TREND MICRO™ Network VirusWall™ Enforcer 1500i (CR100 Series)

Quick Start Guide

Trend Micro™ Network VirusWall™ Enforcer 1500i controls access to your 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 up and running on your network. To obtain more information on product features and advanced settings, see the following documentation:

- Dell™ Product Information Guide—this printed document provides safety, environmental, and regulatory information about the device. Read the safety information in this document before using Network VirusWall Enforcer.
- Readme—a text file on the USB flash drive, the Readme covers basic getting started instructions, new features, known issues, and late-breaking information.
- Installation and Deployment Guide—provided on the USB flash drive, this PDF document describes installation, planning, deployment, and initial configuration.
- Administrator's Guide—also in the USB flash drive, this PDF document contains a comprehensive overview of Network VirusWall Enforcer. It also provides detailed configuration and management information.

For the latest versions of Network VirusWall Enforcer documents, visit the Trend Micro Update Center at *http://www.trendmicro.com/download*.

1 Open and inspect the package.

Your package should include the following items:

Device with bezel

Power cord

Rack kit

Documents and USB drive

If there are any items missing in your package, please contact your Trend Micro sales representative.

2 Understand the device interface.

Review the physical interface of your Network VirusWall Enforcer device.

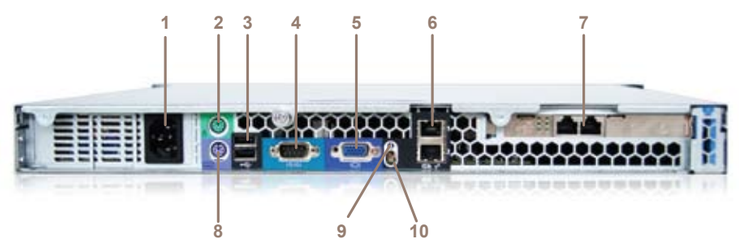
Front panel

The front panel provides a quick way to connect a keyboard and a VGA monitor to the device.

Item	Icon	Component
1	⏻	Power-on indicator, power button
2	⇐	USB 2.0 connectors
3		Video connector
4		Diagnostic indicators (4) for troubleshooting hardware-related issues with support
5		Nonmaskable interrupt (NMI) button for troubleshooting software and driver issues with support
6		Hard drive activity indicator
7		Device identification button for locating the device in a rack
8		Device status indicator is blue during normal operation and amber when there are hardware issues

Back Panel

The back panel contains all the network interface ports. These ports are grouped into the management interface ports and the data interface ports.



Item	Icon	Component
1		Power supply connector
2		PS/2 mouse connector
3	⇐	USB 2.0 connectors
4		Serial connector
5		Video connector
6		Onboard Ethernet ports (management interface)
7		Expansion card ports using a Silicom™ LAN bypass server adapter card (data interface)
8		PS/2 keyboard connector
9		Device status indicator is blue during normal operation and amber when there are hardware issues
10		Device identification button for locating the device in a rack

3 Plan your deployment.

Decide how to integrate the device into your network and determine which topology it will support. Position Network VirusWall Enforcer between layer 2 and layer 3 switches 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.

Network Settings

As part of your deployment planning, prepare the network settings that the devices should use to successfully connect to your network and scan packets.

Setting	Value
IP Address	
Netmask/Prefix Length	
Default gateway	
DNS Server 1	
DNS Server 2	
VLAN	

Note: *If you are connecting Network VirusWall Enforcer to a dual-stack network, you need to supply IPv4 and IPv6 addresses.*

TREND MICRO™
Network VirusWall™ Enforcer
1500i (CR100 Series)

Quick Start Guide

4 Mount the device.

Mount the Network VirusWall Enforcer device to a standard 19-inch four-post rack cabinet or place it on a stable surface as a freestanding device. When mounting the device, allow at least two inches clearance in all directions for cooling. For detailed instructions, see the *Installation* and *Deployment Guide*.

After mounting the device, attach a VGA monitor and a keyboard to the device. These peripherals will allow you to access the Preconfiguration console, where you can configure the device for network connection and remote management.

5 Log on to the Preconfiguration console.

Important: Before connecting the device to a power source, see the safety information in the *Dell Product Information Guide* and the device specifications in the *Installation* and *Deployment Guide*.

To log on to the Preconfiguration console:

1. Power on the device and the attached VGA monitor. A few minutes after powering on the device, the attached monitor will display the Preconfiguration console. If the console does not display, press CTRL+R.
2. To get full access to the Preconfiguration console, type the default administrator user name and password.
   User name: admin
   Password: admin

6 Configure the device.

You can quickly assign Network VirusWall Enforcer 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, select **Device Settings**.
2. Type a host name that properly represents the device in the network.
3. Type or select the necessary IP address settings.
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**.

Note: *You can register Network VirusWall Enforcer to Trend Micro Control Manager™ from the Preconfiguration console. For additional information about Control Manager and connecting the device to your network, see the Administrator's Guide.*

7 Connect the device to the network.

After performing initial configuration, connect the device to your network.

To connect Network VirusWall Enforcer to your network:

1. Disconnect the device from its power source.
2. Connect one end of a network cable to a port in the data interface and the other to a segment of your network.
3. Reconnect the device to a power source and power it on.

Note: *For information on selecting the right ports and specifying interface speeds and duplex modes, see the Installation and Deployment Guide.*

8 Log on to the Web console and change the default passwords.

Secure the console by immediately changing the passwords to the default "admin" and "poweruser" accounts.

To log on to the console and change the passwords:

1. Open the Web console from a computer that can access the device. To do this, go to the following URL using Internet Explorer 6.0 or later:

   ```
   http://<Device IP address>
   ```

   Note: *When specifying an IPv6 address as part of a URL, enclose the IPv6 address in square brackets.*

2. Log on to the Web console using the default "admin" account.
   User name: admin
   Password: admin
3. Click **Administrative Accounts** in the **Administration** menu.
4. Click the name of the account to edit.
5. Type the new password and retype it for confirmation.

   Note: *Use passwords that are at least 8 characters long and a combination of upper and lower case letters, numbers, punctuation marks, and other special characters. Avoid using words in the dictionary, names, and dates.*

6. Click **Save**.

9 Activate and update the device.

Ensure that the device can connect to the Internet and then activate your license. After activation, you will be able to perform updates.

To activate and update your device:

1. If necessary, configure proxy server settings so the device can connect to the Internet. Click **Proxy Settings** in the **Administration** menu.
2. Activate the device license. Click **Product License** in the **Administration** menu.
3. If you are using a Control Manager server as a local update server, specify the URL of the server so the device can download updates from this server. Click **Update Source** in the **Updates** menu.
4. Perform an update of Network VirusWall Enforcer pattern and program files. Click **Manual** in the **Updates** menu. You may need to reset the device after the update.
5. Schedule automatic pattern and engine updates. Click **Scheduled** in the **Updates** menu.

10 Define your own policies and test your deployment.

After updating components, you can create multiple policies directed at different types of endpoints and traffic. You can define policies for different IP address ranges, ports, and users. If you have multiple policies, only the first policy that matches an endpoint will apply to the endpoint. During policy creation, you will also need to define how you will deploy the Threat Management Agent and how often endpoints are assessed for compliance.

To get a better understanding of component updates and policy enforcement, consult the *Administrator's Guide*.

Item Code: NVEQ34451/100419