



Application Note:

Onsight Device VPN Configuration V1.1

Table of Contents

OVERVIEW	2
1 SUPPORTED VPN TYPES	2
1.1 OD VPN CLIENT	2
1.2 SUPPORTED PROTOCOLS AND CONFIGURATION	2
2 OD VPN CONFIGURATION	2
2.1 VPN MANAGEMENT SCREEN	3
2.2 VPN MODIFY DIALOG	4
2.2.1 <i>General</i>	5
2.2.2 <i>General TCP/IP</i>	6
2.2.3 <i>Name Servers</i>	7
2.2.4 <i>Security</i>	8
2.2.5 <i>IPSec</i>	11
2.2.6 <i>Connectivity Indication in UI</i>	12
3 SUPPORTED VPN MODES	13
3.1 IPSEC TRANSPORT MODE VS. TUNNEL MODE	13
3.2 SUPPORTED/VALIDATED COMPATIBILITIES	13
3.2.1 <i>InGate SIParator</i>	13
3.3 SUPPORTED IPSEC PHASE 1 TRANSFORMS	13
3.4 SUPPORTED IPSEC PHASE 2 TRANSFORMS	13
3.5 SPLIT TUNNELING	14
4 MPPE OVERVIEW	14
4.1 MPPE ENCRYPTION TYPES (SEE RFC3078)	15
4.2 STATEFUL MPPE ENCRYPTION	15
4.3 STATELESS MPPE ENCRYPTION	15

Overview

This document will focus on the supported VPN protocols and configurations available on the Onsite Device (OD). It will attempt to describe common setups and point out invalid or ambiguous setups. This document is meant to be a compendium of available setups and common issues regarding VPNs with a specific focus on how the OD addresses these. Descriptions of the underlying protocols or VPN infrastructure setup is beyond the scope of this document.

1 Supported VPN Types

1.1 OD VPN Client

Virtual Private Network (VPN) functionality available on the Onsite Device (OD) is provided by components available in the Windows CE operating system. Virtual private networking in Windows CE is implemented through the *Remote Access Service*, the Layer 2 Tunneling Protocol, the IPSec security protocol, and the crypto API (for certificate management). These protocols serve to encapsulate, encrypt, and compress TCP/IP traffic to make them suitable for tunneling.

Access to the RAS API is provided through the Onsite Device application user interface. This allows users to create VPN connections, modify their configurations, dial and hang-up the connections, as well as view status of active connections. VPN user interface organization and terminology is designed to match reasonably closely with the built-in Windows CE Network Connections UI as well as Windows XP UI.

1.2 Supported Protocols and Configuration

The VPN type supported by the OD is Layer 2 Tunneling Protocol with IP Security (L2TP/IPSec). L2TP does not provide authentication or encryption on its own and relies on the underlying PPP for this purpose.

2 OD VPN Configuration

This section will describe the support configurations available on the Onsite Device, while also showing the corresponding UI elements for these configurations.

2.1 VPN Management Screen

The list of VPN connections added to the device is available through Options->Network->VPN. This screen also contains buttons to control management of the VPN connections such as New..., Modify, Delete, Connect/Status, and disconnect.

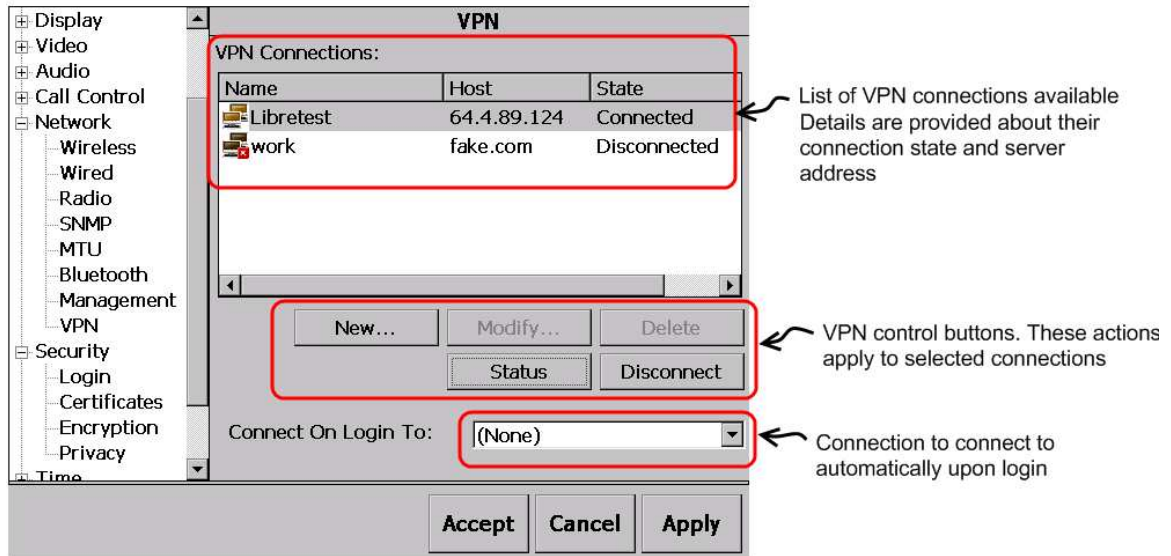


Figure 1 - VPN Management Screen

- **New...:** Create a new L2TP.
- **Modify:** Change the settings for a particular VPN connection including authentication protocol, use of encryption, compression, etc. Connections must be in the 'Disconnected' state to be modified.
- **Delete:** Permanently remove a VPN connection from the device. Hitting the Options screen 'Cancel' button will not reverse this.
- **Connect/Status:** When the selected connection is in the 'Disconnected' state, this button will dial that connection. If the selected connection is in any other state than 'Disconnected', this button will change to 'Status' and will show details regarding this connection.
- **Disconnect:** This button is only enabled if the selected connection is in any state other than 'Disconnected'. It will begin hanging up the selected VPN connection.

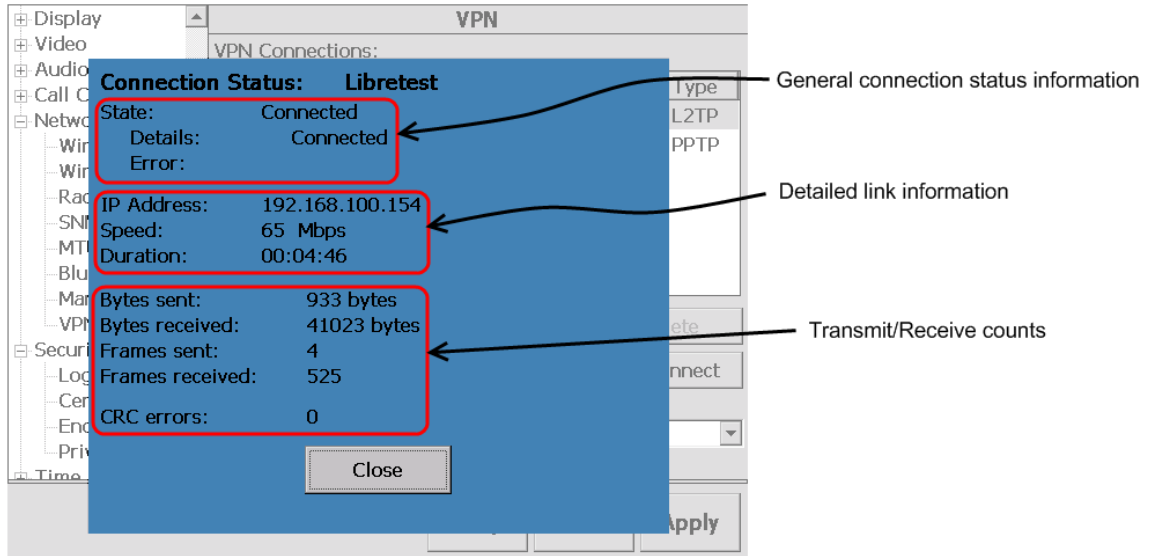


Figure 2 - VPN Connection Status screen

2.2 VPN Modify Dialog

By selecting a disconnected VPN connection from the list and clicking the 'Modify' button, the VPN Modify Dialog will be shown. This allows the configuration of authentication protocols supported, encryption settings, and VPN server configuration. The VPN Modify Dialog is separated in several different screens selected by clicking on the corresponding tree node to the left.

2.2.1 General

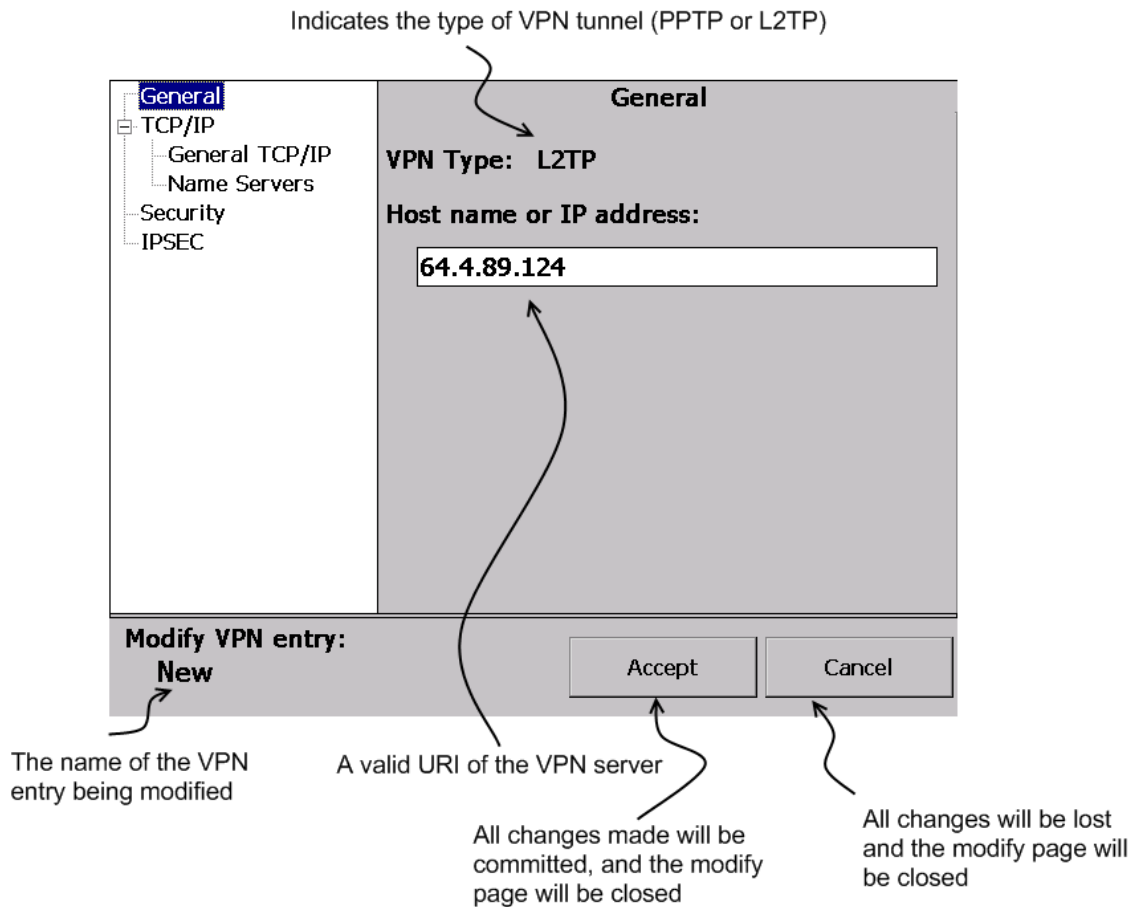


Figure 3 - The VPN Modify General page

- **VPN Type:** Indicates this is a L2TP VPN connection.
- **Host name or IP address:** This is the address of the VPN server that will be connected to. This can be a DNS name such as vpn.librestream.com, or a publicly accessible IP address.

2.2.2 General TCP/IP

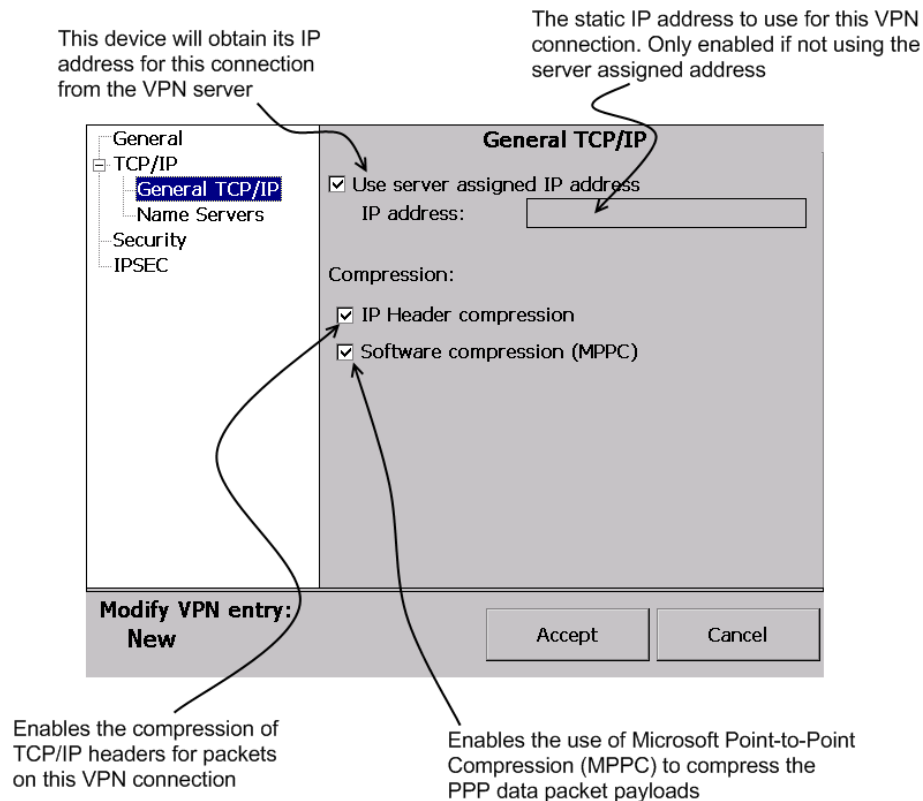


Figure 4 - VPN Modify TCP/IP General Page

- **Use server assigned IP address:** If this box is checked, the server will assign an IP address for this VPN connection. This occurs during the IP Configuration Protocol (IPCP) negotiations when establishing the PPP link. If unchecked, the user must enter a valid static IP address to use in the 'IP Address' text box. For most use cases, the VPN server would be responsible for giving IP addresses to remote clients, so this checkbox is enabled by default in all configurations.
- **IP Header Compression:** Determines whether to use *Van-Jacobson compression* to reduce the size of TCP/IP or UDP headers for the VPN connection.
- **Software Compression:** Determines whether to use Microsoft Point-To-Point Compression (MPPC) to compress the PPP packet payloads.

2.2.3 Name Servers

Use the addresses assigned by the VPN server for Domain Name System (DNS) and Windows Internet Name Service (WINS)

General
TCP/IP
General TCP/IP
Name Servers
Security
IPSEC

Name Servers

Use server assigned IP addresses

DNS: 142.161.130.155

Alternate DNS: 208.67.222.222

WINS: 192.168.100.254

Alternate WINS: 66.77.88.99

Modify VPN entry:
New

Accept Cancel

Enter a valid URI to use for the primary and alternate DNS. These may also be blank

Enter valid URI(s) to use for primary and alternate DNS. These may also be blank

Figure 5 - VPN Modify Name Servers page

- **Use server assigned IP addresses:** If this box is checked, the server will supply IP addresses to use for DNS and WINS during the IPCP negotiations in the PPP link establishment. If unchecked, the user must enter valid IP addresses to use for these services. The default is for the server to supply these addresses, so this box is checked by default.

2.2.4 Security

Enables Microsoft Point-to-Point Encryption (MPPE) to encrypt the PPP payload

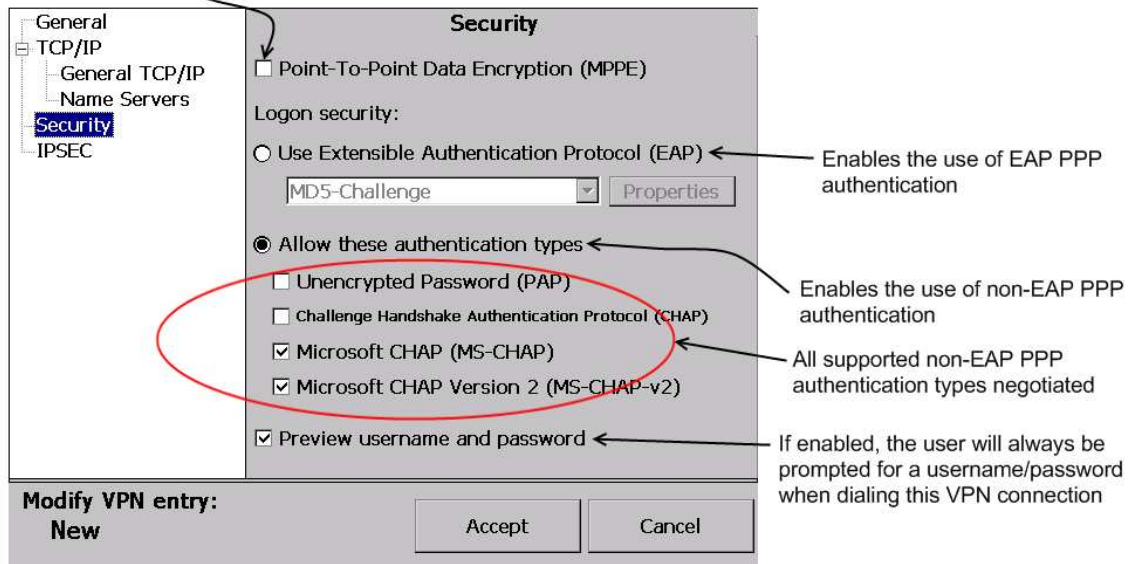


Figure 6 - VPN Modify Security page (not using EAP)

- **Point-To-Point Data Encryption (MPPE):** Selecting this checkbox will enable the negotiation of Microsoft Point-To-Point Encryption (MPPE) on the connection. This algorithm uses the RSA-RC4 stream cipher to encrypt the PPP data packet payloads. Unencrypted Password (PAP) and Challenge Handshake Authentication Protocol (CHAP) authentication types are incapable of negotiating an MPPE encryption key. If this checkbox is selected, the PAP and CHAP checkboxes become cleared and disabled, disallowing those encryption/authentication combinations.
 - **NOTE:** Windows CE 5.0 only supports the 'Stateful' form of MPPE. Many VPN servers will attempt to negotiate 'Stateless' MPPE. If the VPN server is unable to support a Stateful MPPE configuration, the VPN connection will fail.
- **Allow these authentication types:** Selecting this radio button will allow the selection of one or more non-EAP authentication types. If it is not selected, the four following authentication type checkboxes will be disabled and cleared.
- **Unencrypted Password (PAP):** This checkbox enables the support of the simple clear-text username and password authentication method. Since this method send clear text credentials over the network it is not considered secure and is generally not supported. It is disabled by default.
- **Challenge Handshake Authentication Protocol (CHAP):** This checkbox enables the support of the CHAP protocol. This protocol hashes a one-time challenge using a shared secret (such as a password) to avoid sending clear-text credentials. It not generally used.
- **Microsoft CHAP (MS-CHAP):** Version 1 of the Microsoft implementation of CHAP. It is mostly deprecated from new Windows operating systems, not being supported by Vista and later. Tools exists that can crack MS-CHAP relatively easily on a normal desktop computer.
- **Microsoft CHAP Version 2 (MS-CHAP-v2):** An update to MS-CHAP that provides stronger security for the exchange of username and password credentials. Provides mutual authentication. This is the default for most Windows VPN clients when creating a new connection.

- **Preview Username and Password:** if this checkbox is set, when attempting to connect to a VPN, the username/password dialog will always be shown. If this is deselected, cached credentials will be used from a previous successful authentication attempt, and the dialog will not be shown. If there are no previous credentials (no successful prior connections), the dialog will still be shown.

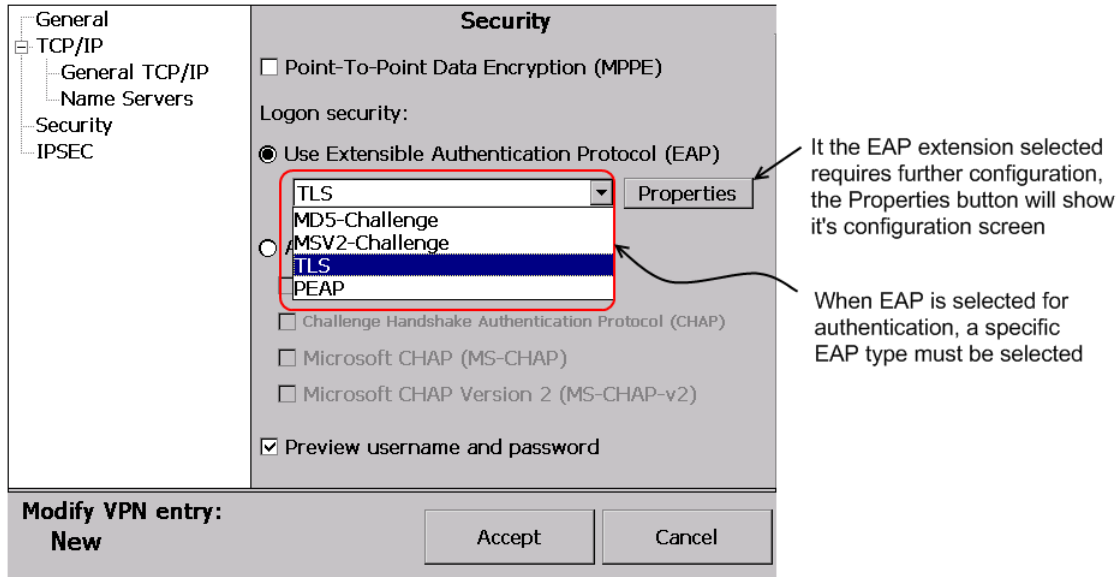


Figure 7 - VPN Modify Security page (with EAP selected)

- **Use Extensible Authentication Protocol (EAP):** Selecting this radio button allows for the use of EAP during the PPP authentication. EAP allows for the negotiation of an arbitrary authentication method. This allows for further authentication modules (different EAP types) to be added or removed while maintaining the PPP standard. If EAP is selected, an EAP extension must be selected from the drop down list
- **EAP Extension Drop Down List:** This list contains all of the EAP extensions available on the Onsite Device.
 - MD5-Challenge – This EAP-type uses the same challenge handshake protocol as CHAP, but the challenges and responses are contained within EAP messages.
 - MSV2-Challenge – This EAP-type uses the same challenge handshake protocol as MS-CHAPv2, but the challenges and responses are contained within EAP messages.
 - EAP – Transport Layer Security (EAP-TLS) – Requires a client side and optional server side certificate to verify mutual identities. This in turn requires a public key infrastructure, as well as an authentication server (such as a RADIUS server) to validate the exchanged credentials. Generally considered very secure.
 - Protected EAP (PEAP) – encapsulates EAP within an encrypted and authentication TLS tunnel. This has the benefit of not requiring a client side certificate, only a username and password pair. A server-side certificate is optional and allows the peer to authenticate the server. PEAP refers to the outer authentication method and the method to create the secure TLS tunnel, the actual client or device authentication is performed by an 'inner EAP-type'. Microsoft implementations commonly use EAP-MSCHAPv2 as the inner type.
- **Properties:** Selecting an EAP extension from the list and clicking the Properties button will bring up an Authentication Settings dialog which will allow the user to configure information necessary to complete that type of EAP authentication.

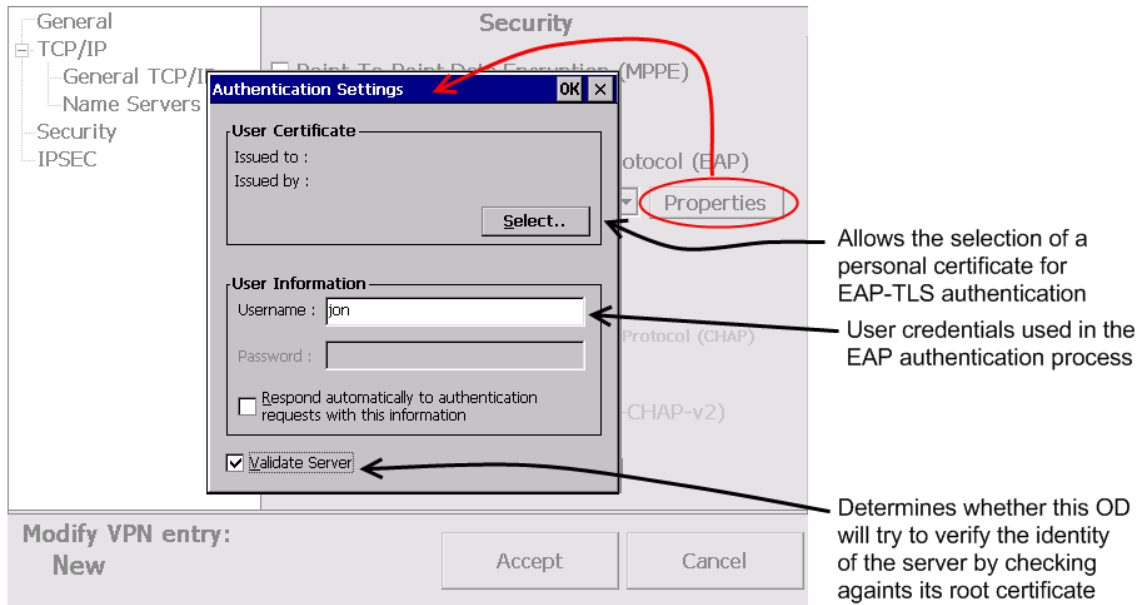


Figure 8 - EAP-TLS Authentication Settings

- **User Certificate:** Lists the personal certificate that has been selected to use for the EAP-TLS authentication. Click the 'Select..' button to select a certificate.
- **Username:** This name will be used in the EAP authentication process. The authentication server will verify it against the certificate credentials provided.
- **Validate Server:** If this checkbox is set, the OD will attempt to verify the identity of the authentication server before allowing the connection to complete. For this validation to succeed, the device must possess a certificate in its trusted store verifying that can be used to verify the server's identity.

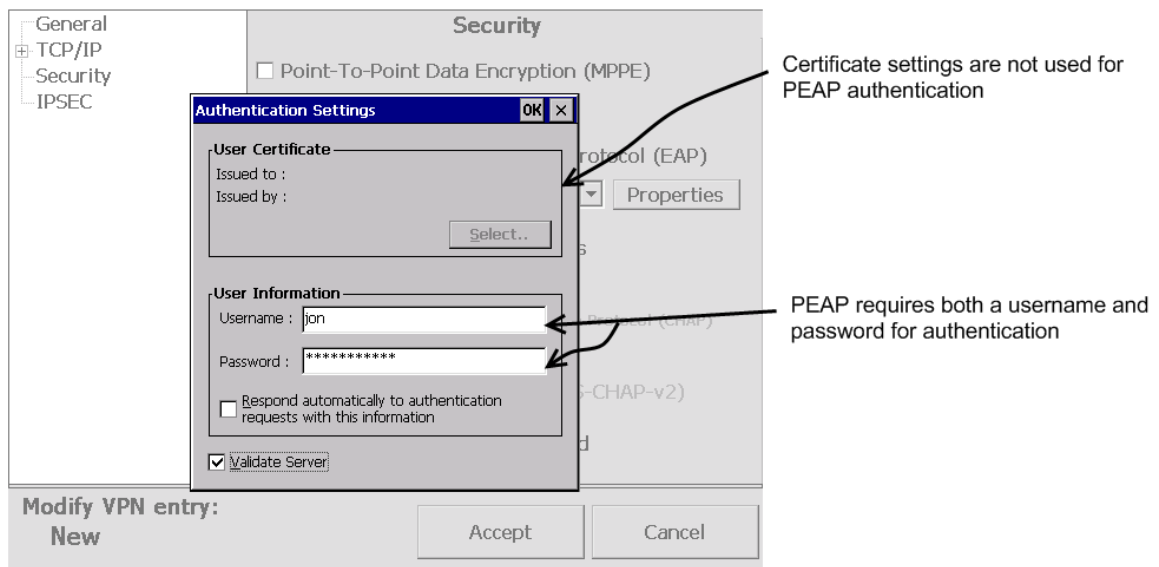


Figure 9 - PEAP Authentication Settings

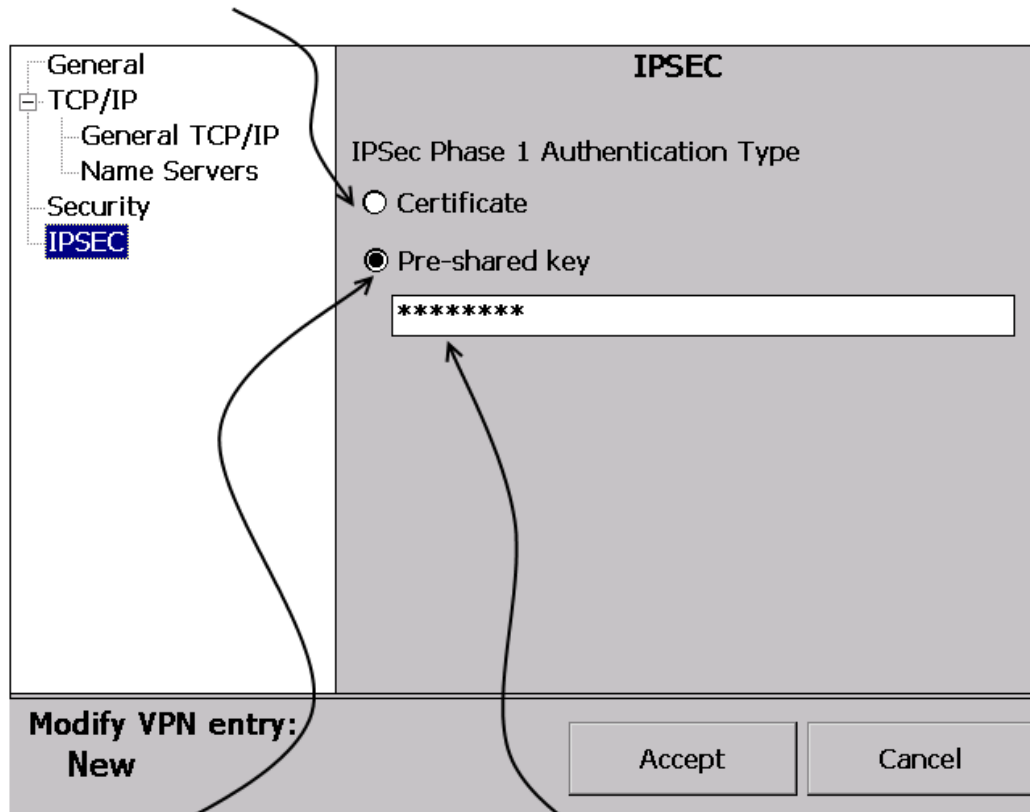
- **User Certificate:** Since the Windows CE implementation of PEAP authentication does not use a certificate to verify the client's identity, these fields are disabled.

- **Username/Password:** The inner-EAP type for this implementation of PEAP is EAP-MS-CHAP-v2. Therefore, a username/password pair that can be authenticated by the server must be entered.

2.2.5 IPsec

Note that IPsec on Windows CE is only used to protect L2TP type VPN connections.

Certificate authentication will be used in establishing the IPsec Security Association



Allows the use of a pre-shared key in creating the IPsec Security Association

The pre-shared key

- **Certificate:** Selecting this radio button will cause the OD to attempt to use a certificate to authenticate the initial IPsec Security Association (SA). If this option is selected, the OD will automatically find an appropriate certificate to use when establishing the IPsec SA.
- **Pre-Shared key:** Selecting this radio button will allow the OD to use a pre-shared secret to authenticate the initial IPsec SA. If this radio button is selected, the user may enter the pre-shared key in the text box below.

2.2.6 Connectivity Indication in UI

The presence of an active VPN connection is indicated by a VPN network icon visible in the icon bar at the top of the viewfinder.

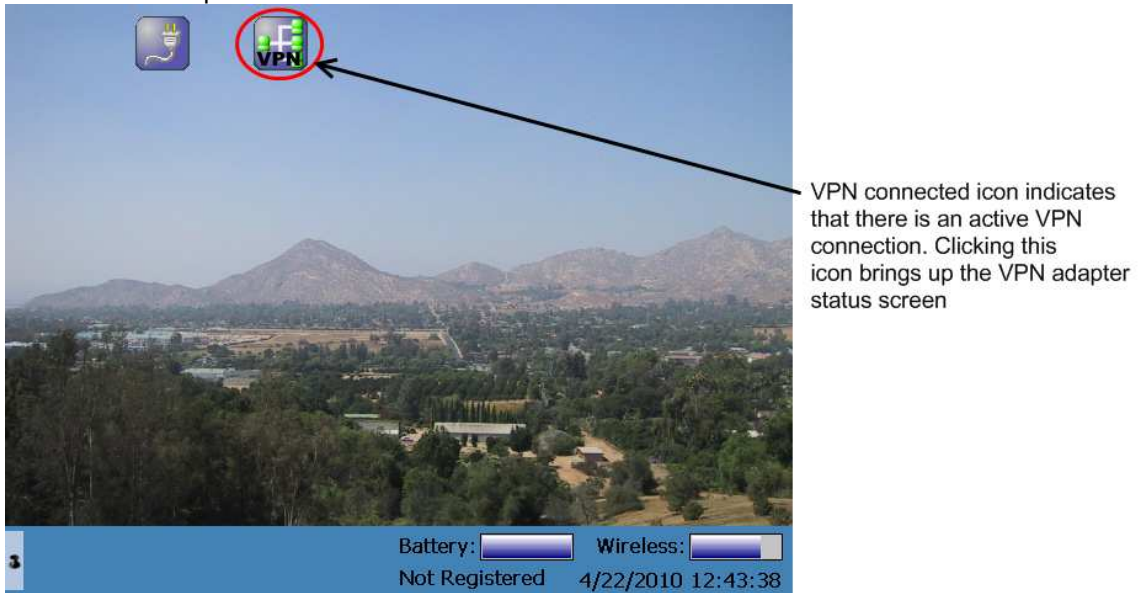


Figure 10 - VPN Network icon

Clicking the VPN icon brings up the Network Status panel which lists the state of the wired, wireless, or VPN adapters. It provides connectivity details such as IP address and connection name.

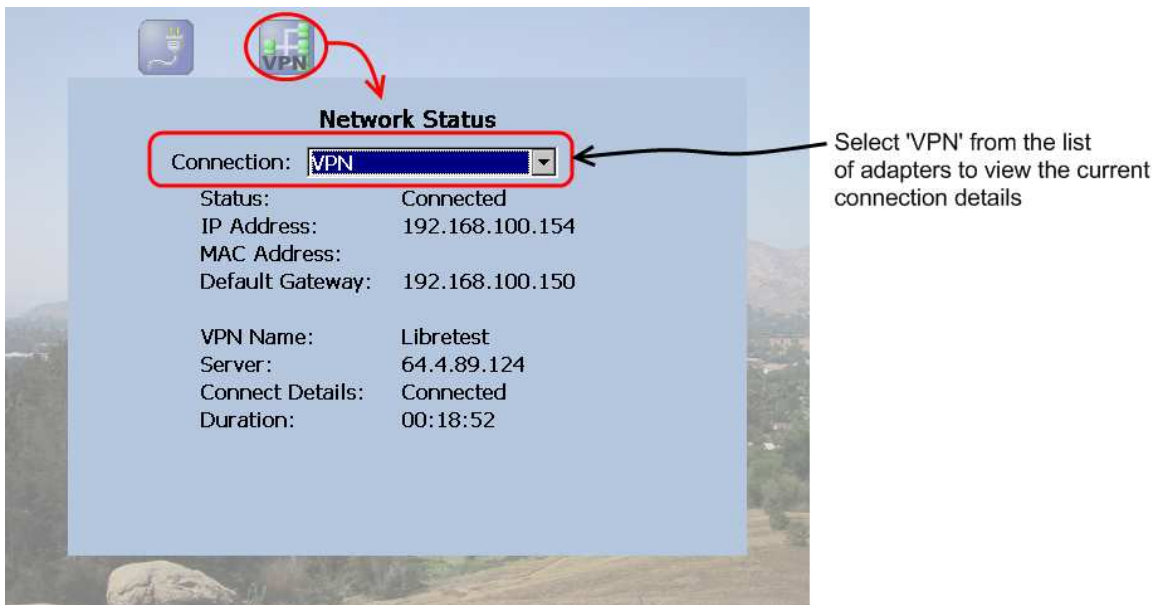


Figure 11 - VPN Network Status panel

3 Supported VPN Modes

3.1 IPsec Transport Mode vs. Tunnel Mode

Windows CE 5.0 only supports IPsec in Transport Mode. In this configuration, only the payload of the IP datagrams is encrypted and/or authenticated. The IP header is unmodified in this situation. Windows CE uses Encapsulating Security Payload (ESP) to provide authenticity, integrity and confidentiality of the IP datagram payloads.

3.2 Supported/Validated Compatibilities

This section will discuss the compatibility of the OD's Windows CE VPN client when connecting to various VPN servers.

3.2.1 InGate SIParator

- L2TP/IPsec: **The Windows CE VPN client can NOT connect to the SIParator using L2TP/IPsec because the SIParator only supports Tunnel mode (IP Header and payload encryption).**
- PPTP: **The Onsight Device does not support PPTP.** However be advised, the Windows CE 5.0 VPN client is not capable of connecting to the InGate SIParator using PPTP regardless. **The SIParator tries to negotiate stateless MPPE (Microsoft Point to Point Encryption), which the CE VPN client does not support. The SIParator is unwilling to accept Stateful MPPE, so the PPP negotiations fail.**

3.3 Supported IPsec Phase 1 Transforms

During Phase 1 of the Internet Security Association and Key Management Protocol (ISAKMP), the device offers a number of available cryptographic transforms. The client and server agree upon an acceptable transform to use in establishing an ISAKMP Security Association.

During Phase 1 of the Internet Key Exchange (IKE)

Transform #	Encryption Algorithm	Hash Function	Diffie-Hellman Group	Authentication
1	3DES	SHA	2048 MODP	RSA-SIG
2	3DES	MD5	2048 MODP	RSA-SIG
3	3DES	SHA	1024 MODP	RSA-SIG
4	3DES	MD5	1024 MODP	RSA-SIG
5	DES	SHA	2048 MODP	RSA-SIG
6	DES	MD5	2048 MODP	RSA-SIG
7	DES	SHA	1024 MODP	RSA-SIG
8	DES	MD5	1024 MODP	RSA-SIG
9	3DES	SHA	768 MODP	RSA-SIG
10	3DES	MD5	768 MODP	RSA-SIG
11	DES	SHA	768 MODP	RSA-SIG
12	DES	MD5	768 MODP	RSA-SIG

3.4 Supported IPsec Phase 2 Transforms

Phase 2 of the ISAKMP negotiations involves establishing security associations for other security protocols. In the case of the Onsight Device L2TP/IPsec VPN connection, this involves setting up an Encapsulating Security Payload (ESP) Security Association (SA). Again, a number of

acceptable crypto transform sets are offered in order of decreasing preference. The two peers will negotiate a set that is acceptable to both.

The Windows CE VPN client supports the following security protocols when negotiating the ESP SA:

- **Encryption:** DES or 3DES. The Windows CE 5.0 Cryptographic API (CAPI) also offers support for AES (128, 192, and 256 bit), but this does not appear to be offered when establishing Phase 2
- **Authentication:** SHA or RSA
- **Key Management algorithms:**
 - Diffie-Hellman (DH) group 2 with 1024 or 2048 bit length.
 - DH group 14 with 1024 or 2048 bit length.
 - DH group 1 with 768.
- **Signature Validation:** DSS or RSA

3.5 Split Tunneling

Normally when a VPN is connected on a Windows device (XP PC or Windows CE), the routing tables are updated to make the remote interface (VPN interface) the default route. This means that any network traffic that is going to a destination not on the local subnet will automatically be routed through the VPN tunnel. This can cause problems for users wishing to connect a VPN to a workplace and still access local network resources, or the internet.

Split tunneling may be configured on a Windows XP machine by modifying the TCP/IP settings for the VPN connection. It is generally considered a security risk as it is nearly equivalent to having a device which is on a corporate LAN, but still has direct access to the internet.

The Onsite Device does not give options to enable split tunneling through the user interface, and there is no such support offered by the Windows CE 5.0 VPN client.

4 MPPE Overview

Reference:

https://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dt_pptp.html#wp1019865

MPPE is an encryption technology developed by Microsoft to encrypt point-to-point links. These PPP connections can be over a dialup line or over a VPN tunnel. MPPE works as a sub-feature of Microsoft Point-to-Point Compression (MPPC).

MPPC is a scheme used to compress PPP packets between Cisco and Microsoft client devices. The MPPC algorithm is designed to optimize bandwidth utilization in order to support multiple simultaneous connections.

MPPE is negotiated using bits in the MPPC option within the Compression Control Protocol (CCP) MPPC configuration option (CCP configuration option number 18).

MPPE uses the RC4 algorithm with either 40- or 128-bit keys. All keys are derived from the cleartext authentication password of the user. RC4 is stream cipher; therefore, the sizes of the encrypted and decrypted frames are the same size as the original frame. The Cisco implementation of MPPE is fully interoperable with that of Microsoft and uses all available options, including historyless mode. Historyless mode can increase throughput

in lossy environments such as VPNs, because neither side needs to send CCP Resets Requests to synchronize encryption contexts when packets are lost.

4.1 *MPPE Encryption Types (See RFC3078)*

4.2 *Stateful MPPE Encryption*

Stateful encryption will provide the best performance but may be adversely affected by networks experiencing substantial packet loss. The sender must change its key before encryption and transmission of the 'flag' packet.

Because of the way that the RC4 tables are reinitialized during stateful synchronization, it is possible that two packets may be encrypted using the same key. For this reason, stateful encryption may not be appropriate for lossy network environments (such as Layer 2 tunnels on the Internet).

4.3 *Stateless MPPE Encryption*

If stateless encryption has been used, the session key changes for each packet sent. In stateless mode the sender must change the key before encryption and transmission of each packet and the receiver must change the key after receiving but before decryption of each packet.