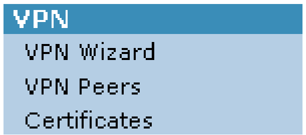
TECHNICAL SUPPORT NOTE

Introduction to the VPN Menu in the Web GUI

Featuring ADTRAN OS and the Web GUI

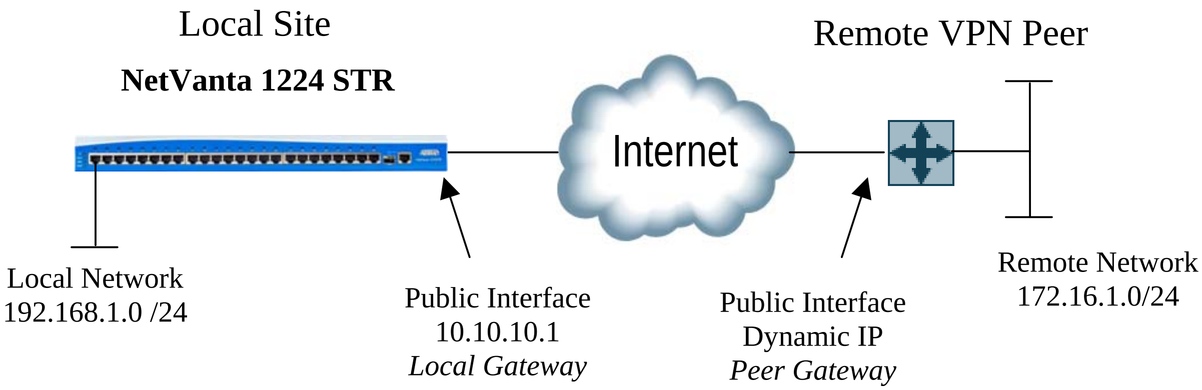
Introduction

This Technical Support Note shows the different options available in the VPN menu of the ADTRAN OS Web GUI.



VPN SECURITY POLICIES

There are many options that affect the connections in a VPN security policy. To establish secure communication with the remote site you need to configure matching VPN policies on both sides of the VPN connection. An outbound VPN policy on one end should match the inbound VPN policy on other end, and vice versa.



SAMPLE MATCHING VPN POLICIES

LOCAL SITE	**REMOTE VPN PEER**
Local Public Address Type = Static/10.10.10.1	Remote Public Add. Type = Static/10.10.10.1
Remote Peer Public Address Type = Dynamic	Local Public Address Type = Dynamic
Remote Private Network = 172.16.1.0 /24	Local Private Network = 172.16.1.0 /24
Local Private Network = 192.168.1.0 /24	Remote Private Network = 192.168.1.0 /24
Auth Type: PSK = GoADTRAN	Auth Type: PSK = GoADTRAN
Remote ID Type = Email Address	Local ID Type = Email Address
Remote ID Value = training@adtran.com	Local ID Value = training@adtran.com
Local ID Type = IP Address	Remote ID Type = IP Address
Local ID Value = 10.10.10.1	Remote ID Value = 10.10.10.1
IKE Phase 1	IKE Phase 1
Respond Mode = Aggressive	Initiate Mode = Aggressive
Initiate Mode = None	Respond Mode = None
Encryption Algorithm: 3DES	Encryption Algorithm: 3DES
Hash Algorithm: SHA	Hash Algorithm: SHA
Diffie Hellman Group: 2	Diffie Hellman Group: 2
IKE SA Lifetime: 10800 seconds	IKE SA Lifetime: 10800 seconds
IPSec Phase 2	IPSec Phase 2
Encryption Algorithm: 3DES	Encryption Algorithm: 3DES
Hash Algorithm: SHA	Hash Algorithm: SHA
PFS: Group 2	PFS: Group 2
IPSec SA Lifetime: 3600 seconds	IPSec SA Lifetime: 3600 seconds
IPSec SA Lifetime : 0 KBytes	IPSec SA Lifetime : 0 KBytes

NetVanta VPN GUI Configuration

The addition of the VPN configuration options to the GUI interface greatly eases the VPN configuration - especially when compared to the command line VPN configuration. This module presents the GUI method of VPN configuration from using wizards to manually defining VPN parameters.

VPN Menu

The VPN menu is only displayed on units with the ADTRAN OS Enhanced Feature Pack Upgrade. The Standard Feature Pack is the default operating system and ships as the standard configuration on every NetVanta platform. The Enhanced Feature Pack adds the VPN functionality to the Standard Feature Pack and can either be added at the time of original purchase or purchased as an Upgrade at a later date.

VPN Wizard

The VPN Wizard will take you through a step by step process of adding a VPN peer to your configuration. You can select from one of two types of wizards. The Typical Setup Wizard is recommended for users not very familiar with the all the settings for IKE and IPSec. The Custom Setup Wizard is recommended for users who have knowledge about IKE and IPSec or for users who want to create non-standard VPN Peer Configurations.

VPN Peers

The VPN Peers menu directs you to the advanced VPN Policy configuration. From here you can create, modify, view, and delete VPN Peers, configure individual IKE and IPSec policies, or disable/enable VPN functionality.

Certificates

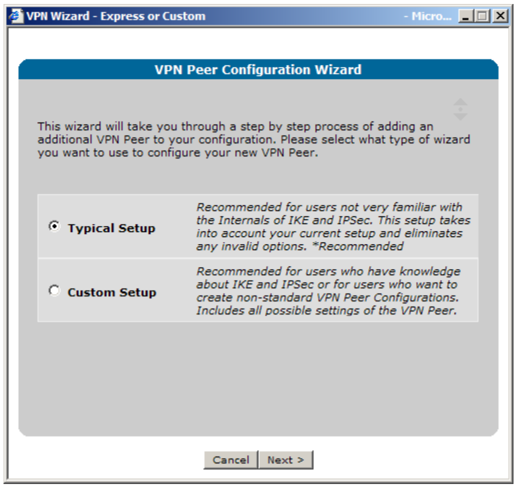
The Certificate menu item accesses the Certificate Authority Profiles screen. From, you can add, modify, or delete Certificate Authority profiles and policies.

VPN Wizard - Typical Setup

This Wizard is recommended for users not very familiar with all the settings for IKE and IPSec. You will be taken through a step by step configuration of a remote VPN peer where you are prompted for the local and remote gateways, ID's, and network traffic to protect with this VPN policy.

Using the 'Typical Setup' VPN Configuration Wizard

1) After selecting the VPN Wizard, choose Typical Setup.



VPN Wizard - Express or Custom - Micro...

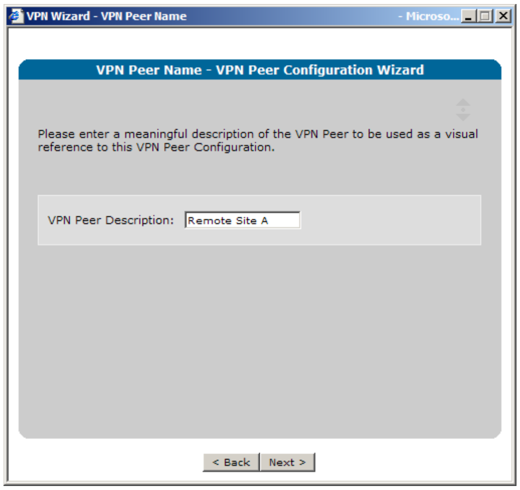
VPN Peer Configuration Wizard

This wizard will take you through a step by step process of adding an additional VPN Peer to your configuration. Please select what type of wizard you want to use to configure your new VPN Peer.

● **Typical Setup** — *Recommended for users not very familiar with the Internals of IKE and IPSec. This setup takes into account your current setup and eliminates any invalid options. *Recommended*

○ **Custom Setup** — *Recommended for users who have knowledge about IKE and IPSec or for users who want to create non-standard VPN Peer Configurations. Includes all possible settings of the VPN Peer.*

2) Enter a description of the remote VPN peer.



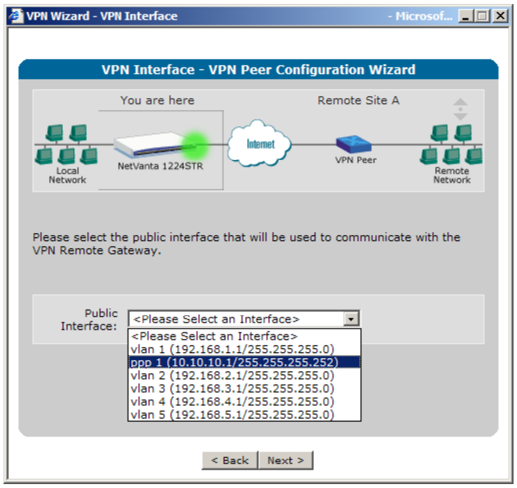
VPN Wizard - VPN Peer Name - Microso...

VPN Peer Name - VPN Peer Configuration Wizard

Please enter a meaningful description of the VPN Peer to be used as a visual reference to this VPN Peer Configuration.

VPN Peer Description: Remote Site A

3) Select the local public interface that will be used to communicate with the remote VPN Gateway.



VPN Wizard - VPN Interface - Microsof...

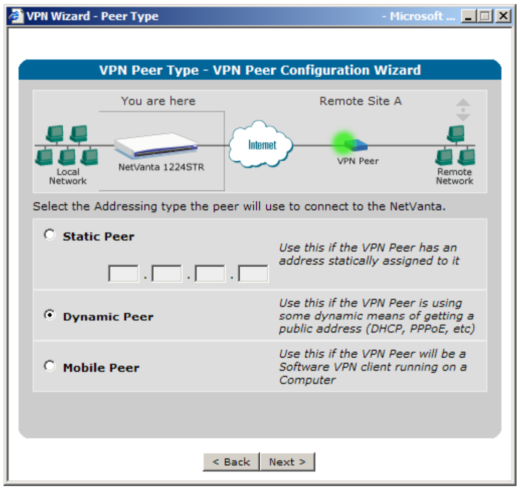
VPN Interface - VPN Peer Configuration Wizard

Please select the public interface that will be used to communicate with the VPN Remote Gateway.

Public Interface: <Please Select an Interface>

<Please Select an Interface>
vlan 1 (192.168.1.1/255.255.255.0)
ppp 1 (10.10.10.1/255.255.255.252)
vlan 2 (192.168.2.1/255.255.255.0)
vlan 3 (192.168.3.1/255.255.255.0)
vlan 4 (192.168.4.1/255.255.255.0)
vlan 5 (192.168.5.1/255.255.255.0)

4) Select the address type the Remote VPN peer will use to connect to the NetVanta.



VPN Wizard - Peer Type - Microsoft ...

VPN Peer Type - VPN Peer Configuration Wizard

Select the Addressing type the peer will use to connect to the NetVanta.

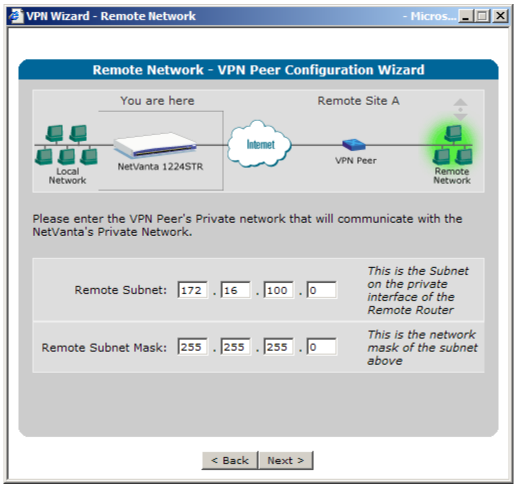
○ **Static Peer** — *Use this if the VPN Peer has an address statically assigned to it* □ . □ . □ . □

● **Dynamic Peer** — *Use this if the VPN Peer is using some dynamic means of getting a public address (DHCP, PPPoE, etc)*

○ **Mobile Peer** — *Use this if the VPN Peer will be a Software VPN client running on a Computer*

Using the 'Typical Setup' VPN Configuration Wizard (*Continued…*)

5) Specify the remote VPN Peer's private network that will communicate with the local private network.

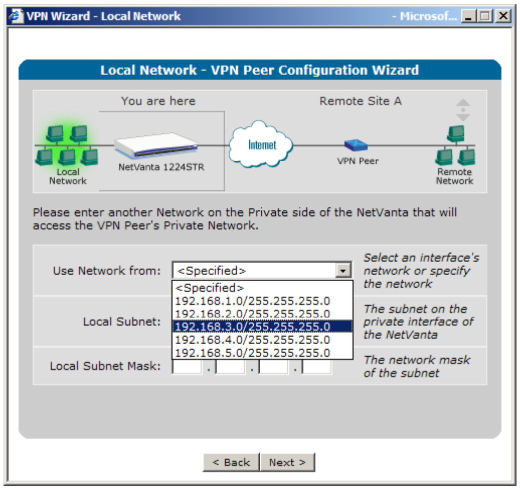


Please enter the VPN Peer's Private network that will communicate with the NetVanta's Private Network.

Remote Subnet: 172 . 16 . 100 . 0 — *This is the Subnet on the private interface of the Remote Router*

Remote Subnet Mask: 255 . 255 . 255 . 0 — *This is the network mask of the subnet above*

6) Select or specify the local private network that will access the remote VPN Peer's private network.



Please enter another Network on the Private side of the NetVanta that will access the VPN Peer's Private Network.

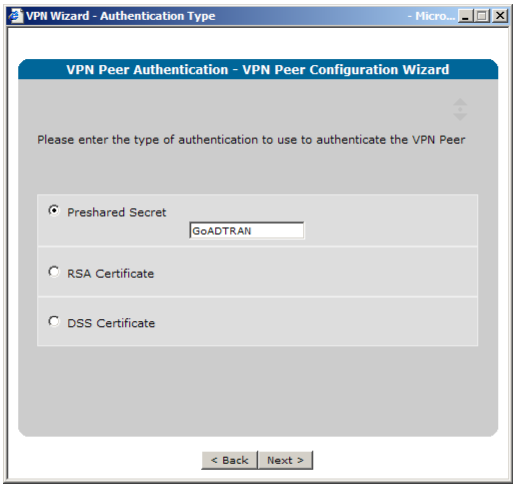
Use Network from: <Specified> — *Select an interface's network or specify the network*

<Specified>
192.168.1.0/255.255.255.0
192.168.2.0/255.255.255.0
192.168.3.0/255.255.255.0
192.168.4.0/255.255.255.0
192.168.5.0/255.255.255.0

Local Subnet: — *The subnet on the private interface of the NetVanta*

Local Subnet Mask: . . . — *The network mask of the subnet*

7) Select the type of authentication to use to authenticate the VPN Peer.



VPN Wizard - Authentication Type - Micro...
VPN Peer Authentication - VPN Peer Configuration Wizard
< Back
Next >

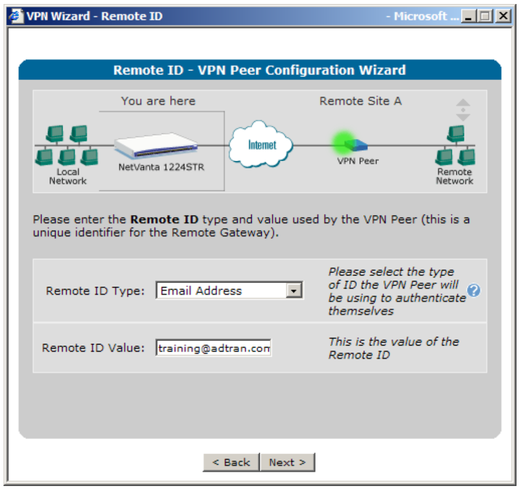
Please enter the type of authentication to use to authenticate the VPN Peer

● Preshared Secret
GoADTRAN

○ RSA Certificate

○ DSS Certificate

8) Enter the Remote ID type and value used by the VPN Peer.



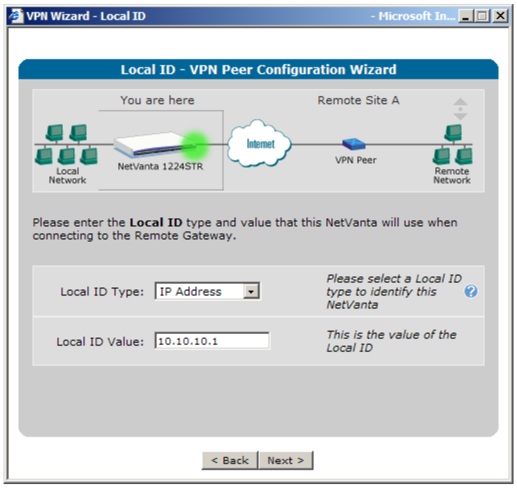
Please enter the **Remote ID** type and value used by the VPN Peer (this is a unique identifier for the Remote Gateway).

Remote ID Type: Email Address — *Please select the type of ID the VPN Peer will be using to authenticate themselves*

Remote ID Value: training@adtran.com — *This is the value of the Remote ID*

Using the ‘Typical Setup’ VPN Configuration Wizard (*Continued…*)

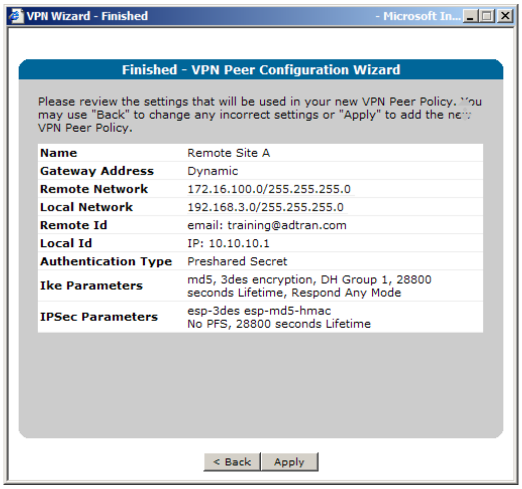
9) Enter the Local ID type and value that this NetVanta will use when connecting to the Remote Gateway.



Please enter the **Local ID** type and value that this NetVanta will use when connecting to the Remote Gateway.

Local ID Type:	IP Address	*Please select a Local ID type to identify this NetVanta*
Local ID Value:	10.10.10.1	*This is the value of the Local ID*

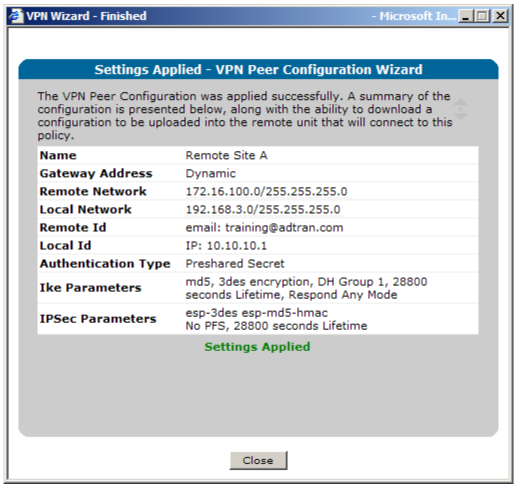
10) Review the settings for your new VPN Peer policy. Click the Back button if you wish to make any changes. Click Apply if you wish to add the new VPN Peer policy.


VPN Wizard - Finished - Microsoft In...
Finished - VPN Peer Configuration Wizard
< Back
Apply

Please review the settings that will be used in your new VPN Peer Policy. You may use "Back" to change any incorrect settings or "Apply" to add the new VPN Peer Policy.

Name	Remote Site A
Gateway Address	Dynamic
Remote Network	172.16.100.0/255.255.255.0
Local Network	192.168.3.0/255.255.255.0
Remote Id	email: training@adtran.com
Local Id	IP: 10.10.10.1
Authentication Type	Preshared Secret
Ike Parameters	md5, 3des encryption, DH Group 1, 28800 seconds Lifetime, Respond Any Mode
IPSec Parameters	esp-3des esp-md5-hmac No PFS, 28800 seconds Lifetime

11) The VPN Peer configuration was applied successfully. A summary of the configuration is displayed.


VPN Wizard - Finished - Microsoft In...
Settings Applied - VPN Peer Configuration Wizard
Close

The VPN Peer Configuration was applied successfully. A summary of the configuration is presented below, along with the ability to download a configuration to be uploaded into the remote unit that will connect to this policy.

Name	Remote Site A
Gateway Address	Dynamic
Remote Network	172.16.100.0/255.255.255.0
Local Network	192.168.3.0/255.255.255.0
Remote Id	email: training@adtran.com
Local Id	IP: 10.10.10.1
Authentication Type	Preshared Secret
Ike Parameters	md5, 3des encryption, DH Group 1, 28800 seconds Lifetime, Respond Any Mode
IPSec Parameters	esp-3des esp-md5-hmac No PFS, 28800 seconds Lifetime

Settings Applied

The VPN policies will be created and applied to the specified interface based on your selections. The following VPN configuration was created based on the above selections:

```
   ip crypto
         :
   crypto ike policy 100
     no initiate
     respond anymode
     local-id address 10.10.10.1
     peer any
     attribute 1
       encryption 3des
       hash md5
       authentication pre-share
         :
   crypto ike remote-id user-fqdn training@adtran.com preshared-key GoADTRAN
    ike-policy 100 crypto map VPN 10 no-mode-config no-xauth
         :
   crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
     mode tunnel
         :
   crypto map VPN 10 ipsec-ike
     description Remote Site A
     match address VPN-10-vpn-selectors
     set transform-set esp-3des-esp-md5-hmac
     ike-policy 100
         :
** ip access-list standard wizard-ics
     remark Internet Connection Sharing
     permit any
         :
** ip access-list extended self
     remark Traffic to NetVanta
     permit ip any  any    log
         :
   ip access-list extended VPN-10-vpn-selectors
     permit ip 192.168.3.0 0.0.0.255  172.16.100.0 0.0.0.255
     deny   ip any  any
         :
   ip policy-class Private
     allow list VPN-10-vpn-selectors
     allow list self self
**   nat source list wizard-ics interface ppp 1 overload
         :
   ip policy-class Public
     allow reverse list VPN-10-vpn-selectors
**   nat destination list wizard-pfwd-1 address 192.168.3.100
```

```
interface vlan 3
  ip address  192.168.3.1  255.255.255.0
  access-policy Private
      :
interface vlan 4
  ip address  192.168.4.1  255.255.255.0
  access-policy Private
      :
interface vlan 5
  ip address  192.168.5.1  255.255.255.0
  access-policy Private
      :

      :
interface vlan 5
  ip address  192.168.5.1  255.255.255.0
  access-policy Private
      :
interface ppp 1
  ip address  10.10.10.1  255.255.255.252
  access-policy Public
  crypto map VPN
      :
```

** Partial output displayed*

*** Created by a previous firewall policy*

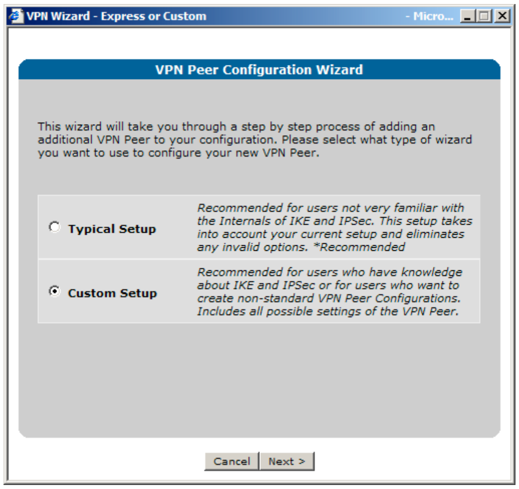
* Remember to save your configuration to ensure the settings will not be lost after a restart.

VPN Wizard - Custom Setup

This Wizard is recommended for users who have knowledge about IKE and IPSec or for users who want to create non-standard VPN Peer Configurations. The first part of the wizard takes you through the same steps as the Typical Wizard where you define the local and remote gateways, ID's, and network traffic to be protected by this VPN policy. You are then given the chance to define remaining IKE and IPSec policy parameters.

Using the 'Custom Setup' VPN Configuration Wizard

1) After selecting the VPN Wizard, choose Custom Setup.



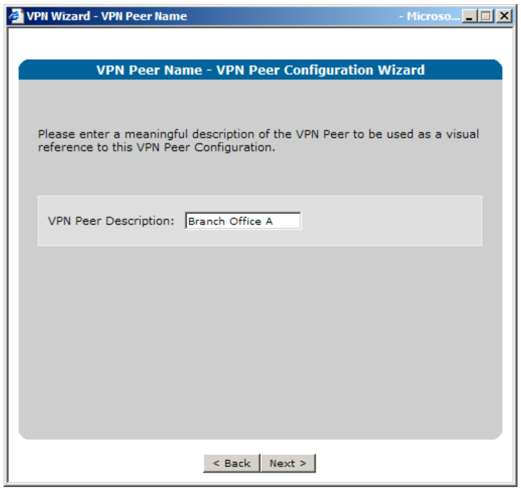
VPN Peer Configuration Wizard

This wizard will take you through a step by step process of adding an additional VPN Peer to your configuration. Please select what type of wizard you want to use to configure your new VPN Peer.

○ **Typical Setup** — *Recommended for users not very familiar with the Internals of IKE and IPSec. This setup takes into account your current setup and eliminates any invalid options. *Recommended*

● **Custom Setup** — *Recommended for users who have knowledge about IKE and IPSec or for users who want to create non-standard VPN Peer Configurations. Includes all possible settings of the VPN Peer.*

2) Enter a description of the remote VPN peer.

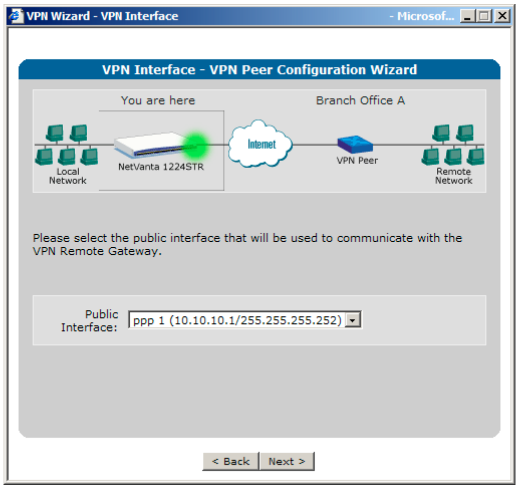


VPN Peer Name - VPN Peer Configuration Wizard

Please enter a meaningful description of the VPN Peer to be used as a visual reference to this VPN Peer Configuration.

VPN Peer Description: Branch Office A

3) Select the local public interface that will be used to communicate with the remote VPN Gateway.

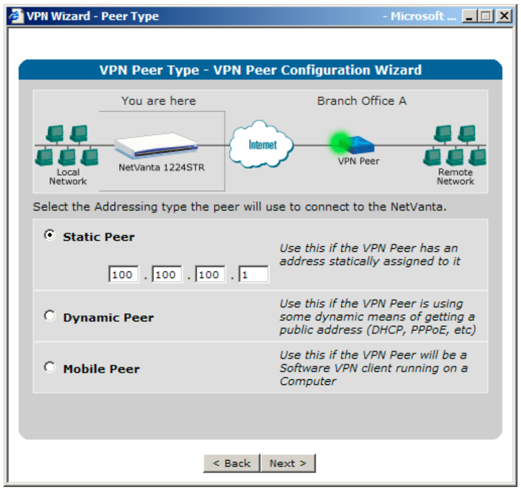


VPN Interface - VPN Peer Configuration Wizard

Please select the public interface that will be used to communicate with the VPN Remote Gateway.

Public Interface: ppp 1 (10.10.10.1/255.255.255.252)

4) Select the address type the Remote VPN peer will use to connect to the NetVanta.



VPN Peer Type - VPN Peer Configuration Wizard

Select the Addressing type the peer will use to connect to the NetVanta.

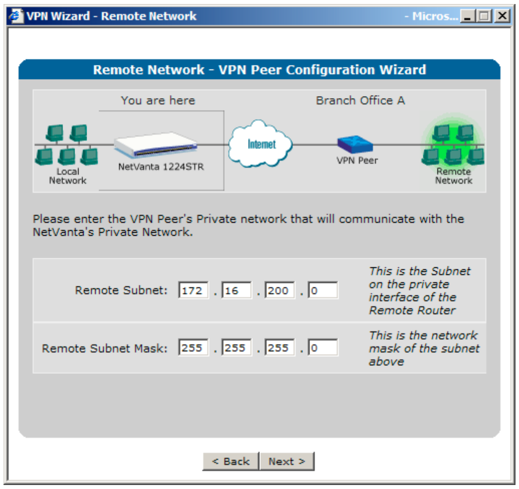
● **Static Peer** — *Use this if the VPN Peer has an address statically assigned to it*
100 . 100 . 100 . 1

○ **Dynamic Peer** — *Use this if the VPN Peer is using some dynamic means of getting a public address (DHCP, PPPoE, etc)*

○ **Mobile Peer** — *Use this if the VPN Peer will be a Software VPN client running on a Computer*

Using the ‘Custom Setup’ VPN Configuration Wizard (*Continued…*)

5) Specify the remote VPN Peer’s private network that will communicate with the local private network.

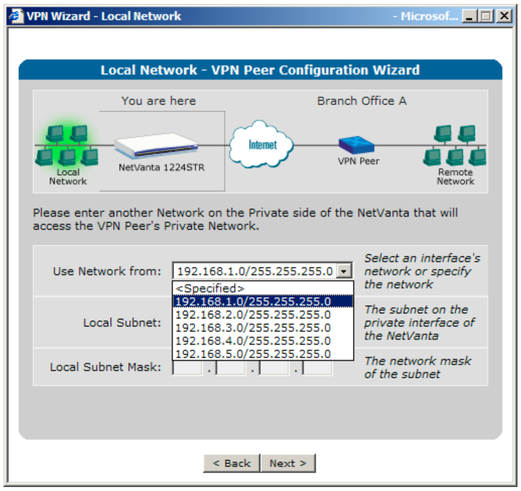


Please enter the VPN Peer's Private network that will communicate with the NetVanta's Private Network.

Remote Subnet: 172 . 16 . 200 . 0 — *This is the Subnet on the private interface of the Remote Router*

Remote Subnet Mask: 255 . 255 . 255 . 0 — *This is the network mask of the subnet above*

6) Select or specify the local private network that will access the remote VPN Peer’s private network.



Please enter another Network on the Private side of the NetVanta that will access the VPN Peer's Private Network.

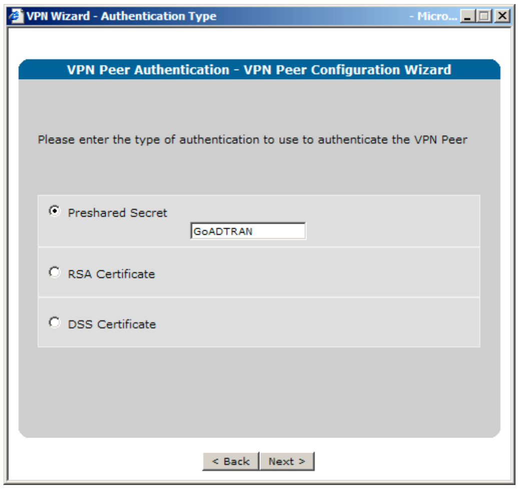
Use Network from: 192.168.1.0/255.255.255.0 — *Select an interface's network or specify the network*

<Specified>
192.168.1.0/255.255.255.0
192.168.2.0/255.255.255.0
192.168.3.0/255.255.255.0
192.168.4.0/255.255.255.0
192.168.5.0/255.255.255.0

Local Subnet: — *The subnet on the private interface of the NetVanta*

Local Subnet Mask: . . . — *The network mask of the subnet*

7) Select the type of authentication to use to authenticate the VPN Peer.


VPN Wizard - Authentication Type - Micro...
VPN Peer Authentication - VPN Peer Configuration Wizard
< Back
Next >

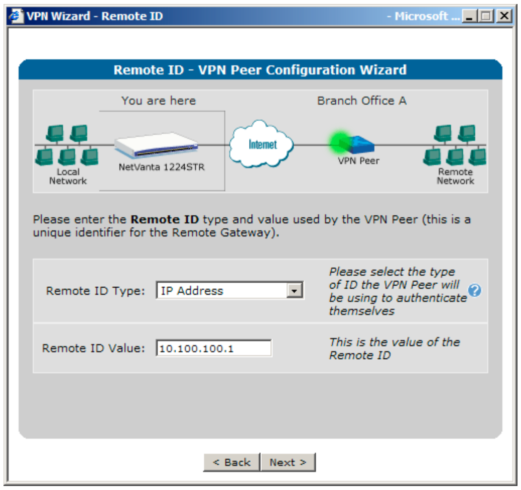
Please enter the type of authentication to use to authenticate the VPN Peer

● Preshared Secret GoADTRAN

○ RSA Certificate

○ DSS Certificate

8) Enter the Remote ID type and value used by the VPN Peer.



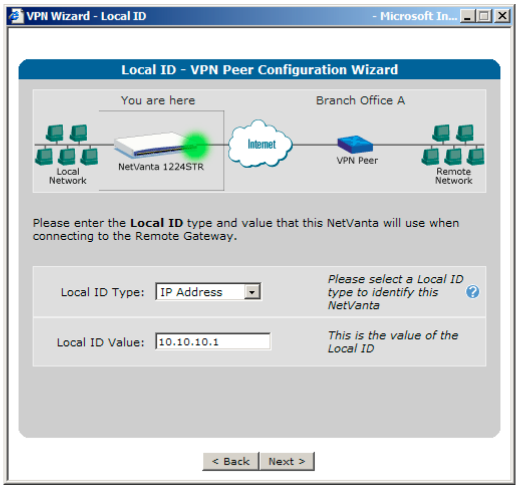
Please enter the **Remote ID** type and value used by the VPN Peer (this is a unique identifier for the Remote Gateway).

Remote ID Type: IP Address — *Please select the type of ID the VPN Peer will be using to authenticate themselves*

Remote ID Value: 10.100.100.1 — *This is the value of the Remote ID*

Using the ‘Custom Setup’ VPN Configuration Wizard (*Continued…*)

9) Enter the Local ID type and value that this NetVanta will use when connecting to the Remote Gateway.

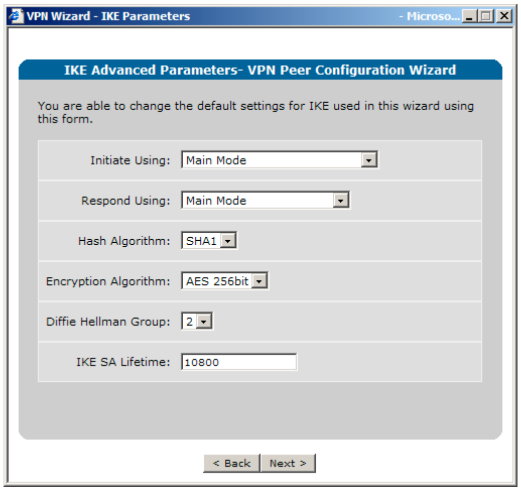


Local ID - VPN Peer Configuration Wizard

Please enter the **Local ID** type and value that this NetVanta will use when connecting to the Remote Gateway.

Local ID Type:	IP Address	*Please select a Local ID type to identify this NetVanta*
Local ID Value:	10.10.10.1	*This is the value of the Local ID*

10) Set desired IKE policy parameters for this VPN policy.

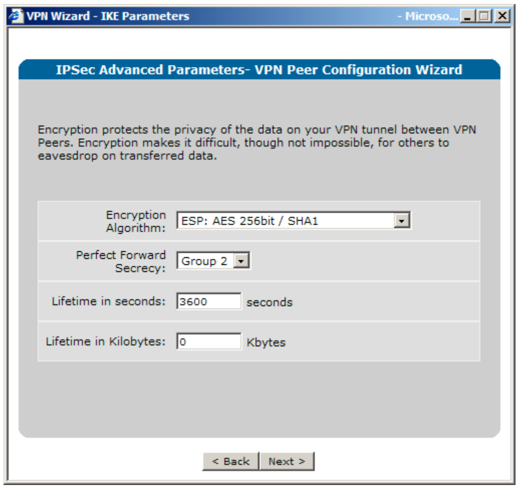


IKE Advanced Parameters- VPN Peer Configuration Wizard

You are able to change the default settings for IKE used in this wizard using this form.

Initiate Using:	Main Mode
Respond Using:	Main Mode
Hash Algorithm:	SHA1
Encryption Algorithm:	AES 256bit
Diffie Hellman Group:	2
IKE SA Lifetime:	10800

11) Set desired IPSec policy parameters for this VPN policy.

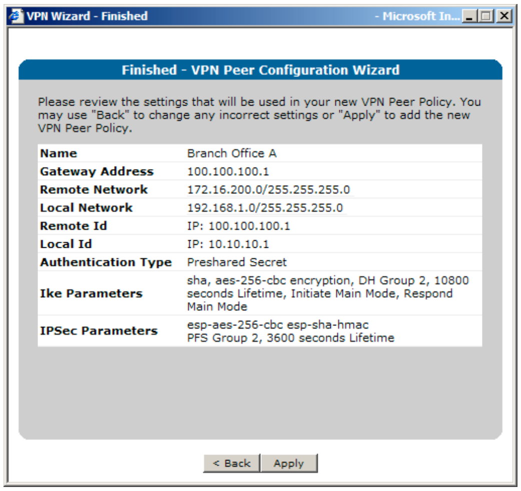


IPSec Advanced Parameters- VPN Peer Configuration Wizard

Encryption protects the privacy of the data on your VPN tunnel between VPN Peers. Encryption makes it difficult, though not impossible, for others to eavesdrop on transferred data.

Encryption Algorithm:	ESP: AES 256bit / SHA1	
Perfect Forward Secrecy:	Group 2	
Lifetime in seconds:	3600	seconds
Lifetime in Kilobytes:	0	Kbytes

12) Review the settings for your new VPN Peer policy. Click the Back button if you wish to make any changes. Click Apply if you wish to add the new VPN Peer policy.



Finished - VPN Peer Configuration Wizard

Please review the settings that will be used in your new VPN Peer Policy. You may use "Back" to change any incorrect settings or "Apply" to add the new VPN Peer Policy.

Name	Branch Office A
Gateway Address	100.100.100.1
Remote Network	172.16.200.0/255.255.255.0
Local Network	192.168.1.0/255.255.255.0
Remote Id	IP: 100.100.100.1
Local Id	IP: 10.10.10.1
Authentication Type	Preshared Secret
Ike Parameters	sha, aes-256-cbc encryption, DH Group 2, 10800 seconds Lifetime, Initiate Main Mode, Respond Main Mode
IPSec Parameters	esp-aes-256-cbc esp-sha-hmac PFS Group 2, 3600 seconds Lifetime

The VPN policies will be created and applied to the specified interface based on your selections. The following VPN configuration was created based on the above selections:

```
   ip crypto
       :
   crypto ike policy 100
     initiate main
     respond main
     local-id address 10.10.10.1
     peer 100.100.100.1
     attribute 1
       encryption aes-256-cbc
       authentication pre-share
       group 2
       lifetime 10800
       :
   crypto ike remote-id address 100.100.100.1 preshared-key GoADTRAN ike-policy 100
    crypto map VPN 10 no-mode-config no-xauth
       :
   crypto ipsec transform-set esp-aes-256-cbc-esp-sha-hmac esp-aes-256-cbc esp-sha-hmac
       :
   crypto map VPN 10 ipsec-ike
     description Branch Office A
     match address VPN-10-vpn-selectors1
     set peer 100.100.100.1
     set transform-set esp-aes-256-cbc-esp-sha-hmac
     set security-association lifetime seconds 3600
     set pfs group2
     ike-policy 100
       :
** ip access-list standard wizard-ics
     remark Internet Connection Sharing
     permit any
       :
** ip access-list extended self
     remark Traffic to NetVanta
     permit ip any  any    log
       :
   ip access-list extended VPN-10-vpn-selectors1
     permit ip 192.168.1.0 0.0.0.255  172.16.200.0 0.0.0.255
       :
   ip policy-class Private
     allow list VPN-10-vpn-selectors1
     allow list self self
**   nat source list wizard-ics interface ppp 1 overload
       :
   ip policy-class Public
     allow reverse list VPN-10-vpn-selectors1
**   nat destination list wizard-pfwd-1 address 192.168.3.100
```

```
interface vlan 3
  ip address  192.168.3.1  255.255.255.0
  access-policy Private
     :
interface vlan 4
  ip address  192.168.4.1  255.255.255.0
  access-policy Private
     :
interface vlan 5
  ip address  192.168.5.1  255.255.255.0
  access-policy Private
     :
     :
     :
     :
interface vlan 5
  ip address  192.168.5.1  255.255.255.0
  access-policy Private
     :
interface ppp 1
  ip address  10.10.10.1  255.255.255.252
  access-policy Public
  crypto map VPN
     :
```

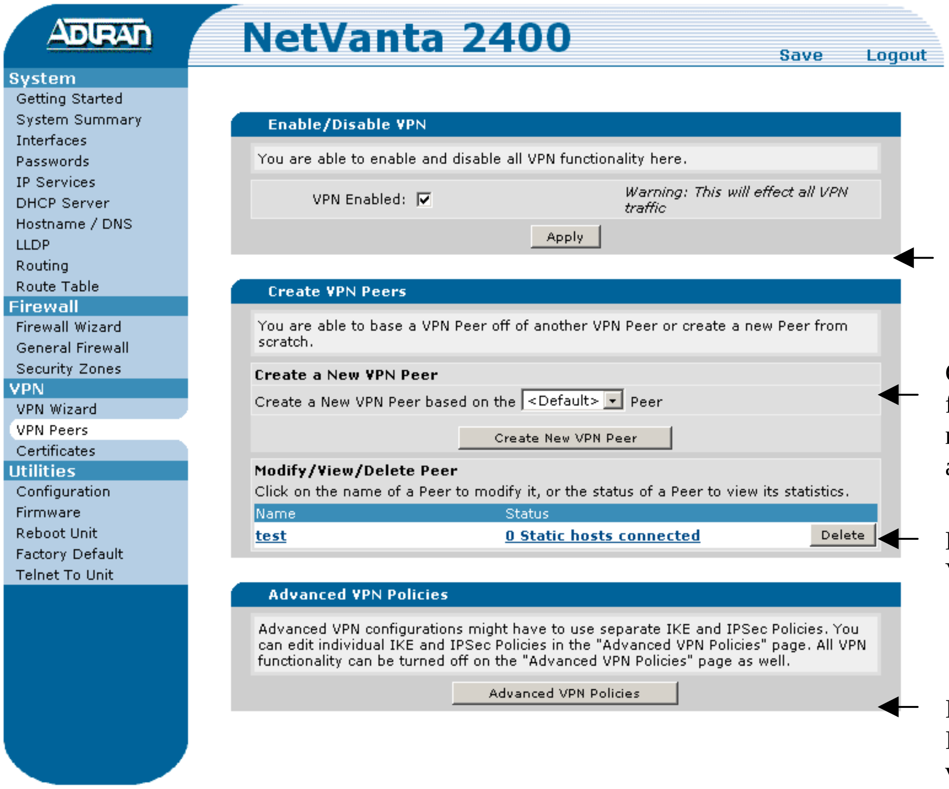
** Partial output displayed*

*** Created by a previous firewall policy*

* Remember to save your configuration to ensure the settings will not be lost after a restart.

VPN Peers Screen

The VPN Peers screen can be used to enable and disable VPN functionality. You can also create, modify, view, and delete VPN Peers from this screen. Individual IKE and IPSec policies can be edited by selecting Advance VPN Policies.



Enable/Disable VPN

You are able to enable and disable all VPN functionality here.

VPN Enabled: ☑ *Warning: This will effect all VPN traffic*

Create VPN Peers

You are able to base a VPN Peer off of another VPN Peer or create a new Peer from scratch.

Create a New VPN Peer

Create a New VPN Peer based on the <Default> Peer

Modify/View/Delete Peer

Click on the name of a Peer to modify it, or the status of a Peer to view its statistics.

Name	Status
test	0 Static hosts connected

Advanced VPN Policies

Advanced VPN configurations might have to use separate IKE and IPSec Policies. You can edit individual IKE and IPSec Policies in the "Advanced VPN Policies" page. All VPN functionality can be turned off on the "Advanced VPN Policies" page as well.

Enable or disable VPN functionality

Create New VPN Peer from scratch or create a new VPN Peer based on an existing VPN Peer

Modify/View/Delete VPN Peer

Individual IKE and IPSec policies can be viewed and edited

Create New VPN Peer

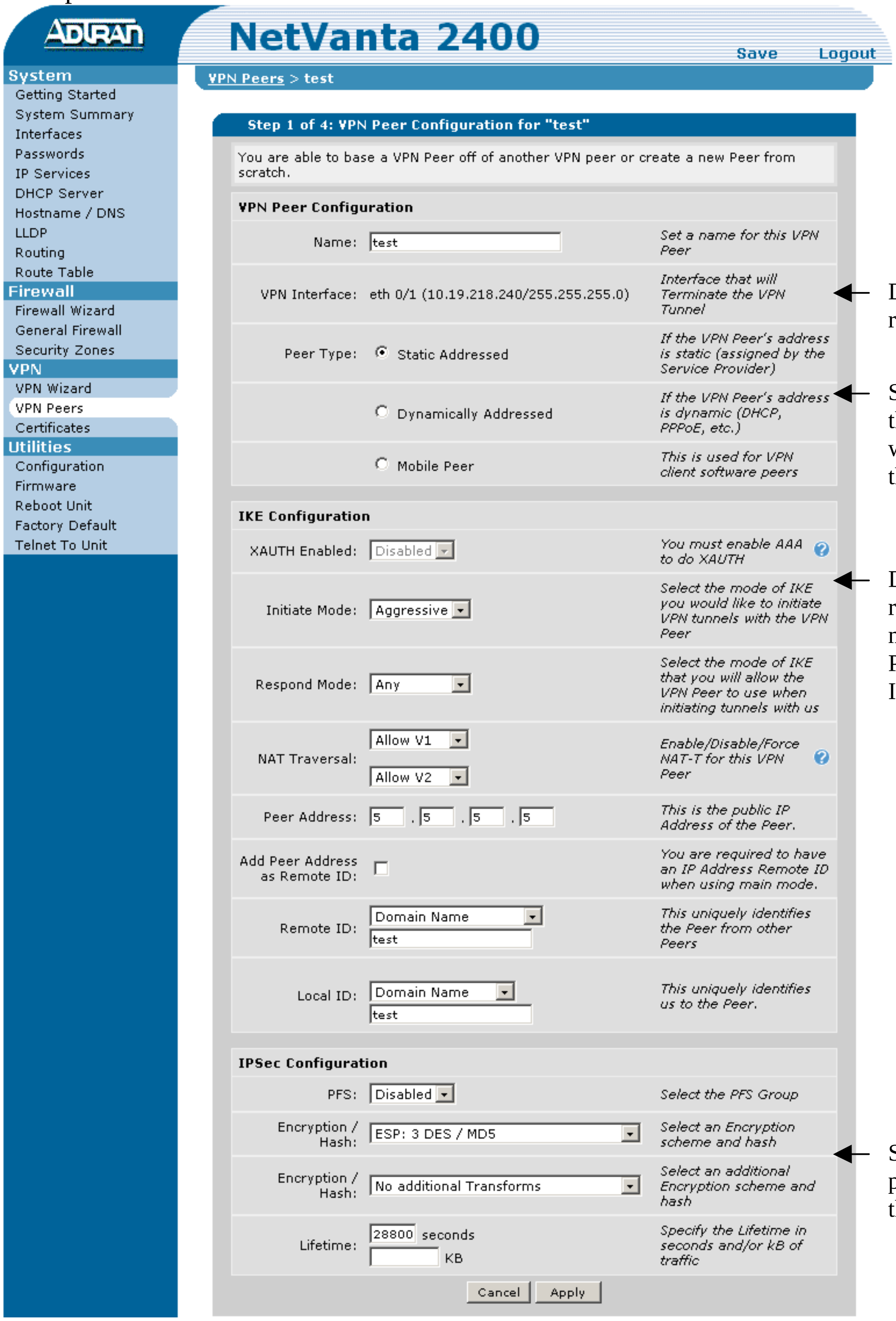
Selecting the Create New VPN Peer button allows you to define a new VPN peer and then assign VPN configuration parameters for that VPN peer.

Advanced VPN Policies

Under Advanced VPN Policies, you can add, modify, or delete individual IKE and IPSec policies. You can also assign Crypto Maps to interfaces and add, modify, or delete individual VPN Remote Ids.

Create New VPN Peer / Edit VPN Peer (*Step 1 of 4*)

Selecting **Create New VPN Peer** or editing an existing VPN peer from the *VPN Peers* screen will display a four step VPN Peer Configuration window for the specific Peer. The individual IKE and IPSec parameters along with VPN traffic selectors can be defined for the selected VPN peer.



Step 1 of 4: VPN Peer Configuration for "test"

You are able to base a VPN Peer off of another VPN peer or create a new Peer from scratch.

VPN Peer Configuration

Name:	test	Set a name for this VPN Peer
VPN Interface:	eth 0/1 (10.19.218.240/255.255.255.0)	Interface that will Terminate the VPN Tunnel
Peer Type:	● Static Addressed	If the VPN Peer's address is static (assigned by the Service Provider)
	○ Dynamically Addressed	If the VPN Peer's address is dynamic (DHCP, PPPoE, etc.)
	○ Mobile Peer	This is used for VPN client software peers

IKE Configuration

XAUTH Enabled:	Disabled	You must enable AAA to do XAUTH
Initiate Mode:	Aggressive	Select the mode of IKE you would like to initiate VPN tunnels with the VPN Peer
Respond Mode:	Any	Select the mode of IKE that you will allow the VPN Peer to use when initiating tunnels with us
NAT Traversal:	Allow V1 Allow V2	Enable/Disable/Force NAT-T for this VPN Peer
Peer Address:	5 . 5 . 5 . 5	This is the public IP Address of the Peer.
Add Peer Address as Remote ID:	□	You are required to have an IP Address Remote ID when using main mode.
Remote ID:	Domain Name test	This uniquely identifies the Peer from other Peers
Local ID:	Domain Name test	This uniquely identifies us to the Peer.

IPSec Configuration

PFS:	Disabled	Select the PFS Group
Encryption / Hash:	ESP: 3 DES / MD5	Select an Encryption scheme and hash
Encryption / Hash:	No additional Transforms	Select an additional Encryption scheme and hash
Lifetime:	28800 seconds KB	Specify the Lifetime in seconds and/or kB of traffic

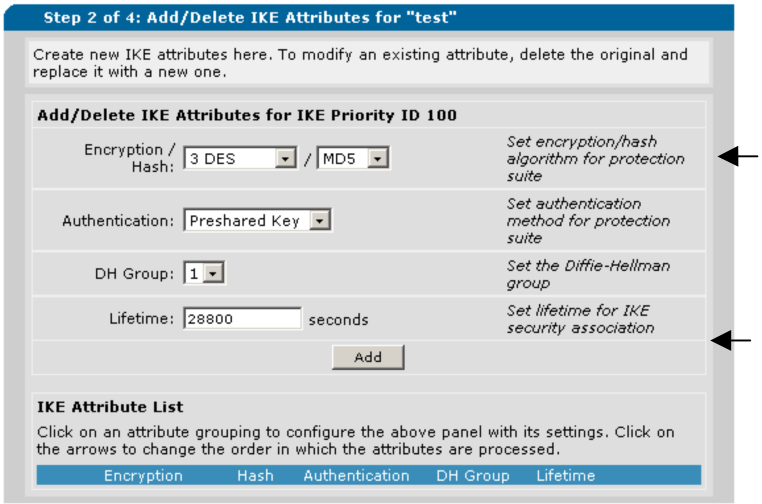
Define description of remote VPN peer

Select the address type the remote VPN peer will use to connect to this NetVanta

Define local and remote ID's, respond mode, and the Preshared key for this IKE policy

Set desired IPSec policy parameters for this VPN policy

Create New VPN Peer / Edit VPN Peer (*Step 2, 3, & 4 of 4*)



Step 2 of 4: Add/Delete IKE Attributes for "test"

Create new IKE attributes here. To modify an existing attribute, delete the original and replace it with a new one.

Add/Delete IKE Attributes for IKE Priority ID 100

Encryption / Hash:	3 DES / MD5	*Set encryption/hash algorithm for protection suite*
Authentication:	Preshared Key	*Set authentication method for protection suite*
DH Group:	1	*Set the Diffie-Hellman group*
Lifetime:	28800 seconds	*Set lifetime for IKE security association*

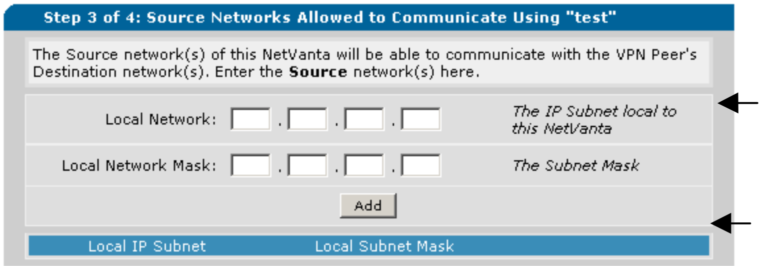
IKE Attribute List

Click on an attribute grouping to configure the above panel with its settings. Click on the arrows to change the order in which the attributes are processed.

Encryption	Hash	Authentication	DH Group	Lifetime

Set desired IKE policy attributes for this VPN policy

Click Add



Step 3 of 4: Source Networks Allowed to Communicate Using "test"

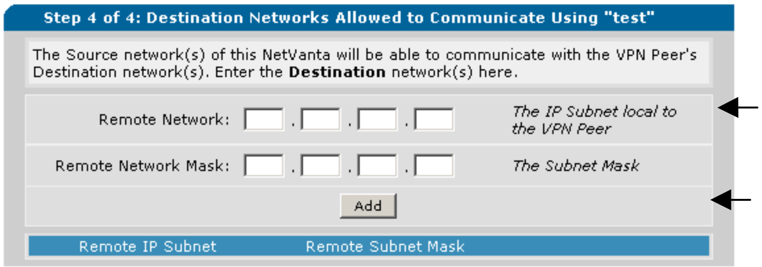
The Source network(s) of this NetVanta will be able to communicate with the VPN Peer's Destination network(s). Enter the **Source** network(s) here.

Local Network:	. . .	*The IP Subnet local to this NetVanta*
Local Network Mask:	. . .	*The Subnet Mask*

Local IP Subnet	Local Subnet Mask

Define the source of the traffic to be protected by this VPN policy.

Click Add



Step 4 of 4: Destination Networks Allowed to Communicate Using "test"

The Source network(s) of this NetVanta will be able to communicate with the VPN Peer's Destination network(s). Enter the **Destination** network(s) here.

Remote Network:	. . .	*The IP Subnet local to the VPN Peer*
Remote Network Mask:	. . .	*The Subnet Mask*

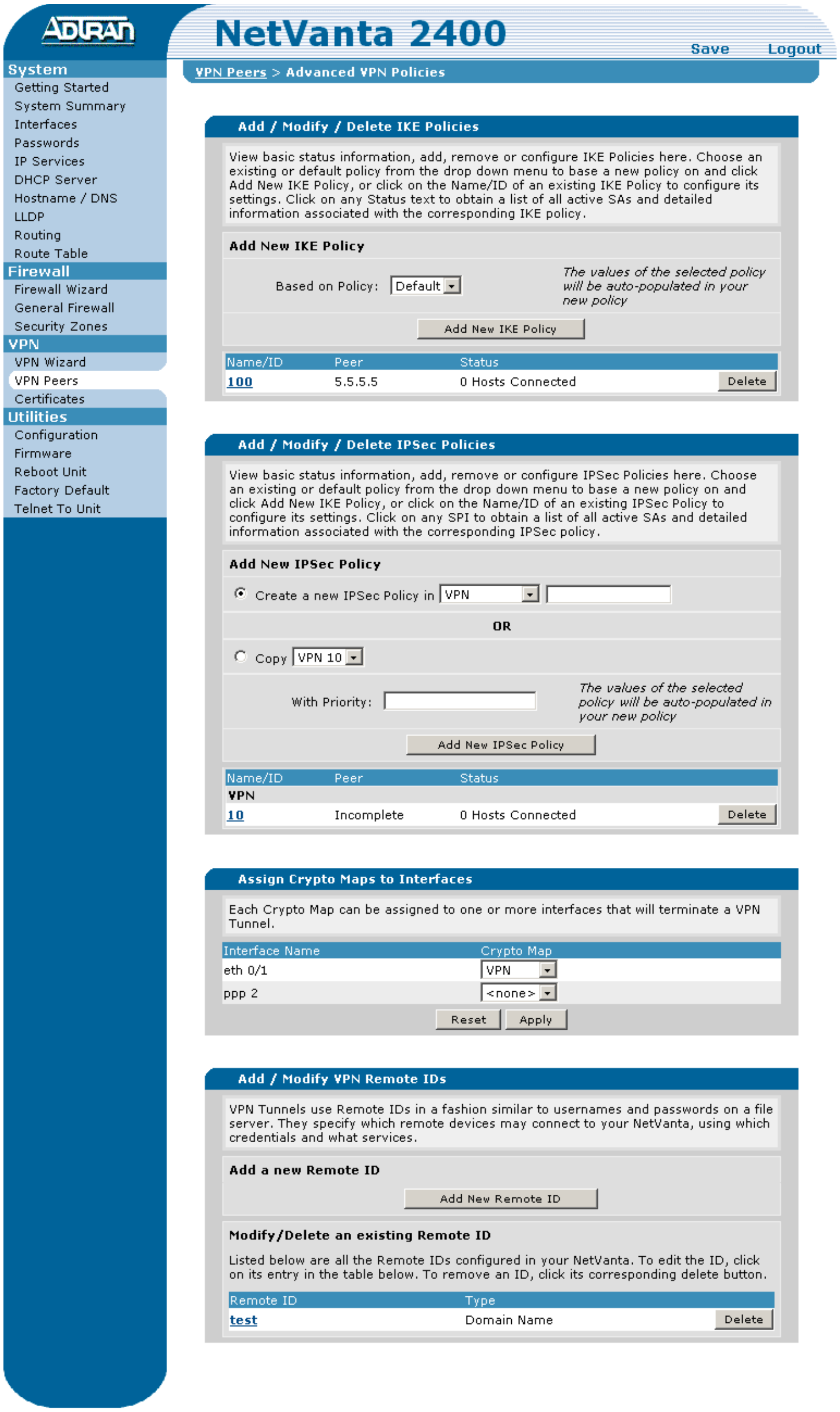
Remote IP Subnet	Remote Subnet Mask

Define the destination of the traffic to be protected by this VPN policy.

Click Add

ADVANCED VPN POLICIES

This area is displayed by selecting **Advanced VPN Policies** from the *VPN Peers* screen. The Advanced VPN Policies screen allows you to add, modify, or delete individual IKE and IPSec policies. You can also assign Crypto Maps to interfaces and add, modify, or delete individual VPN Remote IDs.



VPN Peers > Advanced VPN Policies

Add / Modify / Delete IKE Policies

View basic status information, add, remove or configure IKE Policies here. Choose an existing or default policy from the drop down menu to base a new policy on and click Add New IKE Policy, or click on the Name/ID of an existing IKE Policy to configure its settings. Click on any Status text to obtain a list of all active SAs and detailed information associated with the corresponding IKE policy.

Add New IKE Policy

Based on Policy: Default ▾

The values of the selected policy will be auto-populated in your new policy

Add New IKE Policy

Name/ID	Peer	Status	
100	5.5.5.5	0 Hosts Connected	Delete

Add / Modify / Delete IPSec Policies

View basic status information, add, remove or configure IPSec Policies here. Choose an existing or default policy from the drop down menu to base a new policy on and click Add New IKE Policy, or click on the Name/ID of an existing IPSec Policy to configure its settings. Click on any SPI to obtain a list of all active SAs and detailed information associated with the corresponding IPSec policy.

Add New IPSec Policy

● Create a new IPSec Policy in VPN ▾

OR

○ Copy VPN 10 ▾

With Priority:

The values of the selected policy will be auto-populated in your new policy

Add New IPSec Policy

Name/ID	Peer	Status	
VPN			
10	Incomplete	0 Hosts Connected	Delete

Assign Crypto Maps to Interfaces

Each Crypto Map can be assigned to one or more interfaces that will terminate a VPN Tunnel.

Interface Name	Crypto Map
eth 0/1	VPN ▾
ppp 2	<none> ▾

Reset Apply

Add / Modify VPN Remote IDs

VPN Tunnels use Remote IDs in a fashion similar to usernames and passwords on a file server. They specify which remote devices may connect to your NetVanta, using which credentials and what services.

Add a new Remote ID

Add New Remote ID

Modify/Delete an existing Remote ID

Listed below are all the Remote IDs configured in your NetVanta. To edit the ID, click on its entry in the table below. To remove an ID, click its corresponding delete button.

Remote ID	Type	
test	Domain Name	Delete

← Add / Modify / Delete IKE Policies

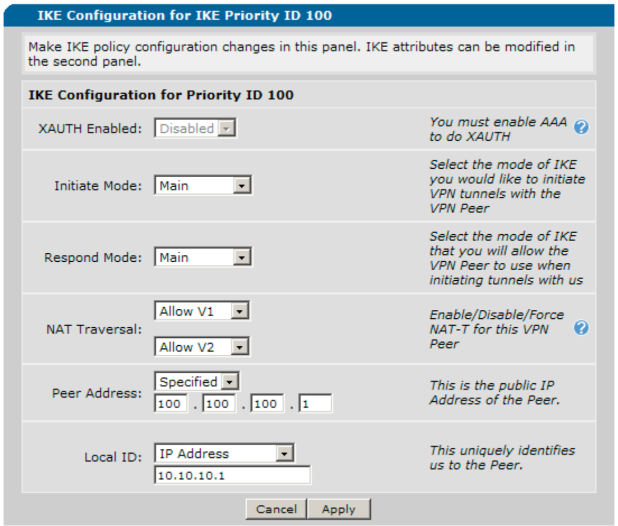
← Add / Modify / Delete IPSec Policies

← Assign Crypto Maps to Interfaces

← Add / Modify VPN Remote IDs

ADVANCED VPN POLICIES - > Add New IKE Policy / Edit IKE Policies

Selecting **Add New IKE Policy** or editing an existing IKE policy from the *VPN Peers - > Advanced VPN Policies* screen will display the IKE Policy configuration screen. The individual IKE policy parameters can be defined here.



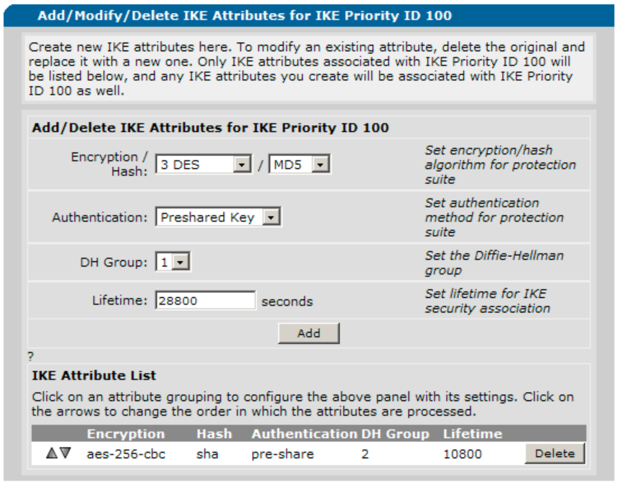
IKE Configuration for IKE Priority ID 100

Make IKE policy configuration changes in this panel. IKE attributes can be modified in the second panel.

IKE Configuration for Priority ID 100

XAUTH Enabled:	Disabled	*You must enable AAA to do XAUTH*
Initiate Mode:	Main	*Select the mode of IKE you would like to initiate VPN tunnels with the VPN Peer*
Respond Mode:	Main	*Select the mode of IKE that you will allow the VPN Peer to use when initiating tunnels with us*
NAT Traversal:	Allow V1 Allow V2	*Enable/Disable/Force NAT-T for this VPN Peer*
Peer Address:	Specified 100 . 100 . 100 . 1	*This is the public IP Address of the Peer.*
Local ID:	IP Address 10.10.10.1	*This uniquely identifies us to the Peer.*

← Configure IKE Policy parameters



Add/Modify/Delete IKE Attributes for IKE Priority ID 100

Create new IKE attributes here. To modify an existing attribute, delete the original and replace it with a new one. Only IKE attributes associated with IKE Priority ID 100 will be listed below, and any IKE attributes you create will be associated with IKE Priority ID 100 as well.

Add/Delete IKE Attributes for IKE Priority ID 100

Encryption / Hash:	3 DES / MD5	*Set encryption/hash algorithm for protection suite*
Authentication:	Preshared Key	*Set authentication method for protection suite*
DH Group:	1	*Set the Diffie-Hellman group*
Lifetime:	28800 seconds	*Set lifetime for IKE security association*

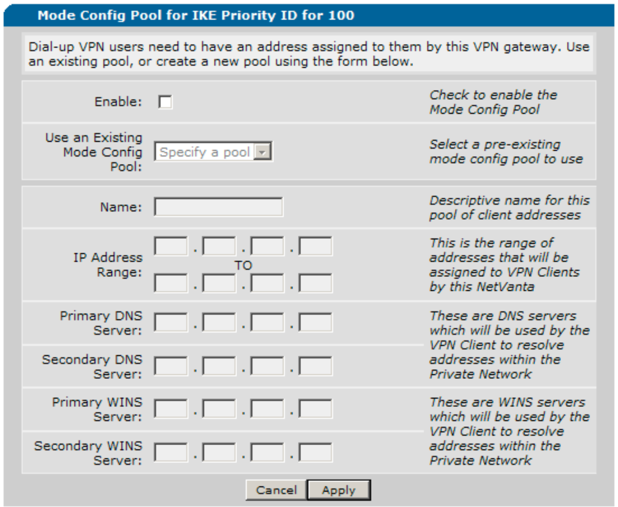
?

IKE Attribute List

Click on an attribute grouping to configure the above panel with its settings. Click on the arrows to change the order in which the attributes are processed.

	Encryption	Hash	Authentication	DH Group	Lifetime	
▲▼	aes-256-cbc	sha	pre-share	2	10800	Delete

← Configure IKE Policy Attributes



Mode Config Pool for IKE Priority ID for 100

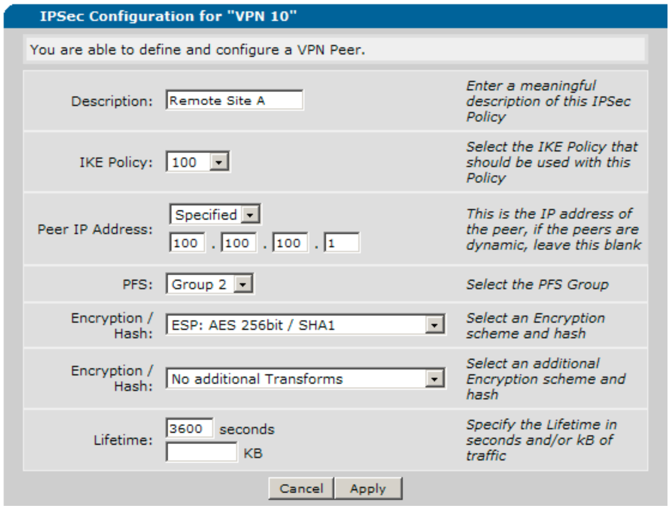
Dial-up VPN users need to have an address assigned to them by this VPN gateway. Use an existing pool, or create a new pool using the form below.

Enable:	□	*Check to enable the Mode Config Pool*
Use an Existing Mode Config Pool:	Specify a pool	*Select a pre-existing mode config pool to use*
Name:		*Descriptive name for this pool of client addresses*
IP Address Range:	. . . TO . . .	*This is the range of addresses that will be assigned to VPN Clients by this NetVanta*
Primary DNS Server:	. . .	*These are DNS servers which will be used by the VPN Client to resolve addresses within the Private Network*
Secondary DNS Server:	. . .	
Primary WINS Server:	. . .	*These are WINS servers which will be used by the VPN Client to resolve addresses within the Private Network*
Secondary WINS Server:	. . .	

← Enable and configure IKE Mode Config to allow a remote host running a VPN client (such as the NetVanta VPN Client) to acquire a virtual IP address when communicating with a VPN gateway.

ADVANCED VPN POLICIES - > Add New IPSec Policy / Edit IPSec Policies

Selecting **Add New IPSec Policy** or editing an existing IPSec policy from the *VPN Peers - > Advanced VPN Policies* screen will display the IPSec Policy configuration screen. The individual IPSec policy parameters can be defined here.

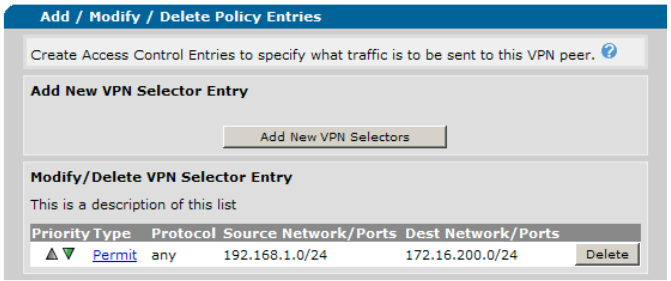


IPSec Configuration for "VPN 10"

You are able to define and configure a VPN Peer.

Description:	Remote Site A	*Enter a meaningful description of this IPSec Policy*
IKE Policy:	100	*Select the IKE Policy that should be used with this Policy*
Peer IP Address:	Specified 100 . 100 . 100 . 1	*This is the IP address of the peer, if the peers are dynamic, leave this blank*
PFS:	Group 2	*Select the PFS Group*
Encryption / Hash:	ESP: AES 256bit / SHA1	*Select an Encryption scheme and hash*
Encryption / Hash:	No additional Transforms	*Select an additional Encryption scheme and hash*
Lifetime:	3600 seconds KB	*Specify the Lifetime in seconds and/or kB of traffic*

Configure IPSec Policy parameters



Add / Modify / Delete Policy Entries

Create Access Control Entries to specify what traffic is to be sent to this VPN peer.

Add New VPN Selector Entry

Modify/Delete VPN Selector Entry

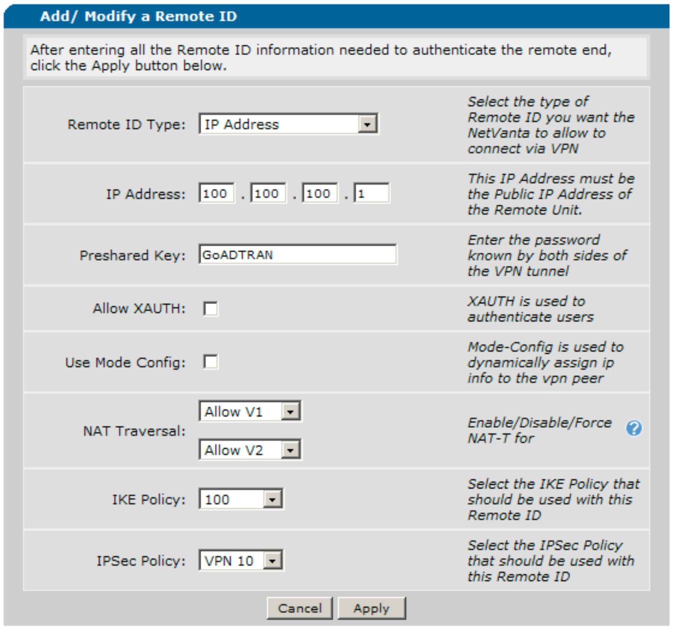
This is a description of this list

Priority	Type	Protocol	Source Network/Ports	Dest Network/Ports	
▲▼	Permit	any	192.168.1.0/24	172.16.200.0/24	Delete

Create new VPN selectors to define the traffic to be protected by this VPN policy. The selectors are read from top down.

ADVANCED VPN POLICIES - > Add New Remote ID / Edit Remote ID

Selecting **Add New Remote ID** or editing an existing Remote ID from the *VPN Peers - > Advanced VPN Policies* screen will display the Remote ID configuration screen. The Remote ID type, Preshared key, IKE Policy and IPSec policy are specified here.



Add/ Modify a Remote ID

After entering all the Remote ID information needed to authenticate the remote end, click the Apply button below.

Remote ID Type:	IP Address	*Select the type of Remote ID you want the NetVanta to allow to connect via VPN*
IP Address:	100 . 100 . 100 . 1	*This IP Address must be the Public IP Address of the Remote Unit.*
Preshared Key:	GoADTRAN	*Enter the password known by both sides of the VPN tunnel*
Allow XAUTH:	□	*XAUTH is used to authenticate users*
Use Mode Config:	□	*Mode-Config is used to dynamically assign ip info to the vpn peer*
NAT Traversal:	Allow V1 Allow V2	*Enable/Disable/Force NAT-T for*
IKE Policy:	100	*Select the IKE Policy that should be used with this Remote ID*
IPSec Policy:	VPN 10	*Select the IPSec Policy that should be used with this Remote ID*

← Select the Remote ID type, ID, and Preshared key the remote VPN peer will use to connect to this NetVanta

← Select the IKE and IPSec policy that will be associated with this Remote ID

Allow XAUTH

Allow eXtended AUTHentication within IKE. This is an Authentication method for remote users which extends existing IKE authentication methods using widely deployed legacy authentication methods such as RADIUS, SecurID, and One Time Passwords.

Use Mode Config

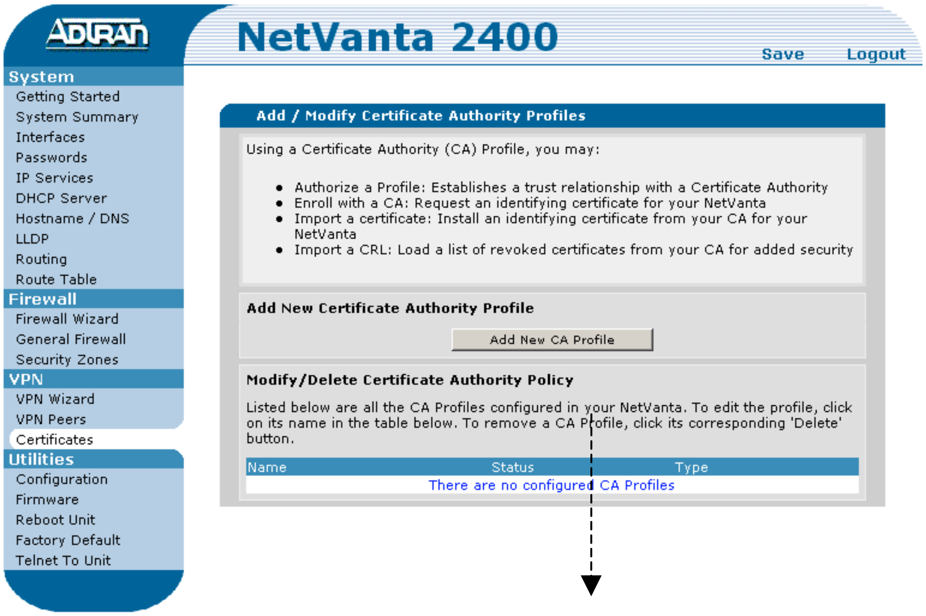
IKE Mode Config allows a remote host running a VPN client (such as the NetVanta VPN Client) to acquire a virtual IP address when communicating with a VPN gateway. The remote host requests an address, and optionally a DNS/WINS server address from the internal network of the VPN gateway. IKE Mode Config parameters can be defined by editing an existing IKE policy under Advanced VPN Polices.

Certificates

The Certificates screen can be used to add, modify, or delete Certificate Authority profiles and policies.

Configure a New Certificate Authority (CA) Profile

Selecting the **Add New CA Profile** button initiates the creation and configuration of Certificate Authority profile. You will be taken through a four-step process of creating the CA profile, loading the CA's certificate, requesting a self-certificate, and importing the self-certificate received from the Certificate Authority.



Add / Modify Certificate Authority Profiles

Using a Certificate Authority (CA) Profile, you may:

- Authorize a Profile: Establishes a trust relationship with a Certificate Authority
- Enroll with a CA: Request an identifying certificate for your NetVanta
- Import a certificate: Install an identifying certificate from your CA for your NetVanta
- Import a CRL: Load a list of revoked certificates from your CA for added security

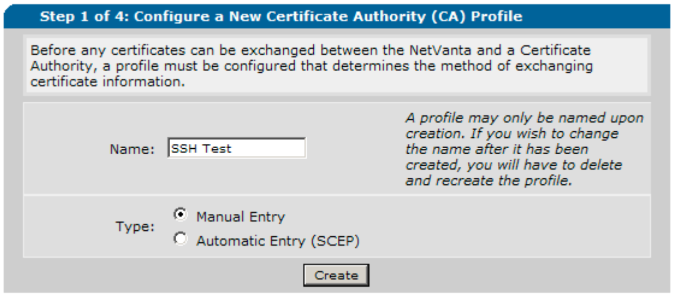
Add New Certificate Authority Profile

Modify/Delete Certificate Authority Policy

Listed below are all the CA Profiles configured in your NetVanta. To edit the profile, click on its name in the table below. To remove a CA Profile, click its corresponding 'Delete' button.

Name	Status	Type
There are no configured CA Profiles		

Add new CA Profile



Step 1 of 4: Configure a New Certificate Authority (CA) Profile

Before any certificates can be exchanged between the NetVanta and a Certificate Authority, a profile must be configured that determines the method of exchanging certificate information.

Name: SSH Test

A profile may only be named upon creation. If you wish to change the name after it has been created, you will have to delete and recreate the profile.

Type: ● Manual Entry
○ Automatic Entry (SCEP)

Name the New CA

Step 1

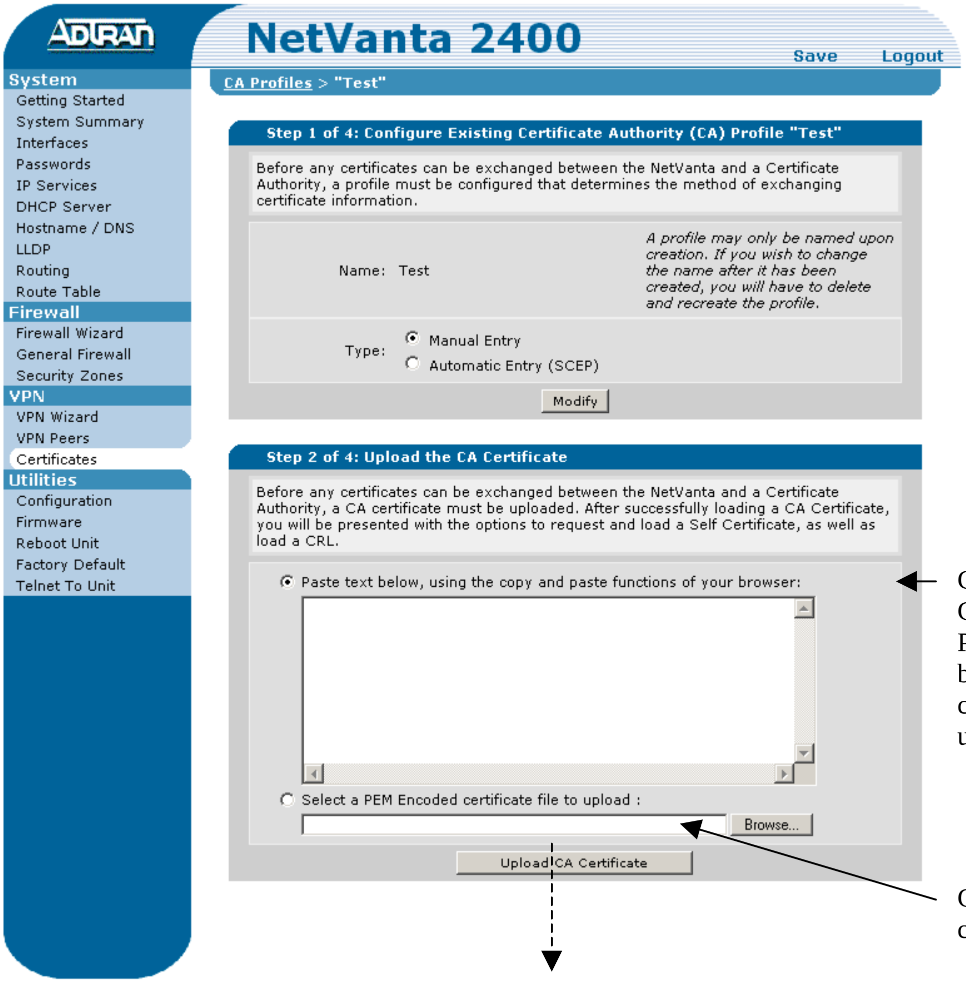
Select the CA enrollment method

Manual Entry Use cut and paste to obtain the CA's certificate, request a self certificate, and import the self Certificate received from the Certificate Authority.

Automatic Entry (SCEP) (Simple Certificate Enrollment Protocol) Requests are sent via SCEP. Using SCEP, the NetVanta will load the CA certificate, issue a self certificate request, and poll for the self certificate.

Upload the CA Certificate

Before any certificates can be exchanged between the NetVanta and Certificate Authority, a CA certificate must be uploaded.



CA Profiles > "Test"

Step 1 of 4: Configure Existing Certificate Authority (CA) Profile "Test"

Before any certificates can be exchanged between the NetVanta and a Certificate Authority, a profile must be configured that determines the method of exchanging certificate information.

Name: Test

A profile may only be named upon creation. If you wish to change the name after it has been created, you will have to delete and recreate the profile.

Type: ● Manual Entry
○ Automatic Entry (SCEP)

Modify

Step 2 of 4: Upload the CA Certificate

Before any certificates can be exchanged between the NetVanta and a Certificate Authority, a CA certificate must be uploaded. After successfully loading a CA Certificate, you will be presented with the options to request and load a Self Certificate, as well as load a CRL.

● Paste text below, using the copy and paste functions of your browser:

○ Select a PEM Encoded certificate file to upload :

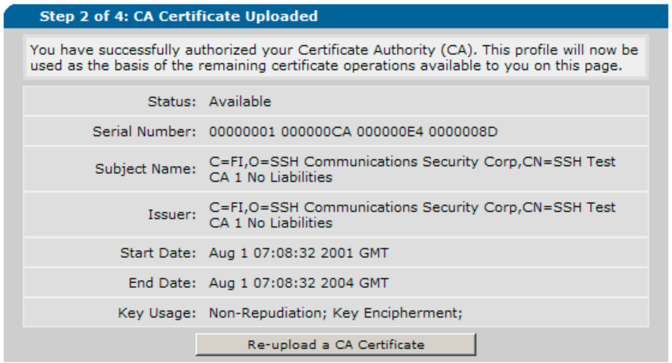
Browse...

Upload CA Certificate

Step 2

Cut and Paste the CA’s certificate in PEM format here or browse to select certificate file to upload

Click to upload CA certificate



Step 2 of 4: CA Certificate Uploaded

You have successfully authorized your Certificate Authority (CA). This profile will now be used as the basis of the remaining certificate operations available to you on this page.

Status:	Available
Serial Number:	00000001 000000CA 000000E4 0000008D
Subject Name:	C=FI,O=SSH Communications Security Corp,CN=SSH Test CA 1 No Liabilities
Issuer:	C=FI,O=SSH Communications Security Corp,CN=SSH Test CA 1 No Liabilities
Start Date:	Aug 1 07:08:32 2001 GMT
End Date:	Aug 1 07:08:32 2004 GMT
Key Usage:	Non-Repudiation; Key Encipherment;

Re-upload a CA Certificate

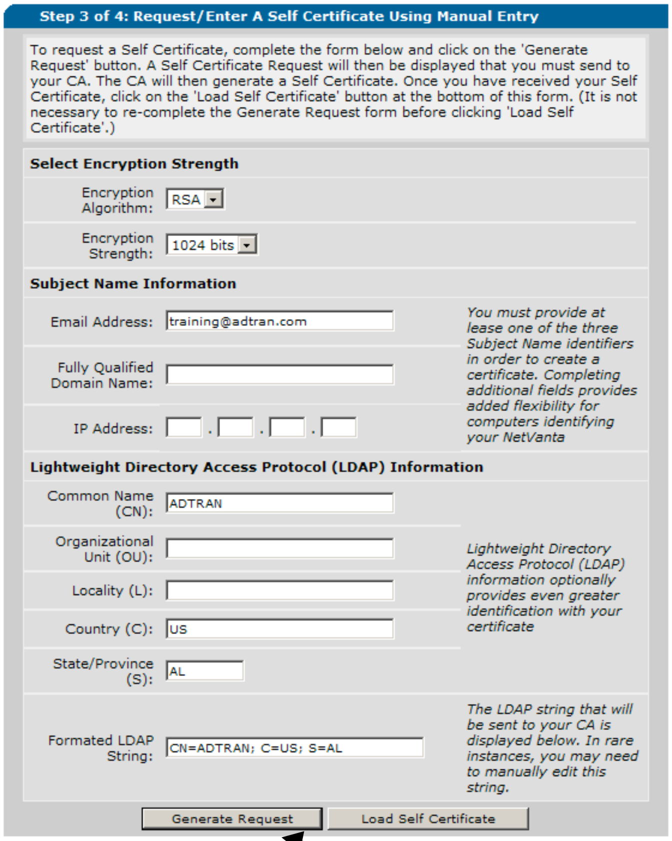
This screen displays if you were successful in uploading the CA’s certificate

PEM: Privacy Enhanced Mail

Request a Self Certificate from CA

To request a Self Certificate, complete the form and then click on the ‘Generate Request’ button. A Self Certificate Request will display that you must send to the CA.

Step 3



Step 3 of 4: Request/Enter A Self Certificate Using Manual Entry

To request a Self Certificate, complete the form below and click on the 'Generate Request' button. A Self Certificate Request will then be displayed that you must send to your CA. The CA will then generate a Self Certificate. Once you have received your Self Certificate, click on the 'Load Self Certificate' button at the bottom of this form. (It is not necessary to re-complete the Generate Request form before clicking 'Load Self Certificate'.)

Select Encryption Strength

Encryption Algorithm: RSA

Encryption Strength: 1024 bits

Subject Name Information

Email Address: training@adtran.com

Fully Qualified Domain Name:

IP Address: . . .

You must provide at lease one of the three Subject Name identifiers in order to create a certificate. Completing additional fields provides added flexibility for computers identifying your NetVanta

Lightweight Directory Access Protocol (LDAP) Information

Common Name (CN): ADTRAN

Organizational Unit (OU):

Locality (L):

Country (C): US

State/Province (S): AL

Lightweight Directory Access Protocol (LDAP) information optionally provides even greater identification with your certificate

Formated LDAP String: CN=ADTRAN; C=US; S=AL

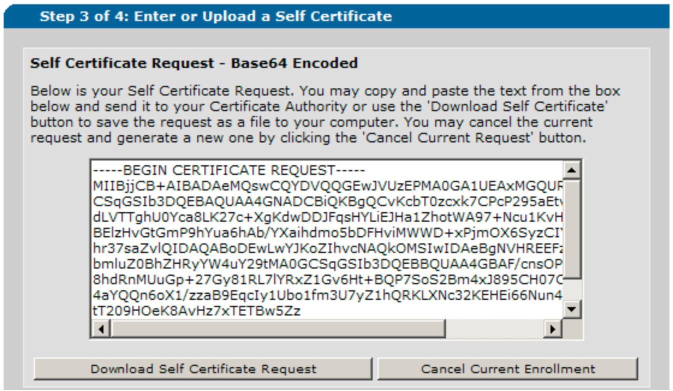
The LDAP string that will be sent to your CA is displayed below. In rare instances, you may need to manually edit this string.

Select Encryption Algorithm and Strength

Select at least one Subject Name Identifier

Define optional LDAP information for greater identification with your certificate

Click to generate Self Certificate Request



Step 3 of 4: Enter or Upload a Self Certificate

Self Certificate Request - Base64 Encoded

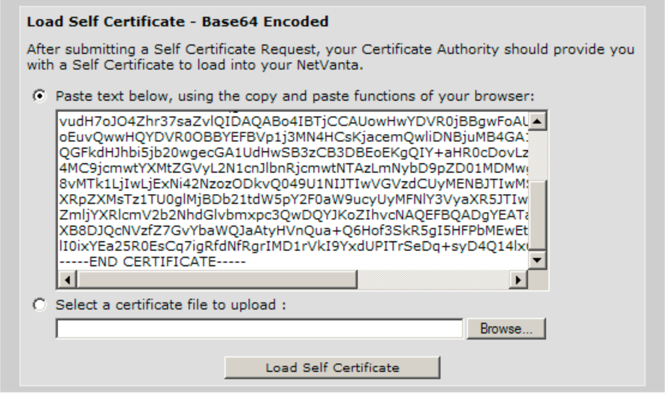
Below is your Self Certificate Request. You may copy and paste the text from the box below and send it to your Certificate Authority or use the 'Download Self Certificate' button to save the request as a file to your computer. You may cancel the current request and generate a new one by clicking the 'Cancel Current Request' button.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBjjCB+AIBADAeMQswCQYDVQQGEwJVUzEPMA0GA1UEAxMGQUR
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvKcbT0zcxk7CPcP295aEtv
dLVTTghU0Yca8LK27c+XgKdwDDJFqsHYLiEJHa1ZhotWA97+Ncu1KvH
BElzHvGtGmP9hYua6hAb/YXaihdmo5bDFHviMWWD+xPjmOX6SyzCI
hr37saZvlQIDAQABoDEwLwYJKoZIhvcNAQkOMSIwIDAeBgNVHREEFz
bmluZ0BhZHRyYW4uY29tMA0GCSqGSIb3DQEBBQUAA4GBAF/cnsOP
8hdRnMUuGp+27Gy81RL7lYRxZ1Gv6Ht+BQP7SoS2Bm4xJ895CH07C
4aYQQn6oX1/zzaB9EqcIy1Ubo1fm3U7yZ1hQRKLXNc32KEHEi66Nun4
tT209HOeK8AvHz7xTETBw5Zz
```

This is your Self Certificate Request. Copy and paste the text in this box and send it to your Certificate Authority

Load Self Certificate from CA

After submitting a Self Certificate Request, your Certificate Authority should provide you with a Self Certificate to load into your NetVanta. Once you have loaded the Self Certificate from your CA, you have completed the loading of your personal certificate.



Load Self Certificate - Base64 Encoded

After submitting a Self Certificate Request, your Certificate Authority should provide you with a Self Certificate to load into your NetVanta.

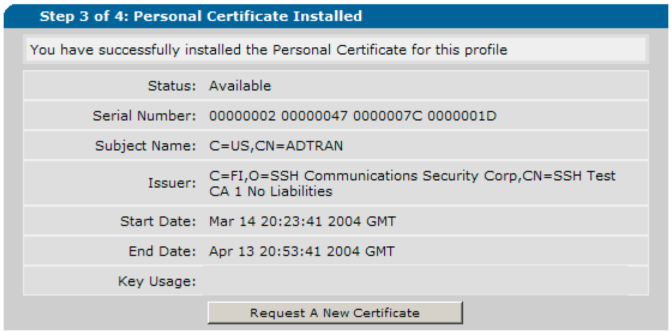
● Paste text below, using the copy and paste functions of your browser:

```
vudH7oJO4Zhr37saZvlQIDAQABo4IBTjCCAUowHwYDVR0jBBgwFoAU
oEuvQwwHQYDVR0OBBYEFBVp1j3MN4HCsKjacemQwliDNBjuMB4GA1
QGFkdHJhbi5jb20wgecGA1UdHwSB3zCB3DBEoEKgQIY+aHR0cDovLz
4MC9jcmwtYXMtZGVyL2N1cnJlbnRjcmwtNTAzLmNybD9pZD01MDMw
8vMTk1LjIwLjExNi42NzozODkvQ049U1NIJTIwVGVzdCUyMENBJTIwM
XRpZXMsTz1TU0glMjBDb21tdW5pY2F0aW9ucyUyMFNlY3VyaXR5JTIw
ZmljYXRlcmV2b2NhdGlvbmxpc3QwDQYJKoZIhvcNAQEFBQADgYEATa
XB8DJQcNVzfZ7GvYbaWQJaAtyHVnQua+Q6Hof3SkR5gI5HFPbMEwEt
lI0ixYEa25R0EsCq7igRfdNfRgrIMD1rVkI9YxdUPITrSeDq+syD4Q14lx
-----END CERTIFICATE-----
```

○ Select a certificate file to upload :

Copy and paste the Self Certificate from your CA into this box

Click to load Self Certificate from CA



Step 3 of 4: Personal Certificate Installed

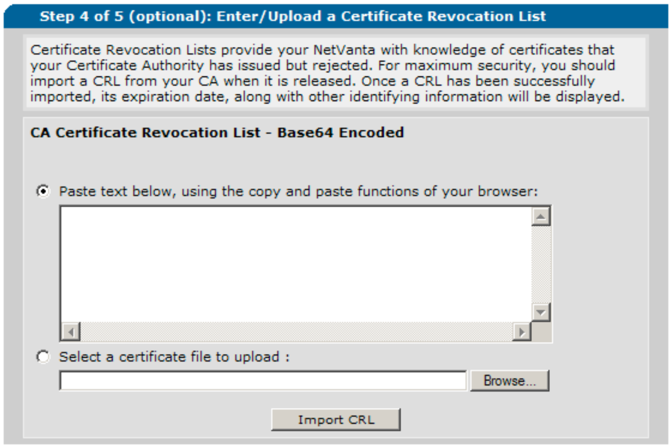
You have successfully installed the Personal Certificate for this profile

Status:	Available
Serial Number:	00000002 00000047 0000007C 0000001D
Subject Name:	C=US,CN=ADTRAN
Issuer:	C=FI,O=SSH Communications Security Corp,CN=SSH Test CA 1 No Liabilities
Start Date:	Mar 14 20:23:41 2004 GMT
End Date:	Apr 13 20:53:41 2004 GMT
Key Usage:	

This screen displays if you were successful in loading your Personal Certificate

Load Certificate Revocation List from CA

Optionally, you can load the Certificate Revocation List from the Certificate Authority.



Step 4 of 5 (optional): Enter/Upload a Certificate Revocation List

Certificate Revocation Lists provide your NetVanta with knowledge of certificates that your Certificate Authority has issued but rejected. For maximum security, you should import a CRL from your CA when it is released. Once a CRL has been successfully imported, its expiration date, along with other identifying information will be displayed.

CA Certificate Revocation List - Base64 Encoded

● Paste text below, using the copy and paste functions of your browser:

○ Select a certificate file to upload :

<u>Step 4</u> *(optional)*

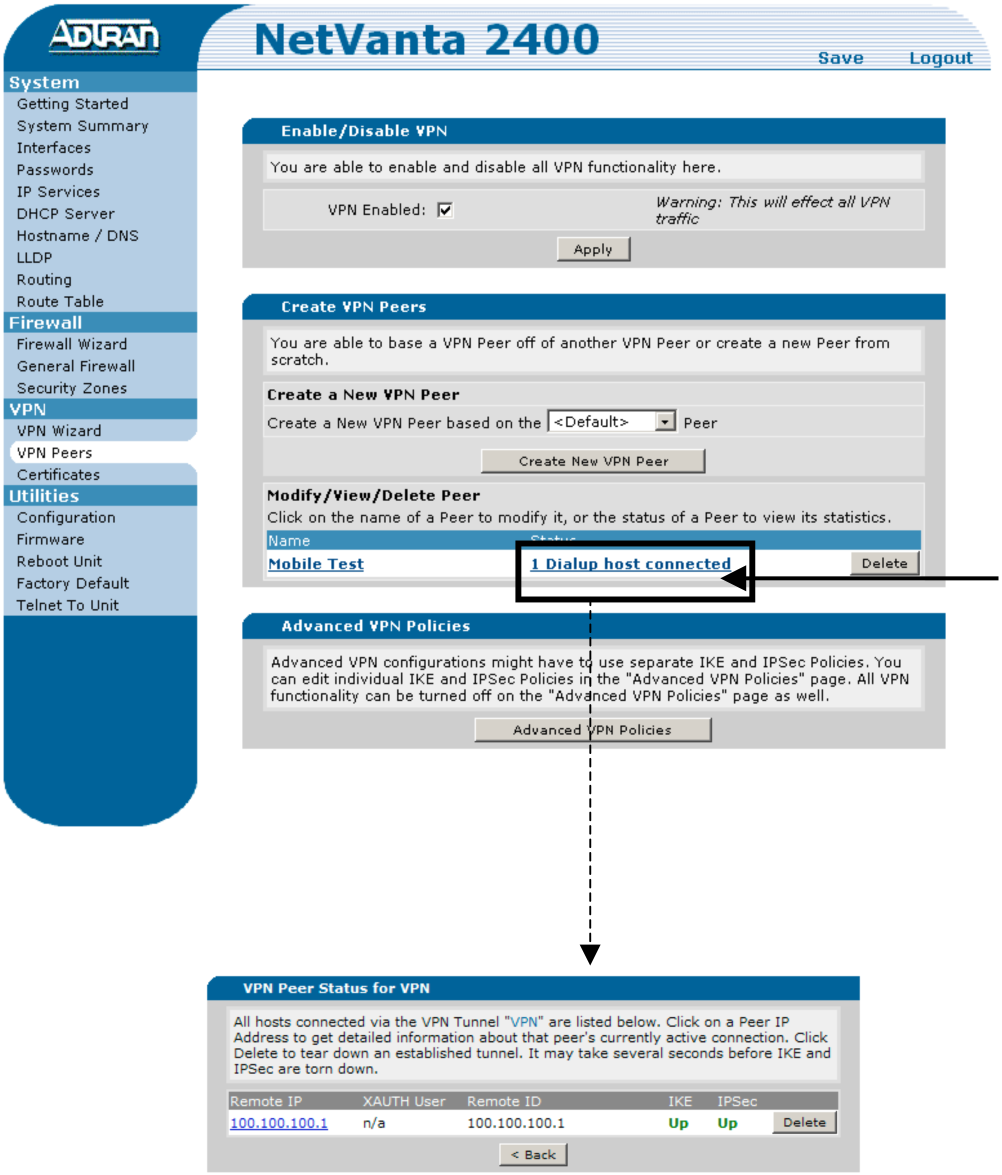
Load the Certificate Revocation List from your Certificate Authority

VPN Troubleshooting with the GUI

The GUI interface of the NetVanta 1224STR provides tools to show the connected VPN peers, display detailed status of the connected VPN peers, and the ability to tear down active VPN tunnels.

Displaying Status of VPN Tunnels

From the *VPN Peers* screen, select the connected VPN peer listed in the **Status** column to display VPN Peer status.



Enable/Disable VPN

You are able to enable and disable all VPN functionality here.

VPN Enabled: ☑ *Warning: This will effect all VPN traffic*

Create VPN Peers

You are able to base a VPN Peer off of another VPN Peer or create a new Peer from scratch.

Create a New VPN Peer

Create a New VPN Peer based on the <Default> Peer

Modify/View/Delete Peer

Click on the name of a Peer to modify it, or the status of a Peer to view its statistics.

Name	Status	
Mobile Test	1 Dialup host connected	Delete

Advanced VPN Policies

Advanced VPN configurations might have to use separate IKE and IPSec Policies. You can edit individual IKE and IPSec Policies in the "Advanced VPN Policies" page. All VPN functionality can be turned off on the "Advanced VPN Policies" page as well.

VPN Peer Status for VPN

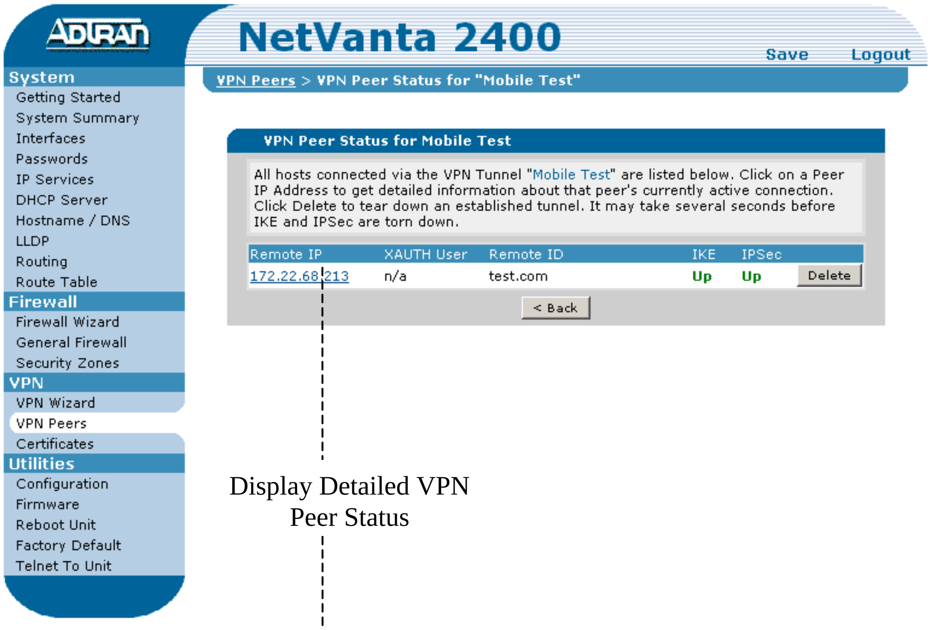
All hosts connected via the VPN Tunnel "VPN" are listed below. Click on a Peer IP Address to get detailed information about that peer's currently active connection. Click Delete to tear down an established tunnel. It may take several seconds before IKE and IPSec are torn down.

Remote IP	XAUTH User	Remote ID	IKE	IPSec	
100.100.100.1	n/a	100.100.100.1	Up	Up	Delete

Display VPN Peer Status

VPN Peer Status

From the VPN Peer Status screen, you can display detailed VPN Peer status and tear down established tunnels.

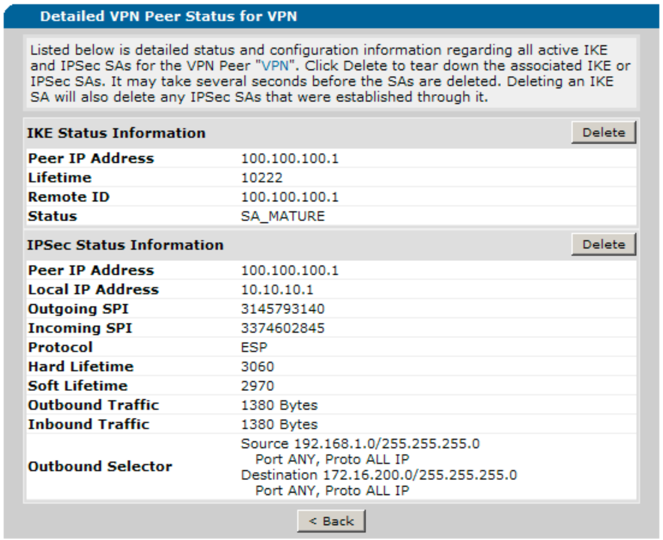


VPN Peer Status for Mobile Test

All hosts connected via the VPN Tunnel "Mobile Test" are listed below. Click on a Peer IP Address to get detailed information about that peer's currently active connection. Click Delete to tear down an established tunnel. It may take several seconds before IKE and IPSec are torn down.

Remote IP	XAUTH User	Remote ID	IKE	IPSec	
172.22.68.213	n/a	test.com	Up	Up	Delete

Display Detailed VPN Peer Status



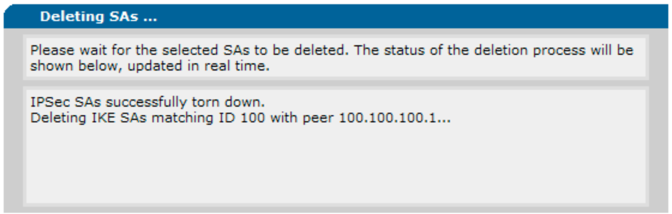
Detailed VPN Peer Status for VPN

Listed below is detailed status and configuration information regarding all active IKE and IPSec SAs for the VPN Peer "VPN". Click Delete to tear down the associated IKE or IPSec SAs. It may take several seconds before the SAs are deleted. Deleting an IKE SA will also delete any IPSec SAs that were established through it.

IKE Status Information	
Peer IP Address	100.100.100.1
Lifetime	10222
Remote ID	100.100.100.1
Status	SA_MATURE

IPSec Status Information	
Peer IP Address	100.100.100.1
Local IP Address	10.10.10.1
Outgoing SPI	3145793140
Incoming SPI	3374602845
Protocol	ESP
Hard Lifetime	3060
Soft Lifetime	2970
Outbound Traffic	1380 Bytes
Inbound Traffic	1380 Bytes
Outbound Selector	Source 192.168.1.0/255.255.255.0 Port ANY, Proto ALL IP Destination 172.16.200.0/255.255.255.0 Port ANY, Proto ALL IP

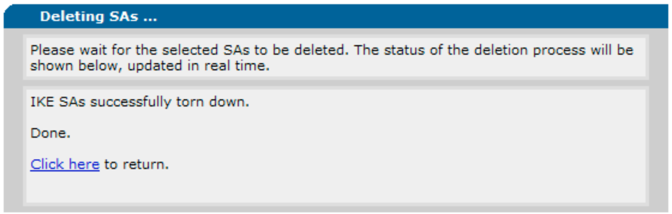
Tear down the established tunnel



Deleting SAs ...

Please wait for the selected SAs to be deleted. The status of the deletion process will be shown below, updated in real time.

IPSec SAs successfully torn down.
Deleting IKE SAs matching ID 100 with peer 100.100.100.1...



Deleting SAs ...

Please wait for the selected SAs to be deleted. The status of the deletion process will be shown below, updated in real time.

IKE SAs successfully torn down.

Done.

Click here to return.