

# IPSec\_Pre shared key and Xauth with CISCO router

## 1. Introduction

### 1.1 Overview

This document contains information regarding the configuration and use of IPSec\_Pre-shared key and Xauth with CISCO router.

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

### 1.2 Compatibility

This application note applies to:

Models Shown: 641M series.

Firmware Version: V1.0.0 (903.0) or newer

Other Compatible Models: None

### 1.3 Version

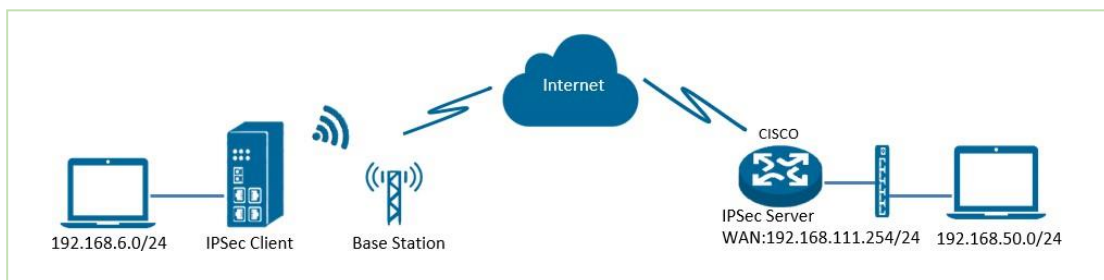
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2018/08/03	V1.0.0	V1.0.0 (903.0)	First released

### 1.4 Corrections

Appreciate for corrections or rectifications to this application note, and if any request for new application notes please email to: [support@elpro.com.au](mailto:support@elpro.com.au)

## 2. Topology



1. 641M runs as IPSec Client with any kind of IP, which can ping IPSec server IP successfully.
2. CISCO router runs as IPSec Server with a static public IP.
3. IPSec tunnel is established between 641M and cisco router.

## 3. Configuration

### 3.1 Server Configuration

1. Login to CISCO router and setting like below:

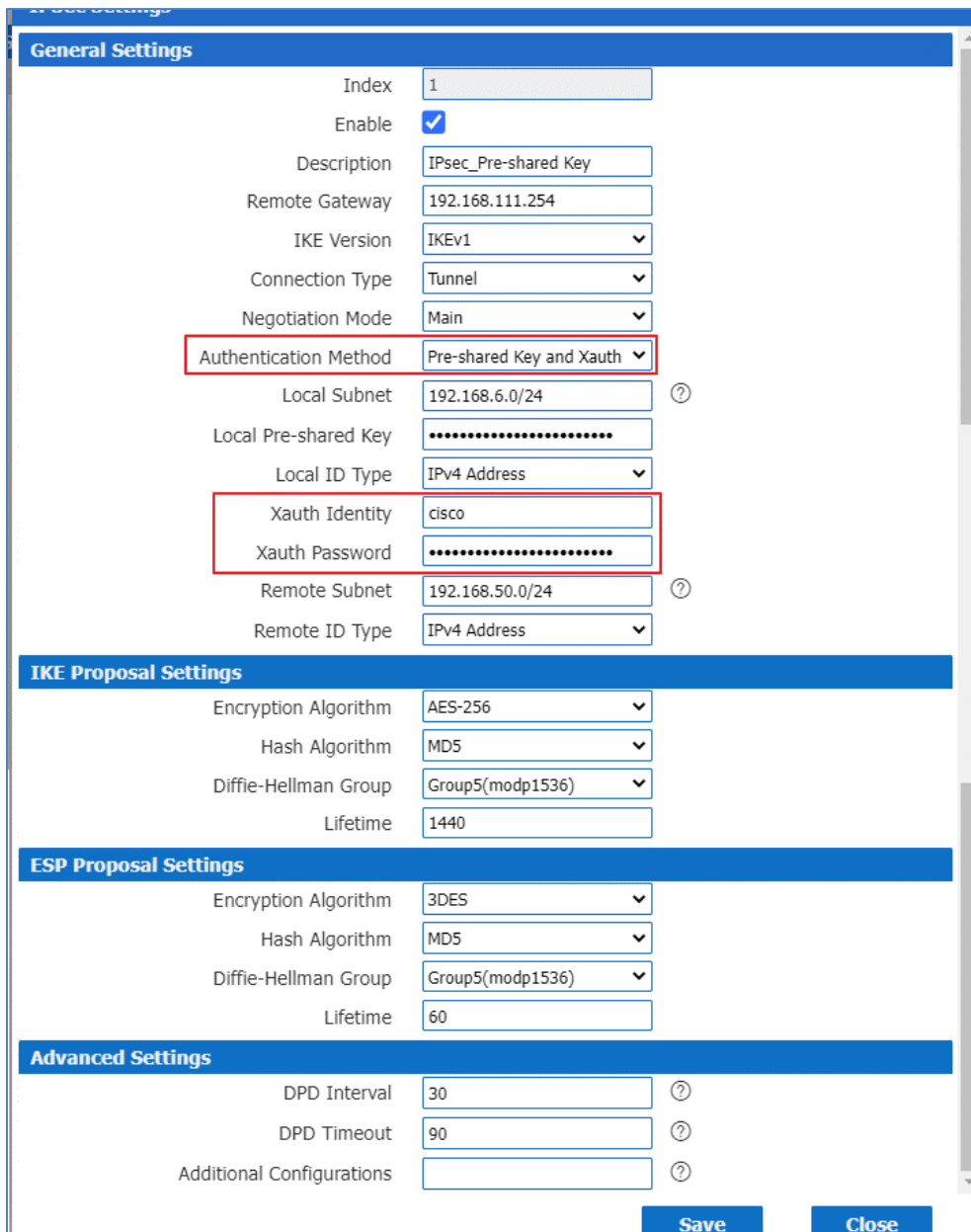
```
=====
cisco2811#show running
config
version 12.4
hostname cisco2811
!
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgj.
new-model
authentication login LOGIN local
!
session
id common
dot11 syslog
ip source route
!
ip cef
ip domain name cisco.com
ip name
server 192.168.111.1
ip address pool local
no ipv6 cef
!
username cisco password 0 cisco
archive
log config
hidekeys
!
crypto isakmp policy 10
encr aes 256
hash md5
authentication pre share
group 5
crypto isakmp key 6 cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set 641M esp 3des esp md5 hmac
!
```

```
crypto dynamic-map DYN 10
set transform set 641M
set pfs group5
match address 101
reverse-route
!
crypto map MAP client authentication list LOGIN
crypto map MAP 10 ipsec--isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line
protocol
interface Loopback0
ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
ip address 192.168.111.254 255.255.255.0
ip nat outside
ip nat enable
ip virtual reassembly
duplex full
speed auto
no mop enabled
crypto map MAP
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual reassembly
duplex auto
speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
```

```
!!  
line con 0  
line vty 5 15  
exec timeout 5 2  
end
```

### 3.2 Client Configuration

1. Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure IPSec VPN as per below picture. Click Save.



General Settings	
Index	1
Enable	<input checked="" type="checkbox"/>
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Main
Authentication Method	Pre-shared Key and Xauth
Local Subnet	192.168.6.0/24
Local Pre-shared Key	.....
Local ID Type	IPv4 Address
Xauth Identity	cisco
Xauth Password	.....
Remote Subnet	192.168.50.0/24
Remote ID Type	IPv4 Address

IKE Proposal Settings	
Encryption Algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman Group	Group5(modp1536)
Lifetime	1440

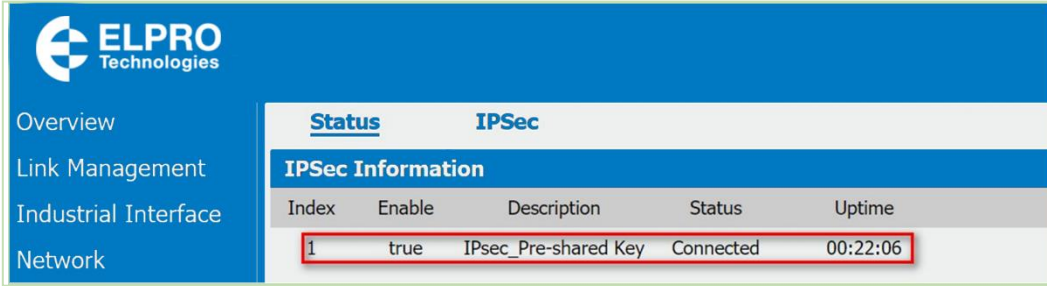
ESP Proposal Settings	
Encryption Algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman Group	Group5(modp1536)
Lifetime	60

Advanced Settings	
DPD Interval	30
DPD Timeout	90
Additional Configurations	

Save Close

2. Click Save>Apply.

- IPSec had been connected successfully. Go to **VPN>IPSec>Status** to check the connection status.



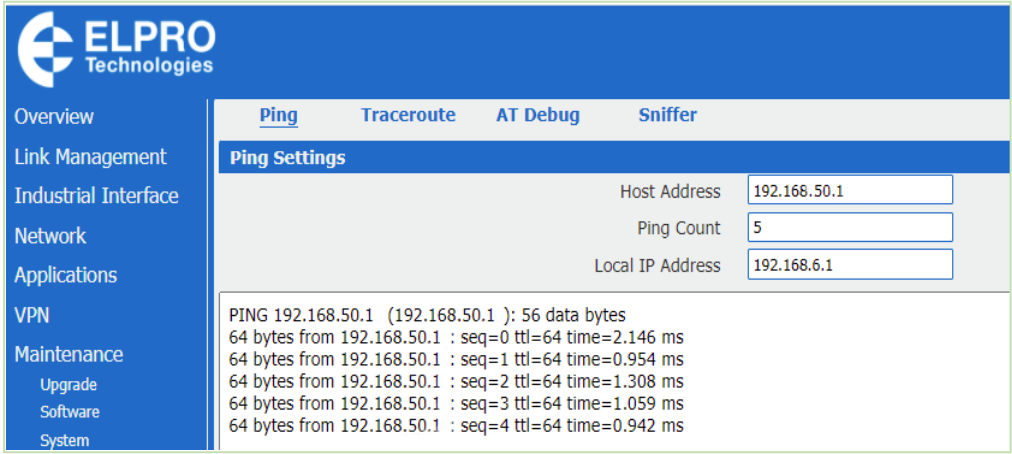
ELPRO Technologies	
Overview	Status IPSec
Link Management	IPSec Information
Industrial Interface	Index Enable Description Status Uptime
Network	1 true IPsec_Pre-shared Key Connected 00:22:06

## 4. Testing

- Ping from CISCO router to 641M, LAN to LAN communication is working correctly.

```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

- Ping from 641M to CISCO router, LAN to LAN communication is working correctly.



ELPRO Technologies	
Overview	Ping Traceroute AT Debug Sniffer
Link Management	Ping Settings
Industrial Interface	Host Address 192.168.50.1
Network	Ping Count 5
Applications	Local IP Address 192.168.6.1
VPN	PING 192.168.50.1 (192.168.50.1) : 56 data bytes
Maintenance	64 bytes from 192.168.50.1 : seq=0 ttl=64 time=2.146 ms
Upgrade	64 bytes from 192.168.50.1 : seq=1 ttl=64 time=0.954 ms
Software	64 bytes from 192.168.50.1 : seq=2 ttl=64 time=1.308 ms
System	64 bytes from 192.168.50.1 : seq=3 ttl=64 time=1.059 ms
	64 bytes from 192.168.50.1 : seq=4 ttl=64 time=0.942 ms

- Test successfully.