

NetVanta 2630 Series

Getting Started Guide

NETWORK SECURITY APPLIANCE

ADURAN[®]

ADTRAN NetVanta 2630 Series Getting Started Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the ADTRAN NetVanta 2630 series appliance.

Document Contents

This document contains the following sections:

- 1 [Setting Up Your Network](#) - page 1
- 2 [Registering Your Appliance](#) - page 9
- 3 [Enabling Security Services](#) - page 13
- 4 [Advanced Network Configuration](#) - page 21
- 5 [Advanced Deployments](#) - page 33
- 6 [Product Safety and Regulatory Information](#) - page 53

NetVanta 2630 Series Front Panel

LAN/WAN Port Status

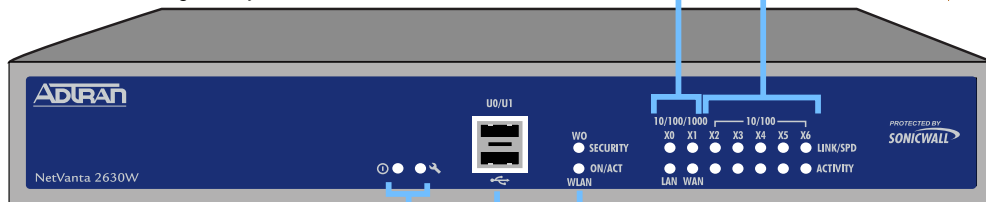
Provides dedicated LAN/WAN port status as follows:

- link/spd:**
- Off=10M
 - Green=100M
 - Amber=1,000M
- activity:**
- Solid=link
 - ✱ Blinking=activity

10/100 Ethernet Port Status

Provides Ethernet port status as follows:

- link/spd:**
- Off=10M
 - Green=100M
 - Amber=1,000M
- activity:**
- Solid=link
 - ✱ Blinking=activity



Indicator LEDs

Provides power and test status
(refer to page iv)

USB Ports

For future applications

Wireless LAN Status

(Wireless version only)

Provides Ethernet port status as follows:

- security:**
- Off=no activity
 - ✱ Blinking=activity
- on/act:**
- Off=wireless radio off
 - Solid=wireless radio on

NetVanta 2630 Series Rear Panel

WAN Port (X1)

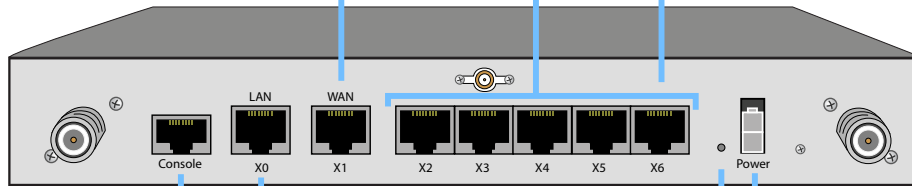
Provides dedicated WAN (Internet)

Ethernet Ports (X2-X6)

Provides configurable 10/100 Ethernet ports for connection to network devices on WAN, LAN, DMZ, and other zone types

HA Ethernet Port (X6)

Provides 10/100 Ethernet port for high availability (HA) connectivity



Console Port

Provides access to the Command Line Interface (CLI) via the DB9 -> RJ45 cable

LAN Port (X0)

Provides dedicated LAN access to local area network resources

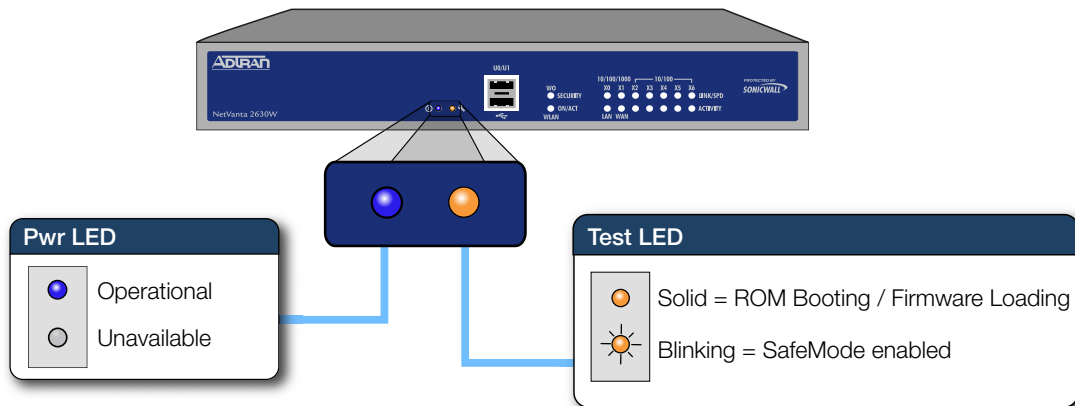
Power Supply

Provides power connection using supplied power cable

Reset Button

Press and hold to manually reset the appliance to SafeMode

NetVanta 2630 Series LED Reference



In this Section:






This section provides pre-configuration information. Review this section before setting up your ADTRAN NetVanta 2630 series appliance.

- [System Requirements - page 2](#)
- [Recording Configuration Information - page 2](#)
- [Completing the Setup Wizard - page 4](#)
- [Accessing the Management Interface - page 4](#)
- [Verifying WAN \(Internet\) Connectivity - page 5](#)
- [Connecting Your Network Devices - page 5](#)
- [Troubleshooting Initial Setup - page 6](#)

System Requirements

Before you begin the setup process, verify that you have:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads. Supported browsers include the following:

	Supported Browsers	Browser Version Number
	Internet Explorer	6.0 or higher
	Firefox	2.0 or higher
	Netscape	9.0 or higher
	Opera	9.10 or higher for Windows
	Safari	2.0 or higher for MacOS

Recording Configuration Information

Record the following setup information to use during the setup process and for future reference:

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your ADTRAN appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your ADTRAN appliance.

Networking Information

LAN IP Address: _____	Select a static IP address for your ADTRAN appliance that is within the range of your local subnet. If you are unsure, you can use the default IP address (192.168.168.168).
Subnet Mask: _____	Record the subnet mask for the local subnet where you are installing your ADTRAN appliance.
Ethernet WAN IP Address: _____	Select a static IP address for your Ethernet WAN. <i>This setting only applies if you are already using an ISP that assigns a static IP address.</i>

Administrator Information

Admin Name:	Select an administrator account name. (default is <i>admin</i>)
Admin Password:	Select an administrator password. (default is <i>password</i>)

Primary Internet Service Provider (ISP) Information

Record the following information about your current ISP:

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	<i>No Internet connection information is usually required, although some service providers require a host name.</i> Host Name: _____
Home DSL	PPPoE	User Name: _____ Password: _____ <i>Note: Your ISP may require your user name in the format: name@ISP.com</i>
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____ Subnet Mask: _____ Default Gateway (IP Address): _____ Primary DNS: _____ Secondary DNS (optional): _____
Dial-in to a server	PPTP	Server Address: _____ User Name: _____ Password: _____

Secondary ISP Information

Record the following information about your secondary ISP:

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	Host Name: _____
Home DSL	PPPoE	User Name: _____ Password: _____
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____ Subnet Mask: _____ Default Gateway (IP Address): _____ Primary DNS: _____ Secondary DNS (optional): _____
Dial-in to a server	PPTP	Server Address: _____ User Name: _____ Password: _____

Completing the Setup Wizard

The Setup Wizard takes you through several basic steps to get your ADTRAN NetVanta 2630 series appliance configured for your network. **Use the *Recording Configuration Information* section, on page 2 to record your configuration information as you complete the wizard.**



Note: *If you are having trouble accessing the Setup Wizard, see the *Troubleshooting the Setup Wizard* section, on page 6 of this document.*

The Setup Wizard guides you through the following steps:

Change Password—Create a new password so that only you have access to the management interface. The default password is “password.”

Change Time Zone—Select the correct time zone for proper updates and time-based functionality.

WAN Network Mode—Choose your method of connecting to the Internet. This information is provided by your Internet Service Provider (ISP).

WAN Settings—Required for some WAN modes. This information is also provided by your ISP.

LAN Settings—Enter custom local network address settings, or use the default values, which work well for most networks.

LAN DHCP Settings—Allow your ADTRAN NetVanta 2630 series appliance to automatically connect other local computers by specifying a DHCP range, or use the default.


Ports Assignment—Configure the extra interfaces (X2-X6) for different network requirements.

At the end of the wizard, a configuration summary displays. It is recommended that you record this information in the *Recording Configuration Information* section, on page 2 of this guide.

After the Setup Wizard completes, the appliance may reboot. Please wait a few minutes while the ADTRAN appliance reboots to save the updated firmware settings, and then continue with the next section of this guide.

Accessing the Management Interface

The computer you use to manage the ADTRAN NetVanta 2630 series appliance must be set up to connect using DHCP, or with a static IP address in your chosen subnet. The default subnet for LAN zone ports is 192.168.168.x.

If your ADTRAN NetVanta 2630 series appliance required a reboot after completing the Setup Wizard, wait until the  LED is no longer lit before continuing.

To access the Web-based management interface:

1. Enter the default IP address of **http://192.168.168.168**, or the LAN IP address you chose during the Setup Wizard, in the **Location** or **Address** field of your Web browser.



Tip: *If you changed the LAN IP of your ADTRAN during the Setup Wizard, you may need to **restart your computer** for changes to take effect.*

- When the ADTRAN Management Login page displays, enter your **username** and **password** (default values are "admin" for user name and "password" for password).

If the **System > Status** page displays, then you have correctly configured the ADTRAN NetVanta 2630 series appliance to work with the computer on your LAN.

Verifying WAN (Internet) Connectivity

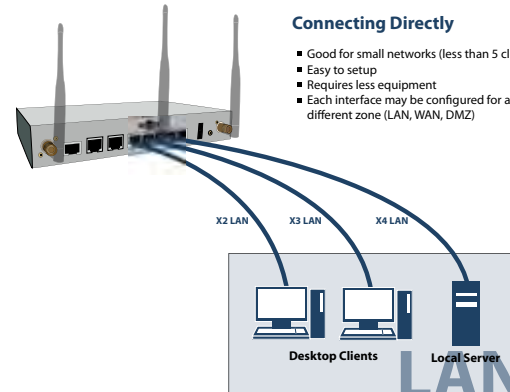
Complete the following steps to confirm your Internet connectivity:

- In the Windows interface, launch your Web browser.
- Enter "http://www.adtran.com" in the address bar and press **Enter** on the keyboard. The ADTRAN website displays. If you are unable to browse to a Website, see "Troubleshooting Internet Connection" on page 6.

Connecting Your Network Devices

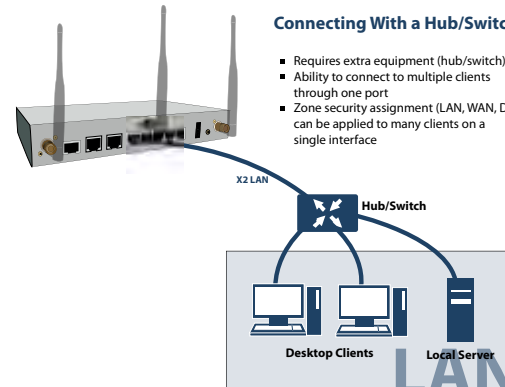
Connecting Directly

- Good for small networks (less than 5 clients)
- Easy to setup
- Requires less equipment
- Each interface may be configured for a different zone (LAN, WAN, DMZ)



Connecting With a Hub/Switch

- Requires extra equipment (hub/switch)
- Ability to connect to multiple clients through one port
- Zone security assignment (LAN, WAN, DMZ) can be applied to many clients on a single interface



Troubleshooting Initial Setup

This section provides troubleshooting tips for the following initial setup topics:

- [Troubleshooting the Setup Wizard](#) - page 6
- [Troubleshooting Internet Connection](#) - page 6
- [Configuring DHCP IP Addressing](#) - page 7

Troubleshooting the Setup Wizard

- **If you see the login screen, but not the Setup Wizard:**
 - Configure your Web browser to allow pop-ups.
 - Log into the security appliance using “**admin**” as the user name and “**password**” as the password. After you log in, click the **Wizards** button at the top right.
- **If you do not see the login screen or the Setup Wizard, verify the following:**
 - Did you correctly enter the NetVanta 2630 series appliance management IP address, *192.168.168.168*, in your Web browser?
 - Is your computer set to accept DHCP addressing or set to a static IP address within the 192.168.168.x subnet range? If not, see the *Configuring DHCP IP Addressing* section, on page 7 for instructions.
 - Is the Ethernet cable connected between your computer and the LAN (X0) port on your appliance?

- Do you need to add the ADTRAN appliance to your list of trusted sites in your Web browser? Use the default IP address (192.168.168.168) for this.
- Is the Test LED on the front panel of your ADTRAN appliance lit? If the Test LED stays lit for more than a few minutes after the initial power on sequence, power cycle the ADTRAN appliance.

Troubleshooting Internet Connection

If you can view the ADTRAN home page, you have configured your ADTRAN NetVanta 2630 series appliance correctly. If you cannot view the ADTRAN home page, try the following:

- **Renew your management station DHCP address** if you changed the IP address/subnet of your network during setup.
- **Restart your management station** to accept new network settings from the DHCP server in the ADTRAN appliance.
- **Restart your Internet router or modem** to communicate with the DHCP client in the ADTRAN appliance.
- **Log into the management interface** and launch the Setup Wizard again by clicking the Wizards button in the top right corner of the interface. Ensure that all of your settings are correct.

Configuring DHCP IP Addressing

If you are having trouble connecting to the ADTRAN NetVanta 2630 series appliance, complete the following section based on your Windows operating system flavor. Configure your management computer to obtain an IP address using DHCP.

Windows Vista

1. From the **Start** menu, right-click **Network** and select **Properties**.
2. In the **Tasks** menu, click **Manage network connections**. The Network Connections window displays.
3. Right-click on your **Local Area Connection** and select **Properties**.
4. In the list, double-click **Internet Protocol Version 4 (TCP/IP)**.
5. Select **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
6. Click **OK**, and then click **OK** again for the settings to take effect.

Windows XP

1. From the **Start** menu, highlight **Connect To** and then select **Show All Connections**.
2. Right-click on your **Local Area Connection** and select **Properties**.
3. In the list, double-click **Internet Protocol (TCP/IP)**.
4. Select **Obtain an IP address automatically** and **Obtain a DNS address automatically**.
5. Click **OK**, and then click **OK** again for the settings to take effect.

In this Section:

This section provides instructions for registering your ADTRAN NetVanta 2630 series appliance.

- [Creating a NetVanta Security Portal Account - page 10](#)
- [Registering and Licensing Your Appliance on NetVanta Security Portal - page 10](#)



Note: *Registration is an important part of the setup process and is necessary to receive the benefits of ADTRAN security services, firmware updates, and technical support.*

Creating a NetVanta Security Portal Account

A NetVanta Security Portal account is required for product registration. If you already have an account, continue to the *Registering and Licensing Your Appliance on NetVanta Security Portal* section.

Perform the following steps to create a NetVanta Security Portal account:

1. In your browser, navigate to www.adtran.com/NetVantaSecurityPortal.
2. In the login screen, click the [Not a registered user?](#) link.



User Login

Log in to manage your AdTran Security Services

(Username/Email)
(Password)

[Forgot Username?](#)
[Forgot Password?](#)
[Not a registered user?](#)

3. Complete the Registration form and click **Register**.

4. Verify that the information is correct and click **Submit**.
5. In the screen confirming that your account was created, click **Continue**.

Registering and Licensing Your Appliance on NetVanta Security Portal

This section contains the following subsections:

- [Product Registration - page 10](#)
- [Security Services and Software - page 10](#)
- [Activating Security Services and Software - page 12](#)
- [Trying or Purchasing Security Services - page 12](#)

Product Registration

You must register your ADTRAN security appliance on NetVanta Security Portal to enable full functionality.

1. Login to your NetVanta Security Portal account. If you do not have an account, you can create one at www.adtran.com/NetVantaSecurityPortal.
2. On the main page, type the appliance serial number in the **Register A Product** field. Then click **Next**.
3. On the My Products page, under **Add New Product**, type the friendly name for the appliance, select the **Product Group** if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**.

Security Services and Software

The Service Management - Associated Products page in NetVanta Security Portal lists security services, support options, and software that you can purchase or try with a free trial. For details, click the **Info** button.

If you purchased an appliance that is pre-licensed, you may be required to enter your activation key here unless current licenses are already indicated in the **Status** column with either a license key or an expiration date.

The following products and services are available for the ADTRAN NetVanta 2630 series appliances:

- **Gateway Service Bundles:**
 - Client/Server Anti-Virus Suite
 - Comprehensive Gateway Security Suite
- **Individual Gateway Services:**
 - Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention
 - Global Management System
 - Content Filtering: Premium Edition
 - High Availability Upgrade
- **Desktop and Server Software:**
 - Enforced Client Anti-Virus and Anti-Spyware
 - Global VPN Client
 - Global VPN Client Enterprise
 - ViewPoint
- **Support Services:**
 - Dynamic Support 8x5

- Dynamic Support 24x7
- Software and Firmware Updates

Activating Security Services and Software

If you purchase a service subscription or upgrade from a sales representative, you will receive an activation key. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase.

To activate existing licenses, perform the following tasks:

1. Navigate to the **My Products** page and select the registered product you want to manage.
2. Locate the product on the Service Management page and click **Enter Key** in that row.
3. In the Activate Service page, type or paste your key into the **Activation Key** field and then click **Submit**.

Once the service is activated, you will see an expiration date or a license key string in the **Status** column on the Service Management page.

Trying or Purchasing Security Services

To try a Free Trial of a service, click **Try** in the Service Management page. **To purchase a product or service**, click **Buy Now** in the Service Management page.

When activation is complete, NetVanta Security Portal displays an activation screen with service status and expiration information. The service management screen also displays the product you licensed.

[Gateway AV/Anti-Spyware/Intrusion Prevention](#)



Expiry: 11 Jun 2009

You have successfully registered your ADTRAN appliance. Now, you need to enable ADTRAN appliance security services. ADTRAN appliance security services are not enabled by default.

In this Section:

Security services are an essential component of a secure network deployment. This section provides instructions for registering and enabling security services on your ADTRAN NetVanta 2630 series appliance.

- [Enabling Security Services](#) - page 14
- [Verifying Security Services on Zones](#) - page 19

Enabling Security Services

After completing the registration process, perform the tasks listed below to activate your licenses and enable your licensed services from within the user interface.

ADTRAN security services are key components of threat management. The core security services are Gateway Anti-Virus, Intrusion Prevention Services, and Anti-Spyware.

You must enable each security service individually in the user interface. See the following procedures to enable and configure your security services:

- [Verifying Licenses](#) - page 14
- [Enabling Gateway Anti-Virus](#) - page 15
- [Enabling Intrusion Prevention Services](#) - page 16
- [Enabling Anti-Spyware](#) - page 17
- [Enabling Content Filtering Service](#) - page 18

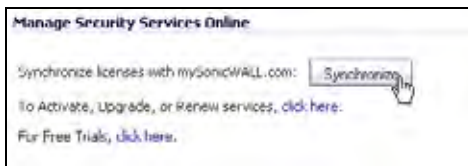
Verifying Licenses

Verify that your security services are licensed on the **System > Status** page.



If services that are already activated on NetVanta Security Portal do not display as licensed, you need to synchronize your ADTRAN with the licensing server.

If initial setup is already complete, click the **Synchronize** button to synchronize licenses from the **System > Licenses** page.



Enabling Gateway Anti-Virus

To enable Gateway Anti-Virus (GAV):


1. Navigate to the **Security Services > Gateway Anti-Virus** page.
2. Select the **Enable Gateway Anti-Virus** checkbox and click **Accept** to apply changes.



3. Verify that the **Enable Inbound Inspection** checkboxes are selected for the protocols you wish to inspect. See the following table for an explanation of these protocols.

The following table gives descriptions and default values for GAV-enforced protocols:

Protocol	Default	Description
HTTP	Enabled	Hyper-Text Transfer Protocol, common Web-browsing traffic
FTP	Enabled	File Transfer Protocol, dedicated file download servers
IMAP	Enabled	Internet Message Access Protocol, standard method for accessing email
SMTP	Enabled	Simple Mail Transfer Protocol, standard method for accessing email
POP3	Enabled	Post Office Protocol 3, standard method for accessing email
CIFS/Netbios	Disabled	Intra-network traffic on Windows operating system (network file-sharing)
TCP Stream	Disabled	Any other non-standard type of network data transfer

4. Click the **Accept**  button to apply changes.

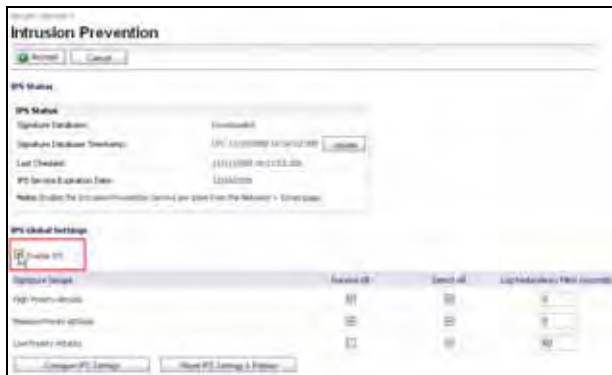
GAV contains many other useful features, including:

- **Outbound SMTP Inspection** scans outbound email
- **User Notification** notifies users when content is blocked
- **File-Type Restrictions** blocks various non-scannable files
- **Exclusion Lists** for network nodes where Gateway Anti-Virus enforcement is not necessary.


Enabling Intrusion Prevention Services

To enable Intrusion Prevention (IPS):

1. Navigate to the **Security Services > Intrusion Prevention** page.
2. Select the **Enable Intrusion Prevention** checkbox.



3. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes based on attack priority.

 **Note:** *Prevent All blocks attacks of the chosen priority, and Detect All saves a log of these attacks that can be viewed on the Log > View page.*

4. Click the **Accept**  button to apply changes.

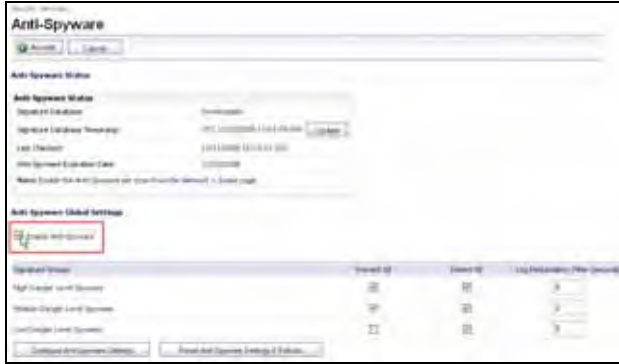
Intrusion Prevention contains other useful features, including:

- **Exclusion Lists** for network nodes where IPS enforcement is not necessary.
- **Log Redundancy** to control log size during high-volume intrusion attack attempts by enforcing a delay between log entries.


Enabling Anti-Spyware


To enable Anti-Spyware:

1. Navigate to the **Security Services > Anti-Spyware** page.
2. Select the **Enable Anti-Spyware** checkbox.



3. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes for each spyware danger level that you want to prevent.

 **Note:** *Prevent all blocks attacks of the chosen priority, Detect All saves a log of these attacks which can be viewed in the **Log > View** screen.*

4. Click the **Accept**  button to apply changes.

Anti-Spyware contains other useful features, including:


- **Exclusion Lists** excludes network nodes when Anti-Spyware enforcement is not necessary.
- **Log Redundancy** controls log size during high-volume intrusion attack attempts by enforcing a delay between log entries.
- **Clientless Notification** displays messages to users when content is blocked by ADTRAN Anti-Spyware.
- **Outbound Inspection** enables scanning and logging of outbound spyware communication attempts.
- **Disable SMTP Responses** suppresses the sending of email messages to clients when spyware is detected.

Enabling Content Filtering Service

To enable Content Filtering Service (CFS):

1. Navigate to the **Security Services > Content Filter** page.
2. Select **ADTRAN CFS** in the Content Filter Type drop-down list and then click the **Configure** button.



3. In the **Policy** tab, click the **Configure** button for the default policy. The Edit CFS Policy window displays.
4. In the **URL List** tab, review and select additional exclusion categories as needed.
5. Click **OK** in both pop-up windows.
6. Click the **Accept**  button to apply changes.

Content Filtering Service contains other useful features, including:

- **URL Rating Review** allows the administrator and users to review blocked URL ratings if they think a URL is rated incorrectly.
- **Restrict Web Features** restricts features such as cookies, Java, ActiveX, and HTTP Proxy access.
- **Trusted Domains** allows access to restricted features on trusted domains.
- **CFS Exclusion List** excludes administrators and/or IP ranges from content filtering enforcement.
- **Blocked Content Web Page** displays a custom HTML page to users when content is blocked.

Verifying Security Services on Zones

Security services such as Gateway Anti-Virus are automatically applied to the LAN and WAN network zones. To protect other zones such as the DMZ, you must apply the security services to the network zones.

To apply services to network zones:

1. Navigate to the **Network > Zones** page.



Name	Security Type	Member Interfaces	Security Tools	Content Filtering	Client AV	Gateway AV	AV Services	IPV	SD-WAN	Configure
LAN	Trusted	VL1, VL2, VL3, VL4, VL5, VL6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	Untrusted	V1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DMZ	Public	LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WIFI	Untrusted	WIFI	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WIRELESS	Untrusted	WIFI	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ADSL	Trusted	ADSL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. In the Zone Settings table, click the **Configure** icon for the zone where you want to apply security services.
3. In the **Edit Zone** dialog box on the **General** tab, select the checkboxes for the security services to enable on this zone.
4. Click **OK**.

Congratulations! Your ADTRAN NetVanta 2630 series appliance is registered and fully functional with active security services enabled.

For advanced network setup information, continue to:

- [Advanced Network Configuration](#) - page 21
- [Advanced Deployments](#) - page 33

In this Section:

This section provides detailed overviews of advanced deployment scenarios, as well as configuration instructions for connecting your ADTRAN NetVanta 2630 series appliance to various network devices.

- [An Introduction to Zones and Interfaces](#) - page 22
- [Configuring Interfaces](#) - page 23
- [Creating Network Access Rules](#) - page 26
- [Address Objects](#) - page 28
- [Network Address Translation](#) - page 30



Tip: *Before completing this section, fill out the information in [Recording Configuration Information](#) - page 2.*

An Introduction to Zones and Interfaces

Zones split a network infrastructure into logical areas, each with its own set of usage rules, security services, and policies. Most networks include multiple definitions for zones, including those for trusted, untrusted, public, encrypted, and wireless traffic.

Some basic (default) zone types include:

WAN—Untrusted resources outside your local network.

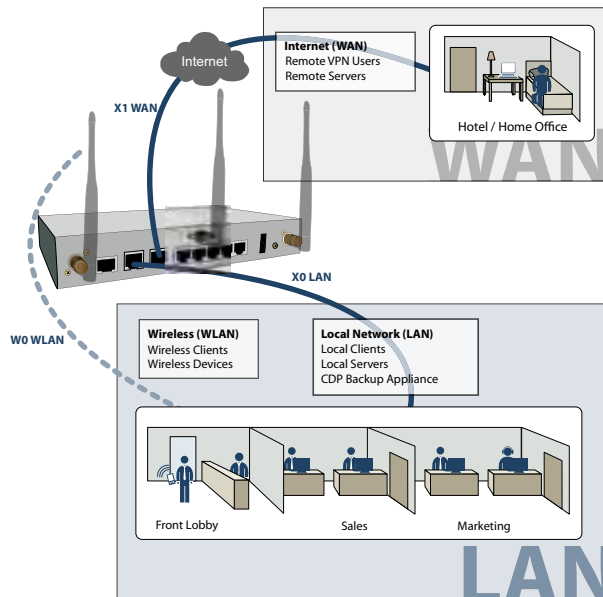
LAN—Trusted local network resources.f

DMZ—Local network assets that must be accessible from the WAN zone (such as Web and FTP servers).

VPN—Trusted endpoints in an otherwise untrusted zone, such as the WAN.


The security features and settings that zones carry are enforced by binding a zone to one or more physical interfaces (such as, X0, X1, or X2) on the ADTRAN NetVanta 2630 series appliance.

The X1 and X0 interfaces are preconfigured as WAN and LAN respectively. The remaining ports (X2-X6) are also LAN ports by default, however, these ports can be configured to meet the needs of your network, either by using basic zone types (WAN, LAN, DMZ, VPN) or configuring a custom zone type to fit your network requirements (Gaming Console Zone, Wireless Printer Zone, Wireless Ticket Scanner Zone, and more).



Configuring Interfaces

Interfaces, also known as ports, are physical network connections that can be configured to provide different networking and security features based on your network needs.

 **Note:** For more information on Zone types, see “An Introduction to Zones and Interfaces” on page 22.

This section contains the following sub-sections:

- [Configuring an Interface](#) - page 23
- [PortShield Wizard](#) - page 24
- [Manual PortShield Configuration](#) - page 25

Configuring an Interface

The Web-based management interface allows you to configure each individual Ethernet port (from X2-X6) with its own security settings through the use of zones.

To configure a network interface:

1. In the **Network > Interfaces** panel, click the **Configure** button for the interface you wish to configure. The Edit Interface window displays.



Note: If only X0 and X1 interfaces are displayed in the Interfaces list, click the **Show PortShield Interfaces** button to show all interfaces.



2. Select a **Zone Type** for this interface.
3. Select an **IP assignment** for this interface. If you intend to create a new network segment on this interface such as a DMZ or secondary LAN, this value should be set to **Static**.
4. Enter a static **IP Address** for the interface. For private and semi-private network segments, any private static IP address such as 10.10.20.1 is appropriate. Ensure that the static IP address you choose does not conflict with any currently existing interfaces. The newly created interface appears in the Interfaces list. You may now connect the appropriate network resources to this interface.

ID	Zone	IP Address	Subnet Mask	IP Assignment	Management
100	DMZ	10.10.20.1	255.255.255.0	Static	HTTP, HTTPS, Ping, SNMP, SSH

PortShield Wizard

With PortShield, multiple ports can share the network settings of a single interface. The PortShield feature enables you to easily configure the ports on the ADTRAN NetVanta 2630 series appliance into common deployments.



Tip: *Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.*

To configure ports using the PortShield Wizard:

1. Click the **Wizards** button on the top-right of the management interface.
2. Choose **PortShield Interface Wizard** and click Next.

3. Select from the following:

Selection	Port Assignment	Usage
WAN/LAN	X0, X2-X6: LAN X1: WAN	Connect any local network device to X0, or X2-X6 for local and Internet connectivity.
WAN/LAN/DMZ	X0, X3-X6: LAN X1: WAN X2: DMZ	Connect any local network device to X0, or X3-X6 for local and Internet connectivity. Connect public-facing servers or other semi-public resources to X2.

4. WAN/LAN or WAN/LAN/DMZ and click **Next** to continue. This will prompt a configuration summary to appear. Verify that the ports assigned are correct.
5. Click **Apply** to change port assignments.

Manual PortShield Configuration

You can also manually group ports together using the graphical PortShield Groups interface. Grouping ports allows them to share a common network subnet as well as common zone settings.

To manually configure a PortShield interface:


1. Navigate to the **Network > PortShield Groups** page.
2. Click one or more interfaces in the PortShield interface and then click the **Configure** button.



3. Select Enabled from the **Port Enable** drop-down menu.
4. Select the port with which you wish to group this interface from the **PortShield Interfaces** drop-down menu



Note: *Interfaces must be configured before being grouped with PortShield. For instructions, see the [Configuring an Interface](#) section, on page 23.*



Switch Port Settings	
Name:	X4
Port Enable:	Enabled
PortShield Interface:	X2
Link Speed:	Auto Negotiate

5. Click the **OK** button. Your new port groupings display as color-coded ports.



Creating Network Access Rules

A Zone is a logical grouping of one or more interfaces designed to make management a simpler and more intuitive process than following a strict physical interface scheme.

By default, the ADTRAN security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the ADTRAN security appliance:

Originating Zone	Destination Zone	Action
LAN	WAN, DMZ	Allow
DMZ	WAN	Allow
WAN	DMZ	Deny
WAN and DMZ	LAN	Deny

To create an access rule:

1. On the **Firewall > Access Rules** page in the matrix view, select two zones that will be bridged by this new rule.
2. On the Access Rules page, click **Add**.



The access rules are sorted from the most specific to the least specific at the bottom of the table. At the bottom of the table is the **Any** rule.



Note: *ADTRAN's default firewall rules are set in this way for ease of initial configuration, but do not reflect best practice installations. Firewall rules should only allow the required traffic and deny all other traffic.*

3. In the Add Rule page on the **General** tab, select **Allow** or **Deny** or **Discard** from the **Action** list to permit or block IP traffic.

The screenshot shows the 'Settings' window for an access rule. It has three tabs: 'General', 'Advanced', and 'QoS', with 'General' selected. The 'Settings' section includes the following fields:

- Action:** Radio buttons for Allow, Deny, and Discard.
- From Zone:** A dropdown menu with 'WAN' selected.
- To Zone:** A dropdown menu with 'LAN' selected.
- Service:** A dropdown menu with '--Select a service--' selected.
- Source:** A dropdown menu with '--Select a network--' selected.
- Destination:** A dropdown menu with '--Select a network--' selected.
- Users Allowed:** A dropdown menu with 'All' selected.
- Schedule:** A dropdown menu with 'Always on' selected.
- Comment:** A text input field.

At the bottom of the settings section, there are two checkboxes: Enable Logging and Allow Fragmented Packets. Below the settings is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

4. Configure the other settings on the **General** tab as explained below:
- Select the service or group of services affected by the access rule from the **Service** drop-down list. If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
 - Select the source of the traffic affected by the access rule from the **Source** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
 - Select the destination of the traffic affected by the access rule from the **Destination** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
 - Select a user or user group from the **Users Allowed** drop-down list.
 - Select a schedule from the **Schedule** drop-down list. The default schedule is **Always on**.
 - Enter any comments to help identify the access rule in the **Comments** field.

- Click on the **Advanced** tab.



- Configure the other settings on the **Advanced** tab as explained below:
 - In the **TCP Connection Inactivity Timeout (minutes)** field, set the length of TCP inactivity after which the access rule will time out. The default value is **15** minutes.
 - In the **UDP Connection Inactivity Timeout (minutes)** field, set the length of UDP inactivity after which the access rule will time out. The default value is **30** minutes.
 - In the **Number of connections allowed (% of maximum connections)** field, specify the percentage of maximum connections that is allowed by this access rule. The default is 100%.
 - Select **Create a reflexive rule** to create a matching access rule for the opposite direction, that is, from your destination back to your source.
- Click on the **QoS** tab to apply DSCP marking to traffic governed by this rule.
- Click **OK** to add the rule.

Address Objects

Address Objects are one of four object classes: Address, User, Service, and Schedule. Once you define an Address Object, it becomes available for use wherever applicable throughout the management interface. For example, consider an internal Web server with an IP address of 67.115.118.80.

Rather than repeatedly typing in the IP address when constructing Access Rules or NAT policies, you can create an Address Object to store the Web server's IP address. This Address Object, "My Web Server," can then be used in any configuration screen that employs Address Objects as a defining criterion.

Available Address Object types include the following:

- Host** – Define a single host by its IP address.
- Range** – Define a range of contiguous IP addresses.
- Network** – Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask.
- MAC Address** – Allows for the identification of a host by its hardware address.
- FQDN Address** – Fully Qualified Domain Names (FQDN) Address Objects allow for the identification of a host by its domain name, such as www.adtran.com.


Creating an Address Object

The **Network > Address Objects** page allows you to create and manage your Address Objects. You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** – displays all configured Address Objects.
- **Custom Address Objects** – displays Address Objects with custom properties.
- **Default Address Objects** – displays Address Objects configured by default on the ADTRAN security appliance.

To add an Address Object:

1. Navigate to the **Network > Address Objects** page.
2. Below the **Address Objects** table, click **Add**.
3. In the **Add Address Object** dialog box, enter a name for the Address Object in the **Name** field.



The screenshot shows a dialog box for adding an address object. It contains the following fields and controls:

- Name:** An empty text input field.
- Zone Assignment:** A dropdown menu with 'LAN' selected.
- Type:** A dropdown menu with 'Host' selected.
- IP Address:** An empty text input field.
- Status:** A text box displaying 'Ready'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

4. Select the zone to assign to the Address Object from the **Zone Assignment** drop-down list.
5. Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.
 - For **Host**, enter the IP address in the **IP Address** field.
 - For **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
 - For **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.
 - For **MAC**, enter the MAC address in the **MAC Address** field.
 - For **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.
6. Click **OK**.

Network Address Translation

The Network Address Translation (NAT) engine allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the ADTRAN security appliance has a preconfigured NAT policy to perform Many-to-One NAT between the systems on the LAN and the IP address of the WAN interface. The appliance does not perform NAT by default when traffic crosses between the other interfaces.

You can create multiple NAT policies on an appliance for the same object – for instance, you can specify that an internal server uses one IP address when accessing Telnet servers, and uses a different IP address for all other protocols. Because the NAT engine supports inbound port forwarding, it is possible to access multiple internal servers from the WAN IP address of the ADTRAN security appliance. The more granular the NAT Policy, the more precedence it takes.

Before configuring NAT Policies, you must create all Address Objects that will be referenced by the policy. For instance, if you are creating a One-to-One NAT policy, first create Address Objects for your public and private IP addresses.

Configuring NAT Policies

NAT policies allow you to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously. The following NAT configurations are available:

- Many-to-One NAT Policy
- Many-to-Many NAT Policy
- One-to-One NAT Policy for Outbound Traffic
- One-to-One NAT Policy for Inbound Traffic (Reflexive)
- One-to-Many NAT Load Balancing
- Inbound Port Address Translation via One-to-One NAT Policy
- Inbound Port Address Translation via WAN IP Address

This section describes how to configure a One-to-One NAT policy. One-to-One is the most common NAT policy used to route traffic to an internal server, such as a Web server. Most of the time, this means that incoming requests from external IP addresses are *translated* from the IP address of the ADTRAN security appliance WAN port to the IP address of the internal Web server. The following example configuration illustrates the use of the fields in the Add NAT Policy procedure. To add a One-to-One NAT policy that allows all Internet traffic to be routed through a public IP address, two policies are needed: one policy for the outbound traffic, and one policy for the inbound traffic.

To add the components of a One-to-One NAT policy, perform the following steps:

1. Navigate to the **Network > NAT Policies** page. Click **Add**. The **Add NAT Policy** dialog box displays.
2. For **Original Source**, select **Any**.
3. For **Translated Source**, select **Original**.
4. For **Original Destination**, select **X0 IP**.
5. For **Translated Destination**, select **Create new address object** and create a new address object using **WAN** for Zone Assignment and **Host** for Type.
6. For **Original Service**, select **HTTP**.
7. For **Translated Service**, select **Original**.
8. For **Inbound Interface**, select **X0**.
9. For **Outbound Interface**, select **Any**.
10. For **Comment**, enter a short description.
11. Select the **Enable NAT Policy** checkbox.
12. Select the **Create a reflexive policy** checkbox if you want a matching NAT policy to be automatically created in the opposite direction. This will create the outbound as well as the inbound policies.
13. Click **Add**.

In this Section:

The advanced deployments contained in this chapter are based on the most common customer deployments and contain best-practice guidelines for deploying your ADTRAN NetVanta 2630 series appliances. These deployments are designed as modular concepts to help in deploying your ADTRAN appliance as a comprehensive security solution.

- [Public Server on DMZ](#) - page 34
- [Configuring High Availability](#) - page 38
- [Multiple ISP / WAN Failover and Load Balancing](#) - page 46



Tip: *Before completing this section, fill out the information in the [Recording Configuration Information](#) section, on page 2.*

Public Server on DMZ

This section provides instructions for configuring your ADTRAN NetVanta 2630 series appliance to support a public Web server on a DMZ zone.

A Web server can be placed on the LAN by completing the server wizard, which creates the proper address objects and rules for safe access.

Many network administrators, however, choose to place the Web server on a DMZ, as it provides a dedicated Ethernet interface for added security and bandwidth management.

This section contains the following subsections:

- [Completing the Public Server Wizard - page 35](#)
- [Configuring a DMZ Zone - page 36](#)
- [Editing the Address Object - page 37](#)
- [Editing the Firewall Access Rule - page 37](#)

Completing the Public Server Wizard

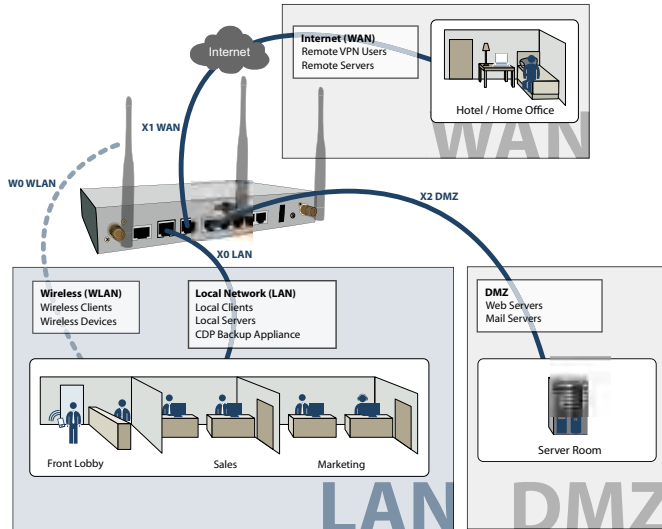
The Public Server Wizard guides you through a few simple steps, automatically creating address objects and rules to allow server access. To complete the public server wizard, perform the following steps:

1. Click the **Wizards** button in the upper right corner of the management interface to launch the wizard.
2. Select **Public Server Wizard** and click **Next** to continue.
3. Select **Web Server** as the server type and ensure that the **HTTP** and **HTTPS** services are selected.




Tip: *HTTPS is required for servers authenticating SSL or other HTTPS-supported encryption methods. If your server does not require encryption, you can de-select the HTTPS service.*

4. Enter a **Server Name** in the field that is easy to remember such as “My Web Server”. This name is for your reference and does not necessarily need to be a domain or address.
5. Enter the **Private IP Address** of your server. This is the IP address where the server will reside within the DMZ zone. If you do not have a DMZ configured yet, select a private IP address (such as 192.168.168.123) and write it down, you will need to refer to this later.
6. Enter a **Server Comment** (optional) and click **Next**.



7. Enter the **Server Public IP Address** in the field (normally your primary WAN IP address). This IP Address is used to access your Web server from the Internet.
8. Click **Next** and then click **Apply** to finish the wizard.

 **Note:** *If your server is on the LAN zone, you have completed the required steps for basic server access.*

If you wish to continue with an advanced DMZ zone configuration, turn to the [Configuring a DMZ Zone](#) section, on page 36.

Configuring a DMZ Zone

Since the public server is added to the LAN zone by default, configure a DMZ zone by performing the following steps:

1. In the **Network > Interfaces** panel, click the **Configure** button for the X2 interface. The Edit Interface window displays.

 **Note:** *If the X2 interface is not displayed in the Interfaces list, click the **Show PortShield Interfaces** button to show all interfaces.*



Interface 'X2' Settings

Zone: DMZ

IP Assignment: Static

IP Address: 192.168.168.1

Subnet Mask: 255.255.255.0

Comment:

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

2. Select DMZ as the **Zone Type**.
3. Select Static as the **IP assignment**.
4. Enter an **IP Address** for the interface. This IP address must be in the same subnet as your Web server's local IP address.



Tip: Since we used 192.168.168.123 in the example on page 35, use **192.168.168.1** as the DMZ interface IP.

The newly created DMZ interface appears in the Interfaces list.



Editing the Address Object

The address object that was automatically created must be changed from the LAN zone to DMZ zone.

1. On the **Network > Address Objects** page, click the configure button corresponds to your Web server object. In our case, the object is called “My Web Server Private”.

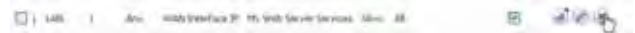
Name: My Web Server Private
 Zone Assignment: DMZ
 Type: Host
 IP Address: 192.168.168.123

2. Change the **Zone Assignment** to DMZ and click **OK**.

Editing the Firewall Access Rule

An access rule that allows traffic from the WAN zone to the server on the DMZ must be created, and the original WAN > LAN rule that was created by the Public Server Wizard should be deleted.

1. On the **Firewall > Access Rules** page, chose Drop-down Boxes as the **View Style**.
2. Select WAN as the **From Zone** and ALL as the **To Zone**, then click **OK**. All of the WAN-based access rules display.
3. Click the **Delete** button corresponding to the WAN My Web Server Services rule. Click **OK** when prompted.



4. On the **Firewall > Access Rules** page, click the **Add** button. The **Add Rule** window displays.
5. Configure the new rule as follows:

Selection	Port Assignment
Action	Allow
From Zone	WAN
To Zone	DMZ
Service	My Web Server Services. This service was automatically created during the Public Server Wizard and is named based on the Server Name you provided during setup.
Source	Any
Destination	WAN Interface IP. All traffic attempting to access your WAN IP address will be bound by this rule.
Users Allowed	All

Schedule	Always on, unless you choose to specify an uptime schedule such as "business hours only".
Comment	Leave a comment such as "Web server on DMZ"

6. Click **OK** to create this rule.
The new rule displays in the Access Rules table:



Configuring High Availability

This section provides instructions for configuring a pair of ADTRAN NetVanta 2630 series appliances for redundant High Availability (HA) networking.

This section contains the following subsections:

- [About High Availability](#) - page 39
- [Initial HA Setup](#) - page 39
- [HA License Synchronization Overview](#) - page 40
- [Associating Pre-Registered Appliances](#) - page 41
- [Disabling PortShield Before Configuring HA](#) - page 41
- [Configuring HA Settings](#) - page 42
- [Configuring Advanced HA Settings](#) - page 42
- [Configuring HA Monitoring](#) - page 44
- [Synchronizing Settings](#) - page 45
- [Verifying HA Functionality](#) - page 46

About High Availability

In this scenario, one ADTRAN NetVanta 2630 series appliance operates as the Primary gateway device and the other acts as the Backup. Once configured for High Availability, the Backup ADTRAN appliance contains a real-time mirrored configuration of the Primary ADTRAN appliance via an Ethernet link between the designated HA interfaces on each appliance.

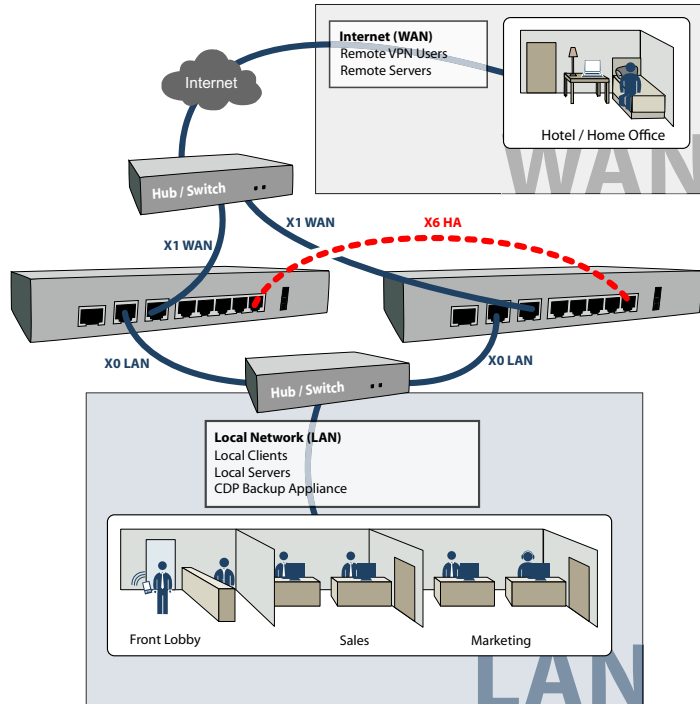
During normal operation, the Primary appliance is in Active mode and the Backup appliance is in Idle mode. If the Primary device loses connectivity, the Backup appliance transitions to Active mode and assumes the configuration and role of the Primary gateway device. This automatic failover ensures a reliable connection between the protected network and the Internet.

After a failover to the Backup appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated.

Initial HA Setup

Before you begin the configuration of HA on the Primary ADTRAN security appliance, perform the following setup:

1. On the back panel of the Backup ADTRAN security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability > Settings** page.
2. Verify that the Primary ADTRAN appliance is registered and licensed for the desired ADTRAN security services.



3. Associate the two ADTRAN appliances as HA Primary and HA Secondary on NetVanta Security Portal, for license synchronization.
4. Make sure the Primary ADTRAN and Backup ADTRAN security appliances' LAN, WAN and other interfaces are properly configured for failover.
5. Connect the **X6** ports on the Primary ADTRAN and Backup ADTRAN appliances with a CAT 5 Ethernet cable. The Primary and Backup ADTRAN security appliances must have a dedicated connection.
6. Power up the Primary ADTRAN security appliance, and then power up the Backup ADTRAN security appliance.
7. Do not make any configuration changes to the Primary's X6 interface; the High Availability configuration in an upcoming step takes care of this issue.

HA License Synchronization Overview

You can configure HA license synchronization by associating two ADTRAN security appliances as HA Primary and HA Secondary on NetVanta Security Portal. Note that the Backup appliance of your HA pair is referred to as the HA Secondary unit on NetVanta Security Portal.

You need only purchase a single license, a single Support subscription, and a single set of security services licenses for the HA Primary appliance. These licenses are shared with the HA Secondary appliance. See [Registering and Licensing Your Appliance on NetVanta Security Portal - page 10](#).

License synchronization is used during HA so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable HA, you can use the UI to configure your two appliances as a HA pair in Active/Idle mode.

NetVanta Security Portal provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. You can associate two units that are both already registered. Or you can select a registered unit and then add a new appliance with which to associate it.

Associating Pre-Registered Appliances

To associate two already-registered ADTRAN security appliances so that they can use HA license synchronization, perform the following steps:

1. Login to NetVanta Security Portal and click **My Products**.
2. On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the parent, or primary, unit. Click the product **name** or **serial number**.
3. On the Service Management page, scroll down to the Associated Products section.
4. Under Associated Products, click **HA Secondary**.
5. On the My Product - Associated Products page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the appliance that you want to associate as the secondary/backup unit.
6. Select the group from the **Product Group** drop-down list. The product group setting specifies the NetVanta Security Portal users who can upgrade or modify the appliance.
7. Click **Register**.

Disabling PortShield Before Configuring HA

The HA feature can only be enabled if PortShield is disabled on *all* interfaces of *both* the Primary and Backup appliances. You can disable PortShield either by using the **PortShield Wizard**, or manually from the **Network > PortShield Groups** page.

To use the PortShield Wizard to disable PortShield on each appliance, perform the following steps:

1. On one appliance of the HA Pair, click the **Wizards** button at the top right of the management interface.
2. In the **Welcome** screen, select **PortShield Interface Wizard**, and then click **Next**.
3. In the **Ports Assignment** screen, select **WAN/LAN/HA**, and then click **Next**.



4. In the **Configuration Summary** screen, click **Apply**.
5. In the **PortShield Wizard Complete** screen, click **Close**.
6. Log into the management interface of the other appliance in the HA Pair, and repeat this procedure.

Configuring HA Settings

After disabling PortShield on all interfaces of both appliances, the next task in setting up HA is configuring the **High Availability > Settings** page on the Primary ADTRAN security appliance. Once you configure HA on the Primary, it communicates the settings to the Backup ADTRAN security appliance.

To configure HA on the Primary ADTRAN, perform the following steps:

1. Navigate to the **High Availability > Settings** page.
2. Select the **Enable High Availability** checkbox.
3. Under **ADTRAN Address Settings**, type in the serial number for the Backup ADTRAN appliance.
You can find the serial number on the back of the ADTRAN security appliance, or in the **System > Status** screen of the backup unit. The serial number for the Primary ADTRAN is automatically populated.
4. Click **Apply** to retain these settings.

Configuring Advanced HA Settings

1. Navigate to the **High Availability > Advanced** page.

High Availability >
Advanced

Accept Cancel

High Availability Advanced Settings

Enable Preempt Mode

Generate/Overwrite Backup Settings When Upgrading Firmware

Enable Virtual MAC

Heartbeat Interval (milliseconds):

Failover Trigger Level (missed heartbeats):

Probe Interval (seconds):

Probe Count:

Election Delay Time (seconds):

Include Certificates/Keys

2. To configure the HA Pair so that the Primary ADTRAN resumes the Active role when coming back online after a failover, select **Enable Preempt Mode**.
3. To backup the settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.

4. Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two appliances are connected needs to be notified. All outside devices will continue to route to the single shared MAC address.
5. The **Heartbeat Interval** controls how often the two units communicate. The default is 5000 milliseconds; the minimum supported value is 1000 milliseconds.
6. Set the **Failover Trigger Level** to the number of heartbeats that can be missed before failing over. By default, this is set to 5 missed heartbeats.
7. Set the **Probe Interval** to the interval in seconds between probes sent to specified IP addresses to monitor that the network critical path is still reachable. This is used in logical monitoring. ADTRAN recommends that you set the interval for at least 5 seconds. The default is 20 seconds, and the allowed range is 5 to 255 seconds. You can set the Probe IP Address(es) on the **High Availability > Monitoring** screen.
8. Set the **Probe Count** to the number of consecutive probes before the firmware concludes that the network critical path is unavailable or the probe target is unreachable. This is used in logical monitoring. The default is 3, and the allowed range is 3 to 10.
9. The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role. The default is 3 seconds.
10. Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
11. You do not need to click **Synchronize Settings** at this time, because all settings will be automatically synchronized to the Idle unit when you click **Accept** after completing HA configuration. To synchronize all settings on the Active unit to the Idle unit immediately, click **Synchronize Settings**. The Idle unit will reboot.
12. Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Backup unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Backup appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
13. When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

Configuring HA Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring. By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability.

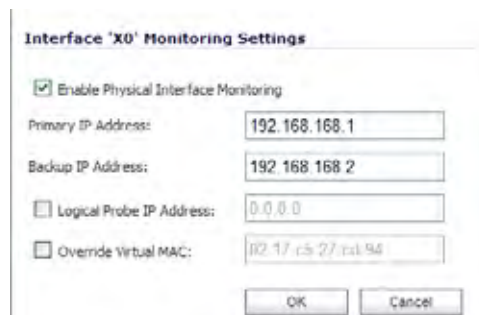
Logical monitoring involves configuring the ADTRAN to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Idle unit. If neither unit in the HA Pair can connect to the device, no action will be taken.

The Primary and Backup IP addresses configured on this page are used for multiple purposes:

- As independent management addresses for each unit (only on X0 and X1 interfaces)
- To allow synchronization of licenses between the Idle unit and the ADTRAN licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring, perform the following steps on the Primary unit:

1. Navigate to the **High Availability > Monitoring** page.
2. Click the **Configure** icon for the **X0** interface.



The screenshot shows a dialog box titled "Interface 'X0' Monitoring Settings". It contains the following fields and controls:

- Enable Physical Interface Monitoring
- Primary IP Address: 192.168.168.1
- Backup IP Address: 192.168.168.2
- Logical Probe IP Address: 0.0.0.0
- Override Virtual MAC: 02:17:c5:27:c4:94
- Buttons: OK, Cancel

3. To enable link detection between the designated HA interfaces on the Primary and Backup units, leave the **Enable Physical Interface Monitoring** checkbox selected.
4. In the **Primary IP Address** field, enter the unique LAN management IP address of the Primary unit.
5. In the **Backup IP Address** field, enter the unique LAN management IP address of the Backup unit.
6. In the **Logical Probe IP Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.) The

Primary and Backup appliances will regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the ADTRAN appliances. But, if one appliance can ping the target but the other appliance cannot, failover will occur to the appliance that can ping the target.

The **Primary IP Address** and **Backup IP Address** fields must be configured with independent IP addresses on the **X0** interface (**X1** for probing on the WAN) to allow logical probing to function correctly.

7. ADTRAN recommends that you do not select **Override Virtual MAC**. When Virtual MAC is enabled, the firmware automatically generates a Virtual MAC address for all interfaces. Allowing the firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.
8. Click **OK**.
9. To configure monitoring on any of the other interfaces, repeat the above steps.
10. When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

Synchronizing Settings

Once you have configured the HA settings on the Primary ADTRAN security appliance, it will automatically synchronize the settings to the Backup unit, causing the Backup to reboot. You do not need to click the **Synchronize Settings** button. However, if you later choose to do a manual synchronization of settings, click the **Synchronize Settings** button. You will see a **HA Peer Firewall has been updated** notification at the bottom of the management interface page. Also note that the management interface displays **Logged Into: Primary ADTRAN Status: Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that certificates, certificate revocation lists (CRL), and associated settings are synchronized between the Primary and Backup units. When local certificates are copied to the Backup unit, the associated private keys are also copied. Because the connection between the Primary and Backup units is typically protected, this is generally not a security concern.



Tip: *A compromise between the convenience of synchronizing certificates and the added security of not synchronizing certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.*

Verifying HA Functionality

To verify that Primary and Backup ADTRAN security appliances are functioning correctly, wait a few minutes, then trigger a test failover by logging into the Primary unit and powering it off. The Backup ADTRAN security appliance should quickly take over. After a failover to the Backup appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated.

From your management workstation, test connectivity through the Backup appliance by accessing a site on the public Internet. Note that unless virtual MAC is enabled, the Backup appliance will not assume the Ethernet MAC address.

Log into the Backup ADTRAN's unique LAN IP address. The management interface should now display **Logged Into: Backup ADTRAN Status: Active** in the upper-right-hand corner.

Now, power the Primary appliance back on, wait a few minutes, then log back into the management interface. If the Backup appliance is active, you can use the shared IP address to log into it.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure correct configuration.

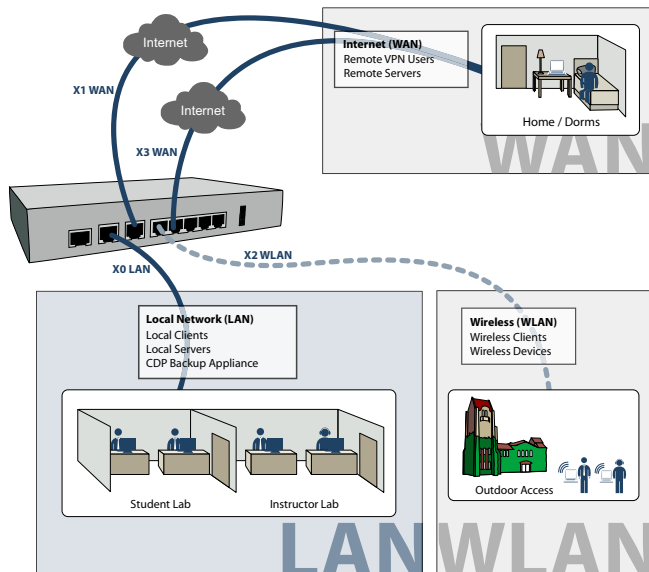
Multiple ISP / WAN Failover and Load Balancing

WAN Failover and Load Balancing allows you to designate an interface as a Secondary or backup WAN port.

The secondary WAN port can be used as a backup if the primary WAN port is down and/or unavailable, or it can maintain a persistent connection for WAN port traffic to divide outbound traffic flows between the Primary fixed WAN port and the user-assigned Secondary WAN port.

This section contains the following subsections:

- [Configuring Secondary WAN Interface](#) - page 47
- [Activating and Configuring WAN Failover](#) - page 48
- [Configuring WAN Interface Monitoring](#) - page 49
- [WAN Probe Monitoring Overview](#) - page 49
- [Configuring WAN Probe Monitoring](#) - page 50



Configuring Secondary WAN Interface

Perform the following steps to configure WAN Failover and Load Balancing on the ADTRAN security appliance:

1. On **Network > Interfaces** page, configure the chosen port to be in WAN zone, and enter the correct address settings provided by the Secondary ISP.



Note: *In the example Multiple ISP / WAN Failover and Load Balancing section, on page 46, the ADTRAN security appliance is acquiring its secondary WAN address dynamically from ISP #2, using DHCP. Any interface added to the WAN zone by default creates a NAT policy allowing internal LAN subnets to enforce NAT on this Secondary WAN interface.*

Activating and Configuring WAN Failover

To configure the appliance for WAN failover and load balancing, follow the steps below:

1. On **Network > WAN Failover & LB** page, select **Enable Load Balancing**.
2. If there are multiple possible secondary WAN interfaces, select an interface from the **Secondary WAN Ethernet Interface**.

WAN Failover & Load Balancing

Primary WAN Ethernet Interface:

Secondary WAN Ethernet Interface:

Enable Load Balancing

Basic Active/Passive Failover

Preempt and fallback to Primary WAN when possible

Per Destination Round-Robin

Spillover-Based

Send traffic to Secondary WAN when bandwidth exceeds Kbps

Percentage-Based

Use Source and Destination IP Addresses Binding

Primary WAN Percentage:

Secondary WAN Percentage:

3. Select a load balancing method. By default, the appliance will select **Basic Active/Passive Failover** as the method, but there are four load balancing methods available:

Basic Active/Passive Failover	Only sends traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. If the Primary WAN fails, then the ADTRAN security appliance reverts to this method. This mode will automatically return back to using the Primary WAN interface once it has been restored (preempt mode).
Per Destination Round-Robin	Load balances outgoing traffic on a per-destination basis. This is a simple load balancing method which allows you to utilize both links in a basic fashion (instead of the method above, which does not utilize the capability of the Secondary WAN until the Primary WAN has failed).
Spillover-Based	Allows you to control when and if the Secondary interface is used. You can specify when the ADTRAN security appliance starts sending traffic through the Secondary WAN interface.
Percentage-Based	Specifies the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces. Optionally, enable Source and Destination IP Address Binding : Enables you to maintain a consistent mapping of traffic flows with a single outbound WAN interface, regardless of the percentage of traffic through that interface.

Configuring WAN Interface Monitoring

Under the **WAN Interface Monitoring** heading, you can customize how the ADTRAN security appliance monitors the WAN interface:

1. Enter a number between 5 and 300, in the **Check Interface Every _ Seconds** field. The default value is 5 seconds.
2. In the **Deactivate Interface after _ missed intervals**, enter a number between 1 and 10. The default value is 3, which means the interface is considered inactive after 3 consecutive unsuccessful attempts.
3. Enter a number between 1 and 100 in the **Reactivate Interface after _ successful intervals**. The default value is 3, which means the interface is considered active after 3 consecutive successful attempts.

WAN Probe Monitoring Overview

If Probe Monitoring is not activated, the ADTRAN security appliance performs physical monitoring only on the Primary and Secondary WAN interfaces, meaning it only marks a WAN interface as failed if the interface is disconnected or stops receiving an Ethernet-layer signal. This is not an assured means of link monitoring, because it does not address most failure scenarios (for example, routing issues with your ISP or an upstream router that is no longer passing traffic). If the WAN interface is connected to a hub or switch, and the router

providing the connection to the ISP (also connected to this hub or switch) were to fail, the ADTRAN will continue to believe the WAN link is usable, because the connection to the hub or switch is good.

Enabling probe monitoring on the **Network > WAN Failover & Load Balancing** page instructs the ADTRAN security appliance to perform logical checks of upstream targets to ensure that the line is indeed usable.

Under the default probe monitoring configuration, the appliance performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring, because service interruption may be occurring farther upstream. If your ISP is experiencing problems in its routing infrastructure, a successful ICMP ping of their router causes the ADTRAN security appliance to believe the line is usable, when in fact it may not be able to pass traffic to and from the public Internet at all.

To perform reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port.

Configuring WAN Probe Monitoring

To configure WAN probe monitoring, follow these steps:

1. On the **Network > WAN Failover & Load Balancing** page, under the **WAN Interface Monitoring** heading, select the **Enable Probe Monitoring** checkbox.

WAN Interfaces Monitoring

Check interface every seconds

Deactivate interface after missed intervals

Reactivate interface after successful intervals

Enable Probe Monitoring

Respond to Probes

Current probe rate: < 1 per second, 0 total

Any TCP-SYN to Port

2. Select the **Respond to Probes** checkbox to have the ADTRAN security appliance respond to ADTRAN TCP probes received on any of its WAN ports. Do not select this checkbox if the ADTRAN security appliance should not respond to TCP probes.
3. Select the **Any TCP-SYN to Port** checkbox to instruct the ADTRAN security appliance to respond to TCP probes to the specified port number without validating them first..

4. If there is a NAT device between the two appliances sending and receiving TCP probes, the **Any TCP-SYN to Port** checkbox must be selected, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.
5. Click on the **Configure** button. The **Configure WAN Probe Monitoring** window is displayed.
6. In the **Primary WAN Probe Settings** menu, select one of the following options:
 - Probe succeeds when either Main Target or Alternate Target responds
 - Probe succeeds when both Main Target and Alternative Target respond
 - Probe succeeds when Main Target responds
 - Succeeds Always (no probing)
7. Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.
8. Enter the host name or IP address of the target device in the **Host** field.
9. Enter a port number in the **Port** field.
10. If there is a NAT device between the two devices sending and receiving TCP probes, the **Any TCP-SYN to Port** checkbox must be selected, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.
11. Optionally, you can enter a default target IP address in the **Default Target IP** field. In case of a DNS failure when a host name is specified, the default target IP address is used.

12. An IP address of 0.0.0.0 or a DNS resolution failure will use the Default Target IP configured. If 0.0.0.0 is entered and no default target IP address is configured, the default gateway on that interface will be used.
13. Configure the **Secondary WAN Probe Settings**, which provide the same options as the **Primary WAN Probe Settings**.
14. Click **OK**.

In this Section:

This section provides regulatory, trademark, and copyright information.

- [Safety and Regulatory Information for the NetVanta 2630 Appliance - page 54](#)
- [Safety and Regulatory Information in German for the NetVanta 2630 Appliance - page 55](#)
- [FCC Part 15 Class B Notice for the NetVanta 2630 Appliance - page 56](#)
- [Safety and Regulatory Information for the NetVanta 2630W Appliance - page 57](#)
- [Safety and Regulatory Information in German for the NetVanta 2630W Appliance - page 58](#)
- [FCC Part 15 Class B Notice for the NetVanta 2630W Appliance - page 59](#)
- [FCC RF Radiation Exposure Statement - page 59](#)
- [Copyright Notice - page 60](#)
- [Trademarks - page 60](#)



Note: *Safety and Regulatory compliance in this section is based on SonicWALL, Inc. regulatory model / type as shown.*

Safety and Regulatory Information for the NetVanta 2630 Appliance

Regulatory Model/Type	Product Name
APL20-063	NetVanta 2630

Mounting the Appliance

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104° F (40° C).
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.
- If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum recommended ambient temperature shown above.

Lithium Battery Warning

The Lithium Battery used in the security appliance may not be replaced by the user. Return the security appliance to an authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or security appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the appliance is located.

Power Supply Information

If the power supply is missing from your ADTRAN product package, please contact ADTRAN Technical Support (1-888-4-ADTRAN) for a replacement. This product should only be used with a UL listed power supply marked "I.T.E. LPS", with an output rated 12 VDC, minimum 1.66 A.

Safety and Regulatory Information in German for the NetVanta 2630 Appliance

Weitere Hinweise zur Montage

- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Achten Sie darauf, das sich die Netzkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden.
- Das beigefügte Netzkabel ist nur für den Gebrauch in Nordamerikas vorgesehen. Für Kunden in der Europäischen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist.
- Wenn das Gerät in einem geschlossenen 19"-Gehäuse oder mit mehreren anderen Geräten eingesetzt ist, wird die Temperatur in der Gehäuse höher sein als die Umgebungstemperatur. Achten Sie darauf, daß die Umgebungstemperatur nicht mehr als 40° C beträgt.
- Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts.

Hinweis zur Lithiumbatterie

Die in der Internet Security Appliance verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die in ein von autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der Internet Security Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der Produkt keine Kabel an, die aus dem Gebäude herausgeführt werden, in dem sich das Gerät befindet.

Informationen zur Stromversorgung

Sollte das Netzteil nicht im Lieferumfang der ADTRAN enthalten sein, wenden Sie sich diesbezüglich an den technischen Support von ADTRAN(T +1-888-4-ADTRAN). Dieses Produkt darf nur in Verbindung mit einem nach den Normen der Underwriter Laboratories, USA als „UL-gelistet“ zugelassenen Netzteil der Kategorie „I.T.E. LPS“ verwendet werden. Ausgang: 12 VDC Gleichspannung, mind. 1,66 A.

FCC Part 15 Class B Notice for the NetVanta 2630 Appliance

NOTE: This equipment was tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. And, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from the receiver connection.
- Consult ADTRAN (1-888-4-ADTRAN) for assistance.

Complies with EN55022 Class B and CISPR22 Class B.

*Refer to the label on the bottom of the unit for device information including Class A or Class B FCC information.

Canadian Radio Frequency Emissions Statement

This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Caution: Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL could void the user's authority to operate this equipment.


Declaration of Conformity

Application of council Directive	2004/108/EC (EMC) and 2006/95/EC (LVD)
Standards to which conformity is declared	EN 55022 (2006) Class B EN 55024 (1998) +A2 EN 61000-3-2 (2006) EN 61000-3-3 (1995) +A2 EN 60950-1 (2001) +A11 National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI

VCCI Statement

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

Regulatory Information for Korea

 방송통신위원회	Ministry of Information and Telecommunication Certification Number SWL-APL20-063
--	---

All products with country code "" (blank) and "A" are made in the USA.
All products with country code "B" are made in China.
All products with country code "C" or "D" are made in Taiwan R.O.C.
All certificates held by Secuwide, Corp.

B급 기기 (가정용 정보통신기기)

이 기기는 가정용으로 전자파적합등록을 한 기기로서
주거지역에서는 물론 모든지역에서 사용할 수 있습니다.

Safety and Regulatory Information for the NetVanta 2630W Appliance

Regulatory Model/Type	Product Name
APL20-065	NetVanta 2630W
APL20-064	NetVanta 2630W

Mounting the Appliance

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104° F (40° C).
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.
- If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum recommended ambient temperature shown above.

Lithium Battery Warning

The Lithium Battery used in the security appliance may not be replaced by the user. Return the security appliance to an authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or security appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the product is located.

Power Supply Information

If the power supply is missing from your ADTRAN product package, please contact ADTRAN Technical Support (1-888-4-ADTRAN) for a replacement. This product should only be used with a UL listed power supply marked "I.T.E. LPS", with an output rated 12 VDC, minimum 1.66 A.

Safety and Regulatory Information in German for the NetVanta 2630W Appliance

Weitere Hinweise zur Montage

- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Achten Sie darauf, das sich die Netzkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden.
- Das beigegefügte Netzkabel ist nur für den Gebrauch in Nordamerikas vorgesehen. Für Kunden in der Europäischen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist.
- Wenn das Gerät in einem geschlossenen 19"-Gehäuse oder mit mehreren anderen Geräten eingesetzt ist, wird die Temperatur in der Gehäuse höher sein als die Umgebungstemperatur. Achten Sie darauf, daß die Umgebungstemperatur nicht mehr als 40° C beträgt.
- Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts.

Hinweis zur Lithiumbatterie

Die in der Internet Security Appliance von verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die in ein von autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der Internet Security Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der Produkt keine Kabel an, die aus dem Gebäude herausgeführt werden, in dem sich das Gerät befindet.

Informationen zur Stromversorgung

Sollte das Netzteil nicht im Lieferumfang der ADTRAN enthalten sein, wenden Sie sich diesbezüglich an den technischen Support von ADTRAN (T +1-888-4-ADTRAN). Dieses Produkt darf nur in Verbindung mit einem nach den Normen der Underwriter Laboratories, USA als „UL-gelistet“ zugelassenen Netzteil der Kategorie „I.T.E. LPS“ verwendet werden. Ausgang: 12 VDC Gleichspannung, mind. 1,66 A.

FCC Part 15 Class B Notice for the NetVanta 2630W Appliance

NOTE: This equipment was tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. And, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from the receiver connection.
- Consult ADTRAN (1-888-4-ADTRAN) for assistance.

Complies with EN55022 Class B and CISPR22 Class B.

*Refer to the label on the bottom of the unit for device information including Class A or Class B FCC information.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (7.9 inches) between the radiator (antenna) and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. For more information regarding the above statement, please contact SonicWALL.

North American Authorized Channels

ADTRAN declares that the APL20-065 (FCC ID: QWU-06C) (IC: 4408A-06C) and APL20-064 (FCC ID: QWU-06D) (IC: 4408A-06D) when sold in US or Canada is limited to CH1-CH11 by specified firmware controlled in the USA.

Canadian Radio Frequency Emissions Statement

This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Declaration of Conformity

Certificate #: EU00165-A

Application of council Directive	2004/108/EC (EMC) 2006/95/EC (LVD) 1999/5/EC (R&TTE)
Standard(s) to which conformity is declared	EN 55022 (2006) +A1(2007) Class B EN 55024 (1998) +A1 (2001), +A2 (2003) EN 61000-3-2 (2006) EN 61000-3-3 (2006) EN 60950-1 (2006) National Deviations: AR, AT, AU, BE, CA, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IL, IN, IT, JP, KE, KR, MY, NL, NO, PL, SE, SG, SI, SK, US EN 300 328 V1.7.1:2006 EN 301 893 V1.5.1:2008 EN 301 489-17 V2.1.1 2009 EN50385 : (2002)
Manufacturer/ Responsible Party	SonicWALL, Inc. 2001 Logic Drive San José, CA 95124 USA
Type of Equipment	Information Technology Equipment Internet Security (Firewall/VPN) Appliance, with 802.11b/g/n Wireless Router Tabletop with external power supply.
Type Numbers	APL20-065, APL20-064

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards. Quality control procedures will ensure series production of equipment will be compliant.

Signature /s/ Larry Wagner
Sr. Engineering Director

Date 10/22/10

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, Except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Copyright Notice

© 2010 ADTRAN

All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

ADTRAN is a registered trademark of ADTRAN.

Microsoft Windows Vista, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Notes



P/N: 232-001869-50
10/10/2010

ADTRAN, Inc.
901 Explorer Boulevard
Huntsville, AL 35806

WWW.ADTRAN.COM