OpenVPN Client

An OpenVPN client (version 2.3.8) is available in Obihai OBi1000 series IP phones. It is disabled by default. To enable, the specific VPN related configuration parameters must be programmed.

When the OpenVPN client feature is enabled, the OBi1000 series IP phone will configure the OpenVPN client according to the related parameters and the specified configuration file. When enabled, the OBi1000 series IP phone device will start the OpenVPN client at the same time the physical network interface connects (Ethernet or WiFi). If the VPN connection is successful, all network traffic – except for local network traffic – will be directed to the VPN. E.g. the "VPN" gateway – Provided via the route option "route_vpn_gateway" by the server – will be set as the default route on the OBi device. The server provided DNS options (via dhcp-option) will take over as only the DNS servers used by the OBi device. Hence, the DNS servers assigned by a local DHCP server or statically set in the OBi device's WAN settings will be ignored. After the VPN connection is successfully established, the "locked" icon will appear on the status bar of the phone's LCD screen. Details / information regarding the VPN connection will be displayed in the "System Status" on the OBi1000 series IP phone native device web page.

VPN Client Configuration Parameters

The VPN client is configured by the following parameters:

Parameter	Description	Default Setting
Enable	Enable OpenVPN client feature	Disable
Username	Username of the client, when using username/password to authentication with server is required	
Password	Password of the client, when using username/password to authentication with server is required	
Configuration	The path of the client configuration file (The following section for detail)	

VPN Client Configuration File

The VPN client must be configured using the configuration file in the same syntax and options described at the following link:

https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage

Important notes regarding the configuration file.

- Client mode only, all server related options not supported
- Any script running in client mode is disabled
- "Standalone" options are not supported
- Plugin module not supported

- Management features not supported
- Not all client options are supported. Please refer to unsupported option list at the end of this section
- Must use INLINE file in configuration for options**: connection, ca, cert, dh, extra-certs, key, pkcs12, secret, tls-auth**
- Password-protected private key not supported
- Syslog or status related options not supported
- Writing of any data to any file not supported
- IPv6 not supported
- Username and Password for client authentication must be specified in the OBi parameters instead of in the configuration file
- The following options are always controlled by the OBi Device, internally**: nobind, presist-key inactive, auth-retry, write-pid, daemon**
- Incorrect or unsupported options could cause client to stop

A configuration file must be installed in the OBi Device by copying from the USB flash drive interface or using remote provisioning via the customization data package. See corresponding section for details.

Annex

I. List of unsupported client options:

- Networking related options: **tun-ipv6, dev-node, local, iproute, ifconfig, route, client-nat, max-routes, allow-pull-fqdn, socket-flags, redirect-gateway, redirect-private, up, down, ineted.**
- Process control options: **mlock, setenv, ignore, disable-occ, user, group, cd, chroot, setcon, nice, fast-io, mode, multihome, echo, remap-usr1**, **ping-exit**
- Security feature related options: **auth-nocache, static-challenge, askpass, tls-verify, crl-verify, show, genkey, test-crypto,**

II. Example of a configuration file:

client
dev tun
tun-mtu 48000
fragment 0
mssfix 0
proto udp
remote 192.168.15.28 1194
float
key-direction 1
<ca> *…*
…
</ca>
<pkcs12>

…
</pkcs12>
<tls-auth>
…
</tls-auth>
remote-cert-tls server
cipher AES-256-CBC
comp-lzo yes