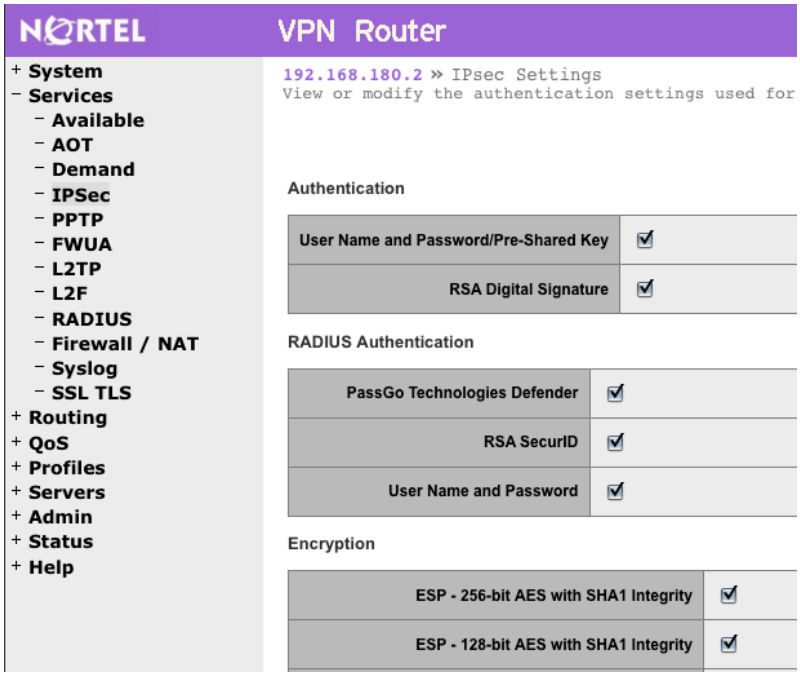
Setting up VPN Tracker with Nortel VPN Routers

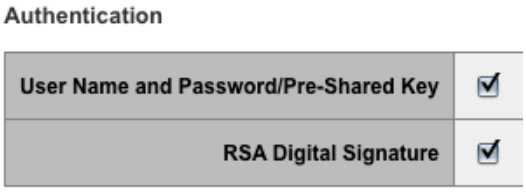


1.Configuring the Nortel VPN Router (Contivity)

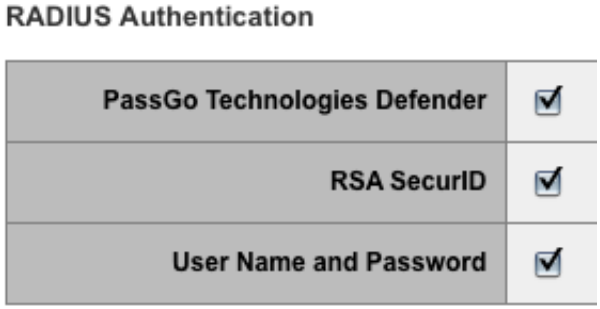
1.1.Configuring the global IPSec settings

You'll need to change the following settings under **Services > IPSec**:

1.1.1. Authentication

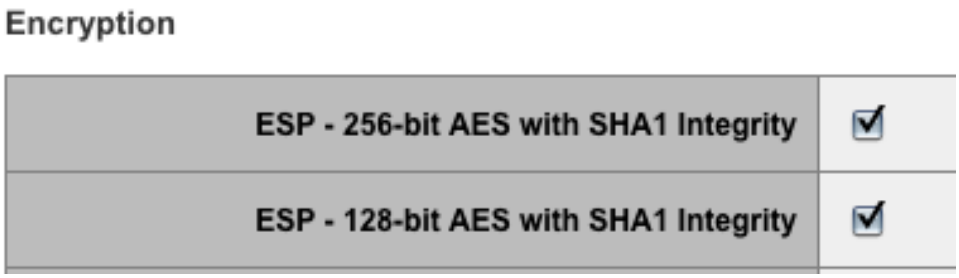


1.1.2. RADIUS Authentication



1.1.3.Encryption

You can use AES 128-bit encryption if you have VPN Tracker 6 Personal and AES 256-bit if you have VPN Tracker 6 Professional or Player. Deactivate all other encryption options.



1.1.4. IKE Encryption and Diffie-Hellman Group

Enable all AES groups

IKE Encryption and Diffie-Hellman Group

56-bit DES with Group 1 (768-bit prime)	☐
Triple DES with Group 2 (1024-bit prime)	☐
Triple DES with Group 7 (ECC 163-bit field)	☐
128-bit AES with Group 5 (1536-bit prime)	☑
128-bit AES with Group 8 (ECC 283-bit field)	☑
128-bit AES with Group 2 (1024-bit prime)	☑
256-bit AES with Group 5 (1536-bit prime)	☑
256-bit AES with Group 8 (ECC 283-bit field)	☑

1.1.5. NAT Traversal

NAT Traversal*

Enabled	☑ User Tunnel ☐ Branch Office Tunnel
Disable Client IKE Source Port Switching	☐
UDP Port	10001

*Changing NAT traversal settings will cause active tunnels to disconnect.

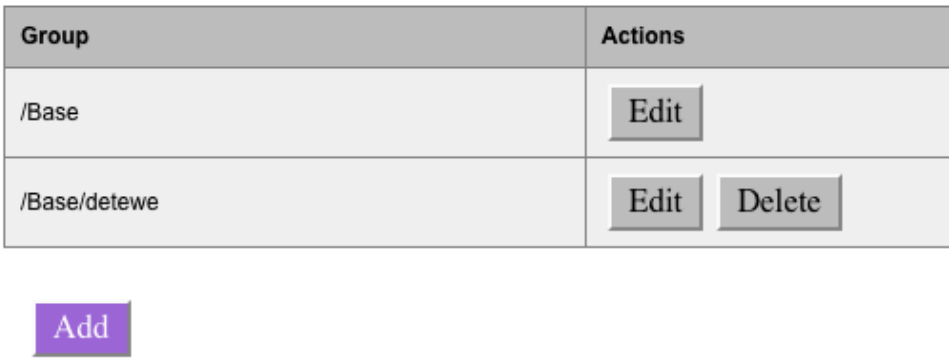
1.1.6. Save your changes

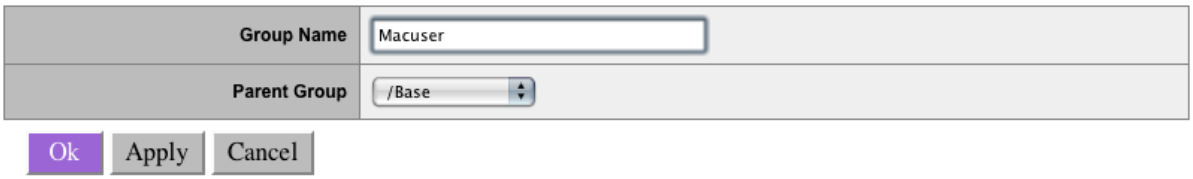
OK Cancel

1.2. Configuring your user groups

1.2.1. Create a user group for your Mac users

Go to **Profiles > Groups** to configure your new group.





Rename your group (e.g. “Macuser”) and click Ok.

You can also configure additional user access options for your group, however those settings aren’t described in this guide.

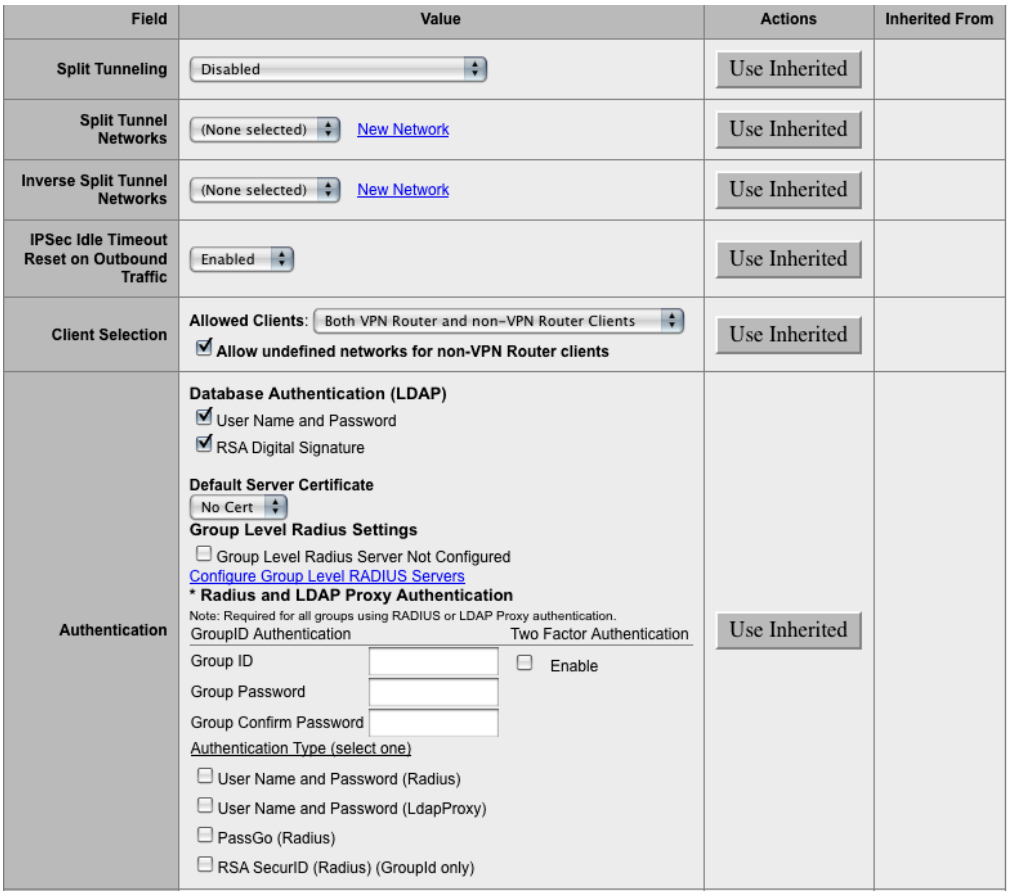
1.2.2. IPSec Settings for your Macuser Group

Go right to the bottom and click the “Configure” button for “All Fields”

You probably won’t need to change any other settings, as the Macuser group will inherit the settings from the “/Base” group.

However: If your “/Base” group isn’t configured correctly, your Mac user group should be configured like this:

Field	Value	Actions	Inherited From
Split Tunneling	Disabled	Use Inherited	
Split Tunnel Networks	(None selected) New Network	Use Inherited	
Inverse Split Tunnel Networks	(None selected) New Network	Use Inherited	
IPSec Idle Timeout Reset on Outbound Traffic	Enabled	Use Inherited	
Client Selection	Allowed Clients: Both VPN Router and non-VPN Router Clients Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	Database Authentication (LDAP) User Name and Password RSA Digital Signature Default Server Certificate No Cert Group Level Radius Settings Group Level Radius Server Not Configured Configure Group Level RADIUS Servers * Radius and LDAP Proxy Authentication Note: Required for all groups using RADIUS or LDAP Proxy authentication. GroupID Authentication / Two Factor Authentication Group ID / Enable Group Password Group Confirm Password Authentication Type (select one) User Name and Password (Radius) User Name and Password (LdapProxy) PassGo (Radius) RSA SecurID (Radius) (GroupId only)	Use Inherited	



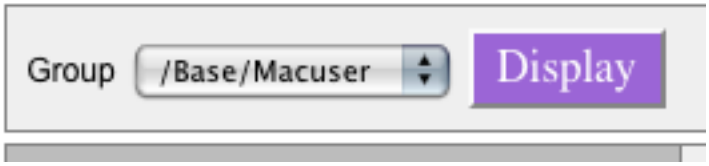
Field	Value	Actions	Inherited From
Split Tunneling	Disabled	Use Inherited	
Split Tunnel Networks	(None selected) New Network	Use Inherited	
Inverse Split Tunnel Networks	(None selected) New Network	Use Inherited	
IPSec Idle Timeout Reset on Outbound Traffic	Enabled	Use Inherited	
Client Selection	Allowed Clients: Both VPN Router and non-VPN Router Clients Allow undefined networks for non-VPN Router clients	Use Inherited	
Authentication	Database Authentication (LDAP) User Name and Password RSA Digital Signature Default Server Certificate No Cert Group Level Radius Settings Group Level Radius Server Not Configured Configure Group Level RADIUS Servers * Radius and LDAP Proxy Authentication Note: Required for all groups using RADIUS or LDAP Proxy authentication. GroupID Authentication / Two Factor Authentication Group ID / Enable Group Password Group Confirm Password Authentication Type (select one) User Name and Password (Radius) User Name and Password (LdapProxy) PassGo (Radius) RSA SecurID (Radius) (GroupId only)	Use Inherited	

You won’t need to enter any additional settings, as you can configure your DNS server etc. directly within VPN Tracker.

1.2.3. Adding users

Go to **Profiles > Users** to add additional users

As your **Group** select ***"/Base/Macuser"*** and then click *Display.* Now you can add additional users.



Enter the user's first and last name. Under "IPsec" you'll also need to set a password for every user.

You'll also need to enter a static IP address for VPN Tracker users.

General

	First	Last
Name	mac	test
Group	/Base/Macuser	

	Static IP Address	Static Subnet Mask
Remote User	192.168.180.99	255.255.255.224

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)	Status
IPsec	mactest	•••••••	•••••••		
PPTP					
L2TP					
L2F					
Firewall User Authentication					

Must Change Password at Next Logon	☐ (Nortel IPSEC Client Only)

(Automatic configuration is currently not supported.)

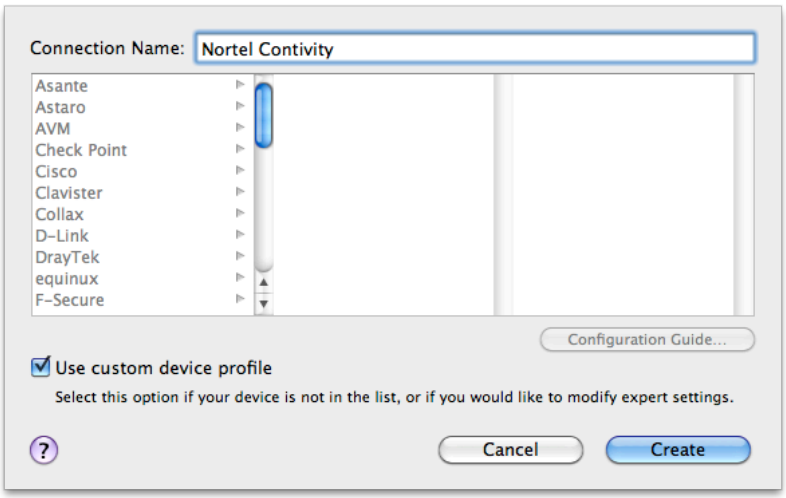
Congratulations! You've finished your Nortel router's configuration.

2. Configuring VPN Tracker

2.1. Creating a new connection

Select **File > New Connection**

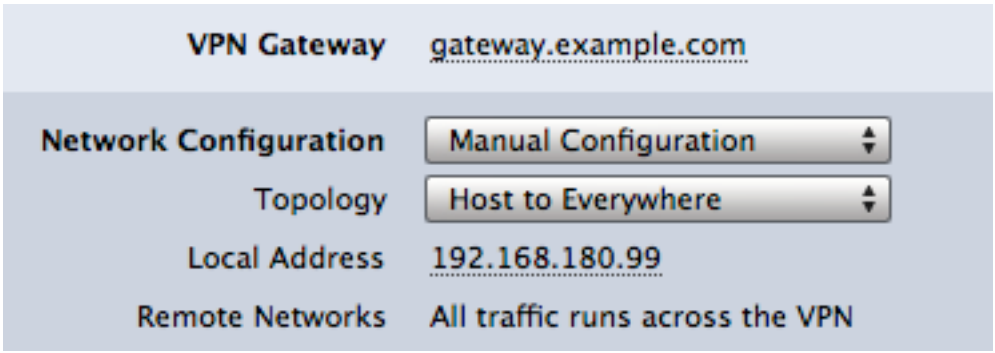
Enter any name for your connection and check the “custom device profile” box at the bottom of the bottom of the window.



2.2. Basic settings

2.2.1. Network settings

Select ***Manual Configuration*** for your Network Configuration.
Depending on your preference, choose between Host to Everywhere or Host to Network.
If you select ***Host to Network*** to enter your remote networks in VPN Tracker.
In this example, we’ll use ***Host to everywhere***.



Enter your Contivitiy’s external IP address in the VPN Gateway field.

As the Local Address, enter the user’s IP address you configured on your VPN router earlier.

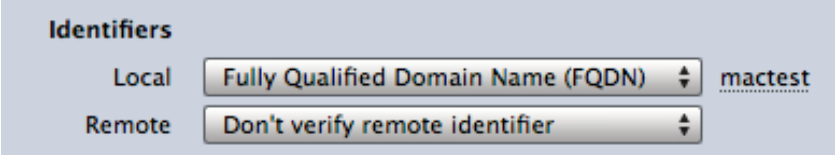
2.2.2. Authentification

Select ***Pre-Shared Key*** for authentication.

2.2.3. Identifier

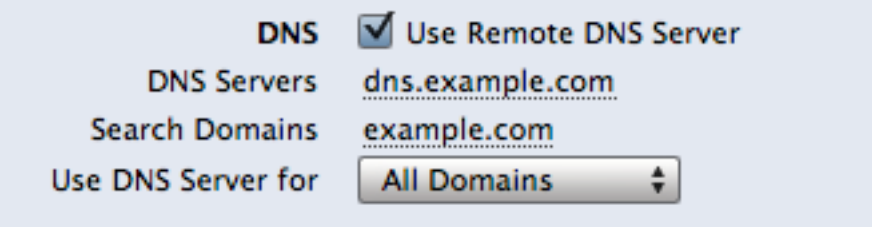
The **Local Identifier type** is ***Fully Qualified Domain Name (FQDN)***. Enter the user's ID.

Set **Remote Identifier** to "Don't verify remote identifier".

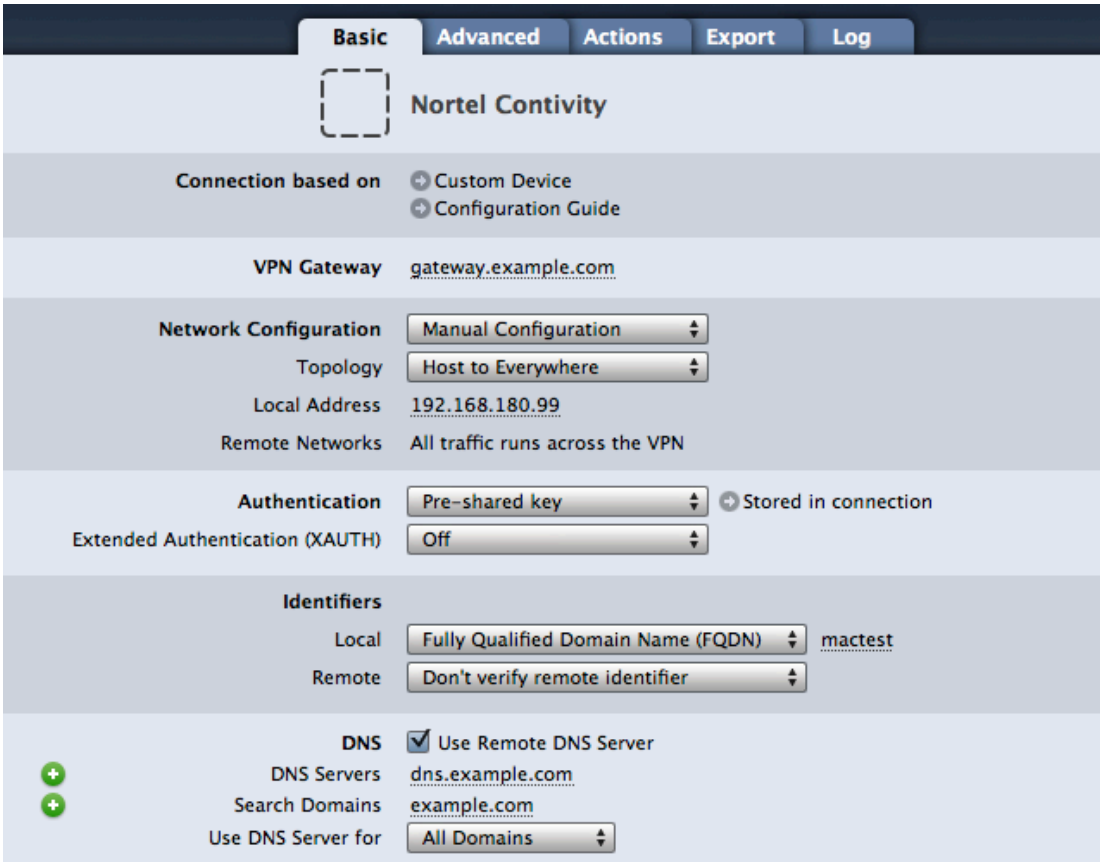


2.2.4. DNS

Enable "Use **Remote DNS-Server"** if required and enter your DNS server address and search domains.

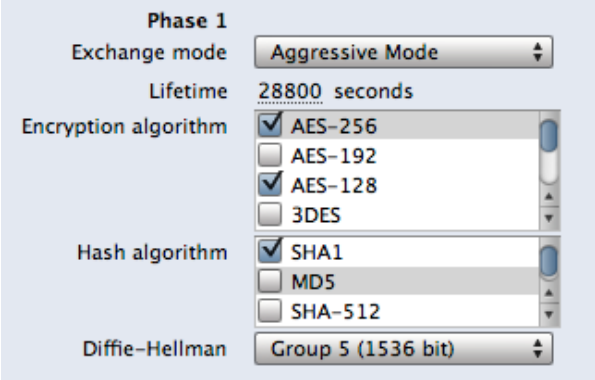


Once you've entered your settings, it should look something like this.
Now head on over to the Advanced tab.



2.3. Advanced Settings

2.3.1. Phase 1

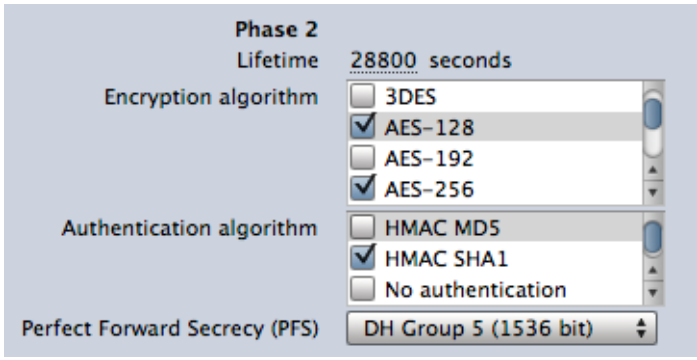


Select ***Aggressive Mode*** as your ***Exchange Mode.***

Deactivate all the Encryption algorithms, except ***AES-128*** & ***AES-256***.

Select the ***SHA1*** Hash algorithm and ***Diffie-Hellman Group 5 (1536 bit).***

2.3.2. Phase 2



Deactivate all the Encryption algorithms, except ***AES-128*** & ***AES-256***.

Select the ***HMAC SHA1*** Authentication algorithm and ***Diffie-Hellman Group 5 (1536 bit).***

Select ***DH Group 5 (1536 bit)*** for **Perfect Forward Secrecy (PFS).**

3. Start your connection

Now you're ready to test your VPN Tunnel!
Click the slider and try to act your network resources.

For more information & tips, refer to VPN Tracker - The Complete Manual, available under Help > Complete Manual.