



NETVANTA 2000 SERIES

System Manual

- 1200362L1 NetVanta 2050 System**
- 1200361L1 NetVanta 2100 System**
- 1200366L1 NetVanta 2300 System**
- 1200367L1 NetVanta 2400 System**

Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.



901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35814-4000
Phone: (256) 963-8000

©2001 ADTRAN, Inc.
All Rights Reserved.
Printed in U.S.A.

About this Manual

This manual provides a complete description of the NetVanta 2000 series system and system software. The purpose of this manual is to provide the technician, system administrator, and manager with general and specific information related to the planning, installation, operation, and maintenance of the NetVanta 2000 series. This manual is arranged so that needed information can be quickly and easily found. The following is an overview of the contents.

Section 1 System Description

Provides managers with an overview of the NetVanta 2000 series system.

Section 2 Engineering Guidelines

Provides information to assist network designers with incorporating the NetVanta 2000 series system into their networks.

Section 3 Network Turnup Procedure

Provides step-by-step instructions on how to install the NetVanta 2000 series unit, determine the parameters for the system, install the network and option modules, and power up the system.

Section 4 User Interface Guide

A reference guide listing all menu options contained in the NetVanta 2000 series.

Section 5 Detail Level Procedures

Provides the Provides the Detail Level Procedures to perform various unit functions (upgrading firmware, telnet, etc). Level Procedures called out in Section 3.

Glossary and Acronyms

Gives definitions of terms and acronyms used in the manual.

Revision History

This is the 4th issue of this manual. Revisions include:

- NetVanta 2050 and 2400 additions



Notes provide additional useful information.



Cautions signify information that could prevent service interruption.



Warnings provide information that could prevent damage to the equipment or endangerment to human life.

Safety Instructions

When using your telephone equipment, please follow these basic safety precautions to reduce the risk of fire, electrical shock, or personal injury:

1. Do not use this product near water, such as a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement, or near a swimming pool.
2. Avoid using a telephone (other than a cordless-type) during an electrical storm. There is a remote risk of shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.
4. Use only the power cord, power supply, and/or batteries indicated in the manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for special disposal instructions.

Save These Important Safety Instructions

Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio frequencies. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



Shielded cables must be used with this unit to ensure compliance with Class A FCC limits.



Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Canadian Emissions Requirements

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Class A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques," NMB-003 édictée par le ministre des Communications.

Canadian Equipment Limitations

Notice: The Canadian Industry and Science Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above limitations may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.



Users should not attempt to make such connections themselves, but should contract the appropriate electric inspection authority, or an electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all devices does not exceed 100.

Warranty and Customer Service

ADTRAN will repair and return this product within five years from the date of shipment if it does not meet its published specifications or fails while in service. For detailed warranty, repair, and return information refer to the ADTRAN Equipment Warranty and Repair and Return Policy Procedure.

Return Material Authorization (RMA) is required prior to returning equipment to ADTRAN.

For service, RMA requests, or further information, contact one of the numbers listed at the end of this section.

LIMITED PRODUCT WARRANTY

ADTRAN warrants that for five years from the date of shipment to Customer, all products manufactured by ADTRAN will be free from defects in materials and workmanship. ADTRAN also warrants that products will conform to the applicable specifications and drawings for such products, as contained in the Product Manual or in ADTRAN's internal specifications and drawings for such products (which may or may not be reflected in the Product Manual). This warranty only applies if Customer gives ADTRAN written notice of defects during the warranty period. Upon such notice, ADTRAN will, at its option, either repair or replace the defective item. If ADTRAN is unable, in a reasonable time, to repair or replace any equipment to a condition as warranted, Customer is entitled to a full refund of the purchase price upon return of the equipment to ADTRAN. This warranty applies only to the original purchaser and is not transferable without ADTRAN's express written permission. This warranty becomes null and void if Customer modifies or alters the equipment in any way, other than as specifically authorized by ADTRAN.

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, THE FOREGOING CONSTITUTES THE SOLE AND EXCLUSIVE REMEDY OF THE CUSTOMER AND THE EXCLUSIVE LIABILITY OF ADTRAN AND IS IN LIEU OF ANY AND ALL OTHER WARRANTIES (EXPRESSED OR IMPLIED). ADTRAN SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING (WITHOUT LIMITATION), ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THIS EXCLUSION MAY NOT APPLY TO CUSTOMER.

In no event will ADTRAN or its suppliers be liable to the Customer for any incidental, special, punitive, exemplary or consequential damages experienced by either the Customer or a third party (including, but not limited to, loss of data or information, loss of profits, or loss of use). ADTRAN is not liable for damages for any cause whatsoever (whether based in contract, tort, or otherwise) in excess of the amount paid for the item. Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to the Customer.

Customer Service, Product Support Information, and Training

ADTRAN will repair and return this product if within five years from the date of shipment the product does not meet its published specification or the product fails while in service.

A return material authorization (RMA) is required prior to returning equipment to ADTRAN. For service, RMA requests, training, or more information, use the contact information given below.

Repair and Return

If you determine that a repair is needed, please contact our Customer and Product Service (CAPS) department to have an RMA number issued. CAPS should also be contacted to obtain information regarding equipment currently in house or possible fees associated with repair.

CAPS Department (256) 963-8722

Identify the RMA number clearly on the package (below address), and return to the following address:

ADTRAN Customer and Product Service
901 Explorer Blvd. (East Tower)
Huntsville, Alabama 35806

RMA # _____

Pre-Sales Inquiries and Applications Support

Your reseller should serve as the first point of contact for support. If additional pre-sales support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, latest product documentation, application briefs, case studies, and a link to submit a question to an Applications Engineer. All of this, and more, is available at:

<http://support.adtran.com>

When needed, further pre-sales assistance is available by calling our Applications Engineering Department.

Applications Engineering (800) 615-1176

Post-Sale Support

Your reseller should serve as the first point of contact for support. If additional support is needed, the ADTRAN Support web site provides a variety of support services such as a searchable knowledge base, updated firmware releases, latest product documentation, service request ticket generation and trouble-shooting tools. All of this, and more, is available at:

<http://support.adtran.com>

When needed, further post-sales assistance is available by calling our Technical Support Center. Please have your unit serial number available when you call.

Technical Support (888) 4ADTRAN

Installation and Maintenance Support

The ADTRAN Custom Extended Services (ACES) program offers multiple types and levels of installation and maintenance services which allow you to choose the kind of assistance you need. This support is available at:

<http://www.adtran.com/aces>

For questions, call the ACES Help Desk.

ACES Help Desk (888) 874-ACES (2237)

Training

The Enterprise Network (EN) Technical Training Department offers training on our most popular products. These courses include overviews on product features and functions while covering applications of ADTRAN's product lines. ADTRAN provides a variety of training options, including customized training and courses taught at our facilities or at your site. For more information about training, please contact your Territory Manager or the Enterprise Training Coordinator.

Training Phone (800) 615-1176, ext. 7500
Training Fax (256) 963-6700
Training Email training@adtran.com

SYSTEM DESCRIPTION

CONTENTS

System Overview	12
Features and Benefits	13
Physical Interfaces	13
Firewall Features	13
Address Translation	13
IPSec Tunnel	13
Administration	13
DHCP	14
PPPoE	14
Routing	14

1. SYSTEM OVERVIEW

The NetVanta 2000 series of VPN products include small to mid-range IPSec compliant gateways providing all the necessary components required to secure an integrated VPN solution. Used primarily for remote access and site-to-multisite connectivity, the NetVanta 2050 and NetVanta 2100 targets the corporate branch office, the small office/home office (SOHO), as well as business-to-business applications. As a branch office or mid-size host security gateway, the NetVanta 2300 provides the same features as the NetVanta 2100 with an added DMZ port for public server access. For networks supporting a large VPN network, the NetVanta 2400 is available to provide all necessary host site gateway functionality. The NetVanta 2000 series provides several key security and data management features such as IPSec VPN tunneling, stateful inspection firewall (providing cyber assault protection), authenticated remote user access, and Network Address Translation. Adhering to IPSec standards (established and maintained by the IETF) enables the NetVanta 2000 series to be interoperable with many other IPSec compliant gateways, allowing for a multi-vendor VPN solution.

On a public infrastructure like the Internet, security is of the utmost importance. The NetVanta 2000 series protect the corporate network against attacks with a built in firewall and provides data security through encryption, authentication and key exchange. The NetVanta 2000 series employ a stateful inspection firewall that protects an organization's network from common cyber attacks including TCP syn-flooding, IP spoofing, ICMP redirect, land attacks, ping-of-death, and IP reassembly problems.

For encryption, the NetVanta 2000 series encrypt the data being sent out onto the network, using either the Data Encryption Standard (DES) or 3DES encryption algorithms. Data integrity is ensured using MD5 or SHA1 as it is transported across the public infrastructure. In addition, Internet Key Exchange (IKE) can be used for user authentication supporting public and private keys or digital certificates, assuring that the proper VPN tunnel is established and that the tunnel has not been redirected or compromised.

NetVanta 2000 series are Internet Protocol Security (IPSec) compliant devices that supports both ESP and AH protocols and provides secure communication over potentially unsecure network components. Acting as a security gateway, the NetVanta 2050 and 2100 can provide up to 10 private encryption communication tunnels through the Internet with remote locations while the larger scale NetVanta 2300 offers support for up to 100 private encryption tunnels. For networks requiring more than 100 tunnels, the NetVanta 2400 provides 1000 private encryption tunnels. The NetVanta 2000 series can also hide IP addresses from the external world by performing Network Address Translation (NAT). The internal router allows multiple users to share a VPN connection and can also direct incoming IP traffic.

A remote NetVanta 2000 series can easily be configured and managed using a standard web browser. NetVanta 2000 series also have built-in alert and logging mechanisms for messaging and mail services. This enables the unit to warn administrators about activities that are going on in the network by logging them into a Syslog server or sending an email to the administrator.

Unlike a software implemented VPN solution, which depends on local CPU and memory performance to implement encryption, the NetVanta 2000 series are standalone, hardware platforms that off-load the CPU intensive encryption process. 3DES encryption significantly impacts CPU performance, possibly slowing all the local processes on the computer. Since the NetVanta 2000 series offers dedicated processing platforms to drive the encryption process, local computer performance is unaffected.

2. FEATURES AND BENEFITS

The NetVanta 2000 series provide granular control over network access that includes maximum security, data authenticity and privacy, and significant ease of use. The major features of the NetVanta 2000 series are described below.

Physical Interfaces

- WAN: RJ-45 10/100 Auto-sensing ethernet interface
- LAN: RJ-45 10/100 Auto-sensing ethernet interface
- Serial Port: RS-232 for off-net configuration (NetVanta 2300 Only)
- DMZ: RJ-45 10/100 Auto-sensing ethernet interface

Firewall Features

- Stateful inspection firewall
- Application content filtering
- Cyber assault protection
- HTTP relay

Address Translation

- Basic NAT (1:1)
- NAT (Many:1)
- Reverse NAT (translation of an inbound session's destination IP address)

IPSec Tunnel

- Encapsulating Security Payload (ESP)
- Authentication Header (AH)
- Manual key management or automatic key management using Internet Key Exchange (IKE)
- X.509 certificate support
- MD5-HMAC 128-bit authentication algorithm
- SHA1-HMAC 160-bit authentication algorithm
- DES-CBC 56-bit encryption
- 3DES-CBC 168-bit encryption

Administration

- Web-based management
- Syslog logging in WELF format
- E-mail alerts (SMTP)
- User and group access control policies based on time-of-day
- User accounting policy statistics

DHCP

- Server (to manage IP addresses on local network)
- Client (to acquire the WAN-side IP address from service provider)

PPPoE

- Client (to acquire the WAN-side IP address from service provider)

Routing

- TCP/IP
- Static routes
- RIP (V1 and V2)
- RIP with Authentication

ENGINEERING GUIDELINES

CONTENTS

Equipment Dimensions	16
Power Requirements	16
Reviewing the front Panel Design	16
Front Panel LEDs	17
Reviewing the Rear Panel Design	18
LAN Interface	19
WAN Connection	19
DMZ Connection (NetVanta 2300 Only)	20
COM1 Interface	21
Power Connection	21
At-A-Glance Specifications	22

FIGURES

Figure 1. NetVanta 2000 series Front Panel Layout	16
Figure 2. NetVanta 2300 Front Panel Layout	17
Figure 3. NetVanta 2000 series Rear Panel Layout	18
Figure 4. NetVanta 2300 Rear Panel Layout	19

TABLES

Table 1. NetVanta 2000 series Front Panel Description	17
Table 2. NetVanta 2000 series LEDs	17
Table 3. LAN Pinout	19
Table 5. DMZ Pinout	20
Table 4. WAN Pinout	20
Table 6. DB-9 Connector Pinout	21
Table 7. Specifications	22

1. EQUIPMENT DIMENSIONS

NetVanta 2050 and 2100

The NetVanta 2050 and 2100 units are 9.0" W, 6.375" D, and 1.625" H and come equipped for table top and wallmount use. An optional rackmount shelf is available from ADTRAN.

NetVanta 2300 and 2400

The NetVanta 2300 units are 17.25" W, 7.75" D, and 1.26" H and come equipped for rackmount use.

2. POWER REQUIREMENTS

NetVanta 2050 and 2100

The NetVanta 2000 series has a maximum power consumption of 9W and a maximum current draw of 800mA.

NetVanta 2300 and 2400

The NetVanta 2300 has a maximum power consumption of 11W and a maximum current draw of 0.2A.

3. REVIEWING THE FRONT PANEL DESIGN

NetVanta 2050

The NetVanta 2100 front panel monitors operation by providing status LEDs for both the LAN and WAN interfaces, as well as VPN tunnels and traffic. The front panel is shown in **Figure 1**.

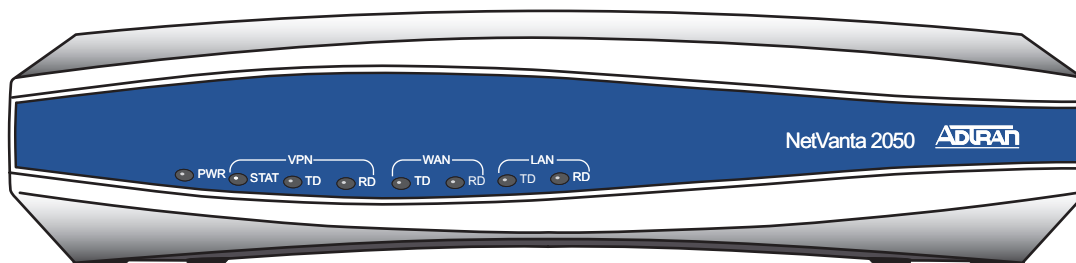


Figure 1. NetVanta 2050 Front Panel Layout

NetVanta 2100

The NetVanta 2100 front panel monitors operation by providing status LEDs for both the LAN and WAN interfaces, as well as VPN tunnels and traffic. The front panel is shown in **Figure 2**.

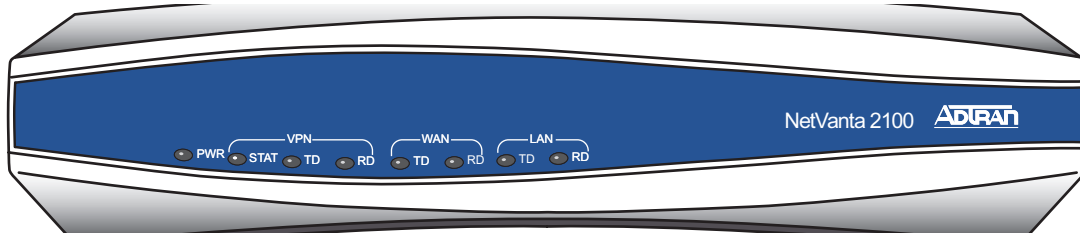


Figure 2. NetVanta 2100 Front Panel Layout

NetVanta 2300

The NetVanta 2300 front panel monitors operation by providing status LEDs for the LAN, WAN, and DMZ interfaces, as well as VPN tunnels and traffic. The front panel is shown in **Figure 3**.

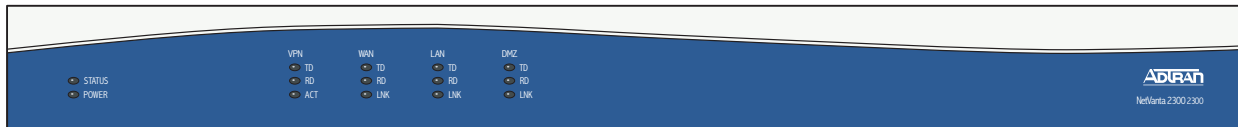


Figure 3. NetVanta 2300 Front Panel Layout

NetVanta 2400

The NetVanta 2400 front panel monitors operation by providing status LEDs for the LAN, WAN, and DMZ interfaces, as well as VPN tunnels and traffic. Additionally, a LCD display provides quick-glance access to the LAN IP parameters (IP address and subnet mask). The front panel is shown in **Figure 4**.

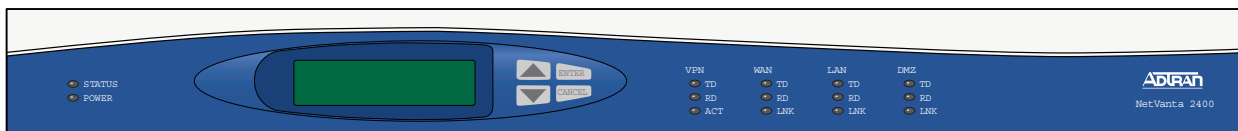


Figure 4. NetVanta 2400 Front Panel Layout

Front Panel LEDs

With the NetVanta 2000 series powered-up, the front panel LEDs provide visual information about the status of the system. Table 1 provides a brief description of the front panel features, and Table 2 provides detailed information about the LEDs.

Table 1. NetVanta 2000 series Front Panel Description

Feature	Description
PWR	Indicates whether the unit has power.
VPN (2050/2100 only)	Indicates status of VPN negotiations.
VPN TD	Indicates VPN traffic transmitted by the NetVanta.
VPN RD	Indicates VPN traffic received by the NetVanta.
VPN ACT (2300/2400 only)	Indicates status of VPN Negotiations.
LAN TD	Indicates LAN traffic transmitted by the NetVanta.
LAN RD	Indicates LAN traffic received by the NetVanta.
LAN LNK (2300/2400 Only)	Indicates active physical link on the LAN port.
WAN TD	Indicates WAN traffic transmitted by the NetVanta.
WAN RD	Indicates WAN traffic received by the NetVanta.
WAN LNK (2300/2400 Only)	Indicates active physical link on the WAN port.

Table 2. NetVanta 2000 series LEDs

For these LEDs...	This color light...	Indicates that...
PWR	Red (solid)	The unit has power and is in the boot process.
	Green (solid)	Unit has power and has successfully completed the boot process.
VPN (2050/2100 only) VPN ACT (2300/2400 Only)	Amber (slow blink)	Initial Phase 1 IKE negotiation in progress.
	Green (slow blink)	Initial Phase 1 IKE negotiation completed successfully.
	Red (slow blink)	Phase 1 IKE negotiation failed.
	Amber (fast blink)	Phase 2 IKE negotiation in progress.
	Green (solid)	Phase 2 IKE negotiation completed successfully.
	Red (fast blink)	Phase 2 IKE negotiation failed.
	Amber and Green (alternating slow blink)	There is an active tunnel and an additional IKE Phase 1 negotiation in progress.

Table 2. NetVanta 2000 series LEDs (Continued)

For these LEDs...	This color light...	Indicates that...
VPN TD	Green (blink)	Flashes with VPN data transmitted by the NetVanta 2000 series.
VPN RD	Green (blink)	Flashes with VPN data received by the NetVanta 2000 series.
LAN TD	Green (blink)	Flashes with data transmitted on the LAN interface.
LAN RD	Green (blink)	Flashes with data received on the LAN interface.
LAN LNK (2300/2400 Only)	Green (solid)	Unit has active physical connection on the LAN interface.
WAN TD	Green (blink)	Flashes with data transmitted on the WAN interface.
WAN RD	Green (blink)	Flashes with data received on the WAN interface.
WAN LNK (2300/2400 Only)	Green (solid)	Unit has active physical connection on the WAN interface.

4. REVIEWING THE REAR PANEL DESIGN

NetVanta 2050 and 2100

The NetVanta 2050 and 2100 rear panel contains 2 Ethernet ports, a DB-9 serial connection, and a power connection (see **Figure 5**).

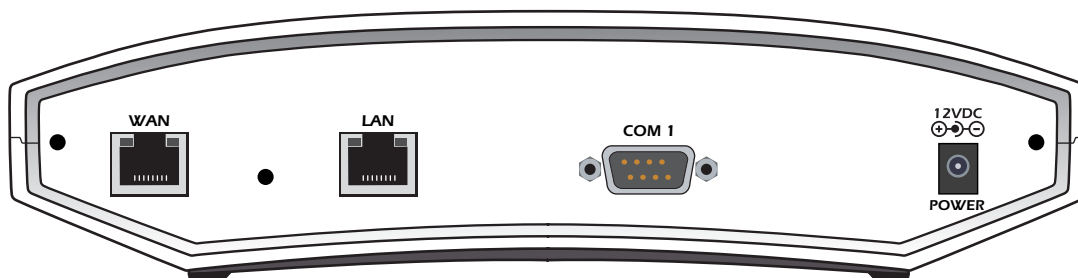


Figure 5. NetVanta 2050 Rear Panel Layout

NetVanta 2300

The NetVanta 2300 rear panel contains 3 Ethernet ports, a DB-9 serial connection, and a power connection (see **Figure 6**).

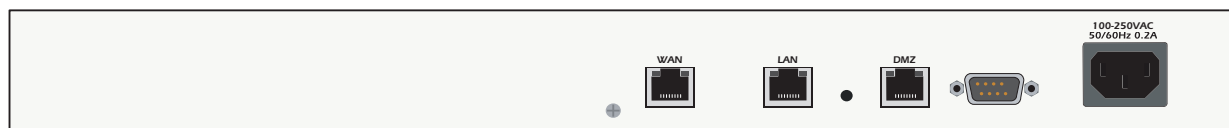


Figure 6. NetVanta 2300 Rear Panel Layout

NetVanta 2400

The NetVanta 2300 rear panel contains 3 Ethernet ports, a DB-9 serial connection, a power connection and ventilation openings (see **Figure 7**).



Figure 7. NetVanta 2400 Rear Panel Layout

LAN Interface

The NetVanta 2000 series provides a standard 10/100BaseT Ethernet interface for connection to the local corporate network. Connect the LAN interface to a hub located on your local corporate network. A DHCP Server is enabled on the LAN interface by default. References to the LAN interface include LAN, CORP, and Eth0

The LAN connection follows, and **Table 3** shows the pinout.

Connector Type RJ-48C

Table 3. LAN Pinout

Pin	Name	Description
1	TX1	Transmit Positive
2	TX2	Transmit Negative
3	RX1	Receive Positive
4, 5	UNUSED	—
6	RX2	Receive Negative
7, 8	UNUSED	—

WAN Connection

The NetVanta 2000 series provides a standard 10/100BaseT Ethernet interface for connection to the wide area network. Connect the WAN interface to a hub connected to the router interfacing with the non-secure Internet or the modem (cable or DSL) used for Internet access. A DHCP Client is enabled on the WAN interface by default. References to the WAN interface include Internet, WAN, and Eth1.

Connector Type (USOC) RJ-48C

Table 4. WAN Pinout

Pin	Name	Description
1	TX1	Transmit Positive
2	TX2	Transmit Negative
3	RX1	Receive Positive
4, 5	UNUSED	—
6	RX2	Receive Negative
7, 8	UNUSED	—

DMZ Connection (NetVanta 2300 and 2400 Only)

The NetVanta 2300 and 2400 provide a standard 10/100BaseT Ethernet interface for providing public server access. **Table 5** shows the pinout for the DMZ port.

Connector Type (USOC) RJ-48C

Table 5. DMZ Pinout

Pin	Name	Description
1	TX1	Transmit Positive
2	TX2	Transmit Negative
3	RX1	Receive Positive
4, 5	UNUSED	—
6	RX2	Receive Negative
7, 8	UNUSED	—

COM1 Interface

The NetVanta 2000 series provides a DB-9 serial communication port for future command line. **Table 6** shows the pinout for the DB-9 connector.

Connector Type DB-9

Table 6. DB-9 Connector Pinout

Pin	Name	Description
1	DCD	Data Carrier Detect
2	RD	Receive Data
3	TD	Transmit Data
4	DTR	Data Transmit Ready
5	SG	Signal Ground
6	DSR	Data Set Ready
7	RTS	Request to Send
8	CTS	Clear to Send
9	RI	Ring Indicator

Power Connection

NetVanta 2050 and 2100

The NetVanta 2000 series includes a 12 VDC power supply. Connect the power supply to a standard 120VAC, 60-Hz electrical outlet for proper operation.

NetVanta 2300 and 2400

The NetVanta 2300 and 2400 include an auto sensing 100-250 VAC, 50/60 Hz power supply with a three prong removable cable. Connect the power supply to a standard 120 VAC, 60 Hz or 220 VAC, 50 Hz electrical outlet for proper operation.

5. AT-A-GLANCE SPECIFICATIONS

Table 7 lists the specifications for the NetVanta 2000 series system.

Table 7. Specifications

Application	Feature	Specification
Firewall		
	Stateful Inspection Firewall	Provides support against the following attacks: IP Spoofing, Land Attack, Ping of Death, and Reassembly Attack Provides checks for the following attacks: ICMP Redirect, Syn Flooding, Winnuke, and Source Routing
IPSEC Tunnel		
	Encryption	Encapsulating Security Payload (ESP) DES-CBC 56-bit encryption 3DES-CBC 168-bit encryption
	Authentication	Authentication Header (AH) MD5-HMAC 128-bit authentication algorithm SHA1-HMAC 160-bit authentication algorithm
	Certificate Support	X.509 certificate support
	IKE	Manual key management for automatic key management

Table 7. Specifications (Continued)

Application	Feature	Specification
DHCP		
	Server	Supports three IP address ranges on local network User defined lease duration Real time status of active leases
	Client	Ability to acquire the WAN-side IP address from Service Provider DHCP Server
Routing		
	RIP	Supports RIP v1, RIP v2 and a combination of both Separate RIP Configuration for the LAN and WAN side Supports RIP using Authentication Keys
Address Translation		
	NAT	Supports one-to-one NAT (Static NAT)
	NAPT	Supports many-to-one (Dynamic NAT)
	Reverse NAT	Translates an inbound session destination IP address

Table 7. Specifications (Continued)

Application	Feature	Specification
Administration		
	Web Management	Provides a GUI (graphical user interface) for configuring the NetVanta 2000 series
	SYSLOG	Provides levels for logging events to an active SYSLOG server on the network
	E-Mail Alerts	Capability to e-mail an alert message when programmed thresholds are reached
	Statistics	User monitoring, policy, and access statistics available

NETWORK TURNUP PROCEDURE

CONTENTS

- Introduction** 26
- Tools Required** 26
- Unpack and Inspect the SYSTEM** 26
 - Contents of ADTRAN Shipments - NetVanta 2100 26
 - Contents of ADTRAN Shipments - NetVanta 2300 26
- Supplying Power to the Unit** 27
 - NetVanta 2100 27
 - NetVanta 2300 27
- Installing NetVanta 2000 series Management Components** 27
 - Browsing Hosts Running Microsoft Windows NT, Windows 2000, or Windows 98/95 28
 - Browsing Hosts Running POSIX-Compliant UNIX 28

1. INTRODUCTION

This section discusses the installation process of the NetVanta 2000 series systems.

2. TOOLS REQUIRED

The tools required for installation of the NetVanta 2000 series systems are:

- CATV-UTP Ethernet cable to connect the unit to the existing network
- An Internet browser for configuring the unit

WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

3. UNPACK AND INSPECT THE SYSTEM

Each NetVanta 2000 series unit is shipped in its own cardboard shipping carton. Open each carton carefully and avoid deep penetration into the carton with sharp objects.

After unpacking the unit, inspect it for possible shipping damage. If the equipment has been damaged in transit, immediately file a claim with the carrier, then contact ADTRAN Customer Service (see *Customer Service, Product Support Information, and Training* in the front of this manual).

Contents of ADTRAN Shipments - NetVanta 2050 and 2100

Your ADTRAN shipment includes the following items:

- The NetVanta 2050 or 2100 Unit
- The NetVanta 2000 series *User Manual* CD (ADTRAN P/N 3253041)
- AC Power supply - (ADTRAN P/N 336012 VUR01)
- Crossover Ethernet cable for connecting the NetVanta 2100 directly to a PC (ADTRAN P/N 8125M012)

Contents of ADTRAN Shipments - NetVanta 2300 and 2400

Your ADTRAN shipment includes the following items:

- The NetVanta 2300 or 2400 Unit
- The NetVanta 2000 series *User Manual* CD (ADTRAN P/N 3253041)
- AC Power cable (ADTRAN P/N 3127009)
- (2) Brackets for installing the unit in a rackmount configuration (ADTRAN P/N 3265479)

4. SUPPLYING POWER TO THE UNIT

NetVanta 2050 and 2100

The AC powered NetVanta 2050 and 2100 come equipped with a detachable 12 VDC at 800 mA wallmount power supply for connecting to a grounded power receptacle. As shipped, the NetVanta 2050 and 2100 are set to factory default conditions. After installing the unit, the NetVanta 2050 and 2100 are ready for power-up. To power-up the unit, connect the unit to an appropriate power source.



- *This unit shall be installed in accordance with Article 400 and 364.8 of the NEC NFPA 70 when installed outside of a Restricted Access Location (i.e., central office, behind a locked door, service personnel only area).*
- *Power to the NetVanta 2050/2100 AC system must be from a grounded 90-130 VAC, 50/60 Hz source.*
- *The power receptacle uses double-pole, neutral fusing.*
- *Maximum recommended ambient operating temperature is 45 °C.*

NetVanta 2300 and 2400

The AC powered NetVanta 2300 and 2400 come equipped with an auto-sensing 100-240 VAC, 50-60 Hz power supply for connecting to a grounded power receptacle. A grounded three plug detachable cable is included with the shipment. As shipped, the NetVanta 2300 and 2400 are set to factory default conditions. After installing the unit, the NetVanta 2300 and 2400 are ready for power-up. To power-up the unit, connect the unit to an appropriate power source.



- *This unit shall be installed in accordance with Article 400 and 364.8 of the NEC NFPA 70 when installed outside of a Restricted Access Location (i.e., central office, behind a locked door, service personnel only area).*
- *Power to the NetVanta 2300/2400 AC system must be from a grounded 100-240 VAC, 50/60 Hz source.*
- *The power receptacle uses double-pole, neutral fusing.*
- *Maximum recommended ambient operating temperature is 45 °C.*

5. INSTALLING NETVANTA 2000 SERIES MANAGEMENT COMPONENTS

Configuring the NetVanta 2000 series unit through the web interface requires a host computer with an Ethernet interface and a web browser. ADTRAN recommends using Internet Explorer 5.0 or greater for optimal viewing of configuration web pages.

The NetVanta 2000 series of products contains a default IP address of 10.10.10.1 and a netmask of 255.255.255.0. Select an IP address in the same range as the NetVanta unit and assign it to the host computer running the web browser. An example IP address is 10.10.10.10 with a subnet mask of 255.255.255.0. This section contains detailed procedures for assigning the selected IP address to a host computer for each of the popular operating systems.



If you have a PC with DHCP client capabilities enabled, connect the NetVanta 2000 series unit directly to your computer using the supplied ethernet crossover cable and follow the procedure in DLP-1, Connecting to the Netvanta 2000 Series to connect for the first time.



The NetVanta 2000 series products have a DHCP Server capabilities enabled by default. Connecting the unit to a network with a functioning DHCP server can cause IP address assignment conflicts.



For any operating system not discussed in this section, refer to the system's user documentation for instructions on assigning IP addresses.

Browsing Hosts Running Microsoft Windows NT, Windows 2000, or Windows 98/95

1. Follow the menu path **START>SETTINGS>CONTROL PANEL**.
2. After the **CONTROL PANEL** appears, double-click the **NETWORK** icon to display the existing network configuration.
3. Select **TCP/IP** from the list of installed network components. If there are multiple sessions, select the one for the Ethernet card in the host computer.
4. Click **PROPERTIES**, which shows the existing properties of the TCP/IP protocol running on the host computer in a multi-paned window.
5. Select the **IP ADDRESS** pane by clicking on it.
6. Check the **SPECIFY AN IP ADDRESS** radio button.
7. Enter the **IP ADDRESS** as: 10.10.10.50 and **SUBNET MASK** as: 255.255.255.0.
8. Click **OK** to close the properties window.
9. Click **OK** on the network configuration window, which will ask you to reboot the browser computer.
10. Click **YES** to reboot your computer.

Browsing Hosts Running POSIX-Compliant UNIX

1. Log in as **root**, or change to **superuser**.
2. Run the **ifconfig** command **-a** option to list the configured network interfaces in the system. This will show the Ethernet interface name as well. For example:

```
#ifconfig -a
```

```
lo0: flags=863<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232 inet 127.0.0.1 netmask  
ff000000
```

```
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500  
inet 192.103.55.186 netmask ffffff00 broadcast 192.103.255.255
```

```
ether 8:0:20:a8:38:c6
```

3. Change the IP address of the Ethernet interface to 10.10.10.50 with subnet mask 255.255.255.0 by using the **ifconfig** command. For example:

```
# ifconfig eth0 10.10.10.50 netmask 255.255.255.0
```

4. Run the **ifconfig** command **-a** option again to make sure the interface address change is effective.

USER INTERFACE GUIDE

CONTENTS

Navigating the Administration Console	34
Administration Console	34
Menu Overview	35
Config	35
Admin	36
Policies	37
Monitor	38
Menu Descriptions	39
> Config	39
> Admin	47
> Logout	49
> Policies	50
Changing the Priority of a Policy	59
Default Access Policies	59
Changing the Priority of a Policy	64
Default Access Policies	64
Deleting A VPN Policy	64
Editing A VPN Policy	65
Viewing A VPN Policy	65
Changing Priority of A VPN Policy	65
ESP Configuration	67
AH Configuration	69
ESP Configuration	69
> Monitor	72

FIGURES

Figure 1. NetVanta 2000 series Administration Console	34
Figure 2. CONFIG Menu Information	35
Figure 3. ADMIN Menu Information	36
Figure 4. POLICIES Menu Information	37
Figure 5. MONITOR Menu Information	38

1. NAVIGATING THE ADMINISTRATION CONSOLE

The NetVanta 2000 series uses a web-based Administration Console for displaying both menu options and data fields. All menu options display in the Administration Console Header (see Figure 1), through which you have complete control of the NetVanta 2000 series.

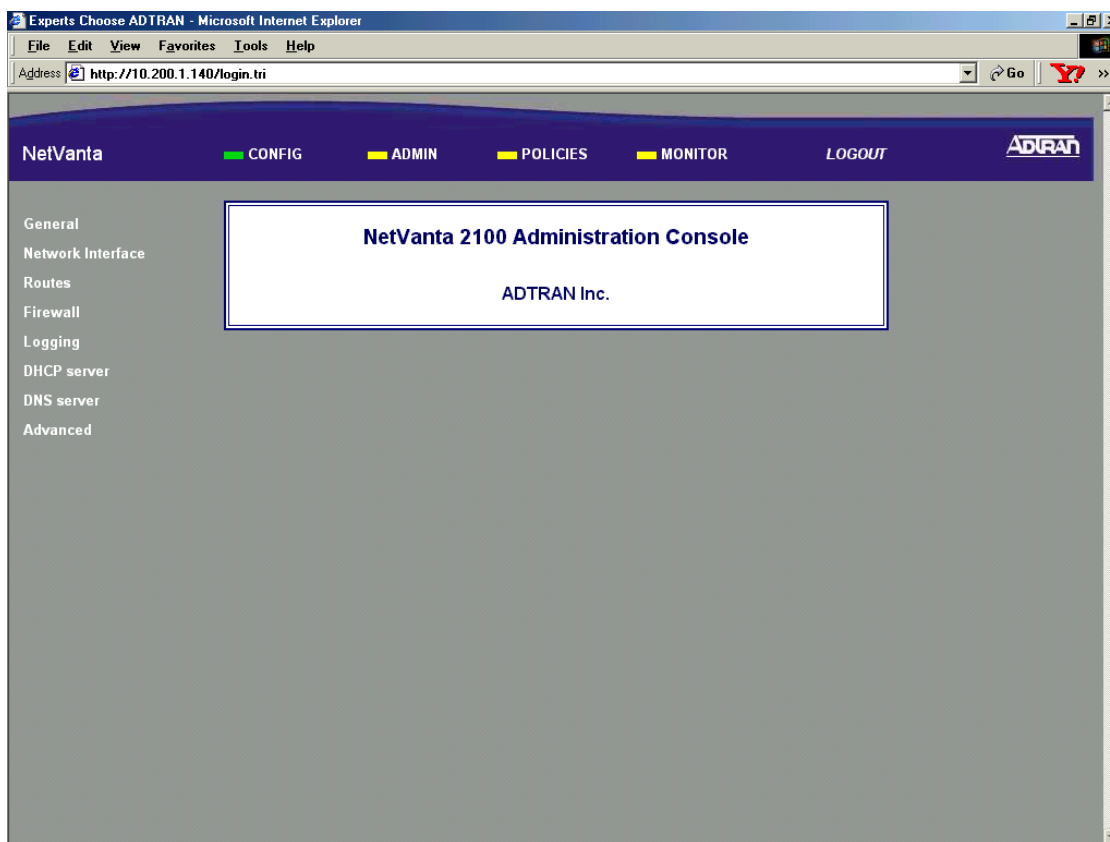


Figure 1. NetVanta 2000 series Administration Console

Administration Console

The **ADMINISTRATION CONSOLE** shows the available areas of configuration for the NetVanta 2000 series and the appropriate menu selections. This header remains visible as you navigate through the individual menu pages. The console contains a main menu bar and a menu list.

Menu Bar

The **ADMINISTRATION CONSOLE** menu bar displays the four areas of configuration for the NetVanta 2000 series. They are **CONFIG**, **ADMIN**, **POLICIES**, and **MONITOR**. Selecting an area of configuration by clicking on the hyperlink displays the applicable menu options in the menu list (located on the left side of the screen).

Menu List

The **ADMINISTRATION CONSOLE** menu list displays the selections available from the active menu (enable the desired menu from the menu bar). Each menu list selection is a hyperlink which displays the applicable menu items and data fields in the display window.

2. MENU OVERVIEW

The NetVanta 2000 series configuration is divided into four main areas: **CONFIG**, **ADMIN**, **POLICIES**, and **MONITOR**. This section gives a brief discussion of each area and the menu options available. *Menu Descriptions* on page 39 and following gives a more detailed discussion of these menu options.

CONFIG

The **CONFIG** menu contains the basic configuration parameters of the NetVanta 2000 series box including IP addresses assigned to the network interfaces, setting up a routing table, Firewall settings, and DHCP server configuration. Figure 2 shows the available menu options (displayed in the option list) for the **CONFIG** menu.

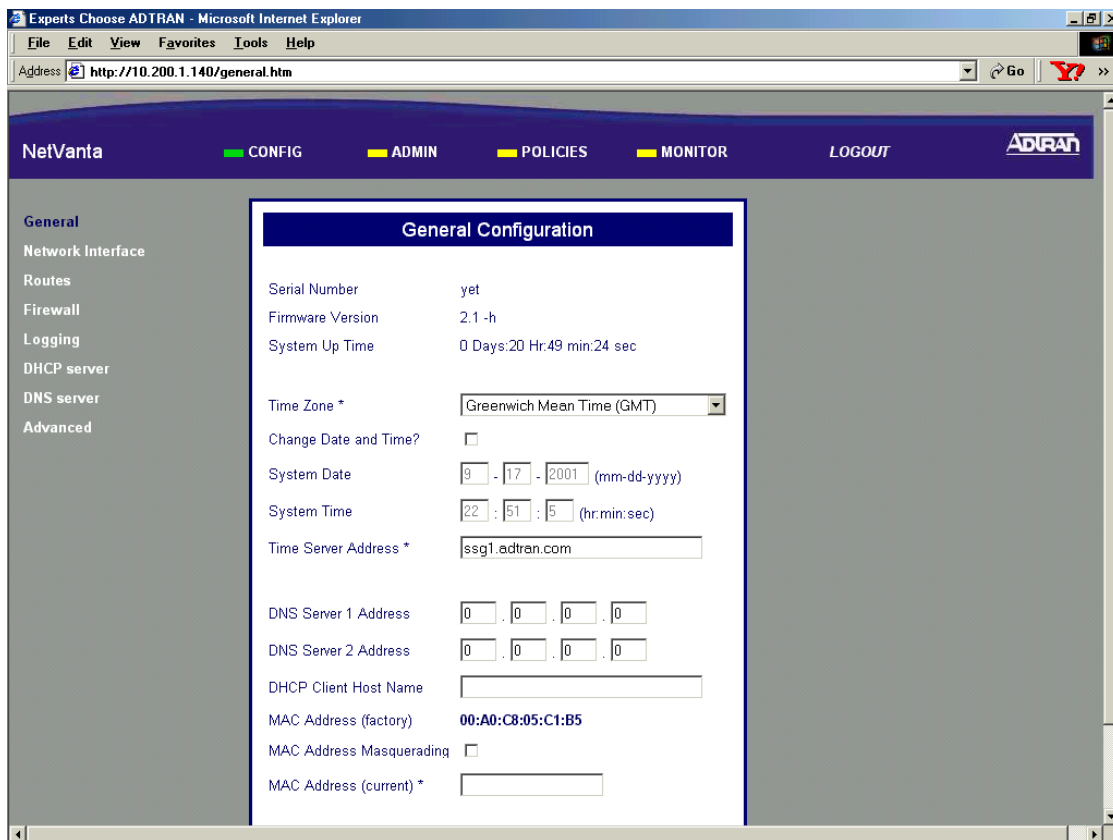


Figure 2. CONFIG Menu Information

ADMIN

The **ADMIN** menu contains the various system administration activities on the NetVanta 2000 series box such as changing the root password, saving the configuration to permanent storage, factory defaults, and rebooting the system. Figure 3 shows the available menu options (displayed in the option list) for the **ADMIN** menu.

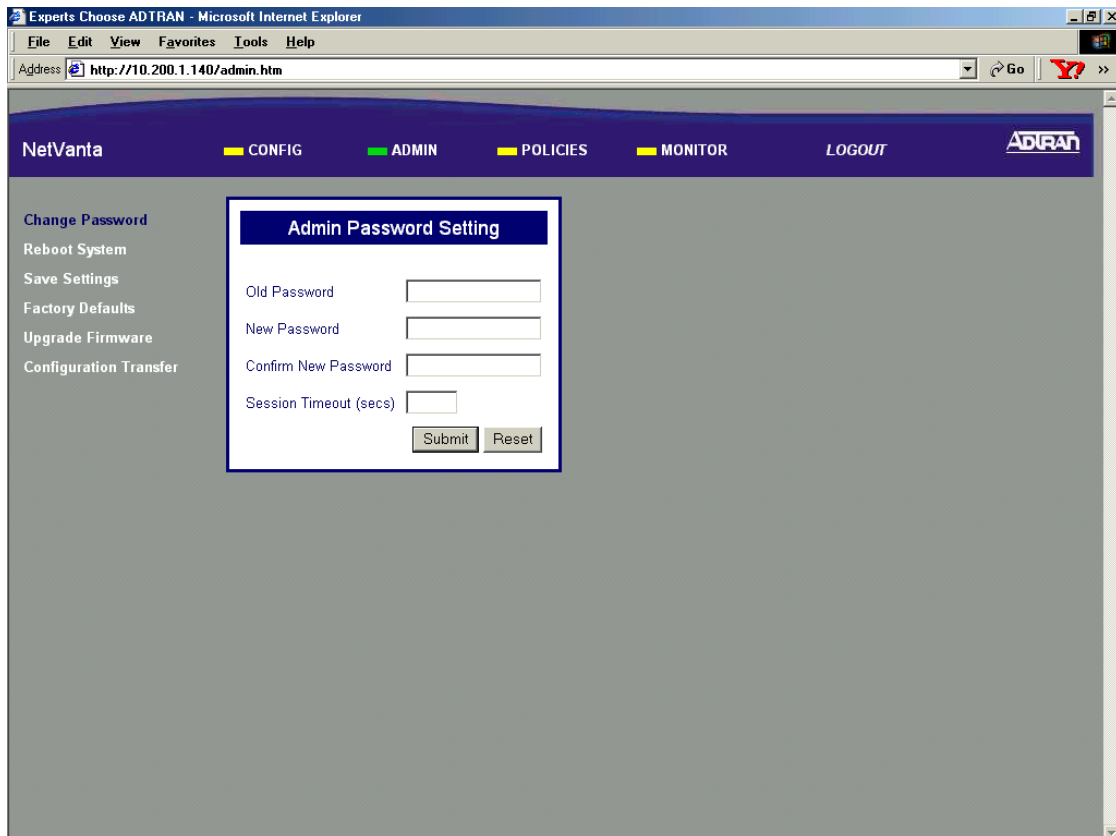


Figure 3. ADMIN Menu Information

POLICIES

The **POLICIES** menu contains the system wide access policies and user-group specific access policies. Through the available menu options you can define the policies and determine how to maintain different policy component tables (see Figure 4).

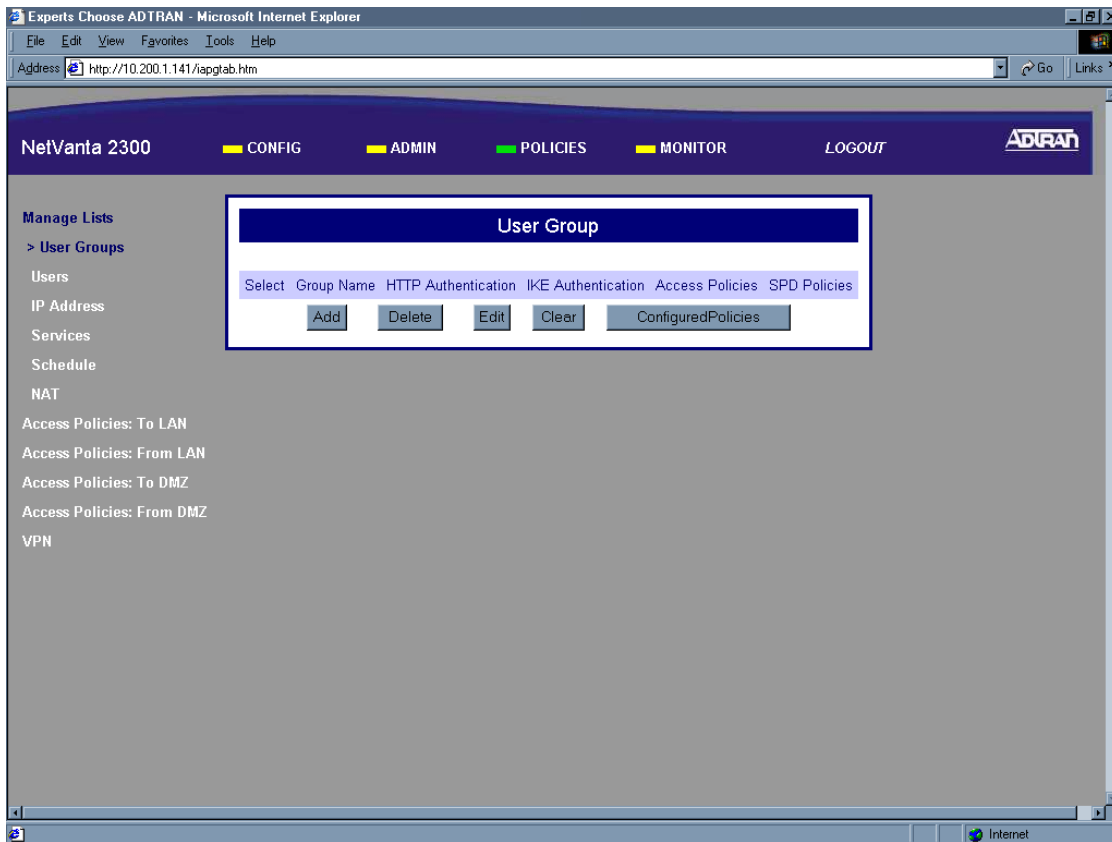


Figure 4. POLICIES Menu Information

MONITOR

The **MONITOR** menu contains all information pertinent to policy statistics, user accounting, and log usage. Through the available menu options you can view the status of remote user sessions, configure the log message categories, and view the log messages stored in the NetVanta 2000 series event log queue. Figure 5 shows the available menu options (displayed in the option list) for the **MONITOR** menu.

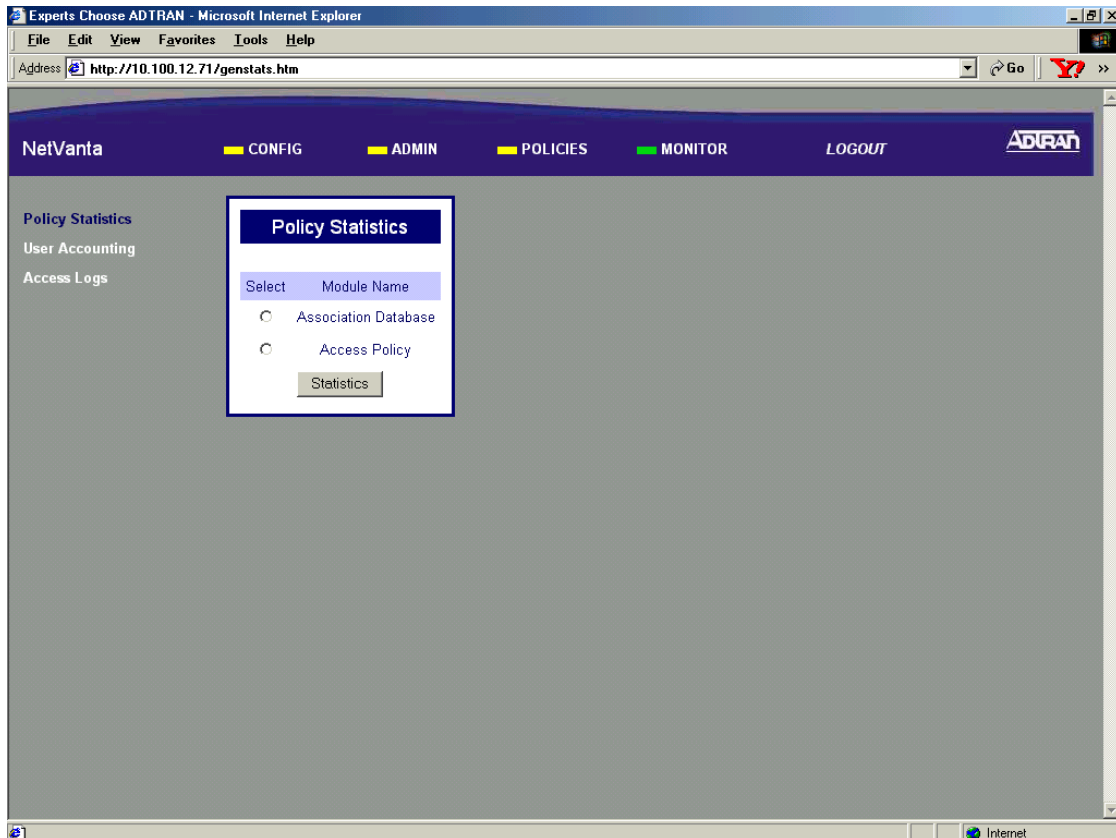


Figure 5. MONITOR Menu Information

3. MENU DESCRIPTIONS

The NetVanta 2000 series comes pre-configured with a default IP address of 10.10.10.1 assigned to the corporate interface (LAN). To begin the configuration of the NetVanta 2000 series, point the active browser on your computer to <http://10.10.10.1>. Once the browser has successfully connected to the unit you will be presented with the login screen. You must log in using a valid user name and password to start the NetVanta 2000 series configuration in a MD5 authenticated web session. When setting up the first MD5 authenticated session, the default user name is **admin**. There is no password set for this user. Refer to *DLP-001, Connecting to the Netvanta 2000 Series*, for more instructions on logging in to the unit.

Enter **admin** in the user name field and click on the **LOGIN NOW** button. The NetVanta 2000 series Welcome page will display after the login process has been successfully completed. You can now proceed with the NetVanta 2000 series configuration.



ADTRAN strongly recommends immediately changing the admin password. Refer to DLP-002, Changing the Admin Password in the NetVanta.

> CONFIG

This section discusses the basic configuration of the NetVanta 2000 series including IP addresses assigned to the network interfaces, setting up a routing table, Firewall settings, and DHCP server configuration.

The basic configuration of the NetVanta 2000 series can be displayed by clicking on the **CONFIG** menu on the Administration Console. Basic configuration includes setting the date and time on the box, network interface configuration, setting up the IP routing table, basic firewall configuration, event logging configuration, web proxy configuration, and DHCP (Dynamic Host Configuration Protocol) server configuration.

> CONFIG > GENERAL

The General Configuration page is displayed by clicking on **GENERAL** found in the menu list on the left side of the display window.

This page displays the important information of your NetVanta 2000 series system including the **SERIAL NUMBER**, current **FIRMWARE VERSION**, and **SYSTEM UP TIME**. Please have this information available before contacting the ADTRAN Technical Support team at (888) 4-ADTRAN (423-8726).

To set the system date and time, enter the current date in the form mm-dd-yyyy (example: March 3, 2001 is 03-03-2001) and time in the form hours:minutes:seconds (example 11:02 pm is 23:02:00). Select the **CHANGE DATE AND TIME?** checkbox and click the **SUBMIT** button to enter the new date and time.

The DNS server configuration for the NetVanta 2000 series is also located on the General Configuration page. If the NetVanta 2000 series needs to resolve domain names it will use the DNS server IP address configured here. Configuring a DNS server IP address is optional.

> CONFIG > NETWORK INTERFACE

The Network Interface configuration page is displayed by clicking on **NETWORK INTERFACE** found in the option list on the left side of the display window.

> CONFIG > NETWORK INTERFACE > ETHERNET CONFIG > ETHERNET IP ADDRESS

The **ETHERNET IP ADDRESS** section contains the information for both the Corporate (LAN) and WAN IP addresses, and subnet masks.

The **CORPORATE IP** and **SUBNET MASK** fields should be configured with parameters that correspond to the corporate network connected to the LAN interface located on the back of the NetVanta 2000 series unit.

The **WAN IP TYPE** should be set to **DYNAMIC** if your ISP is using DHCP to assign IP addresses dynamically or **STATIC** if your ISP has assigned you a specific IP address to use each time you connect. If your **WAN IP TYPE** is **STATIC**, the **WAN IP** and **SUBNET MASKS** fields should be configured with the specific information provided by your ISP.

The NetVanta 2000 series also supports PPPoE (PPP over Ethernet) to obtain a WAN interface IP address. Select the **PPPoE** radio button and enter the **USERNAME** and **PASSWORD** provided by your ISP in the appropriate fields.

> CONFIG > NETWORK INTERFACE > RIP CONFIG > RIP CONFIGURATION

The **RIP CONFIGURATION** field selects the RIP version being used by the NetVanta 2000 series. **RIPONE** is standard Rip V1. The NetVanta 2000 series supports RIP V1 on both the LAN and WAN interfaces. **RIP TWO** is standard RIP V2. NetVanta 2000 series supports RIP V2 on both the LAN and WAN interfaces. **RIPCOMP** is a combination of RIP V1 and RIP V2. When configured for **RIPCOMP**, the NetVanta 2000 series is capable of listening to RIP V1 updates while maintaining full compatibility with RIP V2 systems.

> CONFIG > NETWORK INTERFACE > RIP CONFIG > AUTHENTICATION TYPE

The Authentication Type field configures the NetVanta 2000 series to use the selected authentication when performing RIP functions. If authentication is configured, other systems providing the NetVanta 2000 series with RIP updates must be configured for matching authentication. The NetVanta 2000 series supports both **SIMPLEAUTH** (using a single password) or MD5 authentication (requiring the use of keys entered in the **MD5 AUTH KEY ID** and **MD5 AUTH KEY** fields).

> CONFIG > NETWORK INTERFACE > DHCP INFO

The **DHCP INFO** table for the NetVanta 2000 series displays the current DHCP client interface information for both the LAN and WAN ports. This table is only valid if the NetVanta 2000 series is connected to a network with an active DHCP server.

> CONFIG > ROUTES

The Routing table for the NetVanta 2000 series can be reached by clicking on **ROUTES** found in the menu list on the left side of the display window. The following is a description of the routing table fields.

> CONFIG > ROUTES > DESTINATION IP

The **DESTINATION IP** address field displays the IP address of the destination network for the route. The NetVanta 2000 series uses this information when making routing decisions.

> CONFIG > ROUTES > INTERFACE NAME

The **INTERFACE NAME** field displays the name of the interface that is accessed to send data using the listed route. The options are: **ETH0** (the **LAN** port located on the back panel of the unit) and **ETH1** (the **WAN** port located on the back panel of the unit).

> CONFIG > ROUTES > NETMASK

The **NET MASK** field displays the current subnet mask used for the listed route. Subnet masks are used to identify subnetworks to allow for IP sharing on a LAN.

> CONFIG > ROUTES > GATEWAY IP

The **GATEWAY IP** field displays the IP address of the first intelligent device that intercepts and steers data for its assigned network. The IP route table for the gateway of a network should contain routes to all available subnets on the network.

> CONFIG > ROUTES > HOP COUNT

The **HOP COUNT** field displays the number of gateways datagrams pass through when taking this route to their destination.

> CONFIG > ROUTES > TYPE

The **TYPE** field designates whether a route was configured or learned. Configured routes show up as **LOCAL**. Learned routes show up as **DYNAMIC**.

> CONFIG > ROUTES > DELETE ROUTE

Select the routing entry you want to delete by choosing the corresponding checkbox and clicking the **DELETE ROUTE** button. This will delete the selected route entry.



*Before clicking the **DELETE ROUTE** button, make sure that you have selected the correct routing entry. Removing the routing entry for a destination may make it inaccessible.*

> CONFIG > FIREWALL

The **FIREWALL CONFIGURATION** page can be accessed by clicking on **FIREWALL** found in the menu list on the left side of the display window. This page provides control to activate different cyber attack checks. The event logging thresholds for cyber attacks are also configured on the **FIREWALL CONFIGURATION** page.

> CONFIG > FIREWALL > IP SPOOFING CHECK

IP Spoofing is a network intrusion that occurs when an outside user gains access to a computer on the network by pretending to be at a trusted IP address. **IP SPOOFING CHECK** is always **ENABLED**, and the NetVanta 2000 series discards any packets received on the WAN interface containing a source IP address on the corporate network.

> CONFIG > FIREWALL > PING OF DEATH CHECK

Ping of Death is a denial of service attack which exploits the errors in the oversize datagram handling mechanism of a TCP/IP stack. Many popular operating systems have difficulty handling datagrams larger than the maximum datagram size defined by the IP standard. If hosts running these operating systems encounter oversized ping packets, it is likely they will hang or crash causing network problems. **PING OF DEATH CHECK** is always **ENABLED**, and the NetVanta 2000 series becomes the central entry point for all traffic entering the corporate network and it watches for such non-standard IP datagrams to filter them before they reach vulnerable hosts on the network.

> CONFIG > FIREWALL > LAND ATTACKS CHECK

Land Attacks are a special type of denial of service attack on TCP-based services such as HTTP, SMTP, and FTP. In a Land Attack an attacker forges the equal values for the source and destination port, and source and destination IP addresses. These port values are often the well-known service port values, and the IP addresses are the target hosts' IP address. This attack exploits the inappropriate implementation of the TCP connections establishment protocol in a TCP/IP stack; as a result the target server enters an uncontrollable infinite spin and eventually the system crashes. **LAND ATTACK CHECK** is always **ENABLED**, and the NetVanta 2000 series ensures that all service requests made to any of the hosts in the corporate network are Land Attack free.

> CONFIG > FIREWALL > REASSEMBLY ATTACK

Datagrams traveling in the Internet may pass through heterogeneous networks which require them to be fragmented and reassembled at their destinations. Certain popular TCP/IP implementations cannot handle all datagram reassembly scenarios properly. If an attacker sends datagram fragments to a host with limited datagram reassembly capabilities the host is likely to behave unpredictably. **REASSEMBLY ATTACK** is always **ENABLED**, and the NetVanta 2000 series invokes its robust datagram reassembly engine to perform the datagram reassembly strictly conforming to IP standards.

> CONFIG > FIREWALL > SYN FLOODING ATTACK CHECK

SYN Flooding is a well-known denial of service attack on TCP based services. TCP requires a 3-way handshake before the actual communications between two hosts begins. A server must allocate resources to process new connection requests that are received. A malicious intruder is capable of transmitting large amounts of service requests in a very short period causing servers to allocate all resources to process the incoming requests. If **SYN FLOODING ATTACK CHECK** is selected, the NetVanta 2000 series filters out phony service requests and allows only legitimate requests to pass through.

> CONFIG > FIREWALL > ICMP REDIRECT CHECK

ICMP Redirect is a standard ICMP message used to provide hosts with better route information to the source. When this message is received, the recipient updates its routing table with the new routing information provided with no authentication required. An intruder can provide a target with the route information of his or her interest thereby gaining access to the hosts routing table. It is possible for an intruder to access the data originated from the target hosts once the hosts routing table has been compromised. If **ICMP REDIRECT CHECK** is **ENABLED**, the NetVanta 2000 series discards all ICMP Redirect messages.

> CONFIG > FIREWALL > SOURCE ROUTING CHECK

Strict and loose source routing (as specified in IP standard RFC 791) allows datagrams to take a predefined path towards a destination. An intruder can gain detailed information about the corporate network by tracking datagrams through the corporate network. If **SOURCE ROUTING CHECK** is **ENABLED**, the NetVanta 2000 series filters out all datagrams that contain the strict or loose source routing option.

> CONFIG > FIREWALL > WINNUKE ATTACK CHECK

WinNuke attack is a well-known denial of service attack on hosts running Windows operating systems. A malicious intruder sends Out of Band (OOB) data over an established connection to a Windows user. Windows cannot properly handle the OOB data and the host reacts unpredictably. Normal shut-down of the hosts will generally return all functionality. If **WINNUKE ATTACK CHECK** is selected, the NetVanta 2000 series filters OOB data to prevent network problems.

> CONFIG > FIREWALL > EVENT LOGGING THRESHOLDS

Event logging thresholds prevent large quantities of duplicate logs if the NetVanta 2000 series or the corporate network connected to it is under attack.

The **LOG ATTACKS FOR EVERY** threshold indicates the number of attack mounting attempts the NetVanta 2000 series should see before generating a log message. The default value for an attack log threshold is 100.

The **LOG POLICY FOR EVERY** threshold defines the number of connections required by an access policy through the NetVanta 2000 series before a log message is generated for that policy. The default value for the policy access log threshold is 100.

The **LOG VPN FOR EVERY** threshold defines the number of VPN enabled connections required by a VPN policy before generating a log message for that policy. The default value for the VPN log threshold is 100.

> CONFIG > LOGGING

The NetVanta 2000 series periodically exports event log messages to well-secured external systems for secondary storage. The NetVanta 2000 series provides two industry-standard ways to export the event log: e-mail and syslog. Log messages may be e-mailed to specified addresses, exported to a standard syslog service, or a combination of both. The Logging Configuration page is displayed by clicking on Logging in the menu list on the left side of the display window.

> CONFIG > LOGGING > LOG EXPORT SYSTEM

The Syslog Configuration page is displayed by clicking on the **LOG EXPORT SYSTEM** hyperlink listed as a Logging submenu in the menu list. The configuration parameters for exporting event log messages using the syslog service are displayed on this page.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > LOG QUEUE LENGTH

The **LOG QUEUE LENGTH** field defines the number of events to be collected in the log queue before triggering the log export process.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > LOGTIME THRESHOLD

The **LOGTIME THRESHOLD** defines the maximum time interval (in minutes) which passes before triggering the log export process.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > DEVICE NAME

The **DEVICE NAME** field is an alphanumeric string attached to each log and alert message. This helps identify the event log messages generated by the NetVanta 2000 series in a common log file. Using a descriptive firewall name is useful when searching through the large log files.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > ENABLE SYSLOG NOTIFICATION

The **ENABLE SYSLOG NOTIFICATION** check box configures the NetVanta 2000 series to export the log to the syslog service.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > SYSLOG SERVER

The **SYSLOG SERVER** field defines the syslog server's IP address. The syslog server should be maintained on the corporate network.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > SYSLOG FACILITY

The **SYSLOG FACILITY** drop-down menu selects the syslog priority level which the NetVanta 2000 series uses for exporting log entries to the syslog service. Nine priority levels are provided ranging from **SYSLOG_LOCAL0** to **SYSLOG_LOCAL8**. Choose any one of these priority levels and configure the syslog service accordingly. For configuring the syslog service on the server, refer to the syslog documentation.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > ENABLE E-MAIL NOTIFICATION

The **ENABLE E-MAIL NOTIFICATION** check box configures the NetVanta 2000 series to export event logs through e-mail.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > MAIL SERVER ADDRESS

The **MAIL SERVER ADDRESS** field defines the IP address of the SMTP server used by the NetVanta 2000 series to e-mail out the log.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > RETURN MAIL ADDRESS

The **RETURN MAIL ADDRESS** field is an alphanumeric string that appears in the ‘**From:**’ field in all e-mail containing the NetVanta 2000 series event log messages.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > EMAIL GENERAL LOG TO:

The **EMAIL GENERAL LOG TO:** address is used by the NetVanta 2000 series when exporting event log messages via e-mail.

> CONFIG > LOGGING > LOG EXPORT SYSTEM > EMAIL ALERT LOG TO:

The **EMAIL ALERT LOG TO:** address allows the NetVanta 2000 series to send alert logs only to the specified address.

> CONFIG > DHCP SERVER

The NetVanta 2000 series is equipped with Dynamic Host Configuration Protocol (DHCP) server capabilities. A DHCP server eliminates static network configuration for hosts connected to the corporate network by configuring them dynamically. A DHCP server manages the IP address pool in the corporate network by leasing IP addresses to requesting hosts. It also supplies DNS configuration and default route information to the requesting hosts. All requesting hosts must be running DHCP enabled operating systems.

> CONFIG > DHCP SERVER > DHCP CONFIG

The **DHCP CONFIG** page is displayed by clicking on the **DHCP CONFIG** hyperlink listed as a DHCP server submenu in the menu list. A description of the DHCP Server Configuration parameters follows.

> CONFIG > DHCP SERVER > DHCP CONFIG > DHCP ENABLED

The **DHCP ENABLED** radio button allows you to enable or disable the DHCP server capabilities of NetVanta 2000 series.

> CONFIG > DHCP SERVER > DHCP CONFIG > IP ADDRESS RANGE

IP ADDRESS RANGE (1-3) fields specify up to three disjoint IP address ranges for leasing IP addresses to DHCP enabled hosts. The IP address ranges must be included in the corporate network.

> CONFIG > DHCP SERVER > DHCP CONFIG > GATEWAY IP ADDRESS

The **GATEWAY IP ADDRESS** field specifies the default gateway supplied to DHCP enabled hosts. Normal configuration requires this to be populated with the IP address assigned to the LAN port of NetVanta 2000 series.

> CONFIG > DHCP SERVER > DHCP CONFIG > DNS1/DNS2

The **DNS 1-2** fields define the primary and secondary DNS server IP addresses supplied to the DHCP enabled hosts in the corporate network.

> CONFIG > DHCP SERVER > DHCP CONFIG > LEASE DURATION

The **LEASE DURATION** field defines the amount of time (in seconds) that a DHCP enabled host may lease an assigned IP address. At the end of the lease duration, the host must send the DHCP server a lease renewal request for the assigned IP address. If the request is denied the host must relinquish the address and send a request for a new IP address to be assigned.

> CONFIG > DHCP SERVER > ACTIVE LEASES

The **ACTIVE LEASES** page displays the DHCP leases that have been assigned (by the NetVanta 2000 series DHCP server) to devices located on the LAN network.

> CONFIG > DNS SERVER

The NetVanta 2000 series comes equipped with a DNS server. To enter DNS names to the DNS Server lookup table, enter the **DNS NAME** in the appropriate field and the corresponding IP address beside it in the **IP ADDRESS** field.

> CONFIG > ADVANCED

The **ADVANCED CONFIGURATION** page is displayed by clicking **ADVANCED** in the menu list located on the left side of the display window. The NetVanta 2000 series advanced configuration includes, box access configuration and service timeout parameters.

> CONFIG > ADVANCED > BOX ACCESS

The Box Access **CONFIGURATION** page is displayed by clicking on the **BOX ACCESS** hyperlink listed as an Advanced Configuration submenu in the menu list. This page defines the access scheme for the NetVanta 2000 series system including both corporate network (LAN) and Internet (WAN) access.

> CONFIG > ADVANCED > BOX ACCESS > LAN

The **ALWAYS ALLOW ADMIN LOGIN** field defines a specific IP address that overrides the **ALLOW ADMIN LOGIN** status for the NetVanta 2000 series corporate network (LAN) interface. NetVanta 2000 series remote administration is always allowed from the host having the specific IP address configured in this field.



*Only use a trusted host IP address in the **ALWAYS ALLOW ADMIN LOGIN** field.*

The **ALLOW ADMIN LOGIN** check box enables the NetVanta 2000 series HTTP configuration access from the corporate network (LAN) interface. By default, HTTP configuration access is enabled from the corporate network (LAN) interface.

The **ALLOW PING** check box controls the NetVanta 2000 series's response to ICMP Echo Request messages received on the corporate network (LAN) interface. Selecting this checkbox configures the NetVanta 2000 series to reply to the ICMP Echo Request received on the LAN interface. By default, Ping response is enabled on the corporate network (LAN) interface.

> CONFIG > ADVANCED > BOX ACCESS > WAN

The **ALLOW ADMIN LOGIN** check box enables the NetVanta 2000 series HTTP configuration access from the Internet (WAN) interface. By default, HTTP configuration access is disabled on the Internet (WAN) interface.

The **ALLOW PING** check box controls the NetVanta 2000 series's response to ICMP Echo Request messages received on the Internet (WAN) interface. Selecting this checkbox configures the NetVanta 2000 series to reply to the ICMP Echo Request received on the WAN interface. By default, Ping response is disabled on the Internet (WAN) interface.

Disabling ping on the Internet (WAN) network interface filters out ICMP-based trace route traffic and gives implicit protection to the ADVANTA 2100 and the corporate network behind it from many ICMP Echo message based cyber attacks (Ping of Death, Ping Flood, Smurf, etc.).

The **ALLOW TELNET** check box enables telnet access to the NetVanta 2000 series system on the Internet (WAN) interface. By default, telnet access to the ADVANTA 2100 is disabled on the Internet (WAN) interface.

> ADMIN

This section discusses all system administration activities including changing passwords, saving the NetVanta 2000 series configuration to permanent storage, and factory defaulting the system. The system administration options can be displayed by clicking on the **ADMIN** menu on the Administration Console.

> ADMIN > CHANGE PASSWORD

The Password Setting page allows the user to change the current password. Click on **CHANGE PASSWORD** found in the menu list on the left side of the display window. Refer to DLP-002, *Changing the Admin Password in the NetVanta* for more details.

> ADMIN > CHANGE PASSWORD > OLD PASSWORD

Enter the existing password in the **OLD PASSWORD** field. Leave this field blank when setting the admin password for the first time.

> ADMIN > CHANGE PASSWORD > NEW PASSWORD

Enter the new password in the **NEW PASSWORD** field. A valid password is any alphanumeric string up to 16 characters in length.

> ADMIN > CHANGE PASSWORD > CONFIRM NEW PASSWORD

Re-enter the new password in the **CONFIRM NEW PASSWORD** field.

> ADMIN > CHANGE PASSWORD > SESSION TIMEOUT

The **SESSION TIMEOUT** field defines the length of time (in seconds) that a user session may be inactive before the NetVanta 2000 series automatically performs a forced logout. The default **SESSION TIMEOUT** is 300 seconds.

> ADMIN > REBOOT SYSTEM

The Reboot System page allows users to reboot the NetVanta 2000 series system from a remote location. Click on **REBOOT SYSTEM** found in the option list on the left side of the display window to display the Reboot System page.

Rebooting the NetVanta 2000 series system requires confirmation. Click **YES** to proceed with the reboot sequence or **NO** to cancel. When you restart the system, the following actions take place:

1. The NetVanta 2000 series is unresponsive until the system reboot sequence is complete.
2. All network accesses currently active in the system will be terminated/interrupted until the system reboot sequence is complete.
3. The NetVanta 2000 series reboot sequence is approximately 30 seconds in length. To resume configuration of the NetVanta 2000 series successfully complete the login procedures.
4. After a system reboot, the NetVanta 2000 series resumes service using the last saved configuration. To ensure a configuration change becomes permanent save the configuration once all changes are complete. For saving configuration procedure details refer to > *Admin > Save Settings* on page 48.

> ADMIN > SAVE SETTINGS

During an NetVanta 2000 series web session all configuration changes are immediately implemented. The updated configuration is not saved to flash memory until a manual configuration download is performed. Until the configuration is saved to flash memory, it is not available across power failures and system reboots. To save the current configuration of the NetVanta 2000 series, click on **SAVE SETTINGS** found in the option list on the left side of the display window. Saving the NetVanta 2000 series system configuration requires confirmation. Click **YES** to proceed with the configuration download or **NO** to cancel. Once the configuration download is complete a confirmation message is displayed. Refer to DLP-003, *Saving the Current Settings of the NetVanta* for more details.

> ADMIN > FACTORY DEFAULTS

Restore the NetVanta 2000 series to default configuration by clicking on **FACTORY DEFAULTS** found in the menu list on the left side of the display window. Factory defaulting the NetVanta 2000 series requires confirmation. Click **YES** to proceed with the factory default process or **NO** to cancel. During the factory default process, the NetVanta 2000 series erases the current configuration from memory and displays the operation progress. When the configuration erase procedure is complete (estimated duration is a few seconds) an operation completion message will be displayed and you will be instructed to reboot the system manually to restore the factory default configuration. Refer to > *Admin > Reboot System* on page 48 for instructions on rebooting the NetVanta 2000 series system. Refer to DLP-021, *Restoring the NetVanta to Factory Defaults* for more details.

> ADMIN > UPGRADE FIRMWARE

The NetVanta 2000 series firmware may be upgraded using the **UPGRADE FIRMWARE** page. Refer to DLP-008, *Upgrading the Firmware of the NetVanta 2000 series* for more details.



When displaying the **UPGRADE FIRMWARE** page, a Windows security warning page will be displayed. Install and run the necessary file to continue the upgrade firmware process. This file is signed with full permissions by ADTRAN, Inc.

> ADMIN > CONFIGURATION TRANSFER

The NetVanta 2000 series supports configuration transfers from the unit (via either the LAN or WAN interface) using an active browser session.

> ADMIN > CONFIGURATION TRANSFER > CONFIGURATION DOWNLOAD

The NetVanta 2000 series configuration can be saved to a file by clicking on the **DOWNLOAD** button in the **CONFIGURATION DOWNLOAD** dialog box under **CONFIGURATION TRANSFER**. The **WINDOWS DOWNLOAD** dialog box will appear, indicating that you have chosen to download a **.bin** file from this location. Select **SAVE THIS FILE TO DISK** and click **OK**. When the **WINDOWS SAVE AS** dialog box appears, enter the filename and select the location in which to store it. Click the **SAVE** button. A **WINDOWS DOWNLOAD COMPLETE** dialog box will appear, indicating the download is complete and the file has been saved. Click on **CLOSE**. Refer to DLP-009, *Saving the Current Configuration of the NetVanta* for more details.



If you want the **DOWNLOAD COMPLETE** dialog box to automatically close when the download is complete, select that option inside the **WINDOWS DOWNLOAD COMPLETE** dialog box prior to selecting **CLOSE**.

> ADMIN > CONFIGURATION TRANSFER > CONFIGURATION UPLOAD

A configuration can be uploaded into the NetVanta 2000 series by choosing the **CONFIGURATION UPLOAD** dialog box under **CONFIGURATION TRANSFER**. If the filename is known, it can be entered directly into the file box. If the filename is not known, the user may select the **BROWSE** button. After clicking **BROWSE**, a Windows file browser will display. Select the appropriate file and click **OPEN**. Once the correct filename appears in the file box, click the **UPLOAD** button. The following message will display:

Upload done. The unit is rebooting with the new configuration...

After waiting for the unit to complete the reboot cycle, the user should close out the active browser session, initiate a new session, and login to the unit as before. Refer to DLP-010, *Loading a Saved Configuration into the NetVanta* for more details.

> LOGOUT

To logout of the NetVanta 2000 series system, click on **LOGOUT** found on the right side of the menu bar. Logging out requires confirmation by clicking the **LOGOUT** button on the logout confirmation dialog. After confirming the logout, the web session will immediately be terminated and the **LOGGED OUT SUCCESSFULLY** page will be displayed.

> POLICIES

This configuration section describes the various NetVanta 2000 series policies, including user access and VPN policies, and how to create and maintain different policy component tables. To make the policies configuration process easier, the NetVanta 2000 series is equipped with policy component tables that store configuration parameters that are used repetitively during configuration. These tables are divided into six categories: Users, User Groups, IP Address, Services, Schedule, and NAT. Policy component tables make policy configuration quick and dynamic. The policy component tables and their respective applications are discussed in this chapter.

The Policies Configuration page is displayed by clicking the **POLICIES** menu found on the Administration Console. All access policies and policy component tables are accessed and configured through the **POLICIES** menu. These include Corporate Inbound and Outbound policies, VPN policies, and User-Group Access policies.

> POLICIES > MANAGE LISTS

The Manage Lists Configuration page contains information and configuration parameters for the six policy component table categories and is displayed by clicking on **MANAGE LISTS** found in the option list on the left side of the display window.

> POLICIES > MANAGE LISTS > USERS

The Users table is used to define and classify the user community. To display the Users table, click on the **USER** hyperlink shown as a Manage Lists submenu in the menu list on the left side of the display window. Refer to *DLP-014, Adding a User to the Users Component Table* for more details.

> POLICIES > MANAGE LISTS > USERS > USER NAME

The **USER NAME** field defines an alphanumeric string (up to 64 characters in length) used as the user login name. The ADVANTA 2100 users use this respective **USER NAME** as a trigger to activate individual access and VPN policies.

> POLICIES > MANAGE LISTS > USERS > PASSWORD

The Password field defines an alphanumeric string (up to 64 characters in length) used as the user password used for web based authentication.

> POLICIES > MANAGE LISTS > USERS > CONFIRM PASSWORD

Re-enter the user password from the **PASSWORD** field in the **CONFIRM PASSWORD** text box.

> POLICIES > MANAGE LISTS > USERS > GROUP NAME

The **GROUP NAME** drop down menu defines the user group this user is assigned to.



*A user group must be configured in the **USER GROUP** table, before a specific user may be added. Refer to *DLP-013, Defining a User Group in the NetVanta*, for more details.*

> POLICIES > MANAGE LISTS > USER GROUPS

The User Groups table allows you to classify your network user community into multiple sets of similar users. Access and VPN policies can be created for a specific user group and members can be added/removed dynamically. For example, a user wants to access the Internet from the corporate network or vice versa and is required to login to the ADVANTA 2100 box first. Once the login is successful, the ADVANTA 2100 finds the user group for the new user. The NetVanta 2000 series then makes a copy of the user group's network access and VPN policies and activates them for the user's IP address.

The User Groups table is displayed by clicking on the **USER GROUPS** hyperlink shown as a Manage Lists submenu in the menu list on the left side of the display window. Refer to DLP-013, *Defining a User Group in the NetVanta* for more details.

> POLICIES > MANAGE LISTS > USER GROUPS > GROUP NAME

The **GROUP NAME** field defines an alphanumeric string (up to 20 characters) used as the name of the user group.

> POLICIES > MANAGE LISTS > USER GROUPS > AUTHENTICATION TYPE

The **AUTHENTICATION TYPE** checkbox allows you to set the authentication type for the selected user group for either HTTP or IKE. Enabling this option allows all users belonging to this user group to login to the ADVANTA 2100 and activate their policies. If this checkbox is left unchecked, the user group is disabled and members of the group cannot login to the NetVanta 2000 series.

> POLICIES > MANAGE LISTS > USER GROUPS > IKE POLICY NAME

The **IKE POLICY NAME** drop down menu displays a list of all available IKE policies.



*If **AUTHENTICATION TYPE** is set to **IKE**, a specific **IKE** policy must be selected in the **IKE POLICY NAME** field.*

> POLICIES > MANAGE LISTS > IP ADDRESS

The IP Address table is used to save frequently used IP addresses. To display the IP Address table, click on the IP Address hyperlink shown as a Manage Lists submenu in the menu list on the left side of the display window. Refer to DLP-015, *Using the IP Address Component Table* for more details.

> POLICIES > MANAGE LISTS > IP ADDRESS > IP NAME

The **IP NAME** field defines an alphanumeric string (up to 64 characters) used as the identifier for the IP address group.

> POLICIES > MANAGE LISTS > IP ADDRESS > ADDRESS CATEGORY

The **ADDRESS CATEGORY** field configures the IP address group to be an IP **RANGE**, an IP **SUBNET**, a **SINGLE** IP address, or **ANY** IP address.

An IP **RANGE** is a set of IP addresses defined by start and end addresses. To add an IP **RANGE**, enter the start IP Address in the **IP ADDRESS 1** field and the end address in the **IP ADDRESS 2** field.

An IP **SUBNET** is a set of IP addresses defined by a network address and subnet mask. To add an IP **SUBNET**, enter the network address in the **IP ADDRESS 1** field and the subnet mask in the **IP ADDRESS 2** field.



*To add a **SINGLE** IP Address, enter the specific address in the **IP ADDRESS 1** field.*

> POLICIES > MANAGE LISTS > SERVICES

The Services table defines the transport protocol options and configuration parameters. The Services table is displayed by clicking on the **SERVICES** hyperlink shown as a Manage Lists submenu in the option list on the left side of the display window. Refer to DLP-016, *Adding a Service to the Services Component Table* for more details.

> POLICIES > MANAGE LISTS > SERVICES > SERVICE NAME

The **SERVICE NAME** field defines an alphanumeric string (up to 20 characters) used as the display name for the service.

> POLICIES > MANAGE LISTS > SERVICES > PROTOCOL TYPE

The **PROTOCOL** radio button allows you to define the transport protocol used by this service.

> POLICIES > MANAGE LISTS > SERVICES > SERVICE PORT

The **PORT NUMBER** field defines the port number used by this service.

> POLICIES > MANAGE LISTS > SCHEDULE

The Time Schedule table is used to define weekly time schedules to use when defining policies. To display the Time Schedule table, click on the **SCHEDULE** hyperlink shown as a Manage List submenu in the menu list on the left side of the display window.

To add a new time schedule record to the Time Schedule table, click the **ADD** button in the Time Schedule dialog box. The Time Window Configuration page is displayed. A discussion of the fields listed on the Time Window Configuration page follows.

> POLICIES > MANAGE LISTS > SCHEDULE > WINDOW NAME

The **WINDOW NAME** field defines an alphanumeric string (up to 20 characters) used as the identifying name of the time schedule record.

> POLICIES > MANAGE LISTS > SCHEDULE > OPTION 1, 2, 3

The **OPTION (1-3)** field allows you to define up to three distinct time windows in a week.

> POLICIES > MANAGE LISTS > SCHEDULE > WORKING DAYS

The **WORKING DAYS** drop down menus define the start and end days of the time interval for the selected option.

> POLICIES > MANAGE LISTS > SCHEDULE > OPEN HRS AND MINS

The **OPEN HRS & MINS** drop down menus define the beginning of the time interval in hours and minutes on each week day configured in the **WORKING DAYS** field.

> POLICIES > MANAGE LISTS > SCHEDULE > CLOSE HRS AND MINS

The **CLOSE HRS & MINS** drop down menus define the end of the time interval in hours and minutes on each week day configured in the **WORKING DAYS** field.

> POLICIES > MANAGE LISTS > NAT

The NAT table is displayed by clicking on the NAT hyperlink shown as a Manage Lists submenu in the option list on the left side of the display window.

To add a new NAT filter scheme to the NAT table, click the **ADD** button found in the NAT Configuration dialog box. The NAT Configuration page is displayed. A discussion of the fields on the NAT Configuration page follows.

> POLICIES > MANAGE LISTS > NAT > NAT NAME

The **NAT NAME** field defines an alphanumeric string (up to 20 characters) assigned to this NAT content filtering scheme.

> POLICIES > MANAGE LISTS > NAT > MANY TO ONE MAPPING - FROM LAN POLICY

Many to One Mapping configures the NetVanta 2000 series to use the defined NAT parameters on all traffic associated with the particular From LAN policy that references the NAT record. To NAT all policy specific traffic to a specific public IP address, enter the IP address in the **NAT IP ADDRESS** field. To NAT all policy traffic to the IP address associated with a particular interface, select the interface name from the Dynamic Interface drop down menu. Enabling NAT on the From LAN policy and selecting the NAT name from the drop down menu will activate the NAT configuration.

> POLICIES > MANAGE LISTS > NAT > MANY TO ONE MAPPING - TO LAN POLICY

Many to One Mapping configures the NetVanta 2000 series to use the defined NAT parameters on all traffic associated with the particular To LAN policy that references the NAT record. To Reverse NAT all policy specific traffic to a specific private IP address, enter the IP address in the **NAT IP ADDRESS** field. Enabling NAT on the To LAN policy and selecting the NAT name from the drop down menu will activate the NAT configuration.

> POLICIES > MANAGE LISTS > NAT > ONE TO ONE MAPPING - FROM LAN POLICY

One to One Mapping configures the NetVanta 2000 series to perform NAT on traffic (associated with a particular policy) that originates from a specified range of IP addresses. One to One NAT requires a specified range of public IP addresses to use while performing NAT. Enter the range of private IP addresses to NAT in the Source Range fields. Enter the range of public IP addresses to be used while performing NAT in the Destination Range fields.



The number of IP address in the specified Source and Destination Range fields must match for One to One Mapping.

Enabling NAT on the LAN Outbound policy and selecting the NAT name from the drop down menu will activate the NAT configuration.

> POLICIES > MANAGE LISTS > NAT > ONE TO ONE MAPPING - TO LAN POLICY

One to One Mapping configures the NetVanta 2000 series to perform NAT on traffic (associated with a particular policy) that originates from a specified range of IP addresses. One to One NAT requires a specified rate of public IP addresses to use while performing NAT. Enter the range of public IP addresses to NAT in the Source Range fields. Enter the range of private IP addresses to be used while performing NAT in the Destination Range fields.



The number of IP address in the specified Source and Destination Range fields must match for One to One Mapping.

Enabling NAT on the To LAN policy and selecting the NAT name from the drop down menu will activate the NAT configuration.

> POLICIES > ACCESS POLICIES: TO LAN

The To LAN Policy Configuration page is displayed by clicking **ACCESS POLICIES: TO LAN** in the menu list on the left side of the display window. To LAN Inbound policies apply to all data received by the NetVanta 2000 series that is to be transmitted out the Corporate Network Interface (LAN).

The To LAN Policy Configuration page displays a list of all current policies and provides an easy way to organize them using the **RULE ID** field.

Before creating a new To LAN inbound policy decide the appropriate priority for the policy. All policies are displayed in descending order according to priority. Using the **ADD** drop down menu containing **BEFORE**, **AFTER**, **BEGINNING**, and **END** options, configure the placement of the policy and click the **ADD** button. The Internet Access Policy Configuration page is displayed. A discussion of the fields found on the Internet Access Policy Configuration page follows.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > RULE ID

The **RULE ID** number is a system-wide unique policy ID generated by the NetVanta 2000 series when a new access policy is created.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > POLICY CLASS

The **POLICY CLASS** field is populated automatically by the NetVanta 2000 series using the current policy class (VPN, Corporate Inbound, Corporate Outbound).

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > SOURCE IP

The **SOURCE IP** displays the source addresses of incoming traffic used for the policy. All IP records previously defined in the IP table will appear in this drop down menu. Select the predefined IP record, or choose **OTHER** and define the source IP using the IP and Mask Bits text boxes below the drop down menu. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > DESTINATION IP

The **DESTINATION IP** displays the destination IP addresses of incoming traffic used for the policy. All IP records previously defined in the IP table will appear in this drop down menu. Select the predefined IP record, or choose **OTHER** and define the destination IP using the IP and Mask Bits text boxes below the drop down menu. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > DESTINATION PORT

The **DESTINATION PORT** drop down menu lists all definitions made in the services table. Choose one of the predefined destination port entries, or choose **OTHER** and define the destination port or port range using the text boxes below the drop down menu. To define a single port, enter the desired port value in the port range start text box and leave the port range text box empty. **ANY** option in this menu represents the complete port range from 1 to 65535.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > PROTOCOL TYPE

The **PROTOCOL TYPE** drop down menu selects the transport protocol for this access policy. If the desired transport protocol is not listed in the menu, choose **OTHER** and enter the desired IP based transport protocol number in the text box below the drop down menu.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > ACTION TYPE

The **ACTION TYPE** menu defines the policy as a Permit or Deny policy. Permit policies allow traffic matched by the policy selectors to pass through and Deny policies blocks that traffic.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > TIME SCHEDULE USED

The **TIME SCHEDULE USED** menu attaches a predefined time schedule to the Permit type access policy. This activates the policy only in the time windows defined in the selected time schedule.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > ENABLE LOG

The **ENABLE LOG** radio button selectively enables or disables event logging for the access policy.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > ENABLE NAT

The **ENABLE NAT** radio button provides control to enable or disable NAT for the policy.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > NAT NAME

The **NAT NAME** drop down menu lists all entries from the NAT table. To manually define the NAT out pool address here, select **OTHER** and enter the out pool IP address in the text boxes below the drop down menu. Enabling NAT on a To LAN inbound policy applies a Reverse NAT filtering scheme to incoming traffic received on this policy by the NetVanta 2000 series.

> POLICIES > ACCESS POLICIES: TO LAN > CONFIGURATION > SECURITY

Since access policy and VPN policy selectors are created separately and act independently, the **SECURITY** radio button configures the NetVanta 2000 series to check for the existence of a VPN policy for all the network traffic governed by this access policy. If any traffic that would pass this access policy would be sent in the clear, that is, not over an already defined VPN policy, an error will be generated to notify the user.



*Not selecting the **SECURITY** option may allow insecure data transmission through the NetVanta 2000 series.*



*If insecure data transmission is allowed because a VPN policy is removed after the **SECURITY** option has been performed on an access policy, no user notification will be given. To ensure data security, verify each access policy after VPN changes are made.*

Changing the Priority of a Policy

You can change the access policy priority by two ways: You can do simple priority corrections by using the up (-) and down (⏮) buttons, which are located at the end columns of each policy in the access policy table. Clicking the up or down button increases or decreases the priority of the access policy with respect to its neighboring policies.

Alternative way can be used for major priority corrections. Select the policy whose priority you want to change by entering its Rule ID in the text box located after **PLACE RULE** tab. This is located at the end of the policy table.

Then use the **BEFORE/AFTER** radio button in combination with Rule ID text box following this radio button to decide the new place in the table for this policy, and click the **INSERT** button.

The policy will be moved to the new place in the table.

Checking Policy Statistics

Select the policy whose statistics you want to check from the access policy table and click the **LOG** button. This will display the policy statistics page.

> POLICIES > ACCESS POLICIES: FROM LAN

The From LAN Policy Configuration page is displayed by clicking **ACCESS POLICIES: FROM LAN** in the menu list on the left side of the display window. From LAN outbound policies apply to all data received by the NetVanta 2000 series on the Corporate Network Interface (LAN).

The From LAN Policy Configuration page displays a list of all current policies and provides an easy way to organize them using the **RULE ID** field.

Before creating a new From LAN outbound policy decide the appropriate priority for the policy. All policies are displayed in descending order according to priority. Using the **ADD** drop down menu containing **BEFORE**, **AFTER**, **BEGINNING**, and **END** options, configure the placement of the policy and click the **ADD** button. The Internet Access Policy Configuration page is displayed. A discussion of the fields found on the Internet Access Policy Configuration page follows the figure.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > RULE ID

The **RULE ID** number is a system-wide unique policy ID generated by the NetVanta 2000 series when a new access policy is created.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > POLICY CLASS

The **POLICY CLASS** field is populated automatically by the NetVanta 2000 series using the current policy class (VPN, Corporate Inbound, Corporate Outbound).

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > SOURCE/DESTINATION

The **SOURCE IP/DESTINATION IP** displays the source and destination IP addresses used for the policy. All IP records previously defined in the IP table will appear in this drop down menu. Select the predefined IP record, or choose **OTHER** and define the source/destination IP using the IP and Mask Bits text boxes below the drop down menu. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > DESTINATION PORT

The **DESTINATION PORT** drop down menu lists all definitions made in the services table. Choose one of the predefined destination port entries, or choose **OTHER** and define the destination port or port range using the text boxes below the drop down menu. To define a single port, enter the desired port value in the port range start text box and leave the port range text box empty. **ANY** option in this menu represents the complete port range from 1 to 65535.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > PROTOCOL TYPE

The **PROTOCOL TYPE** drop down menu selects the transport protocol for this access policy. If the desired transport protocol is not listed in the menu, choose **OTHER** and enter the desired IP based transport protocol number in the text box below the drop down menu.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > ACTION TYPE

The **ACTION TYPE** menu defines the policy as a Permit or Deny policy. Permit policies allow traffic matched by the policy selectors to pass through and Deny policies blocks that traffic.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > TIME SCHEDULE USED

The **TIME SCHEDULE USED** menu attaches a predefined time schedule to the Permit type access policy. This activates the policy only in the time windows defined in the selected time schedule.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > ENABLE LOG

The **ENABLE LOG** radio button selectively enables or disables event logging for the access policy.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > ENABLE NAT

The **ENABLE NAT** radio button provides control to enable or disable NAT for the policy.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > NAT NAME

The **NAT NAME** drop down menu lists all entries from the NAT table. To manually define the NAT out pool address here, select **OTHER** and enter the out pool IP address in the text boxes below the drop down menu.

> POLICIES > ACCESS POLICIES: FROM LAN > CONFIGURATION > SECURITY

Since access policy and VPN policy selectors are created separately and act independently, the **SECURITY** radio button configures the NetVanta 2000 series to check for the existence of a VPN policy for all the network traffic governed by this access policy. If any traffic that would pass this access policy would be sent in the clear, that is, not over an already defined VPN policy, an error will be generated to notify the user.



*Not selecting the **SECURITY** option may allow insecure data transmission through the NetVanta 2000 series.*



*If insecure data transmission is allowed because a VPN policy is removed after the **SECURITY** option has been performed on an access policy, no user notification will be given. To ensure data security, verify each access policy after VPN changes are made.*

Changing the Priority of a Policy

You can change the access policy priority by two ways: You can do simple priority corrections by using the up (-) and down () buttons, which are located at the end columns of each policy in the access policy table. Clicking the up or down button increases or decreases the priority of the access policy with respect to its neighboring policies.

Alternative way can be used for major priority corrections. Select the policy whose priority you want to change by entering its Rule ID in the text box located after **PLACE RULE** tab. This is located at the end of the policy table.

Then use the **BEFORE/AFTER** radio button in combination with Rule ID text box following this radio button to decide the new place in the table for this policy, and click the **INSERT** button.

The policy will be moved to the new place in the table.

Default Access Policies

By default, the NetVanta 2000 series has eight corporate outbound policies configured for accessing popular Internet services from corporate network. With these default access policies any host in the corporate network can access the specified services on any host in the Internet. You can modify these policies to suite your network access policy.



Default access policies have NAT enabled.

> POLICIES > ACCESS POLICIES: TO DMZ

The To DMZ Policy Configuration page is displayed by clicking **ACCESS POLICIES: TO DMZ** in the menu list on the left side of the display window. To DMZ Inbound policies apply to all data received by the NetVanta 2000 series that is to be transmitted out the DMZ Interface.

The To DMZ Policy Configuration page displays a list of all current policies and provides an easy way to organize them using the **RULE ID** field.

Before creating a new To DMZ inbound policy decide the appropriate priority for the policy. All policies are displayed in descending order according to priority. Using the **ADD** drop down menu containing **BEFORE**, **AFTER**, **BEGINNING**, and **END** options, configure the placement of the policy and click the **ADD** button. The Internet Access Policy Configuration page is displayed. A discussion of the fields found on the Internet Access Policy Configuration page follows.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > RULE ID

The **RULE ID** number is a system-wide unique policy ID generated by the NetVanta 2000 series when a new access policy is created.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > POLICY CLASS

The **POLICY CLASS** field is populated automatically by the NetVanta 2000 series using the current policy class (VPN, Corporate Inbound, Corporate Outbound).

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > SOURCE IP

The **SOURCE IP** displays the source addresses of incoming traffic used for the policy. All IP records previously defined in the IP table will appear in this drop down menu. Select the predefined IP record, or choose **OTHER** and define the source IP using the IP and Mask Bits text boxes below the drop down menu. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > DESTINATION IP

The **DESTINATION IP** displays the destination IP addresses of incoming traffic used for the policy. All IP records previously defined in the IP table will appear in this drop down menu. Select the predefined IP record, or choose **OTHER** and define the destination IP using the IP and Mask Bits text boxes below the drop down menu. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > DESTINATION PORT

The **DESTINATION PORT** drop down menu lists all definitions made in the services table. Choose one of the predefined destination port entries, or choose **OTHER** and define the destination port or port range using the text boxes below the drop down menu. To define a single port, enter the desired port value in the port range start text box and leave the port range text box empty. **ANY** option in this menu represents the complete port range from 1 to 65535.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > PROTOCOL TYPE

The **PROTOCOL TYPE** drop down menu selects the transport protocol for this access policy. If the desired transport protocol is not listed in the menu, choose **OTHER** and enter the desired IP based transport protocol number in the text box below the drop down menu.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > ACTION TYPE

The **ACTION TYPE** menu defines the policy as a Permit or Deny policy. Permit policies allow traffic matched by the policy selectors to pass through and Deny policies blocks that traffic.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > TIME SCHEDULE USED

The **TIME SCHEDULE USED** menu attaches a predefined time schedule to the Permit type access policy. This activates the policy only in the time windows defined in the selected time schedule.

> POLICIES > ACCESS POLICIES: TO DMZN > CONFIGURATION > ENABLE LOG

The **ENABLE LOG** radio button selectively enables or disables event logging for the access policy.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > ENABLE NAT

The **ENABLE NAT** radio button provides control to enable or disable NAT for the policy.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > NAT NAME

The **NAT NAME** drop down menu lists all entries from the NAT table. To manually define the NAT out pool address here, select **OTHER** and enter the out pool IP address in the text boxes below the drop down menu. Enabling NAT on a To DMZ inbound policy applies a Reverse NAT filtering scheme to incoming traffic received on this policy by the NetVanta 2000 series.

> POLICIES > ACCESS POLICIES: TO DMZ > CONFIGURATION > SECURITY

Since access policy and VPN policy selectors are created separately and act independently, the **SECURITY** radio button configures the NetVanta 2000 series to check for the existence of a VPN policy for all the network traffic governed by this access policy. If any traffic that would pass this access policy would be sent in the clear, that is, not over an already defined VPN policy, an error will be generated to notify the user.



Not selecting the **SECURITY** option may allow insecure data transmission through the NetVanta 2000 series.



If insecure data transmission is allowed because a VPN policy is removed after the **SECURITY** option has been performed on an access policy, no user notification will be given. To ensure data security, verify each access policy after VPN changes are made.

Changing the Priority of a Policy

You can change the access policy priority by two ways: You can do simple priority corrections by using the up (-) and down () buttons, which are located at the end columns of each policy in the access policy table. Clicking the up or down button increases or decreases the priority of the access policy with respect to its neighboring policies.

Alternative way can be used for major priority corrections. Select the policy whose priority you want to change by entering its Rule ID in the text box located after **PLACE RULE** tab. This is located at the end of the policy table.

Then use the **BEFORE/AFTER** radio button in combination with Rule ID text box following this radio button to decide the new place in the table for this policy, and click the **INSERT** button.

The policy will be moved to the new place in the table.

Checking Policy Statistics

Select the policy whose statistics you want to check from the access policy table and click the **LOG** button. This will display the policy statistics page.

> POLICIES > ACCESS POLICIES: FROM DMZ

The From DMZ Policy Configuration page is displayed by clicking **ACCESS POLICIES: FROM DMZ** in the menu list on the left side of the display window. From DMZ outbound policies apply to all data received by the NetVanta 2000 series on the DMZ interface.

The From LAN Policy Configuration page displays a list of all current policies and provides an easy way to organize them using the **RULE ID** field.

Before creating a new From DMZ outbound policy decide the appropriate priority for the policy. All policies are displayed in descending order according to priority. Using the **ADD** drop down menu containing **BEFORE**, **AFTER**, **BEGINNING**, and **END** options, configure the placement of the policy and click the **ADD** button. The Internet Access Policy Configuration page is displayed. A discussion of the fields found on the Internet Access Policy Configuration page follows the figure.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > RULE ID

The **RULE ID** number is a system-wide unique policy ID generated by the NetVanta 2000 series when a new access policy is created.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > POLICY CLASS

The **POLICY CLASS** field is populated automatically by the NetVanta 2000 series using the current policy class (VPN, To/From LAN, To/From DMZ).

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > SOURCE/DESTINATION

The **SOURCE IP/DESTINATION IP** displays the source and destination IP addresses used for the policy. All IP records previously defined in the IP table will appear in this drop down menu. Select the predefined IP record, or choose **OTHER** and define the source/destination IP using the IP and Mask Bits text boxes below the drop down menu. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > DESTINATION PORT

The **DESTINATION PORT** drop down menu lists all definitions made in the services table. Choose one of the predefined destination port entries, or choose **OTHER** and define the destination port or port range using the text boxes below the drop down menu. To define a single port, enter the desired port value in the port range start text box and leave the port range text box empty. **ANY** option in this menu represents the complete port range from 1 to 65535.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > PROTOCOL TYPE

The **PROTOCOL TYPE** drop down menu selects the transport protocol for this access policy. If the desired transport protocol is not listed in the menu, choose **OTHER** and enter the desired IP based transport protocol number in the text box below the drop down menu.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > ACTION TYPE

The **ACTION TYPE** menu defines the policy as a Permit or Deny policy. Permit policies allow traffic matched by the policy selectors to pass through and Deny policies blocks that traffic.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > TIME SCHEDULE USED

The **TIME SCHEDULE USED** menu attaches a predefined time schedule to the Permit type access policy. This activates the policy only in the time windows defined in the selected time schedule.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > ENABLE LOG

The **ENABLE LOG** radio button selectively enables or disables event logging for the access policy.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > ENABLE NAT

The **ENABLE NAT** radio button provides control to enable or disable NAT for the policy.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > NAT NAME

The **NAT NAME** drop down menu lists all entries from the NAT table. To manually define the NAT out pool address here, select **OTHER** and enter the out pool IP address in the text boxes below the drop down menu.

> POLICIES > ACCESS POLICIES: FROM DMZ > CONFIGURATION > SECURITY

Since access policy and VPN policy selectors are created separately and act independently, the **SECURITY** radio button configures the NetVanta 2000 series to check for the existence of a VPN policy for all the network traffic governed by this access policy. If any traffic that would pass this access policy would be sent in the clear, that is, not over an already defined VPN policy, an error will be generated to notify the user.



*Not selecting the **SECURITY** option may allow insecure data transmission through the NetVanta 2000 series.*



*If insecure data transmission is allowed because a VPN policy is removed after the **SECURITY** option has been performed on an access policy, no user notification will be given. To ensure data security, verify each access policy after VPN changes are made.*

Changing the Priority of a Policy

You can change the access policy priority by two ways: You can do simple priority corrections by using the up (-) and down (⏮) buttons, which are located at the end columns of each policy in the access policy table. Clicking the up or down button increases or decreases the priority of the access policy with respect to its neighboring policies.

Alternative way can be used for major priority corrections. Select the policy whose priority you want to change by entering its Rule ID in the text box located after **PLACE RULE** tab. This is located at the end of the policy table.

Then use the **BEFORE/AFTER** radio button in combination with Rule ID text box following this radio button to decide the new place in the table for this policy, and click the **INSERT** button.

The policy will be moved to the new place in the table.

Default Access Policies

By default, the NetVanta 2000 series has eight corporate outbound policies configured for accessing popular Internet services from corporate network. With these default access policies any host in the corporate network can access the specified services on any host in the Internet. You can modify these policies to suite your network access policy.



Default access policies have NAT enabled.

> POLICIES > VPN

When adding a VPN policy, decide its priority. By default, new VPN policies will be added with the least priority (i.e., at the end of the VPN policy table).

For setting the priority of a new VPN policy, select the **AFTER** or **BEFORE** option from the drop down **ADD** menu. Enter the existing VPN policy name to use as the placing guide for the newly added VPN policy.

VPN policies may be added using either manual or automatic key management.

Deleting A VPN Policy

Select the VPN policy you want to delete from the VPN policy table and click the **DELETE** button. This will bring up the VPN policy delete confirmation dialog.

If you answer affirmative to this dialog by clicking **YES**, the VPN policy will be removed.



If there are secure communications active using this VPN policy, they may get disrupted.

Editing A VPN Policy

Select the VPN policy you want to edit from the VPN policy table and click **MODIFY** button. This brings the selected VPN policy in the edit mode.

Here you can make the desired changes to the VPN policy.



If there are secure communications active using this VPN policy, they may get disrupted due to the changes in the VPN policy parameters.

Viewing A VPN Policy

Select the VPN policy you want to view from the VPN policy table. Click on the **SHOW** button. This shows the selected VPN policy in non-editable form.

This VPN policy view does not show any keying information.

Changing Priority of A VPN Policy

Similar to access policies you can change the priority of VPN policy by two ways: You can do simply priority corrections by using the up (-) and down (⏮) buttons, which are located at the end columns of each policy in the VPN policy table. Clicking the up or down button increases or decreases the priority of the access policy with respect to its neighboring policies.

Alternative way can be used for major priority corrections. Select the policy whose priority you want to change by entering its policy name in the text box located after **PLACE** tab. This is located at the end of the policy table.

Then use the drop down menu with **BEFORE/AFTER** options and the next VPN policy-name text box to define the new place for this VPN policy in the table. Click the **OK** button.

The VPN policy will be moved to the new place in the table.



If the access policies are wider than IPsec policies the traffic which doesn't falls in the range will be passed through as plain packets.

To configure security policy you have to select the choice **YES** in the **ACCESS POLICIES**.

> POLICIES > VPN > TUNNELS (IPSEC TUNNELS) > MANUAL KEY MANAGEMENT

To use manual key management click **MANUAL** button. This will bring up the VPN policy configuration screen.

POLICY NAME - is a symbolic name of the VPN policy. Each policy should have a unique policy name.

SOURCE ADDRESS - Drop down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Mostly, this address will be from your corporate network address space. All entries in the IP Address Table appear in this drop down menu. You can choose one of these, or select **OTHER** option from this menu and define the source IP address/subnet in the immediately following text boxes. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

DESTINATION ADDRESS - Drop down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Mostly, this address will be from remote site's corporate network address space. All entries in the IP Address Table appear in this drop down menu. You can choose one of these, or select **OTHER** option from this menu and define the destination IP address/subnet in the immediately following text boxes. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

SOURCE PORT - Drop down menu allows you select the source port value for this VPN policy selector. All entries in the Services table appear in this menu. You can choose one from these, or select **OTHER** option and define the Source Port in the immediately following text box. **ANY** option in this menu indicates the complete port range i.e. 1 to 65535.

DESTINATION PORT - Drop down menu allows you select the destination port value for this VPN policy selector. All entries in the Services table appear in this menu. You can choose one from these, or select **OTHER** option and define the Destination Port in the immediately following text box. **ANY** option in this menu indicates the complete port range i.e. 1 to 65535.

PROTOCOL - Drop down menu allows you to choose the transport protocol for this VPN policy selector. **ALL** option in this menu represents all transport protocols riding on IP.

PEER SECURITY GATEWAY - is the IP address of the remote end of the VPN tunnel, i.e. WAN IP address of the remote Security Gateway.

LOCAL SECURITY GATEWAY - is the IP address of the local end of the VPN tunnel, i.e. WAN interface IP address of your ADVANTA 2100.

AH Configuration

AUTHENTICATION - this menu allows you to enable or disable AH transform for this VPN policy.

AUTH ALGORITHM - If you choose to enable AH, then this menu allows you to select authentication algorithm. You can choose **MD5** or **SHA1**; default is **MD5**.

IN KEY - is HMAC key used for computing ICV (Integrity Check Value) on the inbound traffic with the selected authentication algorithm. Length of this key for MD5 must be 16 bytes, and for SHA1 it must be

20 bytes. Enter 16 or 20 characters (depending on authentication algorithm) and the NetVanta 2000 series will use the ASCII of each character to create the hex bytes needed for the algorithm. This key value should match to the corresponding outbound key value on the remote end SG.

IN SPI - is SPI value for identifying the inbound SA created by this AH transform. This should match with the corresponding outbound SPI value configured on the remote end SG. For AH, values entered for the SPI are interpreted and used as hex by the NetVanta 2000 series.

OUT KEY - is HMAC key used for computing ICV on the outbound traffic with the selected authentication algorithm. Length of this key for MD5 must be 16 bytes, and for SHA1 it must be 20 bytes. Enter 16 or 20 characters (depending on authentication algorithm) and the NetVanta 2000 series will use the ASCII of each character to create the hex bytes needed for the algorithm. This key value should match to the corresponding inbound key value on the remote end SG.

OUT SPI - is SPI value for identifying the outbound SA created by this AH transform. This should match with the corresponding inbound SPI value configured on the remote end SG. For AH, values entered for the SPI are interpreted and used as hex by the NetVanta 2000 series.

ESP Configuration

ENCRYPTION - drop down menu allows you to enable or disable ESP transform for this VPN policy. You can select the ESP mode also with this menu. The NetVanta 2000 series supports plain ESP and ESP with Authentication.

ESP ALGORITHM - allows you to choose the encryption algorithm for this VPN policy. Two options are available - one is DES other is 3DES; DES is the default value.

AUTH ALGORITHM - allows you to configure authentication algorithm if you enable ESP with Authentication mode. You can choose one from MD5 or SHA1. MD5 is the default value.

IN SPI - is SPI value for identifying the inbound SA created by this ESP transform. For ESP, values entered for the SPI are interpreted and used as decimal data. This should match with the corresponding outbound SPI value configured on the remote end SG.

IN AUTH KEY - is HMAC key used for computing ICV on the inbound traffic with the selected authentication algorithm if ESP with Authentication mode is configured. Length of this key for MD5 must be 16 bytes, and for SHA1 it must be 20 bytes. Enter 16 or 20 characters (depending on authentication algorithm) and the NetVanta 2000 series will use the ASCII of each character to create the hex bytes needed for the algorithm. This key value should match to the corresponding outbound key value on the remote end SG.

OUT SPI - is SPI value for identifying the outbound SA created by this ESP transform. For ESP, values entered for the SPI are interpreted and used as decimal data. This should match with the corresponding inbound SPI value configured on the remote end SG.

OUT AUTH KEY - is HMAC key used for computing ICV on the outbound traffic with the selected authentication algorithm if ESP with Authentication mode is configured. Length of this key for MD5 must be 16 bytes, and for SHA1 it must be 20 bytes. Enter 16 or 20 characters (depending on authentication

algorithm) and the NetVanta 2000 series will use the ASCII of each character to create the hex bytes needed for the algorithm. This key value should match to the corresponding inbound key value on the remote end SG.

IN ESP KEY - is encryption key used for deciphering the datagrams coming in from the remote end SG. Length of this key for DES must be 8 bytes, and for 3DES must be 24 bytes. For utilizing the 3DES advantage, each 8-byte set in this keying material should be different. This key value should match to the outbound ciphering key on the remote end SG.

OUT ESP KEY - is encryption key used for ciphering the datagrams going out to the remote end SG through the Internet. Length of this key for DES must be 8 bytes, and for 3DES must be 24 bytes. For utilizing the 3DES advantage, each 8-byte set in this keying material should be different. This key value should match to the inbound deciphering key on the remote end SG.



If the access policies are wider than the IPSec policies, the traffic which doesn't fall in the range of the IPSec policy will be passed through as plain packets.

> POLICIES > VPN > TUNNELS (IPSEC TUNNELS) > AUTOMATIC KEY MANAGEMENT

To use the automatic key management click **AUTO** button. This will bring up the **AUTO VPN POLICY CONFIGURATION** screen.

POLICY NAME - is a symbolic name of the VPN policy. Each policy should have an unique policy name.

SOURCE ADDRESS - Drop down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Mostly, this address will be from your corporate network address space. All entries in the IP Address Table appear in this drop down menu. You can choose one of these, or select OTHER option from this menu and define the source IP address/subnet in the immediately following text boxes. ANY option in this menu represents all valid IP addresses in the Internet address space.

DESTINATION ADDRESS - Drop down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Mostly, this address will be from remote site's corporate network address space. All entries in the IP Address Table appear in this drop down menu. You can choose one of these, or select OTHER option from this menu and define the destination IP address/subnet in the immediately following text boxes. ANY option in this menu represents all valid IP addresses in the Internet address space.

SOURCE PORT - Drop down menu allows you select the source port value for this VPN policy selector. All entries in the Services table appear in this menu. You can choose one from these, or select OTHER option and define the Source Port in the immediately following text box. ANY option in this menu indicates the complete port range i.e. 1 to 65535.

DESTINATION PORT - Drop down menu allows you select the destination port value for this VPN policy selector. All entries in the Services table appear in this menu. You can choose one from these, or select OTHER option and define the Destination Port in the immediately following text box. ANY option in this

menu indicates the complete port range i.e. 1 to 65535.

PROTOCOL - Drop down menu allows you to choose the transport protocol for this VPN policy selector. ALL option in this menu represents all transport protocols riding on IP.

PEER SECURITY GATEWAY - is the IP address of the remote end of the VPN tunnel, i.e. WAN IP address of the remote Security Gateway.

LOCAL SECURITY GATEWAY - is the IP address of the local end of the VPN tunnel, i.e. WAN interface IP address of your ADVANTA 2100.

AH Configuration

AUTHENTICATION - this menu allows you to enable or disable AH transform for this VPN policy.

AUTH ALGORITHM - If you choose to enable AH, then this menu allows you to select authentication algorithm. You can choose MD5 or SHA1; default is MD5.

ESP Configuration

ENCRYPTION - drop down menu allows you to enable or disable ESP transform for this VPN policy. You can select the ESP mode also with this menu. Two ESP modes are available, one is plain ESP and other is ESP with Authentication.

ESP ALGORITHM - allows you to choose the encryption algorithm for this VPN policy. Two options are available - one is DES other is 3DES; DES is the default value.

AUTH ALGORITHM - allows you to configure authentication algorithm if you enable ESP with Authentication mode. You can choose one from MD5 or SHA1. MD5 is the default value.

> POLICIES > VPN > IKE POLICIES

To add an IKE policy, click the **ADD** button to display the IKE Policy Configuration page. A description of the IKE configuration parameters follows.

POLICY NAME - is a symbolic name of the VPN policy. Each policy should have an unique policy name.

DIRECTION -- You may specify any of the available options in the drop down menu. It includes Both directions, Initiator only, Responder only. Choosing Both directions will allow the box to act both as initiator and responder.



*Currently only **BOTH DIRECTIONS** is supported*

EXCHANGE TYPE - You may select any one of the options available in the drop down menu. It includes Main Mode and Aggressive Mode.

LOCAL ID TYPE -- Select any one of the options available in the drop down menu. It includes **IP ADDRESS** (IP v.4 address), **FQDN** (fully qualified domain name), **USER FQDN** (fully qualified username string) and **DER ANS1 DN** (X.500 distinguished name).

LOCAL ID DATA -- Based on the **LOCAL ID TYPE** selected, enter the appropriate Local ID data. If **IP ADDRESS** is selected, enter an IP v.4 address in the **LOCAL ID DATA** field. If **FQDN** is selected, enter a fully qualified domain name (i.e. netvanta1.adtran.com) in the **LOCAL ID DATA** field. If **USER FQDN** is selected, enter a fully qualified username string (i.e. networkmaster@adtran.com) in the **LOCAL ID DATA** field. If **DER ANS1 DN** is selected, enter the X.500 Distinguished name (X.501) of the principal whose certificates are being exchanged to establish the SA in the **LOCAL ID DATA** field.

Remote ID Type -- Select any one of the options available in the drop down menu. It includes IP Address (IP v.4 address), FQDN (fully qualified domain name), User FQDN (fully qualified username string) and DER ANS1 DN (X.500 distinguished name).

REMOTE ID DATA - Based on the **REMOTE ID TYPE** selected, enter the appropriate Local ID data. If **IP ADDRESS** is selected, enter an IP v.4 address in the **REMOTE ID DATA** field. If **FQDN** is selected, enter a fully qualified domain name (i.e. advanta.adtran.com) in the **REMOTE ID DATA** field. If **USER FQDN** is selected, enter a fully qualified username string (i.e. networkmaster@adtran.com) in the **REMOTE ID DATA** field. If **DER ANS1 DN** is selected, enter the X.500 Distinguished name (X.501) of the principal whose certificates are being exchanged to establish the SA in the **REMOTE ID DATA** field. You can specify up to 10 **REMOTE ID TYPES** and **REMOTE ID DATA**.

LOCAL IP ADDRESS - You **MUST** specify the Local IP address of the system.

REMOTE IP ADDRESS - You must specify the Remote IP address.

ENCRYPTION ALGORITHM - You may select one of the algorithms specified in the drop down menu. It includes DES and 3DES.

AUTHENTICATION ALGORITHM - You may select one of the algorithms specified in the drop down menu. It includes MD5 and SHA1.

AUTHENTICATION MODE - You may select any one of the authentication modes specified in the drop down menu. This includes Pre-Shared Key, DSS_SIGN, RSA_SIGN, RSA_ENC, RSA_REV_ENC.

KEY- If you select Pre-Shared key as your authentication mechanism, you must specify the key. This depends on the Authentication algorithm which you have selected. If you have selected the MD5 algorithm then the key length should be 16 bytes. If it is SHA1, the key length should be 20 bytes.

LIFE TIME -Lifetime in seconds of the IKE SA.

DH GROUP - There are two groups to choose from in the drop down menu. You may have to choose one of them.

Submit with these changes and this will be stored in the memory.

SOURCE ADDRESS - Drop down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Mostly, this address will be from your corporate network address space. All entries in the IP Address Table appear in this drop down menu. You can choose one of these, or select **OTHER** option from this menu and define the source IP address/subnet in the immediately following text boxes. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

DESTINATION ADDRESS - Drop down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Mostly, this address will be from remote site's corporate network address space. All entries in the IP Address Table appear in this drop down menu. You can choose one of these, or select **OTHER** option from this menu and define the destination IP address/subnet in the immediately following text boxes. **ANY** option in this menu represents all valid IP addresses in the Internet address space.

SOURCE PORT - Drop down menu allows you select the source port value for this VPN policy selector. All entries in the Services table appear in this menu. You can choose one from these, or select **OTHER** option and define the Source Port in the immediately following text box. **ANY** option in this menu indicates the complete port range i.e. 1 to 65535.

DESTINATION PORT - Drop down menu allows you select the destination port value for this VPN policy selector. All entries in the Services table appear in this menu. You can choose one from these, or select **OTHER** option and define the Destination Port in the immediately following text box. **ANY** option in this menu indicates the complete port range (i.e., 1 to 65535).

> POLICIES > VPN > CERTIFICATES

The NetVanta 2000 series supports the use of both RSA and DSS Signature Algorithm Certificates. The NetVanta 2000 series provides the capability to generate self-certificate requests, and maintains a listing of private keys (certificate requests) that currently have no public key (self-certificate assigned by the Certificate Authority).

Always contact your Certificate Authority (VeriSign, Entrust, etc.) before generating your self-certificate request. The parameters configured in your request must match what the Certificate Authority requires for you to receive your self-certificate. Once the request is generated, follow your Certificate Authority's guidelines for supplying them with your request. Many Certificate Authorities allow e-mail requests, but some do not.

> POLICIES > VPN > CERTIFICATES > SELF CERTIFICATE

The NetVanta 2000 series provides the capability to generate self certificate requests in PEM (Privacy Enhanced Mail) format for either RSA or DSS signature algorithms. Refer to DLP-017, *Generating a Self-Certificate Request* for more details.

> POLICIES > VPN > CERTIFICATES > CA CERTIFICATE

The NetVanta 2000 series supports loading Certificate Authority certificates in PEM (Privacy Enhanced Mail) format for either RSA or DSS signature algorithms. Refer to DLP-018, *Uploading a CA Certificate to the NetVanta* for more details.

> **POLICIES > VPN > CERTIFICATES > PRIVATE KEY WITHOUT PUBLIC KEY**

The NetVanta 2000 series provides the capability to generate self certificate requests in PEM (Privacy Enhanced Mail) format for either RSA or DSS signature algorithms. Refer to DLP-017, *Generating a Self-Certificate Request* for more details. The NetVanta 2000 series tracks all self certificate generated requests and maintains them in the Private Key Without Public Key until the corresponding self certificate is loaded into the unit.

> **POLICIES > VPN > CERTIFICATES > CRL**

The NetVanta 2000 series supports loading Certificate Revocation Lists obtained from Certificate Authorities. Upload the CRL by clicking the **BROWSE** button to find the Certificate Authority's CRL file, then click the **UPLOAD** button to make it active in the NetVanta 2000 series system.

> **MONITOR**

This section discusses the monitoring capabilities of NetVanta 2000 series including access policy and association database statistics, user session information, and NetVanta 2000 series access records. The NetVanta 2000 series monitor configuration parameters are displayed by clicking on the **MONITOR** menu on the Administration Console.

> **MONITOR > POLICY STATISTICS**

The Policy Statistics page is displayed by clicking on **POLICY STATISTICS** found in the menu list.

> **MONITOR > POLICY STATISTICS > ACCESS POLICY STATISTICS**

The Access Policy Statistics page displays static and dynamic policy allocation attempts, policy allocation failures, and policy request successes and failures. This table shows the policy statistics for the current hour, previous hour, and a daily total.

> **MONITOR > POLICY STATISTICS > ASSOCIATION DATABASE STATISTICS**

The Association Database Statistics page displays association memory statistics as well as broadcast, connection, security association (SA), and other security and traffic-related statistics. Using the same format as the Access Policy Statistics display, it shows the association database statistics for current hour, previous hour, and a daily total.

> **MONITOR > USER ACCOUNTING**

The User Accounting page provides remote user session statistics. This includes **USER NAME**, **LOGIN TIME**, **LOGOUT TIME**, **BYTES** transferred **IN** and **OUT**, and the user's **SOURCE IP** address. These fields summarize a remote user's session. Effective network administrators will have a sense of normal activity on the network making it easier to spot abnormal activity or behavior. The User Accounting page is displayed by clicking on User Accounting found in the menu list.

> **MONITOR > ACCESS LOG**

The Access Log page is displayed by clicking on **ACCESS LOG** found in the menu list. The Log Window shows all event log messages that have not been exported by NetVanta 2000 series.

The NetVanta 2000 series log queue can be cleared by clicking on the **CLEAR LOG** button found in the Log Window dialog box.



Messages in the log queue when it is cleared are permanently lost.

DETAIL LEVEL PROCEDURES

Connecting to the Netvanta 2000 Series	DLP-001
Changing the Admin Password in the NetVanta	DLP-002
Saving the Current Settings of the NetVanta	DLP-003
Setting the Time and Date in the NetVANTA	DLP-004
Configuring the LAN Interface IP Address	DLP-005
Configuring the WAN Interface Using Dynamic or Static IP Addressing	DLP-006
Configuring the WAN Interface For PPPoE Addressing	DLP-007
Upgrading the Firmware of the NetVanta 2000 series	DLP-008
Saving the Current Configuration of the NetVanta	DLP-009
Loading a Saved Configuration into the NetVanta	DLP-010
Adding a Default Route to the NetVanta Route Table	DLP-011
Configuring the LAN Interface DHCP Server	DLP-012
Defining a User Group in the NetVanta	DLP-013
Adding a User to the Users Component Table	DLP-014
Using the IP Address Component Table	DLP-015
Adding a Service to the Services Component Table	DLP-016
Generating a Self-Certificate Request	DLP-017
Uploading a CA Certificate to the NetVanta	DLP-018
Uploading a Self-Certificate to the NetVanta	DLP-019
Reviewing the Various Keys of the NetVanta	DLP-020
Restoring the NetVanta to Factory Defaults	DLP-021
Viewing the DHCP Info Table	DLP-022

CONNECTING TO THE NETVANTA 2000 SERIES

Introduction

The NetVanta 2000 series can be accessed and managed via the LAN interface using an ethernet crossover cable (provided). Alternately, the NetVanta 2000 series may be accessed using a hub and two ethernet cables (one for the PC and one for the NetVanta 2000 series). Using a PC with an installed browser (Internet Explorer 5.5 for optimal viewing), the NetVanta 2000 series can be configured using an easy GUI.

Prerequisite Procedures

The NetVanta 2000 series should be accessible to connect to a PC with an installed browser.

Tools and Materials Required

- Ethernet crossover cable (provided)
- DHCP-enabled PC with installed browser



This DLP assumes that a PC with DHCP-client software enabled will be used when initially connecting to the NetVanta 2000 series.

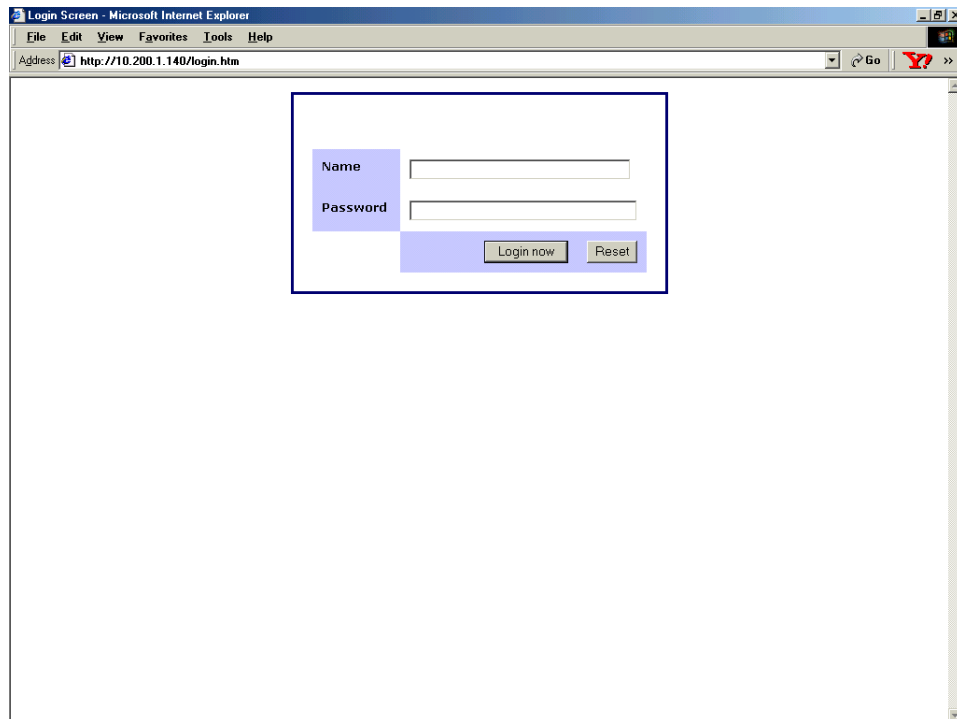


To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

DLP-001

Perform Steps Below in the Order Listed

1. Connect power to the NetVanta 2000 series using the provided wallmount power supply.
2. Connect the NetVanta 2000 series LAN interface to the PC using the provided ethernet crossover cable.
3. Supply power to the PC and begin the operating system bootup process. During the bootup process, the PC will obtain an IP address from the NetVanta 2000 series DHCP server. Alternately, complete the process for releasing and renewing captured IP addresses to obtain a new IP address from the NetVanta 2000 series DHCP server. Please refer to your specific operating system documentation for your PC details on that process.
4. Open your installed browser and in the URL field enter 10.10.10.1. The NetVanta 2000 series login screen will appear.

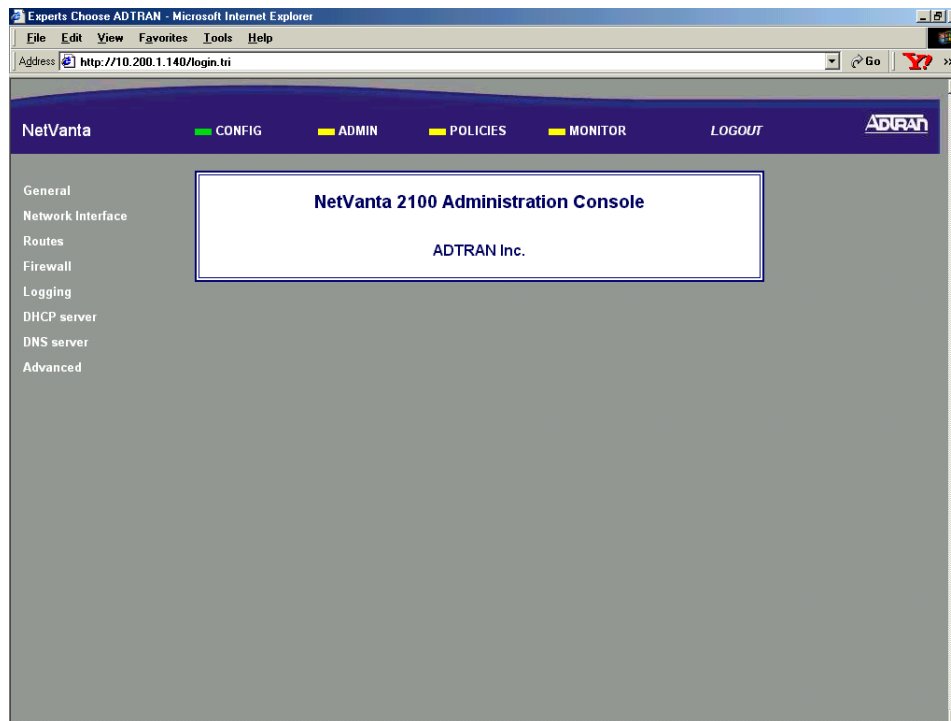


5. Enter your username and password and click the login button. When connecting to the NetVanta 2000 series for the first time, the username is **admin** and there is no set password.



*ADTRAN strongly recommends immediately changing the **admin** password for security purposes. Refer to DLP-002 for details.*

6. After logging in to the NetVanta 2000 series, the welcome screen will appear.



Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

CHANGING THE ADMIN PASSWORD IN THE NETVANTA

Introduction

This DLP explains how to change the existing admin password in the NetVanta 2000 series access list.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials are required.

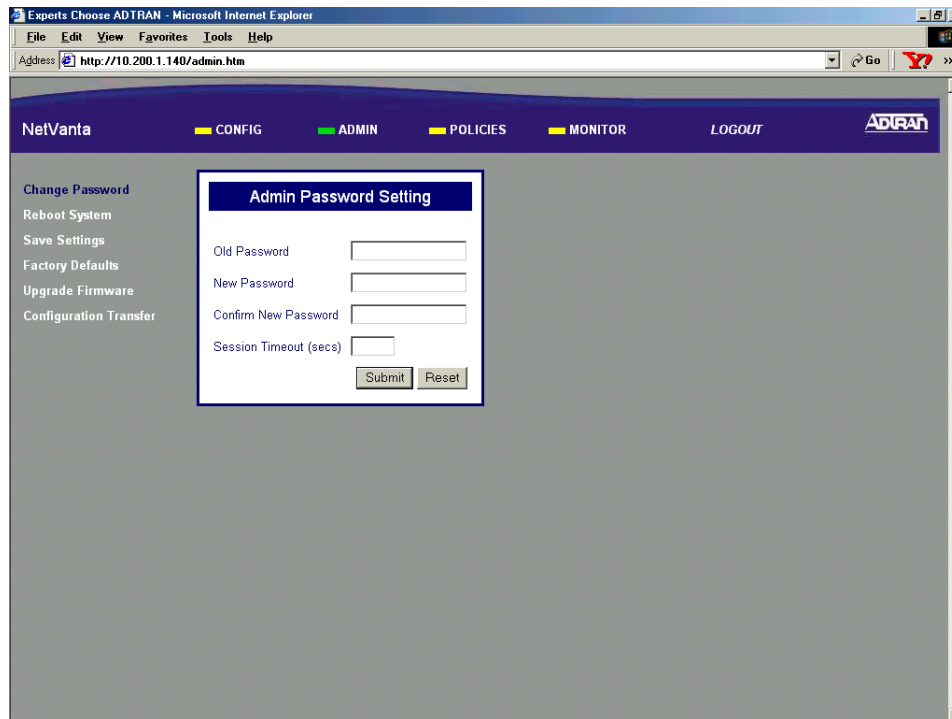
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

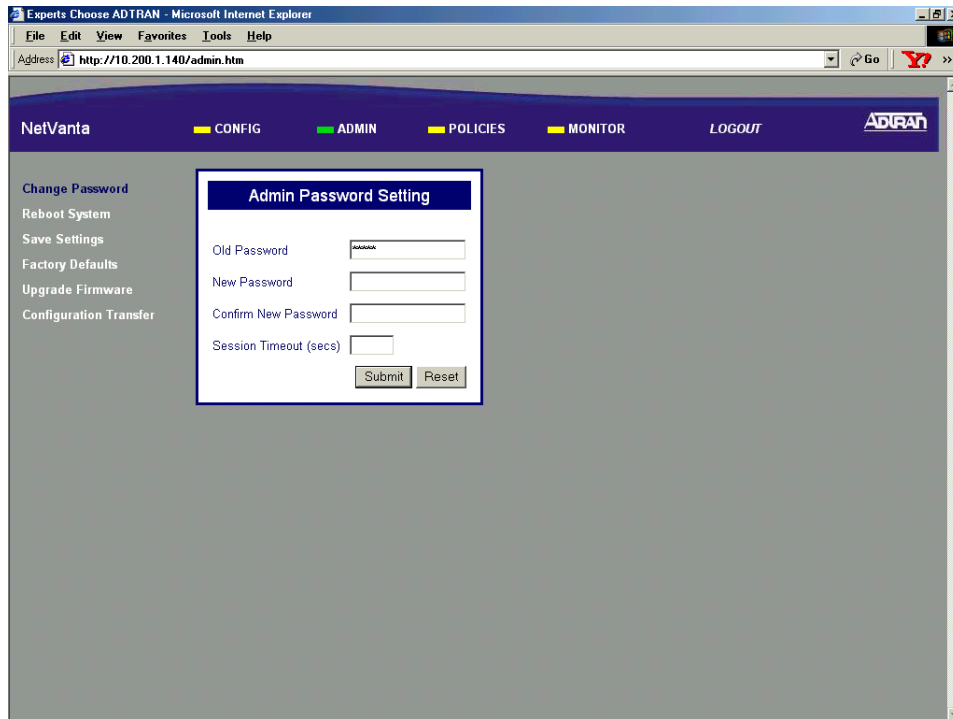
DLP-002

Perform Steps Below in the Order Listed

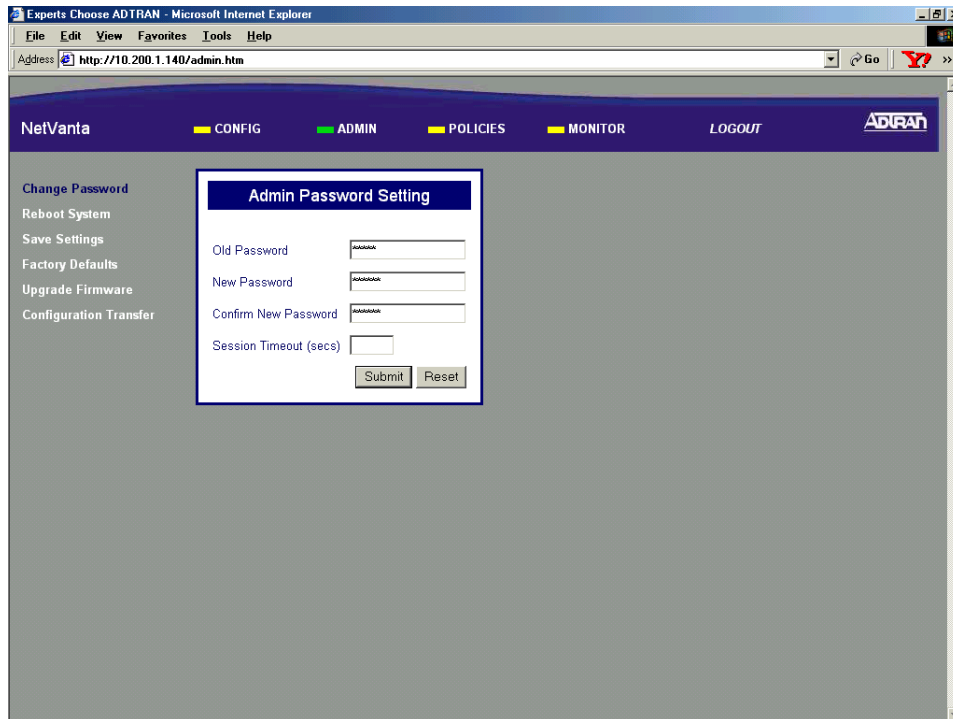
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **ADMIN**. This displays the **CHANGE PASSWORD** dialog box.



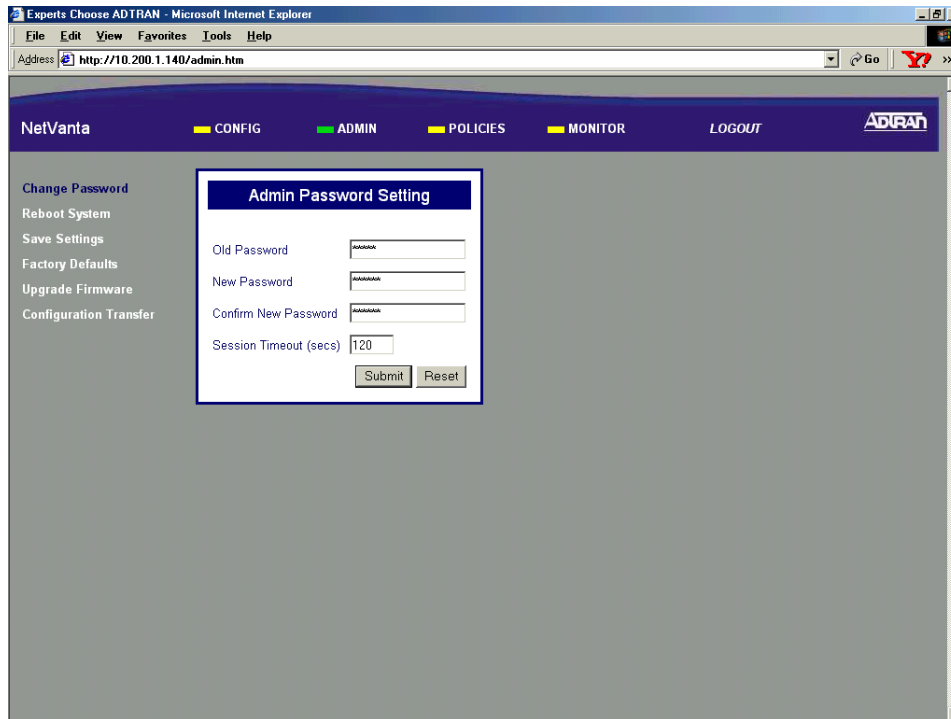
3. Enter the existing password in the **OLD PASSWORD** data field. If this is the first time changing the password in the NetVanta 2000 series, this field will be blank.



4. Enter the new password in both the **NEW PASSWORD** data field and **CONFIRM NEW PASSWORD** data fields.

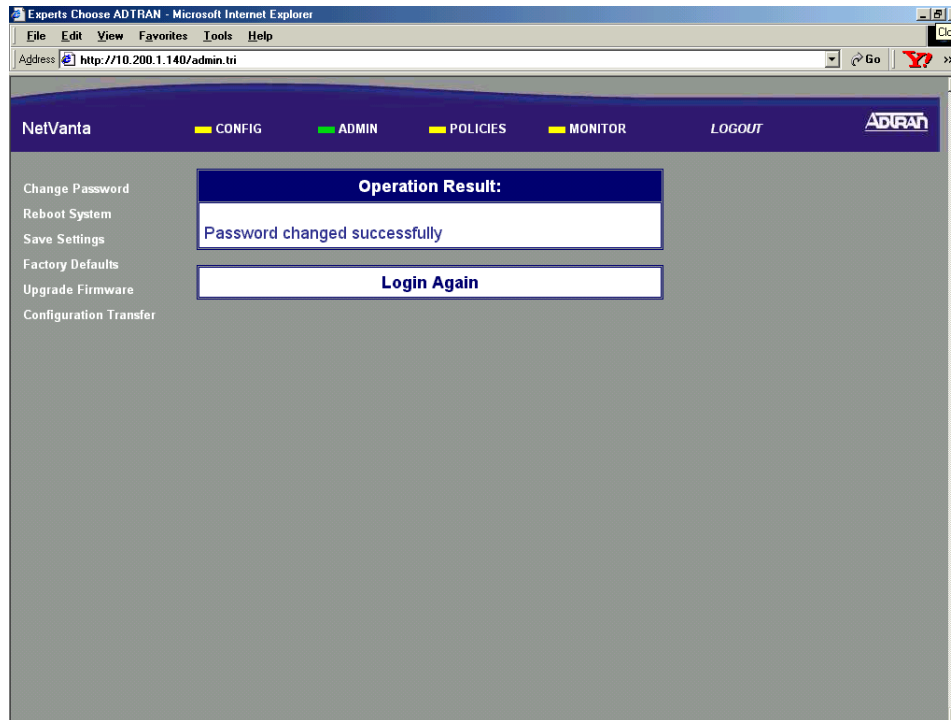


5. You may enter a **SESSION TIMEOUT** (in seconds). Leaving this field blank results in a infinite **SESSION TIMEOUT**.

**WARNING**

A Session Timeout less than 120 sec is not recommended. Having a short session timeout will make it difficult to configure the NetVanta 2000 series before timing out.

- Once all fields are completed, click the **SUBMIT** button to register the password change. Once the **SUBMIT** button has been clicked, the **OPERATION RESULT** screen will appear.



- Click the **LOGIN AGAIN** hyperlink and enter **admin** as the username and the new password in the **PASSWORD** field.
- Follow the procedures outlined in DLP-003 to save the settings to nonvolatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

SAVING THE CURRENT SETTINGS OF THE NETVANTA

Introduction

After making a configuration change in the NetVanta 2000 series, it is necessary to save the new settings to non-volatile memory. If the changes are not saved, a power loss to the NetVanta 2000 series will result in a configuration loss. This DLP details the process for saving settings to NetVanta 2000 series non-volatile memory.

Prerequisite Procedures

This procedure assumes that the NetVanta 2000 series unit is connected to a PC with an internet browser and is powered up. Refer to DLP-001 for instructions on connecting the PC to the NetVanta 2000 series LAN port and logging in to the NetVanta 2000 series system.

Tools and Materials Required

- No special tools or materials are required.

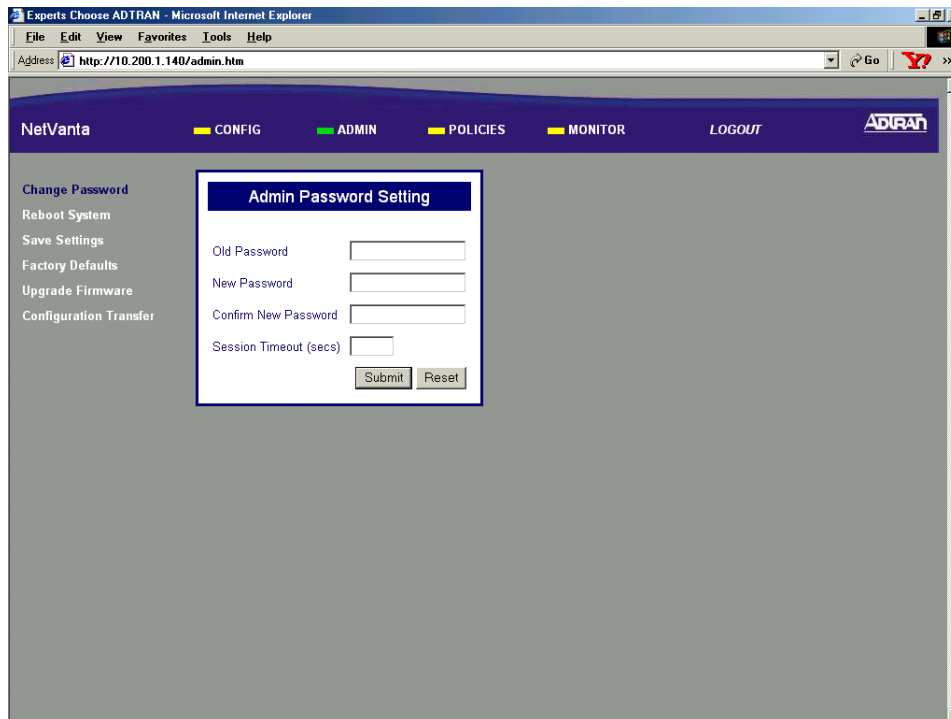
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

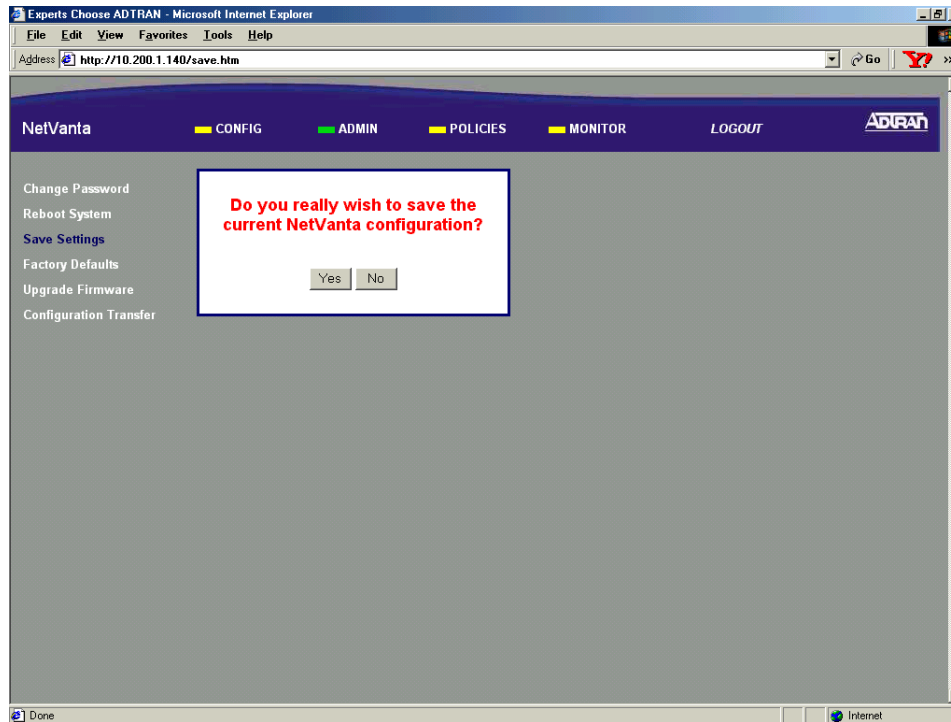
DLP-003

Perform Steps Below in the Order Listed

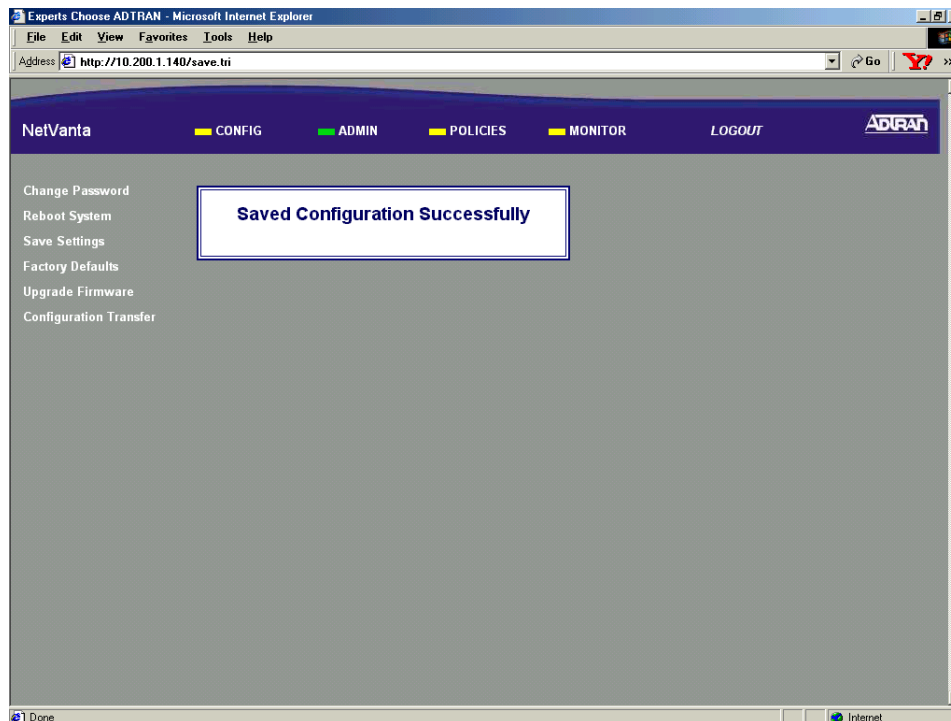
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **ADMIN**.



- From the menu list (located on the left side of the screen), select **SAVE SETTINGS**. The save settings confirmation page will display.



- Select Yes to save the current NetVanta 2000 series settings to non-volatile memory. A status page will display when the settings have been successfully saved.



Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

SETTING THE TIME AND DATE IN THE NETVANTA

Introduction

Many security operations are time and date critical. This DLP provides the procedures for setting the NetVanta 2000 series system time and date to ensure proper operation.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials are required.

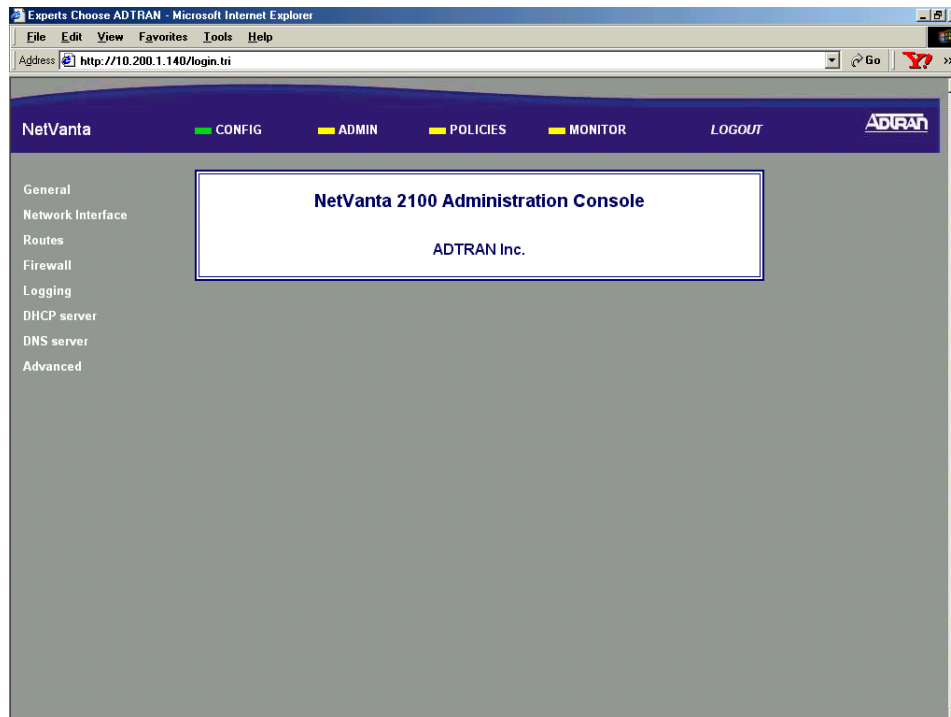
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

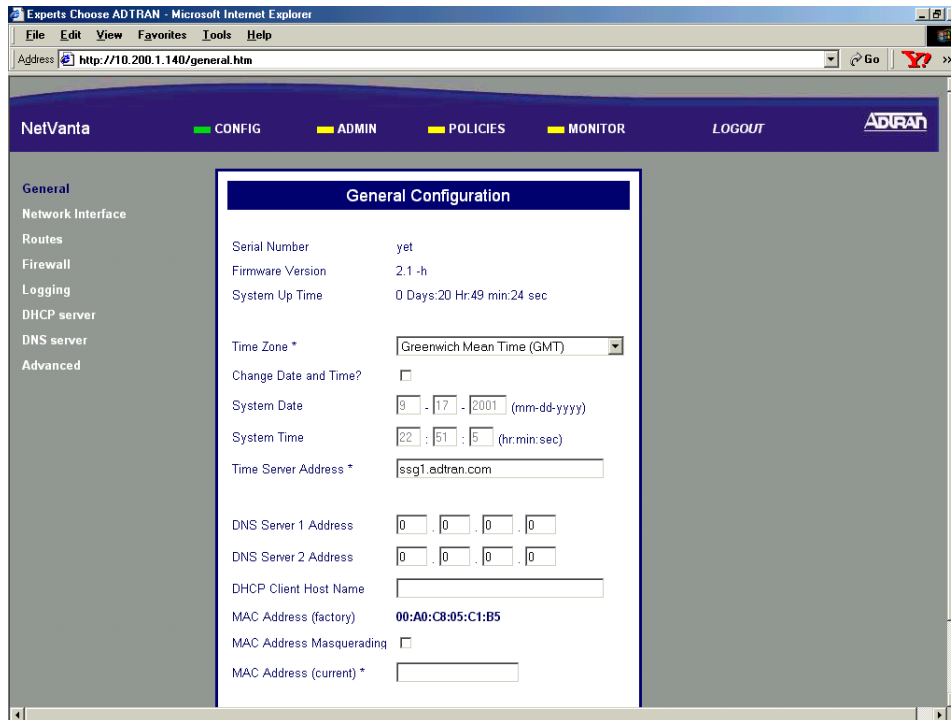
DLP-004

Perform Steps Below in the Order Listed

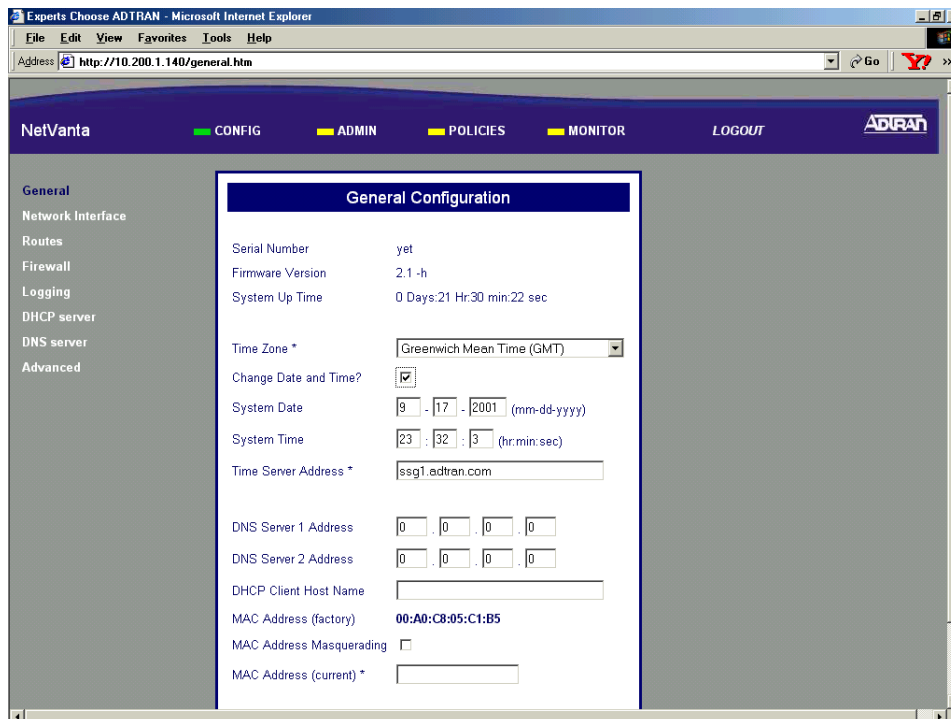
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **CONFIG**.



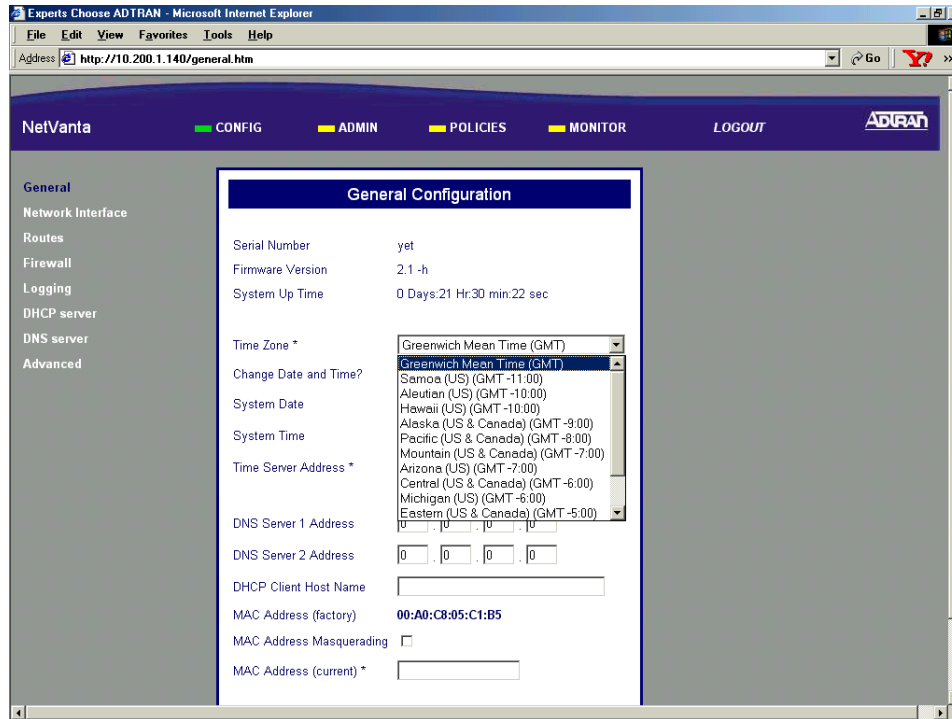
- From the menu list (located on the left side of the screen), select **GENERAL**. The **GENERAL CONFIGURATION** page will appear.



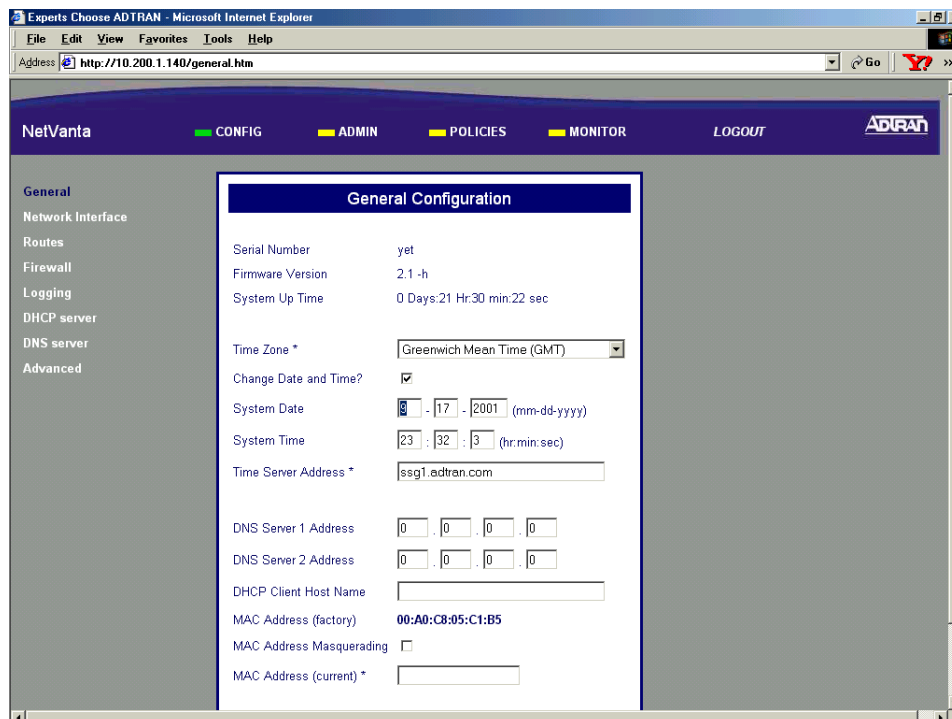
- Click the **CHANGE DATE AND TIME?** checkbox (located in the upper third of the screen).



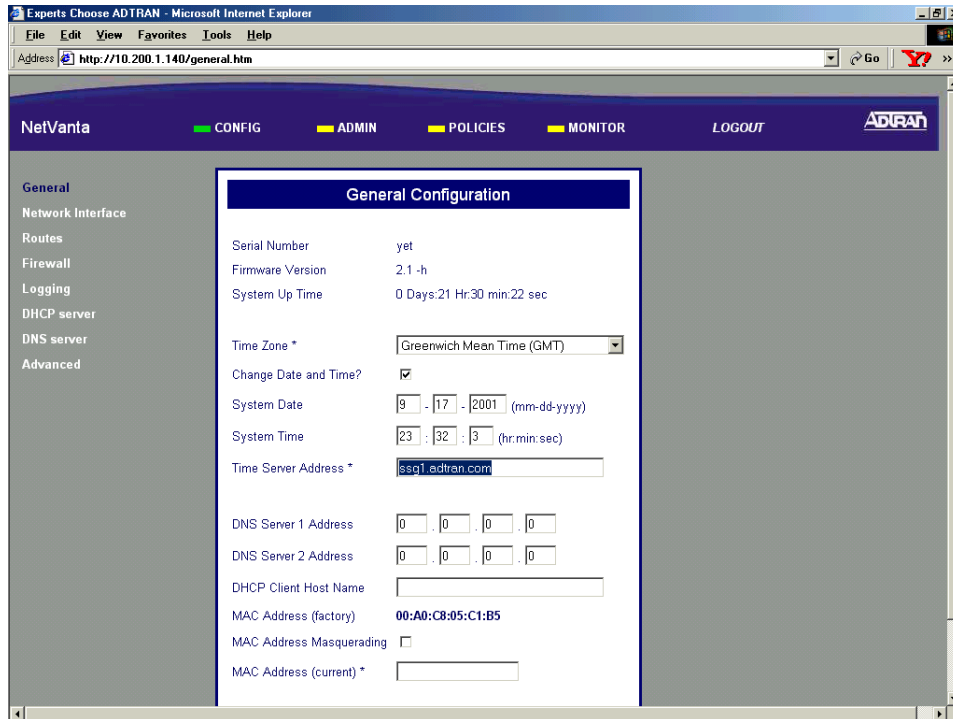
5. Select the appropriate time zone from the **TIME ZONE** drop-down menu (located in the upper third of the screen).



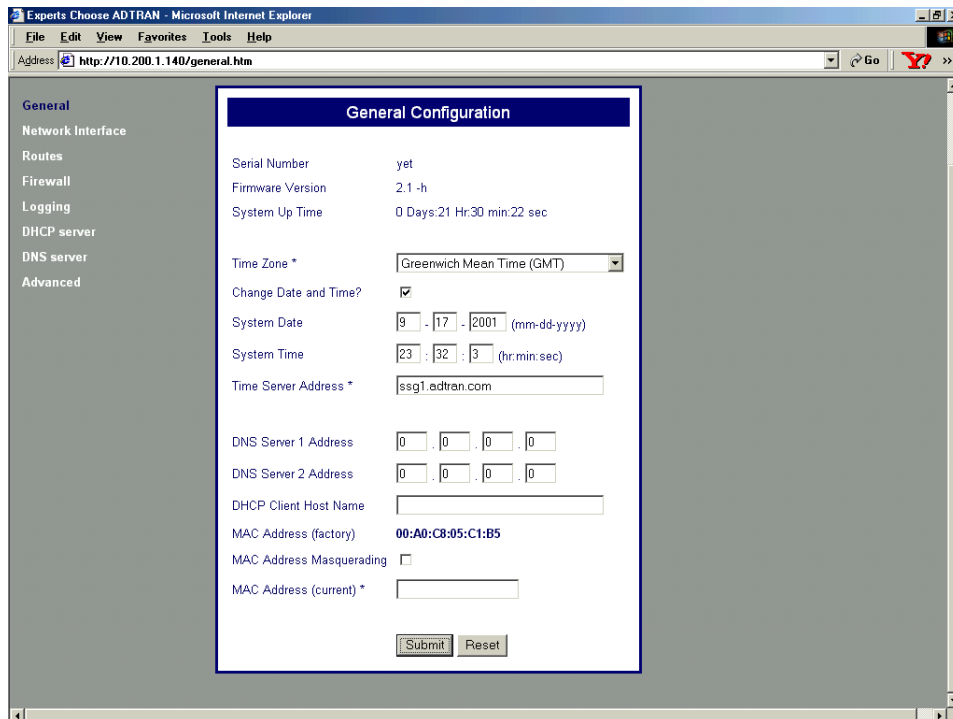
6. Enter the **SYSTEM DATE** and **SYSTEM TIME** in the appropriate fields.



- Alternately, enter the address of a time server to be used (instead of the local NetVanta 2000 series date and time) in the **TIME SERVER ADDRESS** field.



- Scroll to the bottom of the page and click the **SUBMIT** button.



9. Follow the procedures outlined in DLP-003 to save the settings to nonvolatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

CONFIGURING THE LAN INTERFACE IP ADDRESS

Introduction

When the NetVanta 2000 series is connected to an IP network, there are several IP parameters that must be set in order for the unit to communicate with the network. These parameters are described in this DLP along with the procedures for setting them.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials are required.

WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

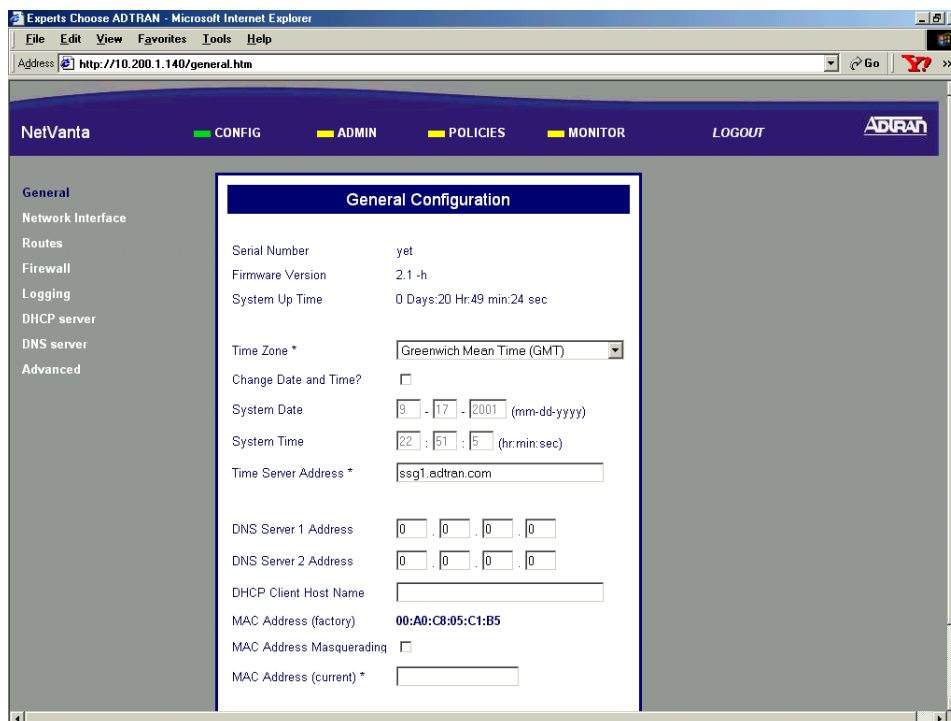
DLP-005

Perform Steps Below in the Order Listed

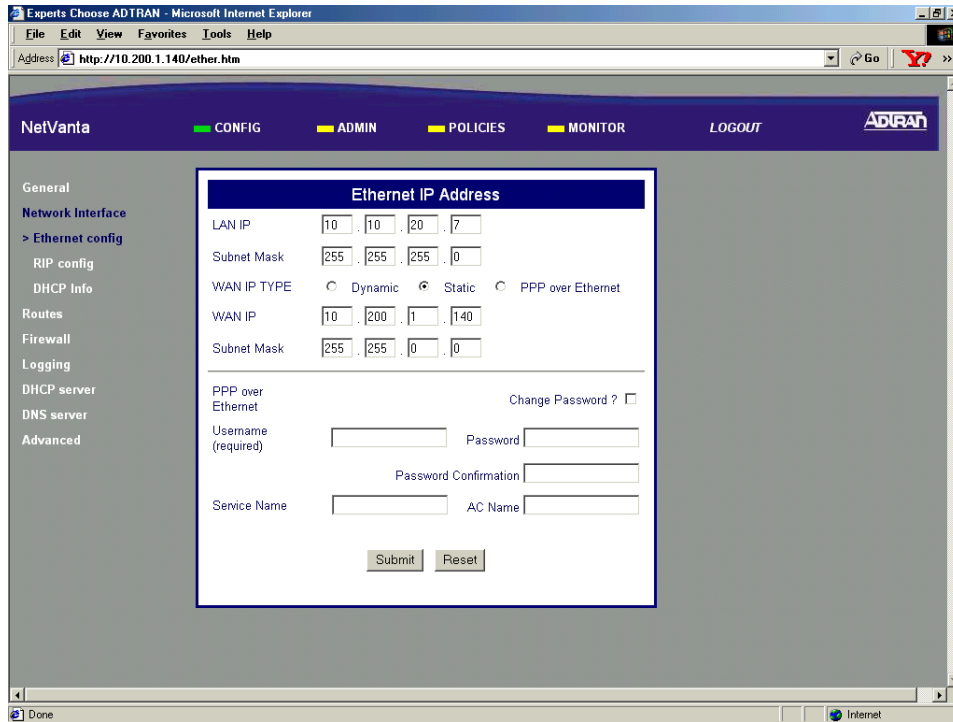
WARNING

*If you are connected to the NetVanta 2000 series through the LAN interface, changing the LAN interface IP address will result in a loss of communication with the unit. Before changing the LAN IP address, follow the steps in **DLP-012, Configuring the LAN Interface DHCP Server** to assign the DHCP server a range of IP addresses on the same subnet as the new LAN IP address.*

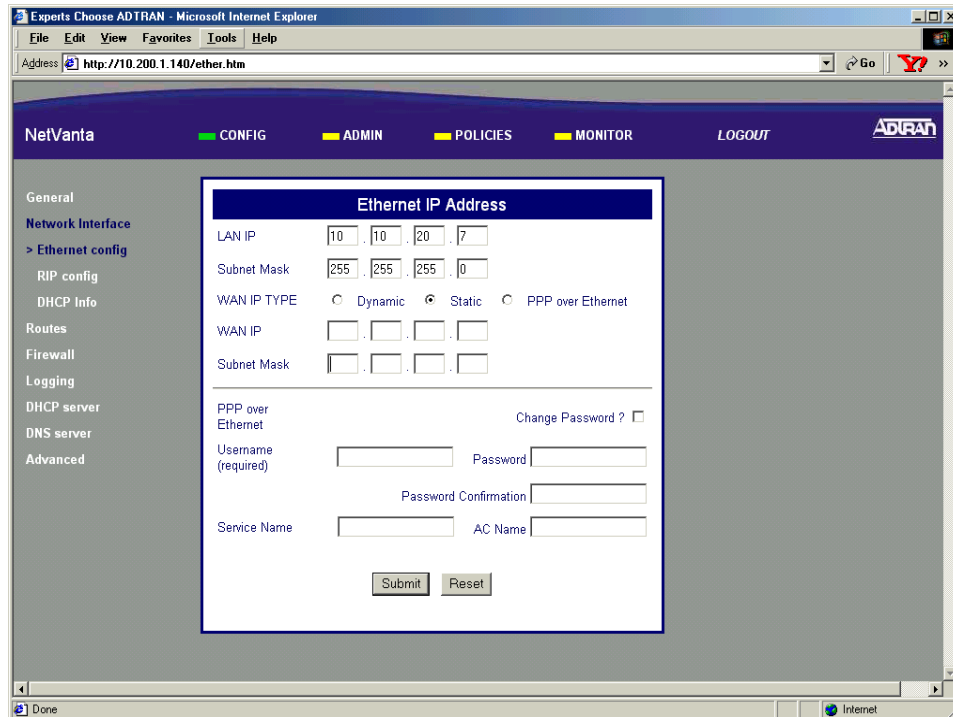
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **CONFIG**.



- From the menu list (located on the left side of the screen), select **NETWORK INTERFACE**. This displays the **ETHERNET CONFIG** page.



- Enter the IP address for the LAN side of the NetVanta 2000 series in the **LAN IP** field. Enter the appropriate subnet mask in the field below.



5. Scroll to the bottom of the screen and click the **SUBMIT** button. The screen will blink and you will return to the Ethernet Config page.
6. Follow the procedures outlined in DLP-003 to save the settings to nonvolatile memory.
7. If you are connecting to the unit via the LAN interface, it will be necessary for you to log into the unit again once the IP address has been changed (see DLP-001 for details).

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

CONFIGURING THE WAN INTERFACE USING DYNAMIC OR STATIC IP ADDRESSING

Introduction

The NetVanta 2000 series supports three IP addressing schemes on the WAN interface -- dynamic, static, and PPP over Ethernet (PPPoE). This DLP discusses the procedure for using either the dynamic IP or static addressing schemes.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials are required.

WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

DLP-006

Perform Steps Below in the Order Listed -- Dynamic Addressing

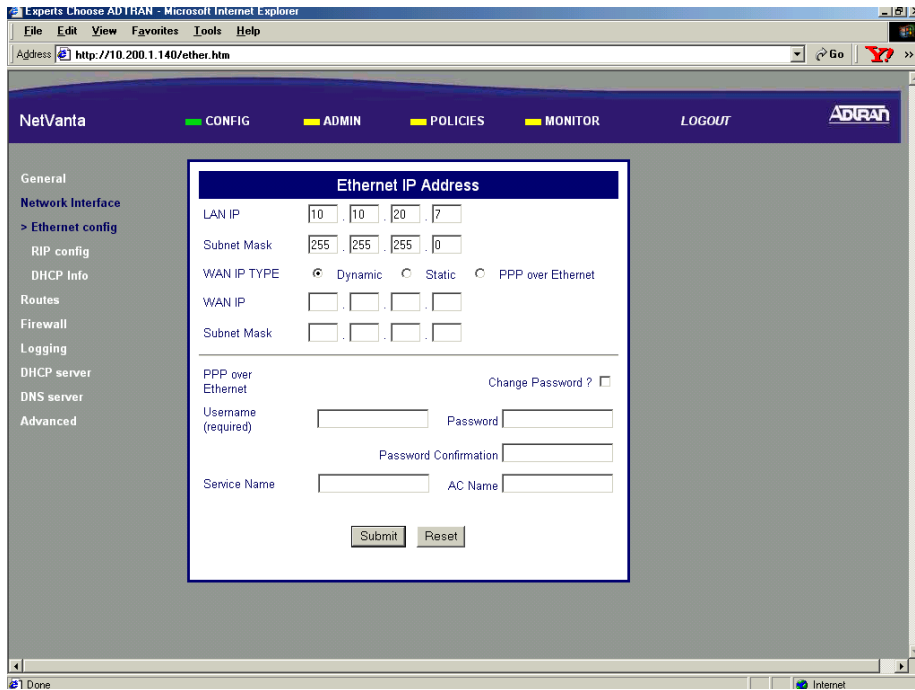
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **CONFIG**. The **ETHERNET CONFIG** page will appear.

The screenshot shows a web browser window titled "Experts Choose ADTRAN - Microsoft Internet Explorer" with the address bar displaying "http://10.200.1.140/ether.htm". The main content area is titled "Ethernet IP Address" and contains the following configuration options:

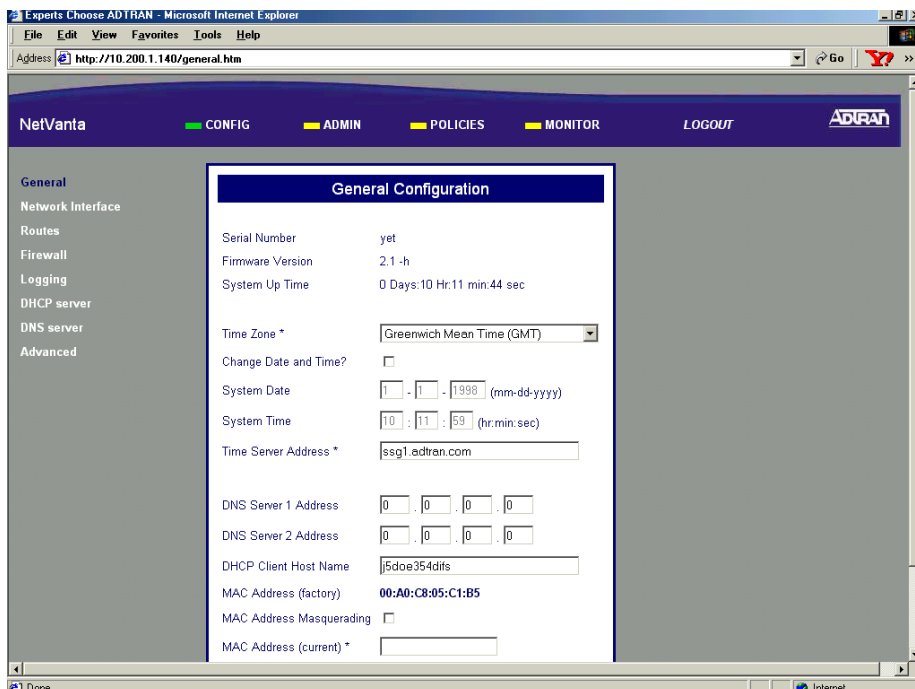
- LAN IP:** 10 . 10 . 20 . 7
- Subnet Mask:** 255 . 255 . 255 . 0
- WAN IP TYPE:** Dynamic Static PPP over Ethernet
- WAN IP:** 10 . 200 . 1 . 140
- Subnet Mask:** 255 . 255 . 0 . 0
- PPP over Ethernet:** Change Password ?
- Username (required):** **Password:**
- Password Confirmation:**
- Service Name:** **AC Name:**

At the bottom of the form are "Submit" and "Reset" buttons. The left sidebar contains a navigation menu with items: General, Network Interface, > Ethernet config, RIP config, DHCP Info, Routes, Firewall, Logging, DHCP server, DNS server, and Advanced. The top navigation bar includes "NetVanta", "CONFIG", "ADMIN", "POLICIES", "MONITOR", "LOGOUT", and the ADTRAN logo.

3. Select the **DYNAMIC** radio button in the **WAN IP TYPE CONFIGURATION** section.



4. Scroll to the bottom of the screen and click the **SUBMIT** button. The screen will blink and you will return to the Ethernet Config page.
5. Some Service Providers require the use of a unique DHCP Client Name to acquire an IP address dynamically. Enter this unique name (given to you by your provider) by selecting Config from the main menu (located across the top of the screen) and then selecting General from the menu list (located down the left side of the screen) and typing it in the DHCP Client Name field.



6. Follow the procedures outlined in DLP-003 to save the settings to nonvolatile memory.

Perform Steps Below in the Order Listed -- Static Addressing

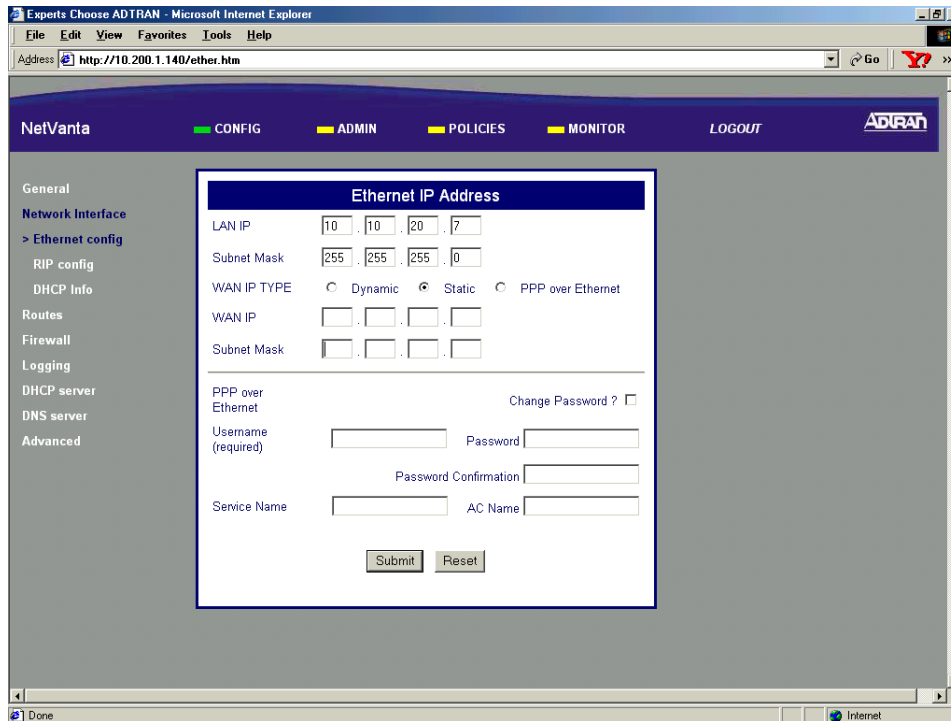
1. Connect the NetVanta 2000 series to a PC and initiate an active browser session (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **CONFIG**. The **ETHERNET CONFIG** page will appear.

The screenshot shows a Microsoft Internet Explorer browser window displaying the NetVanta configuration page. The browser's address bar shows the URL `http://10.200.1.140/ether.htm`. The page has a dark blue header with the NetVanta logo and navigation tabs for CONFIG, ADMIN, POLICIES, MONITOR, and LOGOUT. A left sidebar contains a menu with options like General, Network Interface, RIP config, DHCP Info, Routes, Firewall, Logging, DHCP server, DNS server, and Advanced. The main content area is titled "Ethernet IP Address" and contains the following configuration fields:

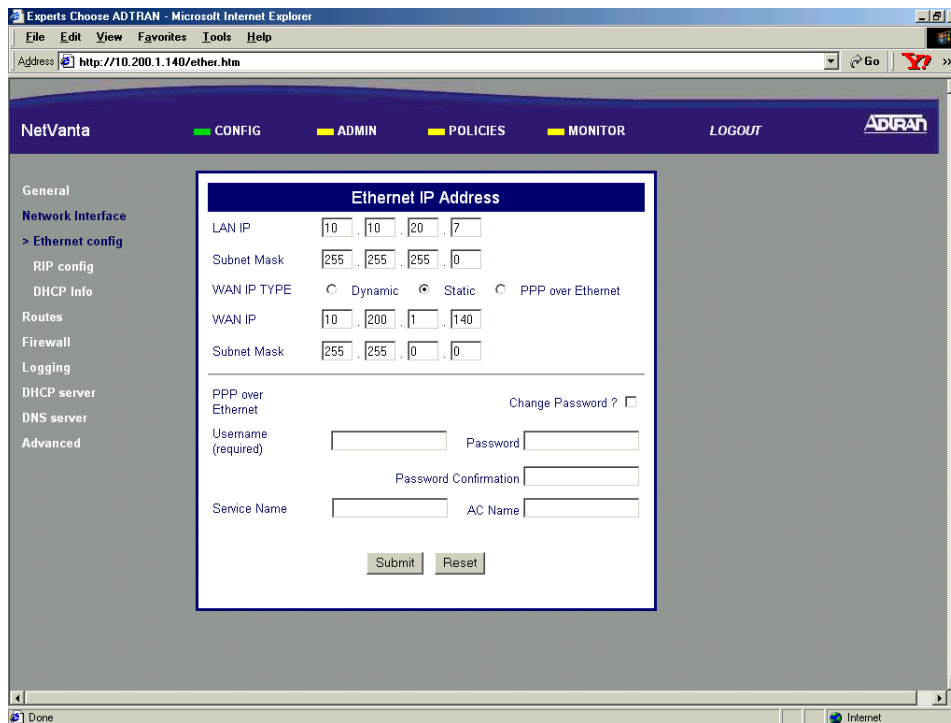
- LAN IP: 10 . 10 . 20 . 7
- Subnet Mask: 255 . 255 . 255 . 0
- WAN IP TYPE: Dynamic Static PPP over Ethernet
- WAN IP: 10 . 200 . 1 . 140
- Subnet Mask: 255 . 255 . 0 . 0
- PPP over Ethernet: Change Password ?
- Username (required): Password:
- Password Confirmation:
- Service Name: AC Name:

At the bottom of the form are "Submit" and "Reset" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

3. Select the **STATIC** radio button in the **WAN IP TYPE CONFIGURATION** section.



4. Enter the IP address of the NetVanta 2000 series WAN interface in the **WAN IP** data field. Enter the appropriate subnet mask in the fields below.



5. Scroll to the bottom of the screen and click the **SUBMIT** button. The screen will blink and you will return to the Ethernet Config page.
6. Follow the procedures outlined in DLP-003 to save the settings to nonvolatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

CONFIGURING THE WAN INTERFACE FOR PPPoE ADDRESSING

Introduction

The NetVanta 2000 series supports three IP addressing schemes on the WAN interface -- dynamic, static, and PPP over Ethernet (PPPoE). This DLP discusses the procedure for using the PPPoE addressing scheme.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials are required.

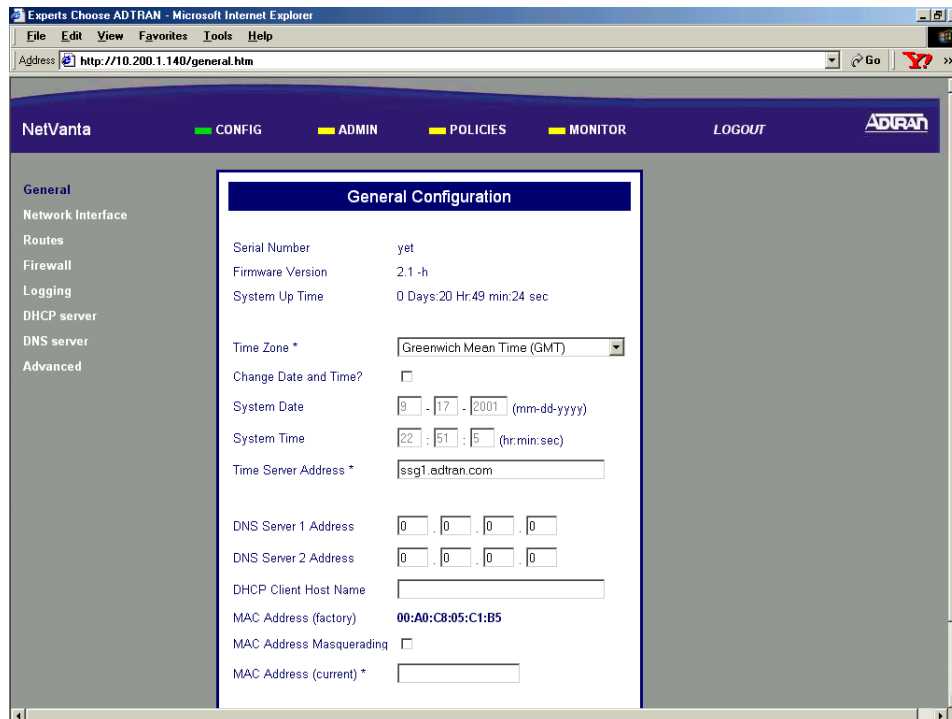
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

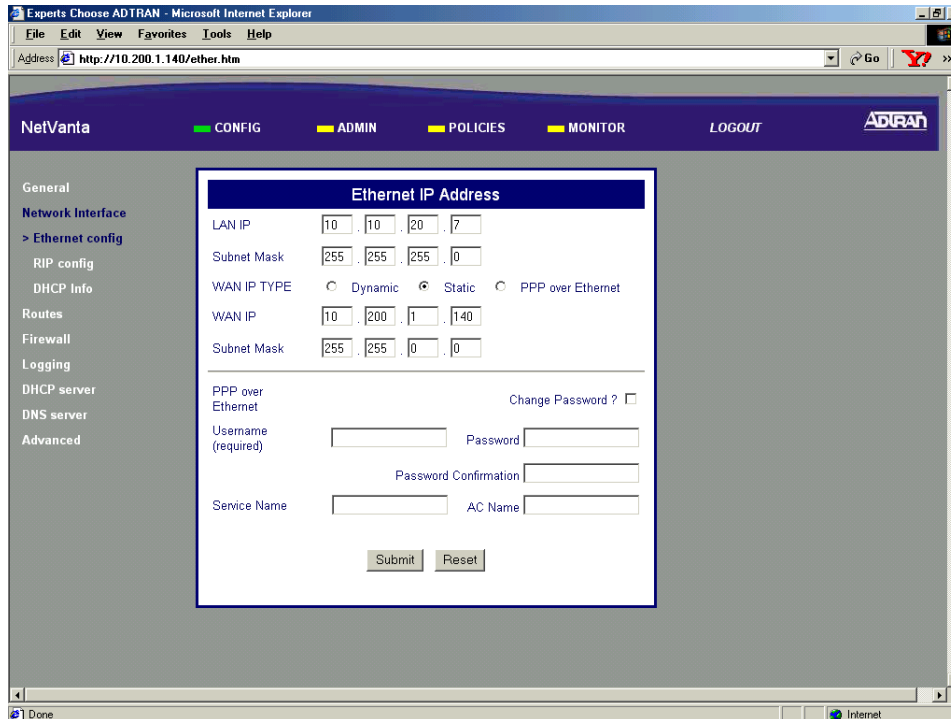
DLP-007

Perform Steps Below in the Order Listed

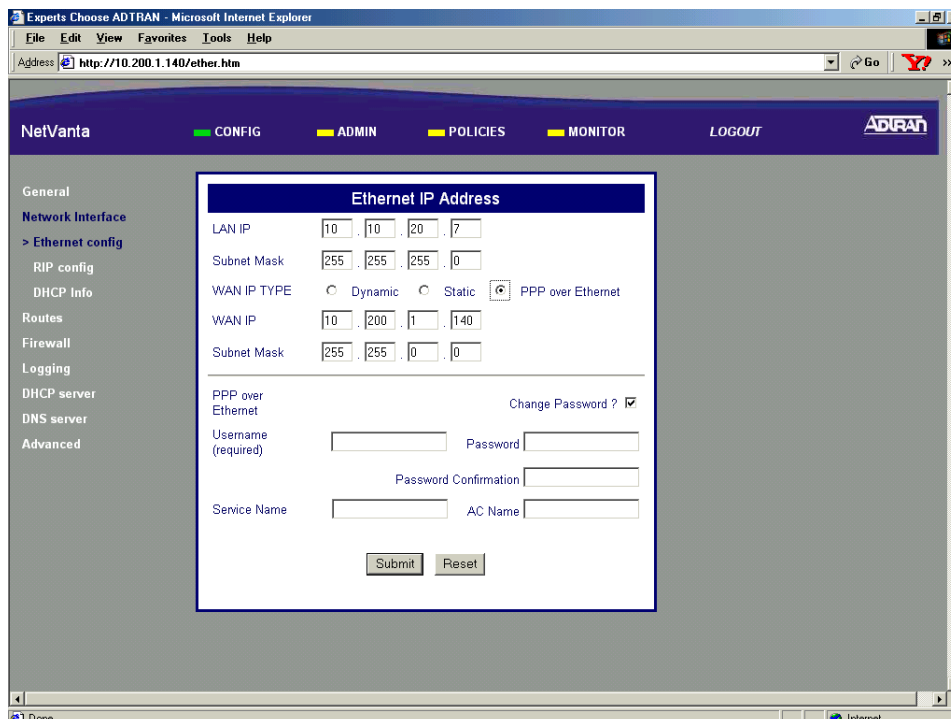
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **CONFIG**. The **GENERAL** page will appear.



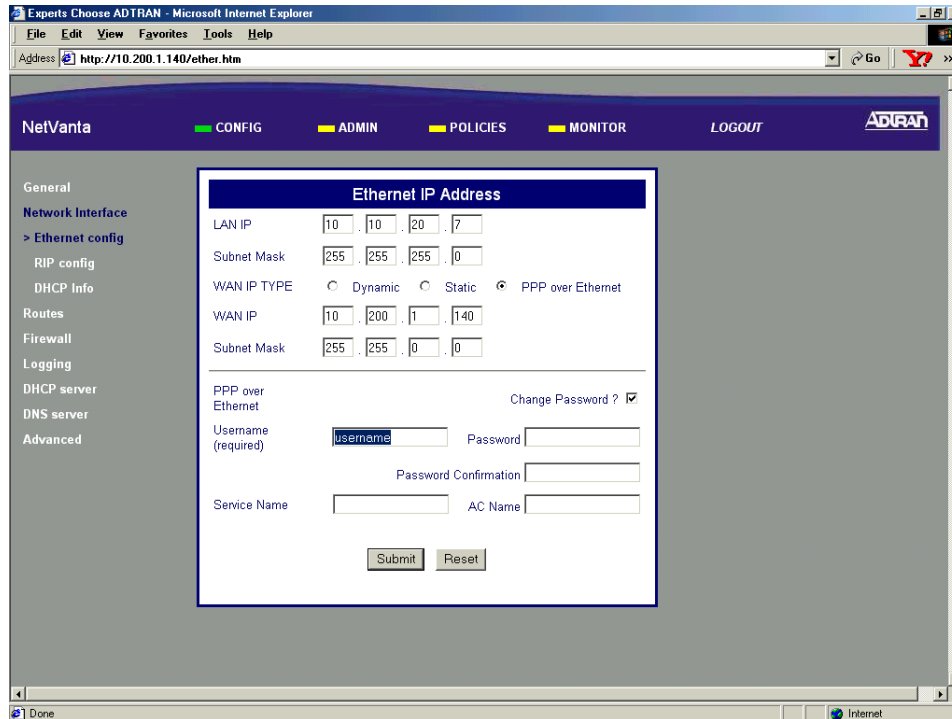
- From the menu list (located on the left side of the screen) select **NETWORK INTERFACE**. The Ethernet Config page will appear.



- Select the **PPP OVER ETHERNET** radio button in the **WAN IP TYPE CONFIGURATION** section.



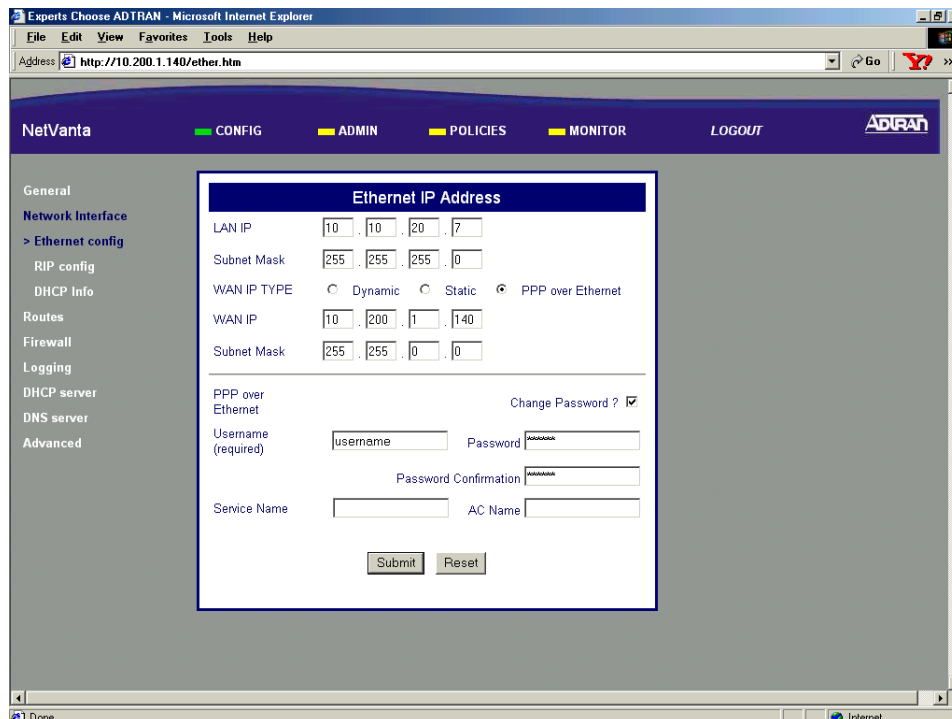
5. Enter the username (provided by your service provider) in the **USERNAME** field in the **PPP OVER ETHERNET** configuration section.



The screenshot shows the NetVanta configuration interface in a Microsoft Internet Explorer browser window. The address bar shows <http://10.200.1.140/ether.htm>. The page title is "Experts Choose ADTRAN - Microsoft Internet Explorer". The main navigation bar includes "NetVanta", "CONFIG", "ADMIN", "POLICIES", "MONITOR", and "LOGOUT". The left sidebar lists various configuration sections: General, Network Interface, Ethernet config, RIP config, DHCP Info, Routes, Firewall, Logging, DHCP server, DNS server, and Advanced. The main content area is titled "Ethernet IP Address" and contains the following fields and options:

- LAN IP: 10 . 10 . 20 . 7
- Subnet Mask: 255 . 255 . 255 . 0
- WAN IP TYPE: Dynamic Static PPP over Ethernet
- WAN IP: 10 . 200 . 1 . 140
- Subnet Mask: 255 . 255 . 0 . 0
- PPP over Ethernet: Change Password ?
- Username (required): Password:
- Password Confirmation:
- Service Name: AC Name:
- Buttons:

6. Enter the password for the username entered in Step 4 in both the **PASSWORD** and **PASSWORD CONFIRMATION** fields.



The screenshot shows the NetVanta configuration interface in a Microsoft Internet Explorer browser window. The address bar shows <http://10.200.1.140/ether.htm>. The page title is "Experts Choose ADTRAN - Microsoft Internet Explorer". The main navigation bar includes "NetVanta", "CONFIG", "ADMIN", "POLICIES", "MONITOR", and "LOGOUT". The left sidebar lists various configuration sections: General, Network Interface, Ethernet config, RIP config, DHCP Info, Routes, Firewall, Logging, DHCP server, DNS server, and Advanced. The main content area is titled "Ethernet IP Address" and contains the following fields and options:

- LAN IP: 10 . 10 . 20 . 7
- Subnet Mask: 255 . 255 . 255 . 0
- WAN IP TYPE: Dynamic Static PPP over Ethernet
- WAN IP: 10 . 200 . 1 . 140
- Subnet Mask: 255 . 255 . 0 . 0
- PPP over Ethernet: Change Password ?
- Username (required): Password:
- Password Confirmation:
- Service Name: AC Name:
- Buttons:



For most applications, the **SERVICE NAME** and **AC NAME** (Access Concentrator) fields should remain blank. Only populate these fields if specific information has been provided by the service provider.

7. Scroll to the bottom of the screen and click the **SUBMIT** button.

The screenshot shows a web browser window titled "Experts Choose ADTRAN - Microsoft Internet Explorer". The address bar shows "http://10.200.1.140/ether.htm". The page content includes a navigation menu with "CONFIG", "ADMIN", "POLICIES", "MONITOR", and "LOGOUT". The main content area is titled "Ethernet IP Address" and contains the following fields and options:

- LAN IP: 10 . 10 . 20 . 7
- Subnet Mask: 255 . 255 . 255 . 0
- WAN IP TYPE: Dynamic Static PPP over Ethernet
- WAN IP: 10 . 200 . 1 . 140
- Subnet Mask: 255 . 255 . 0 . 0
- PPP over Ethernet: Change Password ?
- Username (required): Password:
- Password Confirmation:
- Service Name: AC Name:

At the bottom of the form are "Submit" and "Reset" buttons.

8. Follow the procedures outlined in DLP-003 to save the settings to nonvolatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

UPGRADING THE FIRMWARE OF THE NETVANTA 2000 SERIES

Introduction

The NetVanta 2000 series supports firmware updates via the LAN and WAN interfaces and an active **ADMIN** login session. Using an active browser session and the provided GUI, the NetVanta 2000 series may be upgraded by loading firmware files(**.bin**) into the unit.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials are required.



The NetVanta 2000 series upgrade firmware feature is only available using the Internet Explorer web browser.

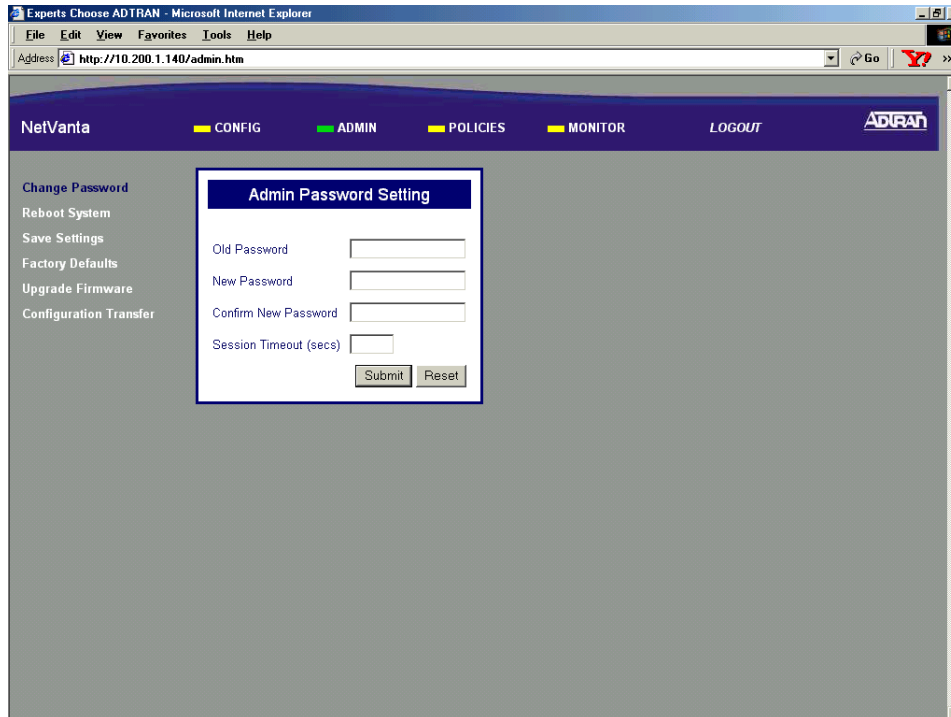


To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

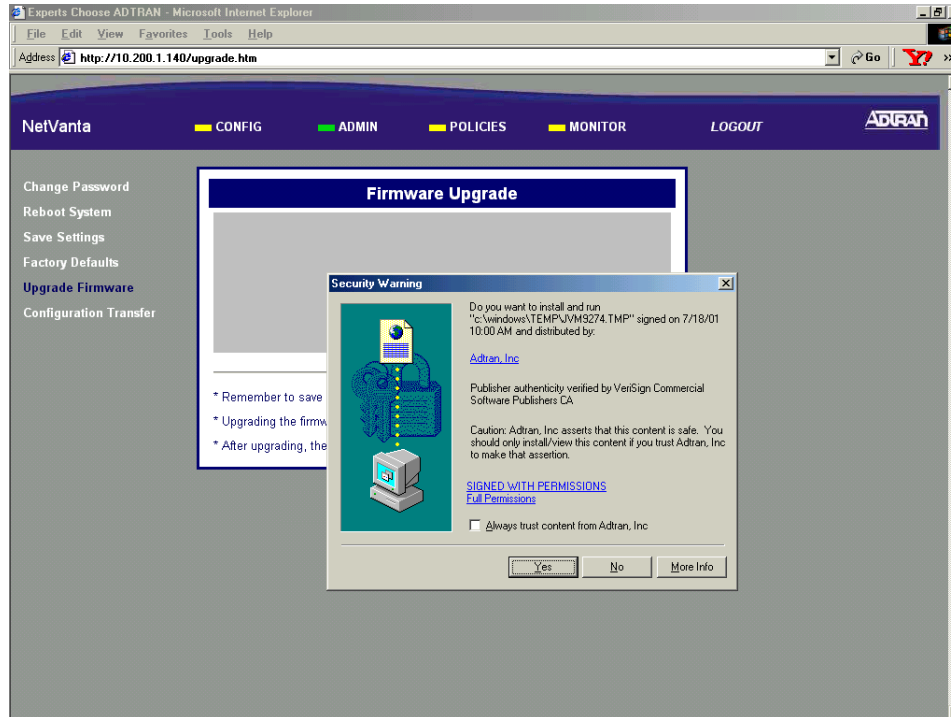
DLP-008

Perform Steps Below in the Order Listed

1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **ADMIN**.



- From the menu list (located down the left side of the screen), select **UPGRADE FIRMWARE**. While this page is loading, you will be asked to install and run a Java applet distributed by ADTRAN, Inc., and verified by VeriSign Commercial Software Publishers. If security is not enabled on your internet browser, the screen below will not be shown.

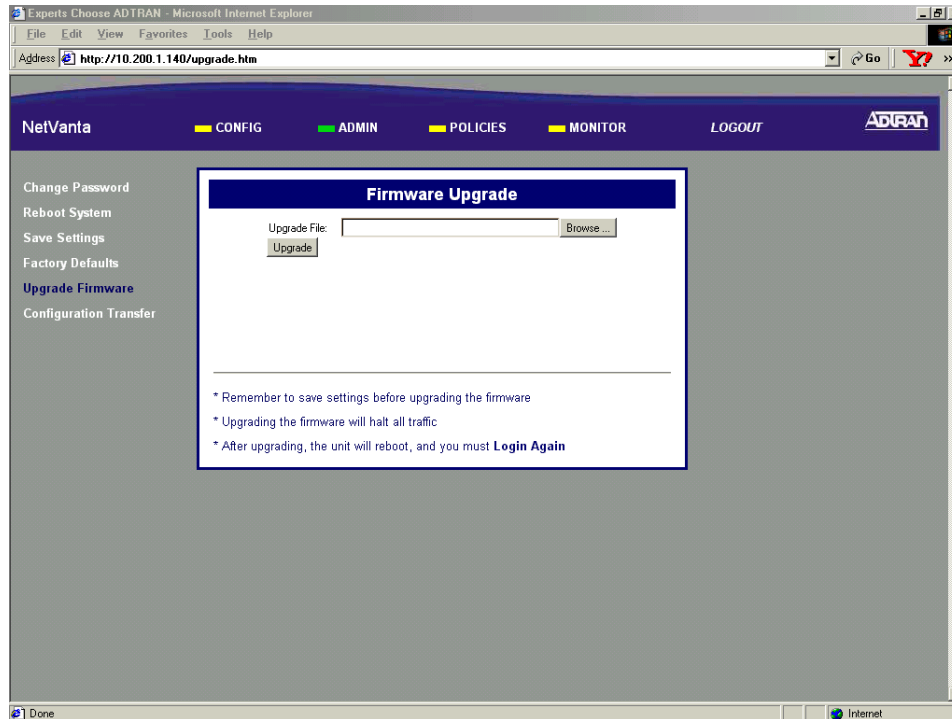


- Click **YES** to install and run the Java applet.

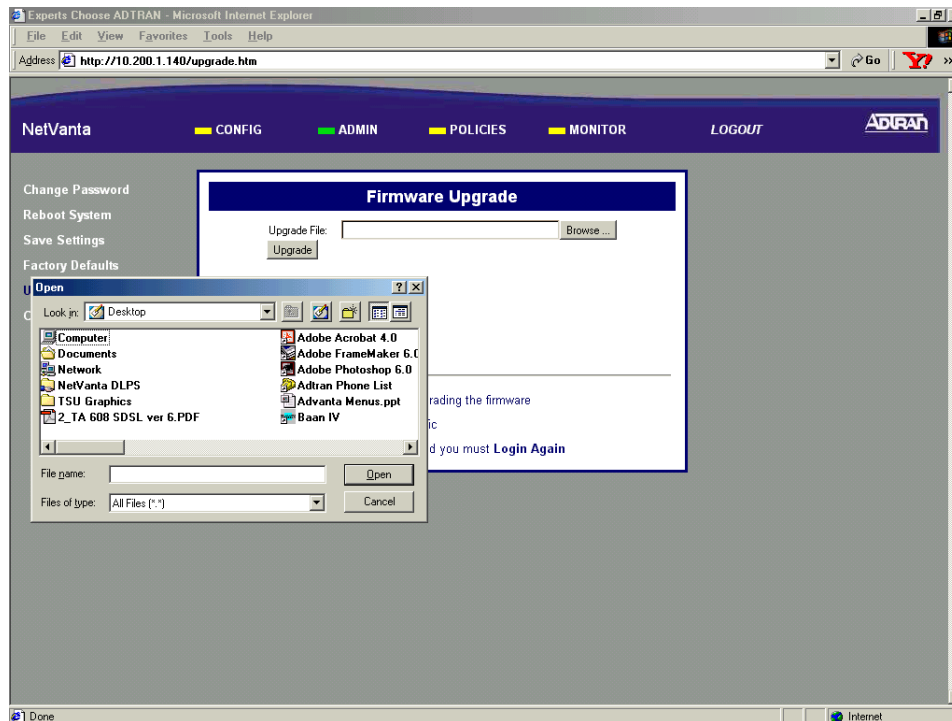


The Java script must be installed for the firmware update capabilities to function properly.

5. Enter the filename (including path) of the firmware file you wish to load. Firmware files for the NetVanta 2000 series will have a **.bin** extension.



Alternately, click the **BROWSE** button to navigate to the file using the pop-up explorer window.



6. Click the **UPGRADE** button to begin the upgrade.

WARNING

All settings not saved into nonvolatile memory (following the procedures in DLP-002) will be lost during the firmware upgrade.

**NOTE**

During the firmware upgrade, all traffic will be halted through the NetVanta 2000 series. The unit will reboot and you will be asked to log in again.

7. Log in to the NetVanta 2000 series using the admin username and appropriate password to continue configuration.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

SAVING THE CURRENT CONFIGURATION OF THE NETVANTA

Introduction

The NetVanta 2000 series supports configuration transfers from the unit (via either the LAN or WAN interface) using an active browser session. This DLP provides the steps to follow for a successful configuration transfer using a PC and an active browser session.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required

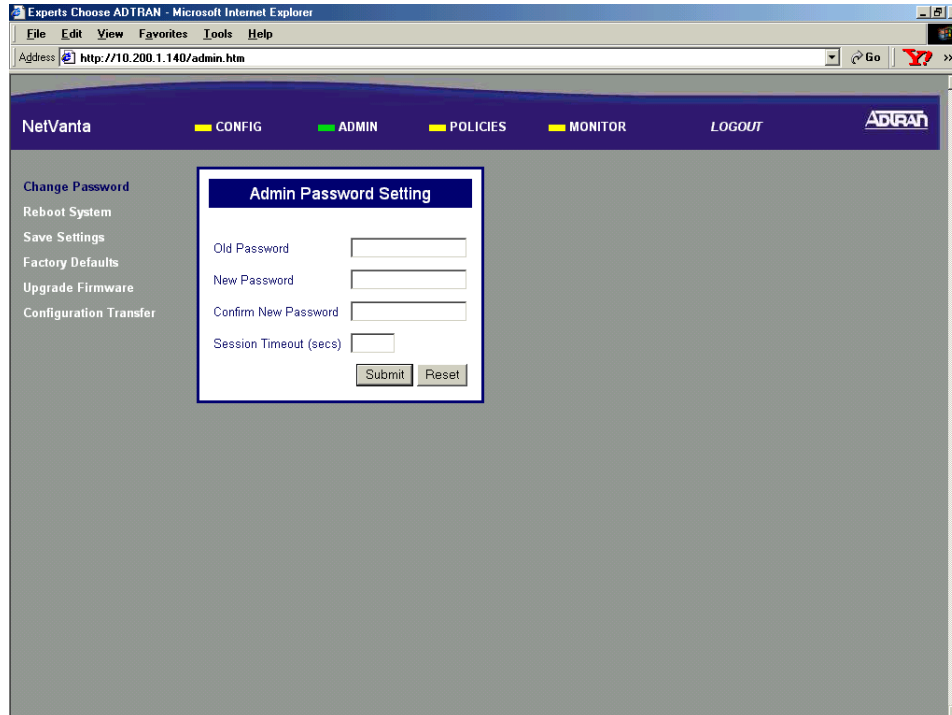
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

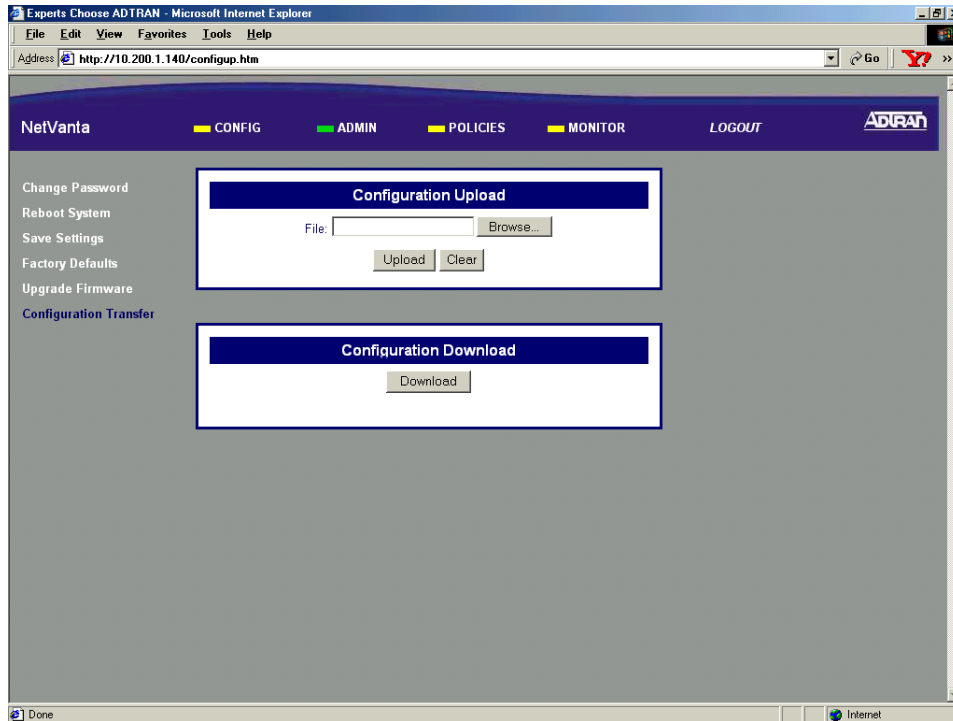
DLP-009

Perform Steps Below in the Order Listed

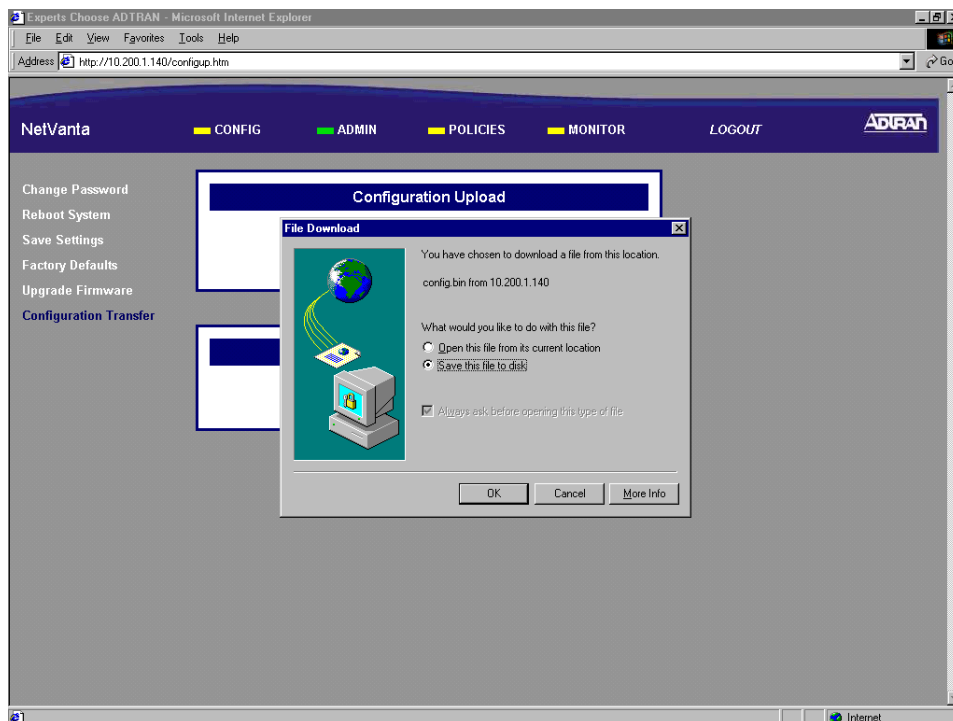
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select ADMIN.



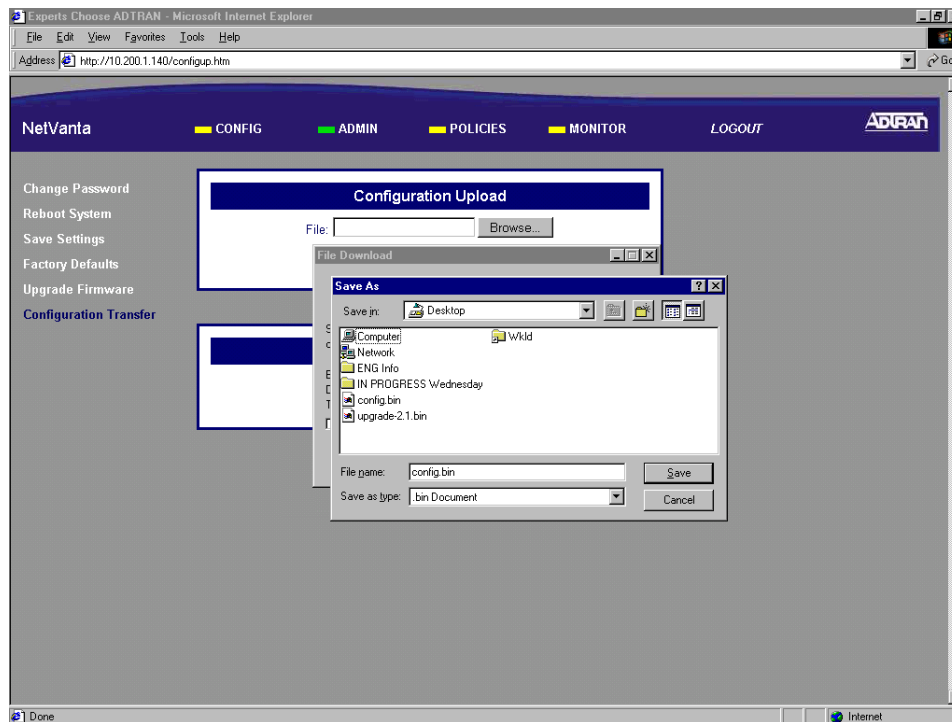
- From the menu list (located on the left side of the screen) select Configuration Transfer.



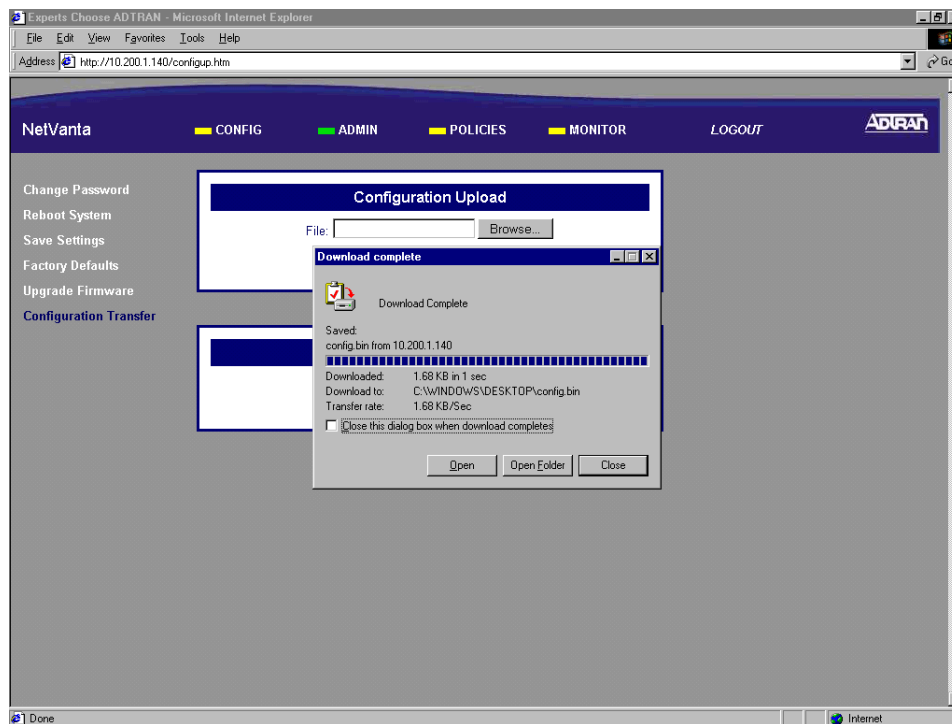
- In the Configuration Download dialog box, click the Download button. A Windows file download dialog box will appear. Click the Save file to disk radio button and click OK.



5. In the Save As dialog box enter the name for the NetVanta configuration file (all filenames must have a .bin extension). Browse to the location where you would like to save the file and click the Save button.



6. A Windows File Download status dialog will briefly display showing the current status of the download.



7. Using your file manager, check to make sure your configuration file was saved in your desired location.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

LOADING A SAVED CONFIGURATION INTO THE NETVANTA

Introduction

The NetVanta 2000 series supports configuration transfers from the unit (via the LAN interface) using an active browser session. This DLP provides the steps to follow for a successful configuration transfer using a PC and an active browser session.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.



The NetVanta 2000 series upgrade firmware feature is only available using the Internet Explorer web browser.

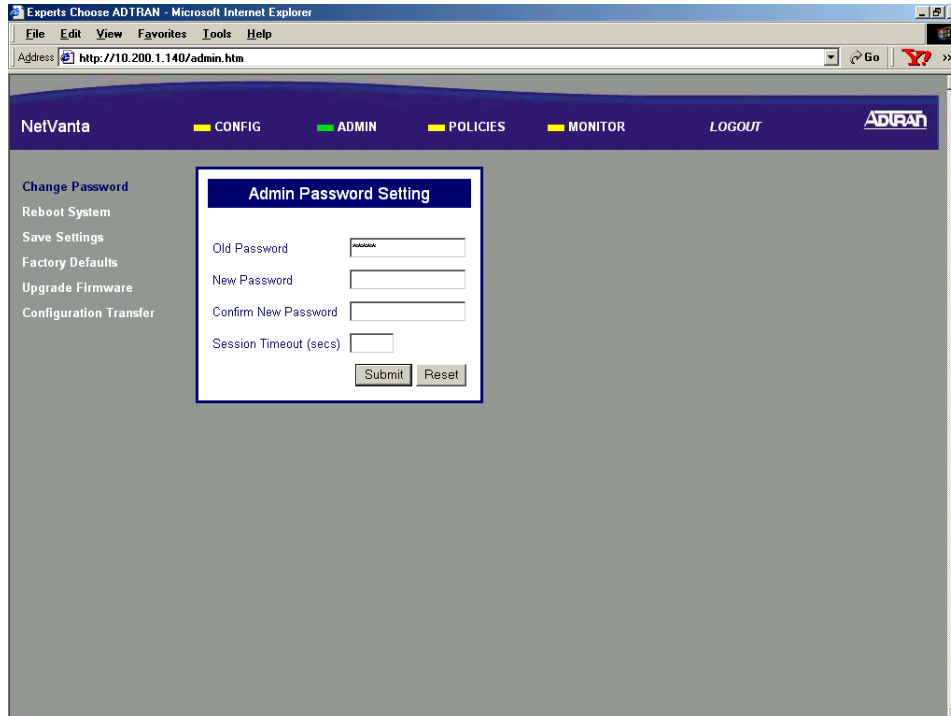


To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

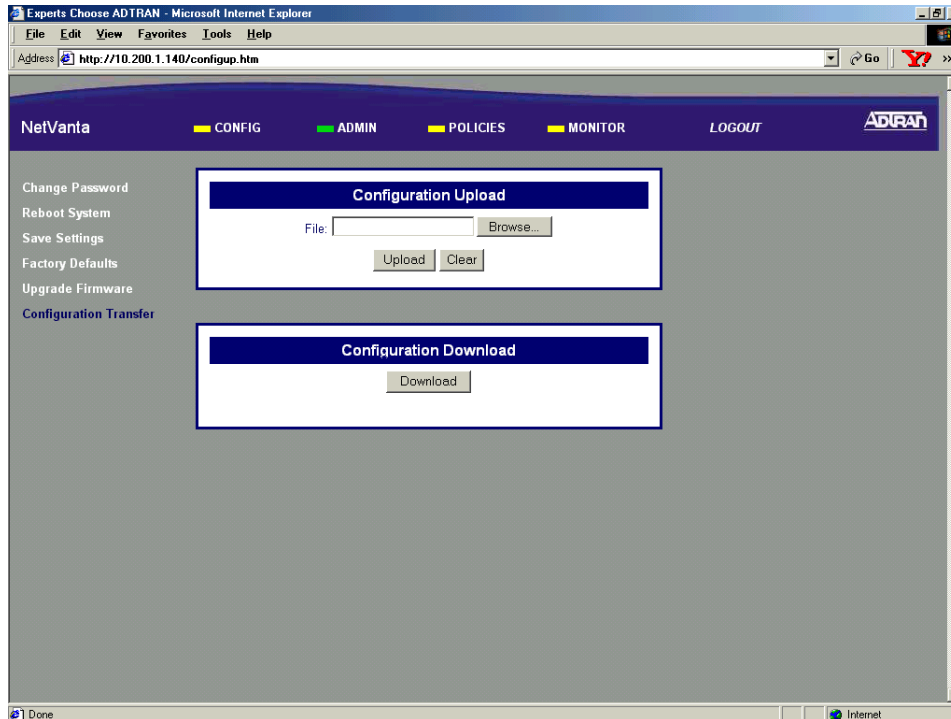
DLP-010

Perform Steps Below in the Order Listed

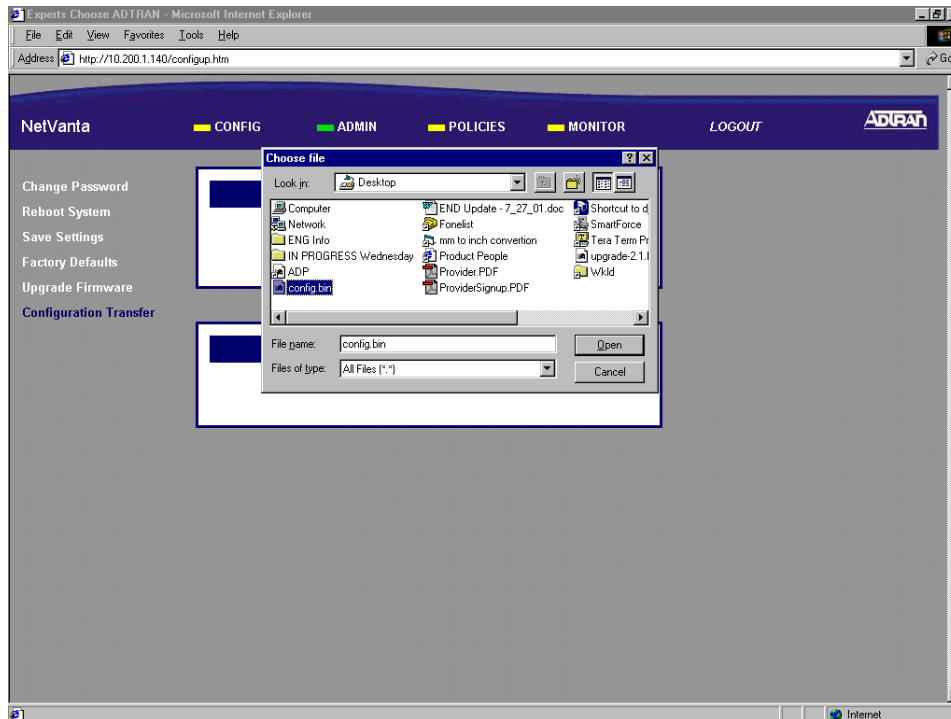
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select ADMIN.



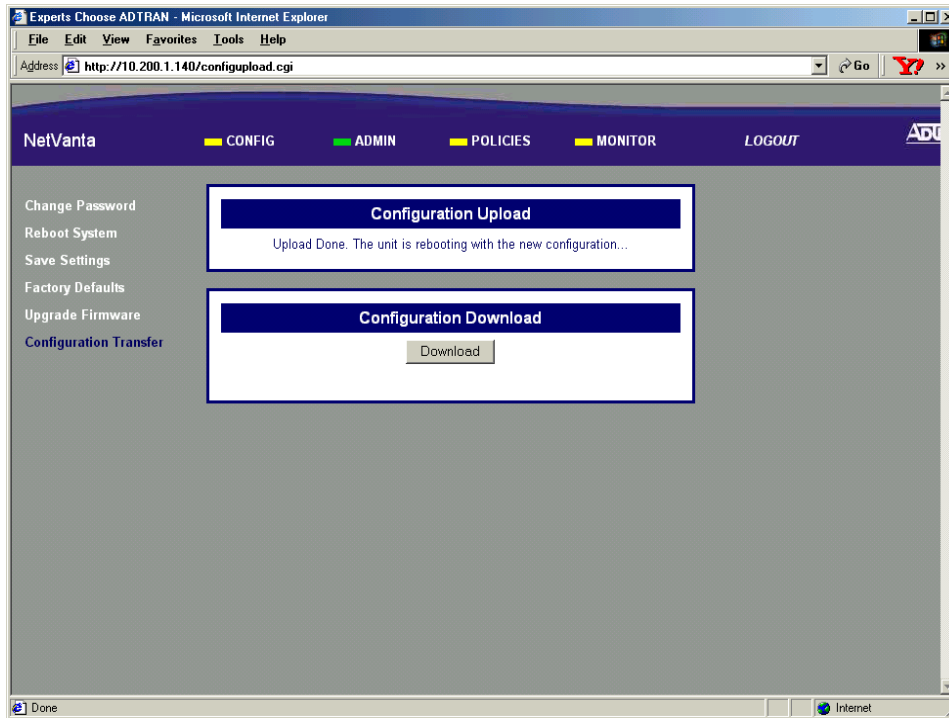
- From the menu list (located on the left side of the screen) select Configuration Transfer.



- In the Configuration Upload dialog box either enter the filename of the configuration file you want to load into the unit (including path), or click the Browse button to open a Windows Choose file dialog box and select the desired file. All configuration files for the NetVanta 2000 series must have a .bin extension.



5. In the Configuration Upload dialog box click the Upload button. If a successful upload is completed, the unit will display the status message in the Configuration Upload dialog box.



6. Once the upload is complete the NetVanta 2000 series unit will reboot to install the new configuration. You will need to log in to the unit after the reboot is complete (see DLP-001 for details).

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

ADDING A DEFAULT ROUTE TO THE NETVANTA ROUTE TABLE

Introduction

The NetVanta 2000 series contains an internal router which allows multiple users to share a VPN connection while the unit is still directing incoming IP traffic. The NetVanta 2000 series router supports standard TCP/IP operation, static routes, and the use of RIP V1 and V2. This DLP discusses the procedure for adding a default route to the NetVanta 2000 series route table.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.



*If you are using Static IP addressing on your WAN interface your Internet Service Provider must provide you with the IP address of your first hop router. If you are using DHCP (Dynamic) or PPPoE addressing, please complete the steps in **DLP-022, Viewing the DHCP Info Table** before beginning this DLP. You will need to record the IP address listed next to Gateways in the WAN interface column.*

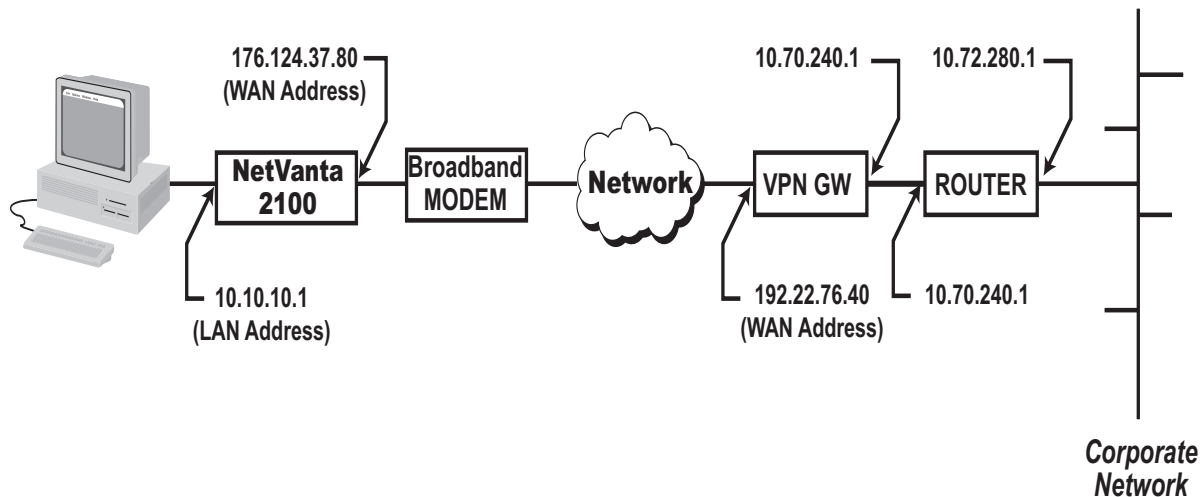
Tools and Materials Required

- No special tools or materials required.



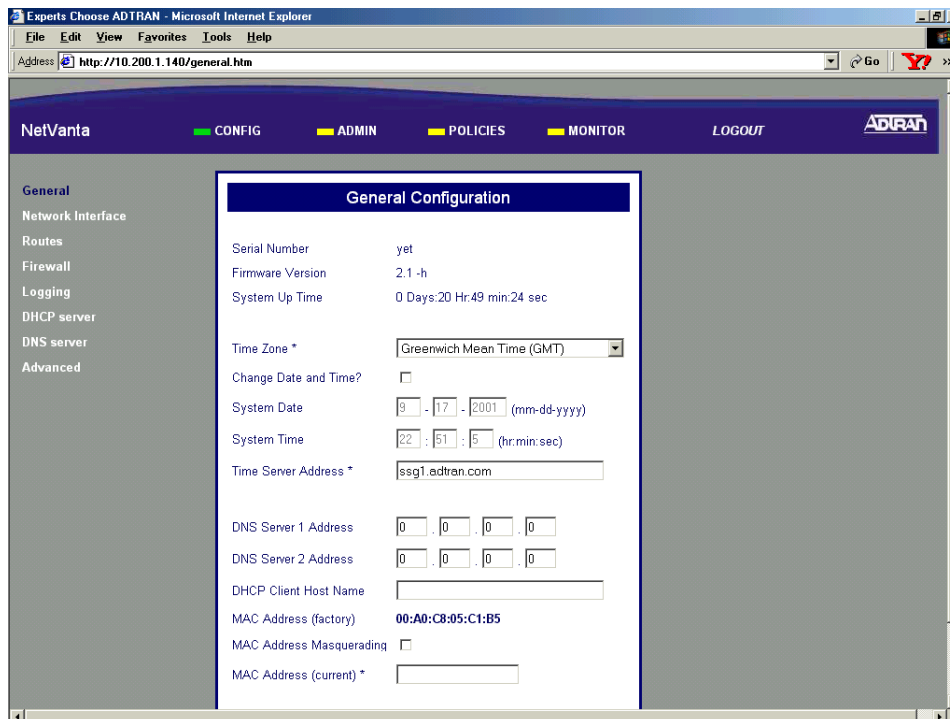
To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

DLP-011



Perform Steps Below in the Order Listed - Default Route

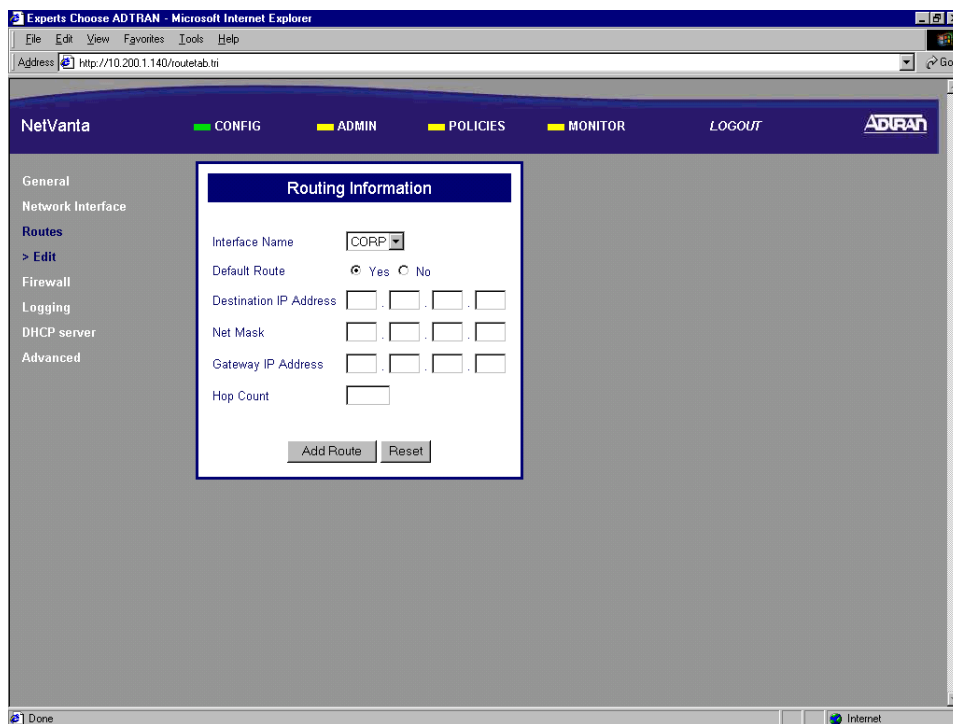
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **CONFIG**.



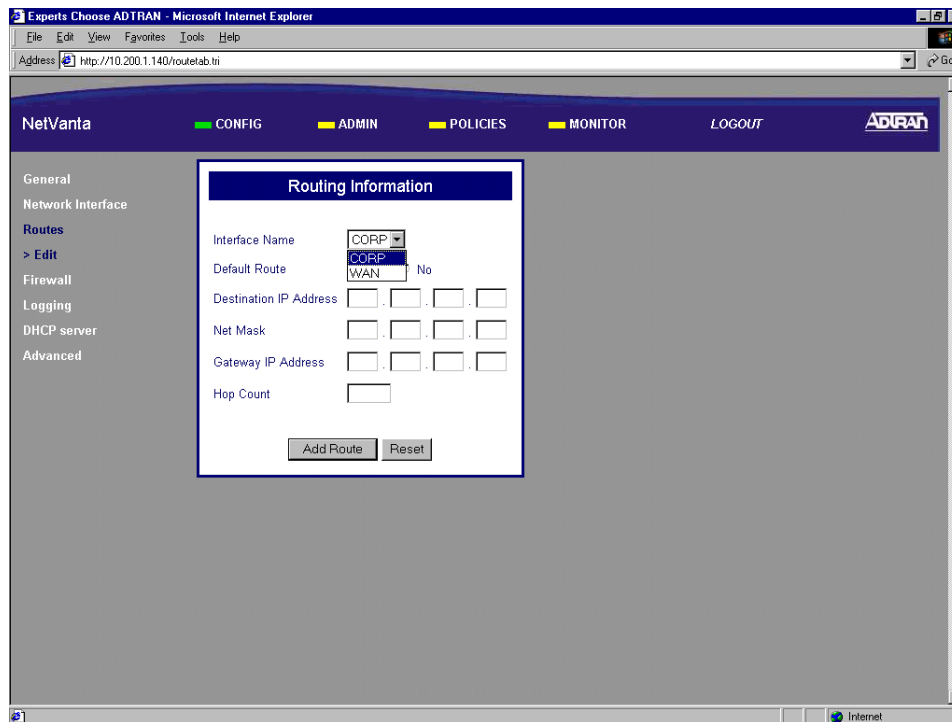
- From the menu list (located on the left side of the screen) select **ROUTES**.



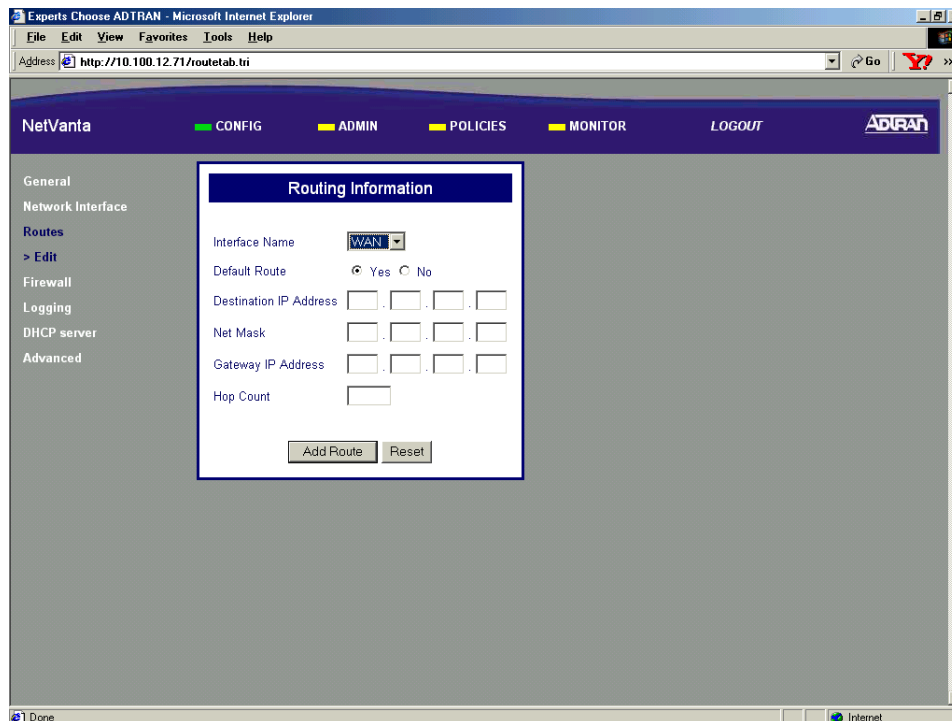
- Click the Add Route button found in the Route Table dialog box. The Routing Information page will appear.



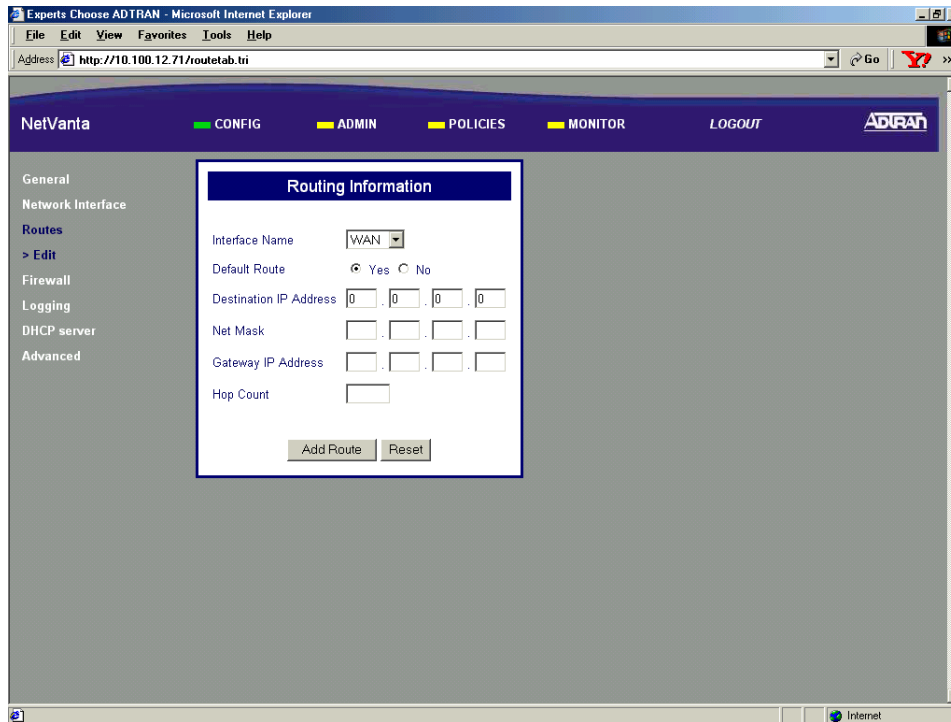
5. Select the interface associated with the new route from the Interface Name drop down menu. The options are CORP (the LAN interface) and WAN. Select WAN to add a default route.



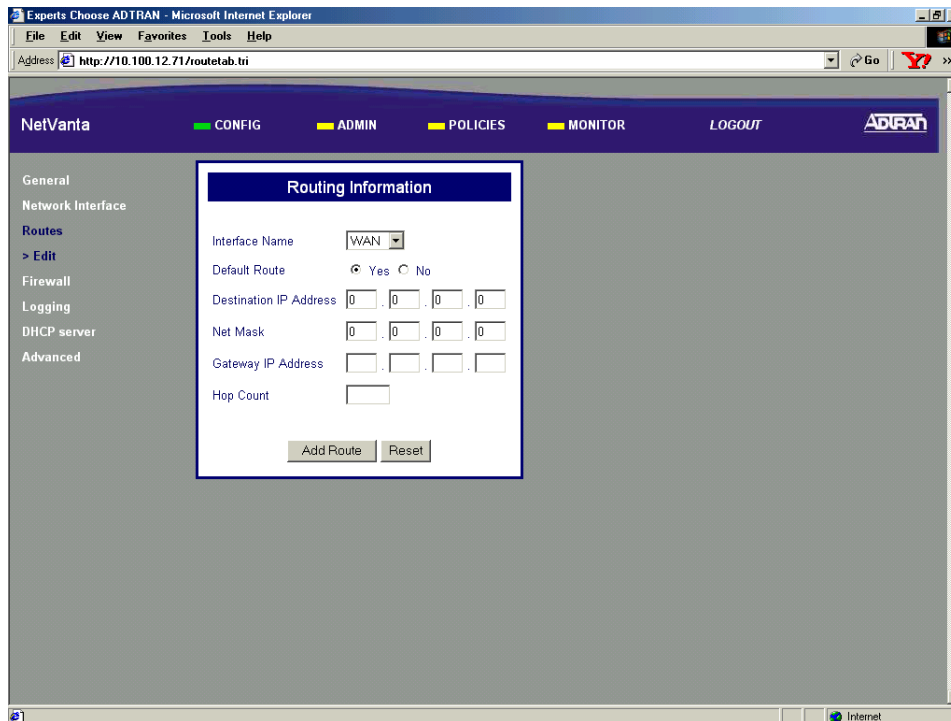
6. Specify whether this route is the default route by selecting the appropriate radio button next to Default Route. For this example we will be entering the default route so YES will be selected.



- Enter the IP address of the far-end network in the Destination IP Address field. For this example we are entering a default route so the Destination IP Address will be 0.0.0.0.



- Enter the subnet mask for the far-end network in the Net Mask field. For this example we are entering a default route so the Net Mask will be 0.0.0.0.



9. If you are using Static IP Addressing on the WAN interface, enter the IP address of the next hop router (provided by your ISP). Alternately, if you are using DHCP (Dynamic) or PPPoE addressing, enter the IP address found in the DHCP Info window (see DLP-022 for details).



10. Enter the number of routers a packet would travel through to reach its destination in the Hop Count field. This field is optional and will be left blank for this example.
11. Click the Add Route button to submit the route to the route table.
12. Follow the procedures in DLP-003 to save the settings to non-volatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

CONFIGURING THE LAN INTERFACE DHCP SERVER

Introduction

The NetVanta 2000 series contains an internal DHCP server to manage IP addresses on the local network. The DHCP server functions on the LAN interface only. This DLP discusses the procedure for configuring the DHCP server for standard operation.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

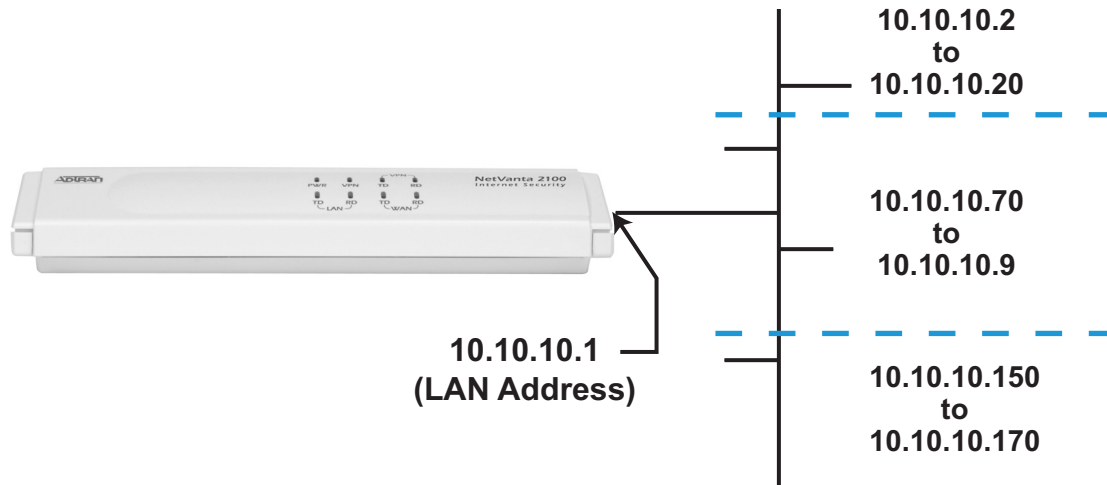
Tools and Materials Required

- No special tools or materials required.

WARNING

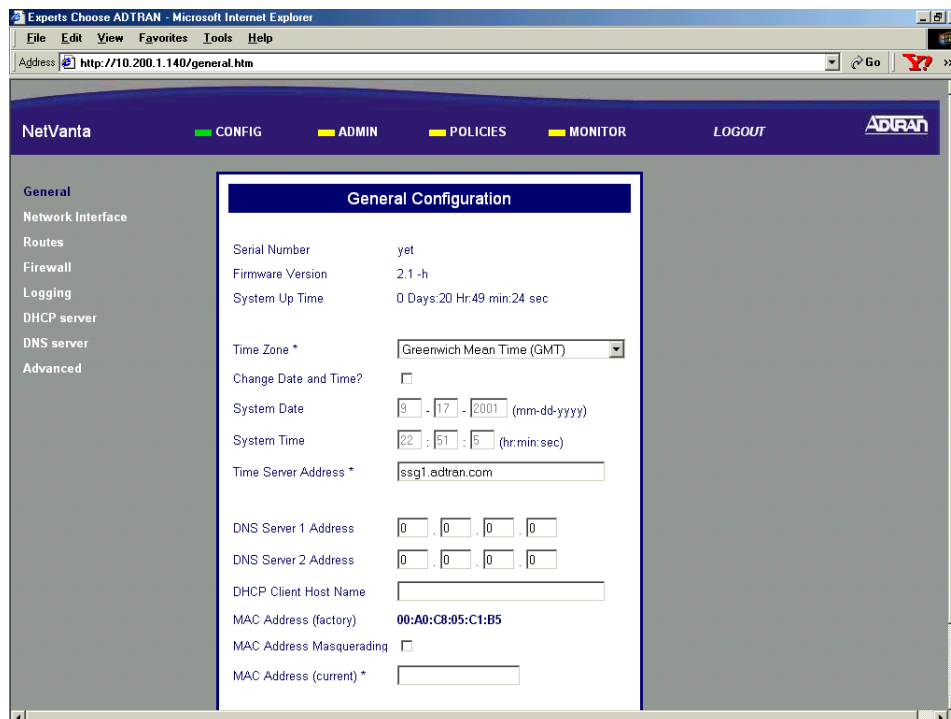
To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

DLP-012

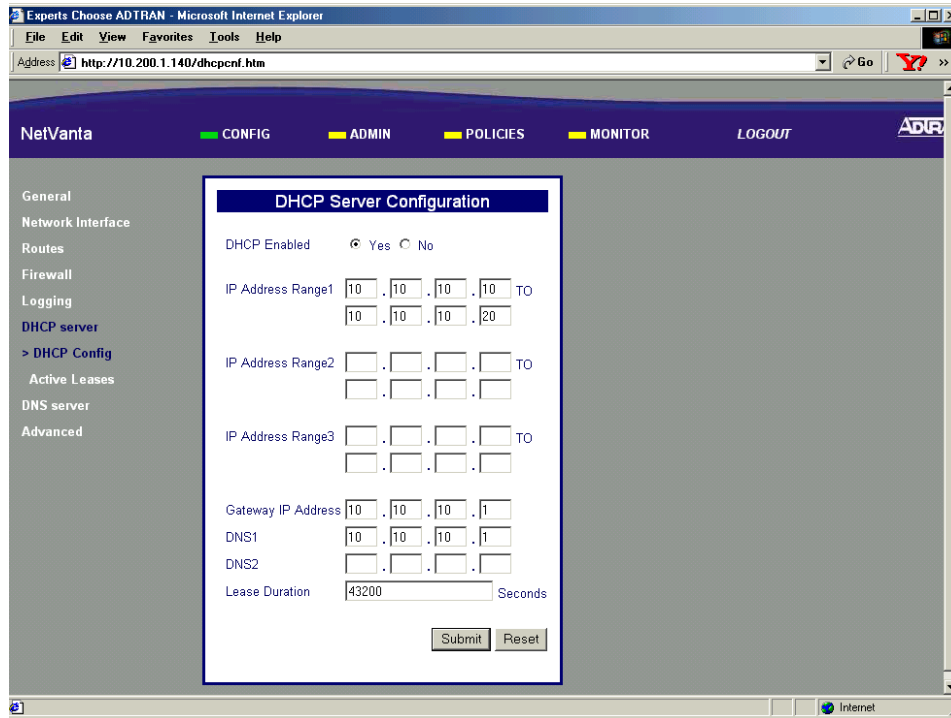


Perform Steps Below in the Order Listed

1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select CONFIG.

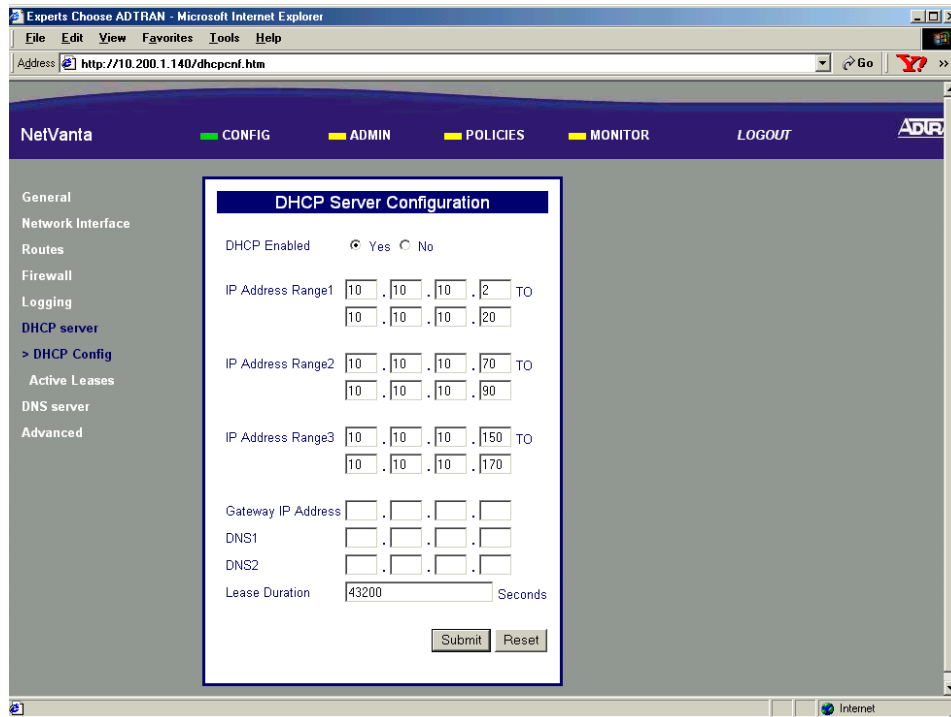


- From the menu list (located on the left side of the screen) select DHCP Server. The DHCP Server Configuration page will appear.



- Click the DHCP Enable Yes radio button to enable the DHCP server. The DHCP server is enabled by default.

5. Enter the selected range of IP addresses to be assigned by the NetVanta 2000 series DHCP server in the IP Address Range 1-3 fields. If only one range of IP addresses are desired, enter them in the IP Address Range 1 field. For our example we will enter three separate ranges.

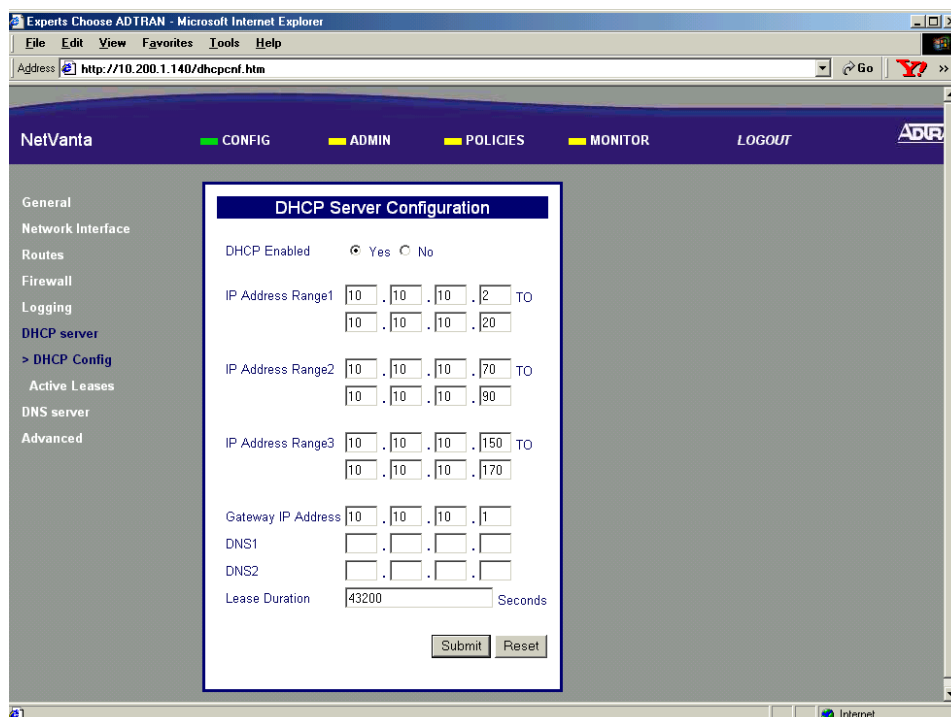


The screenshot shows the NetVanta web interface in Microsoft Internet Explorer. The browser address bar shows `http://10.200.1.140/dhpcnf.htm`. The page title is "NetVanta" and the navigation menu includes CONFIG, ADMIN, POLICIES, MONITOR, and LOGOUT. The left sidebar shows a tree view with "DHCP server" expanded to "DHCP Config". The main content area is titled "DHCP Server Configuration" and contains the following fields:

- DHCP Enabled: Yes No
- IP Address Range1: . . . TO . .
- IP Address Range2: . . . TO . .
- IP Address Range3: . . . TO . .
- Gateway IP Address: . . .
- DNS1: . . .
- DNS2: . . .
- Lease Duration: Seconds

Buttons for "Submit" and "Reset" are located at the bottom of the configuration area.

6. Enter the LAN IP address of the NetVanta 2000 series unit in the Gateway IP Address field. For our example we will enter 10.10.10.1.



This screenshot is identical to the previous one, but the "Gateway IP Address" field is now populated with the value "10.10.10.1".

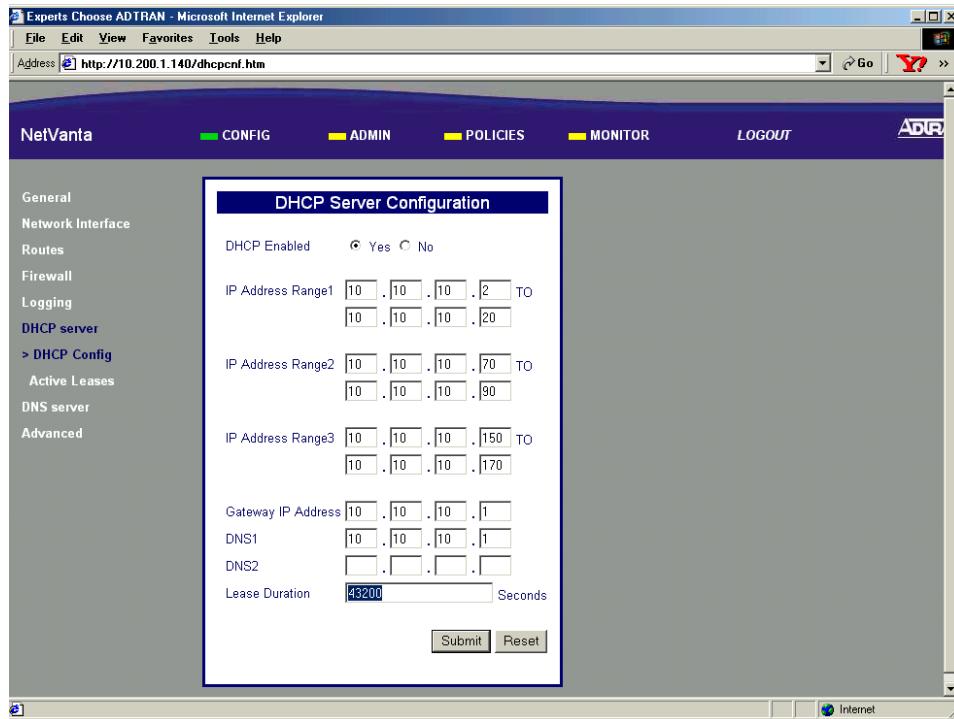
7. Enter the IP address for the primary DNS server you wish the NetVanta 2000 series to use in the DNS 1 field. For our example we will use the DNS capability of the NetVanta 2000 series so we will enter the LAN IP address (10.10.10.1) in the DNS 1 field. You may enter a secondary DNS server in the DNS 2 field.

The screenshot shows a web browser window titled "Experts Choose ADTRAN - Microsoft Internet Explorer" with the address bar displaying "http://10.200.1.140/dhccnf.htm". The page content is a configuration interface for a DHCP server. The top navigation bar includes "NetVanta" and buttons for "CONFIG", "ADMIN", "POLICIES", "MONITOR", and "LOGOUT". A left sidebar lists menu items: "General", "Network Interface", "Routes", "Firewall", "Logging", "DHCP server", "> DHCP Config", "Active Leases", "DNS server", and "Advanced". The main content area is titled "DHCP Server Configuration" and contains the following fields:

- DHCP Enabled: Yes No
- IP Address Range1: 10 . 10 . 10 . 2 TO 10 . 10 . 10 . 20
- IP Address Range2: 10 . 10 . 10 . 70 TO 10 . 10 . 10 . 90
- IP Address Range3: 10 . 10 . 10 . 150 TO 10 . 10 . 10 . 170
- Gateway IP Address: 10 . 10 . 10 . 1
- DNS1: 10 . 10 . 10 . 1
- DNS2:
- Lease Duration: 43200 Seconds

At the bottom of the configuration area are "Submit" and "Reset" buttons.

8. Enter the number of seconds you want the NetVanta 2000 series to use for the active lease timer in the Lease Duration field. We will use the default 43,200 seconds for this example.



9. Click the submit button to make the changes take effect. The page will blink and return you to the DHCP Server Configuration page.
10. Follow the procedures in [DLP-003](#) to save the settings to non-volatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

DEFINING A USER GROUP IN THE NETVANTA

Introduction

The NetVanta 2000 series has the flexibility to allow policies to be implemented on a per-user basis. With the User Group component tables you are able to create groups and assign users that share the same access policies. The User Group feature allows each policy to be implemented dynamically as the user logs on and off the system. This DLP discusses the procedure for creating a user group in the NetVanta 2000 series.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

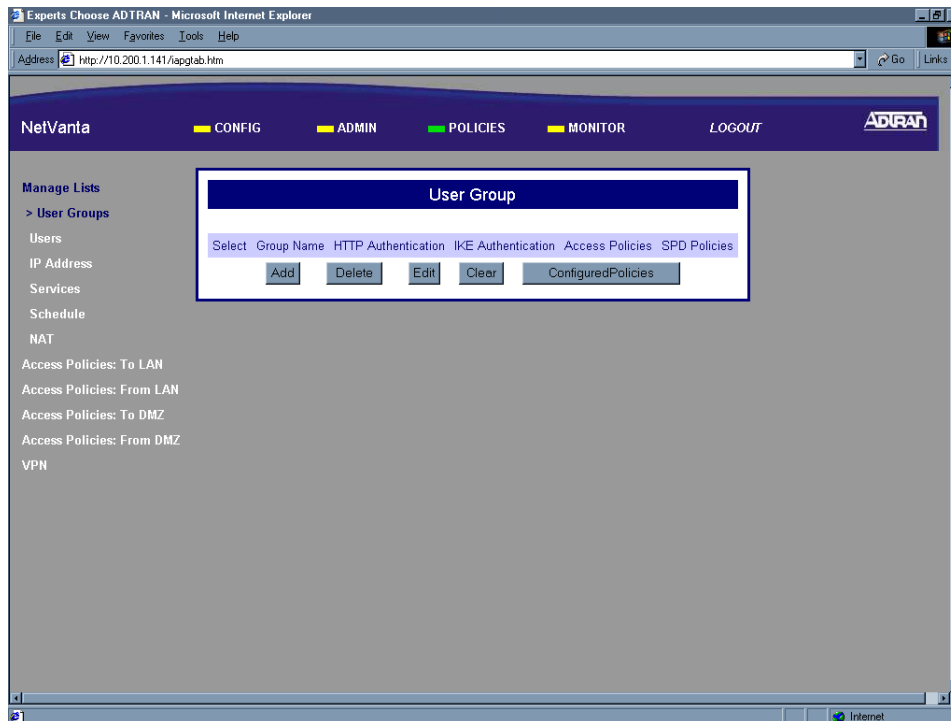
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

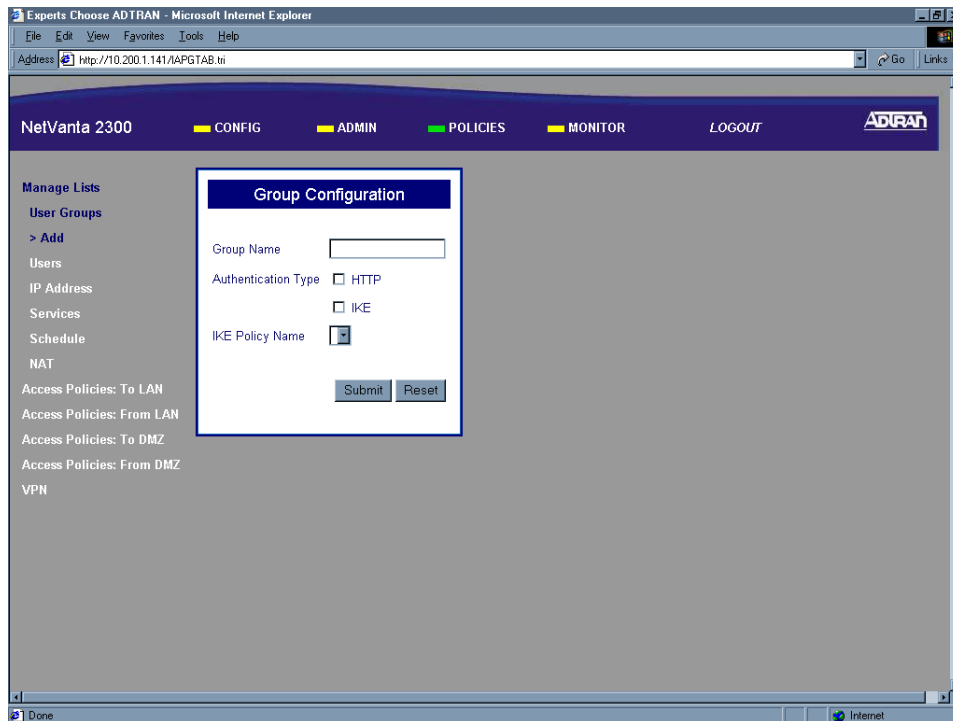
DLP-013

Perform Steps Below in the Order Listed

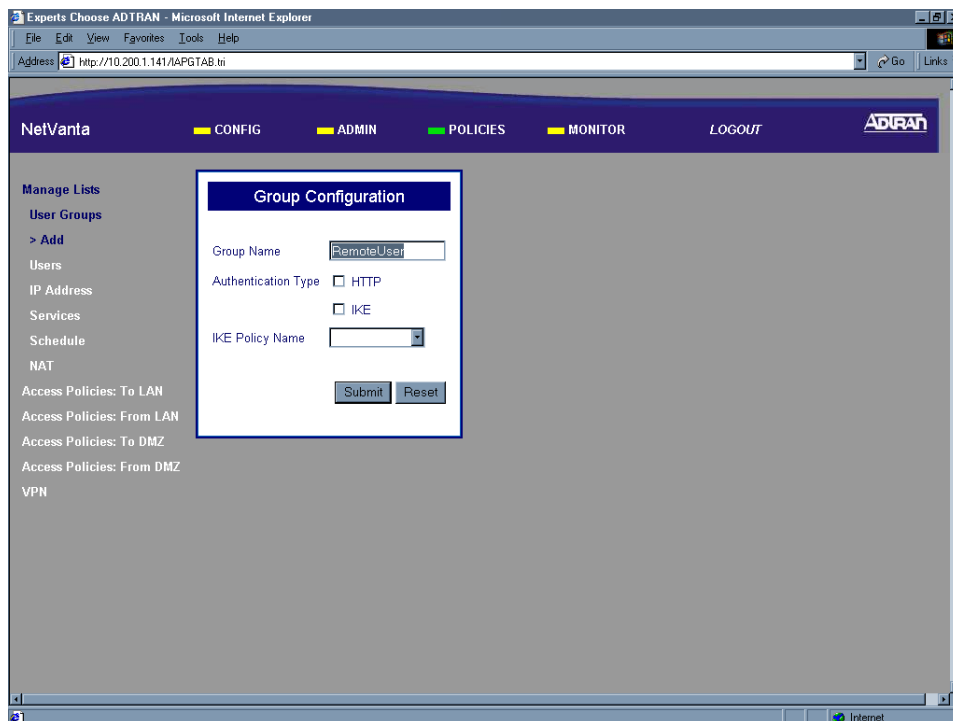
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **POLICIES**. The **MANAGE LISTS** menu and **USER GROUP** submenu are automatically displayed.



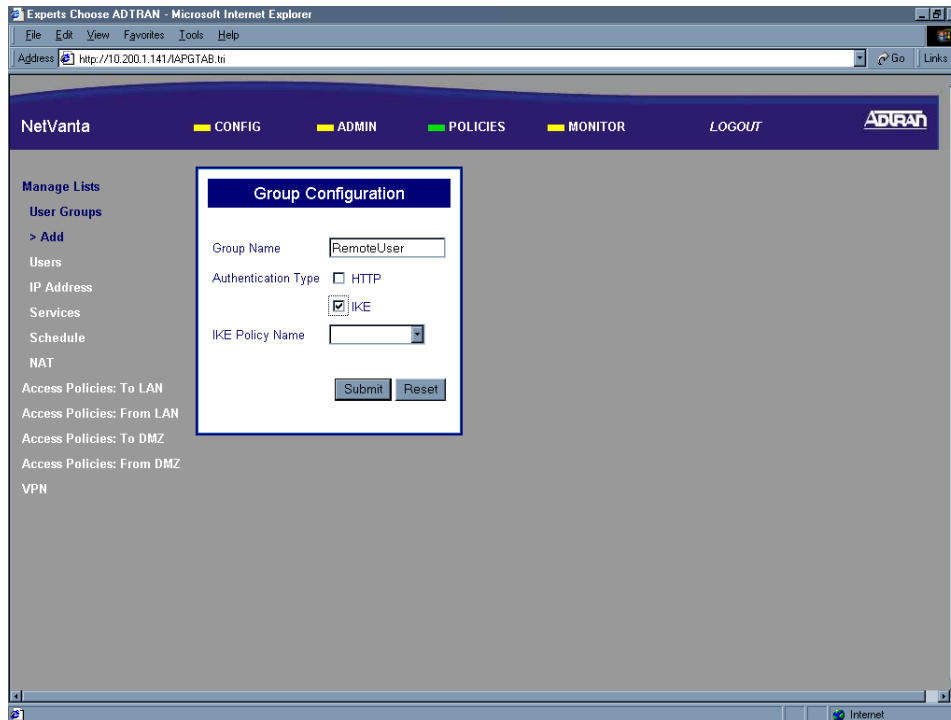
- Click the Add button in the User Group dialog box. The **GROUP CONFIGURATION** page will appear.



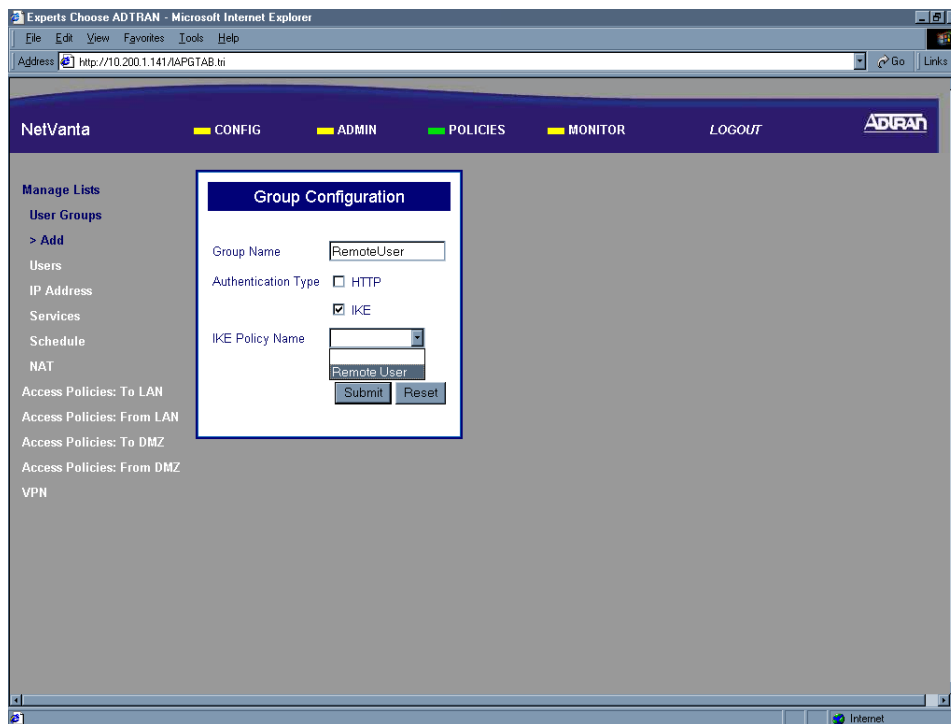
- Enter a descriptive name for the group in the Group Name field. This is a character field for up to 16 characters, and spaces are not allowed.



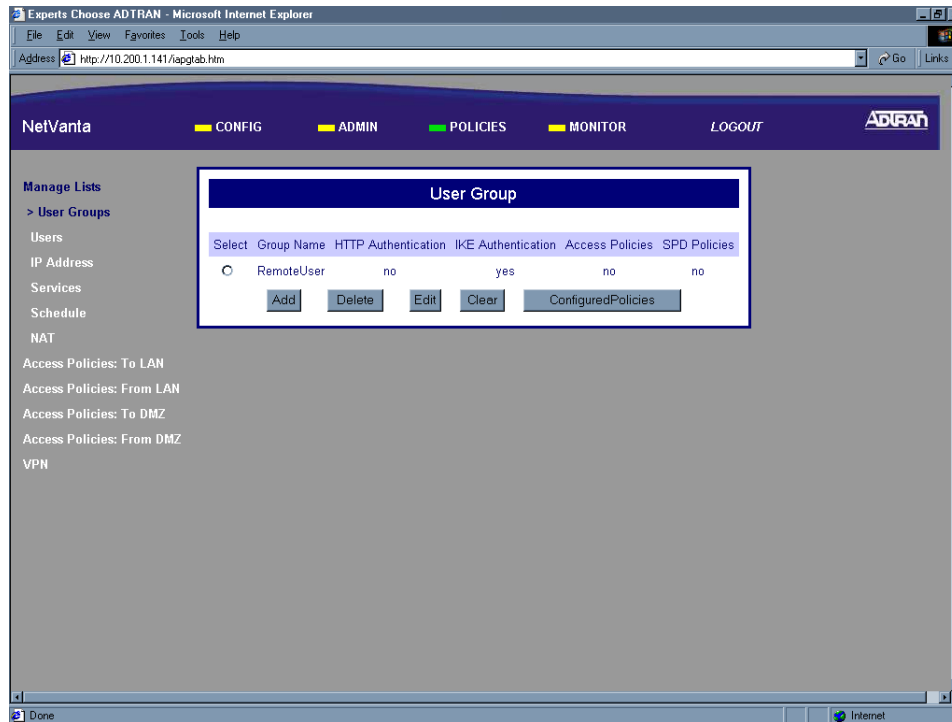
5. Select the appropriate authentication type (HTTP or IKE) checkbox. This field may be left blank if no authentication is necessary.



6. If IKE was selected as the authentication method in Step 5, select the appropriate IKE policy from the IKE Policy Name drop down menu.



- Click the Submit button to add the configured group to the User Group component table. If the group is successfully added the User Group page will appear and the added group will be listed.



- Follow the procedures in DLP-003 to save the settings to non-volatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

ADDING A USER TO THE USERS COMPONENT TABLE

Introduction

The NetVanta 2000 series has the flexibility to allow policies to be implemented on a per-user basis. With the User Group component tables you are able to create groups and assign users that share the same access policies. The User Group feature allows each policy to be implemented dynamically as the user logs on and off the system. This DLP discusses the procedure for adding a user to a user group in the NetVanta 2000 series.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

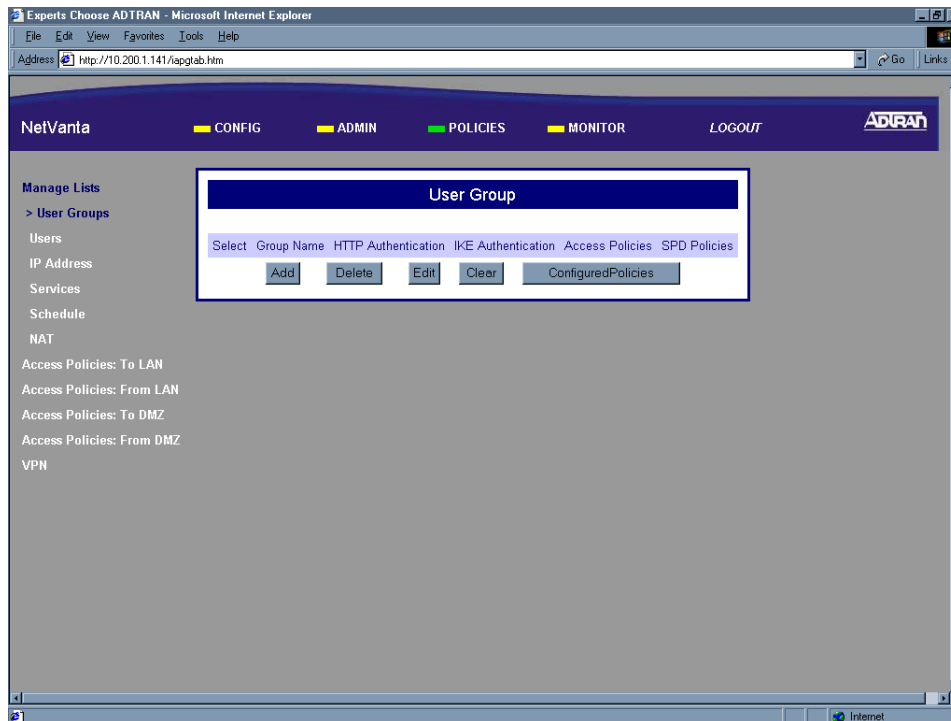
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

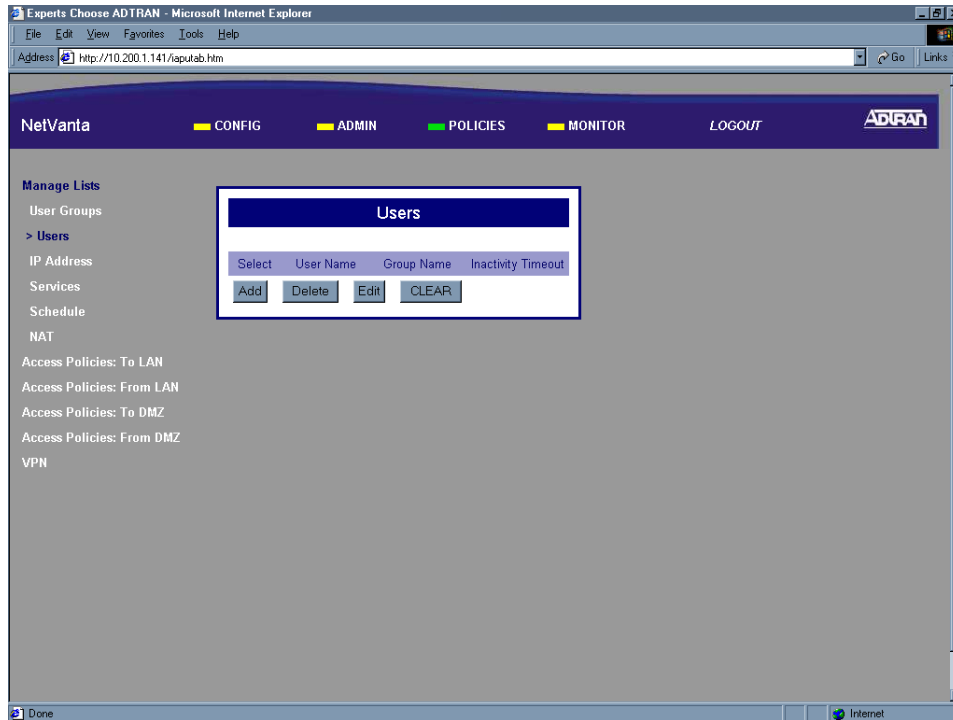
DLP-014

Perform Steps Below in the Order Listed

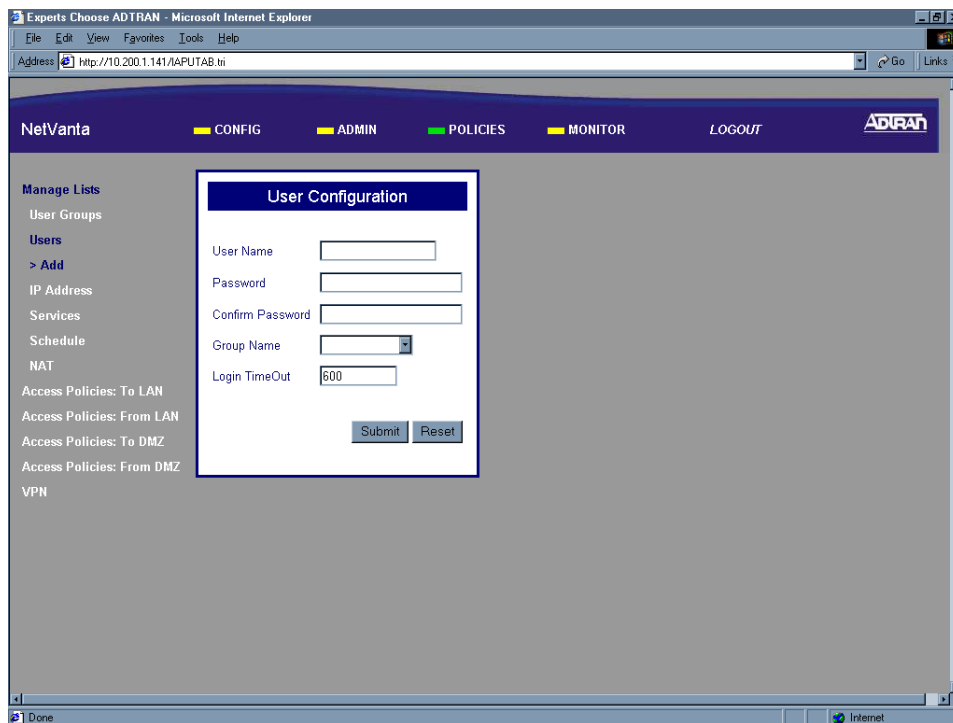
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **POLICIES**. The **MANAGE LISTS** menu and **USER GROUP** submenu are automatically displayed.



- From the menu list (located on the left side of the screen) select **USERS** (listed as a **MANAGE LISTS** submenu).



- Click the Add button in the Users dialog box. The User Configuration page will appear.



5. Enter a descriptive name for the User in the User Name field. This is a character field and spaces are not allowed.

The screenshot shows the NetVanta web interface in Microsoft Internet Explorer. The address bar displays `http://10.200.1.141/NAPUTAB.tn`. The page header includes the NetVanta logo and navigation tabs for CONFIG, ADMIN, POLICIES, and MONITOR, along with a LOGOUT link. On the left, a 'Manage Lists' sidebar contains links for User Groups, Users, Add, IP Address, Services, Schedule, NAT, and various Access Policies. The main content area is titled 'User Configuration' and contains the following fields:

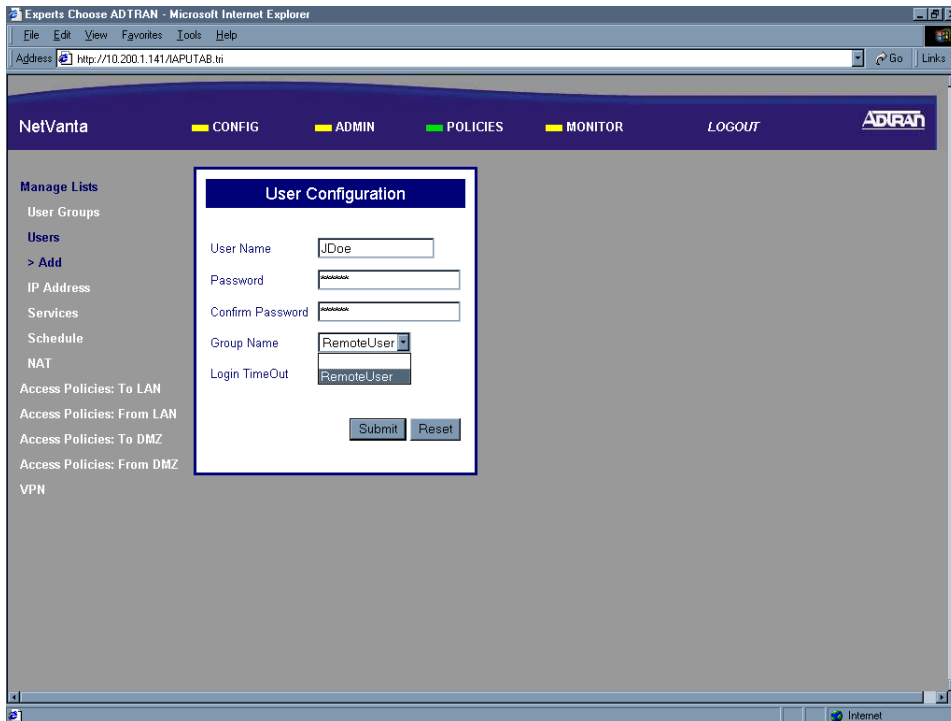
- User Name:
- Password:
- Confirm Password:
- Group Name:
- Login TimeOut:

At the bottom of the form are 'Submit' and 'Reset' buttons.

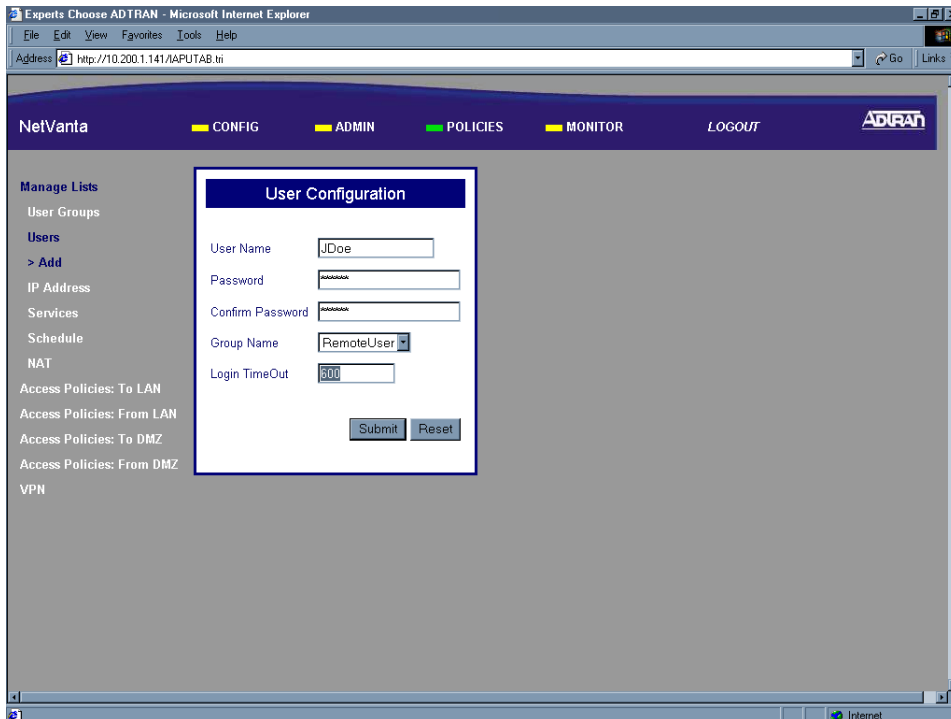
6. Enter the assigned password in both the Password and Confirm Password fields. This will be the user's log on password to activate the associated policies.

This screenshot is identical to the previous one, but the Password and Confirm Password fields now contain masked characters (asterisks), indicating that a password has been entered. The rest of the interface, including the navigation menu and the User Name field containing 'JDoe', remains the same.

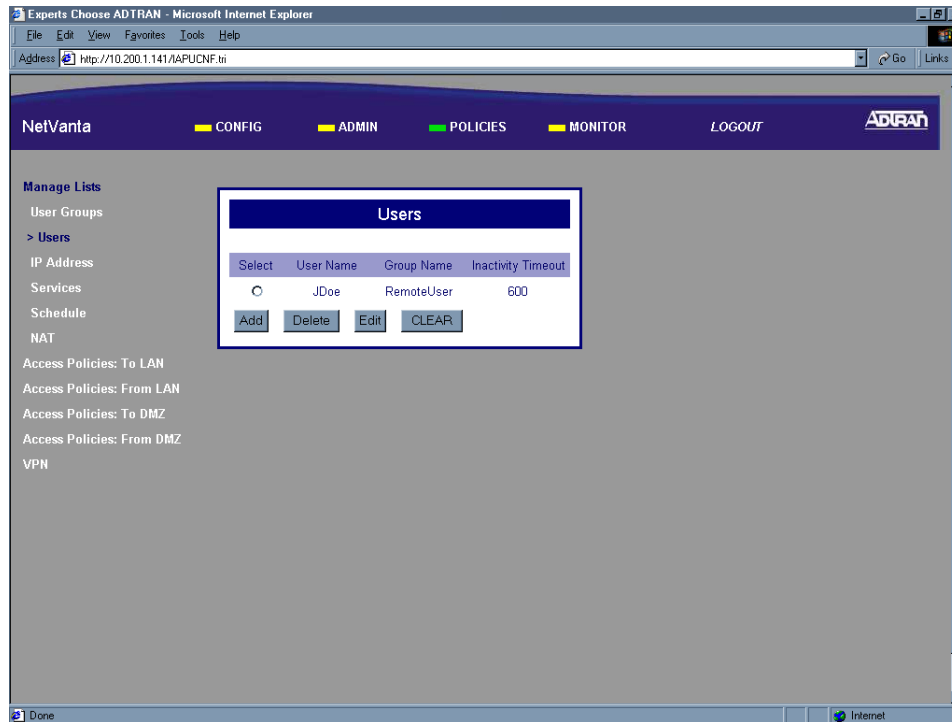
7. Select the group you want to assign this user to in the Group Name drop down menu.



8. Enter the login timeout you want to assign to this user in the Login Timeout field.



9. Click the Submit button to add the configured user to the Users component table. If the user is successfully added the Users page will appear and the added user will be listed.



10. Follow the procedures in [DLP-003](#) to save the settings to non-volatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

USING THE IP ADDRESS COMPONENT TABLE

Introduction

When configuring the NetVanta 2000 series, IP addresses are used repeatedly in many different components of the setup. To make the configuration process easier, the NetVanta 2000 series is equipped with an IP Address Component Table. The IP Address Component Table stores entered IP addresses for use throughout the configuration. This DLP discusses adding an IP address to this table.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

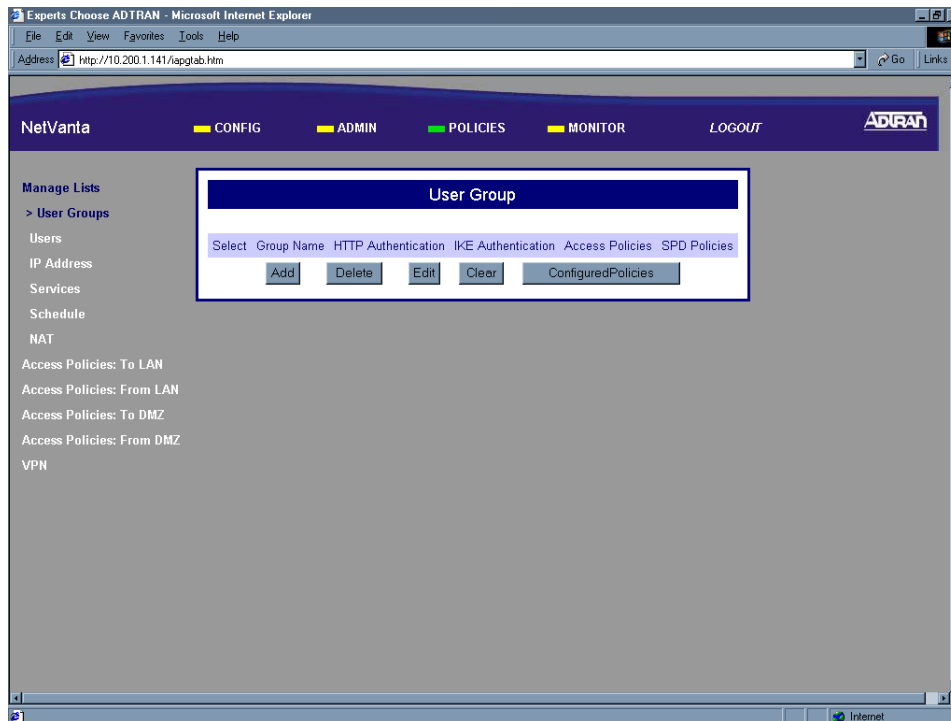
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

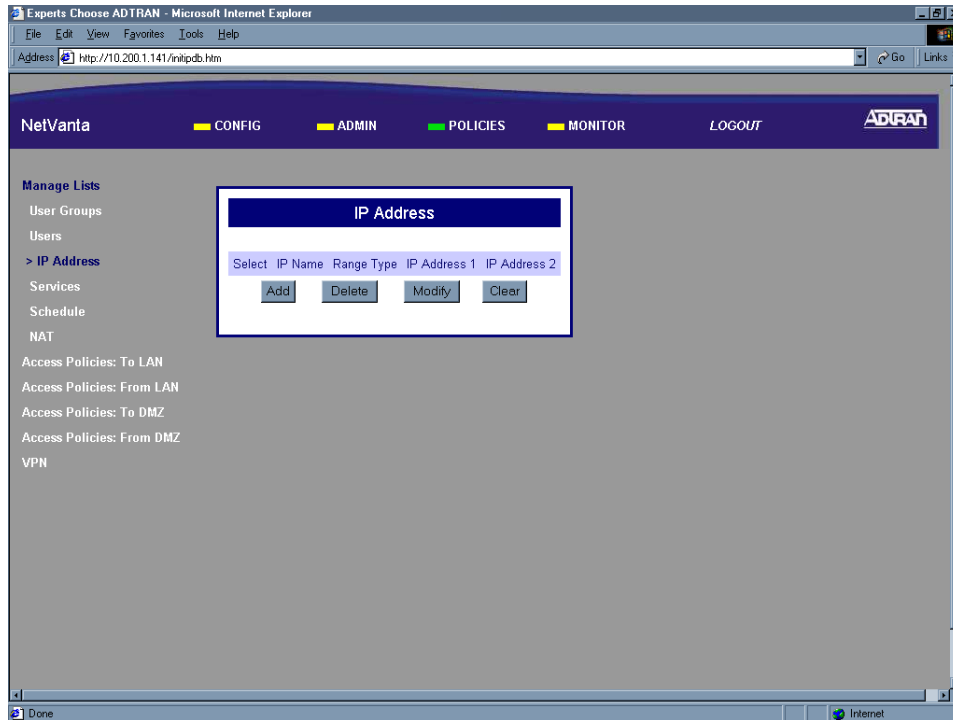
DLP-015

Perform Steps Below in the Order Listed

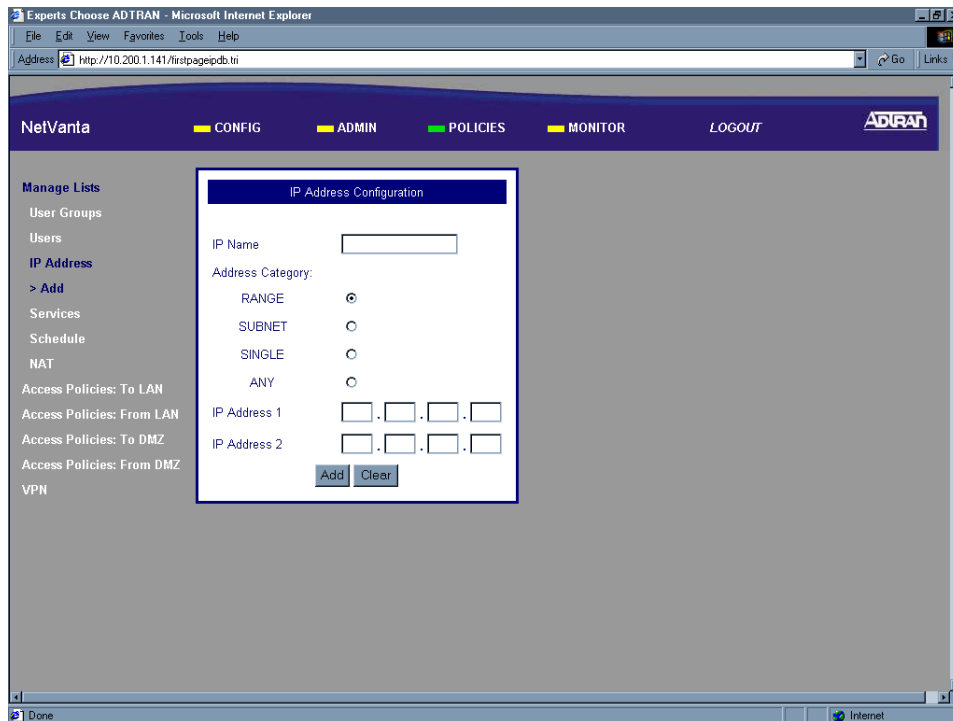
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **POLICIES**. The **MANAGE LISTS** menu and **USER GROUP** submenu are automatically displayed.



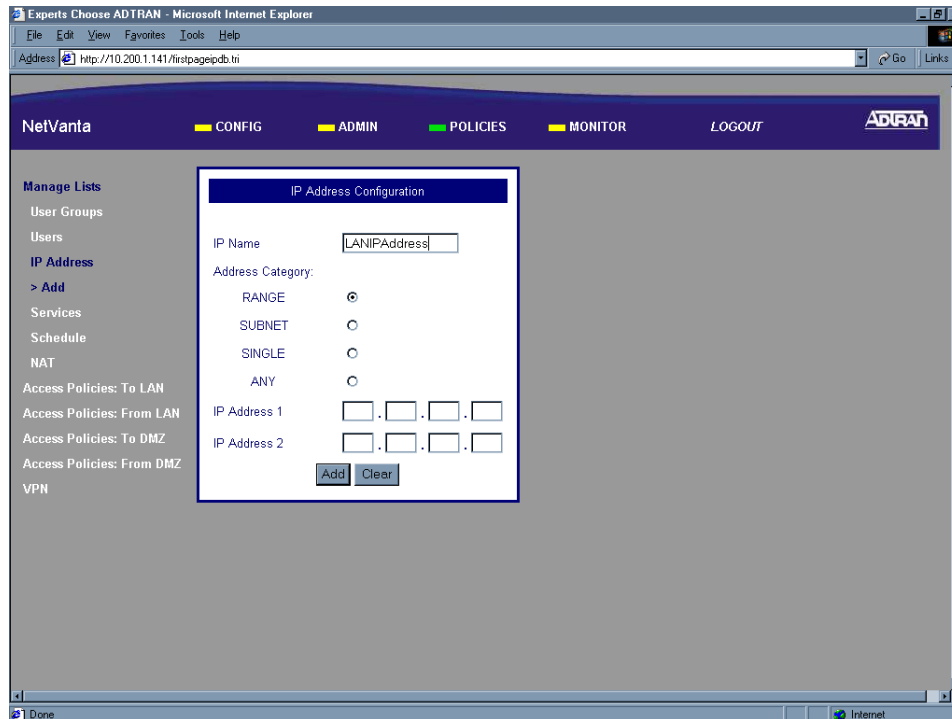
- From the menu list (located on the left side of the screen) select **IP ADDRESS** (listed as a **MANAGE LISTS** submenu).



- Click the Add button in the IP Address dialog box. The IP Address Configuration page will appear.



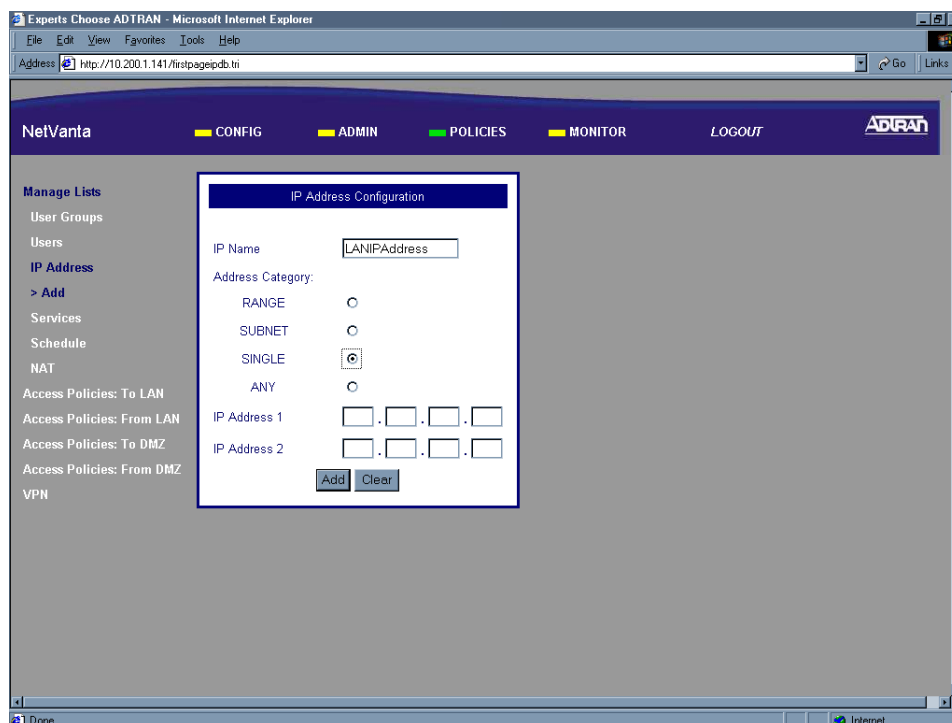
5. Enter a descriptive name for the IP address in the IP Name field. This is a character field and spaces are not allowed.



The screenshot shows the NetVanta web interface in Microsoft Internet Explorer. The browser's address bar displays `http://10.200.1.141/firstpageipdb:tri`. The page header includes the NetVanta logo and navigation tabs for CONFIG, ADMIN, POLICIES, and MONITOR, along with a LOGOUT link. On the left, a 'Manage Lists' sidebar contains links for User Groups, Users, IP Address, Services, Schedule, NAT, and various Access Policies. The main content area is titled 'IP Address Configuration' and contains the following form elements:

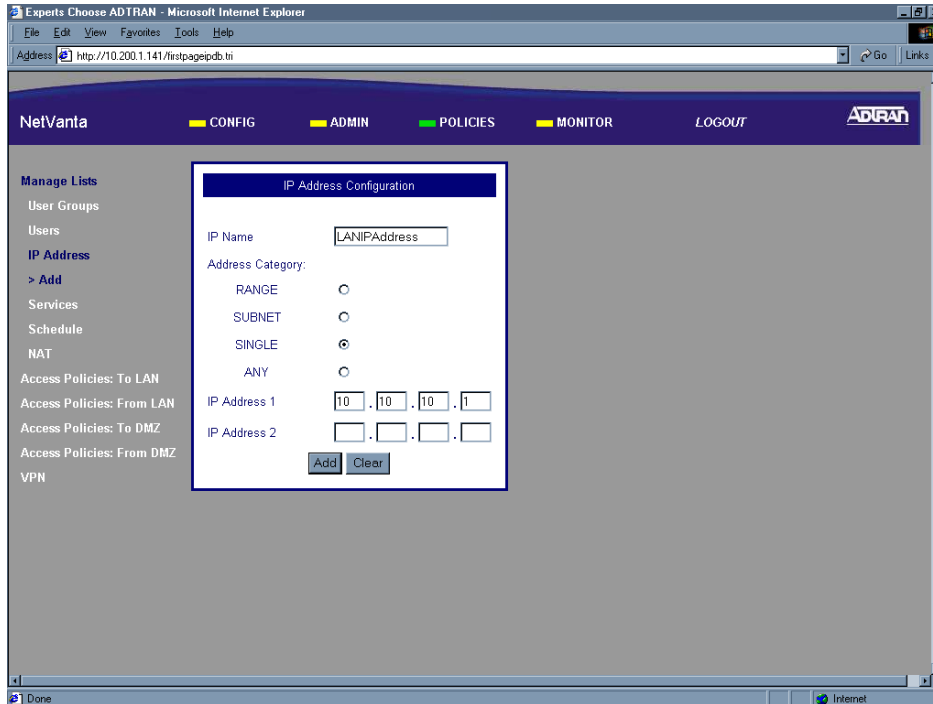
- IP Name:** A text input field containing the text 'LANIPAddress'.
- Address Category:** A group of four radio buttons: RANGE (selected), SUBNET, SINGLE, and ANY.
- IP Address 1:** A dotted IP address input field, currently empty.
- IP Address 2:** A dotted IP address input field, currently empty.
- Buttons:** 'Add' and 'Clear' buttons located at the bottom of the form.

6. Specify what type of IP address this record will hold. The IP Address Component Table can hold single IP addresses, a range of IP addresses, an entire subnet of addresses, or any address. Click the appropriate radio button.

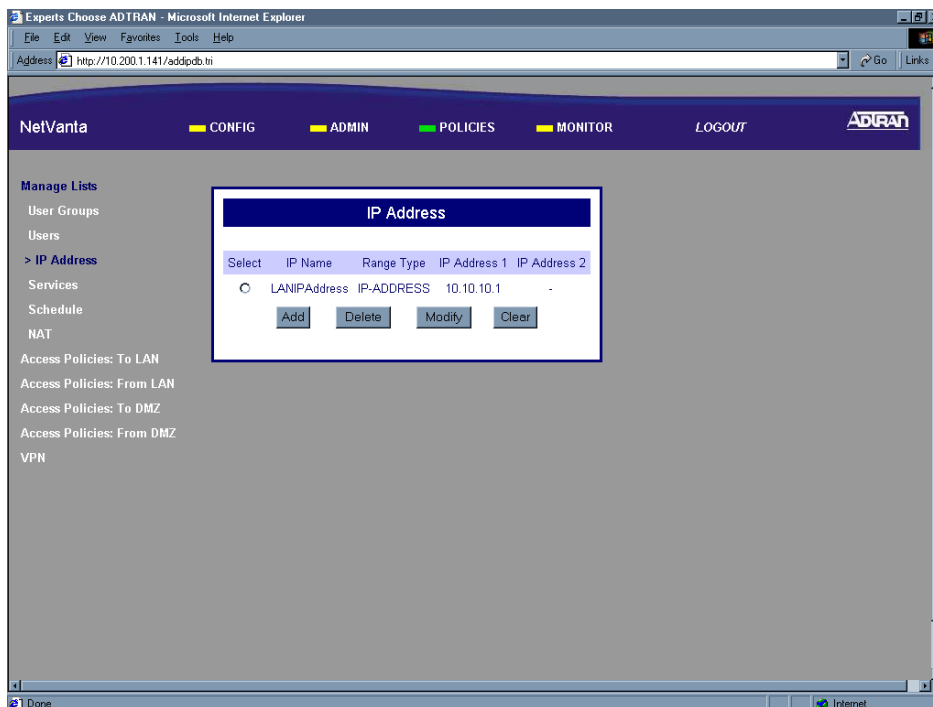


This screenshot is identical to the previous one, but with the 'SINGLE' radio button selected under the 'Address Category' section. The 'RANGE' radio button is now unselected.

7. Enter the IP address for this record in the **IP ADDRESS 1** and **2** fields located at the bottom of the IP Address Configuration dialog box. Enter a single IP address in the **IP ADDRESS 1** field. Enter a range using both fields. Enter a subnet of IP addresses by putting the network IP address in the **IP ADDRESS 1** field and the subnet mask for that network in the **IP ADDRESS 2** field.



8. Click the Submit button to add the configured IP address to the IP Address component table. If the IP address is successfully added the IP Address page will appear and the added address will be listed.



9. Follow the procedures in **DLP-003** to save the settings to non-volatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

ADDING A SERVICE TO THE SERVICES COMPONENT TABLE

Introduction

When configuring the NetVanta 2000 series, references to specific services (using port numbers) can be used over and over again in many different components of the setup. To make the configuration process easier, the NetVanta 2000 series is equipped with a Services Component Table. The Services Component Table stores entered services (using port numbers) for use throughout the configuration. This DLP discusses adding a service to this table.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

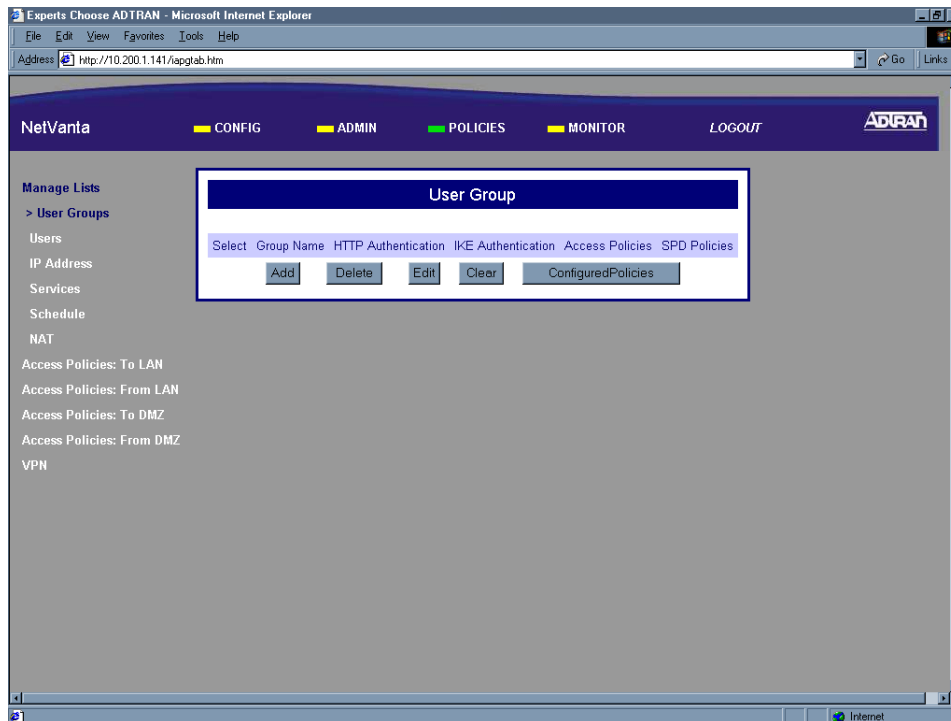
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

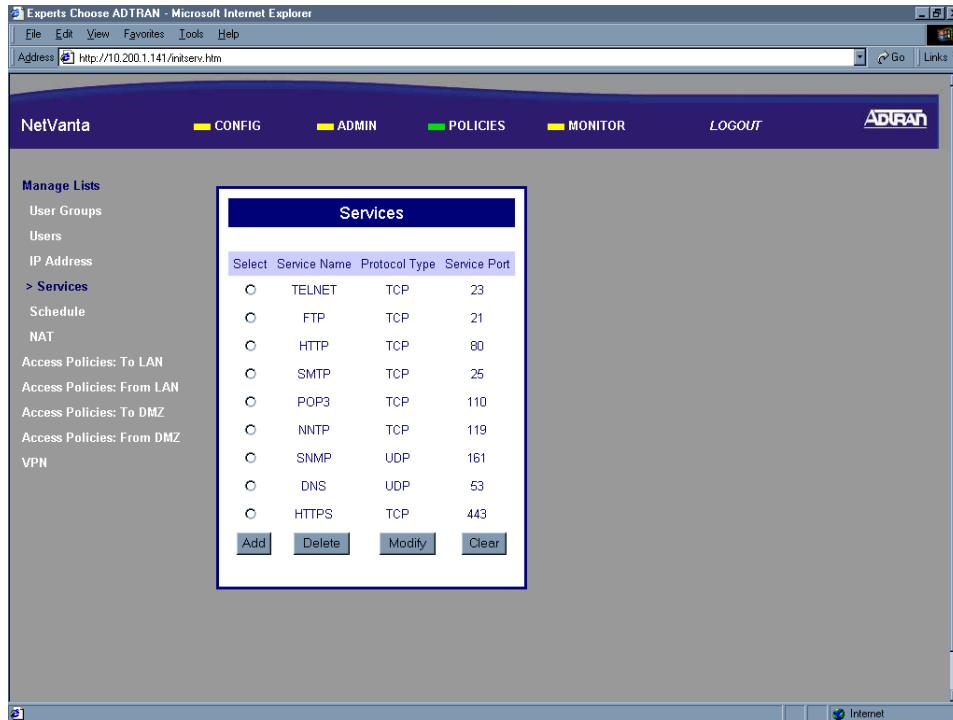
DLP-016

Perform Steps Below in the Order Listed

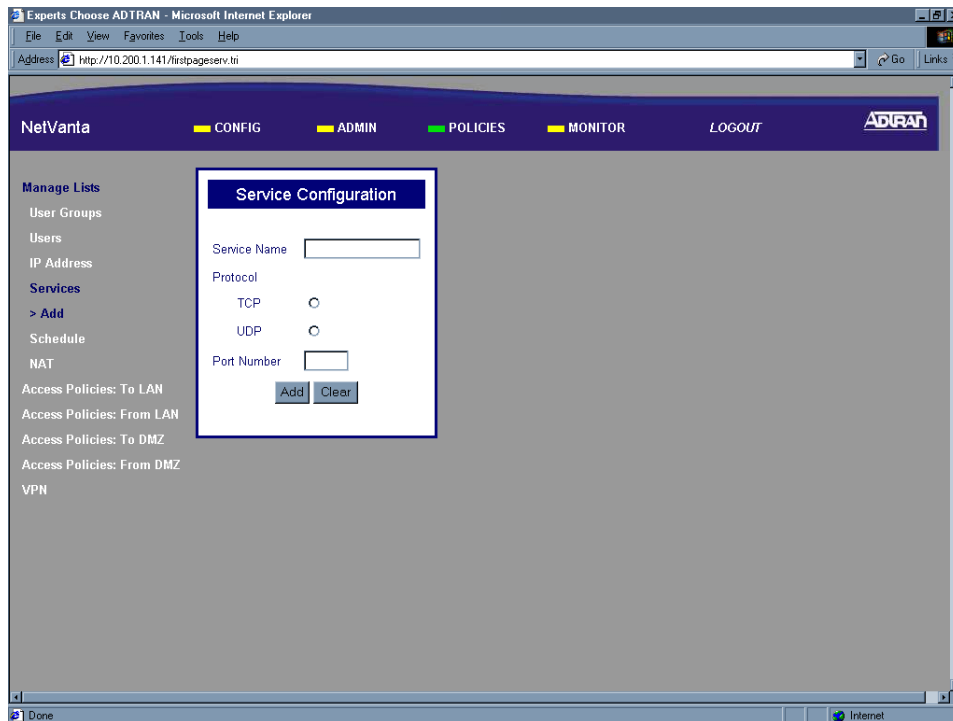
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **POLICIES**. The **MANAGE LISTS** menu and **USER GROUP** submenu are automatically displayed.



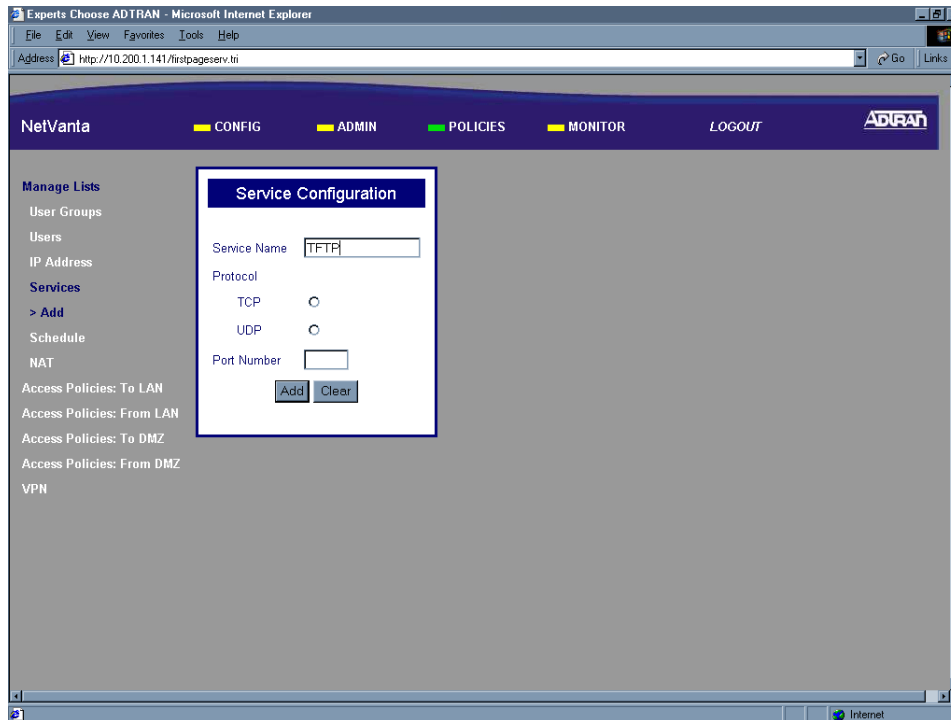
- From the menu list (located on the left side of the screen) select **SERVICES** (listed as a **MANAGE LISTS** submenu).



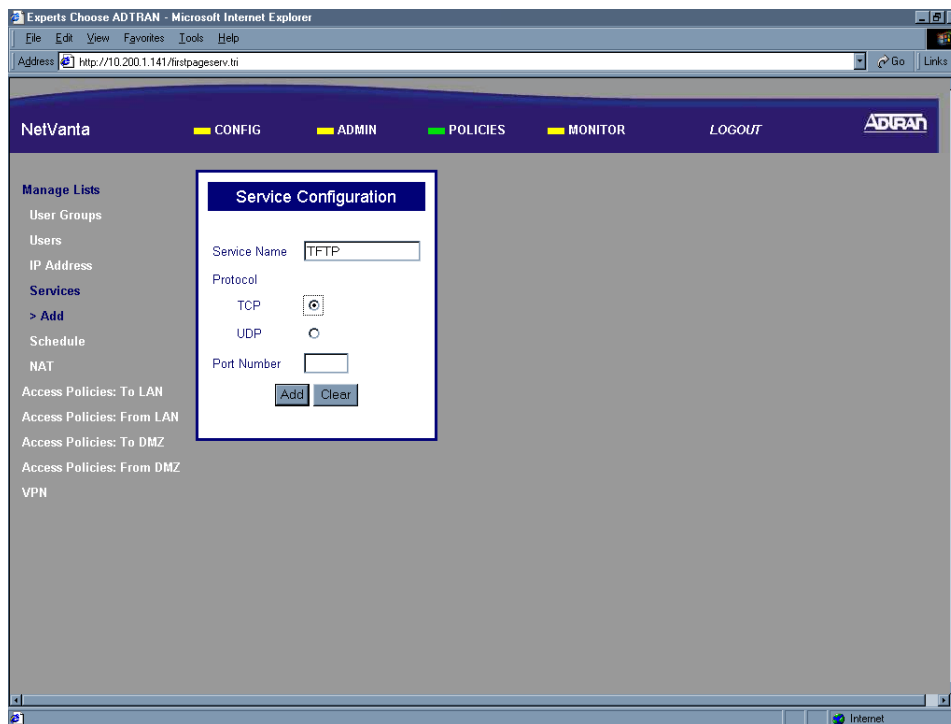
- Click the Add button in the Services dialog box. The Service Configuration page will appear.



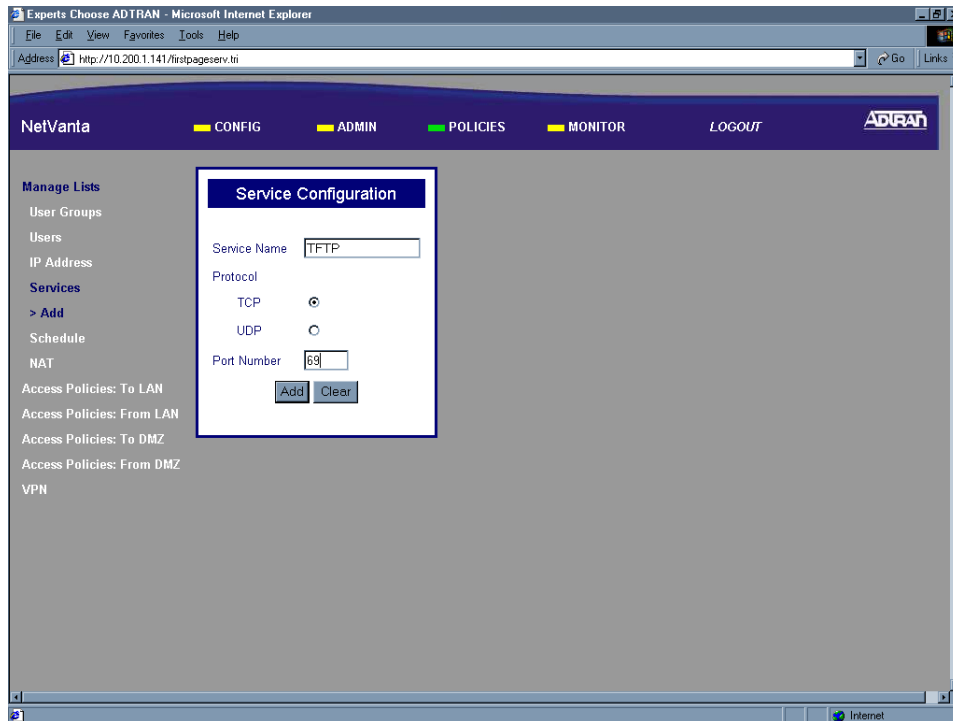
5. Enter a descriptive name for the IP address in the IP Name field. This is a character field and spaces are not allowed.



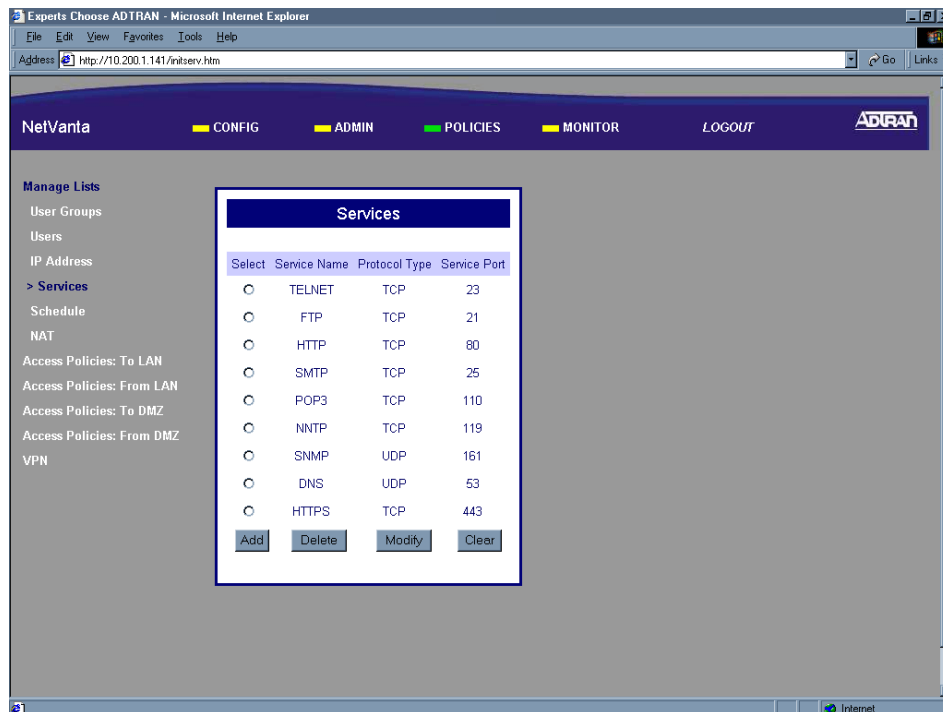
6. Specify whether this uses TCP or UDP protocol by selecting the appropriate radio button next to the protocol.



- Enter the port number associated with the service for this record in the Port Number field.



- Click the Submit button to add the configured service to the Services component table. If the service is successfully added the Services page will appear and the added service will be listed.



9. Follow the procedures in DLP-003 to save the settings to non-volatile memory.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

GENERATING A SELF-CERTIFICATE REQUEST

Introduction

The NetVanta 2000 series supports the use of both RSA and DSS Signature Algorithm Certificates. The NetVanta 2000 series provides the capability to generate self-certificate requests, and maintains a listing of private keys (certificate requests) that currently have no public key (self-certificate assigned by the Certificate Authority).

Always contact your Certificate Authority (VeriSign, Entrust, etc.) before generating your self-certificate request. The parameters configured in your request must match what the Certificate Authority requires for you to receive your self-certificate. Once the request is generated, follow your Certificate Authority's guidelines for supplying them with your request. Many Certificate Authorities allow e-mail requests, but some do not.

This DLP discusses the steps for generating a self-certificate request and submitting it to a SSH Communications Security test certificate website (isakmp-test.ssh.fi) to receive the corresponding self-certificate. DLP-018 discusses uploading your Certificate Authority's certificate into the NetVanta 2000 series and DLP-019 discusses uploading the received self-certificate.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

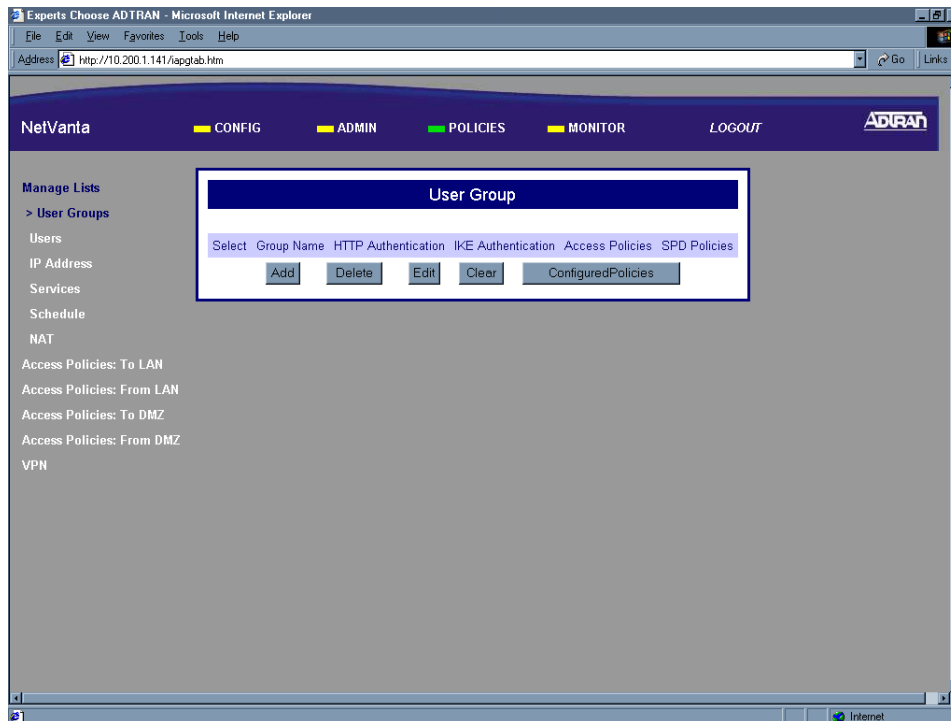
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

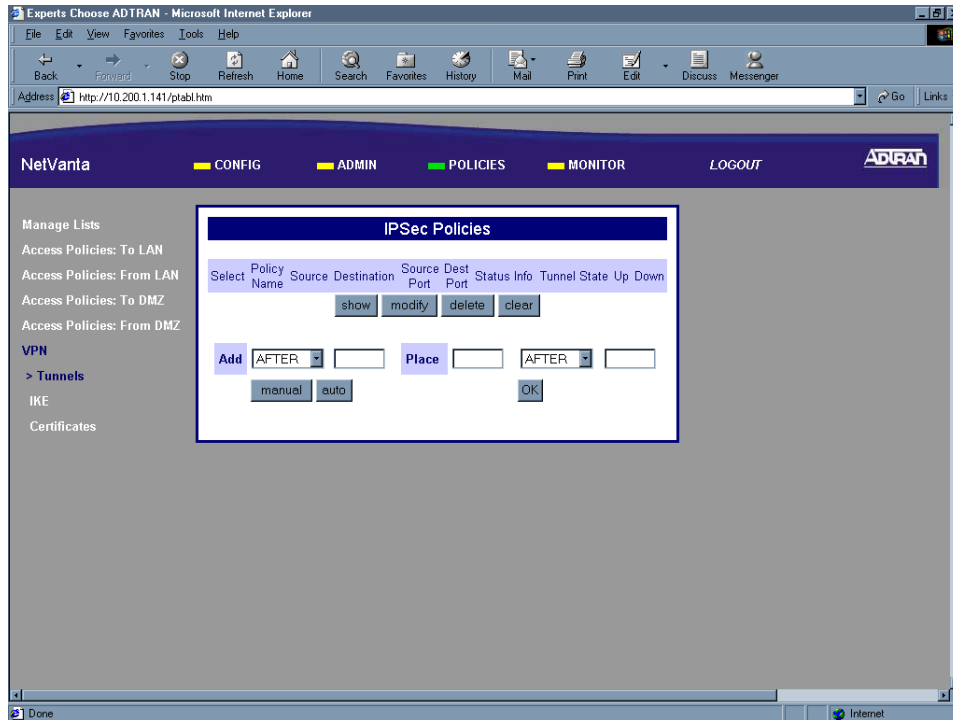
DLP-017

Perform Steps Below in the Order Listed

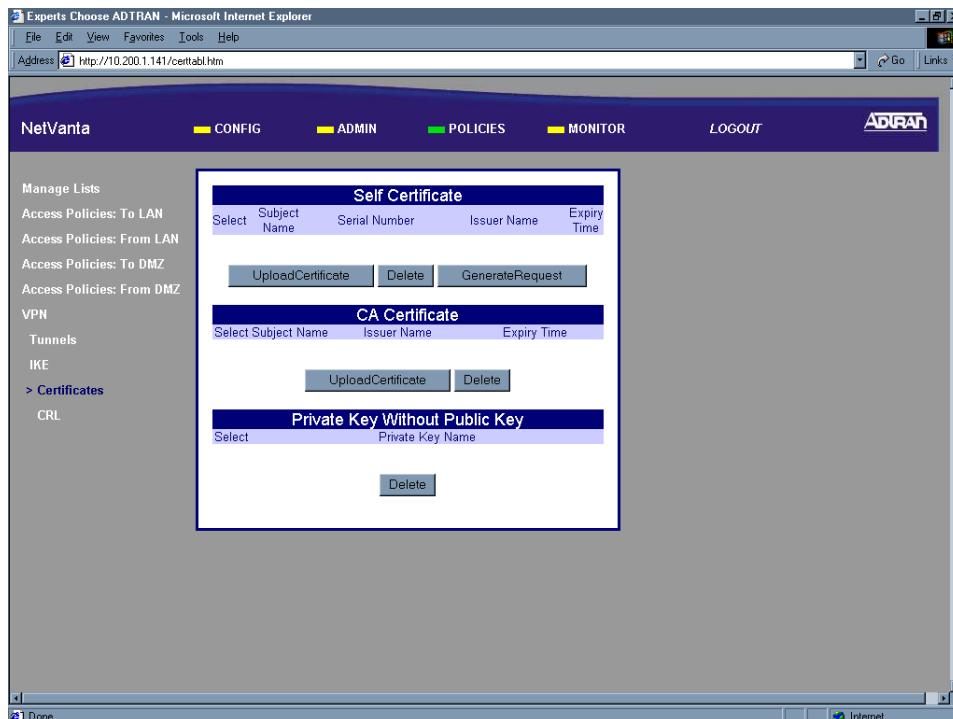
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **POLICIES**. The **MANAGE LISTS** menu and **USER GROUP** submenu are automatically displayed.



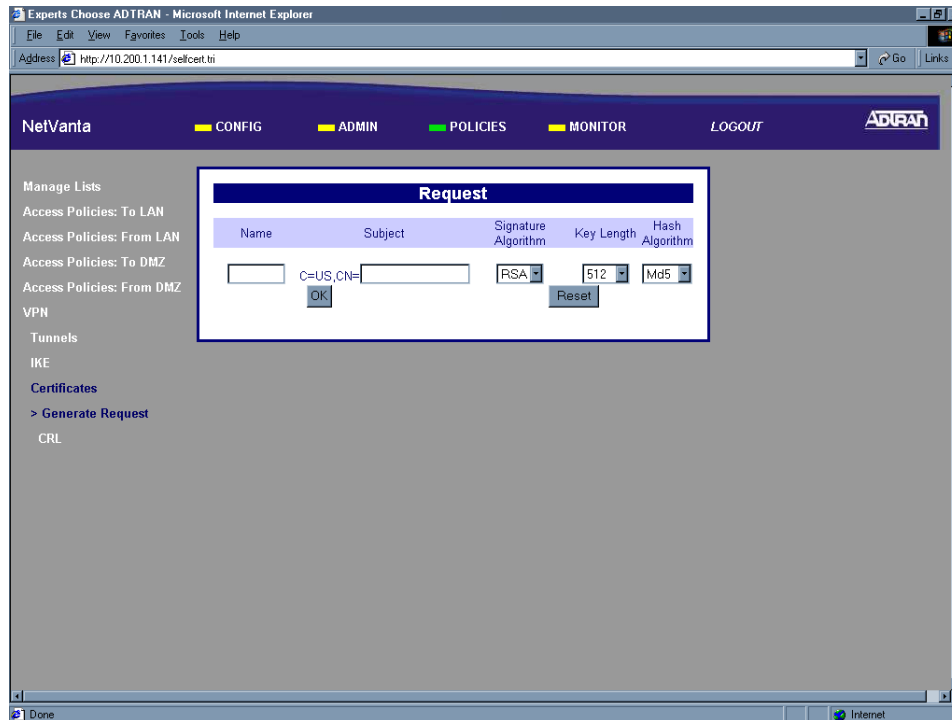
- From the menu list (located on the left side of the screen) select **VPN**. The IPsec Policies page will appear.



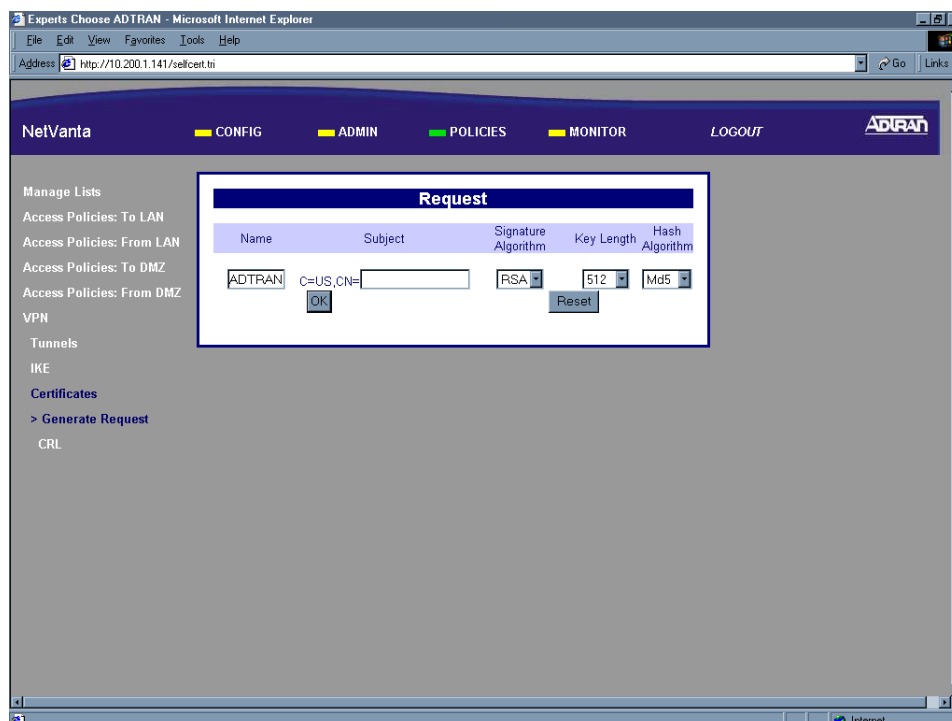
- From the menu list (located on the left side of the screen) select **CERTIFICATES** (listed as a VPN submenu).



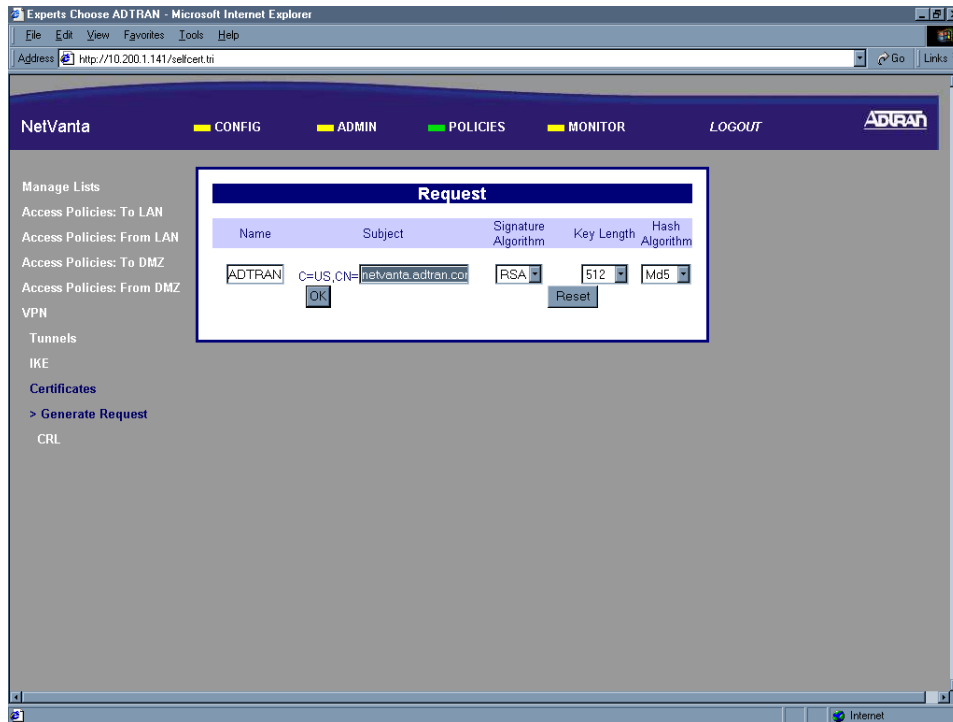
- In the Self-Certificate section of the page click the Generate Request button. The Request parameters box appears.



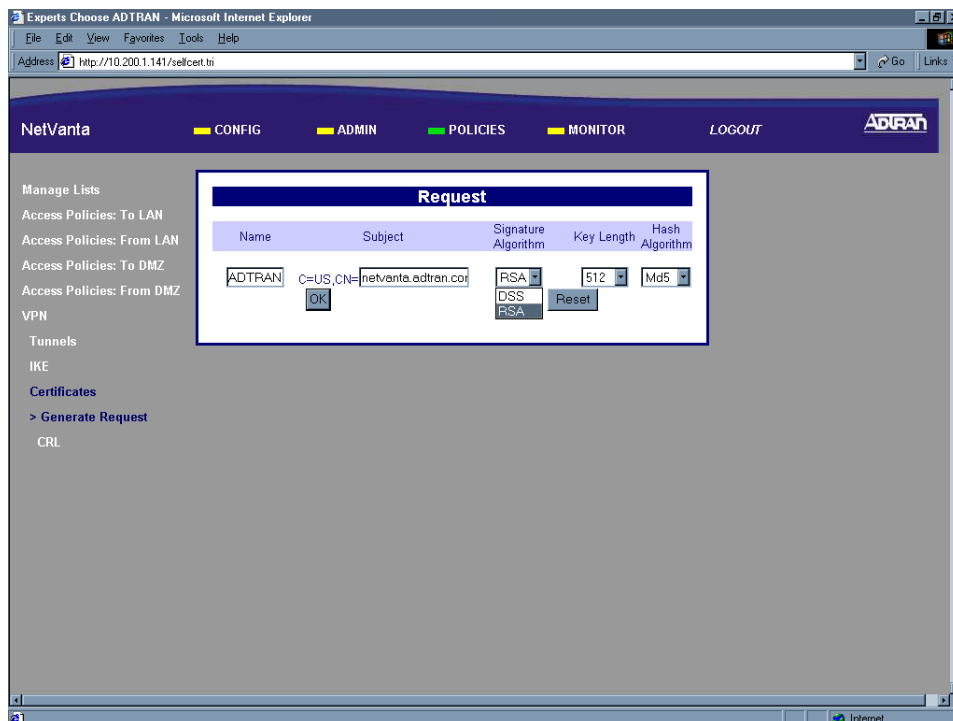
- Enter a text string (up to 7 characters with no spaces) in the Name field. This name is locally significant and should be used to identify different certificate requests generated in the same NetVanta 2000 series unit.



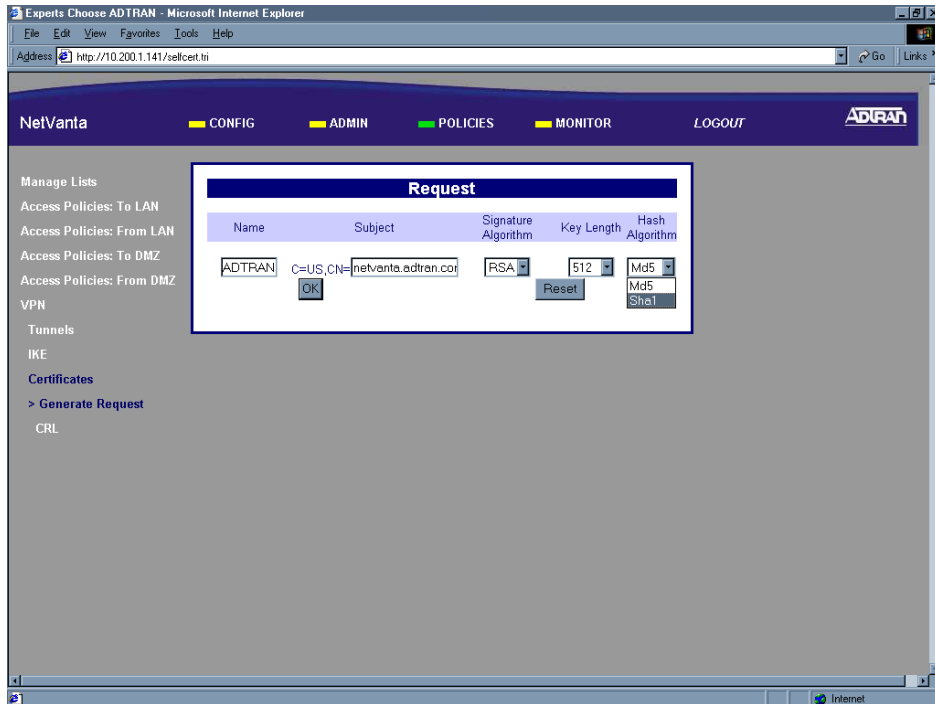
7. Enter a subject name to be used when generating the certificate request. For our example we will use the fully qualified domain name (FQDN) of the test NetVanta 2000 series unit.



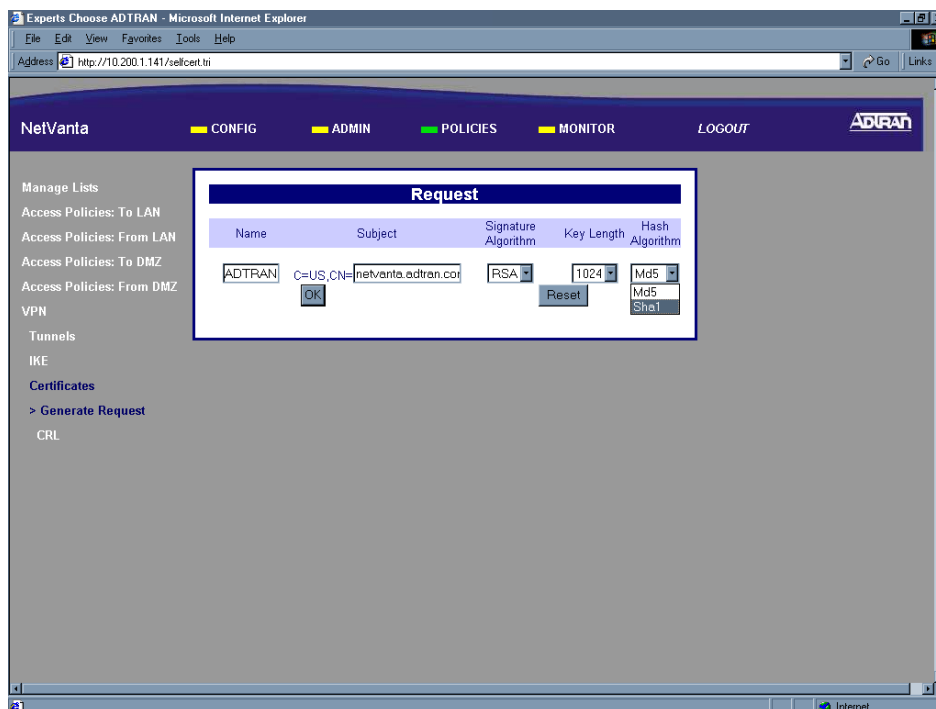
8. Select the desired algorithm for generating the certificate request from the Signature Algorithm drop down menu. The NetVanta 2000 series supports both DSS and RSA algorithms. When determining the algorithm to use, remember that RSA is more secure than DSS.



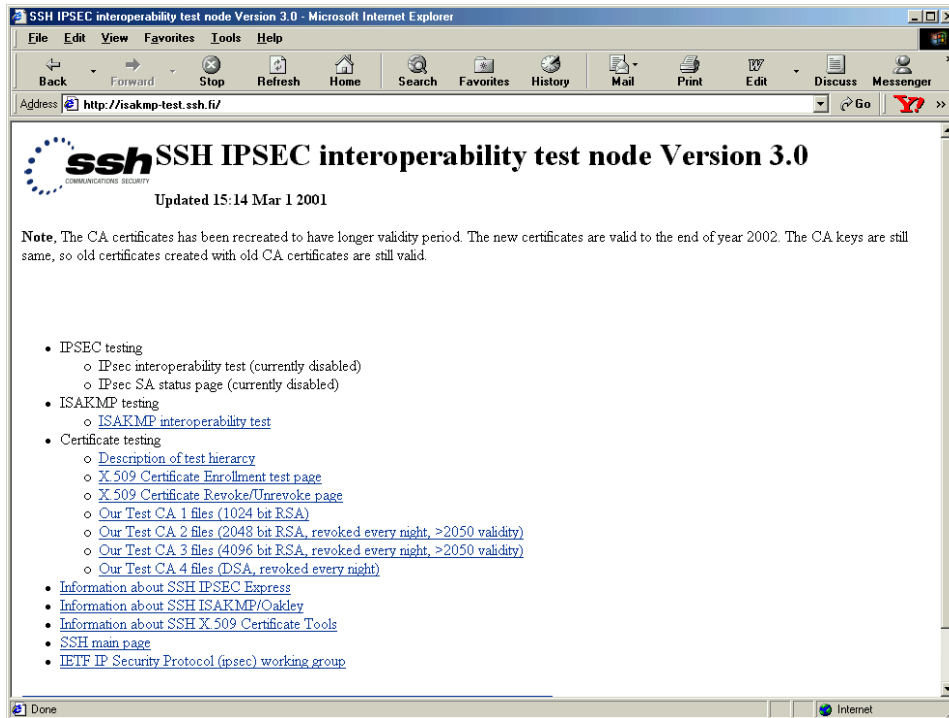
9. Select the key length used for the request from the drop down menu. The NetVanta 2000 series supports both 512 and 1024 key lengths. When determining the key length to use, remember that the bigger the key length the more security you have.



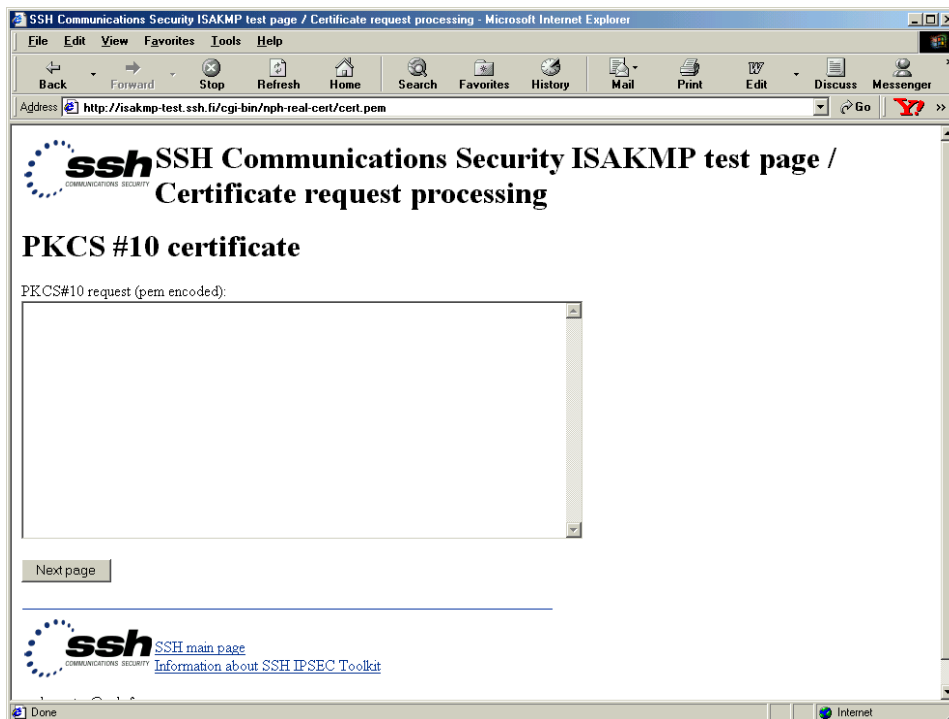
10. Select the hash algorithm used for the request from the drop down menu. The NetVanta 2000 series supports both MD5 and SHA1 hash algorithms. When determining the hash algorithm to use, remember that SHA1 is more secure.



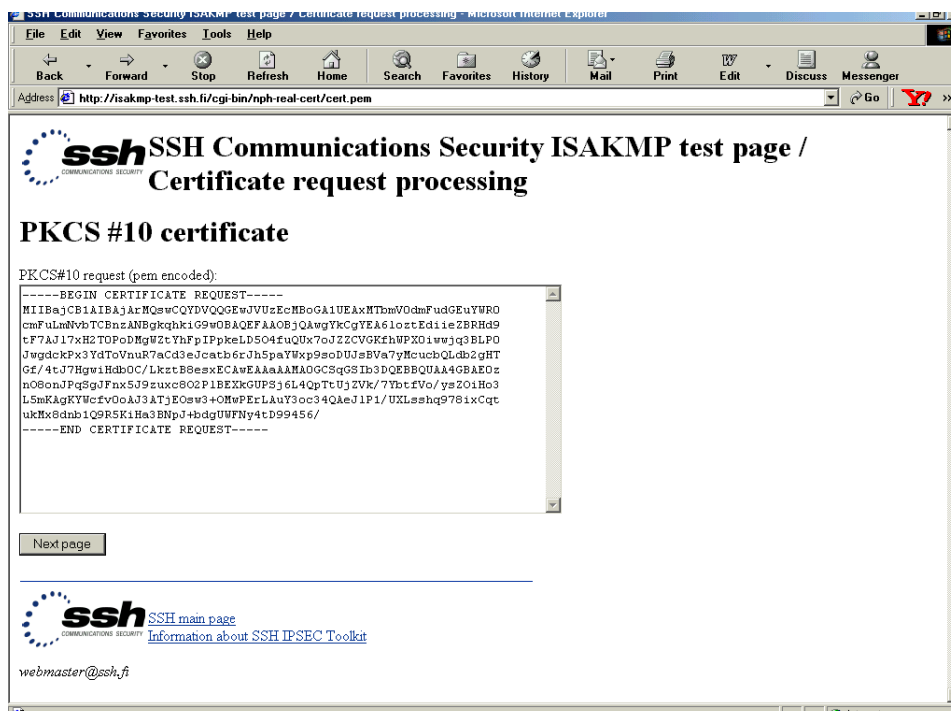
- Open a second browser session and enter `isakmp-test.ssh.fi` in the URL Address field. This will display the SSH Communications Security test certificate site.



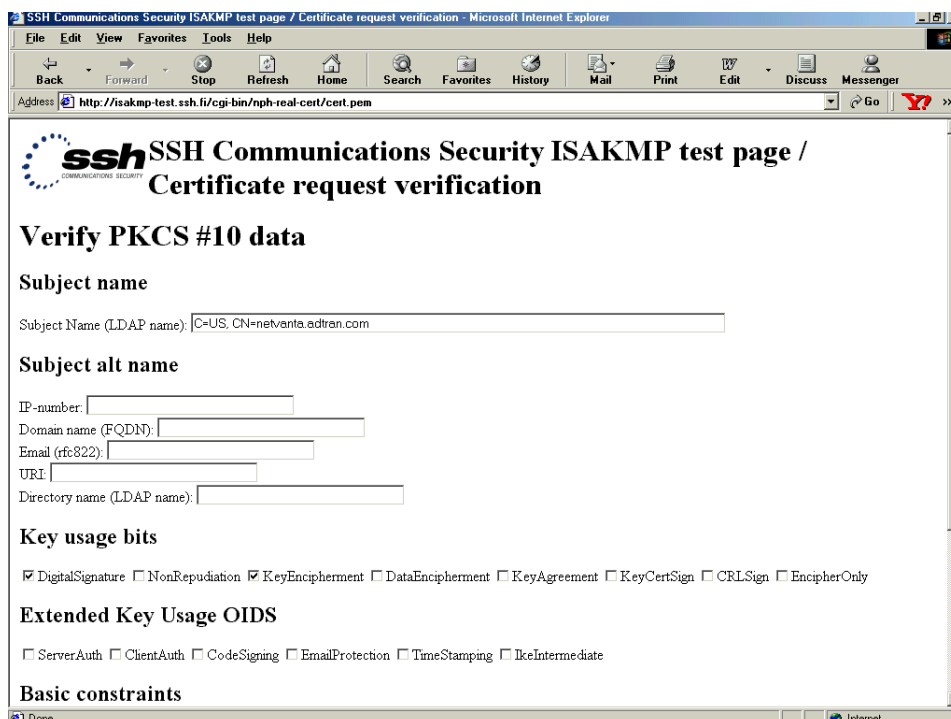
- Click on the X.509 Certificate Enrollment test page link to display the certificate request processing screen.



- Place your cursor in the text box on the screen and hit <Ctrl + V> to paste the copied certificate request into the text box.



- Click on the Next Page button to display the PKCS#10 Data Verification page. On this page you will need to verify the information used to generate your request. If you were working with a Certificate Authority, you would have already agreed on this data and submitted it to them before generating the request.



17. Enter the alternate subject data you wish the Certificate Authority to use when generating your certificate in the appropriate Subject Alt Name field. This information will be used again when configuring your IKE tunnel, so a review of these fields is appropriate. The NetVanta 2000 series supports four types of alternate subject data - IP address, Fully Qualified Domain Name (FQDN), User FQDN (listed as e-mail rfc 822 on the test site), and Der ANS1 DN (binary DER encoding of an ASN.1 X.500 Distinguished Name listed as LDAP on the test site). To use the IP address you must enter the WAN IP address of the NetVanta 2000 series that will contain this certificate. If the NetVanta 2000 series is configured for Dynamic or PPPoE addressing on the WAN interface, using the IP address is not valid. To use the FQDN you must enter the DNS name for the NetVanta 2000 series that will contain this certificate (example - netvanta.adtran.com). To use the User FQDN (rfc 822) enter your e-mail address (example - netvantasupport@adtran.com). To use the Der ANS1 DN (LDAP Name) enter the X.500 ASN1 name for the NetVanta 2000 series that will contain this certificate (example - 1.3.6.1.4.1.664.1.147.5.1 or iso.org.dod.internet.private.enterprises.adtran.adProducts.adTSUIQ.TechSupport.Unit1).

SSH Communications Security ISAKMP test page / Certificate request verification - Microsoft Internet Explorer

Address: http://isakmp-test.ssh.fi/cgi-bin/nph-real-cert/cert.pem

SSH Communications Security ISAKMP test page /
Certificate request verification

Verify PKCS #10 data

Subject name
 Subject Name (LDAP name): C=US, CN=netvanta.adtran.com

Subject alt name
 IP-number:
 Domain name (FQDN):
 Email (rfc822): john.doe@othercompany.com
 URI:
 Directory name (LDAP name):

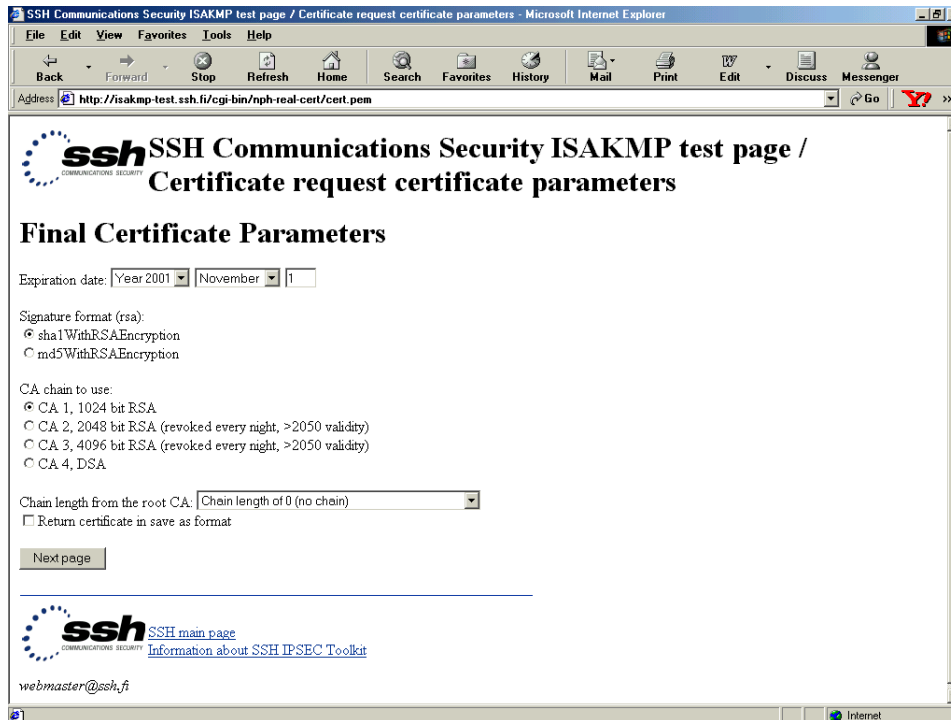
Key usage bits
 DigitalSignature NonRepudiation KeyEncipherment DataEncipherment KeyAgreement KeyCertSign CRLSign EncipherOnly

Extended Key Usage OIDs
 ServerAuth ClientAuth CodeSigning EmailProtection TimeStamping IkeIntermediate

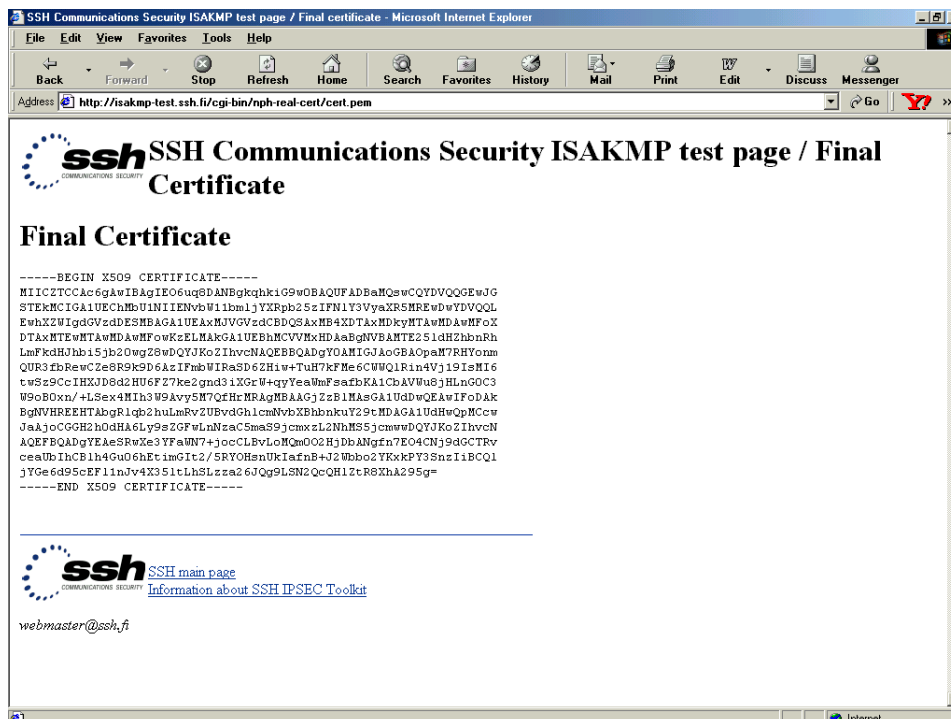
Basic constraints

The remaining parameters on the test site Verify PKCS #10 data page are beyond the scope of this DLP. These parameters would be established by your Certificate Authority and have no bearing on the NetVanta 2000 series functionality.

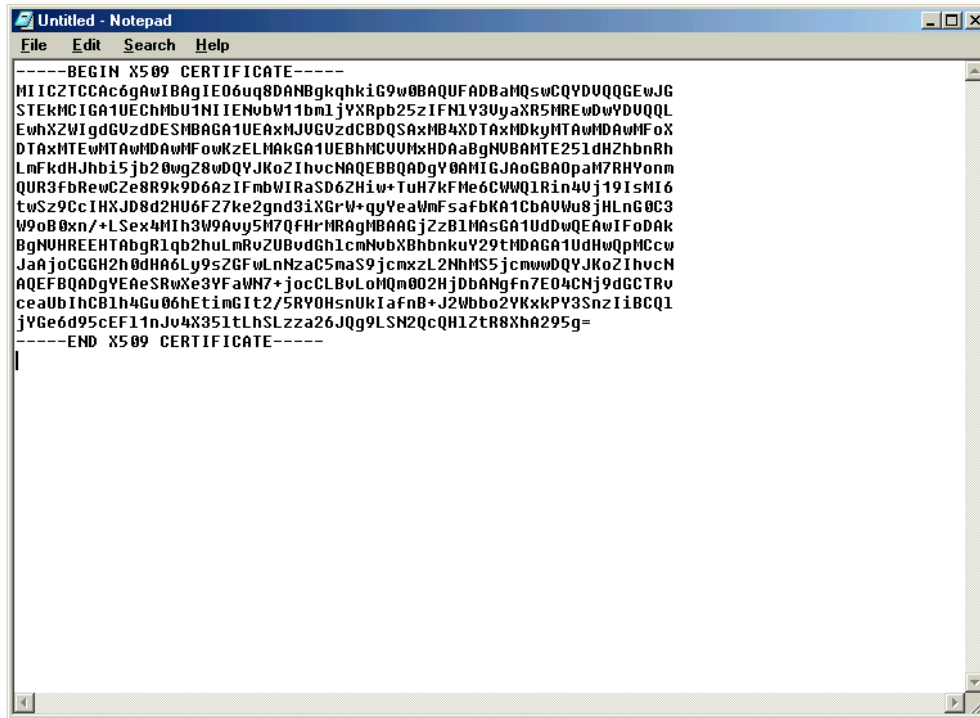
18. Scroll to the bottom of the page and click the Next Page button. The Final Certificate Parameters page will appear.



19. Select the radio button next to the appropriate CA chain you want the CA to use when generating your certificate. This should match the key length you selected when generating the request. For our example we used 1024, so we will select the first CA chain. Click the Next Page button.



20. Highlight all the text in the box and hit <Ctrl + C> to copy the text. Paste this text to a notepad file to be used later.



```

-----BEGIN X509 CERTIFICATE-----
MIICZTCCAc6gAwIBAgIE06uq8DANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJG
STEKMCIGA1UEChMU1N1IENubW11bm1jYXRpb25zIFN1Y3VyaXR5MREwDwYD
VUQL EwhXZWIgdGVzdDESMBAGA1UEAxMJUGVzdCB0QSxMB4XDTAxMDkyMTAw
MDAwMFoXDTAxMTEwMTAwMDAwMFowKzELMAKGA1UEBhMCVVHxHDAaBgN
UBAMTE251dHZhbnRhLmFkdHJhb15jb20uqZ8wDQYJKoZIhucNAQEBBQAD
gY0AMIGJAoGBA0paM7RHYonmQUR3FbRwCZe8R9k9D6AzIFmbWIRaSD6ZHiw+TuH7kFMe6C
WwQ1Rin4Uj191sHI6twSz9CcIHxJD8d2HU6FZ7ke2gnd31XGrW+qyYe
aWmfSaFbKA1CbAUWu8jHLnG0C3W9oB0xn/+LSex4HIh3W9Auy5M7
QFhrMRAGMBAAGjZzB1MA5GA1UdDwQEAwIFoDAkBgNVHREHTAbGR1qb2huLmRvZ
UBvdGh1cmNvbXBhbnkuY29tMDAGA1UdHwQpMCcwJAAjocGGH2h0dHA6L
y9sZGFwLnNzaC5maS9jcmxzL2NhMS5jcmwwDQYJKoZIhucNAQEFBQAD
gYEAeSRwXe3YFaWN7+jocCLBvLoMQm002HjDbANgFn7E04CNj9dGCT
RvceaUbIhCB1h4Gu06hEtimGI t2/5RY0HsnUKIaFnB+J2Wbbo2YKxk
PY3Snzi1BCQ1jYGe6d95cEF11nJv4X351tLhSLzza26JQg9LSN2QcQH12
tr8XhA295g=
-----END X509 CERTIFICATE-----

```

21. The Certificate Authority's certificate must be uploaded to the NetVanta 2000 series before loading the self-certificate. Follow the instructions in DLP-019 to upload the Certificate Authority's certificate to the NetVanta 2000 series.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

UPLOADING A CA CERTIFICATE TO THE NETVANTA

Introduction

The NetVanta 2000 series supports the use of both RSA and DSS Signature Algorithm Certificates. The NetVanta 2000 series provides the capability to generate self-certificate requests, and maintains a listing of private keys (certificate requests) that currently have no public key (self-certificate assigned by the Certificate Authority).

Before you can load the self-certificate provided by your Certificate Authority (CA) to the NetVanta 2000 series, you must load the CA's certificate to the NetVanta 2000 series. Without the CA's certificate the NetVanta 2000 series cannot verify the received self-certificate.

This DLP discusses the steps for uploading a CA certificate from a test certificate website (isakmp-test.ssh.fi). DLP-017 discusses generating the self-certificate request and DLP-018 discusses uploading the received self-certificate.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

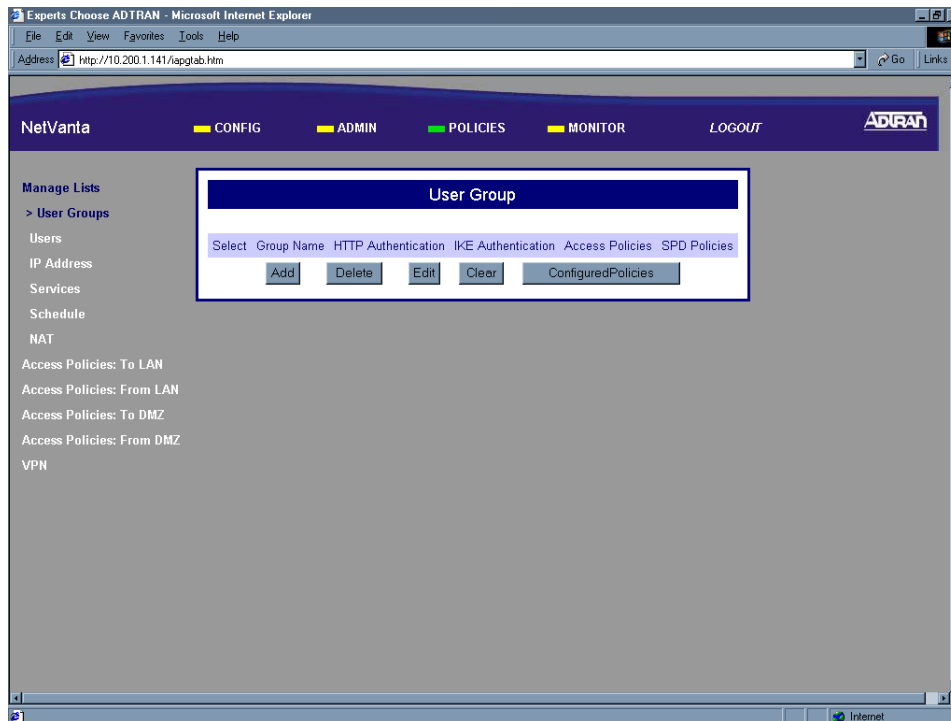
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

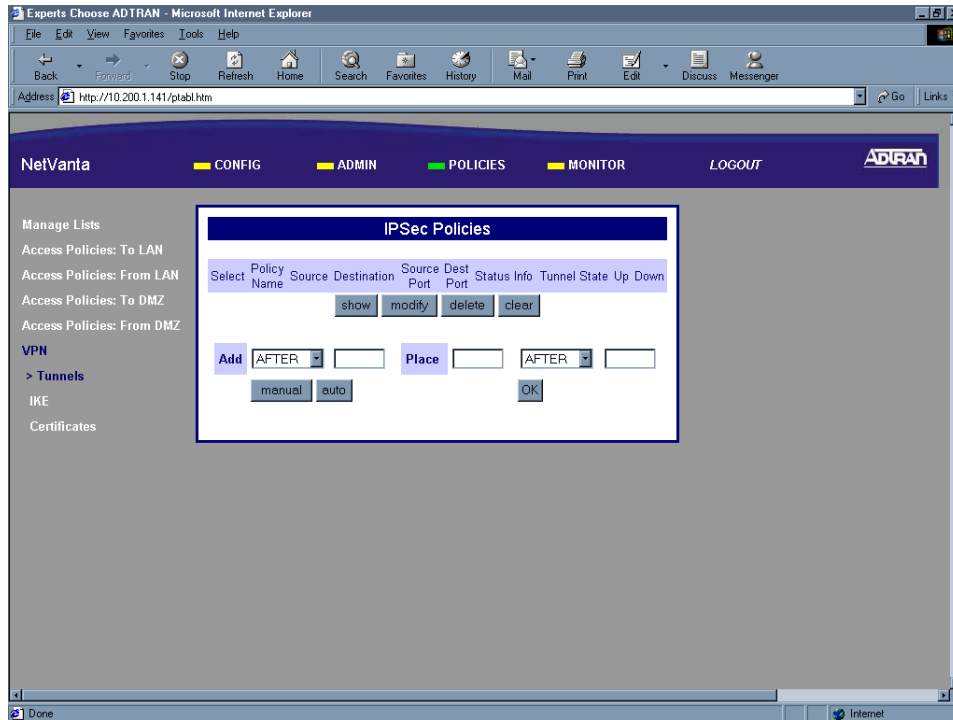
DLP-018

Perform Steps Below in the Order Listed

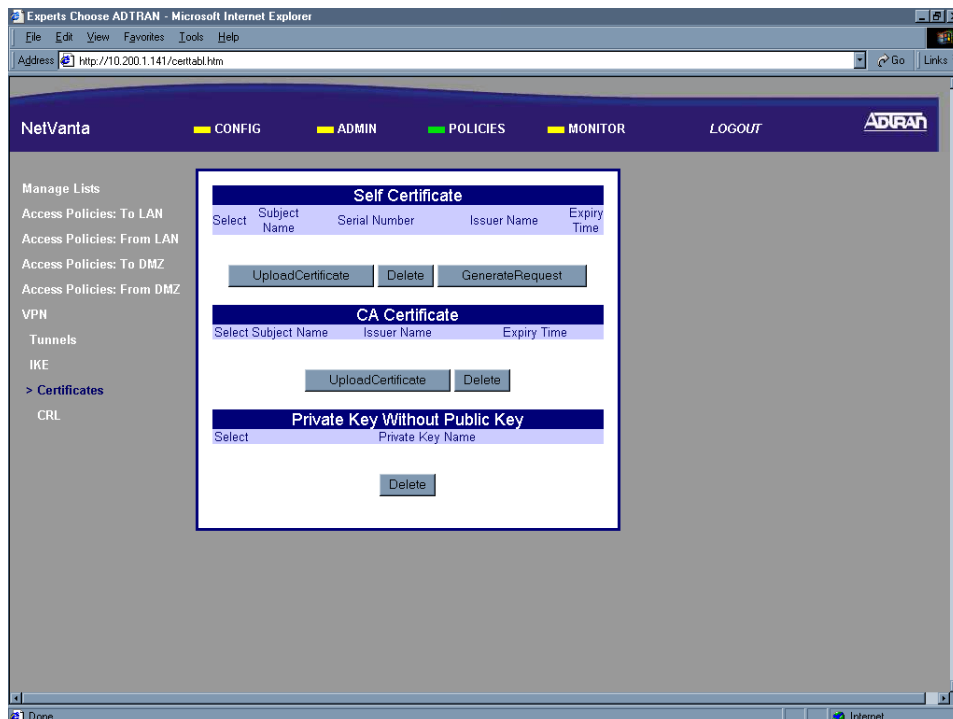
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **POLICIES**. The **MANAGE LISTS** menu and **USER GROUP** submenu are automatically displayed.



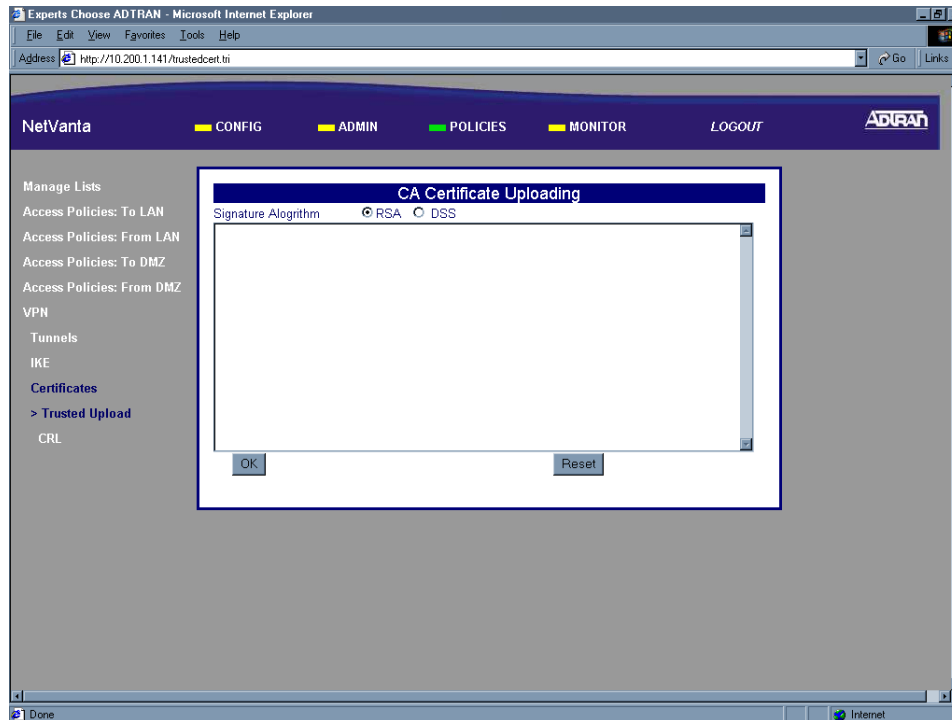
- From the menu list (located on the left side of the screen) select **VPN**. The IPsec Policies page will appear.



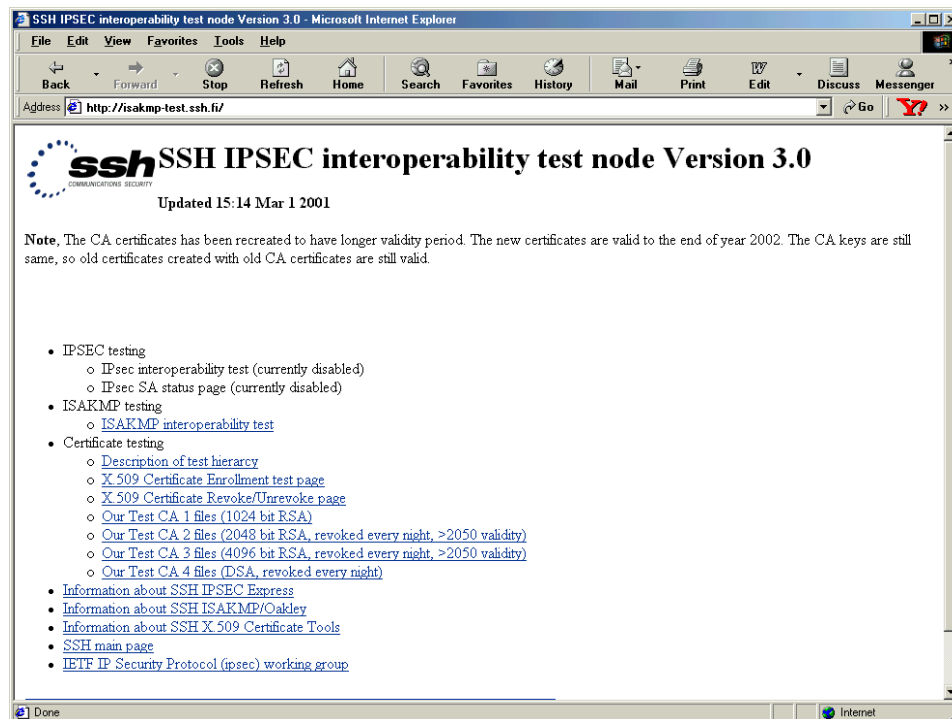
- From the menu list (located on the left side of the screen) select **CERTIFICATES** (listed as a VPN submenu).



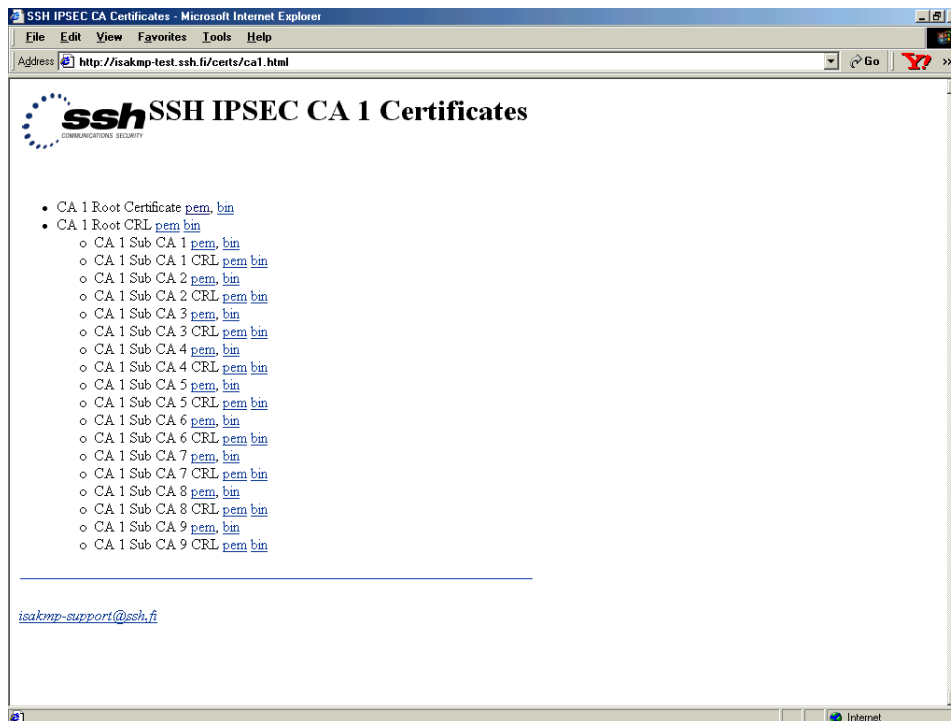
- In the CA Certificate section of the page click the Upload Certificate button. The CA Certificate Uploading parameters box appears.



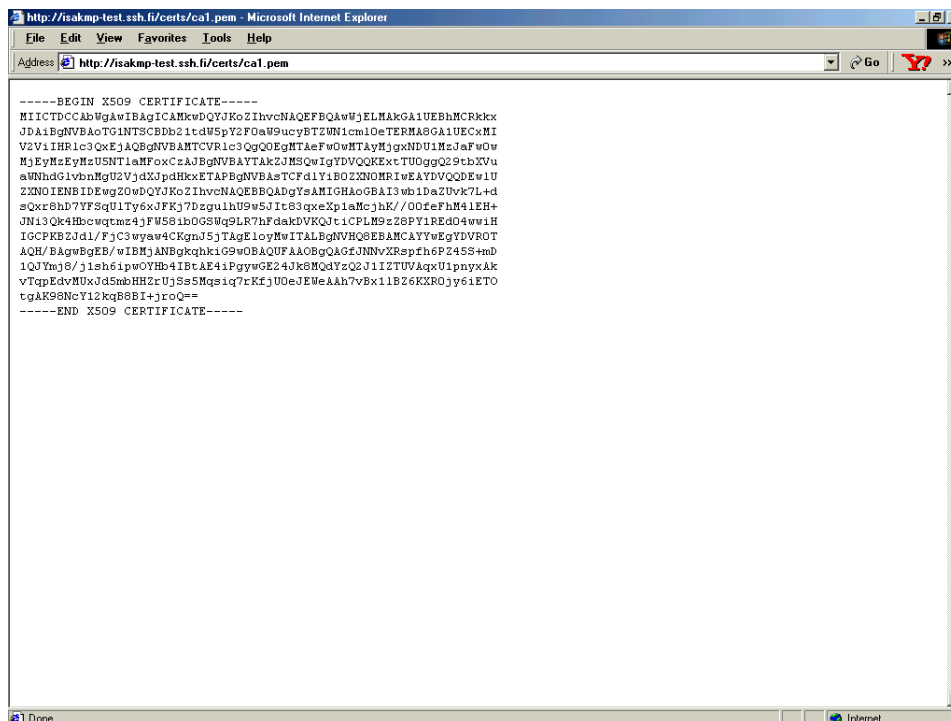
- Open a second browser session and enter isakmp-test.ssh.fi in the URL Address field. This will display the SSH Communications Security test certificate site.



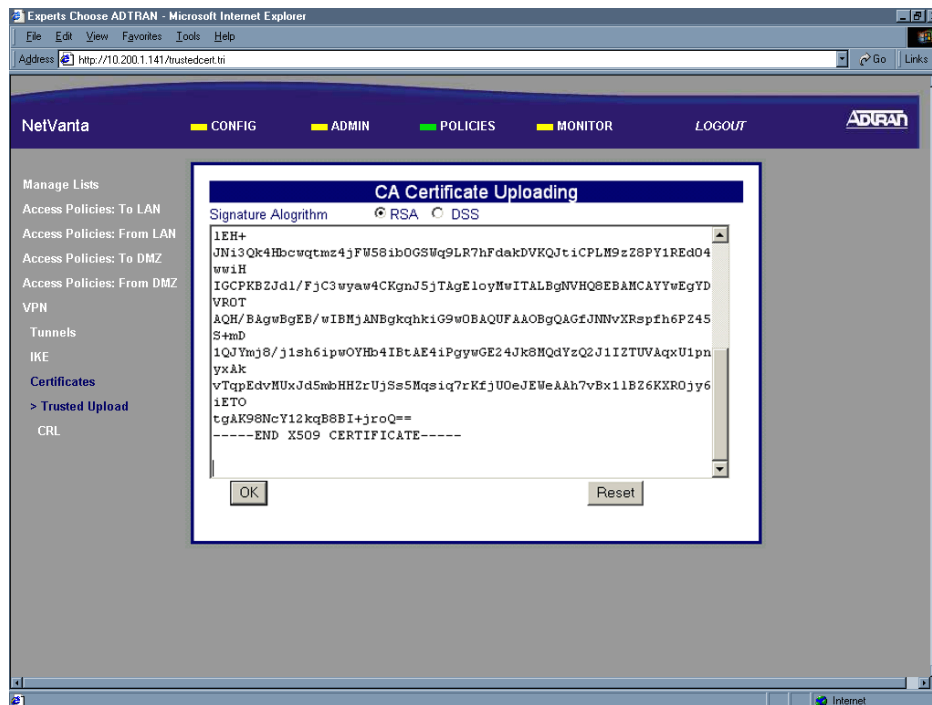
- Click on the appropriate Our CA Test CA link. Choose the link that matches the key length you used to generate the self-certificate request. In DLP-017 we applied a 1024 bit key to generate our request, so we will choose the Our CA Test CA 1 Files (1024 bit RSA) hyperlink.



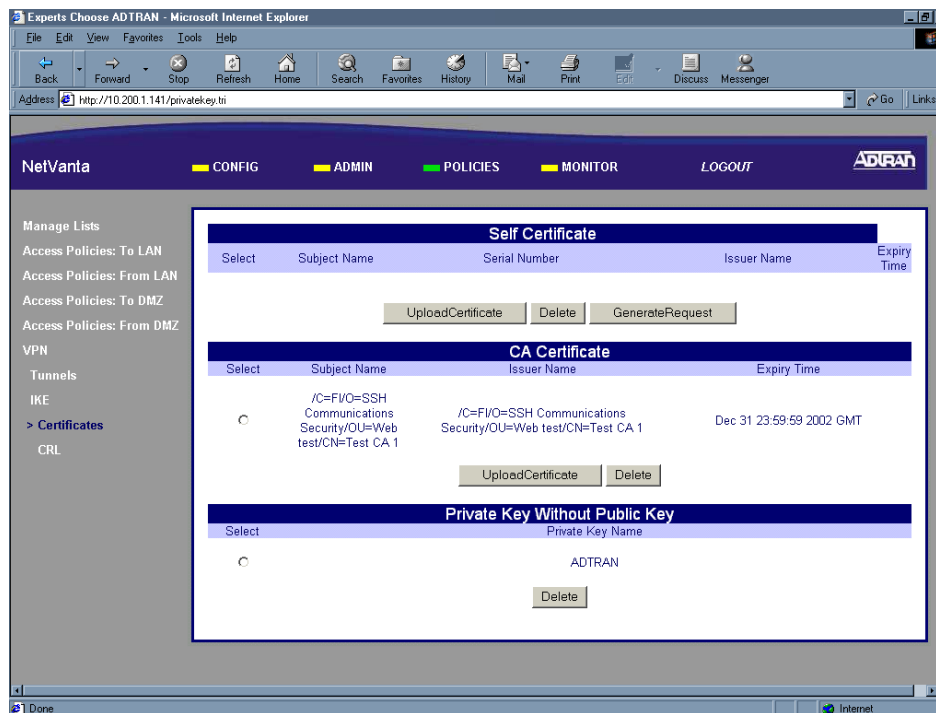
- The NetVanta 2000 series supports uploading certificates in PEM (Privacy Enhanced Mail) format. Select the CA 1 Root Certificate in PEM format.



- Highlight all the text in the box and hit <Ctrl + C> to copy the text. Return to the NetVanta 2000 series CA Certificate Uploading screen and paste the CA Certificate in the text box.



- Click the OK button to submit the certificate. When the certificate is successfully loaded the Certificates page will appear and the certificate will be listed in the CA Certificate section.



11. The Certificate Authority's certificate must be uploaded to the NetVanta 2000 series before loading a self-certificate. After loading the CA certificate you may proceed to DLP-019 for instructions on loading the self-certificate.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

UPLOADING A SELF-CERTIFICATE TO THE NETVANTA

Introduction

The NetVanta 2000 series supports the use of both RSA and DSS Signature Algorithm Certificates. The NetVanta 2000 series provides the capability to generate self-certificate requests, and maintains a listing of private keys (certificate requests) that currently have no public key (self-certificate assigned by the Certificate Authority).

Before you can load the self-certificate provided by your Certificate Authority (CA) to the NetVanta 2000 series, you must load the CA's certificate to the NetVanta 2000 series. Without the CA's certificate the NetVanta 2000 series cannot verify the received self-certificate.

This DLP discusses the steps for uploading a CA certificate from a test certificate website (isakmp-test.ssh.fi). DLP-017 discusses generating the self-certificate request and DLP-018 discusses uploading the received self-certificate.

Prerequisite Procedures

This DLP assumes that all steps outlined in DLP-017 and DLP-018 are complete and the user has the self-certificate in PEM (Privacy Enhanced Mail) format available.

Tools and Materials Required

- No special tools or materials required.

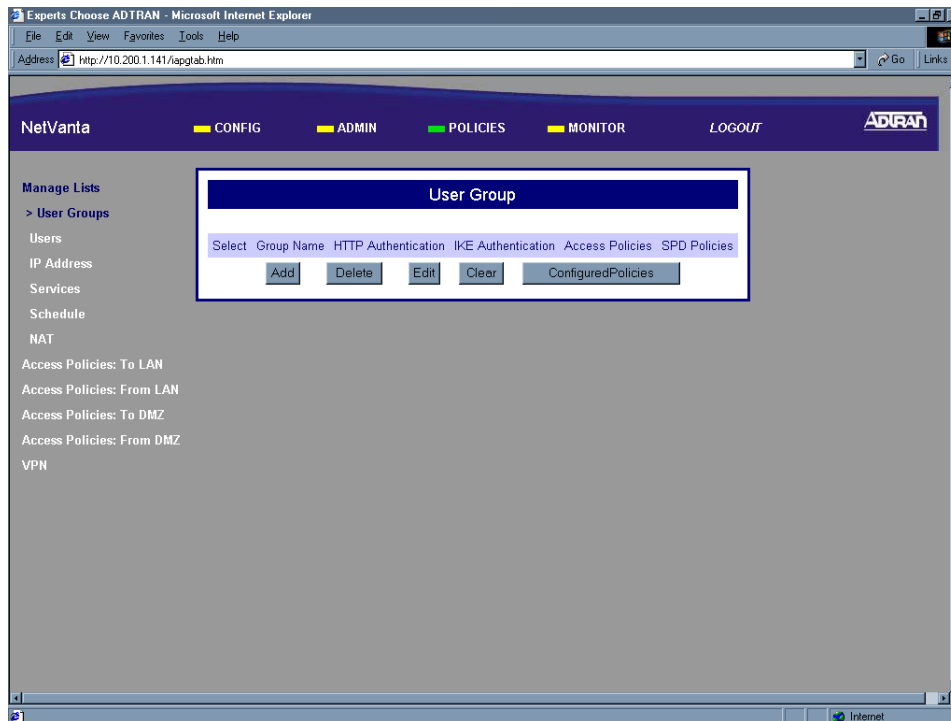
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

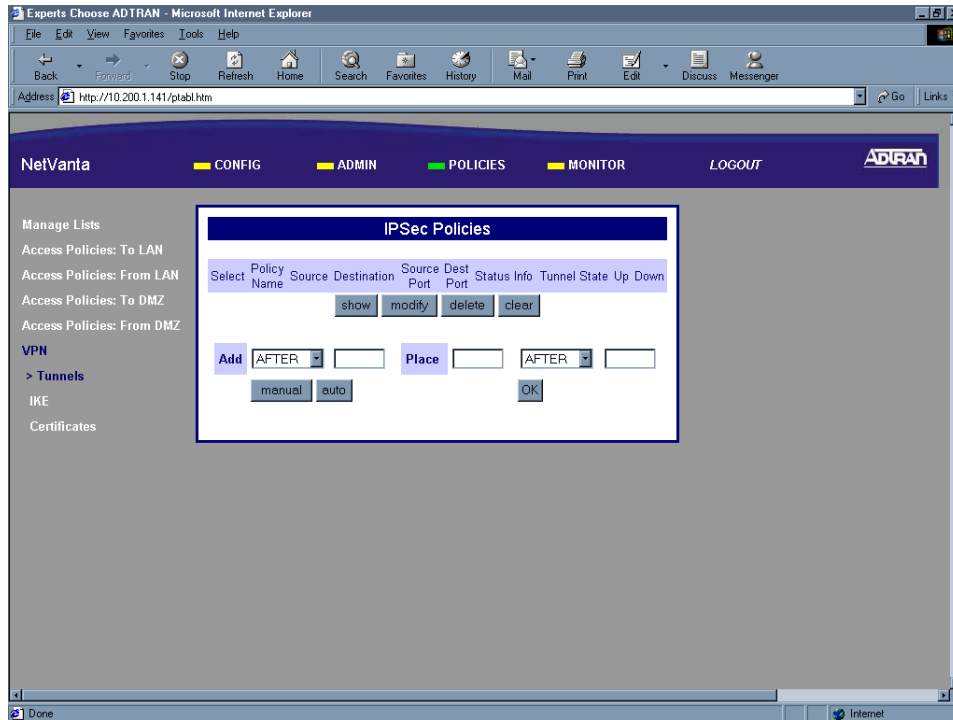
DLP-019

Perform Steps Below in the Order Listed

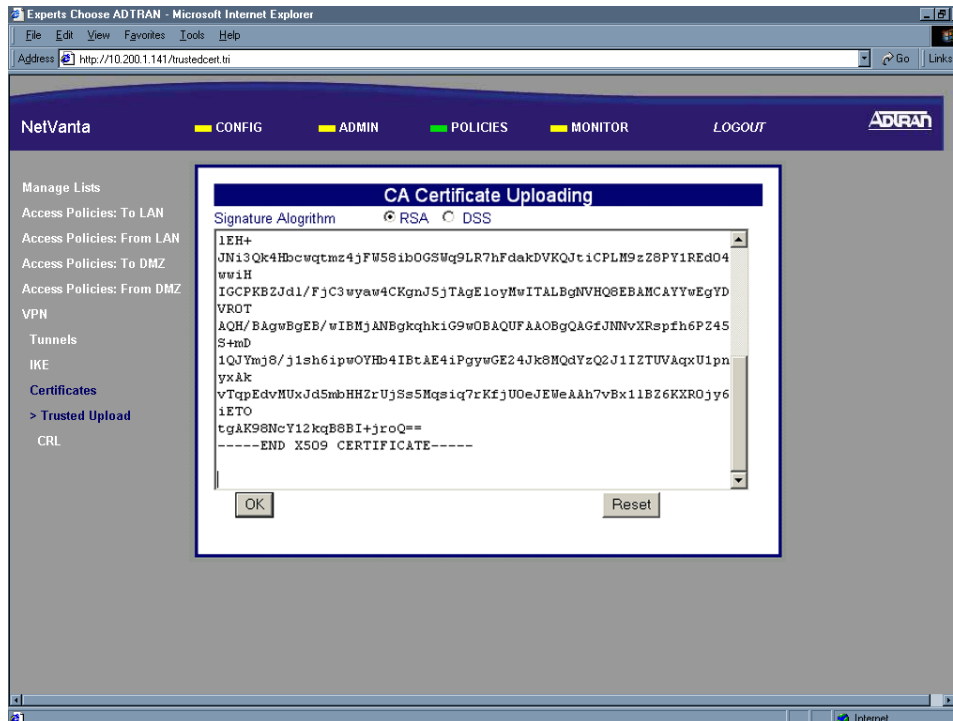
1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **POLICIES**. The **MANAGE LISTS** menu and **USER GROUP** submenu are automatically displayed.



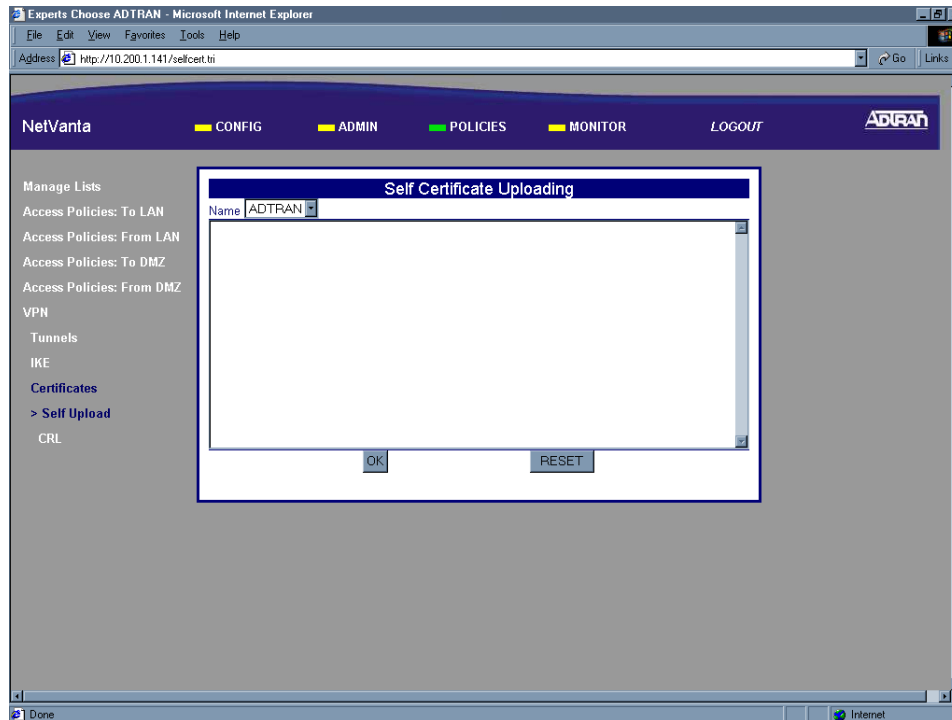
- From the menu list (located on the left side of the screen) select **VPN**. The IPsec Policies page will appear.



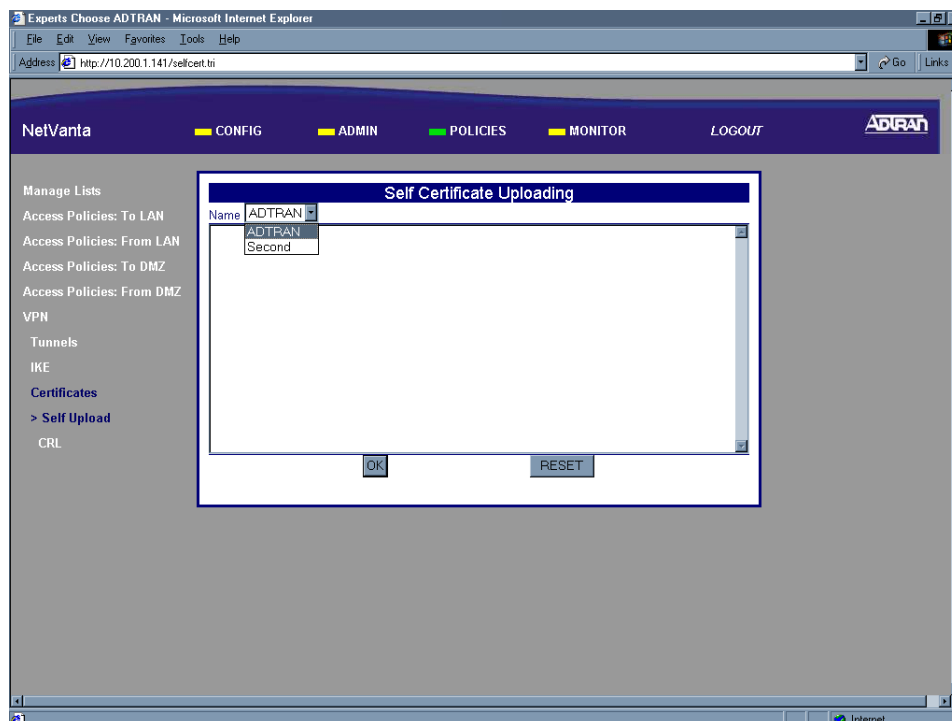
- From the menu list (located on the left side of the screen) select **CERTIFICATES** (listed as a VPN submenu).



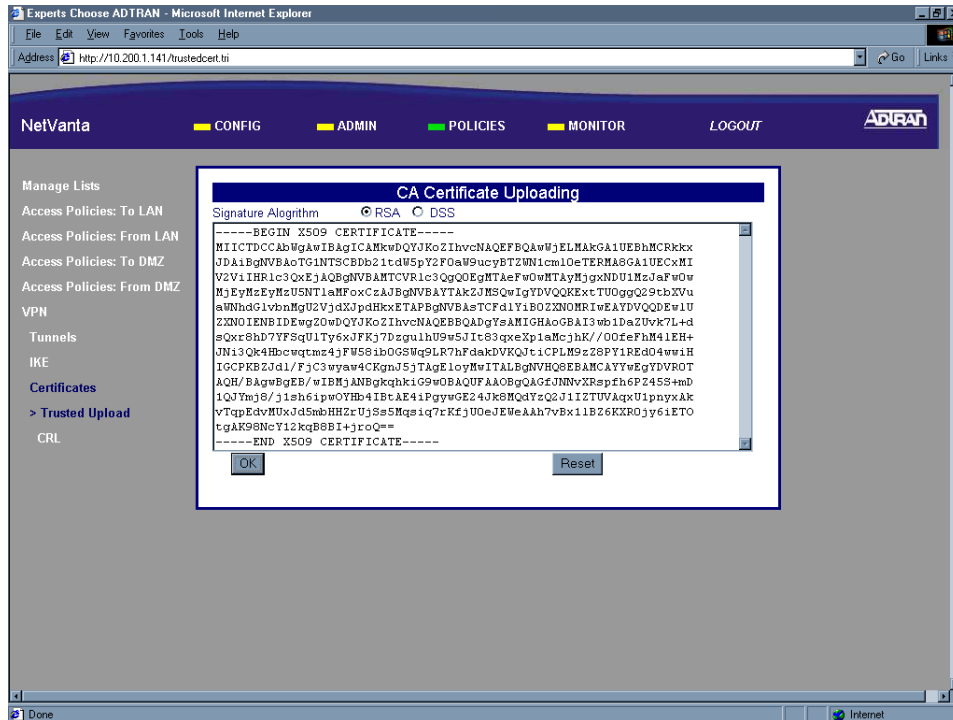
5. In the Self-Certificate section of the page click the Upload Certificate button. The Self-Certificate Uploading box appears.



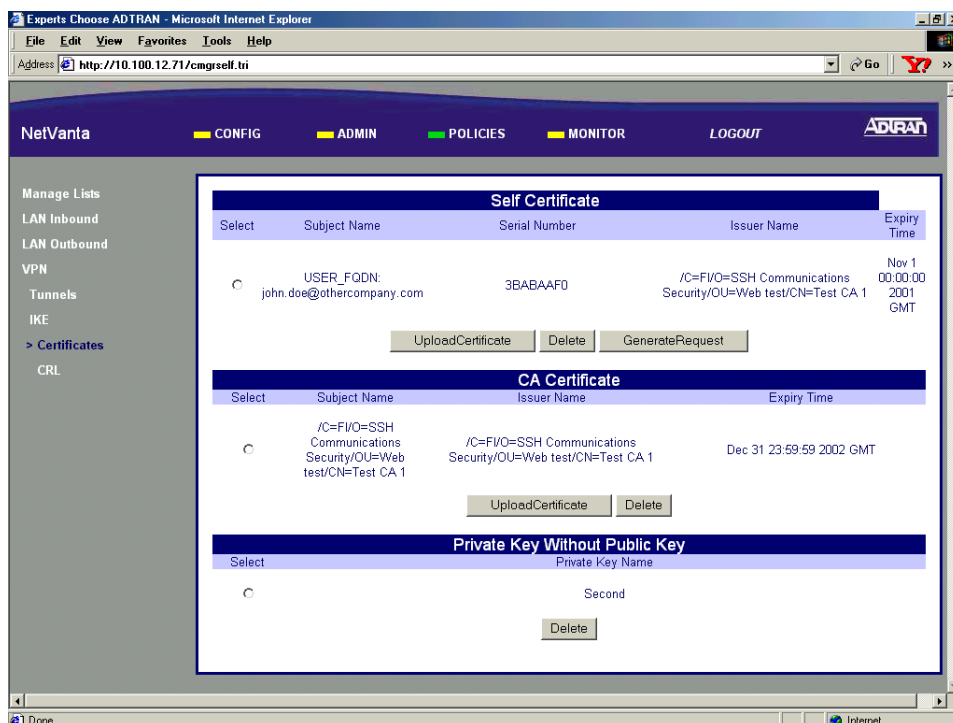
6. Select the name of the request this self-certificate corresponds to from the Name drop down menu. This is the locally significant name that was entered during the self-certificate request process (see DLP-017).



- Place your cursor in the text box portion of the Self-Certificate Uploading dialog and paste in the self-certificate text. If you followed the steps in DLP-017, this certificate text will be in a notepad file.



- Click the OK button to submit the self-certificate. When the certificate is successfully loaded the Certificates page will display and the self-certificate will be listed. Once the self-certificate is loaded for a particular request, the request is no longer visible in the Private Key Without Public Key list.



Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

REVIEWING THE VARIOUS KEYS OF THE NETVANTA

Introduction

Implementing a secure network requires the use of encryption, authentication, and the exchange of keys. The NetVanta 2000 series provides Encapsulating Security Payload (ESP) with support for both DES and 3DES encryption methods. The NetVanta 2000 series also provides Authentication Header (AH) with support for MD5-HMAC 128-bit and SHA1-HMAC 160-bit authentication algorithms. This DLP provides a quick reference table listing the various keys and the character requirements for each of them.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

DLP-020

Please Refer to the Table Below When Defining Keys in the NetVanta 2000 series

Key Name	Key Length	Use this key.....
MD5 AUTH KEY	16 digits	when using MD5 authentication for RIP updates on the LAN and/or WAN interface.
MD5 IN and OUT	16 digits	when configuring MD5 authentication for Manual VPN tunnels.
MD5 IN SPI and OUT SPI	numerical >255	when configuring MD5 authentication for Manual VPN tunnels.
MD5 IN AUTH KEY and OUT AUTH KEY	16 alphanumeric*	when configuring MD5 authentication for Manual VPN tunnels using ESP with AUTH encryption.
SHA1 IN and OUT	20 alphanumeric*	when configuring SHA1 authentication for Manual VPN tunnels.
SHA1 IN SPI and OUT SPI	numerical >255	when configuring SHA1 authentication for Manual VPN tunnels.
DES IN SPI and OUT SPI	numerical >255	when configuring DES encryption for Manual VPN tunnels using ESP or ESP with AUTH encryption.
3DES IN SPI and OUT SPI	numerical >255	when configuring 3DES encryption for Manual VPN tunnels using ESP or ESP with AUTH encryption.
DES IN and OUT ESP	8 alphanumeric*	when configuring DES encryption for Manual VPN tunnels using ESP or ESP with AUTH encryption.
3DES IN and OUT ESP	24 alphanumeric*	when configuring 3DES encryption for Manual VPN tunnels using ESP or ESP with AUTH encryption.

* The NetVanta 2000 series translates the inputted alphanumeric digits to their ASCII equivalent, then uses the result in Hexadecimal notation for operation.

RESTORING THE NETVANTA TO FACTORY DEFAULTS

Introduction

The NetVanta 2000 series provides two methods of restoring the unit to factory defaults - software and hardware. This DLP discusses each method and the necessary steps.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

DLP-021

Perform Steps Below in the Order Listed - Software Default

WARNING

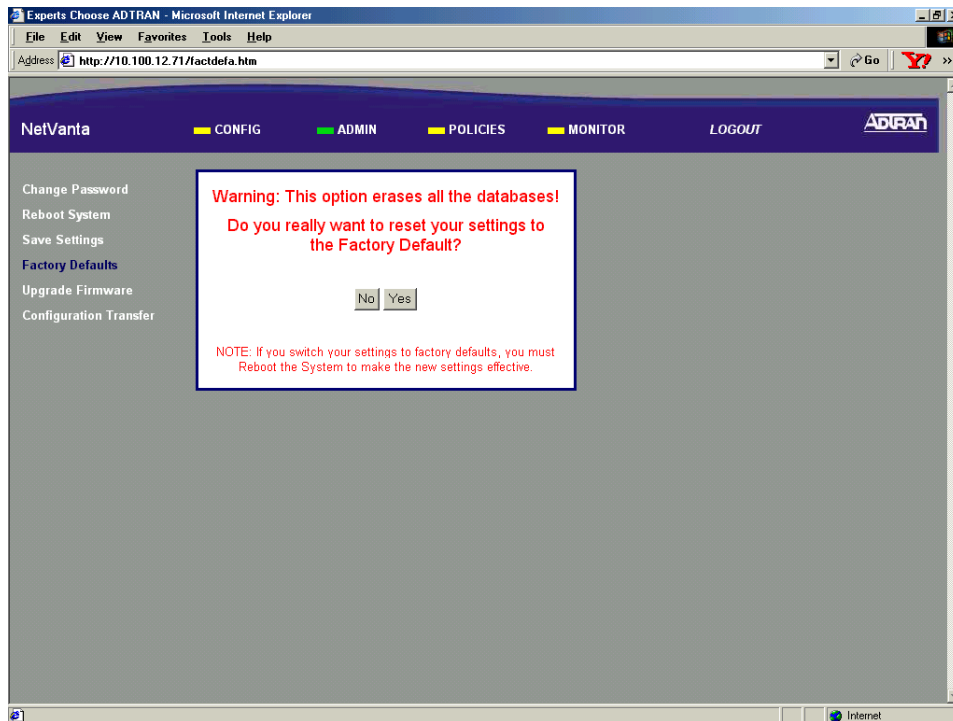
Performing a factory default using software will restore ALL configurable parameters of the NetVanta 2000 series to factory conditions. All modified interface address will be lost and may disrupt communications with the unit.

1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen), select **ADMIN**. This displays the **CHANGE PASSWORD** dialog box.

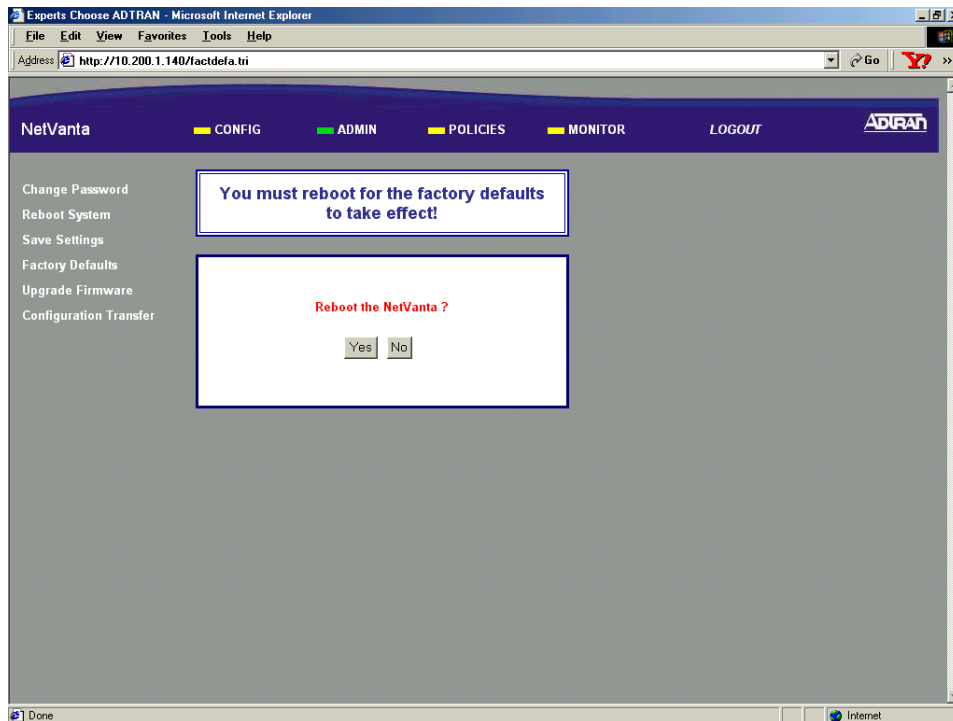
The screenshot shows a Microsoft Internet Explorer browser window displaying the NetVanta 2000 series web interface. The address bar shows the URL <http://10.200.1.140/admin.htm>. The main menu at the top includes **NetVanta**, **CONFIG**, **ADMIN**, **POLICIES**, **MONITOR**, and **LOGOUT**. The **ADMIN** menu item is highlighted. The **Admin Password Setting** dialog box is displayed, containing the following fields and buttons:

- Old Password:
- New Password:
- Confirm New Password:
- Session Timeout (secs):
- Submit:
- Reset:

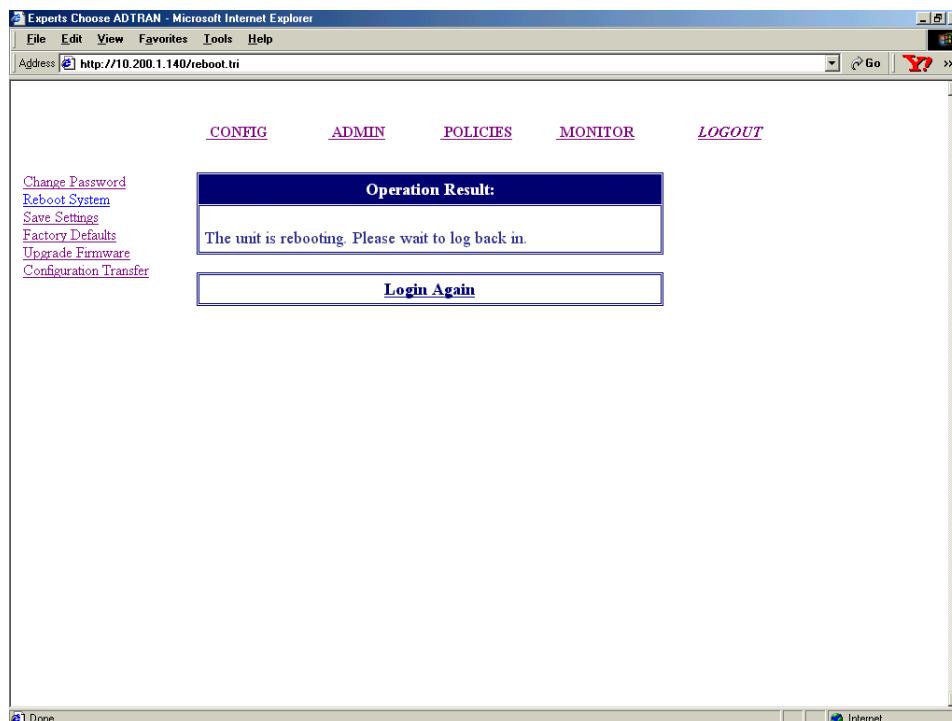
- From the menu list (located on the left side of the screen) select **FACTORY DEFAULT**.



- Click the Yes button to submit the operation. This will display the Reboot Confirmation screen.



- Click Yes to reboot the NetVanta 2000 series and restore all parameters to factory default settings.



- Complete the steps in DLP-001 to access the NetVanta 2000 series unit.

Perform Steps Below in the Order Listed - Hardware Default

WARNING

Performing a factory default using hardware only restores the LAN interface parameters to default state. The DHCP server will be enabled and the LAN interface will be given an IP address of 10.10.10.1.

- Make sure the NetVanta 2000 series unit is powered up.
- On the rear panel of the NetVanta 2000 series unit there is a factory default pinhole located between the LAN and WAN interfaces. Push the factory default pinhole for 1-2 seconds to restore the LAN interface factory settings.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

VIEWING THE DHCP INFO TABLE

Introduction

The NetVanta 2000 series supports three IP addressing schemes on the WAN interface -- dynamic, static, and PPP over Ethernet (PPPoE). When the WAN interface is configured for dynamic (DHCP) or PPPoE addressing, important information can be obtained by viewing the DHCP information the NetVanta 2000 series receives from your provider's DHCP server. The NetVanta 2000 series contains a table listing all DHCP information for both the LAN and WAN interfaces. This DLP discusses viewing that information.

Prerequisite Procedures

This DLP assumes the NetVanta 2000 series is connected to a PC and a browser session is active. Refer to DLP-001 for more details.

Tools and Materials Required

- No special tools or materials required.

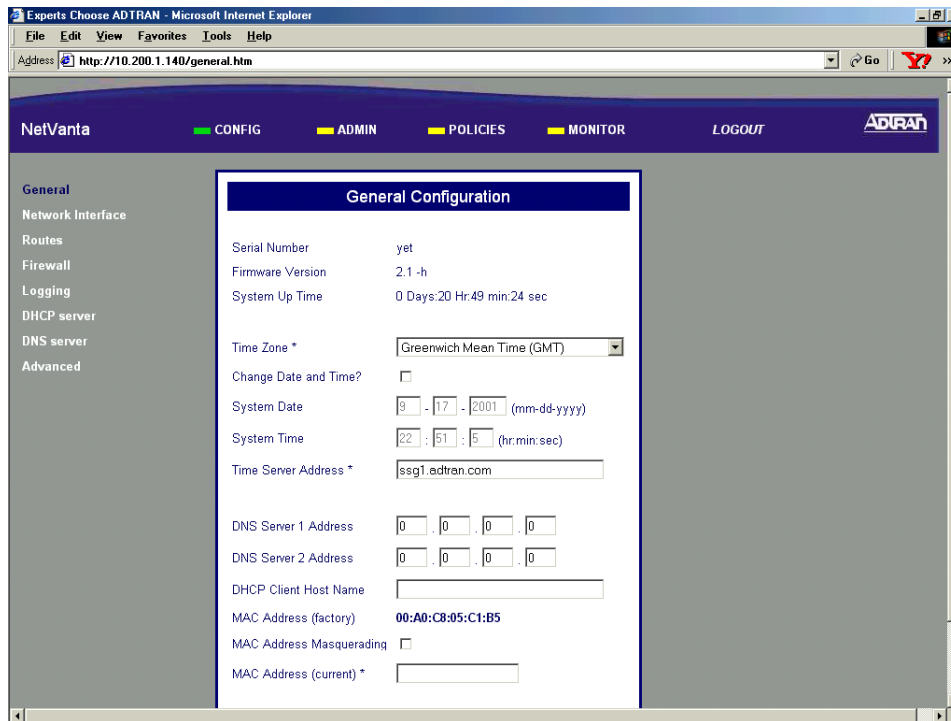
WARNING

To prevent electrical shock, do not install equipment in a wet location or during a lightning storm.

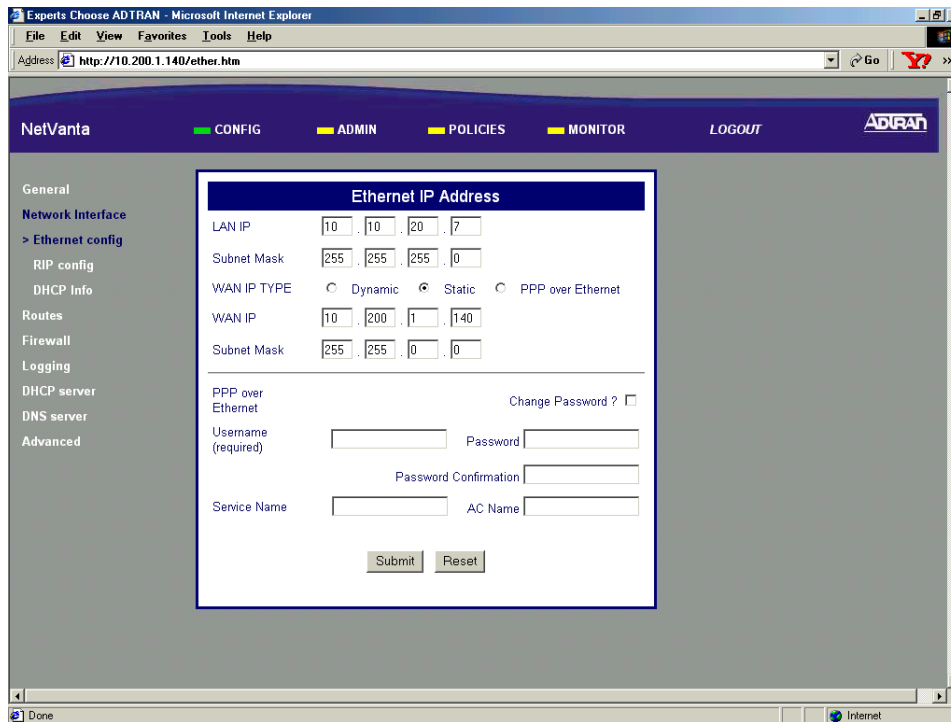
DLP-022

Perform Steps Below in the Order Listed

1. Log in to the NetVanta 2000 series as **admin** (see DLP-001 for details).
2. From the main menu (located across the top of the screen) select **CONFIG**.



- From the menu list (located on the left side of the screen) select **NETWORK INTERFACE**. The **ETHERNET CONFIG** page will appear.



- From the menu list (located on the left side of the screen) select **DHCP INFO**.



5. Record any information needed from this table for future use.



The IP address listed next to Gateways in the WAN column (172.124.37.252 for this example) will be used when adding the default route to the NetVanta 2000 series route table (see DLP-011). Record this address for future reference.

Follow-up Procedures

Once this procedure is complete, return to the procedure which referred you to this DLP and continue with the tasks indicated there.

GLOSSARY

Authentication

Identifying and validating a given user.

Data integrity

Traditionally, data integrity checking has involved attaching a checksum to a string of data to check against accidental data corruption. More sophisticated security algorithms add other validators such as time and date stamps to make sure data is not intercepted or altered.

Data Encryption Standard (DES)

Is a symmetric block cipher algorithm used as a confidentiality mechanism for the encapsulating security payload (ESP).

Data privacy

To prevent data from being read by humans or machines during transmission, data privacy algorithms such as Data Encryption Standard (DES) encrypt and then decrypt the data before and after transmission.

Denial of service (DOS) attack

A method of flooding a site with "spoofed" (artificially generated) packets. A DOS tries to generate enough traffic deny service to legitimate users. One recent method has been called "smurfing."

Encapsulating Security Payload

Provides confidentiality for IP datagrams by encrypting the payload data to be protected.

Encryption

The use of algorithms such as MD5 or SHA to encrypt (code) and the decrypt (decode) a password. Most encryption algorithms rely upon some sort of private key.

Filtrating

The process of statistically sampling the queue size and dropping packets when the queue reaches a threshold. Common methods are random early detection (RED) weighted random early detection (WRED).

Firewall

Usually a combination of hardware and software that protects an organization's network from external attacks or intrusions. Most firewalls make use of a proxy server that performs a validation and filtering function for the organization.

Hash Values

Locator numbers that replace a given value with a location in a table. The locator number is later used to retrieve the original data. Hashing is analogous to storing a coat on a coat rack. The hash ID is saved and used later for retrieval.

HTTP

HyperText Transfer Protocol is the protocol that carries requests from a browser to a Web server and also transports Web pages from a Web server back to the requesting browser. HTTP is the most universally used Web transfer protocol, but it is not inherently a secure protocol.

ICMP Redirect

Not necessarily a malicious condition, some routers generate a redirection message whenever a packet is rerouted. If these messages become excessive or if some mischievous person is generating these messages in an exponential fashion this condition can become invasive.

IP Reassembly

TCP/IP is a system of packet creation, packet disassembly, packet transmission, and packet reassembly. An intruder sometimes tries to intervene in the reassembly process and insert bogus extra or replacement segments.

IPSec

A method of providing secure communication (Internet Protocol security) over potentially insecure network components such as intermediate routers. IPSec defines encryption, authentication, and key management standards. IPSec protocols support transport mode and tunnel mode operations.

IP Spoofing

Gaining access to a computer by pretending to be at a trusted IP address. By setting up a firewall, all access must come through the firewall and pick up the only authorized address of the firewall after adequate authentication is completed.

Land attacks

A special type of denial of service attack where an intruder or intruding program identifies a source and direction of a particular packet and reverses (or swaps) these two IP addresses. This kind of attack can range from being a nuisance, to being a tragic menace if it prevents the delivery of an important document or message.

Masquerading

An unauthorized user assumes the identity of an authorized user.

Packet filtering

Is access control at the Internet Protocol layer. This includes accepting or rejecting (dropping) frames of data based on source and destination addresses. This is a very basic filtering method that does not include using passwords or authentication algorithms.

Ping of death

Is a denial of service attack that relies upon TCP/IP's difficulty handling unusually large ping packets. If not protected, a system that receives an oversize ping packet may hang or crash.

Proxy server

A firewall component that manages Internet traffic to and from a network and provides other features such as file caching and access control. A proxy server can also improve performance by

caching frequently requested web pages and can filter unauthorized user requests for access to files or designated web sites.

Replay attack

Capturing and storing a password-included packet and then reissuing that packet in an attempt to gain unauthorized access.

Routing Information Protocol

A protocol for exchanging routing information among gateways and other hosts.

Security Associations

Agreements or negotiations between two or more communicating parties. The details of these agreements involve decisions on which keys and algorithms are going to be used, and when these security elements are going to be changed.

Security Parameter Index (SPI)

An arbitrary 32-bit value that is assigned to an SA when it is first created. The SPI, when combined with the destination IP address and security protocol (AH or ESP), uniquely identifies the SA.

Source Routing

Source routing is a strict method of routing datagrams that uses a 32-bit header that embeds a source address, a destination address, a type of service, and other constants and variables that combine to protect the datagram from incorrect or failed routing.

SYN Flooding

Typically most systems process a queue of about 10 connections attempts (SYNs) at a time. A malicious intruder who fabricates connection attempts and tries to “flood” a system is using a denial of service attack known as SYN flooding.

Traffic Shaping

Is a process of minimizing the congestion of a stream of traffic at every connection, physical or virtual. The net effect is to optimize the overall result.

Virtual Private Network (VPN)

Is a private connection that sends private data traffic over the Internet. This lets organizations extend network service over the Internet to branch offices and remote users creating a private WAN (Wide Area Network).

ACRONYMS

AH

Authentication Header

ALG

Application Level Gateway

ASP

Active Server Protocol

ATM

Asynchronous Transfer Mode

CERT

Computer Emergency Response Team

DDOS

Distributed Denial of Service

DES

Data Encryption Standard

DH

Diffie Helman shared secret algorithm

DHCP

Dynamic Host Configuration Protocol

DNS

Domain Name Server

DSA

Digital Signature Algorithm

DSL

Digital Subscriber Loop

DSU/CSU

Data Service Unit/Channel Service Unit

ECN

Explicit Congestion Notification

ESP

Encapsulating Security Payload

HTTP

Hyper Text Transfer Protocol

ICMP

Internet Control Message Protocol

IETF

Internet Engineering Task Force

IEEE-SA

IEEE Standards Association

IKE

Internet Key Exchange

IPSec

Internet Protocol Security

MPOA

Multiprotocol Over ATM

NAT

Network Address Translation

NIST

National Institute of Standards and Technology

NNTP

Network News Transfer Protocol

NSA

National Security Agency

RIP

Routing Information Protocol

RSA

A public key encryption algorithm

RSVP

Resource Reservation Protocol

QOS

Quality of Service

SA

Security Association

SG

Security Gateway

SHA

Secure Hash Algorithm

SPD

Security Policy Database

SPI

Security Parameter Index

VPN

Virtual Private Network

VRRP

Virtual Router Redundancy Protocol

WAN

Wide area network

WELF

Webtrend Extended Log Format

WFQ

Weighted fair queuing

