

# Configuring VPN on the Tadpole M1400

## Supported Features

The VPN client on the Tadpole M1400 is a standards based IPsec VPN client compliant with RFC 2406 for encryption and authentication; RFCs 2407, 2408, 2409, 4109 for key generation and maintenance; RFC 3706 for dead peer detection; RFC's 3947 and 3948 for connection behind NAT devices.

IP Encapsulating Security Payload (ESP) with authentication provide encryption and authentication services, ensuring confidentiality and integrity of data. Confidentiality is provided by a set of encryption algorithms including 3DES, AES 128, AES 192 and AES 256. Integrity/authentication is provided by MD5, SHA-1 and SHA-2. Null Encryption can be negotiated alongside one of the authentication algorithms to enable ESP to operate in a mode similar to IP Authentication Header (AH). Encryption and authentication keys are provided as dynamic keys negotiated via Internet Key Exchange (IKE).

Under IKE, Main Mode (also called Identity Protection Mode) and Aggressive Mode are supported for the generation of ISAKMP Security Associations during Phase 1 negotiations. After Phase 1 a pair of encryption and authentication (excluding Null) algorithms are selected to protect Phase 2 of the negotiation. Phase 2 is conducted using Quick Mode resulting in a pair of IKE Security Associations between the VPN peers, detailing encryption, authentication algorithms and keys for the IP ESP traffic.

Perfect Forward Secrecy (PFS) is provided using a selected Diffie-Hellman group as the source of the key material. PFS ensures that if the keys established in Phase 1 are compromised, the security of the data protected by the Phase 2 keys, the ESP traffic, is not effected.

Dynamic IP Address assignment is supported using Mode Config. XAuth is an extension of Mode Config and will be used to further authenticate the user if it is required by the VPN peer. User authentication using standard username/password mechanism as well as RSA Securid is supported.

In order to be a good VPN neighbour, a Tadpole M1400 will advertise itself as supporting dead peer detection (DPD). A VPN peer which recognises this may send messages to the Tadpole M1400 to check that it is still alive, if so the Tadpole M1400 will respond with an appropriate acknowledgement. The VPN peer can then detect sooner when a connection has failed and perform cleanup and recovery actions.

Connection of a VPN enabled Tadpole M1400 behind a NAT is supported with NAT Traversal (NAT-T). The presence of the NAT is automatically detected by the VPN client and the use of NAT-T is completely transparent.

## Preparing for Configuration

Before commencing with any configuration some preparatory work is required. The following may be needed:

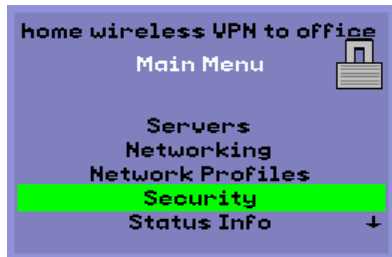
- Tadpole M1400 thin client laptops typically use DHCP to obtain an IP address and to get IP addresses of the Sunray Auth and Firmware servers. In VPN configurations the

Sunray server information is not likely to be available via DHCP. The server addresses can be configured in the *Servers* menu.

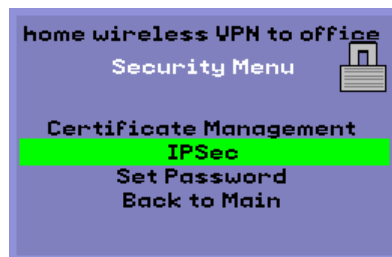
- Is the Tadpole M1400 likely to be behind a NAT? This is not directly configured but some of the configuration options are affected by this. Specifically, the use of Main Mode and Identification via IP Address is not supported with a NAT router. Aggressive mode must be configured when behind a NAT.
- Determine which method of identification is to be used, for example Key Identifier or Email Address and gather the relevant Id values. Eg When connecting to a Cisco VPN concentrator the Key Identifier will be the Group you wish to connect to.
- Determine the pre-shared secret relevant to the identifier previously chosen. Currently, pre-shared secret is the only method of authentication supported.
- Is the user to be separately verified using Xauth?
- Is Aggressive mode to be used during Phase 1? If so, the encryption algorithm, authentication algorithm and PFS (Perfect Forward Secrecy) Group need to be determined.

## Configuring Tadpole M1400 for IKE/IPsec

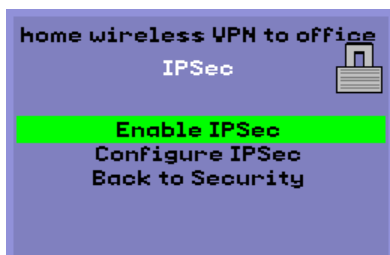
1. From the main menu. Select Security and press [Enter]



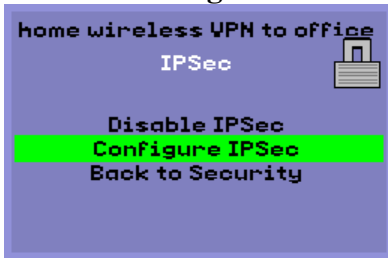
2. Select **IPSEC** and press [Enter]



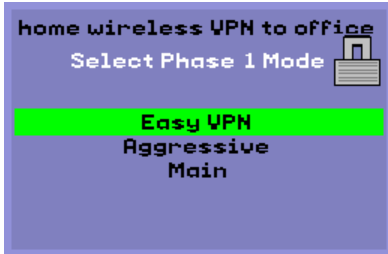
3. Select **Enable IPSEC** and press [Enter] and press [Enter] at the **ok**



4. Select **Configure IPSEC** and press [Enter]



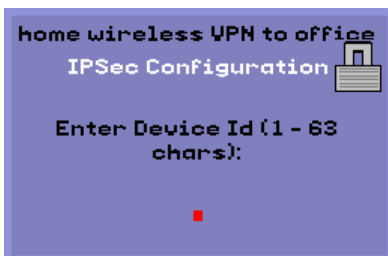
5. Next, select Phase 1 Mode: Easy VPN, Aggressive or Main.



Phase 1 negotiation determines how the traffic is protected for negotiation of the ESP Security Associations.

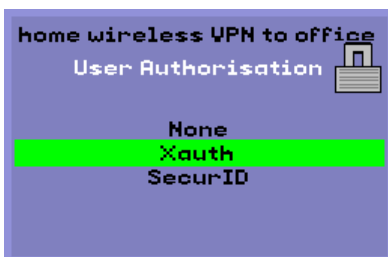
6a. **Easy VPN** is a simplified set of the parameters required by **Aggressive**. For Easy VPN you will only be requested for the following:

Enter the Device Id and press [Enter]

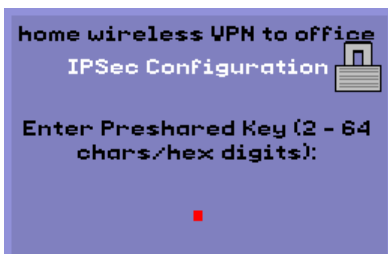


Enter the identifier used to select the pre-share key in the VPN gateway.

6b. Select the User Authorisation mode and press [Enter]

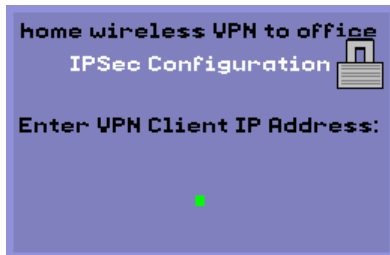


6c. Enter the Pre-shared key and press [Enter] should you select **Xauth** or **SecurID**



The Tadpole M1400 currently only supports pre-shared keys as the method for authentication, the pre-shared key entered here must match that on the VPN gateway. The key can be ASCII characters or, by prefixing with **0x**, hex digits. This is the seed to the creation of the dynamic keys, if this does match the gateway then the Tadpole M1400 will fail to connect to the VPN gateway.

6d. Enter the VPN client fixed IP address else leave blank and press[Enter]



If the Tadpole M1400 has been assigned a fixed IP address within the VPN then enter it here. Leave the address empty to force the Tadpole M1400 to use Mode Config and request an IP address from the VPN gateway.

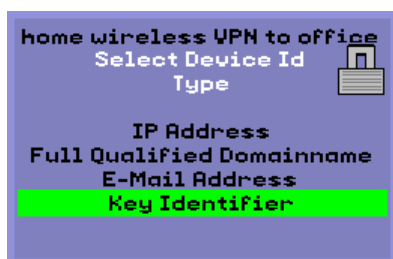
6e. Enter the VPN Server IP address and press [Enter]



This is the public address of the VPN gateway

Go to Step 9

7a. In **Aggressive Mode** knowledge is required of the configuration of the VPN gateway, specifically, which algorithms the gateway is configured to accept. The Tadpole M1400 will send a single proposal with the given algorithms. Aggressive Mode requires more configuration effort but provides more control



Select the Device Id Type

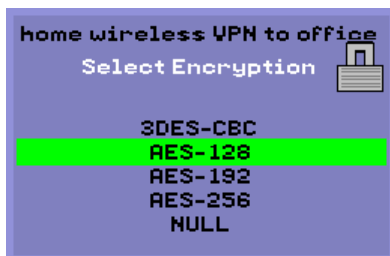
Select one of the four options to determine how the Tadpole M1400 identifies itself to the VPN gateway. The identification is typically used as an identifier to select the pre-shared key in the VPN gateway, most commonly used are **IP Address** and **Key Identifier**. If the Tadpole M1400 is behind a NAT device, NAT precludes the use of **IP Address** as an identifier. You will need to use another option and configure your VPN gateway accordingly.

7b. For **Key Identifier**. Enter the Device Id and press [Enter]

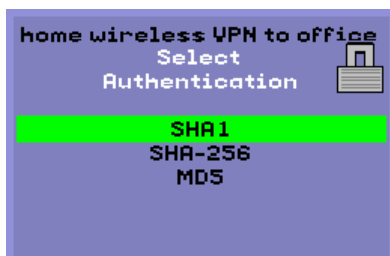


Enter the identifier used to select the pre-share key in the VPN gateway.

7c. Select the encryption algorithm to match your VPN concentrator.

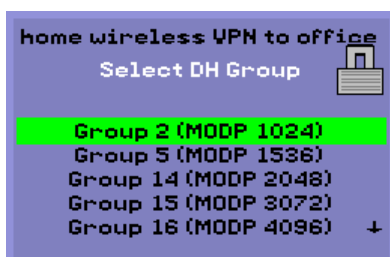


7d. Select the authentication algorithm to match your VPN concentrator.

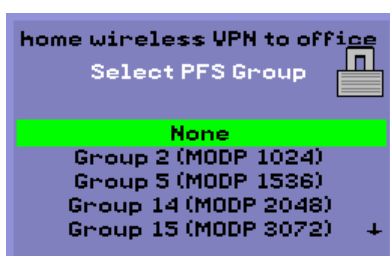


7e. Select the DH group appropriate of your VPN gateway configuration and press [Enter]

The list comprises of the Diffie Hellman groups supported during Phase 1 of the IKE negotiation.

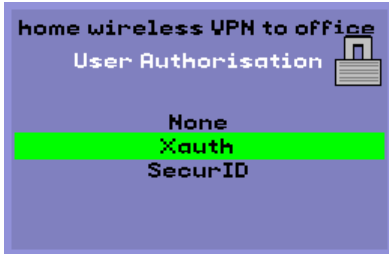


7f. Select PFS group appropriate for your configuration.

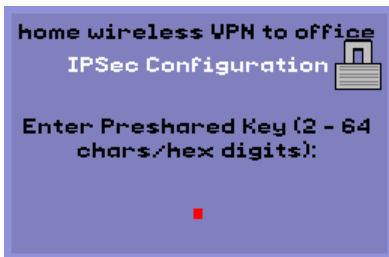


The list comprises of the Diffie Hellman groups available to use to provide Perfect Forward Secrecy between Phase 1 and Phase 2 key generation in IKE.

7g. Select the User Authorisation mode and press [Enter]

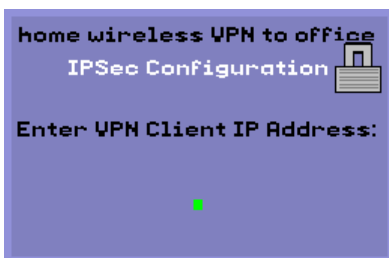


7h. Enter the Pre-shared key and press [Enter] should you select **Xauth** or **SecurID**



The Tadpole M1400 currently only supports pre-shared keys as the method for authentication, the pre-shared key entered here must match that on the VPN gateway. The key can be ASCII characters or, by prefixing with **0x**, hex digits. This is the seed to the creation of the dynamic keys, if this does match the gateway then the Tadpole M1400 will fail to connect to the VPN gateway.

7i. Enter the VPN client fixed IP address else leave blank and press[Enter]



If the Tadpole M1400 has been assigned a fixed IP address within the VPN then enter it here. Leave the address empty to force the Tadpole M1400 to use Mode Config and request an IP address from the VPN gateway.

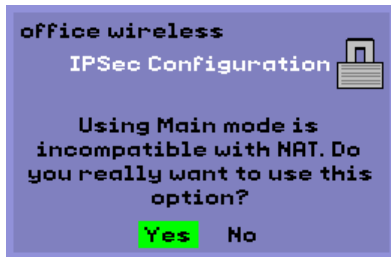
7j. Enter the VPN Server IP address and press [Enter]



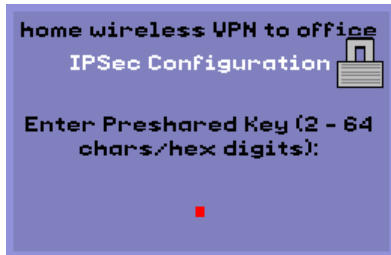
This is the public address of the VPN gateway

Go to Step 9

8a. **Main** mode. In Main Mode the Tadpole M1400 sends a selection of security proposals to the VPN gateway, the gateway will then select the most appropriate. The set of proposals sent includes most permutations of encryption, hash and Diffie-Hellman algorithms supported by the Tadpole M1400. **Main** and **Aggressive**. Select Main Mode and Press [Enter] and select [Yes]

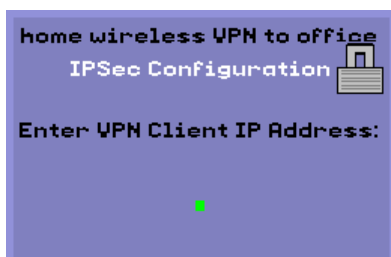


8b. Enter the Pre-shared key and press [Enter]



The Tadpole M1400 currently only supports pre-shared keys as the method for authentication, the pre-shared key entered here must match that on the VPN gateway. The key can be ASCII characters or, by prefixing with **0x**, hex digits. This is the seed to the creation of the dynamic keys, if this does not match the gateway then the Tadpole M1400 will fail to connect to the VPN gateway.

8c. Enter the VPN client fixed IP address else leave blank and press[Enter]



If the Tadpole M1400 has been assigned a fixed IP address within the VPN then enter it here. Leave the address empty to force the Tadpole M1400 to use Mode Config and request an IP address from the VPN gateway.

8d. Enter the VPN Server IP address and press [Enter]



This is the public address of the VPN gateway.

Go to Step 9

**NOTE:**

Certain configuration options are inherently incompatible with NAT.

When the Tadpole M1400 is behind a NAT device, **Main** mode will fail to negotiate keys. If a NAT or there is any uncertainty select **Aggressive** mode.

NAT precludes the use of **IP Address** as an identifier. You will need to use another option and configure your VPN gateway accordingly.

9. At the Save changes menu highlight **Yes** and press **[Enter]** and press **[Enter]** at the ok to confirm configuration saved.

Select **Back to Security** and press **[Enter]** and **Back to Main** and press **[Enter]** to exit the security menu and return to the main menu.