

# How to use OpenVPN Server/Client on TW-EAV510/EAV510 AC

**Note:** Please make sure that both LAN side networks are in different subnet.

## Enable OpenVPN Server Function

Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Server**, make **“Enable OpenVPN Server”** checkbox checked. And you will see the page as below:

## OpenVPN Server

☒ Enabled OpenVPN Server

Protocol:

TCP ▾

Port Number:

443

Tunnel Subnet:

10.8.0.0

Tunnel Mask:

255.255.255.0

Cipher Encryption:

BF-CBC ▾

HMAC Authentication:

SHA1 ▾

☒ Enabled LZO data compression

Apply/Save

## CA

-----BEGIN CERTIFICATE-----  
MIIDvDCCAYWgAwIBAgIJANeF5nRrRo8HMA0GCSqGSIb3DQEBBQUAMIGBMQswCQYD  
VQQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5BMRkwFwYDVQQKEwB3d3cu  
dGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdlbGwuuY29tMRwwGgYDVQPD  
ExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvcNAQkBFg9jYUB0Zw1d2Vs  
bC5jb2w0HhCNMTAxMDAwMTAxMDAwMDE2WmcNMTEkxMjMwMDAwMDE2WjCmZ2ELMAKGA1UE  
BhMCRkxkCzAJBGNVBAcTAKZJMQswCQYDVQGEwJQOQTEZMBCGA1UEChMQd3d3LnRl  
bGV3ZlwxLnMvNvTEZMBCGA1UECmQd3d3LnRlbnV3ZlwxLnMvNvTEcMB0GA1UEAAMT  
d3d3LnRlbnV3ZlwxLnMvNvSBDOQTEeMBwGCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW9HEExBx8ZFMDDKz3nUKPUjbpHSSwC3Z1v1A3J6ZyytXb/xbj  
YnBgFjTLVegKHqI1k1jZ6sb1W0XGx8Jq7knGpwU23ez9ov1MIDfUsN0YfKb3DM27/  
EHDod+veXbuP/5Ir4qfASwIDAQABo4IBDDCCAQAwHQYDVRO0BBYEFGS+yI1V1gT6  
o1Jm7pgCf2TJCx3AMIHQBGMVHSMEEgcgwgcwAFGS+yI1V1gT6o1Jm7pgCf2TJCx3A  
oYghpIGeMIGBMQswCQYDVQGEwJGSTEIEMAKGA1UECBMCRkxkCzAJBGNVBAcTAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuuY29tMRkwFwYDVQLEExB3d3cudGVsZXdl  
bGwuuY29tMRwwGgYDVQDEExN3d3cudGVsZXdlbGwuuY29tIENBMRA4wHAYJKoZIhvc  
NAQkBFg9jYUB0Zw1d2VsY29tMIGfMA0GCSqGSIb3DQEQJARYPY2FADGvYsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQKgBQg1RDUrUyAkw7pgYDD1ADf1BL  
tyXvTeKc+veKRuNkfiW

**Enabled OpenVPN Server:** Make it checked to enable OpenVPN Server function.

**Protocol:** Select the protocol for OpenVPN. It can be TCP or UDP.

**Port Number:** Enter the port number for OpenVPN, default is 443.

**Tunnel Subnet:** The IP subnet for tunnel interface, the system will generate the IP for clients automatically.

**Tunnel Mask:** The subnet mask for tunnel interface.

**Cipher Encryption:** Select the encryption method.

**HMAC Authentication:** Select the authentication way.

**Enabled LSO data compression:** Make it checked to enable data compression.

**Certificate Authority (CA):** You can click **Generate CA** button to generate the CA, all clients must use this CA for OpenVPN connection.

**Send CA to E-mail:** Fill in the E-Mail address and click **Send** button. The system will send the generated CA to the address. You can just copy and paste to your OpenVPN client once you get it via mail.

**Note:** All clients must use the CA that generated from TW-EAV510/AC, otherwise the connection cannot be established.

## Setup OpenVPN account for OpenVPN Server

Go to **Advanced Setup** -> **VPN** -> **Account**.

### Account

Maximum entries: 4

Name	Enable	Username	Connection Type	Peer IP	Peer Netmask	Remove	Edit
------	--------	----------	-----------------	---------	--------------	--------	------

Add

Remove

Click **Add** button to add new user. Totally support up to 4 users for both PPTP, L2TP and OpenVPN.

## Configure Account

Name:	<input type="text" value="test1"/>
<input checked="" type="checkbox"/> Enable	
Username:	<input type="text" value="test1"/>
Password:	<input type="password" value="....."/>
Connection Type:	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN TO LAN
Peer IP:	<input type="text" value="192.168.20.0"/>
Peer Netmask:	<input type="text" value="255.255.255.0"/>

**Name:** The name for user profile.

**Enable:** Enable/Disable this account.

**Username:** The name will be used for authentication.

**Password:** The password will be used for authentication.

**Connection Type:** Setup connection to Remote Access or LAN to LAN.

**Remote Access** - Limited your remote OpenVPN Client as one of clients at local network. The remote client can have full access to local network, but any clients at local network cannot access to remote client's network.

**LAN to LAN** - The clients at both local/remote network can access each other.

**Peer IP:** Enter the remote network's IP address.

**Peer Netmask:** Enter the remote network's netmask.

## Remove/Edit user

### Account

Maximum entries: 4

Name	Enable	Username	Connection Type	Peer IP	Peer Netmask	Remove	Edit
test1	Enable	test1	LAN TO LAN	192.168.20.0	255.255.255.0	<input type="checkbox"/>	<input type="button" value="Edit"/>

Make Remove checkbox checked and click **Remove** button to remove user or click **Edit** button to edit the details of user.

# Setup OpenVPN Client

Go to **Advanced Setup -> VPN -> OpenVPN -> Trusted CA**

## Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
Maximum entries: 4

Name	Subject	Type	Action
------	---------	------	--------

Import Certificate

Click **Import Certificate** button. The content of Certificate can be got from Server side or your mailbox if you did use function **Send CA to E-mail** on TW-EAV510/AC OpenVPN setting page. Click **Apply** button to save your CA. The TW-EAV510/AC can support multiple CAs.

### Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Test

Certificate:

V00GEwJGSTE LMAkGA1UECBMCRkxkCzA3BgNVBAC TAk5BMRkwFwYDVQOKE xB3d3cu dGVsZXdlbGwuY29tMRkwFwYDVQOKE xB3d3cu dGVsZXdlbGwuY29tMRwwGgYDVQO DExN3d3cu dGVsZXdlbGwuY29tIENBMR4wHAYJKoZIhvc NAQkBFg9jYUB0ZWxld2Vs bC5jb20wHhcNMTAwMTAxMDA0NTI4WhcNMTkxMjMwMDA0NTI4WjCBMzELMAkGA1UE BhmCRkxkCzA3BgNVBAGTAKZjM0swCQYDVQOHEwJ0OTEZMBcGA1UECHM0d3d3LnRl bGV3ZWxsLmNvbTEZMBcGA1UECXM0d3d3LnRl bGV3ZWxsLmNvbTEcMB0GA1UEAxMT d3d3LnRl bGV3ZWxsLmNvbSBDO TEeMBwGC5qGS Ib3DOE JARYPY2FAdGVsZXdlbGwu Y29tMIGfMA0GC SgGS Ib3DOEBAQUAA4GNADCBiQKBgQDuiyks4JYC9cymymC xgK1P At211mafmycN/hwi6BIk jJOKqNqv/5dJ sX6Jdh/v1N xVE10yx+xGCC KoXtzvb4Tv kHQ7mCuJ4czH0p1RYLUk4c6HCKTMDbt8wQGFc5+gGpQ0kyj3vV2TNQrEzATDnyQd GE4Gq8Jcs2XUuKV37u1H9wIDAQABo4IBBDCCAQA wHQYDV R00BBYEFBukFzFvXIGI x67bes5c2AB8PvbqMIHOBgNVHSM EgcgwgcwAFBukFzFvXIGI x67bes5c2AB8Pvbq oYGhpIGeMIGbMQswCQYDVQOGEwJGSTE LMAkGA1UECBMCRkxkCzA3BgNVBAC TAk5B MRkwFwYDVQOKE xB3d3cu dGVsZXdlbGwuY29tMRkwFwYDVQOKE xB3d3cu dGVsZXdl bGwuY29tMRwwGgYDVQO DExN3d3cu dGVsZXdlbGwuY29tIENBMR4wHAYJKoZIhvc N AOkBFg9jYUB0ZWxld2Vs bC5jb22CCOC0ag1gn0shGzAMBgNVHRMEBTADAQH/MA0G CSqGS Ib3DOEBBQUAA4GBAE0W i4aUJT0VwMQV kqJqFYhe6BfvHtf/R6w97B41hq6G /F/SA A17Hz7aR9HSLNn9Rjhr6k+Q7NMxUrsF1fwqf2p1dRK75w2IwNbUXfeuXerL aEyIwvgQwxjqThqz14v1FjZUJ0773ZtMabTgeUoM7qcTFAbvJa+CYTxwk1NtRpEd -----END CERTIFICATE-----

Apply

Once it is done, you can see the settings as below. You can also click **View** button to check imported CA or **Remove** button to remove the CA.

## Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
Maximum entries: 4

Name	Subject	Type	Action
Test	C=FI/ST=FI/L=NA/O=www.telewell.fi/OU=www.telewell.fi/CN=www.telewell.fi CA/emailAddress=ca@telewell.fi	ca	<div>ViewRemove</div>

Import Certificate

## Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Client**

### OpenVPN Client

Maximum entries: 4

Name	Local Gateway Interface	Remote Gateway	Username	Protocol	Port Number	Cipher Encryption	HMAC Authentication	LZO	CA Profile	Enable	Remove	Edit
<input type="button" value="Add"/>	<input type="button" value="Enable"/>	<input type="button" value="Remove"/>										

Click **Add** button to add a new OpenVPN Client connection.

### OpenVPN Client

Name:	<input type="text" value="Office"/>
<input checked="" type="checkbox"/> Enable	
Local Gateway Interface:	<input type="text" value="ipoe_eth2/eth2.1"/>
Remote Gateway:	<input type="text" value="10.0.0.254"/>
Username:	<input type="text" value="test1"/>
Password:	<input type="password" value="....."/>
Protocol:	<input type="text" value="TCP"/>
Port Number:	<input type="text" value="443"/>
Cipher Encryption:	<input type="text" value="BF-CBC"/>
HMAC Authentication:	<input type="text" value="SHA1"/>
<input checked="" type="checkbox"/> Enabled LZO data compression	
CA Profile:	<input type="text" value="Test"/>
<input type="button" value="Apply/Save"/>	

**Name:** The name for OpenVPN Client profile.

**Enable:** Enable/Disable this profile.

**Local Gateway Interface:** Select the correct WAN interface that will be used to access to remote network.

**Remote Gateway:** Enter the IP/Domain address of remote OpenVPN Server.

**Username:** The name will be used for authentication.

**Password:** The password will be used for authentication.

**Protocol:** Select the protocol for OpenVPN. It can be TCP or UDP.

**Port Number:** Enter the port number for OpenVPN, default is 443.

**Cipher Encryption:** Select the encryption method.

**HMAC Authentication:** Select the authentication way.

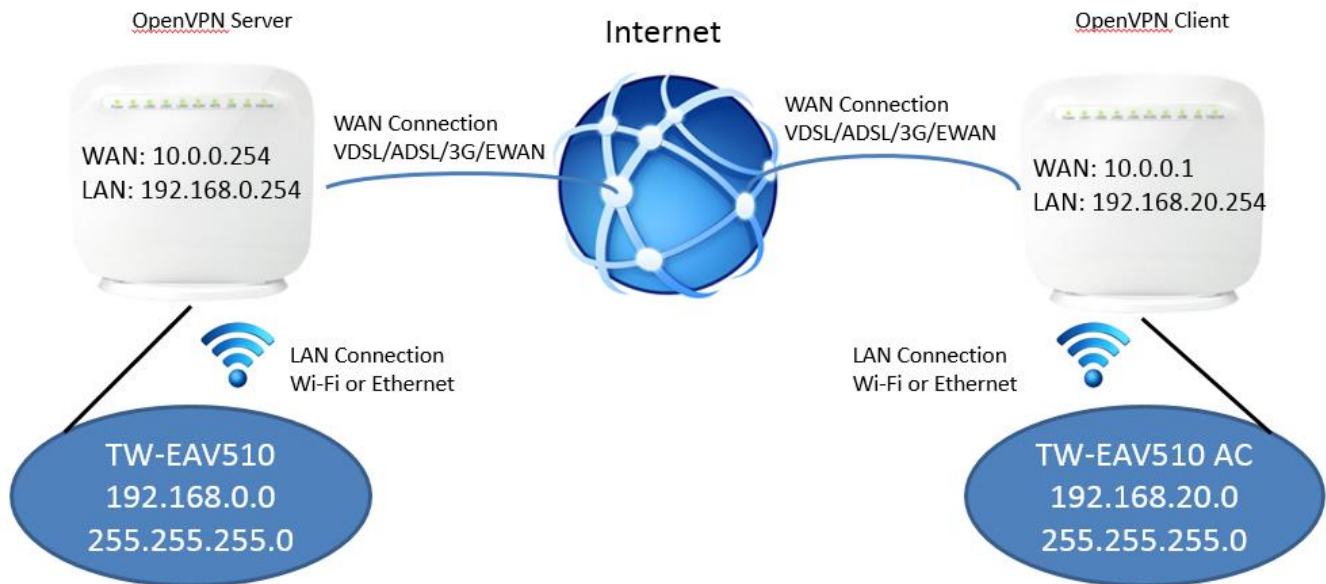
**Enabled LSO data compression:** Make it checked to enable data compression.

**CA Profile:** Select one of imported CA for OpenVPN connection.

**Note:** All clients must use the CA that generated from TW-EAV510/AC, otherwise the connection cannot be established.

# Example 1

TW-EAV510 is activated as OpenVPN Server and TW-EAV510 AC is activated as OpenVPN Client.



## Remote Access

### TW-EAV510 (OpenVPN Server)

1. Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Server**, enable the OpenVPN Server and do the settings as below. Click **Apply/Save** button to save changes.

## OpenVPN Server

☒ Enabled OpenVPN Server

Protocol:

TCP ▾

Port Number:

443

Tunnel Subnet:

10.8.0.0

Tunnel Mask:

255.255.255.0

Cipher Encryption:

BF-CBC ▾

HMAC Authentication:

SHA1 ▾

☒ Enabled LZO data compression

Apply/Save

## CA

-----BEGIN CERTIFICATE-----  
MIIDvDCCAYWgAwIBAgIJALRqDWcc6yEbMA0GCSqGSIb3DQEBBQUAMIGBMQswCQYD  
VQQGEwJSTELMAkGA1UECBMCRkkxZzA3BGNVBAcTAK5BMRkwFwYDVQQKEExB3d3cu  
dGVsZXdlbGwuY29tMRkwFwYDVQQLEExB3d3cudGVsZXdlbGwuY29tMRwwGgYDVQQD  
ExN3d3cudGVsZXdlbGwuY29tIENBMR4wHAYJKoZIhvcNAQkBFg9jYUB0ZWxlid2Vs  
bc5jb20wHhcNMTAwMTAxMDA0NTI4WhcNMTEkxMjMwMDA0NTI4WjCBmzELMAkGA1UE  
BhMCRkkxZzA3BGNVBAcTAKZjMQswCQYDVQQHEwJJOQTETZMBcGA1UEChMQd3d3LnRl  
bGV3ZWxsLmNvbTEZMBcGA1UECxMQd3d3LnRlbGV3ZWxsLmNvbTECMBoGA1UEAxMT  
d3d3LnRlbGV3ZWxsLmNvbSBDOQTEeMBwGCsqGSIb3DQEJARYPY2FAdGVsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAAAGNADCBiQKBggQDuiyks4JYC9cymymCxxgKLP  
At211mafmycn/hwi6BIkjJQkqNQv/5dJsX6Jdh/vlnXVE10yx+xGCCKoXtzvb4Tv  
khQ7mcUj4czH0plRYLUk4c6HCkTMDbt8wQGfc5+qGpQ0kyj30V2TNQRkEzATDnyOd  
GE4Gq8Ujcs2XUAQuK37u1H9wIDAQABo4IBDDCCAQAuHQYDVQDA0BBYEFBukFzfVxIGI  
x67bes5c2AB8PvbqMIHQBgNVHSMEgcgwgcWAfBukFzfVxIGIx67bes5c2AB8Pvbq  
oYGhpIGeMIGBMQswCQYDVQQGEwJSTELMAkGA1UECBMCRkkxZzA3BGNVBAcTAK5B  
MRkwFwYDVQQKEExB3d3cudGVsZXdlbGwuY29tMRkwFwYDVQQLEExB3d3cudGVsZXdl  
bGwuY29tMRwwGgYDVQQDEExN3d3cudGVsZXdlbGwuY29tIENBMR4wHAYJKoZIhvcn  
AQkBFg9jYUB0ZWxlid2Vsbc5jb22CCQC0aglgnoShGzAMBGNVHRMEBTADAQH/MA0G  
CSqGSIb3DQEBBQUAAAGBAE0Wi4aUJT0VwMQvkqJqFYhe6BfvHtf/R6w97B4ihq6g  
/F/SAAI7Hz7ar9HSLNN9Rjhr6k+Q7NMxUrsFlfwqf2p1dRK75w2IWnbUXfeuXerL

2. Go to **Advanced Setup -> VPN -> Account**, add a new user for login.

## Configure Account

Name:

☒ Enable

Username:

Password:

Connection Type: ☒ Remote Access ☐ LAN TO LAN



**Note:** The CA contents must between wording “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”



----“, they cannot be deleted.

3. Once the CA import successfully, you will see the page as below.

#### Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
Maximum entries: 4

Name	Subject	Type	Action
Test_CA	C=FI/ST=FI/L=NA/O=www.telewell.fi/OU=www.telewell.fi/CN=www.telewell.fi CA/emailAddress=ca@telewell.fi	ca	<button>View</button> <button>Remove</button>

Import Certificate

4. Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Client**, click **Add** button to add a new OpenVPN connection.

#### OpenVPN Client

Name:	<input type="text" value="OpenVPN-Test"/>
<input checked="" type="checkbox"/> Enable	
Local Gateway Interface:	<input type="text" value="ipoe_eth4/eth4.1"/>
Remote Gateway:	<input type="text" value="10.0.0.254"/>
Username:	<input type="text" value="test"/>
Password:	<input type="password" value="...."/>
Protocol:	<input type="text" value="TCP"/>
Port Number:	<input type="text" value="443"/>
Cipher Encryption:	<input type="text" value="BF-CBC"/>
HMAC Authentication:	<input type="text" value="SHA1"/>
<input checked="" type="checkbox"/> Enabled LZO data compression	
CA Profile:	<input type="text" value="Test_CA"/>

Apply/Save

Click **Apply/Save** button to save account settings.

#### OpenVPN Client

Maximum entries: 4

Name	Local Gateway Interface	Remote Gateway	Username	Protocol	Port Number	Cipher Encryption	HMAC Authentication	LZO	CA Profile	Enable	Remove	Edit
OpenVPN-Test	eth4.1	10.0.0.254	test	TCP	443	BF-CBC	SHA1	Enable	Test_CA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<button>Edit</button>

Add Enable Remove

5. Go to **Device Info -> VPN -> Client Info** to check connection status. You can also click **Disconnect** button to disconnect the OpenVPN connection.

#### Device Info -- Client Info

Name	Type	Enable	Status	Connection Type	Remote Gateway	Peer IP	Client IP	Action
OpenVPN-Test	OpenVPN	Enabled	Connected		10.0.0.254	10.8.0.1	10.8.0.6	<button>Disconnect</button>

When **Status** shows **Connected**, you can now access to remote network.

Below is Server Info for reference.

#### Device Info -- Server Info

Name	Type	Enable	Status	Connection Type	Peer IP	Connected By	Action
test	OpenVPN	Enabled	Connected	Remote Access		10.8.0.6	

# LAN to LAN

## TW-EAV510 (OpenVPN Server)

1. Go to **Advanced Setup** -> **VPN** -> **OpenVPN** -> **OpenVPN Server**, enable the OpenVPN Server and do the settings as below. Click **Apply/Save** button to save changes.

## OpenVPN Server

☒ Enabled OpenVPN Server

Protocol:

TCP ▾

Port Number:

443

Tunnel Subnet:

10.8.0.0

Tunnel Mask:

255.255.255.0

Cipher Encryption:

BF-CBC ▾

HMAC Authentication:

SHA1 ▾

☒ Enabled LZO data compression

Apply/Save

## CA

-----BEGIN CERTIFICATE-----  
MIIDvDCCAYwIwAgAwIJBALRqDWCc6yEbMA0GCSqGSIb3DQEBBQUAMIGbMQswCQYD  
VQQGEwJGSTEhMAkGA1UECBMRkxkxZCzAJBgNVBACITAK5BRkwFwYDVQQKEwB3d3cu  
dGVsZXdlbGwuY29tMRkwFwYDVQQLEwB3d3cudGVsZXdlbGwuY29tMRwwGgYDVQQD  
ExN3d3cudGVsZXdlbGwuY29tIENBMR4wHAYJKoZIhvcNAQkBFg9jYUB0ZWxlid2Vs  
bC5jb20wHhcNMTAwMTAxMDA0NTI4WwNMTkxMjMwMDA0NTI4WjCBmzELMAkGA1UE  
BhMCRkxkxZCzAJBgNVBAGITAK5JMQswCQYDVQQHEwJ0QTEZMBcGA1UEChMQd3d3LnRl  
bGV3ZWxsLmNvbTEZMBcGA1UECXMqd3d3LnRlbGV3ZWxsLmNvbTEcMBoGA1UEAxMT  
d3d3LnRlbGV3ZWxsLmNvbSBDQTEeMBwGCSqGSIb3DQEJARYPY2FAdGVsZXdlbGwu  
Y29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDuiyks4JYC9cymymCxxGK1P  
At211mafmycHn/hwi6BIkjJQKqNqv/5dJsX6Jdh/v1NxVE10yx+xGCKCoXtzb4Tv  
kHQ7mCuJ4czCH01RYLUk4c6HCKTMDbt8wQGFc5+qGpQ0kyj3vV2TNQrEzATDnyOd  
GE4Gq8Jcs2XUuKv37u1H9wIDAQAB04IBBDCCAQAwwHQYDVR0O0BBYEFBukFzFvXIGI  
x67bes5c2AB8PvbqMIHQBgNVHSMGcgwgclWAFBukFzFvXIGIx67bes5c2AB8Pvbq  
oYGhpIGeMIGbMQswCQYDVQQGEwJGSTEhMAkGA1UECBMRkxkxZCzAJBgNVBACITAK5B  
MRkwFwYDVQQKEwB3d3cudGVsZXdlbGwuY29tMRkwFwYDVQQLEwB3d3cudGVsZXdl  
bGwuY29tMRwwGgYDVQQDEwN3d3cudGVsZXdlbGwuY29tIENBMR4wHAYJKoZIhvcN  
AQkBFg9jYUB0ZWxlid2VsbC5jb22CCQC0ag1gnOshGzAMBgNVHRMEBTADAQH/MA0G  
CSqGSIb3DQEBBQUAA4GBAE0Wi4aUJT0VwMQVqkqJqFYhe6BfvHtF/R6w97B4ihq6g  
/F/SAA17Hz7aR9HSLNn9Rjhr6k+Q7NMxUrsF1fwqf2p1dRK75w2IwNBUXfeuXerL

2. Go to **Advanced Setup** -> **VPN** -> **Account**, add a new user for login. The different with Remote Access is you need to enter peer network information.

## Configure Account

Name:

☒ Enable

Username:

Password:

Connection Type: ☐ Remote Access ☒ LAN TO LAN

Peer IP:

Peer Netmask:

Click **Apply/Save** button to save changes.

## Account

Maximum entries: 4

Name	Enable	Username	Connection Type	Peer IP	Peer Netmask	Remove	Edit
test	Enable	test	LAN TO LAN	192.168.20.0	255.255.255.0	<input type="checkbox"/>	<input type="button" value="Edit"/>

## TW-EAV510 AC (OpenVPN Client)

- Go to **Advanced Setup -> VPN -> OpenVPN -> Trusted CA**, click Import Certificate button to add a new CA.

## Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
Maximum entries: 4

Name	Subject	Type	Action
------	---------	------	--------

- Setup a name for importing certificate and paste the CA to **Certificate** field. Click **Apply** button to save your CA.

Enter certificate name and paste certificate content.

Test\_CA

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDrjCCAxegAwIBAgIJAMdMDbEBCqzKMA0GCsqGSIb3DQEBBQUAMIGXMsowCQYD
VQOGEwJGStELMAkGA1UECBMCRkxkCzA3BgNVBACtAk58MRgwFgYDVQKKEw93d3cu
dGV5ZXdlbGwuzmkxGDAwBgNVBAsTD3d3dy50ZWxld2VsbC5maTEbMBkGA1UEAxMS
d3d3LnRlbGwuzWxsLmZpIENBMR0wGwYJKoZIhvcNAQKBGfG5jYUB0ZWxld2VsbC5m
aTEaFw0xMDAxMDAwMDI0MTA0MTA0Fw0YKzAwMDI0MTA0MTA0MIGXMsowCQYDVQKKEwJG
StELMAkGA1UECBMCRkxkCzA3BgNVBACtAk58MRgwFgYDVQKKEw93d3cudGV5ZXdl
bGwuzmkxGDAwBgNVBAsTD3d3dy50ZWxld2VsbC5maTEbMBkGA1UEAxMSd3d3LnRlb
bGV3ZWxsLmZpIENBMR0wGwYJKoZIhvcNAQKBGfG5jYUB0ZWxld2VsbC5maTECBnZAN
BgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEEAuKHu5YpduQhD+SL33d9NS2lMVX8ezOfI
EiPt8qhvhvCsUsv+MlpKIIXcQolzf+kWQ36iDRcgIyZ2dQPTnJfEfVFunIB0PjXW03W
yHua+dxj1lScqgez+y3oMBt0343H8VRtClpL1faNTUowxAWC0dk7aMnQu46CjPnz
0TAmXQ9S0LkCAwEAABoB/zCB/DadBgNVHQ4EFgQUFIQaenB1UC986ZLSy38JjN1P
q34gwcwGA1UdIwSBwDCBwYAUFIQaenB1UC986ZLSy38JjN1Pq36hgZ2kgZowgZcx
CzA3BgNVBAYTAkZJMQswCQYDVQKKEwJGStELMAkGA1UEBxMCTExxGDAwBgNVBAot
D3d3dy50ZWxld2VsbC5maTEYMBYGA1UECwMPD3d3LnRlbGwuzWxsLmZpMRswGQYD
VQODEwJ3d3cudGV5ZXdlbGwuzmkxGQ0E0XHTABBgkqhkiG9w0BCQEWDMNhOHRlbgV3
ZWxsLmZpZggkAx0wMF4EKROQwDADVR0TBAUwAGBg/zANBgkqhkiG9w0BAQFAAOB
gQATnJkt+gODM9csc5YhGmZedU8y+Uz6VWruVnSIfJccQvvaIe9X07v3jpdQnIdo
5Cc54Amwr/DX+vYzw7n7sS+vgNfQZatVRra+oSBcvPAjswFMHS/xTnG+jKXs1mQ
-----END CERTIFICATE-----
```

### Apply

8. Once the CA import successfully, you will see the page as below.

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
Maximum entries: 4

Name	Subject	Type	Action
Test_CA	C=FI/ST=FI/L=NA/O=www.telewell.fi/OU=www.telewell.fi/CN=www.telewell.fi CA/emailAddress=ca@telewell.fi	ca	<input type="button" value="View"/> <input type="button" value="Remove"/>

Import Certificate

9. Go to **Advanced Setup -> VPN -> OpenVPN -> OpenVPN Client**, click **Add** button to add a new OpenVPN connection.

## OpenVPN Client

Name:	<input type="text" value="OpenVPN-Test"/>
<input checked="" type="checkbox"/> Enable	
Local Gateway Interface:	<input type="text" value="ipoe_eth4/eth4.1"/>
Remote Gateway:	<input type="text" value="10.0.0.254"/>
Username:	<input type="text" value="test"/>
Password:	<input type="password" value="...."/>
Protocol:	<input type="text" value="TCP"/>
Port Number:	<input type="text" value="443"/>
Cipher Encryption:	<input type="text" value="BF-CBC"/>
HMAC Authentication:	<input type="text" value="SHA1"/>
<input checked="" type="checkbox"/> Enabled LZO data compression	
CA Profile:	<input type="text" value="Test_CA"/>

Click **Apply/Save** button to save account settings.

**Note:** The OpenVPN client side will get peer network information from server side, so no need to setup peer network.

### OpenVPN Client

Maximum entries: 4

Name	Local Gateway Interface	Remote Gateway	Username	Protocol	Port Number	Cipher Encryption	HMAC Authentication	LZO	CA Profile	Enable	Remove	Edit
OpenVPN-Test	eth4.1	10.0.0.254	test	TCP	443	BF-CBC	SHA1	Enable	Test_CA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>

10. Go to **Device Info -> VPN -> Client Info** to check connection status. You can also click **Disconnect** button to disconnect the OpenVPN connection.

### Device Info -- Client Info

Name	Type	Enable	Status	Connection Type	Remote Gateway	Peer IP	Client IP	Action
OpenVPN-Test	OpenVPN	Enabled	Connected		10.0.0.254	10.8.0.1	10.8.0.6	<input type="button" value="Disconnect"/>

When **Status** shows **Connected**, you can now access to remote network.

Below is Server Info for reference.

### Device Info -- Server Info

Name	Type	Enable	Status	Connection Type	Peer IP	Connected By	Action
test	OpenVPN	Enabled	Connected	LAN TO LAN	192.168.20.0	10.8.0.6	

# Windows/Mac/Android/iOS Setting

Regarding to the OpenVPN on Windows/Mac/Android/iOS, you can download the software/APP from link below.

<https://openvpn.net/>

There is also a HOW TO documentation which can be found at link below.

<https://openvpn.net/index.php/access-server/docs.html>

Below is example for Windows OpenVPN Client software and connect to TW-EAV510/AC OpenVPN server.

The OpenVPN Client software can be downloaded from the following link.

<https://openvpn.net/index.php/open-source/downloads.html>

## Step 1:

Download the OpenVPN Client software and install it. Enable the OpenVPN Server and setup account on TW-EAV510/AC.

## Step 2:

Before running the OpenVPN client software, we have to make three files ready. All files must be created by user self and put them at "C:\Program Files\OpenVPN\config".

**ca.crt** → The content of this file is the CA on TW-EAV510/AC. You can find it at TW-EAV510/AC WEB GUI *Advanced*

*Setup -> VPN -> OpenVPN -> OpenVPN Server*. Here is the example for reference.

-----BEGIN CERTIFICATE-----

MIIDvDCCAyWgAwIBAgIJAMgl7mr+9en0MA0GCSqGSIb3DQEBBQUAMIGbMQswCQYD

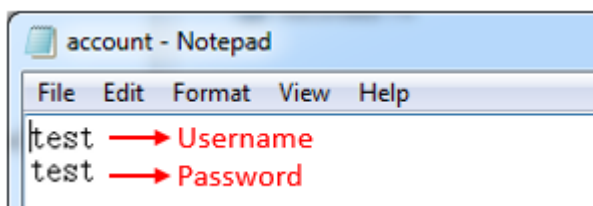
VQQGEwJGSTEMLMAkGA1UECBMCRkxkCzAJBgNVBACeTAk5BMRkwFwYDVQQKEXB3d3cu

...

/wa20SWAlYTBcoqX0kbfGsxSK71uiFWKK7lggHb2ZNix7IAc4JLDT9P46/aNi374

-----END CERTIFICATE-----

**account** → This is for OpenVPN authentication, it must to match the account setting on TW-EAV510/AC which can be found at *Advanced Setup -> VPN -> Account*. The content for first line is username, and second line is password.





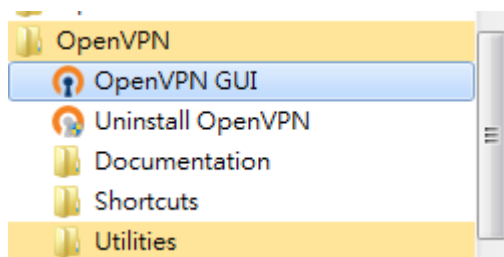
**myconfig.ovpn** → This file contains all the OpenVPN connection settings. This file must be created by user self and you can download the example here and modify the settings to meet your environment.



myconfig.ovpn

### Step 3:

Run OpenVPN GUI with Administrator access right. **It is very important to run as administrator otherwise, the OpenVPN cannot work correctly.**



### Step 4:

After running with OpenVPN GUI, you can the following icon as red marked at system tray.



Right click on this icon and select *Edit Config*.

### Step 5:

Regarding to the configuration of OpenVPN, we just need to focus on the following parts.

1. Connection Type, it must set to client mode.

```
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
```

**client**

2. The protocol setting must be the same as server side.

```
# Are we connecting to a TCP or
# UDP server? Use the same setting as
# on the server.
proto tcp
;proto udp
```

☒ Enabled OpenVPN Server

Protocol:	TCP ▼
Port Number:	443
Tunnel Subnet:	10.8.0.0
Tunnel Mask:	255.255.255.0
Cipher Encryption:	BF-CBC ▼
HMAC Authentication:	SHA1 ▼

☒ Enabled LZO data compression

3. Setup OpenVPN Server Domain/IP address. If it is TCP then use port number 443, and UDP is 1194.

# The hostname/IP and port of the server.

# You can have multiple remote entries

# to load balance between the servers.

remote www.xxx.xxx.net 443

;remote my-server-2 1194

4. Specify the file location for CA and account information.

# SSL/TLS parms.

# See the server config file for more

# description. It's best to use

# a separate .crt/.key file pair

# for each client. A single ca

# file can be used for all clients.

#ca ca.crt

#cert client.crt

#key client.key

ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"

auth-user-pass "C:\\Program Files\\OpenVPN\\config\\account"

5. After above changes, save and close the file. Right click on OpenVPN icon at system tray and select "Connect" to make OpenVPN connection.

