



Digi Connect VPN Settings

How to create a VPN tunnel between Digi and Lancom

1. Lancom Setup

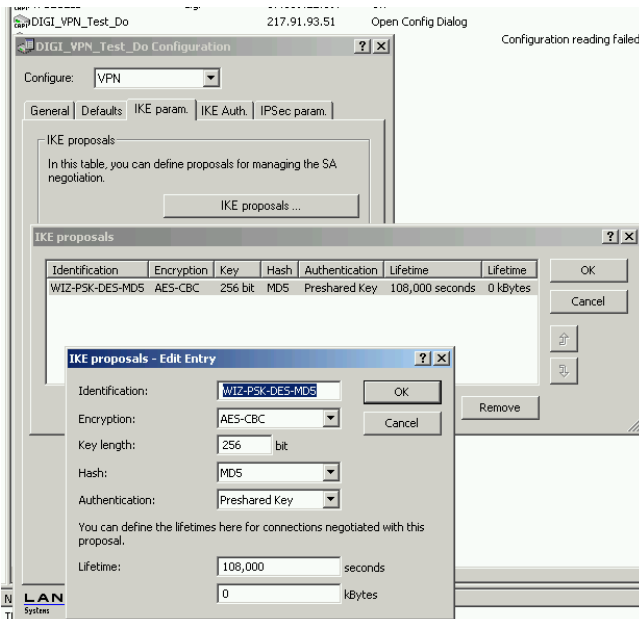
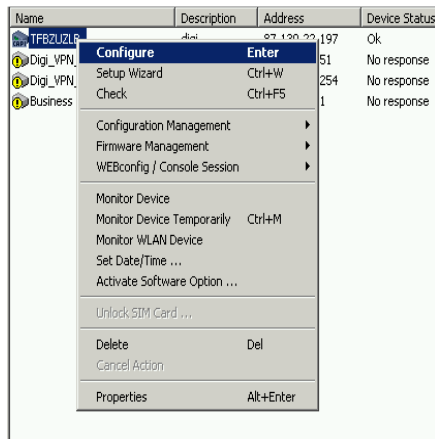
VPN Settings for the Lancom Business R800+ and the Digi Connect VPN

Date: 26-Sep-06

Tool: LANconfig from Lancom

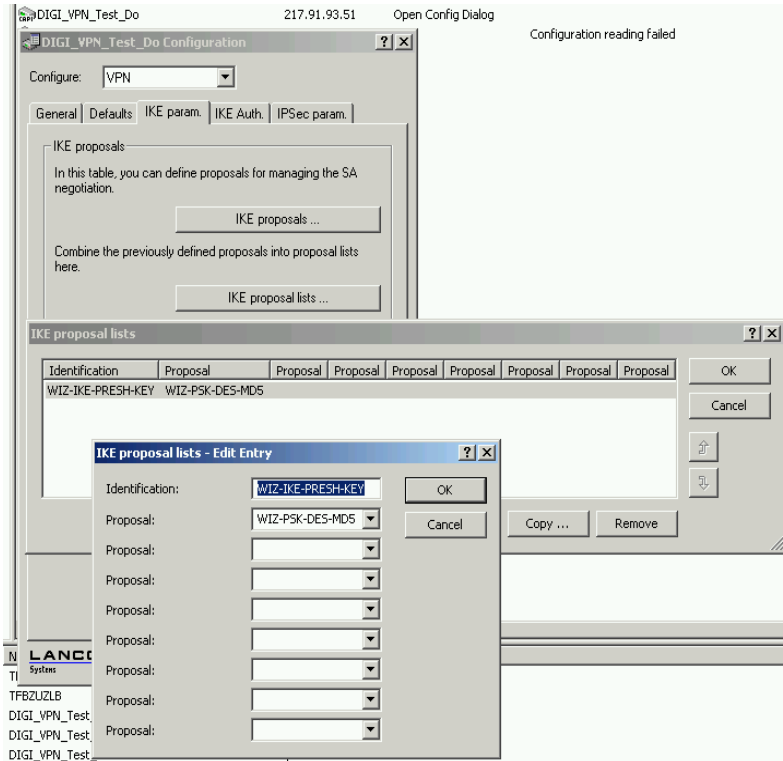


Lancom IKE Parameter

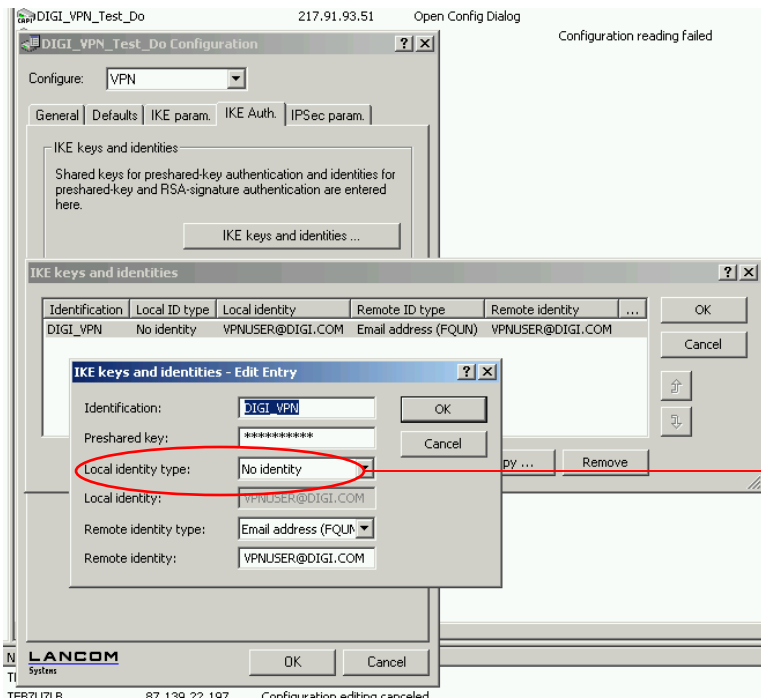




How to create a VPN tunnel between Digi and Lancom



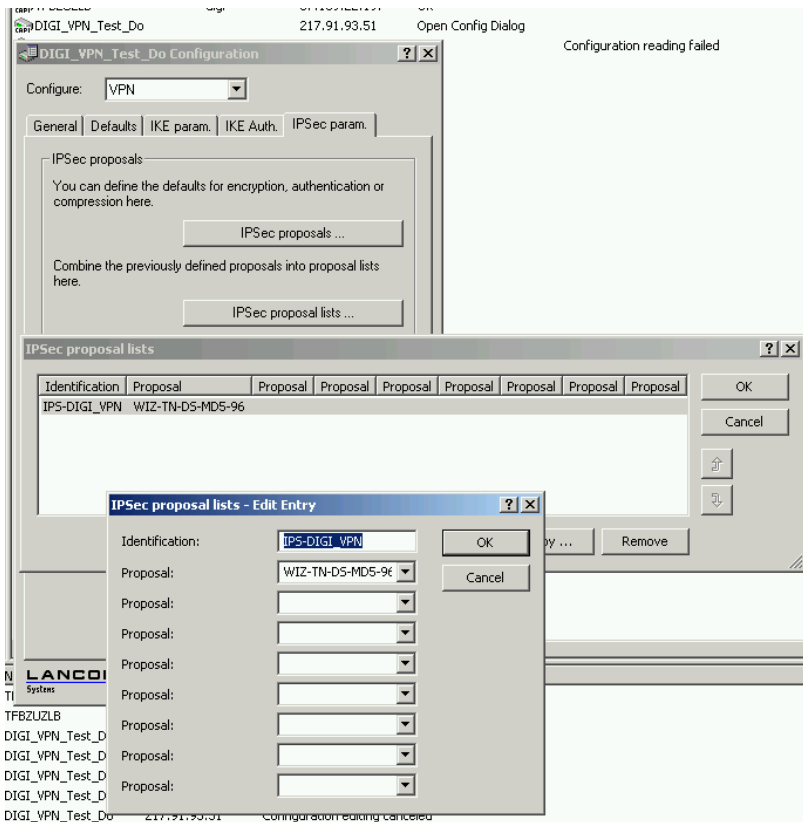
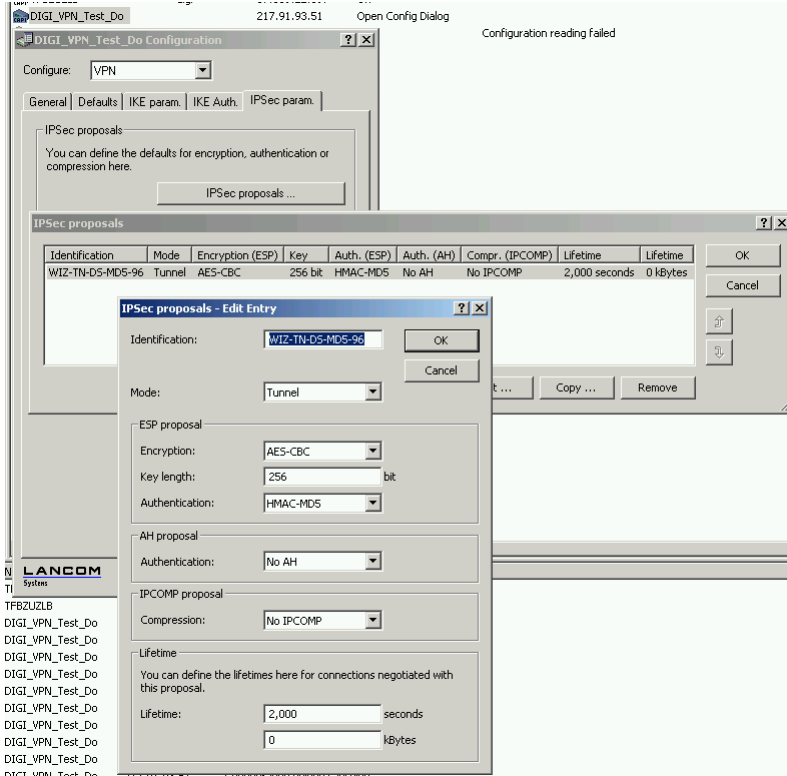
Lancom IKE Authentication Settings



Here insert the preshared key: "geheim1234"

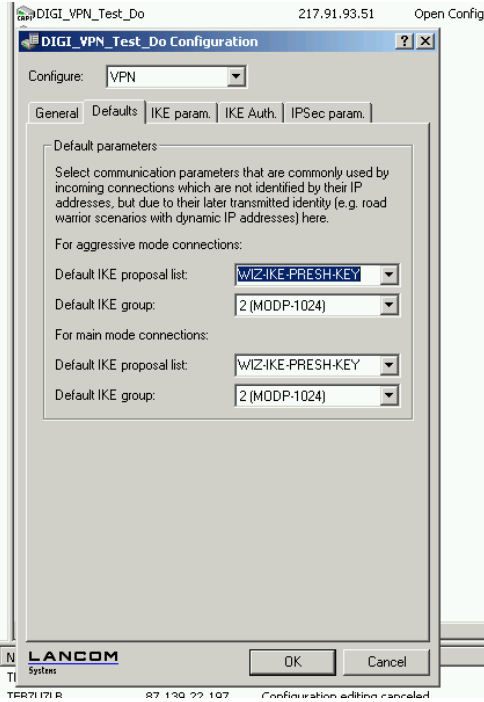


Lancom IPSec Settings

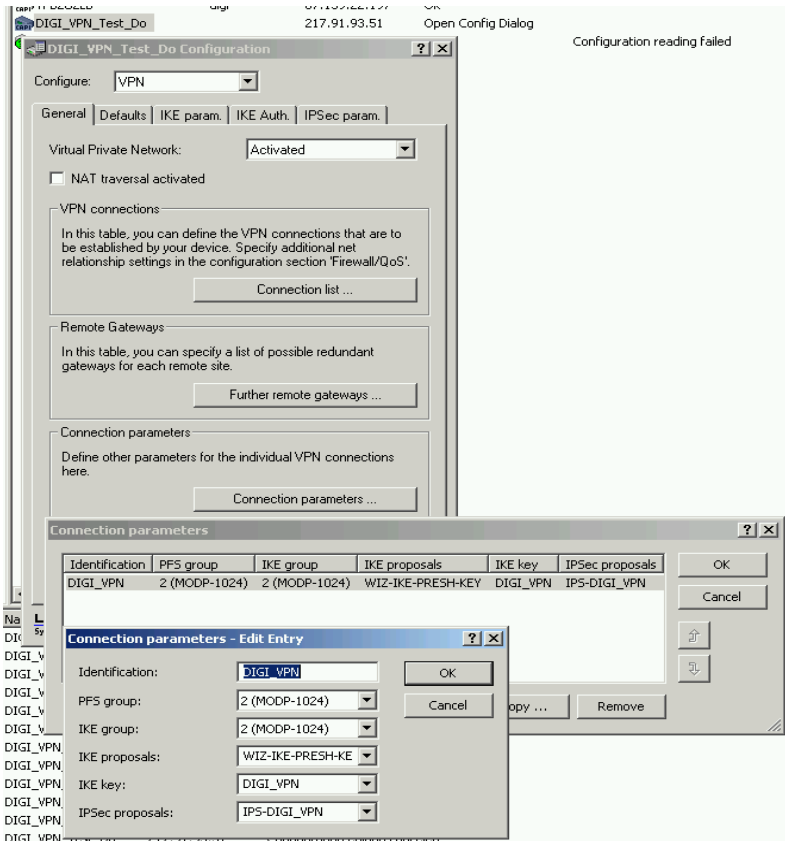




Lancom Default Settings

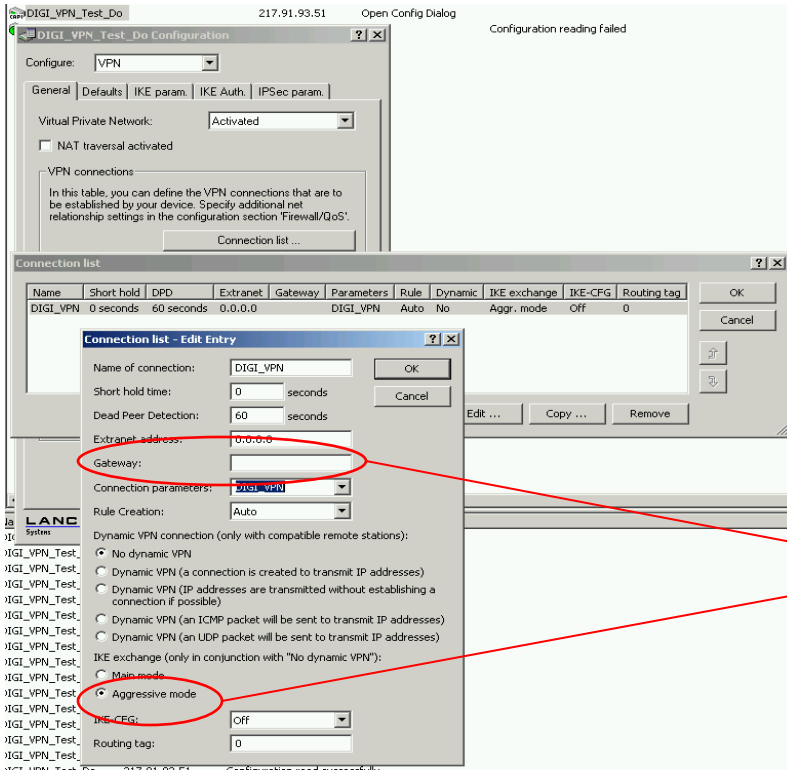


Lancom Connection Settings



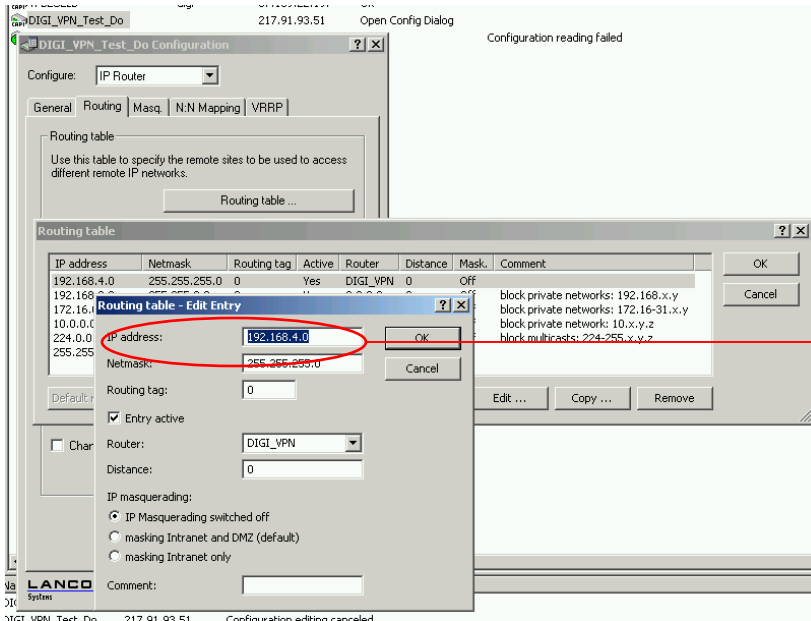


How to create a VPN tunnel between Digi and Lancom



The gateway address is not need for the aggressive mode and FQDN / FQUN

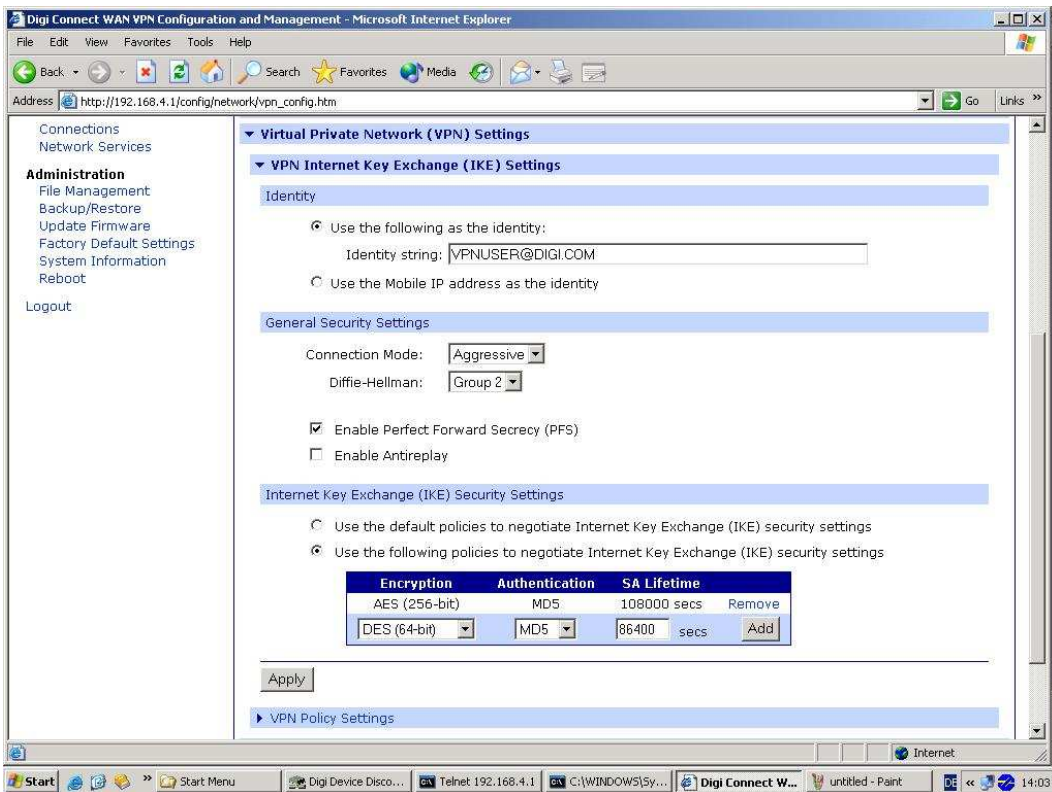
Lancom Routing Settings



This is the remote network site for the VPN tunnel



2. Digi Setup firmware 2.6 and earlier





How to create a VPN tunnel between Digi and Lancom

The screenshot shows the 'VPN - Tunnel #1 - Configuration' page in a web browser. The interface includes a left-hand navigation menu with categories like Configuration, Management, and Administration. The main content area is divided into sections for tunnel endpoints, traffic flow, and security settings.

VPN - Tunnel #1 - Configuration

Description: Linksys_DO

Remote VPN Endpoint: 217.91.93.51

VPN Tunnel: ISAKMP

Tunnel Network Traffic from the following Local Network:

IP Address: 192.168.4.0

Subnet Mask: 255.255.255.0

Tunnel Network Traffic to the following Remote Network:

IP Address: 192.168.3.0

Subnet Mask: 255.255.255.0

Security Settings

Use the following pre-shared key to negotiate IKE security settings:

geheim1234

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
AES (256-bit)	MD5	2000 secs	Remove
None	None	28200 secs	Add

Buttons: Apply, Cancel

Digi SureLink Settings

The screenshot shows the 'Digi SureLink Settings' page in a web browser. The page contains a checkbox to enable link integrity monitoring and several radio button options for different test methods: Ping Test, TCP Connection Test, and DNS Lookup Test. Each test method has associated input fields for addresses, ports, and names. There are also checkboxes for testing only when idle and resetting the link after failures.

The SureLink Link Integrity Monitoring tests are performed only while the mobile network connection is established, and when the tests are enabled in these settings.

Enable Link Integrity Monitoring using the test method selected below.

Ping Test
Verifies that a valid reply is received for a ping request sent to the following:

Primary Address: 192.168.3.1

Secondary Address:

TCP Connection Test
Verifies that a TCP connection can be established with the following:

TCP Port: 80

Primary Address:

Secondary Address:

DNS Lookup Test
Verifies that a DNS reply is received when requesting a DNS lookup of the following:

Primary DNS Name:

Secondary DNS Name:

Repeat the selected link integrity test every: 60 seconds (10-65535)

Test only when idle: if no data is received for the above period of time.

Reset the link after the following number of consecutive link integrity test failures:

6 (1-255)



3. Digi Setup firmware 2.7 and later

Virtual Private Network (VPN) Settings

VPN Global Settings

General Security Settings

Enable Antireplay

Miscellaneous Settings

Suppress SA lifetime during IKE phase 1

Suppress Delete Phase 1 SA Message For PFS

VPN - Tunnel #1 - Configuration

Description: Tunnel 1

Remote VPN Address: 217.91.93.51

VPN Tunnel: ISAKMP

Local Endpoint Type: Local endpoint is a subnet

Identity

Network Interface: mobile0

Negotiate tunnel as soon as interface comes up

Use the following as the identity: VPNUSER@DIGI.COM

Use the interface IP address

Use the identity certificate X.509 distinguished name (DN)

Local Endpoint

Tunnel Network Traffic from the following Local Network:

IP Address: 192.168.4.0

Subnet Mask: 255.255.255.0

Remote Endpoint

Tunnel Network Traffic to the following Remote Network:

IP Address: 192.168.3.0

Subnet Mask: 255.255.255.0

Pre-Shared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID:

217.91.93.51

Use the following pre-shared key to negotiate IKE security settings:

geheim1234



How to create a VPN tunnel between Digi and Lancom

ISAKMP Phase 1 Settings

General Security Settings for Phase 1

Connection Mode:

Enable Perfect Forward Secrecy (PFS)

NAT-T Settings

Enable NAT Traversal (NAT-T)

Keep Alive Interval:

ISAKMP Phase 1 Policies

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	AES (256-bit)	MD5	108000 secs	Group 2	Remove
<input type="text" value="Pre-Shared Key"/>	<input type="text" value="AES (256-bit)"/>	<input type="text" value="MD5"/>	<input type="text" value="108000"/> secs	<input type="text" value="Group 2"/>	<input type="button" value="Add"/>

ISAKMP Phase 2 Settings

General Security Settings for Phase 2

Diffie-Hellman:

ISAKMP Phase 2 Policies

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
AES (256-bit)	MD5	2000 secs	Remove
<input type="text" value="AES (256-bit)"/>	<input type="text" value="MD5"/>	<input type="text" value="2000"/> secs	<input type="button" value="Add"/>