



TrustGate – EasyTunnel VPN quick-guide

This guide covers basic EasyTunnel VPN setup.

Prerequisites:

- TrustGate model 61 “or higher” as VPN concentrator
- TrustGate model 60 “or higher” as VPN client
- Public IP for the VPN concentrator (or at least NAT 500/4500 to the VPN concentrator)

1A – Server preparation:

Log on to the VPN concentrator, and select VPN > EasyTunnel. In dropdown, select Server mode and click next.

Choose a name and a password for the CA server, and click Next.

The screenshot shows the 'EasyTunnel Server Preparation' configuration page. At the top, there is a navigation menu with 'VPN Info', 'General', 'EasyTunnel', 'Peers', 'Tunnels', 'PPTP', and 'Auth'. The main content area contains the following text: 'A CA must be created on the appliance. This is needed to automatically sign certificates for the EasyTunnel Clients that you define. Please enter a password for the CA below. The password is case-sensitive. It must be at least 8 characters long and contain at least 1 non-alphabetic character. If you choose a different name than the one proposed, restrict the choice of characters to the ASCII 7-bit set.' Below this text are three input fields: 'CA Name: VPN_Concentrator_CA', 'Password: *****', and 'Retype: *****'. At the bottom right, there are 'Cancel' and 'Next >>' buttons.

1B – Review the following steps, and click Next

The screenshot shows a confirmation screen for 'EasyTunnel Server Preparation'. The navigation menu is the same as in the previous screenshot. The main text reads: 'The CA certificate will be added to the list of trusted CAs, so that the certificates signed by the CA can pass authentication.' At the bottom, there are 'Cancel' and 'Next >>' buttons.

The screenshot shows a warning screen for 'EasyTunnel Server Preparation'. The navigation menu is the same. The main text reads: 'The local certificate of this appliance needs to be signed by the CA, so that it will pass authentication by the EasyTunnel Clients. If you currently use the certificate to authenticate towards other peers, you may need to take steps to make those peers accept the signed certificate. WARNING: The current local certificate is already signed by another CA. This operation will delete that certificate, and replace it with a new one. If you use the current certificate to authenticate towards other peers, you may need to take steps to make those peers accept the new certificate.' At the bottom, there are 'Cancel' and 'Next >>' buttons.

This is another view of the warning screen from the previous block, showing the same text and navigation elements.

The screenshot shows the final completion screen for 'EasyTunnel Server Preparation'. The navigation menu is the same. The main text reads: 'Enough information has been collected to prepare for EasyTunnel operation. If you want to activate the settings, press "Finish", or press "Cancel" to abort the preparation.' At the bottom, there are 'Cancel' and 'Finish' buttons.

1C - Create a VPN client

- Go to VPN > EasyTunnel. Click new and select Hardware for a TrustGate VPN client and Software for a VPN SoftClient.
- Type in a Device Name and the MAC address of the client.

The screenshot shows the TrustGate VPN web interface. The top navigation bar includes: System, GateManager, Certificates, CA, VPN, Firewall, Routing, Maintenance, Status, Log, and HELP. Below this is a sub-menu: VPN Info • General • EasyTunnel • Peers Tunnels • PPTP • Auth. The main heading is "EasyTunnel Clients". Below the heading, it says "Used: 1 | Free: 24 | SoftClient licenses free: 0". There is a table with the following columns: Disable, Name, Public IP Address, MAC Address, LAN Address, Subnet Mask, Compress, and Comment. A single row is visible with the following values: Disable (checkbox), Name (DeviceName), Public IP Address (0.0.0.0), MAC Address (00:0D:B9:33:32:10), LAN Address (10.160.0.1), Subnet Mask (255.255.255.0), Compress (checkbox), and Comment (trash icon). Below the table are buttons for Save, New, Networks >>, and List Remote.

1D - Define local networks

- Go to VPN > EasyTunnel, and click Networks >>. Then, click new and set the IP address and subnet of the network you wish the client to connect to.

The screenshot shows the TrustGate VPN web interface. The top navigation bar includes: System, GateManager, Certificates, CA, VPN, Firewall, Routing, Maintenance, Status, Log, and HELP. Below this is a sub-menu: VPN Info • General • EasyTunnel • Peers Tunnels • PPTP • Auth. The main heading is "Local Networks". Below the heading, there is a table with the following columns: Disable, Network, Subnet Mask, and Comment. A single row is visible with the following values: Disable (checkbox), Network (172.9.9.0), Subnet Mask (255.255.255.0), and Comment (trash icon). Below the table are buttons for Save, New, and Back.

2 - Tell the client to connect to the EasyTunnel server

- Log on to the webinterface of the TrustGate VPN client, and go to VPN > EasyTunnel. Select Client if presented with the option, and type the public IP of the VPN concentrator. Then, click save.

The screenshot shows the TrustGate VPN web interface. The top navigation bar includes: System, GateManager, Certificates, CA, VPN, Firewall, Routing, Maintenance, Status, Log, and HELP. Below this is a sub-menu: VPN Info • General • EasyTunnel • Peers Tunnels • PPTP • Auth. The main heading is "EasyTunnel Server". Below the heading, there is a form with a label "DNS Name or IP Address" and a text input field containing "1.2.3.4". Below the input field is a Save button.