



OpenVPN for LES Series Console Servers

Works with LES1200, LES1300, and LES1500 Series console servers.

OpenVPN connection on the Black Box console servers

The LES1200 Series (LES1202A-R2, LES1204A-R2, LES1203A-11G, LES1203A-M-R2, LES1204A-3G-R2), LES1300 Series (LES1308A, LES1316A, LES1332A, LES1348A), and LES1500 Series (LES1508A, LES1516A, LES1532A, LES1548A) console servers with Firmware V3.2 and later each have OpenVPN clients and server software embedded.

OpenVPN allows secure VPN tunneling of data through a single TCP/UDP port over an unsecured network. So an OpenVPN tunnel could be established between a roaming Windows client and a console server within a data center. Or, OpenVPN tunnels could be set up between distributed LES1204A-3G-R2 edge devices (which may not have any publicly accessible IP addresses allocated from their carrier) and some third-party OpenVPN server at the enterprise central management site.

Configuring OpenVPN can be complex, so Black Box provides a simple GUI interface for basic set up. More detailed information on the OpenVPN Access server and client can be found at <https://openvpn.net>.

Enabling OpenVPN on your console server:

- Select OpenVPN on the Serial & Networks menu.
- Click Add and complete the Add OpenVPN Tunnel screen (see the illustration on the next page).

The screenshot shows the BlackBox Network Services web interface. On the left is a navigation menu with categories: Serial & Network, Alerts & Logging, System, Status, and Manage. The main content area is titled 'Add OpenVPN Tunnel' and contains several sections: Tunnel Name, Enabled, Security, Tunnel Settings, Server Mode Details, and Networking. The 'Security' section has three options: PKI (X.509 Certificates), Pre-shared Secret (Static Key File), and Custom Configuration. The 'Tunnel Settings' section includes Device Driver, Protocol, Compression, Server Mode, and Client Mode. The 'Server Mode Details' section includes Local Port. The 'Networking' section includes IP Pool Network and IP Pool Netmask. An 'Apply' button is at the bottom of the main form. Below the main form, there is a footer with copyright information and a smaller version of the 'Networking' section.

BLACK BOX
NETWORK SERVICES

Serial & Network

- » Serial Port
- » Users & Groups
- » Authentication
- » Network Hosts
- » Trusted Networks
- » IPsec VPN
- » OpenVPN
- » PPTP VPN
- » Call Home
- » Cascaded Ports
- » UPS Connections
- » RPC Connections
- » Environmental
- » Managed Devices

Alerts & Logging

- » Port Log
- » Auto-Response
- » SMTP & SMS
- » SNMP

System

- » Administration
- » SSL Certificates
- » Configuration Backup
- » Firmware
- » IP
- » Date & Time
- » Dial
- » Firewall
- » Services
- » DHCP Server
- » Nagios
- » Configure Dashboard
- » I/O Ports

Status

- » Port Access
- » Active Users
- » Statistics
- » Support Report
- » Syslog
- » UPS Status
- » RPC Status
- » Environmental Status
- » Dashboard

Manage

- » Devices
- » Port Logs
- » Host Logs
- » Power
- » Terminal

Add OpenVPN Tunnel

Tunnel Name
A descriptive name for the tunnel.

Enabled ☒ Enable this tunnel. Free-for

Security

PKI (X.509 Certificates) ☒
Authenticate and encrypt using SSL/TLS with client and server certificates.

Pre-shared Secret (Static Key File) ☐
Authenticate and encrypt using a shared static key file. *Note: restricted to one client, on*

Custom Configuration ☐
Upload a custom configuration file.

Tunnel Settings

Device Driver
The type of virtual network device.

Protocol
Tunnel transport protocol.

Compression ☒
Enable LZO compression.

Server Mode ☒
Accept remote OpenVPN client connections.

Client Mode ☐
Connect to a remote OpenVPN server.

Server Mode Details

Local Port
The TCP/IP port to listen on. *Default is 1194.*

Networking

IP Pool Network
Network addresses to allocate to clients.

IP Pool Netmask
Network mask for IP Pool.

© BlackBox 2012 / Customer Support Site

The TCP/IP port to listen on. *Default is 1194.*


Networking

IP Pool Network

- Enter any descriptive name you wish to identify the OpenVPN Tunnel you are adding, for example NorthStOutlet-VPN.
- Check Enabled to enable the tunnel.
- Check Control by Auto-Response if the tunnel is to be controlled by "Network Interface" Auto-Response action. If selected, the default state for the tunnel will be Down
- Select the authentication method to be used. To authenticate using certificates, select PKI (X.509 Certificates) or select Custom Configuration to upload custom configuration files. Custom configurations must be stored in/etc/config

NOTE: If you select PKI (public key infrastructure), you will need to establish:

1. Separate certificate (also known as a public key). This Certificate File will be a *.crt file type.
 2. Private Key for the server and each client. This Private Key File will be a *.key file type.
 3. Master Certificate Authority (CA) certificate and key, which is used to sign each of the server and client certificates. This Root CA Certificate will be a *.crt file type.
 4. For a server, you may also need dh1024.pem (Diffie Hellman parameters). Refer to <https://openvpn.net> for a guide to basic RSA key management, or for alternative authentication methods.
- Select the Device Driver to be used, either Tun-IP or Tap-Ethernet. The TUN (network tunnel) and TAP (network tap) drivers are virtual network drivers that support IP tunneling and Ethernet tunneling, respectively. TUN and TAP are part of the Linux® kernel.
 - Select either UDP or TCP as the Protocol. UDP is the default and preferred protocol for OpenVPN.
 - In Tunnel Mode, nominate whether this console server is to be the Client or Server end of the tunnel. When running as a Server, the console server supports multiple clients connecting to the VPN server over the same port.
 - Check or uncheck the Compression button to enable or disable compression, respectively.



Serial & Network

- » Serial Port
- » Users & Groups
- » Authentication
- » Network Hosts
- » Trusted Networks
- » IPsec VPN
- » OpenVPN
- » PPTP VPN
- » Call Home
- » Cascaded Ports
- » UPS Connections
- » RPC Connections
- » Environmental
- » Managed Devices

Alerts & Logging

- » Port Log
- » Auto-Response
- » SMTP & SMS
- » SNMP

System

- » Administration
- » SSL Certificates
- » Configuration Backup
- » Firmware
- » IP
- » Date & Time
- » Dial
- » Firewall
- » Services
- » DHCP Server
- » Nagios
- » Configure Dashboard
- » I/O Ports

Status

- » Port Access
- » Active Users
- » Statistics
- » Support Report
- » Syslog
- » UPS Status
- » RPC Status
- » Environmental Status
- » Dashboard

Manage

- » Devices
- » Port Logs
- » Host Logs
- » Power
- » Terminal

Add OpenVPN Tunnel

Tunnel Name

A descriptive name for the tunnel.

Enabled ☒

Enable this tunnel.

[Rectangular Snip](#)

Security

PKI (X.509 Certificates) ☒

Authenticate and encrypt using SSL/TLS with client and server certificates.

Pre-shared Secret (Static Key File) ☐

Authenticate and encrypt using a shared static key file. *Note: restricted to one client, one server per tunnel*

Custom Configuration ☐

Upload a custom configuration file.

Tunnel Settings

Device Driver Tun - IP

The type of virtual network device.

Protocol UDP

Tunnel transport protocol.

Compression ☒

Enable LZO compression.

Server Mode ☒

Accept remote OpenVPN client connections.

Client Mode ☐

Connect to a remote OpenVPN server.

Server Mode Details

Local Port

The TCP/IP port to listen on. Default is 1194.

Networking

IP Pool Network 10.100.0.0

Network addresses to allocate to clients.

IP Pool Netmask 255.255.255.0

Network mask for IP Pool.

Apply

OpenVPN for LES Series Console Servers

Configure your console server to be the OpenVPN Server or an OpenVPN Client.

- Complete the Client Details or Server Details depending on the Tunnel Mode selected.
- If Client has been selected, the Primary Server Address will be the address of the OpenVPN Server.
- If Server has been selected, enter the IP Pool Network address and the IP Pool Network mask for the IP Pool. The network defined by the IP Pool Network address/mask is used to provide the addresses for connecting clients.
- Click Apply to save changes.
- To enter authentication certificates and files, Edit the OpenVPN tunnel.
- Select the Manage OpenVPN Files tab. Upload or browse to relevant authentication certificates and files.
- Apply to save changes. Saved files will display in red on the right-hand side of the Upload button.
- To enable OpenVPN, Edit the OpenVPN tunnel.
- Check the Enabled button and click Apply to save changes.

NOTE: Make sure that the console server system time is correct when working with OpenVPN. Otherwise, authentication issues may arise.

- Select Statistics on the Status menu to verify that the tunnel is operational.

BLACK BOX
NETWORK SERVICES

Serial & Network

- Serial Port
- Users & Groups
- Authentication
- Network Hosts
- Trusted Networks
- IPsec VPN
- OpenVPN
- PPTP VPN
- Call Home
- Cascaded Ports
- UPS Connections
- RPC Connections
- Environmental
- Managed Devices

Alerts & Logging

- Port Log
- Auto-Response
- SMTP & SMS
- SNMP

System

- Administration
 - SSL Certificates
 - Configuration Backup
 - Firmware
 - IP
 - Date & Time
 - Dial
 - Firewall
 - Services
 - DHCP Server
 - Nagios
 - Configure Dashboard
 - I/O Ports

Status

- Port Access
- Active Users
- Statistics
- Support Report
- Syslog
- UPS Status
- RPC Status
- Environmental Status
- Dashboard

Manage

- Devices
- Port Logs
- Host Logs
- Power
- Terminal

Interfaces Routes/DNS Serial Ports **IP** ICMP

eth0 Link encap:Ethernet HWaddr 00:13:C6:00:A9:06
inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
inet6 addr: fe80::213:c6ff:fe00:a906/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:44235 errors:0 dropped:0 overruns:0 frame:0
TX packets:794 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 brqueuelen:1000
Interrupt:12 Memory:1fff8000-1fff80ff

eth0:0 Link encap:Ethernet HWaddr 00:13:C6:00:A9:06
inet addr:10.8.100.32 Bcast:10.8.255.255 Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Interrupt:12 Memory:1fff8000-1fff80ff

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:481 errors:0 dropped:0 overruns:0 frame:0
TX packets:481 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0

eth0:1 Link encap:Ethernet HWaddr 00:13:C6:00:A9:06
inet addr:10.8.100.33 Bcast:10.8.255.255 Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0

© BlackBox 2012 - Customer Support Site

Windows OpenVPN Server or an OpenVPN Client

For details on installing an OpenVPN Windows client (or server) and connecting to your console server OpenVPN server (or client), refer to <https://openvpn.net>.

Black Box Tech Support: FREE! Live. 24/7.

Tech support the
way it should be.



Great tech support is just 60 seconds away at 877-877-2269 or blackbox.com.



Disclaimer:

Black Box Network Services shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the product information or specifications set forth in this document and Black Box Network Services may revise this document at any time without notice.

About Black Box

Black Box provides an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 60 seconds or less.

© Copyright 2016. Black Box Corporation. All rights reserved. Black Box® and the Double Diamond logo are registered trademarks of BB Technologies, Inc. Linux is a registered trademark of Linus Torvalds. Any third-party trademarks appearing in this manual are acknowledged to be the property of their respective owners.