Dinstar SME IP PBX UC120 Remote Access Setup Guide

Table of Contents

Dinstar SME IP PBX UC120 Remote Access Setup Guide

Version: 1.0 **Date:** December 2025 **Author:** Technical Documentation Team

Table of Contents

1. Introduction

1.1 Purpose

This manual provides step-by-step instructions for configuring remote public access to a Dinstar SME IP PBX UC120 device without adding additional hardware. The solution utilizes an Ubuntu Server on Linode as an OpenVPN gateway.

1.2 Scope

This guide covers: - OpenVPN server configuration on Ubuntu/Linode - OpenVPN client configuration on Dinstar UC120 - Network routing and firewall configuration - Security best practices - Troubleshooting common issues

1.3 Target Audience

- System administrators
- Network engineers
- VoIP technicians
- IT professionals managing IP PBX systems

2. Prerequisites

2.1 Hardware Requirements

- **Dinstar SME IP PBX UC120** with firmware supporting OpenVPN
- **Ubuntu Server** (cloud-based instance on Linode or similar provider)

2.2 Software Requirements

Component	Requirement
Ubuntu Server	Version 20.04 LTS or later
OpenVPN	Version 2.5 or later
Dinstar UC120 Firmware	Latest stable release

2.3 Network Information Needed

Before starting, gather the following information:

□ Ubuntu Server Public IP Address: ________________
□ Dinstar UC120 Local IP Address: ________________
□ Dinstar UC120 Gateway IP: ________________
□ Desired VPN Subnet: ________________ (e.g., 10.8.0.0/24)
□ Domain Name (optional): ________________

2.4 Access Requirements

□ Root or sudo access to Ubuntu Server
□ Administrator credentials for Dinstar UC120 web interface
□ SSH client for Ubuntu Server access

3. Architecture Overview

3.1 Network Topology

```
┌──────────────────────────────────────────────────────────────┐
│                          INTERNET                              │
└──────────────────────────────────────────────────────────────┘
                              │
                              │ Public IP
                              ▼
                    ┌──────────────────┐
                    │  Ubuntu Server   │
                    │    (Linode)      │
                    │                  │
                    │ OpenVPN Server   │
                    │ Port: 1194/UDP   │
                    └──────────────────┘
                              │
                              │ VPN Tunnel
                              │ (10.8.0.0/24)
                              │
                              ▼
                    ┌──────────────────┐
                    │  Dinstar UC120   │
                    │  IP PBX System   │
                    │                  │
                    │ OpenVPN Client   │
                    │ Local Network    │
                    └──────────────────┘
                              │
                              ▼
                    ┌──────────────────┐
                    │  SIP Phones /    │
                    │  Extensions      │
                    └──────────────────┘
```

3.2 Traffic Flow

1. **Management Access**: Users connect to Ubuntu Server's public IP
2. **VPN Tunnel**: Traffic is forwarded through OpenVPN tunnel to UC120
3. **Web Interface**: UC120 web interface accessible via VPN
4. **SIP/VoIP**: Phone calls routed through VPN tunnel

3.3 Key Components

Component	Role	IP Assignment
Ubuntu Server	OpenVPN Server, Gateway	Public IP + 10.8.0.1
Dinstar UC120	OpenVPN Client, PBX	10.8.0.2
VPN Tunnel	Encrypted connection	10.8.0.0/24 network

---

4. Part 1: Ubuntu Server Setup

4.1 Initial Server Configuration

4.1.1 Connect to Ubuntu Server

```
ssh root@your-server-ip
```

4.1.2 Update System

```
apt update && apt upgrade -y
```

4.1.3 Set Timezone

```
timedatectl set-timezone Asia/Kolkata
# Or your preferred timezone
```

4.2 Install OpenVPN and Easy-RSA

4.2.1 Install Packages

```
apt install openvpn easy-rsa -y
```

4.2.2 Verify Installation

```
openvpn --version
```

Expected output:

```
OpenVPN 2.5.x x86_64-pc-linux-gnu
```

4.3 Configure Certificate Authority (CA)

4.3.1 Setup Easy-RSA Directory

```
mkdir -p ~/easy-rsa
ln -s /usr/share/easy-rsa/* ~/easy-rsa/
cd ~/easy-rsa
```

4.3.2 Initialize PKI

```
./easyrsa init-pki
```

4.3.3 Build CA

```
./easyrsa build-ca nopass
```

Prompts: - Common Name: `Dinstar-VPN-CA` (or your preferred name)

4.3.4 Generate Server Certificate and Key

```
./easyrsa gen-req server nopass
./easyrsa sign-req server server
```

4.3.5 Generate Diffie-Hellman Parameters

```
./easyrsa gen-dh
```

Note: This may take 5-10 minutes.

4.3.6 Generate TLS Authentication Key

```
openvpn --genkey secret ~/easy-rsa/pki/ta.key
```

4.3.7 Generate Client Certificate for UC120

```
./easyrsa gen-req dinstar-uc120 nopass
./easyrsa sign-req client dinstar-uc120
```

4.4 Copy Certificates to OpenVPN Directory

```
mkdir -p /etc/openvpn/server
cp ~/easy-rsa/pki/ca.crt /etc/openvpn/server/
cp ~/easy-rsa/pki/issued/server.crt /etc/openvpn/server/
cp ~/easy-rsa/pki/private/server.key /etc/openvpn/server/
cp ~/easy-rsa/pki/dh.pem /etc/openvpn/server/
cp ~/easy-rsa/pki/ta.key /etc/openvpn/server/
```

4.5 Create OpenVPN Server Configuration

4.5.1 Create Configuration File

```
nano /etc/openvpn/server/server.conf
```

4.5.2 Add Configuration

```
# OpenVPN Server Configuration for Dinstar UC120 Access
# Port and Protocol
port 1194
proto udp
dev tun

# SSL/TLS root certificate (ca), certificate (cert), and private key
(key)
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key
dh /etc/openvpn/server/dh.pem

# Network Configuration
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist /var/log/openvpn/ipp.txt

# Route Configuration
# Push routes to clients
push "route 192.168.1.0 255.255.255.0"  # Adjust to your UC120's
local network

# Client-specific configuration
client-config-dir /etc/openvpn/ccd

# TLS Security
tls-auth /etc/openvpn/server/ta.key 0
cipher AES-256-GCM
auth SHA256

# Security Options
key-direction 0
tls-version-min 1.2

# Networking
keepalive 10 120
persist-key
persist-tun

# User/Group
user nobody
group nogroup

# Logging
```

```
status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
verb 3

# Compression (optional, can improve performance)
compress lz4-v2
push "compress lz4-v2"

# Allow multiple clients with same certificate (not recommended for
production)
# duplicate-cn

# Explicit exit notify for UDP
explicit-exit-notify 1
```

4.5.3 Create Required Directories

```
mkdir -p /etc/openvpn/ccd
mkdir -p /var/log/openvpn
```

4.5.4 Create Client-Specific Configuration

```
nano /etc/openvpn/ccd/dinstar-uc120
```

Add:

```
# Assign static IP to Dinstar UC120
ifconfig-push 10.8.0.2 10.8.0.1

# Push specific routes for UC120
iroute 192.168.1.0 255.255.255.0
```

4.6 Enable IP Forwarding

4.6.1 Edit sysctl Configuration

```
nano /etc/sysctl.conf
```

Uncomment or add:

```
net.ipv4.ip_forward=1
```

4.6.2 Apply Changes

```
sysctl -p
```

Verify:

```
cat /proc/sys/net/ipv4/ip_forward
```

Expected output: 1

4.7 Configure Firewall

4.7.1 Install UFW (if not installed)

```
apt install ufw -y
```

4.7.2 Configure UFW Rules

```
# Allow SSH
ufw allow 22/tcp

# Allow OpenVPN
ufw allow 1194/udp

# Allow forwarding
nano /etc/default/ufw
```

Change:

```
DEFAULT_FORWARD_POLICY="ACCEPT"
```

4.7.3 Add NAT Rules

```
nano /etc/ufw/before.rules
```

Add at the top (before `*filter`):

```
# NAT table rules
*nat
:POSTROUTING ACCEPT [0:0]

# Forward traffic from OpenVPN to internet
-A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

COMMIT
```

Note: Replace `eth0` with your actual network interface. Check with:

```
ip addr show
```

4.7.4 Enable and Start Firewall

```
ufw enable
ufw status verbose
```

4.8 Start OpenVPN Service

4.8.1 Enable and Start Service

```
systemctl enable openvpn-server@server
systemctl start openvpn-server@server
```

4.8.2 Check Service Status

```
systemctl status openvpn-server@server
```

Expected output should show `active (running)`.

4.8.3 Verify VPN Interface

```
ip addr show tun0
```

You should see a `tun0` interface with IP `10.8.0.1`.

4.9 Prepare Client Configuration File

4.9.1 Create Client Configuration

```
cd ~/easy-rsa
nano dinstar-uc120.ovpn
```

4.9.2 Add Configuration

```
# Dinstar UC120 OpenVPN Client Configuration
client
dev tun
proto udp

# Server address - REPLACE with your Ubuntu Server's PUBLIC IP
remote YOUR_SERVER_PUBLIC_IP 1194

resolv-retry infinite
nobind

persist-key
persist-tun

# Security
remote-cert-tls server
cipher AES-256-GCM
auth SHA256
key-direction 1

compress lz4-v2

verb 3

# Certificates and Keys (inline)
<ca>
# Paste contents of ca.crt here
</ca>

<cert>
# Paste contents of dinstar-uc120.crt here
</cert>

<key>
# Paste contents of dinstar-uc120.key here
</key>

<tls-auth>
# Paste contents of ta.key here
</tls-auth>
```

4.9.3 Create Inline Configuration

Create a script to generate the complete configuration:

```
nano ~/create-client-config.sh
```

Add:

```
#!/bin/bash

# Output file
OUTPUT="dinstar-uc120.ovpn"
SERVER_IP="YOUR_SERVER_PUBLIC_IP"  # CHANGE THIS

# Base configuration
cat > $OUTPUT <<EOF
client
dev tun
proto udp
remote $SERVER_IP 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-GCM
auth SHA256
key-direction 1
compress lz4-v2
verb 3

EOF

# Add certificates
echo "<ca>" >> $OUTPUT
cat ~/easy-rsa/pki/ca.crt >> $OUTPUT
echo "</ca>" >> $OUTPUT

echo "<cert>" >> $OUTPUT
cat ~/easy-rsa/pki/issued/dinstar-uc120.crt >> $OUTPUT
echo "</cert>" >> $OUTPUT

echo "<key>" >> $OUTPUT
cat ~/easy-rsa/pki/private/dinstar-uc120.key >> $OUTPUT
echo "</key>" >> $OUTPUT

echo "<tls-auth>" >> $OUTPUT
cat ~/easy-rsa/pki/ta.key >> $OUTPUT
echo "</tls-auth>" >> $OUTPUT

echo "Client configuration created: $OUTPUT"
```

4.9.4 Make Executable and Run

```
chmod +x ~/create-client-config.sh
# Edit the script to add your server IP
nano ~/create-client-config.sh
# Run the script
~/create-client-config.sh
```

---

5. Part 2: Dinstar UC120 Configuration

5.1 Access UC120 Web Interface

5.1.1 Connect to UC120

1. Open web browser
2. Navigate to UC120's local IP address: `http://192.168.x.x`
3. Login with administrator credentials

Default Credentials (if not changed): - Username: `admin` - Password: `admin`

⚠ **IMPORTANT:** Change default password immediately!

5.2 Navigate to OpenVPN Client Settings

5.2.1 Access VPN Menu

1. Click **Network** in top menu
2. Select **VPN** submenu
3. Click **OpenVPN**
4. Select **OpenVPN Client** tab

5.3 Configure OpenVPN Client

5.3.1 Basic Settings

Setting	Value	Notes
Config Mode	Import from File	Use .ovpn file
Status	Enable	Activate after configuration
Default Route	Disable	Unless UC120 should route all traffic via VPN
Accept Push Route	Disable	Manual route control

5.3.2 Import Configuration File

Method 1: Using .ovpn File

1. Click **Import from File** dropdown
2. Select `.ovpn` file option
3. Browse to `dinstar-uc120.ovpn` file created earlier
4. Click **Upload**

Method 2: Manual Configuration

If import doesn't work, configure manually:

Field	Value
Proto	UDP
Device	tun

Remote Server	Ubuntu Server Public IP
Port	1194
Auth Username	(leave blank if using certificates)
Auth Password	(leave blank if using certificates)

5.3.3 Upload Certificates

1. Navigate to **CA** tab
2. Upload `ca.crt`
3. Navigate to **Client Certificate** section
4. Upload `dinstar-uc120.crt`
5. Navigate to **Client Key** section
6. Upload `dinstar-uc120.key`

5.3.4 Save Configuration

1. Click **Save** button
2. Wait for configuration to apply
3. Enable the VPN connection

5.4 Verify Connection Status

5.4.1 Check Connection Status

1. Go to **Network** → **VPN** → **OpenVPN** → **Log**
2. Look for connection messages:
   - `Initialization Sequence Completed` ✓
   - `Peer Connection Initiated` ✓

5.4.2 Check Assigned IP

1. Navigate to **Status** → **System Info**
2. Look for VPN interface IP: Should show `10.8.0.2`

5.5 Configure Access Permissions

5.5.1 Enable Web Access via VPN

1. Go to **System** → **Management**
2. Enable HTTP/HTTPS access
3. Configure allowed source IPs (include 10.8.0.0/24)

---

6. Part 3: Testing and Verification

6.1 Test VPN Connection

6.1.1 From Ubuntu Server

```
# Check connected clients
cat /var/log/openvpn/openvpn-status.log

# Expected output should show:
# dinstar-uc120,10.8.0.2:port,bytes_recv,bytes_sent,timestamp
```

6.1.2 Ping Test from Ubuntu Server

```
ping -c 4 10.8.0.2
```

Expected: 4 packets transmitted, 4 received, 0% packet loss

6.1.3 Ping Test from UC120

From UC120 web interface: 1. Go to **System** → **Tools** → **Ping** 2. Target: `10.8.0.1` 3. Click **Ping**

Expected: Successful ping responses

6.2 Test Web Interface Access

6.2.1 Access via VPN

From Ubuntu Server or any machine connected to it:

```
# Create SSH tunnel
ssh -L 8080:10.8.0.2:80 root@your-ubuntu-server-ip
```

Then access from local browser:

```
http://localhost:8080
```

6.3 Test SIP/VoIP Functionality

6.3.1 Configure SIP Extension

1. On UC120, go to **Extension**
2. Create a test extension
3. Configure SIP client to connect via VPN

6.3.2 Test Call

1. Register SIP phone to UC120 via VPN
2. Make test call
3. Verify audio quality

6.4 Performance Testing

6.4.1 Bandwidth Test

```
# Install iperf3 on both sides
apt install iperf3 -y
```

```
# On Ubuntu Server
iperf3 -s

# From another terminal (simulating UC120 traffic)
iperf3 -c 10.8.0.2
```

6.4.2 Latency Test

```
# Monitor round-trip time
ping -c 100 10.8.0.2 | tail -1
```

Target: <50ms average latency for good VoIP quality

---

7. Security Hardening

7.1 Ubuntu Server Security

7.1.1 Disable Root SSH Login

```
nano /etc/ssh/sshd_config
```

Change:

```
PermitRootLogin no
```

Restart SSH:

```
systemctl restart sshd
```

7.1.2 Install Fail2Ban

```
apt install fail2ban -y
systemctl enable fail2ban
systemctl start fail2ban
```

Configure OpenVPN jail:

```
nano /etc/fail2ban/jail.local
```

Add:

```
[openvpn]
enabled = true
port = 1194
protocol = udp
filter = openvpn
logpath = /var/log/openvpn/openvpn.log
maxretry = 3
bantime = 3600
```

7.1.3 Enable Automatic Updates

```
apt install unattended-upgrades -y
dpkg-reconfigure --priority=low unattended-upgrades
```

7.2 UC120 Security

7.2.1 Change Default Credentials

1. **Immediately** change default admin password
2. Use strong password (minimum 12 characters, mixed case, numbers, symbols)

7.2.2 Disable Unused Services

1. Go to **System** → **Services**
2. Disable unnecessary protocols (Telnet, FTP if not needed)
3. Keep only required services enabled

7.2.3 Enable SIP Security

1. Configure SIP authentication
2. Enable SIP over TLS (SIPS) if supported
3. Use strong SIP extension passwords

7.2.4 Firmware Updates

1. Check for latest firmware on Dinstar website
2. Download and verify checksums
3. Apply updates during maintenance window

7.3 Network Security

7.3.1 Port Minimization

Only expose necessary ports: - 1194/UDP (OpenVPN only) - 22/TCP (SSH - consider changing default port)

7.3.2 IP Whitelisting

If accessing from known IPs, add whitelist rules:

```
# Allow SSH only from specific IPs
ufw delete allow 22/tcp
ufw allow from YOUR_OFFICE_IP to any port 22 proto tcp
```

7.3.3 Certificate Expiration Monitoring

Create monitoring script:

```
nano /usr/local/bin/check-cert-expiry.sh
```

Add:

```
#!/bin/bash
CERT="/etc/openvpn/server/server.crt"
DAYS_WARN=30
```

```
EXPIRY=$(openssl x509 -enddate -noout -in $CERT | cut -d= -f2)
EXPIRY_EPOCH=$(date -d "$EXPIRY" +%s)
NOW_EPOCH=$(date +%s)
DAYS_LEFT=$(( ($EXPIRY_EPOCH - $NOW_EPOCH) / 86400 ))

if [ $DAYS_LEFT -lt $DAYS_WARN ]; then
    echo "WARNING: Certificate expires in $DAYS_LEFT days!"
fi
```

Add to crontab:

```
chmod +x /usr/local/bin/check-cert-expiry.sh
crontab -e
```

Add:

```
0 9 * * * /usr/local/bin/check-cert-expiry.sh
```

---

8. Troubleshooting

8.1 Common Issues

8.1.1 VPN Connection Failed

Symptoms: - UC120 shows “Connection Failed” in VPN status - No connection in OpenVPN server logs

Diagnosis:

1. Check server logs:

   ```
   tail -f /var/log/openvpn/openvpn.log
   ```

2. Verify firewall:

   ```
   ufw status
   netstat -ulnp | grep 1194
   ```

3. Test connectivity:

   ```
   # From UC120's network, try to reach server
   telnet YOUR_SERVER_IP 1194
   ```

Solutions:

- **Firewall blocking:** Ensure UFW allows 1194/UDP
- **Wrong server IP:** Verify public IP in UC120 configuration
- **Port forwarding:** If Ubuntu server is behind NAT, configure port forwarding
- **Certificate mismatch:** Regenerate certificates if corrupted

8.1.2 Connection Established but No Routing

Symptoms: - VPN shows “Connected” - Cannot ping or access UC120 from server

Diagnosis:

```
# Check routing table
ip route

# Check VPN interface
ip addr show tun0

# Check OpenVPN status
systemctl status openvpn-server@server
```

Solutions:

- **IP forwarding disabled:**

  ```
  echo 1 > /proc/sys/net/ipv4/ip_forward
  ```

- **Routing rules missing:**

  ```
  # Add route manually
  ip route add 192.168.1.0/24 via 10.8.0.2
  ```

- **NAT not working:**

  ```
  # Check iptables
  iptables -t nat -L -v
  # Re-add masquerade rule
  iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
  ```

8.1.3 Certificate Errors

Symptoms: - "Certificate verification failed" - "TLS handshake failed"

Diagnosis:

Check UC120 logs for specific error messages.

Solutions:

- **Certificate expired:**

  ```
  # Check expiration
  openssl x509 -enddate -noout -in /etc/openvpn/server/server.crt
  ```

- **Wrong certificate:**
  - Verify you uploaded correct files to UC120
  - Regenerate and re-upload certificates
- **Time sync issue:**
  - Ensure both servers have correct time (NTP)

    ```
    timedatectl status
    ```

8.1.4 Poor VoIP Quality

Symptoms: - Choppy audio - Dropped calls - Echo or delay

Diagnosis:

```
# Check latency
ping -c 100 10.8.0.2

# Check packet loss
mtr -c 100 -r 10.8.0.2

# Check bandwidth
iperf3 -c 10.8.0.2
```

Solutions:

- **High latency:** Choose closer Linode datacenter
- **Bandwidth limitation:** Upgrade Linode plan
- **Compression:** Enable compression in OpenVPN config
- **QoS:** Implement traffic prioritization for VoIP

8.1.5 Cannot Access Web Interface

Symptoms: - VPN connected - Can ping UC120 - Cannot access web interface

Diagnosis:

```
# Test HTTP port
telnet 10.8.0.2 80
```

Solutions:

- **Firewall on UC120:** Check UC120 firewall settings allow VPN subnet
- **Wrong port:** Verify UC120 web interface port (may be 80, 443, or custom)
- **Access restrictions:** Configure UC120 to allow access from 10.8.0.0/24

8.2 Logging and Monitoring

8.2.1 Enable Detailed Logging

In `/etc/openvpn/server/server.conf`:

```
verb 4  # or 5 for even more detail
```

Restart service:

```
systemctl restart openvpn-server@server
```

8.2.2 Monitor Real-time Connections

```
watch -n 2 'cat /var/log/openvpn/openvpn-status.log'
```

8.2.3 Log Rotation

Create logrotate config:

```
nano /etc/logrotate.d/openvpn
```

Add:

```
/var/log/openvpn/*.log {
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    create 0640 root root
}
```

---

9. Appendix

9.1 Quick Command Reference

Ubuntu Server Commands

Task	Command
Check VPN status	`systemctl status openvpn-server@server`
Restart VPN	`systemctl restart openvpn-server@server`
View logs	`tail -f /var/log/openvpn/openvpn.log`
List connected clients	`cat /var/log/openvpn/openvpn-status.log`
Check routing	`ip route show`
Test connectivity	`ping 10.8.0.2`
Firewall status	`ufw status verbose`

Certificate Management

Task	Command
List certificates	`cd ~/easy-rsa && ./easyrsa show-cert server`
Revoke certificate	`./easyrsa revoke client-name`
Generate CRL	`./easyrsa gen-crl`
Check expiration	`openssl x509 -enddate -noout -in cert.crt`

9.2 Configuration File Templates

Minimal OpenVPN Server Config

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
server 10.8.0.0 255.255.255.0
keepalive 10 120
cipher AES-256-GCM
```

```
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Minimal Client Config (.ovpn)

```
client
dev tun
proto udp
remote SERVER_IP 1194
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
cipher AES-256-GCM
verb 3
```

9.3 Network Port Reference

Service	Port	Protocol	Purpose
OpenVPN	1194	UDP	VPN tunnel
SSH	22	TCP	Server management
HTTP	80	TCP	UC120 web interface
HTTPS	443	TCP	UC120 web interface (SSL)
SIP	5060	UDP/TCP	SIP signaling
RTP	10000-20000	UDP	Voice/video media

9.4 UC120 Default Settings

Parameter	Default Value
IP Address	192.168.1.1 (DHCP)
Username	admin
Password	admin
HTTP Port	80
HTTPS Port	443

9.5 Glossary

- **CA (Certificate Authority):** Entity that issues digital certificates
- **OpenVPN:** Open-source VPN protocol
- **PBX:** Private Branch Exchange (telephone switching system)
- **SIP:** Session Initiation Protocol (VoIP signaling)
- **TLS:** Transport Layer Security (encryption protocol)
- **TUN:** Network TUNnel device for VPN
- **UFW:** Uncomplicated Firewall (Ubuntu firewall frontend)

9.6 Additional Resources

- **Dinstar Official Website:** https://www.dinstar.com/
- **OpenVPN Documentation:** https://openvpn.net/community-resources/
- **Ubuntu Server Guide:** https://ubuntu.com/server/docs
- **Linode Documentation:** https://www.linode.com/docs/

9.7 Support Information

For technical support:

1. **Dinstar Support:** Contact manufacturer for UC120 specific issues
2. **Community Forums:** OpenVPN and Ubuntu community forums
3. **Linode Support:** For server infrastructure issues

9.8 Revision History

Version	Date	Changes
1.0	December 2025	Initial release

Legal Notices

Disclaimer: This documentation is provided “as is” without warranty of any kind. Always follow your organization’s security policies and consult with network security professionals before deploying production systems.

Trademarks: Dinstar, Ubuntu, and OpenVPN are trademarks of their respective owners.

End of Manual