then click *Generate a new key*.
- Select "RSA" for Keytype and "2048 bit" for Keysize, then click *Create*.
- Click **OK** to generate the CA Certificate. Now we have the Trusted CA Certificate to sign the server certificate and client certificate.

xurce Distinguish	Subject red name	Extensions	Key usage	Netscape Advance	ced	
Internal na	ame	CAtest		organizationName		
countryNa	me	TW		organizationalUnitNar	ne	
stateOrPro	winceNar	ne		commonName	Root	
X Certif	ficate ar	nd Key manage	- ?	× ddress ent	root@ca.ne	t Add
X Certil lew ke case give s ysize ley proper	ficate ar <b>&gt;y</b> a name to ties	nd Key manage	select the des	ired ddress	root@ca.ne	t Add Delete
X Certil lew ke case give size key proper Name	ficate ar <b>Ey</b> a name to ties CAtest	nd Key manage	select the des	ddress ent ired	root@ca.ne	t Add Delete
X Certil lew ke vase give vsize cey proper Name Keytype	ficate ar <b>y</b> a name to ties CAtest RSA	nd Key manage	select the des	× ddress ent ired	root@ca.ne	t Add Delete

#### III. Importing Signed Server Certificate and CA Certificate to the Router.

3.1 Go to *Certificate signing requests*, right-click and select *Paste PEM data* and paste the PEM Format Content copied from the Vigor router in procedure 1.3. and then click *Import All*.



3.2 Right-click on the imported certificate and select **Sign**. Use the CA created in procedure 2 to sign the imported certificate and then click **OK**.

Private Keys Certificate signing requests (	Certificates Templates	Revocat		
Internaî name commonNa 118.166.188.111 118.166.189	me Signed New Import Paste PEM data Rename Delete Export • Transform • Sign Columns •	<ul> <li>✓ X Certificate and Key management</li> <li>Create x509 Certificate</li> <li>Source Extensions Key usage Netscap</li> <li>Signing request</li> <li>Sign this Certificate signing request</li> <li>Copy extensions from the request</li> <li>Modify subject of the request</li> <li>Signing</li> <li>Create a self signed certificate with the serial</li> <li>O the this Certificate for signing</li> <li>Signature algorithm</li> <li>Template for the new certificate</li> <li>[default] CA</li> </ul>	e Advanced 118,196,188,111 Show request CAtest SHA 256 Apply extensions Apply subject OK	? ×

3.3 Under Certificate tab, export the Singed Local Certificate as .crt format. Go back to the Vigor router's GUI and import it to the Vigor router by going to Certificate Management >> Local Certificate >>Import

vivate Keys Certificate si	gning requests Certificates Templates Revocati	ont lists			
Internal name	commonName CA Serial Root Ven 01:	Expiry date CRL I 1028-07-31	Expiration	New Certificate	
A 118.166.189	.189.111 118.166.188.111 02 2019-07-31			Export	
	Sectificate and Key management	7 ×		Import	
	Certificate export	A===		Show Details	
	Name [118,166,188,111			Delete	
	Flename [D:/User/Desktop/118.06.188.111.ett			Import PKCS#12	
	MENT These former with here has			Import PKCS#7	
	Fibe lex forme with sealers Equ	rt Format		Plain View	
			Certifica	te Management >	> Local Certificate
		K Carel			
	-		Import X	509 Local Certifi	cate
			Upicad	Select a	local certificate file.
				Certi	ficate file: 選擇權案 118.166.188.111.crt
				Click Im	port to upload the local certificate.
				Import	Cancel
			1 1000 100	STATISTICS NO.	
			Unload	PKCS12 Certifica	fe

3.4 Make sure that the status of the certificate imported is **OK**.

ertificate Management >> Local Certificate
ertificate Management >> Local Certificate

#### X509 Local Certificate Configuration

Name	Subject	Status	Mo	odify
openvpn	/C=AU/ST=NSW/L=Sydney/O=ilan	ок	View	Delete
12423	22229		View	Delete
			View	Delete

Note:

- 1. Please setup the "System Maintenance >> <u>Time and Date</u>" correctly before signing the local certificate.
- 2. The Time Zone MUST be setup correctly!!

GENERATE	IMPORT	REFRESH
----------	--------	---------

3.5 In XCA, go to *Certificate*, choose the CA certificate and export it as *.crt* format, and then import the CA certificate to the Vigor router, by going to Certificate Management >> Trusted CA Certificate.

Internal name	commonName CA Serial Expiry date CRL Expiration	New Certificate
CAtest Ar 118.166.188.11	Root         ✓ Yes         01 2028-07-31           1 118.166.188.111         02 2019-07-31	Export
	(	Import
	X Certificate and Key management     ?     X	Show Details
	Certificate export	Delete
	Name CAtest	Impert PKCS#12
	Filename [Dr/l/ser/Desktop/CAtest.crt []	Import PKCS#7
	PEM Text format with headers Export Format PEM (2 crt)	Plain Vicw
	Cert	ificate Management >> Trusted CA Certificate
	OK Cancel Imp	ort X509 Trusted CA Certificate
		Select a trusted CA certificate file.

#### 3.6 Make sure that the status of the Trusted CA imported is **OK**.

Certificate Management >	> Trusted CA	Certificate
--------------------------	--------------	-------------

#### X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Root CA			Create
Trusted CA-1	/C=AU/ST=NSW/L=SevenHills/O=	ОК	View Delete
Trusted CA-2			View Delete
Trusted CA-3	(1994)	(4,44)	View Delete

Note:

- 1. Please setup the "System Maintenance >> <u>Time and Date</u>" correctly before you try to generate a RootCA!!
- 2. The Time Zone MUST be setup correctly !!

IMDODT	DEEDEOU
IMPORT	REFRESH

#### IV. Making a Private Certificate and Private Key for VPN Client.

# 4.1 In XCA, go to **Certificates**, click **New Certificate**. Under *Signing*, select *Use this Certificate for singing*.

Internal nar	X Certificate and Key management	2	X	Nam Castification
Atest (Atest 118.166	Create x509 Certificate			Export
	Source Subject Extensions Key usage	Netscape Advanced		Import
	Signing request			Show Details
	Sign this Certificate signing request	118.166.188.111	12	Delete
	Copy extensions from the request	Show request	ļ	Import PKCS#12
	Modify subject of the request			Import PKCS#7
	Signing			Plain View
	Create a self signed certificate with the serial			
	Use this Certificate for signing	CAtest	•	
	Signature algorithm	SHA 256	٠	
	Template for the new certificate			
	[default] CA		•	
		Apply extensions Apply subject Apply	all	

4.2 Go to the Subject tab.

- Enter certificate information under *Distinguished name*, then click *Generate a new key*. Select *"RSA"* for Keytype and *"2048 bit"* for Keysize, then click *Create*.
- Click *OK* to generate the certificate.

ivate Keys Certific	cate signing requests (	Certificates Templates	Revocation lists		
Internal nar	I Certificate and )	Key management		? ×	New Certificate
A 118.166	Create x509 C	Certificate		A	Export
	Source Subject	Extensions Key usa;	ge Netscape Advance	ed	Import
	Distinguished name				Show Details
	Internal name	Oclient	organizationName		Delete
	stateOrProvinceName	e Iw	commonName	Oclient	Import PKCS#12
	localityName		emailAddress		Import PKCS#7
	S Certificate	and Key manage	? × t	Add	Plain View
	New key			Delete	
	Please give a name keysize Key properties	to the new key and select	the desired		
	Name Oclier Keytype RSA Keysize 2048 t	bit		d keys too Generate a new key	
	Remember as d	lefault		OK Control	

4.3 Go to *Certificates*; select the certificate we just created. Export it as *.crt* format.

Private Keys Certificate sign	ting requests Certificates Templates Revocation lists		
Internal name	commonName CA Serial Expiry date	CRL Expiration	New Certificate
A CAtest A 118.166.188.	Root √Yes 01 2028-07-31 111 118.166.188.111 02 2019-07-31		Export
Ar Oclient	Oclient 03 2019-07-31		Import
	The contract of the second sec	×	ingen
	11.0 CONT. 2018.00 CONTROL 10 C		Show Details
	Certificate export		Delete
	Name Oclient		Import PKCS#12
	Filename D:/User/Desktop/Oclient.crt		Import PKCS#7
	PEM Text format with headers		Plain View
	Export Pormat		

4.4 Go to *Private Keys*, export the Private Key (*Oclient.key*), and manually change extension name to *.key* and then click *Ok*.

ivate keys Certificate	signing requests Certificates Templates Revocation lists	
Internal name 1 CAtest RSI Oclient RSI	ype Size Use Password 2048 bit 1 Common 2048 bit 1 Common	New Key
- content int	X Certificate and Key management ? ×	Import
	Export private key [RSA]	Import PFX (PKCS#1
	Name Oclient	Show Details
	Filename [D:/User/Desktor Oclient.key]	Delete
	Unencrypted private key in text format Export Format PEM private (*,pem)	

#### V. Setup the Vigor router as OpenVPN Server.

VPN and Remote Access >> OpenVPN

5.1 Go to VPN and Remote Access >> OpenVPN, General Setup, and follow the settings below.

General Setup	lient Config	
Enable UDP		
UDP Port	1194	
Enable TCP		
TCP Port	1194	
Cipher Algorithm	AES128 V	
HMAC Algorithm	SHA1 •	
Certificate Authentication		

2

Note: OpenVPN on vigor only support TUN device interface currently. So please setup corresponding configurations on the client side.

	1	3	K	1	
	2	~		۰.	

5.2 Go to the *Client Config* tab, specify the file name of **CA Certificate**, **Client Certificate**, and **Client Key** and then click **Export**. Please make sure that your WAN is up before exporting .ovpn file.

PN and Remote Acces	s >> OpenVPN		2
General Setup	Client Config		
Rem <mark>ote</mark> Server	IP WAN1 124.169.	18.18( 🔻 🔍 Domain	
Transport Protocol	TCP	•	
File Name	openvpn	.ovpn	
CA cert Client cert	CAtest Oclient	.crt .crt	
Client key	Oclient	.key	
Note:			
Please make sure the	CA files are located in the	same folder with .ovpn file.	

5.3 Go to VPN and Remote Access >> Remote Dial-in User and create user profiles for OpenVPN Dial-in users. Select Enable this account, enter Username/Password, and select OpenVPN Tunnel under Allowed Dial-In Type.

User account and Authen	tication		Username	OVPNuser			
Enable this account			Password				
Idle Timeout	0	second(s)					
Allowed Dial-In Type			PIN Code				
PPTP							
<ul><li>IPsec Tunnel</li><li>IPsec XAuth</li></ul>			IKE Authentication Met	hod			
L2TP with IPsec Pol	icy None	*	IKE Pre-Shared Key	Max: 64 characters			
SSL Tunnel			Digital Signature()	K.509)			
OpenVPN Tunnel			None 🔻				
IKEv2 EAP							
Specify Remote Nod Remote Client IP	e		Medium(AH) High(ESP) DES	3DES 🖉 AES			
or Peer ID			Local ID (optional)				
Netbios Naming Packet	Pass	Block					
Multicast via VPN	Pass	Block					

VPN and Remote Access >> Remote Dial-in User

5.4 Go to **SSL VPN >> General Setup** to change the Server Certificate to the Local Certificate that we generated in procedure 2.

#### SSL VPN >> General Setup

Bind to WAN	WAN1	🗹 WAN2 🗹 WAN3 🗹 WAN4	
Port	443	(Default: 443)	

### VI. OpenVPN Client setup.

- 6.1 To import the openvpn.ovpn file to the OpenVPN client. Right click the OpenVPN icon, which is located on the bottom right of your taskbar. There are three files to put inside the OpenVPN config folder:
- Trusted CA Certificate (CAtest.crt)
- Private Certificate (Oclient.crt)
- Private Key (Oclient.key)



🕜 OpenVPN - S	Settings	$\times$
General Proxy	Advanced About	
Configuration	Files	
Folder: Extension:	C:\Users\User\OpenVPN\config	
Log Files Folder:	C:\Users\User\OpenVPN\log	
Script Timeou Preconnect	rt script timeout: 10	
Connect scr	ript timeout: 30	
Disconnect	s openvpn >	
	openvpn1 > 🔍 💆	
	Import file	¥
	Settings	H
	Exit	

Pine Home Share View	Move Copy to + to +	Delete Rename	New item •	Properties	Select a
Clipboard	Orgar	iize	New	Open	Sele
← → ∽ ↑ 🔄 > User > OpenVPN	> config > openvp	n			~ Ū
^ Name	^	Dat	te modified T	ype Size	-
A Quick access		6/0	0/2010 2-26 DM S	acurity Cartificata	2 40
Desktop 🖈 🖾 Oclient cr	6 •	6/0	0/2019 2:20 PIM 5	ecurity Certificate	2 KB
📋 Documents 🖈 📄 Oclient ke	с А/	6/0	0/2019 2:27 PM 5	EV File	2 KB
Downloads * O openypp	y nynn	6/0	9/2019 4:53 PM	)nenVPN Config	1 KB
Pictures	stptt -	3, 5	5/2015 455 FM	pentri i comgin	1102
How to configur					
lohn North					
OpenVPN					
Video 1					

6.2 Click **Connect** and enter username/password configured in procedure 5.3.



Tue Jul 31 17:29:54 201	8 OpenVPN 2.4.6 x86_	64-w64-mingw32 [SSL (OpenSSL)	)] [LZO] [LZ4] [Pk	CS11][AEAD
Tue Jul 31 17:29:54 201	8 Windows version 6.2	(Windows 8 or greater) 64bit		
Tue Jul 31 17:29:54 201	8 libraryuneione. Opor	×	0	
	Username:	OVPNuser		
	Password:	•••••		
	Save pass	word		
	ОК	Cancel		
	_			>
٢				

6.3 After establishing the OpenVPN tunnel, go to VPN and Remote Access >> Connection Management in the Vigor router to verify the connection.

## VPN and Remote Access >> Connection Management

	0.000	
General Mode:	•	Dial
Backup Mode:	•	Dial
Load Balance Mode:		Dial

#### **VPN Connection Status**

All VPN Status	LAN-to-LA	N VPN Status	Remote Dia	I-in U	lser Status				
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate(Kbps)	Rx Pkts	Rx Rate(Kbps)	UpTime	
( OVPNuser ) Local User Database	OpenVPN AES-SHA1 Auth	118.166.186.70 via WAN1	192.168.89.11/32	1048	438.40	947	56.10	0:3:56	Drop
					XXXXXXXXX	: Dat	ta is encrypt	ted.	

xxxxxxxx : Data isn't encrypted.