TREND MICRO™ Network VirusWall™ Enforcer 2500 Quick Start Guide

Trend Micro™ Network VirusWall™ Enforcer 2500 (NVWE) controls access to the corporate network to ensure that all devices-managed or unmanaged, local or remote-comply with corporate security policies before they connect. It prevents threats from entering the network by scanning devices for the most up-to-date security software and critical Microsoft patches.

Use this *Quick Start Guide* to get Network VirusWall Enforcer 2500 up and running on your network. To obtain more information on product features and configure more advanced settings, see the following documentation:

- Upgrade Guide—Helps you upgrade to Network VirusWall Enforcer 2500 from Network VirusWall 1.5 or 1.8.
- Getting Started Guide—Helps you plan for deployment and perform initial tasks.
- Administrator's Guide—Helps you configure all product features.
- Online help—Helps you configure all features and is accessible from the Web console. To access the online help, open the Web console and click the help icon .
- Readme—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

Note: Trend Micro recommends checking the corresponding link from the Update Center (http://www.trendmicro.com/download) for updates to the *Upgrade Guide*, *Getting Started Guide*, *Administrator's Guide*, Readme, and program file.

1 Open and inspect the Network VirusWall Enforcer 2500 carton

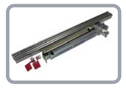
Please verify that the carton contains each of the following items:

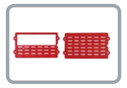

Network VirusWall Enforcer 2500


Power Cord


Ethernet Cable (RJ-45 Crossover)


Console Cable (RS-232)


Rack Accessories


PCI-X Slot Covers

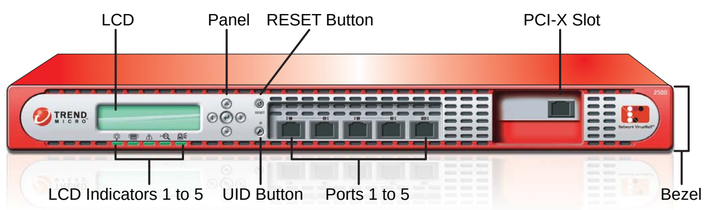

Solutions CD and Document Set

Contact Information

- Local offices: http://www.trendmicro.com/en/about/contact/us.htm
- Phone: + 1 (800) 228-5651 or + 1 (408) 257-1500
- Address: Trend Micro, 10101 N. De Anza Blvd, Cupertino, CA - 95014, USA

2 Understand Network VirusWall Enforcer 2500

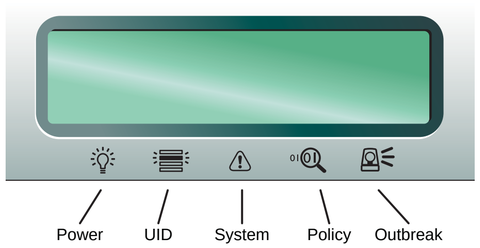
Network VirusWall Enforcer 2500 scans all inbound and outbound traffic.



Explanation of front panel items

The front panel of Network VirusWall Enforcer 2500 contains a Liquid Crystal Display (LCD), panel, ports, and LEDs. The following table describes each front panel element.

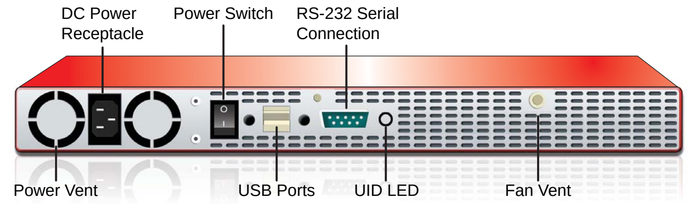
Element	Description
Liquid Crystal Display (LCD)	A 2.6 in x 0.6 in (65mm x 16mm) dot display LCD that is capable of displaying messages in 2 rows of 16 characters each.
Panel	5-button control panel that provides LCD navigation.
RESET Button	Resets the device.
LED Indicators 1 to 5	Indicates the POWER, UID, SYSTEM, POLICY, and OUTBREAK states. POWER and UID have one color each; SYSTEM, POLICY, and OUTBREAK have three colors each.
Ports 1,2,3,4,5	Copper Gigabit LAN port that you designate as the Management, Mirror, Sniffer, Regular, or Failover port. The Network VirusWall Enforcer documentation refers to each port by its number (for example, port 1 or 2).
UID Button	Unique ID button that illuminates the LED, which helps you locate a device for troubleshooting or maintenance.
PCI-X Slot	Slot for fiber, copper Ethernet, and accessory cards.
Bezel	Detachable casing that covers and protects the front panel.



Explanation of LED indicators

Network VirusWall Enforcer 2500 has five light-emitting diodes (LEDs) that indicate POWER, UID, SYSTEM, POLICY, and OUTBREAK status. The following table shows the possible behavior for each LED element.

LED	State	Description
Power	Yellow - steady	Device is operating normally.
	Off (no color)	Device is off.
UID	Blue - steady	The UID LED is illuminated because UID button is pressed.
	Blue - flashing	The Web console is sending the 'light on' command to turn on the UID LED.
	Off (no color)	The UID LED is not illuminated.
System	Red - flashing	Device is booting.
	Red - steady	Power-On Self-Test (POST) error.
	Yellow - flashing	Network VirusWall Enforcer program file (firmware) is starting.
	Yellow - steady	Network VirusWall Enforcer program file (firmware) encountered a critical error.
	Green - steady	Network VirusWall Enforcer program file (firmware) is ready.
Policy	Green - flashing	Network Scan, or Policy Enforcement is enabled.
	Yellow - steady	Failover mode is enabled. (Non Management) .
	Off (no color)	No multiple policy scan.
Outbreak	Green - steady	Outbreak Prevention Services (OPS) is disabled when Control Manager manages Network VirusWall Enforcer.
	Red - flashing	OPS is enabled.



Network Virus Wall Enforcer 2500 back

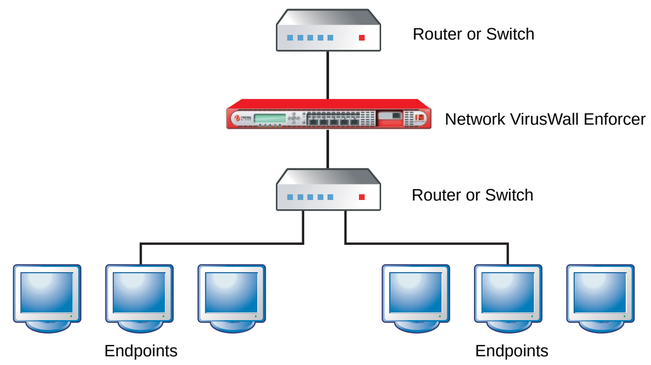
The back panel of Network VirusWall Enforcer 2500 contains a power receptacle, power switch, unused USB ports, serial connection, and fan vent.

Element	Description
DC Power Receptacle	Connects to the power outlet and the device using the power cord.
Power Switch	Powers the device on and off.
RS-232 Serial Connection	Connects to computer's serial port with an RS-232 type connection to perform preconfiguration.
Fan Vent	Cooling vent for 5 system fans.
Power Vent	Cooling vent for the power receptacle.
UID LED	LED at the back panel of a Network VirusWall Enforcer device. When you press the UID button the UID LED illuminates. The illuminated UID LED allows you to easily locate the device for troubleshooting or maintenance.
USB Ports	USB ports, reserved for future releases.

3 Decide the network configuration

Before proceeding with the Network VirusWall Enforcer 2500 setup, decide how to integrate the device into your network and determine which topology it will support. Position Network VirusWall Enforcer 2500 between layer 2 (L2) or layer 3 (L3) devices to scan all packets entering and leaving that section of the network.

Identify segments of your network to protect by considering which kinds of endpoints may introduce viruses or violate security policies. Also, consider the location of resources that are critical to your organization. Policies are applied based on the trigger criteria that the endpoint matches. Once an endpoint matches the trigger criteria of one policy, only that policy is applied to the endpoint.



TREND MICRO™ Network VirusWall™ Enforcer 2500 Quick Start Guide

Hardware Setup

Use the chart below to prepare the network values for which Network VirusWall Enforcer 2500 will prompt you.

Value	Your Answer
IP address	
Netmask	
Default gateway	
DNS server 1	
DNS server 2	
VLAN	

To register Network VirusWall Enforcer 2500 to Trend Micro Control Manager, you need to prepare additional Control Manager specific information. Refer to Appendix B in the *Administrator's Guide* for more information about Control Manager and instructions on registering Network VirusWall Enforcer 2500 to Control Manager.

4 Mount the Network VirusWall Enforcer 2500 device

Mount the Network VirusWall Enforcer 2500 device in a standard, 19-inch four-post rack cabinet, or on any stable surface as a freestanding device. Instructions can be found in the *Getting Started Guide*, which is available in print, on the Network VirusWall Enforcer 2500 CD, and from the Trend Micro Update Center.

When mounting the device, be sure to allow at least two inches clearance in all directions for cooling.

5 Prepare the Preconfiguration console

The computer you choose for preconfiguration must have HyperTerminal.

To prepare the Preconfiguration console:

1. Connect one end of the included console cable to the CONSOLE port on the back panel of the device and the other end to the serial port (COM1, COM2, or other COM port) on a computer.
2. Open HyperTerminal:
   - **a.** Click **Start > Programs > Accessories > Communications > HyperTerminal**. HyperTerminal prompts you for location information.
   - **b.** Click **Cancel** when prompted for dial-up location information.
   - **c.** Type the information and press **Enter** to enter information in the terminal interface.

   Tip: Trend Micro recommends configuring HyperTerminal properties so that the backspace key is set to delete.
   - **d.** On the HyperTerminal window, click **File > Properties**.
   - **e.** Click the **Settings** tab.
   - **f.** Under Backspace key sends, select **Del**.
3. To prepare HyperTerminal for optimal use, set the following properties:
   - Bits per second: 115200
   - Data Bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
   - Emulation: VT100

6 Log on to the Preconfiguration console

After preparing the terminal application, you are ready to access the Preconfiguration console.

To log on to the Preconfiguration console:

1. Power on the device and wait for a welcome message to appear on the LCM panel (approximately 1-2 minutes).

   To power-on a device:
   - **a.** Connect the power cord to the DC power receptacle.
   - **b.** Connect the power cord to an electrical outlet.

   Tip: See Power Requirements and Environmental Specifications in the *Getting Started Guide* for power requirements and environmental specifications.
   - **c.** Push the power switch to the **On** position. The Welcome message appears when the system is successfully powered on.
2. Press Enter. The **User name** logon prompt displays. If the screen does not display, type Ctrl + 'r' or Ctrl + 'l'.
3. Type the default administrator user name and its corresponding password:

   User name: admin
   Password: admin
   Use this login for full access to all preconfiguration features.
4. After logging on, the **Main Menu** appears.

7 Configure device settings

You can quickly assign Network VirusWall Enforcer 2500 a fixed IP address using the Preconfiguration console. You will need the information you prepared in step 3.

To configure device settings:

1. On the **Main Menu** of the Preconfiguration console, type 2 to select **Device Settings**. The Device Setting Summary appears.

   Note: When configuring the device for the first time, the factory default settings appear.
2. Type a host name that properly represents the device in the network.
   Trend Micro recommends a unique descriptive host name to represent and identify the device or devices in a failover pair locally (through the front panel LCD module) or remotely (through the management console). Host names may be up to 30 alphanumeric characters (spaces not allowed).
3. Type or select the Management IP setting details under Management IP settings.

   WARNING!
   If there is a NAT device in your environment, Trend Micro recommends assigning a static IP address to the device. Because different port settings are assigned from your NAT, your device may not work properly if dynamic IP addresses are used.
4. After specifying the device settings, select **Return to main menu** and press **Enter**.
5. Select **Save and log off**. A confirmation message displays.
6. Click **OK**.

You can register Network VirusWall Enforcer 2500 to Trend Micro Control Manager from the Device Settings screen. Refer to the *Administrator's Guide* for more information.

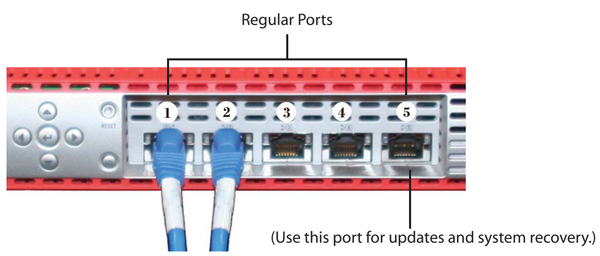
8 Connect Network VirusWall Enforcer 2500 to your test network

After preconfiguration, you must switch off the device before connecting it to the network.

To connect Network VirusWall Enforcer 2500 to your network:

1. Connect one end of a 10/100Mbps Ethernet cable to a REGULAR port and the other to a segment of your network.
2. In a failover deployment, establish the failover pair by connecting the provided Ethernet cable (RJ-45 crossover or a regular LAN cable) to the designated failover port of both devices.
3. Power on the device.

Note: Network VirusWall Enforcer 2500 can handle various interface speed and duplex mode network traffic. See the *Getting Started Guide* for more information.



3. Hardware configuration is now complete. To test the hardware setup and complete the configuration, relocate to a computer with access to the device and open a Web browser. Type the IP address of the device to access the Web console.

9 Log on to the Web console and change the default passwords

Network VirusWall Enforcer 2500 ships with three default accounts - admin, poweruser, and operator. All three accounts use admin, poweruser, and operator, respectively, as their default password. Change the default passwords of these accounts to prevent unauthorized access.

Open the Web console from a desktop or laptop on the network that can access the device (and is running Internet Explorer version 6.0 or later).

To change default passwords:

1. Type the Network VirusWall Enforcer 2500 IP address in your Web browser's address field:
   `http://[IP Address]`
   where `[IP Address]` is the IP you just assigned.
2. Type the default administrator user name and its corresponding password:
   User name: admin
   Password: admin

3. From the main menu, click **Administration > Administrative Accounts**.
4. Click a **User ID**. The Edit Administrative Account screen displays.
5. Type a new password for the account next to **Password**. Repeat this step next to **Password confirm**.
6. Click **Save**.

Change the passwords for each of the three default accounts.

10 Default Policy

Network VirusWall Enforcer 2500 allows you to create multiple policies directed at different types of endpoints and traffic. Network VirusWall Enforcer 2500 follows a first-match rule. **This means that once Network VirusWall Enforcer 2500 matches a policy to an endpoint, the device will no longer search for further matches to the endpoint down the policy list**. So, the device only applies the first policy that matches the endpoint.

Once you have set up Network VirusWall Enforcer 2500, there is one active default sample policy that matches any source and any destination. Following the first-match rule, if you want to use the default sample policy for testing purposes, prioritize policies with very specific settings higher than the default sample policy. Otherwise, the broad settings for the default sample policy may prevent endpoints from matching new policies with very specific settings and those policies will never apply. Refer to the *Administrator's Guide* for more information about policy enforcement.

11 Test and finish setting up Network VirusWall Enforcer 2500

Trend Micro recommends that you update the pattern files and test your installation to confirm that it works. Instructions for these and other important tasks are described in the *Getting Started Guide* and *Administrator's Guide*.