Using Telnet or SSH to Configure the VPN 3002

1. Telnet or SSH to the IP address of the VPN 3002 private interface.
2. Follow Steps 3–5 in the "Using a Console Port to Configure the VPN 3002" section of this card.

LEDs on Front of Unit

LED	State	Explanation
PWR	green	Unit is on and has power.
	off	Unit is powered off.
SYS	flashing amber	Unit is performing diagnostics.
	solid amber	Unit has failed diagnostics.
	flashing green	DHCP or PPPoE negotiations in process.
	green	Unit is operational.
VPN	off	No VPN tunnel exists.
	amber	Tunnel has failed.
	green	Tunnel is established.

LEDs on Private and Public Interface Ports

Green	The interface is connected to the network.
Flashing amber	Data is traveling across the network.

What's Next?

You can configure the system in more detail. In the Main screen of the HTML interface, select **Configuration > Interfaces**. You can explore the VPN 3002 Administration and Monitoring functions, also from the Main screen.

For more information, see the *Cisco VPN 3002 Getting Started* and *Reference* publications. Also go to www.cisco.com, and click the Service and Support section. Find world-wide phone numbers for the Technical Assistance Center at http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

78-14746-01
DOC-7814746=

Cisco VPN 3002 Hardware Client Quick Start

These instructions explain how to install and configure the Cisco VPN 3002 using default values.

How to Start

Configure the VPN 3002 using one of the following:

- The VPN 3002 Hardware Client Manager HTML interface. You can use Microsoft Internet Explorer 4.0 or higher, or Netscape Navigator 4.5–4.7 or 6.0. Be sure to enable both JavaScript and cookies.
- A PC attached to the console port *or* Telnet *or* SSH.

At the central-site Concentrator, configure the connection as a client, *NOT* LAN-to-LAN. See "Settings on the VPN 3000 Series Concentrator" section.

Client Mode or Network Extension Mode?

The VPN 3002 operates in either Client—also called Port Address Translation (PAT)—mode or Network Extension mode. A summary of the differences follows:

Client/PAT Mode (the default)	Network Extension Mode
Easier to configure.	Two more steps to configure than Client mode.
All traffic from the VPN 3002 private network arrives on the private network of the central-site VPN Concentrator with a single source-IP address.	You must assign an IP address other than the default to the VPN 3002 private interface, and you must disable PAT mode.
The IP addresses of the computers on the VPN 3002 private network are hidden. You cannot ping or access a *device* on the VPN 3002 private network from the central site. But you can access the assigned IP address of the VPN 3002 from the central site.	Devices behind the VPN Concentrator have direct access to devices on the VPN 3002 private network only through the tunnel. You can ping or access a device on the VPN 3002 network from the central site.
VPN 3002 initiates tunnel, and always sends data before receiving data.	VPN 3002 initiates tunnel. Central site can send data first, but only if split-tunneling is disabled.
Some applications are incompatible with PAT mode.	

Using Default Values to Configure the VPN 3002

For the simplest configuration, Client/PAT mode, accept default values for all parameters that have defaults. Use the Quick Configuration menu; you can set parameters in any order. Your changes become the running configuration as soon as you make them, and the system automatically saves your changes at the Done screen.

For Either Client or Network Extension Mode

1. You must configure the IPSec parameters. You supply the following:
   - The public IP address of the VPN 3000 Series Concentrator to which this VPN 3002 connects. This is also called the IKE peer address.
   - IPSec group and user names and passwords. These must match the group and user names and passwords you set for this VPN 3002 on the Concentrator.
2. Configure an IP address on the public interface. *If you use DHCP to obtain an IP address for the public interface,* your ISP may require a hostname. Enter this hostname in the Public Interface parameter.
3. We strongly recommend that you change the admin password.

For Network Extension Mode You Must Also

1. Change the IP address of the private interface (Private Interface parameter).
2. Disable PAT (PAT parameter).

Settings on the VPN 3000 Series Concentrator

Configure the VPN Concentrator to which this VPN 3002 connects as follows:

1. Configure the connection as a client, *NOT* LAN-to-LAN.
2. Assign this VPN 3002 to a group. Configure group and user names and passwords. These must match the group and user names and passwords that you set on the VPN 3002.
3. If the VPN 3002 uses Client mode, enable a method of address assignment for the VPN 3002: DHCP, address pools, address from authentication server, or client specified.
4. If the VPN 3002 uses Network Extension mode:
   - Be sure that the subnet behind the VPN 3002 is routable from private networks behind the VPN Concentrator. You can use Reverse Route Injection on the VPN Concentrator if its private network uses RIP or OSPF, or you can configure a static route.
   - Check the box in the Allow Network Extension Mode parameter for the group to which the VPN 3002 belongs (HW Client tab).

Installing the VPN 3002

To install the Cisco VPN 3002 perform these tasks:

1. Use a LAN cable to connect the VPN 3002 public interface to your public network device or Ethernet hub or switch.
2. Connect the power cable between the VPN 3002 and a reliably grounded power outlet.
3. Configure the VPN 3002 using *one* of the following: a browser, console port, Telnet, or SSH.

Using a Browser to Configure the VPN 3002

1. Use a LAN cable to attach a PC to the private interface (3002) or switch (3002-8E) port.
2. Enter the default IP address for the private interface (192.168.10.1) in the browser Location or Address field.
3. At the VPN 3002 Login prompt, enter the login name **admin** and the default password **admin**. Click **Login**.
4. In the Main window, select **Quick Configuration** from the menu. Follow the online instructions for all subsequent screens. Note that to configure Network Extension mode, you must change the private interface IP address and disable PAT.
5. Click **Help** for context-sensitive online help. When you click Help, you also reach links for an online *Quick Configuration* guide that supplements this *Quick Start* card, and an online *Cisco VPN 3002 Reference* publication. These documents are available only online.

Using a Console Port to Configure the VPN 3002

1. Connect the RJ-45 serial cable to the console port on the back of the VPN 3002 to the COM1 or another serial port on the PC.
2. Configure a connection to COM1 with settings of 9600 bps, 8 data bits, No parity, 1 stop bit, and hardware flow control.
3. After the initialization and boot messages complete, press **Enter** until you see a login prompt. Enter the login name, **admin**, and the default password **admin**. Press **Return**.
4. Choose **Configuration**, then **Quick Configuration**.
5. Follow the online instructions for subsequent parameters. Be sure that your entries conform to the formats for current values, displayed in brackets after the prompt. Note that to configure Network Extension Mode, you must change the private interface IP address and disable PAT.