L2TP/IPSec VPN for Windows XP to 3Com X-family

Document Version:	1.1
Publication Date:	10th May 2007
Description:	L2TP/IPSec VPN from Microsoft Windows XP to 3Com X-family
Product:	3Com X-family
3Com TOS Version:	2.5.1.6826
Windows XP version	Version 5.1 (Build 2600.xpsp_sp2_gdr.061219-0316 : Service Pack 2)

Introduction

This document explains how to configure the 3Com X-family devices to terminate a Windows XP VPN client using L2TP/IPSec.

These instructions assume that your corporate network is attached to the LAN security zone of the X-family, and that external (Internet) traffic is on the WAN security zone.

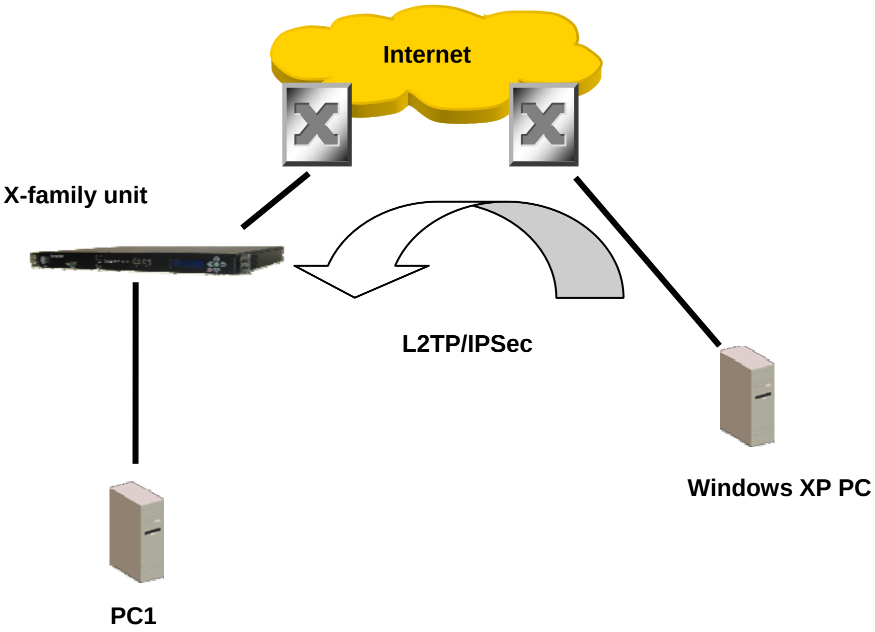
Table of Contents

1 Overview

L2TP over IPSec uses the security attributes of an IPSec tunnel for data transfer, and the Layer 2 tunneling protocol to essentially make the client appear part of the Workplace network. Although more difficult to setup (due to the IPSec steps) this is a far more secure solution than PPTP.

Windows XP can offer a choice of use a Pre-shared Secret Key (PSK) or a X.509 Digital Certificate to secure the IPSec VPN. Both are shown in the following examples.

2 Network Configuration



IP Addresses for this example setup are:

Device	Interface	Address	Mask	Gateway
Router	1 (to X-family unit)	10.10.20.1	255.255.255.0	
Router	2 (to XP PC)	10.10.10.1	255.255.255.0	
X-family	External	10.10.20.147	255.255.255.0	10.10.10.1
XP PC	External	10.10.10.147	255.255.255.0	10.10.20.1
PC1		192.168.1.100	255.255.255.0	192.168.1.254
XP PC	Tunnel	192.168.1.x	255.255.255.0	192.168.1.254

3 Pre-Requisite Configuration

The following configuration steps are required before the X-family device can terminate L2TP/IPSec connections from Windows XP. The instructions assume that the X-family device is at default settings.

3.1.1 Initial Setup via the OBE

Setup the user account and then set the basic configuration as follows. The dialogue shown is the OBE (“Out of Box Experience”) on the Command Line Interface – this could also be set up using the OBE on the Graphical User Interface).

```
Your super-user account has been created.
You may continue initial configuration by logging into your device.
After logging in, you will be asked for additional information.

Login: topuser
Password: t0p--us3r

Entering Setup wizard...

Enter Host Name [myhostname]: 3KB_X_unit_1
Enter Host Location [room/rack]: Lab

            Host Name: 3KB_X_unit_1
        Host Location: Lab
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a

Timekeeping options allow you to set the time zone, enable or disable
daylight saving time, and configure or disable NTP.

Would you like to modify timekeeping options? <Y,[N]>:

The X-Series device may be configured into a number of well known
network deployments.

Would you like to modify the network deployment mode? <Y,[N]>:

Virtual interfaces define how this device integrates with the IP layer 3
network.  You must configure one virtual interface for every IP subnet
that is directly connected to the X-Series device.  For example, you
need
one for the WAN connection (external virtual interface) and one for
every
directly connected network subnet (internal virtual interfaces).

Would you like to modify virtual interfaces? <Y,[N]>:y

Virtual interfaces:
Id  Type      Mode    IP Address       Subnet Mask      NAT
 1  internal  static  192.168.1.254    255.255.255.0    external-ip
 2  external  dhcp                                      disable
 3  <empty>
 4  <empty>
 5  <empty>
 6  <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]:
Enter the number of the entry you want to change []: 2
Mode (static, dhcp, pppoe, pptp, l2tp) [dhcp]: sta
IP address []: 10.10.20.147
Mask [255.255.255.0]:

Virtual interfaces:
Id  Type      Mode    IP Address       Subnet Mask      NAT
 1  internal  static  192.168.1.254    255.255.255.0    external-ip
 2  external  static  10.10.20.147     255.255.255.0    disable
 3  <empty>
 4  <empty>
 5  <empty>
 6  <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]: a

You must configure a default gateway manually if external virtual
interface is static.

Would you like to modify default gateway? <Y,[N]>:y
Default Gateway [0.0.0.0]: 10.10.20.1

Security zones enable you to section your network logically into
security
domains.  As network traffic travels between zones, it is routed and
security-scanned by the firewall and IPS according to the policies you
define.  You need to create security zones that naturally map onto your
intended network security boundaries.  A security zone may or may not be
connected (mapped) to a virtual interface.

Would you like to modify security zones? <Y,[N]>:

Would you like to modify security zone to virtual interface mapping?
<Y,[N]>:

DNS (Domain Name Service) is a system which translates computer
hostnames
to IP addresses. The X-Series device requires DNS configuration in order
to perform web filtering.

Would you like to configure DNS? <Y,[N]>:

Firewall policy rules control the flow of network traffic between
security zones.  Firewall policy rules control traffic flow based
on source and destination security zones and network protocol.

Would you like to modify firewall policy rules? <Y,[N]>:

SMS-based configuration allows the device to retrieve the configuration
for a secure management VPN to the SMS system.  This ensures that
the device can be managed securely from the SMS

Would you like to enable SMS-based configuration? <Y,[N]>:
```

```
If you wish to run this wizard again, use the 'setup' command.

3KB_X_unit_1#
```

Notes:

Virtual Interfaces - There are two virtual interfaces (external and internal) set up as factory default. The only configuration required on them is to set the IP addresses. (In the example, I have kept the internal IP address as default and changed the external IP address).

Security Zones – The factory default configuration sets the LAN security zone to be on Port 1 and linked to the internal Virtual Interface. The WAN security zone is on the last port (Port 4 on an X505 or port 6 on the X506 and X5) and is linked to the external virtual interface. No change is needed to this.

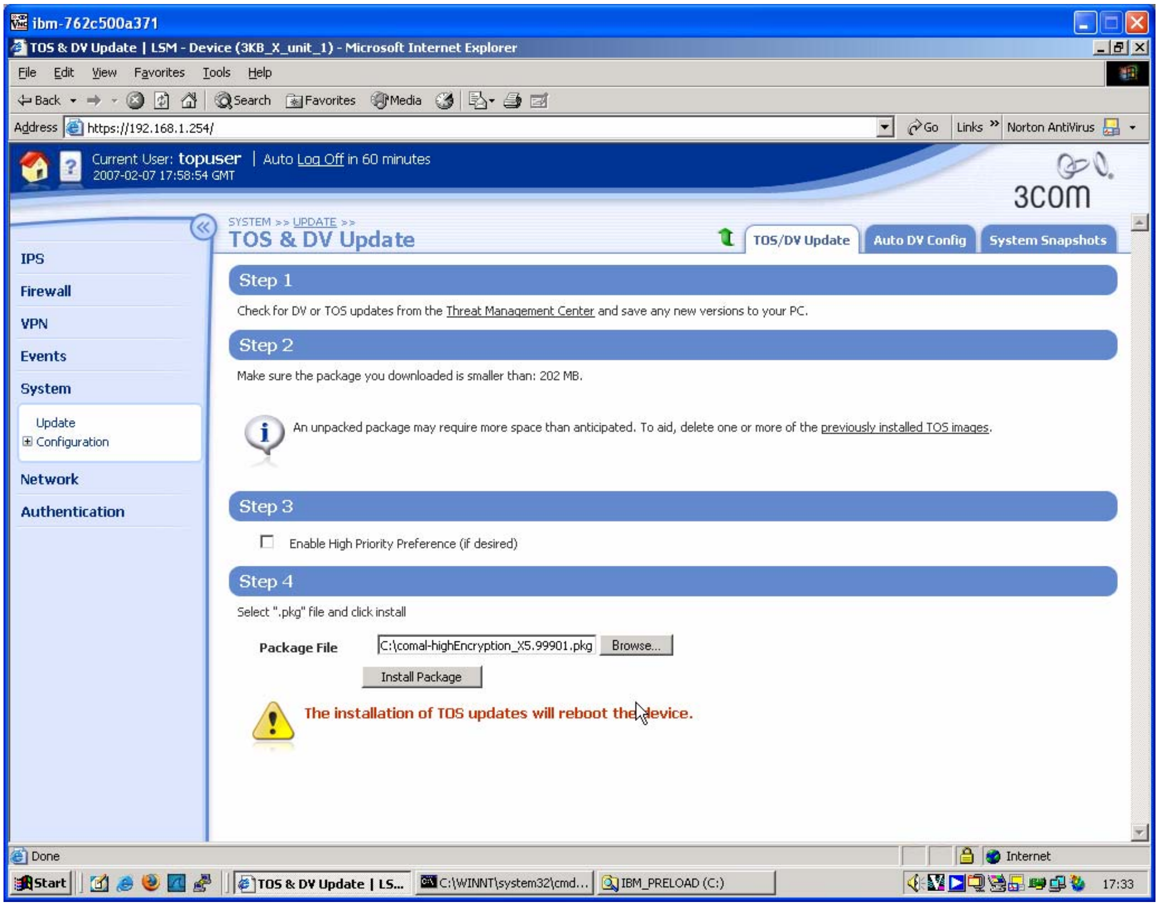
Firewall rules – the firewall rules in the factory default configuration will be sufficient – specifically this one:

```
2        permit      WAN         this-device      vpn-protocols
```

3.1.2 Load the Strong Encryption Package (Recommended)

For compliance with export regulations, the X-family devices are shipped from the factory with encryption types with keys below 64 bits (i.e. DES). This will work with Windows XP, but weak encryption is no longer considered suitable for the protection of commercial VPNs. To enable higher encryption key sizes to be used (e.g. 3DES, AES) a Strong Encryption package must be loaded onto the device. This package is only available to approved end users in approved locations.

1. Acquire the Strong Encryption package from the TMC and load it onto PC1. Select the appropriate encryption package for your X-family device.
2. Open a browser on PC1, connect to https://192.168.1.254 and login as the user you set up during the OBE.
3. Navigate to System -> Update, open the “TOS/DV Update” tab and complete the form as shown below with the path of the Strong Encryption package on PC1. Click “Install Package”.



TOS & DV Update

Step 1

Check for DV or TOS updates from the Threat Management Center and save any new versions to your PC.

Step 2

Make sure the package you downloaded is smaller than: 202 MB.

An unpacked package may require more space than anticipated. To aid, delete one or more of the previously installed TOS images.

Step 3

□ Enable High Priority Preference (if desired)

Step 4

Select ".pkg" file and click install

Package File: C:\comal-highEncryption_X5.99901.pkg [Browse...]

[Install Package]

The installation of TOS updates will reboot the device.

4. The package will be installed and the X-family device will reboot. The X-family device is ready to set up the VPN when reboot has completed.

4 Configuring L2TP/IPSec with Pre-Shared Key (PSK)

4.1 High-level steps …

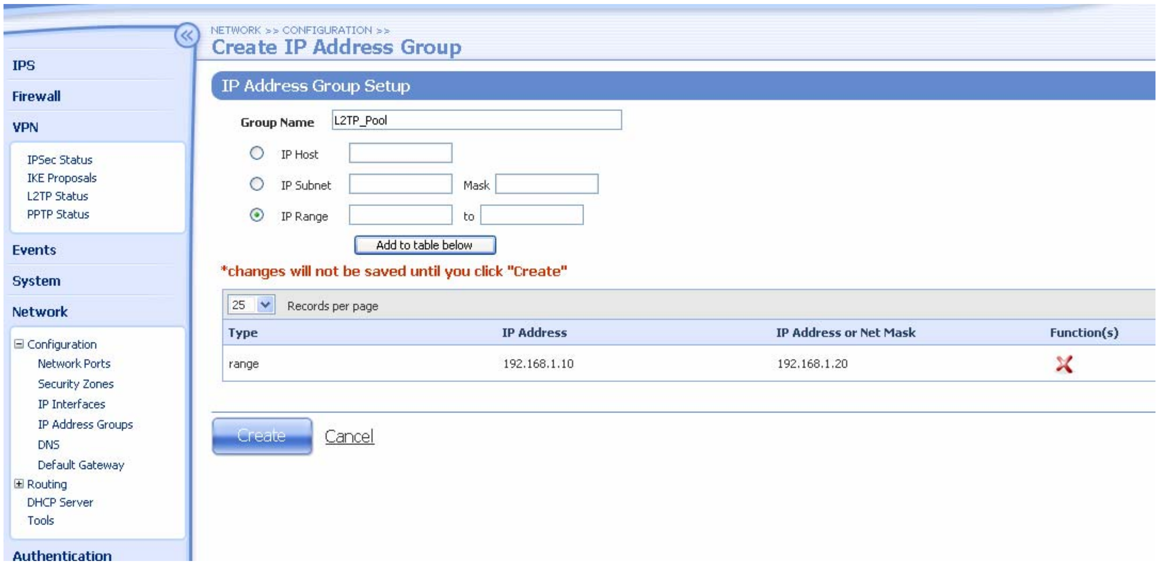
Configuring L2TP/IPSec consists of:

- Create an IP address group for L2TP VPN Clients
- Configure and enable L2TP server on the X-family.
- Configure the Default SA encryption method on the X-family.
- Configure firewall rules to allow IPSec to the X-family WAN interface (for IPSec), and from the terminating security zone to the X-family (for L2TP).
- Configure the Windows XP client using dial-up networking

4.2 3Com X-family Configuration

1) Login to your X-family web interface (LSM).
2) Create an IP address group for the L2TP IP Pool.
    a) Click Network > Configuration > IP Address Groups in the navigation menu.
    b) Click “Create Address Group”

c) Give the Group a name e.g. **L2TP_Pool**
d) Select the method to specify the address group. For this example we'll select "IP Range". Enter the Range e.g. **192.168.1.10 to 192.168.1.20**[1]**. It is recommended to use IP addresses within the same IP subnet as your LAN which are unused by any other device.**
e) Click "Add to table below" to enter that range.
f) Add more ranges, subnets or hosts as required.
g) Click "Create" to commit the changes.



NETWORK >> CONFIGURATION >>
Create IP Address Group

IP Address Group Setup

Group Name: L2TP_Pool

○ IP Host
○ IP Subnet Mask
● IP Range to

*changes will not be saved until you click "Create"

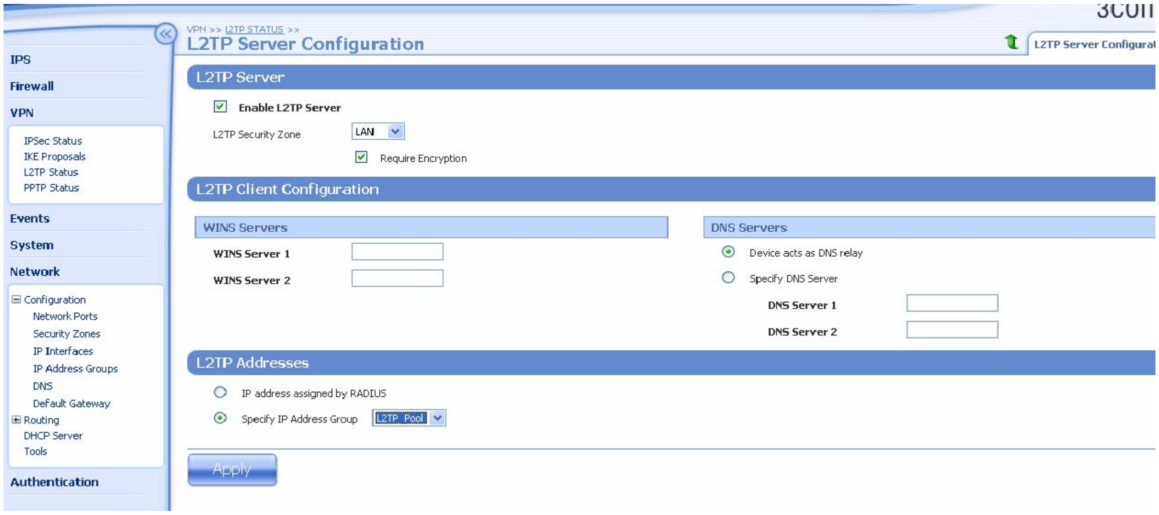
25 Records per page

Type	IP Address	IP Address or Net Mask	Function(s)
range	192.168.1.10	192.168.1.20	✕

3) Enable L2TP Server on X-family.
a) Click VPN > L2TP Status > Server Configuration in the navigation menu.
b) Click the tab in the top right "L2TP Server Configuration"
c) Click "Enable L2TP Server"
d) Set L2TP Security Zone to LAN[2].
e) Select "Require Encryption" - this will ensure IPSec is used
f) Enter any DNS and WINS settings
g) Select the IP Address Group (IP group created in previous step – L2TP_Pool)
h) Click "Apply". The screen will refresh.

[1] You must ensure the address range meets the following criteria:
a) It is part of the Security Zone the L2TP tunnel will be set to terminate within.
b) The terminating Security Zone in the L2TP Server configuration is assigned to an *internal* virtual interface.
c) The address range does not conflict with others used for DHCP server etc.

[2] Note more sophisticated setups are possible here terminating in other zones but this is the simplest setup.



VPN >> L2TP STATUS >>

L2TP Server Configuration

L2TP Server

☑ Enable L2TP Server

L2TP Security Zone: LAN

☑ Require Encryption

L2TP Client Configuration

WINS Servers

WINS Server 1

WINS Server 2

DNS Servers

● Device acts as DNS relay

○ Specify DNS Server

DNS Server 1

DNS Server 2

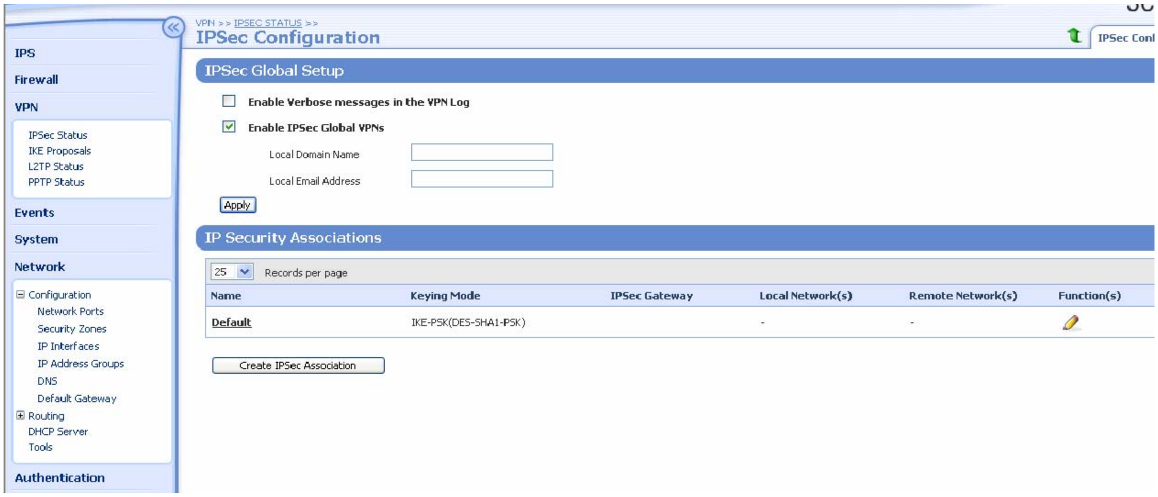
L2TP Addresses

○ IP address assigned by RADIUS

● Specify IP Address Group: L2TP_Pool

Apply

4) Enable IPSec VPNs.
   a) Click VPN > IPSec/IKE Status > IPSEC Configuration in the navigation menu.
   b) Click “Enable IPSec Global VPNs”. Since the tunnel will be Main Mode there is no need to supply a Local Domain Name or Local Email Address. Click Apply.



VPN >> IPSEC STATUS >>

IPSec Configuration

IPSec Global Setup

□ Enable Verbose messages in the VPN Log

☑ Enable IPSec Global VPNs

Local Domain Name

Local Email Address

Apply

IP Security Associations

25 Records per page

Name	Keying Mode	IPSec Gateway	Local Network(s)	Remote Network(s)	Function(s)
Default	IKE-PSK(DES-SHA1-PSK)		-	-	✎

Create IPSec Association

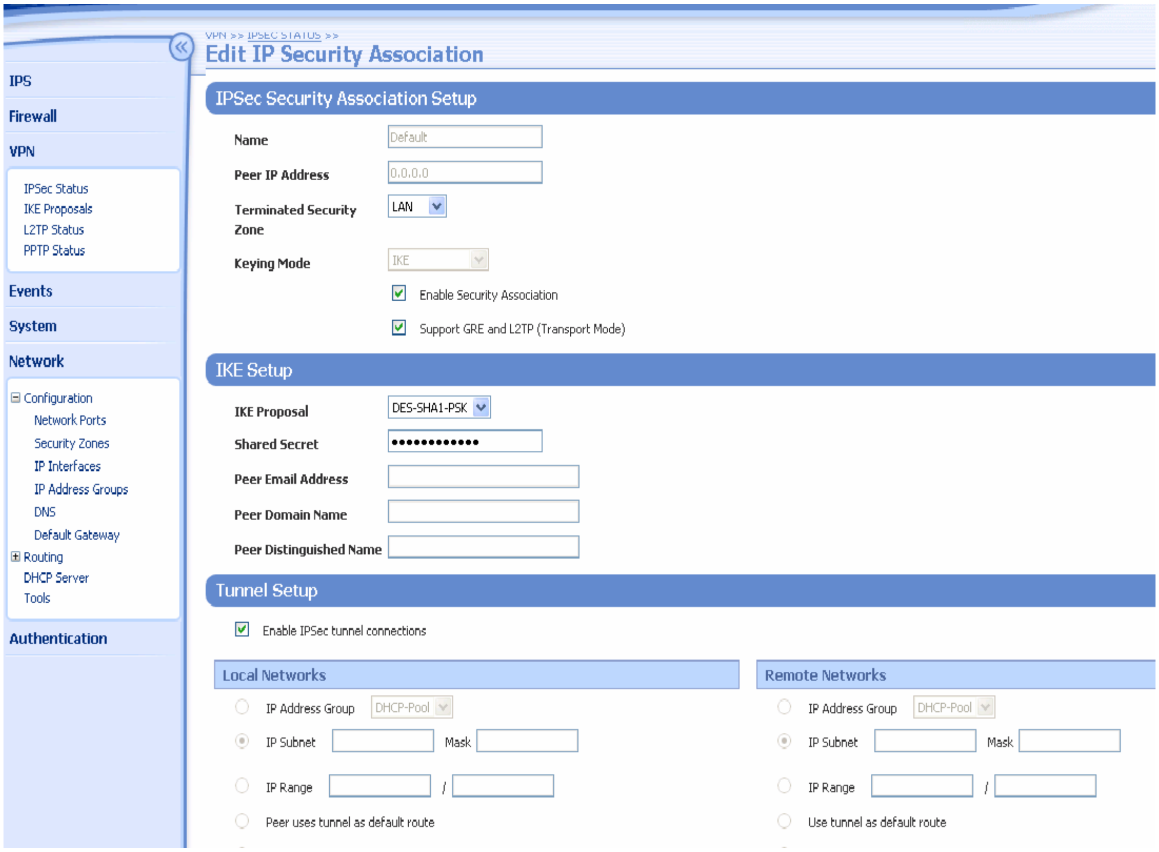
5) In the same dialog, configure the Default SA encryption parameters.
   Note: The default SA is always present and cannot be deleted
   a) Click the pencil icon next to the Security Association called “Default”.
   b) Click “Enable Security Association”.
   c) Ensure that “Support GRE and L2TP” is enabled.
   d) Select the security zone to terminate L2TP/IPSec connections onto – this should be LAN in this example.
   e) The “Keying mode” should already be IKE.
   f) Select the IKE Proposal from the pulldown list. (Note: Only DES encryption will initially be available. It is recommended that a 3DES-SHA1-PSK IKE

proposal is created and used for higher security. However, this requires that the X-family Strong Encryption package has been downloaded onto the unit, before a 3DES IKE proposal may be created.)

g) Enter the shared secret to be used. Note the shared secret will be masked and it must be at least eight characters long. Make a note of the shared secret as it must match the shared secret used by the VPN Client.

h) Ensure that "Enable IPSec tunnel connections" is enabled.

i) Click "Save". Note the screen may not update but the Save has occurred.



Edit IP Security Association

IPSec Security Association Setup

Name: Default

Peer IP Address: 0.0.0.0

Terminated Security Zone: LAN

Keying Mode: IKE

☑ Enable Security Association

☑ Support GRE and L2TP (Transport Mode)

IKE Setup

IKE Proposal: DES-SHA1-PSK

Shared Secret: ••••••••••••

Peer Email Address:

Peer Domain Name:

Peer Distinguished Name:

Tunnel Setup

☑ Enable IPSec tunnel connections

Local Networks

○ IP Address Group: DHCP-Pool

● IP Subnet: Mask:

○ IP Range: /

○ Peer uses tunnel as default route

Remote Networks

○ IP Address Group: DHCP-Pool

● IP Subnet: Mask:

○ IP Range: /

○ Use tunnel as default route

6) Check Firewall Policies.

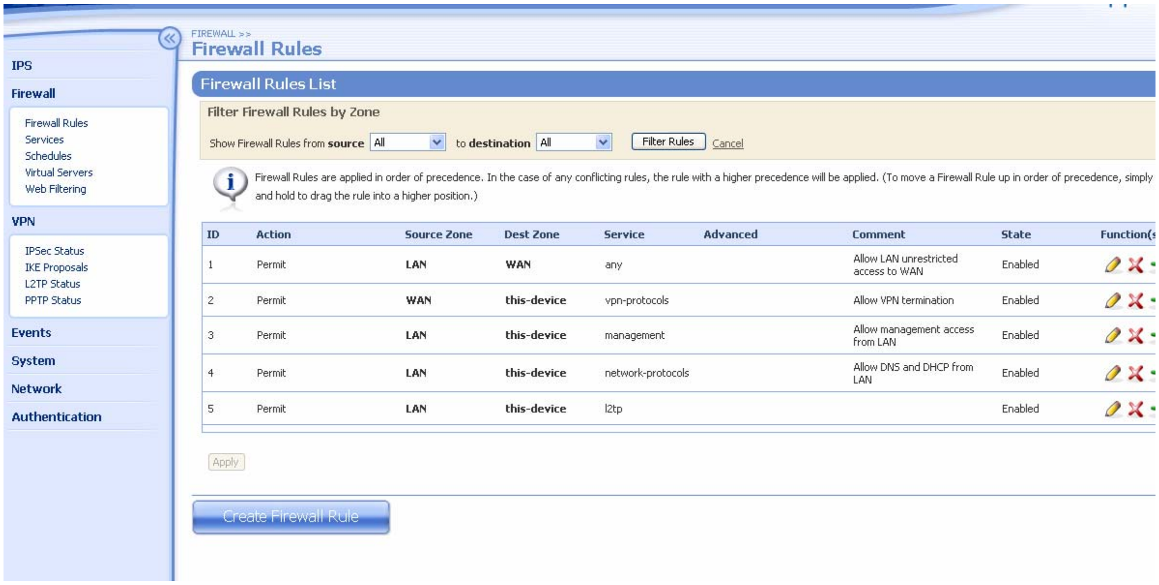
If you are using multiple security zones, and/or have changed the terminating zone from LAN, and/or have change the policy rules for traffic allowed to the X-family from the WAN, you should perform this step.

Note: Remember that the firewall rule table is ordered with traffic being matched top to bottom.

a) Ensure that there are suitable firewall policy rules allowing traffic to/from other Security Zones and the Security Zone you have set for the L2TP Server.

b) Ensure that there is a policy rule allowing the IPSec tunnel traffic to the *WAN* security zone[3].
c) Ensure that there is a policy rule allowing L2TP traffic (UDP port 1701) from the terminating security zone for L2TP Server to this-device. This allows the L2TP traffic to flow after the IPSec tunnel is terminated.
d) Ensure that there is a policy rule allowing this-device to send ANY protocol to ANY zone [4].

Here is a typical table of firewall rules that complies with the above requirements.



Show Firewall Rules from **source** All to **destination** All

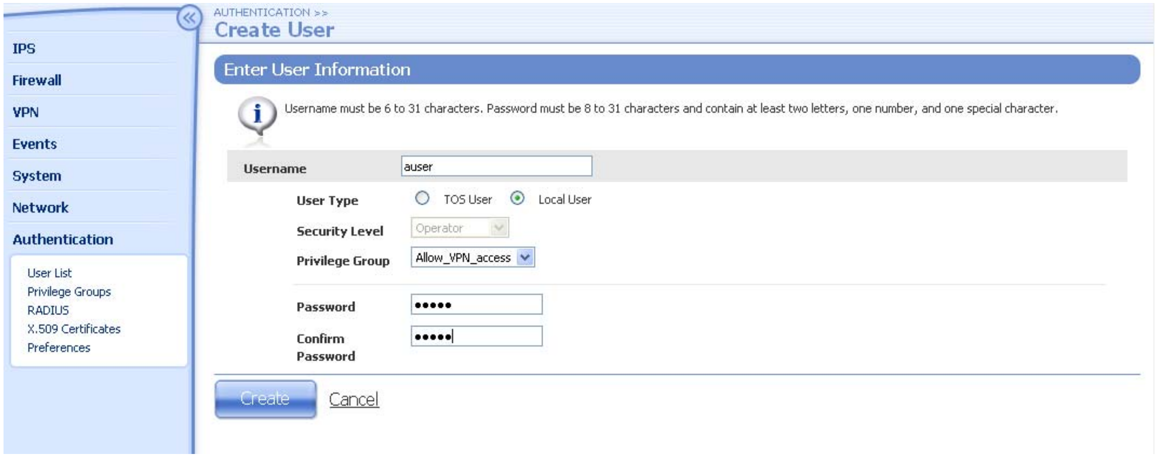
Firewall Rules are applied in order of precedence. In the case of any conflicting rules, the rule with a higher precedence will be applied. (To move a Firewall Rule up in order of precedence, simply and hold to drag the rule into a higher position.)

ID	Action	Source Zone	Dest Zone	Service	Advanced	Comment	State	Function(s
1	Permit	**LAN**	**WAN**	any		Allow LAN unrestricted access to WAN	Enabled	✎ ✗
2	Permit	**WAN**	**this-device**	vpn-protocols		Allow VPN termination	Enabled	✎ ✗
3	Permit	**LAN**	**this-device**	management		Allow management access from LAN	Enabled	✎ ✗
4	Permit	**LAN**	**this-device**	network-protocols		Allow DNS and DHCP from LAN	Enabled	✎ ✗
5	Permit	**LAN**	**this-device**	l2tp			Enabled	✎ ✗

7) Create a User Account. The following uses device authentication but users can also be authenticated via a RADIUS server which is configured on the device.
   a) Click Authentication > User List in the navigation menu.
   b) Click "Create a New User" to create a new user.
   c) Enter the username in the "Login" field - ***note: this is case sensitive.*** In this example we use "auser".
   d) Select User Type as "Local User".
   e) Under "Privilege Group" select "**Allow VPN Access".**
   f) Enter and confirm the password - ***note: this is case sensitive.***
   g) Click Create.

[3] The default Service Group vpn-protocols and default firewall rules will allow this. Protocols required are l2tp, ike and nat-t-ipsec.

[4] There is a "hidden" firewall rule that enables this, unless a "DENY" rule has been specified in the firewall table that overrules it.



AUTHENTICATION >>

Create User

Enter User Information

Username must be 6 to 31 characters. Password must be 8 to 31 characters and contain at least two letters, one number, and one special character.

Username	auser
User Type	○ TOS User ● Local User
Security Level	Operator
Privilege Group	Allow_VPN_access
Password	•••••
Confirm Password	•••••

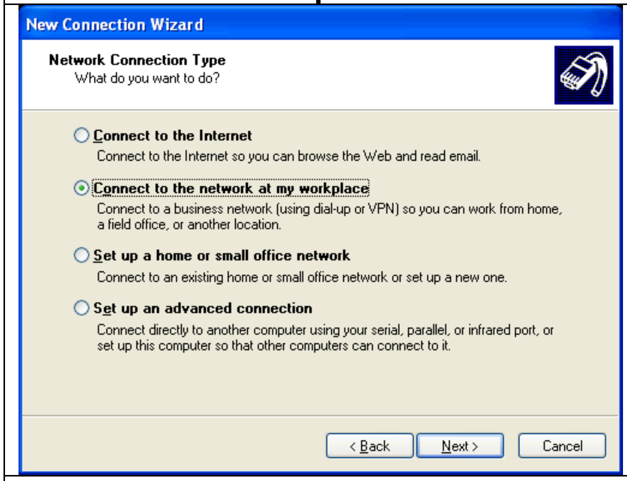
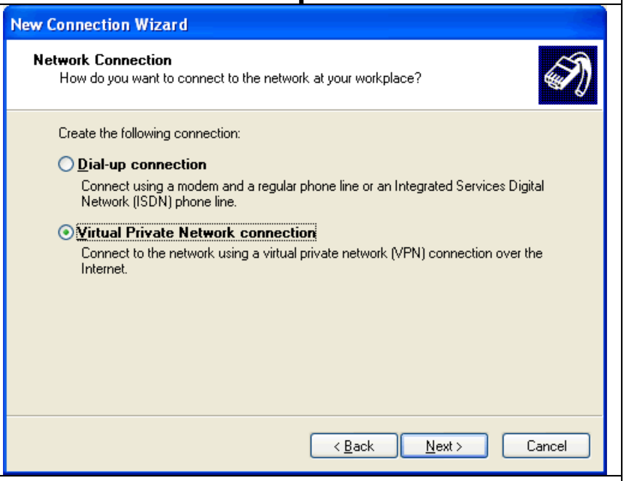
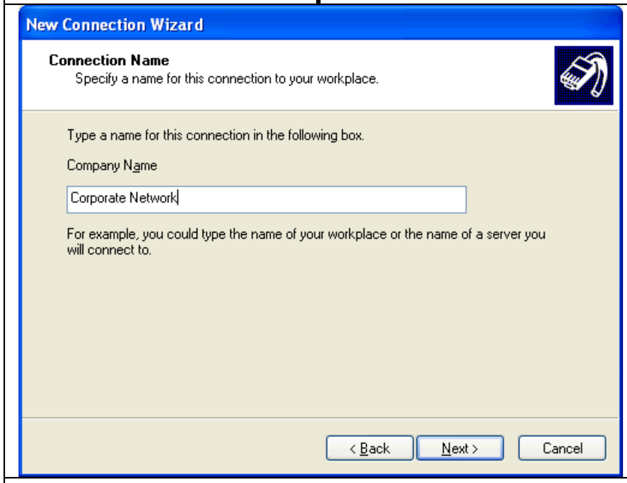
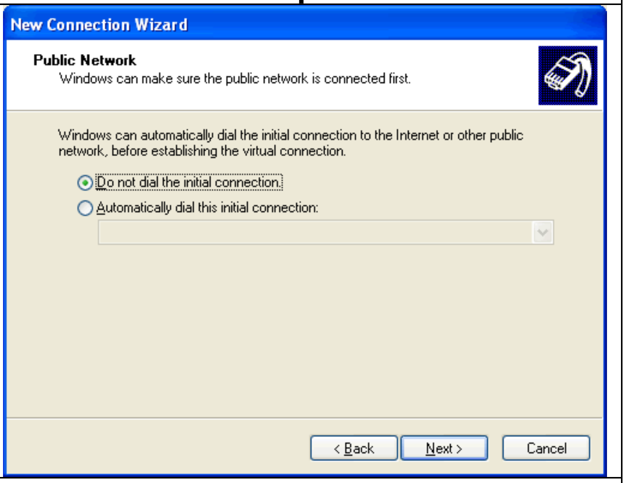
The X-family is now configured, now you need to configure the Windows clients…

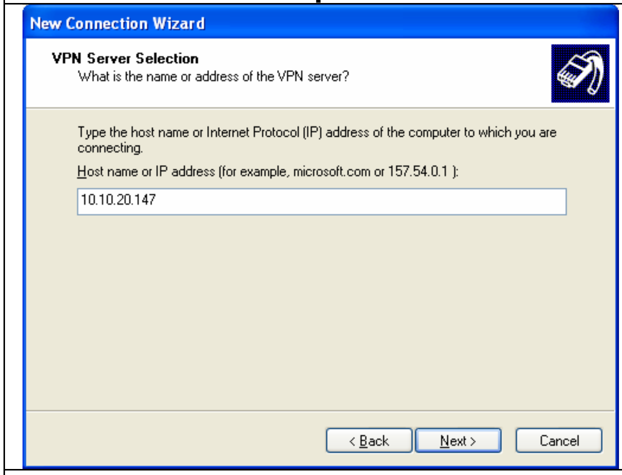
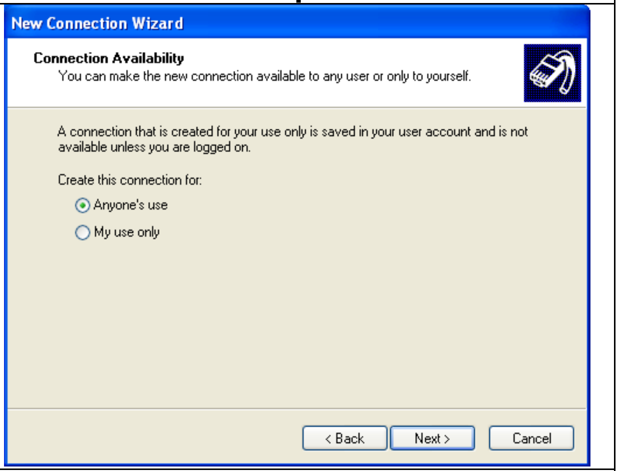
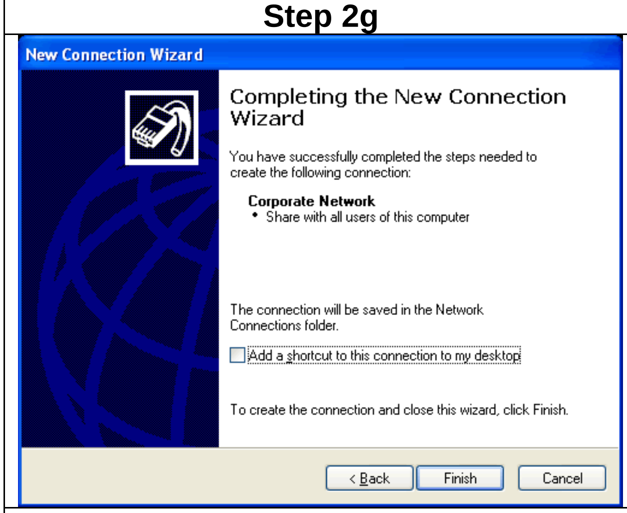
4.3 Windows XP Client Configuration for L2TP/IPSec with PSK

Note: These instructions are for Windows XP. The same principle applies to other operating systems.

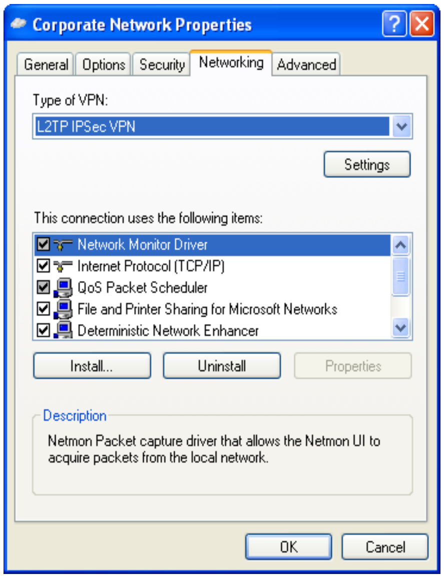
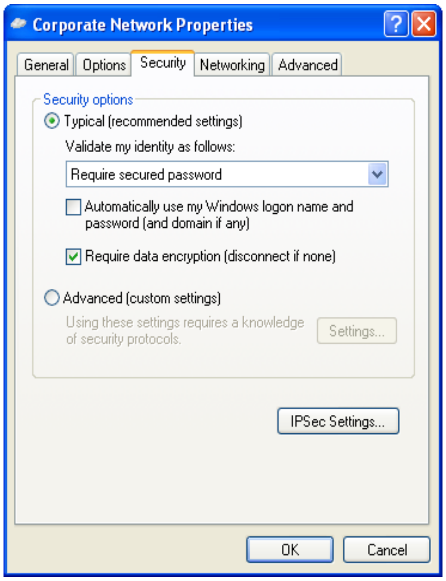
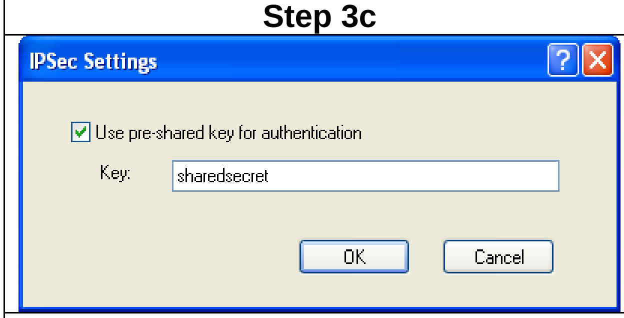
1) From Start Menu, select “Connect To”.

2) Click “Set up a Connection or Network”.
   Windows XP then runs the New Connection Wizard…

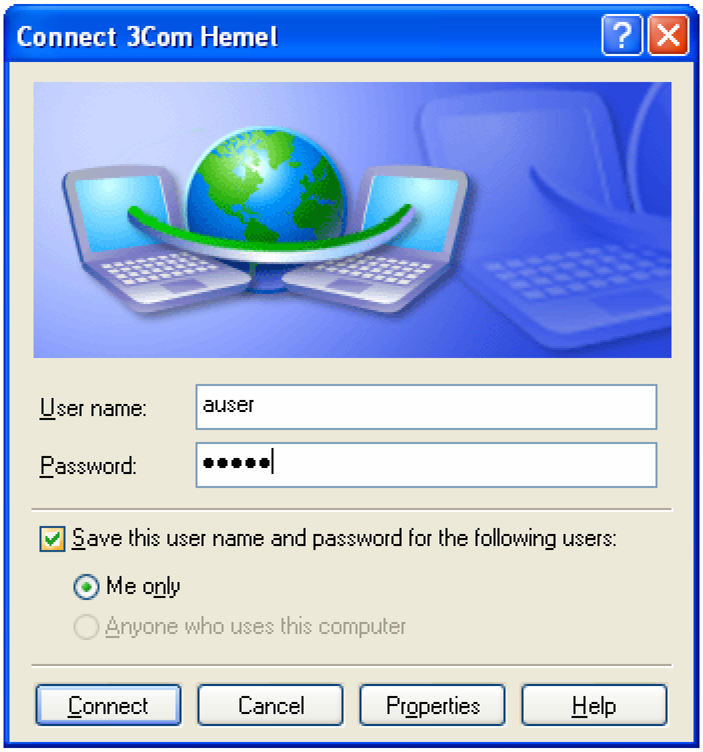
Step 2a	Step 2b
 New Connection Wizard **Network Connection Type** What do you want to do? ○ **Connect to the Internet** Connect to the Internet so you can browse the Web and read email. ● **Connect to the network at my workplace** Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location. ○ **Set up a home or small office network** Connect to an existing home or small office network or set up a new one. ○ **Set up an advanced connection** Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it. < Back · Next > · Cancel	 New Connection Wizard **Network Connection** How do you want to connect to the network at your workplace? Create the following connection: ○ **Dial-up connection** Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line. ● **Virtual Private Network connection** Connect to the network using a virtual private network (VPN) connection over the Internet. < Back · Next > · Cancel
Connect to network at my workplace	Virtual Private Network
Step 2c	**Step 2d**
 New Connection Wizard **Connection Name** Specify a name for this connection to your workplace. Type a name for this connection in the following box. Company Name Corporate Network For example, you could type the name of your workplace or the name of a server you will connect to. < Back · Next > · Cancel	 New Connection Wizard **Public Network** Windows can make sure the public network is connected first. Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection. ● Do not dial the initial connection. ○ Automatically dial this initial connection: < Back · Next > · Cancel
Give the connection a name	Select whether to dial another connection first

Step 2e	**Step 2f**
 New Connection Wizard **VPN Server Selection** What is the name or address of the VPN server? Type the host name or Internet Protocol (IP) address of the computer to which you are connecting. Host name or IP address (for example, microsoft.com or 157.54.0.1): 10.10.20.147 < Back · Next > · Cancel	 New Connection Wizard **Connection Availability** You can make the new connection available to any user or only to yourself. A connection that is created for your use only is saved in your user account and is not available unless you are logged on. Create this connection for: ● Anyone's use ○ My use only < Back · Next > · Cancel
Enter the public WAN IP address of X-family	Select whether this connection is shared.
Step 2g	
 New Connection Wizard Completing the New Connection Wizard You have successfully completed the steps needed to create the following connection: **Corporate Network** • Share with all users of this computer The connection will be saved in the Network Connections folder. □ Add a shortcut to this connection to my desktop To create the connection and close this wizard, click Finish. < Back · Finish · Cancel	
Hit finish to complete the wizard	

3) After creating the connection you will be prompted to connect for the first time. Press "Properties" to force the VPN connection type.

Step 3a	**Step 3b**
 Corporate Network Properties General | Options | Security | Networking | Advanced Type of VPN: L2TP IPSec VPN Settings This connection uses the following items: ☑ Network Monitor Driver ☑ Internet Protocol (TCP/IP) ☑ QoS Packet Scheduler ☑ File and Printer Sharing for Microsoft Networks ☑ Deterministic Network Enhancer Install... Uninstall Properties Description Netmon Packet capture driver that allows the Netmon UI to acquire packets from the local network. OK Cancel	 Corporate Network Properties General | Options | Security | Networking | Advanced Security options ● Typical (recommended settings) Validate my identity as follows: Require secured password ☐ Automatically use my Windows logon name and password (and domain if any) ☑ Require data encryption (disconnect if none) ○ Advanced (custom settings) Using these settings requires a knowledge of security protocols. Settings... IPSec Settings... OK Cancel
Select the Networking Tab. Under "Type of VPN" select L2TP/IPSecVPN from pull-down list – do NOT click "OK".	Select the "Security" tab and click the "IPSec Settings…" button.
Step 3c	
 IPSec Settings ☑ Use pre-shared key for authentication Key: sharedsecret OK Cancel	
Click to enable "Use pre-shared key for authentication" and enter the same shared secret as entered for the Default SA in Step 5 on the X-family. Click "OK" to confirm all the settings on the VPN.	

4) Click OK to get back to the username/password prompt. Enter the user details configured on the X-family for the local user - this must match Step 8 where the local user name and password were configured on the X-family. ***Note: Remember both username and passwords are case sensitive***



User name: auser

Password: ●●●●●

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Connection to X-family should now be established.

5 Configuring L2TP/IPSec with X.509 Digital Certificate

X.509 Digital Certificates provide a stronger level of authentication and security than Pre-Shared Key (PSK) for IPSec connections. X.509 uses Public Key Infrastructure (PKI) encryption mechanisms to ensure full privacy without the need to exchange a private key.

To deploy a VPN client solution using X.509, two certificates are generated by a trusted Certificate Authority (CA) – one for the Windows VPN client, and one for the X-family device terminating the IPSec connection. The certificates uniquely identify each end point of the connection, ensuring that each end point can know with certainty that the partner is who they say they are. If not using a 3rd party Certificate Authority you can still generate certificates that are *self signed* through readily available tools.

5.1 High Level Steps

The high level steps for using X.509 certificates with L2TP/IPSec VPN clients on Windows XP are:

- Generate certificates for use on the X-family and the VPN client Windows machine.

  - Generate the self-signed CA certificate.
  - Create a local certificate request on the X-family, copy it to the certificate machine and sign it with the CA certificate.
  - Create a local certificate request on the XP PC, copy it to the certificate server and sign it with the CA certificate.
- On the X-family:
  - Install the signed CA and local certificates.
  - Associate the local certificate with the IKE proposal.
  - Associate the IKE proposal with the IPSec Default Security Association.
  - Ensure the Default Security Association is using transport mode.
- On Windows XP:
  - Install the signed CA and L2TP client local certificates.
  - Create the Windows client IPSec connection, selecting to use certificates for IPSec authentication.

5.2 Creating and Loading the Certificates

Three certificates are required for this configuration:

- **A CA certificate**. This is created on the certificate server and installed on both the X-family and the Windows XP client.

  The certificates used by Windows for IPSec *must* be signed or Windows will fail the IPSec main mode negotiation. When Windows XP negotiates the main mode IPSec tunnel with the X-family box, it exchanges the list of Certificate Authorities (CA's) it will accept certificates from. A CA certificate must be installed in Windows XP to authenticate the local L2TP client certificate. The X-family can use a similar scheme.

- **A Local certificate on the X-family**.

  The Local certificate request is created on the X-family, is signed by the shared CA and is used to authenticate the IPSec server within the X-family.

- **A Local certificate for the VPN client on Windows XP.**

  The Personal certificate request created on the XP PC is signed by the shared CA and is used to authenticate the Windows XP IPSec client.

It is strongly advised that the Local Certificates are generated through a PKI setup (e.g. the Windows Certificate Server that ships in Windows 200x Server) ensuring that private keys are not exposed on the network. This is outside the scope of this document however. Note that X-family does not currently support an automated certificate enrolment protocol. To demonstrate the techniques, this document will use the OpenSSL utility on a Linux platform with a self-signed certificate.

Below is an example creating the certificates using the CA wrapper normally available in the /etc/pki/tls/misc/CA directory, and openSSL. Once the CA certificate is created, the example signs a certificate request created on the X-family device using the created CA certificate. Note that the signing process could be performed by a trusted CA server such as Verisign or Thawte.

1. Create the Certificates on the Certificate Server.

```
[test]:
[test]: openssl version
OpenSSL 0.9.7a Feb 19 2003
[test]:
[test]: #############################
[test]: # create the CA certificate #
[test]: #############################
[test]:
[test]: ./CA –newca
./CA -newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 1024 bit RSA private key
..++++++
....++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:England
Locality Name (eg, city) [Newbury]:London
Organization Name (eg, company) [My Company Ltd]:3Com
Organizational Unit Name (eg, section) []:3Com
Common Name (eg, your name or your server's hostname) []:MyCA
Email Address []:test@3Com.com
[test]:
[test]:
[test]: #####################################################
[test]: # create Local Certificate request for the X-family #
[test]: #####################################################
test]:
[test]: ./CA –newreq
Generating a 1024 bit RSA private key
...++++++
.++++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:England
Locality Name (eg, city) [Newbury]:London
Organization Name (eg, company) [My Company Ltd]:3Com
Organizational Unit Name (eg, section) []:3Com
Common Name (eg, your name or your server's hostname) []:X505
Email Address []:test@3Com.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request (and private key) is in newreq.pem
[test]:
[test]:
[test]: ###############################################
[test]: # Sign the X-family Local Certificate request #
[test]: ###############################################
[test]:
[test]:./CA -sign
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Apr 10 09:42:18 2006 GMT
            Not After : Apr 10 09:42:18 2007 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = England
            localityName              = London
            organizationName          = 3Com
            organizationalUnitName    = 3Com
            commonName                = X505
            emailAddress              = test@3Com.com
        X.509v3 extensions:
            X.509v3 Basic Constraints:
            CA:FALSE
            Netscape Comment:
```

```
            OpenSSL Generated Certificate
            X.509v3 Subject Key Identifier:
            02:4E:62:5E:C9:C4:D4:FD:69:5C:3C:14:2E:71:45:C9:52:99:AF:A0
            X.509v3 Authority Key Identifier:

keyid:BF:73:F9:05:25:14:B6:B7:CC:BE:13:52:6D:C7:08:1A:03:EA:4C:34

DirName:/C=GB/ST=England/L=London/O=3Com/OU=3Com/CN=MyCA/emailAddress=t
est@3Com.com
            serial:00

Certificate is to be certified until Apr 10 09:42:18 2007 GMT (365
days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=GB, ST=England, L=London, O=3Com, OU=3Com,
CN=MyCA/emailAddress=test@3Com.com
        Validity
            Not Before: Apr 10 09:42:18 2006 GMT
            Not After : Apr 10 09:42:18 2007 GMT
        Subject: C=GB, ST=England, L=London, O=3Com, OU=3Com,
CN=X505/emailAddress=test@3Com.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:9f:39:a3:f1:03:29:82:fd:95:9c:00:c5:16:14:
                    c9:cd:fc:a0:ff:f2:08:d3:ad:7d:bd:82:30:31:ec:
                    43:46:37:b0:a7:49:72:0c:a5:03:f3:f9:e2:68:44:
                    31:a9:5a:54:7e:88:68:b8:7a:38:d6:93:2a:ad:ed:
                    d1:29:20:24:e6:58:b0:34:02:d5:37:f2:87:2f:f6:
                    be:cc:5b:58:29:d6:4a:15:2d:c1:6a:32:45:68:23:
                    dc:44:48:c8:59:22:bf:58:4e:12:e7:88:8b:db:8c:
                    96:38:38:d4:90:75:67:5d:8c:96:04:13:2c:ed:56:
                    7b:08:6f:60:97:0a:d6:e5:29
                Exponent: 65537 (0x10001)
        X.509v3 extensions:
            X.509v3 Basic Constraints:
            CA:FALSE
            Netscape Comment:
            OpenSSL Generated Certificate
            X.509v3 Subject Key Identifier:
```

```
            02:4E:62:5E:C9:C4:D4:FD:69:5C:3C:14:2E:71:45:C9:52:99:AF:A0
            X.509v3 Authority Key Identifier:

keyid:BF:73:F9:05:25:14:B6:B7:CC:BE:13:52:6D:C7:08:1A:03:EA:4C:34

DirName:/C=GB/ST=England/L=London/O=3Com/OU=3Com/CN=MyCA/emailAddress=t
est@3Com.com
            serial:00

    Signature Algorithm: md5WithRSAEncryption
        31:f2:b4:98:10:ca:63:e4:50:b8:af:a0:f7:6e:75:92:18:88:
        ce:51:87:92:16:8f:d0:21:10:81:87:10:02:25:e4:1a:24:f0:
        f7:c7:2c:3e:bf:af:86:7c:61:b7:50:6d:32:ec:a7:aa:d8:50:
        17:3c:3e:d4:30:5a:21:27:cf:bb:15:7f:a6:35:33:66:1f:a1:
        c3:12:a3:d0:bc:57:d8:43:c6:8e:75:20:b7:99:de:25:10:d9:
        69:31:84:63:85:30:15:04:08:45:20:0a:5a:cd:da:18:57:a4:
        55:00:51:45:52:18:23:f9:53:3b:0f:1f:68:c5:80:3e:f3:ef:
        7a:12
-----BEGIN CERTIFICATE-----
MIIDpzCCAxCgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBizELMAkGA1UEBhMCR0Ix
EDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEM0Nv
bTEVMBMGA1UECxMMVGlwcGluZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgYJKoZI
hvcNAQkBFhV0ZXN0QHRpcHBpbmdwb2ludC5jb20wHhcNMDYwNDEwMDk0MjE4WhcN
MDcwNDEwMDk0MjE4WjCBizELMAkGA1UEBhMCR0IxEDAOBgNVBAgTB0VuZ2xhbmQx
DzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEM0NvbTEVMBMGA1UECxMMVGlwcGlu
Z1BvaW50MQ0wCwYDVQQDEwRYNTA1MSQwIgYJKoZIhvcNAQkBFhV0ZXN0QHRpcHBp
bmdwb2ludC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ85o/EDKYL9
lZwAxRYUyc38oP/yCNOtfb2CMDHsQ0Y3sKdJcgylA/P54mhEMalaVH6IaLh6ONaT
Kq3tOSkgJOZYsDQC1Tfyhy/2vsxbWCnWShUtwWoyRWgj3ERIyFkiv1hOEueIi9uM
ljg41JB1Z12MlgQTLO1WewhvYJcK1uUpAgMBAAGjggEXMIIBEzAJBgNVHRMEAjAA
MCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAd
BgNVHQ4EFgQUAk5iXsnE1P1pXDwULnFFyVKZr6AwgbgGA1UdIwSBsDCBrYAUv3P5
BSUUtrfMvhNSbccIGgPqTDShgZGkgY4wgYsxCzAJBgNVBAYTAkdCMRAwDgYDVQQI
EwdFbmdsYW5kMQ8wDQYDVQQHEwZMb25kb24xDTALBgNVBAoTBDNDb20xFTATBgNV
BAsTDFRpcHBpbmdQb2ludDENMAsGA1UEAxMETXlDQTEkMCIGCSqGSIb3DQEJARYV
dGVzdEB0aXBwaW5ncG9pbnQuY29tggEAMA0GCSqGSIb3DQEBBAUAA4GBADHytJgQ
ymPkULivoPdudZIYiM5Rh5IWj9AhEIGHEAIl5Bok8PfHLD6/r4Z8YbdQbTLsp6rY
UBc8PtQwWiEnz7sVf6Y1M2YfocMSo9C8V9hDxo51ILeZ3iUQ2WkxhGOFMBUECEUg
ClrN2hhXpFUAUUVSGCP5UzsPH2jFgD7z73oS
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
[test]:
[test]:
[test]: ##############################################################
[test]: # Convert to PKCS#12 incorporating CA and Local Certificates #
[test]: ##############################################################
[test]:
[test]: openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -
certfile demoCA/cacert.pem -out X505.p12
Enter pass phrase for newreq.pem:
Enter Export Password:
```

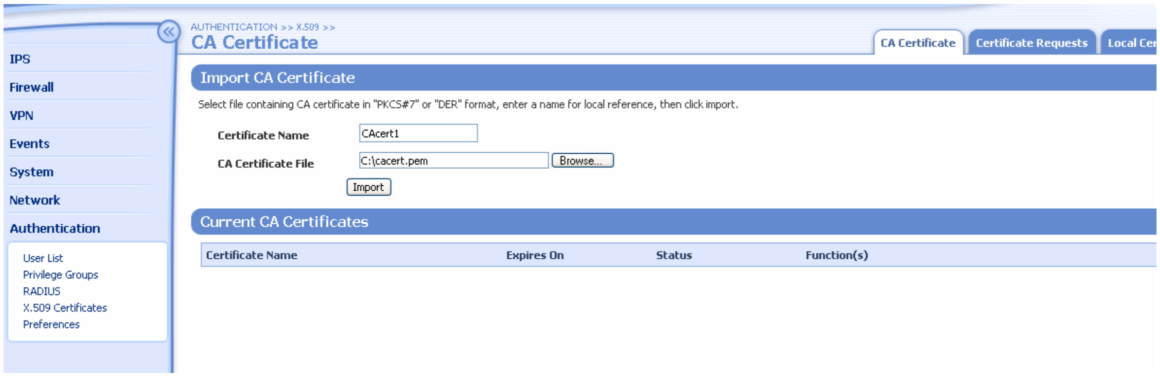
```
Verifying - Enter Export Password:
[test]:
[test]:
[test]: ###################################################
[test]: # create the Windows XP Local certificate request #
[test]: ###################################################
[test]:
[test]: ./CA -newreq
[test]: Generating a 1024 bit RSA private key
........++++++
......................++++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:Scotland
Locality Name (eg, city) [Newbury]:Edinburgh
Organization Name (eg, company) [My Company Ltd]:3Com
Organizational Unit Name (eg, section) []:3Com
Common Name (eg, your name or your server's hostname) []:L2TP Client
Email Address []:user@3Com.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request (and private key) is in newreq.pem
[test]:
[test]:
[test]: #################################################
[test]: # Sign the Windows XP Local Certificate request #
[test]: #################################################
[test]:
[test]:./CA -sign
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
```

```
            Not Before: Apr 10 09:56:41 2006 GMT
            Not After : Apr 10 09:56:41 2007 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = Scotland
            localityName              = Edinburgh
            organizationName          = 3Com
            organizationalUnitName    = 3Com
            commonName                = L2TP Client
            emailAddress              = user@3Com.com
        X.509v3 extensions:
            X.509v3 Basic Constraints:
            CA:FALSE
            Netscape Comment:
            OpenSSL Generated Certificate
            X.509v3 Subject Key Identifier:
            C4:C1:ED:A8:8A:16:F9:6F:95:8F:5C:26:CC:DE:0E:9A:F0:81:95:D6
            X.509v3 Authority Key Identifier:

keyid:BF:73:F9:05:25:14:B6:B7:CC:BE:13:52:6D:C7:08:1A:03:EA:4C:34

DirName:/C=GB/ST=England/L=London/O=3Com/OU=3Com/CN=MyCA/emailAddress=t
est@3Com.com
            serial:00

Certificate is to be certified until Apr 10 09:56:41 2007 GMT (365
days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=GB, ST=England, L=London, O=3Com, OU=3Com,
CN=MyCA/emailAddress=test@3Com.com
        Validity
            Not Before: Apr 10 09:56:41 2006 GMT
            Not After : Apr 10 09:56:41 2007 GMT
        Subject: C=GB, ST=Scotland, L=Edinburgh, O=3Com, OU=3Com,
CN=L2TP Client/emailAddress=user@3Com.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b3:5e:65:5c:45:0f:d6:f7:ad:51:09:5f:ab:d1:
                    bd:b5:28:0a:86:e0:48:82:06:4d:4a:77:5d:db:10:
```

```
                    4c:e4:25:52:16:f2:75:98:8f:b9:2d:88:60:cb:6e:
                    97:56:b2:3c:e4:af:46:d6:d6:b1:1b:f6:4e:40:65:
                    fb:ab:92:7f:8a:9a:48:1d:28:46:e7:81:ec:85:58:
                    8f:1d:70:36:bf:2f:05:2d:a0:ef:7d:47:e4:9d:a7:
                    1f:a2:0e:76:5f:ce:60:f0:76:ae:2c:16:f6:f1:a9:
                    73:df:99:be:35:8c:e9:3a:10:87:e5:ae:a4:93:33:
                    93:5b:08:5a:76:f7:db:a4:a1
                Exponent: 65537 (0x10001)
        X.509v3 extensions:
            X.509v3 Basic Constraints:
            CA:FALSE
            Netscape Comment:
            OpenSSL Generated Certificate
            X.509v3 Subject Key Identifier:
            C4:C1:ED:A8:8A:16:F9:6F:95:8F:5C:26:CC:DE:0E:9A:F0:81:95:D6
            X.509v3 Authority Key Identifier:

keyid:BF:73:F9:05:25:14:B6:B7:CC:BE:13:52:6D:C7:08:1A:03:EA:4C:34

DirName:/C=GB/ST=England/L=London/O=3Com/OU=3Com/CN=MyCA/emailAddress=t
est@3Com.com
            serial:00

    Signature Algorithm: md5WithRSAEncryption
        66:04:78:07:ee:fa:d7:b8:6c:1a:93:d1:4f:dc:b5:f0:3f:29:
        0d:1c:d5:d1:ee:3d:72:77:89:6c:a4:b0:30:ff:e3:2c:a5:a9:
        b6:35:82:21:05:50:8a:cb:05:6d:14:2c:12:03:e0:7a:1b:cf:
        29:81:25:7b:99:bb:74:7e:88:e1:bf:1e:6a:6e:dc:4a:af:13:
        32:79:bb:19:58:29:9a:f3:50:fc:10:f0:fa:aa:28:50:cf:5a:
        e3:e1:ce:5b:54:3f:f3:dc:17:01:c5:eb:df:28:ee:fb:ae:53:
        41:78:c4:5d:9f:78:a9:37:64:57:37:37:4d:d6:d8:41:81:75:
        e4:aa
-----BEGIN CERTIFICATE-----
MIIDsjCCAxugAwIBAgIBAjANBgkqhkiG9w0BAQQFADCBizELMAkGA1UEBhMCR0Ix
EDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEM0Nv
bTEVMBMGA1UECxMMVGlwcGluZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgYJKoZI
hvcNAQkBFhV0ZXN0QHRpcHBpbmdwb2ludC5jb20wHhcNMDYwNDEwMDk1NjQxWhcN
MDcwNDEwMDk1NjQxWjCBljELMAkGA1UEBhMCR0IxETAPBgNVBAgTCFNjb3RsYW5k
MRIwEAYDVQQHEwlFZGluYnVyZ2gxDTALBgNVBAoTBDNDb20xFTATBgNVBAsTDFRp
cHBpbmdQb2ludDEUMBIGA1UEAxMLTDJUUCBDbGllbnQxJDAiBgkqhkiG9w0BCQEW
FXVzZXJAdGlwcGluZ3BvaW50LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAs15lXEUP1vetUQlfq9G9tSgKhuBIggZNSndd2xBM5CVSFvJ1mI+5LYhgy26X
VrI85K9G1taxG/Z0QGX7q5J/ippIHShG54HshViPHXA2vy8FLaDvfUfknacfog52
X85g8HauLBb28alz35m+NYzp0hCH5a6kkz0TWwhadvfbpKECAwEAAaOCARcwggET
MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENl
cnRpZmljYXRlMB0GA1UdDgQWBBTEwe2oihb5b5WPXCbM3g6a8IGV1jCBuAYDVR0j
BIGwMIGtgBS/c/kFJRS2t8y+E1JtxwgaA+pMNKGBkaSBjjCBizELMAkGA1UEBhMC
R0IxEDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChME
M0NvbTEVMBMGA1UECxMMVGlwcGluZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgYJ
KoZIhvcNAQkBFhV0ZXN0QHRpcHBpbmdwb2ludC5jb22CAQAwDQYJKoZIhvcNAQEE
BQADgYEAZgR4B+7617hsGpPRT9y18D8pDRzV0e49cneJbKSwMP/jLKWptjWCIQVQ
```

```
issFbRQsEgPgehvPKYEle5m7dH6I4b8eam7cSq8TMnm7GVgpmvNQ/BDw+qooUM9a
4+HOW1Q/89wXAcXr3yju+65TQXjEXZ94qTdkVzc3TdbYQYF15Ko=
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
[test]:
[test]:
[test]: ##############################################################
[test]: # Convert to PKCS#12 incorporating CA and Local Certificates #
[test]: ##############################################################
[test]:
[test]:openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -
certfile demoCA/cacert.pem -out l2tpclient.p12
Enter pass phrase for newreq.pem:
Enter Export Password:
Verifying - Enter Export Password:
[test]:
[test]:ls *.p12
l2tpclient.p12  X505.p12
[test]:
```

2. Import the CA certificate onto the X-family



Import CA Certificate

Select file containing CA certificate in "PKCS#7" or "DER" format, enter a name for local reference, then click import.

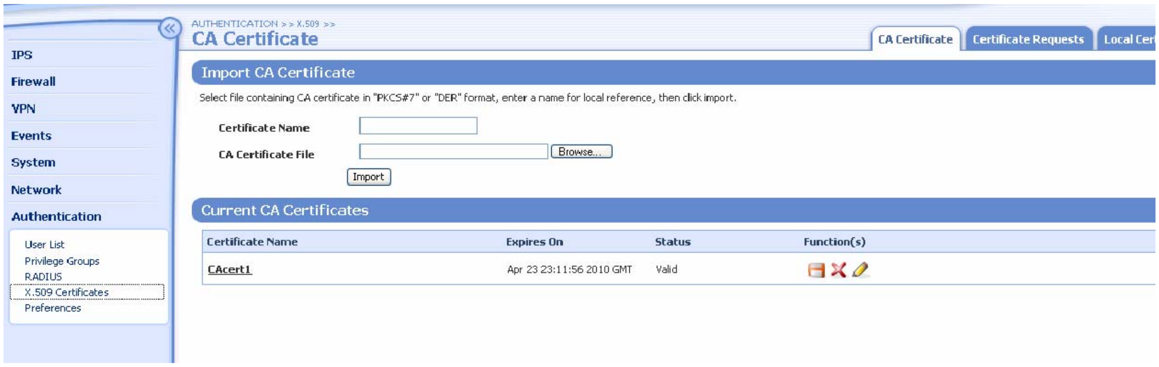
Certificate Name: CAcert1

CA Certificate File: C:\cacert.pem

Current CA Certificates

Certificate Name	Expires On	Status	Function(s)

Status of imported Certificate should be “Valid”.



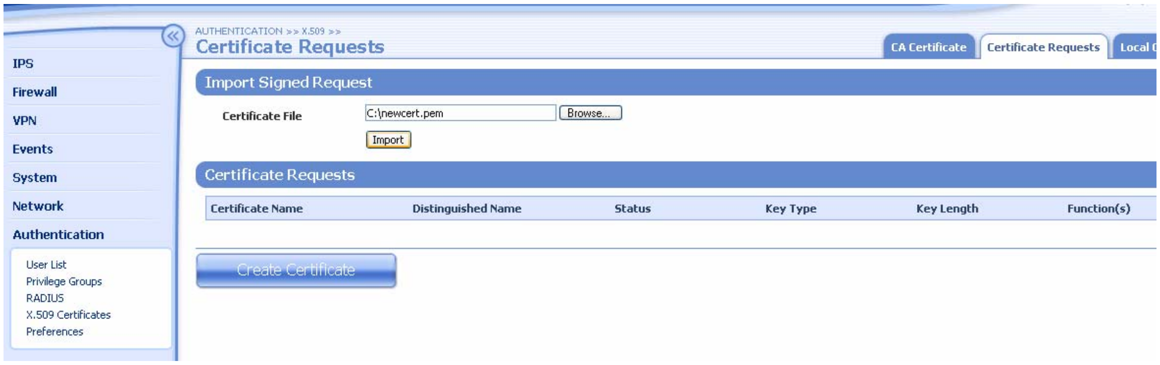
Import CA Certificate

Select file containing CA certificate in "PKCS#7" or "DER" format, enter a name for local reference, then click import.

Current CA Certificates

Certificate Name	Expires On	Status	Function(s)
CAcert1	Apr 23 23:11:56 2010 GMT	Valid	

3. Import the local certificate into the X-family.



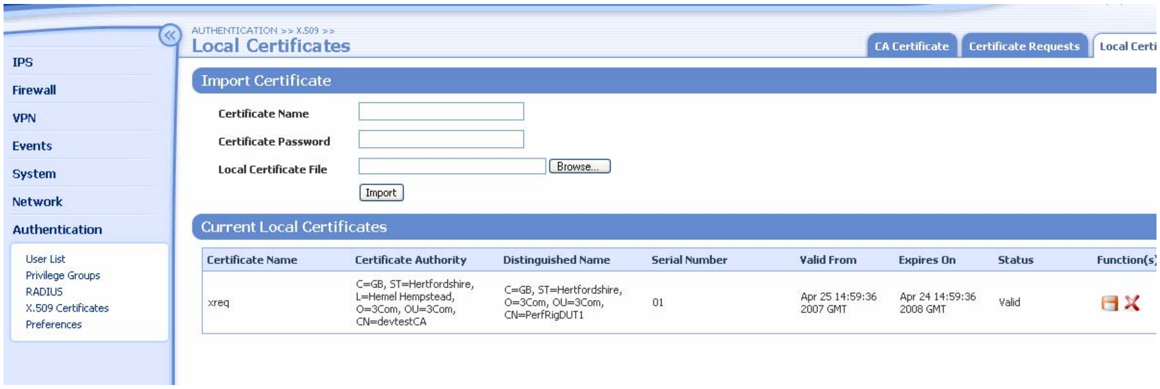
Import Signed Request

Certificate File: C:\newcert.pem

Certificate Requests

Certificate Name	Distinguished Name	Status	Key Type	Key Length	Function(s)

The certificate should appear in the Local Certificates tab and status should be “Valid”.



Import Certificate

Certificate Name

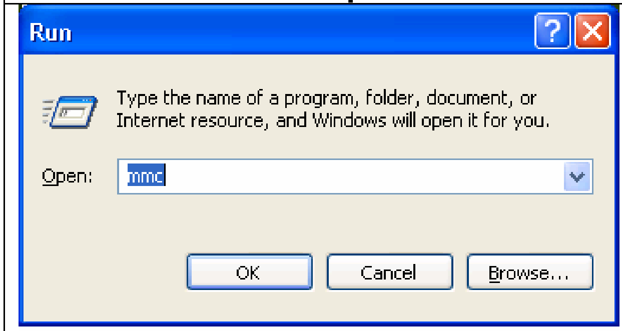
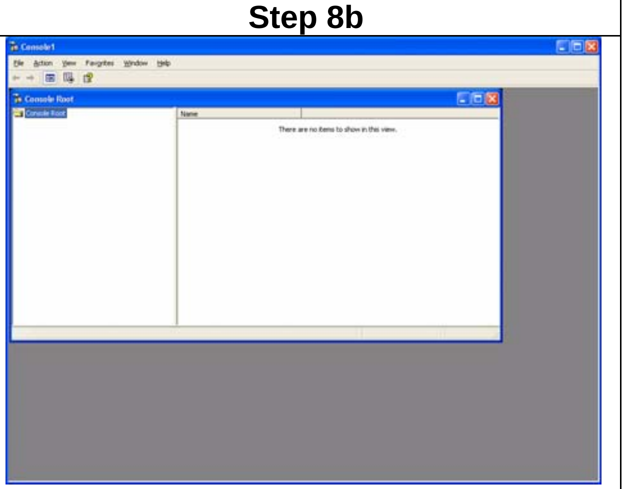
Certificate Password

Local Certificate File

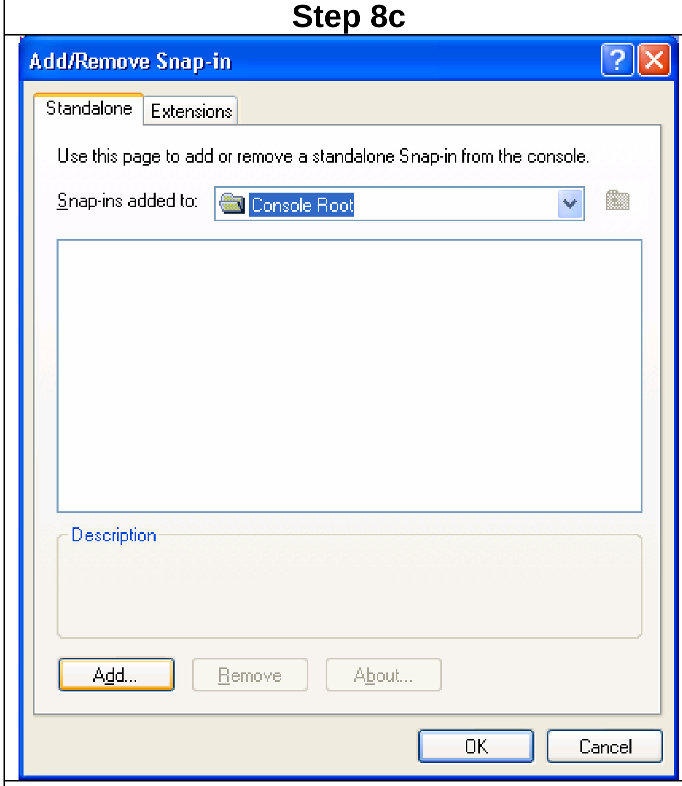
Current Local Certificates

Certificate Name	Certificate Authority	Distinguished Name	Serial Number	Valid From	Expires On	Status	Function(s)
xreq	C=GB, ST=Hertfordshire, L=Hemel Hempstead, O=3Com, OU=3Com, CN=devtestCA	C=GB, ST=Hertfordshire, O=3Com, OU=3Com, CN=PerfRigDUT1	01	Apr 25 14:59:36 2007 GMT	Apr 24 14:59:36 2008 GMT	Valid	

4. Setup the Windows XP PC for Certificate Import.

Step8a	**Step 8b**
 Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: mmc	 Console1 File Action View Favorites Window Help Console Root Console Root Name There are no items to show in this view.
Open “Run” window and type “mmc” and hit return.	MMC opens. Select File > Add/Remove Snap-in

Step 8c



Add/Remove Snap-in

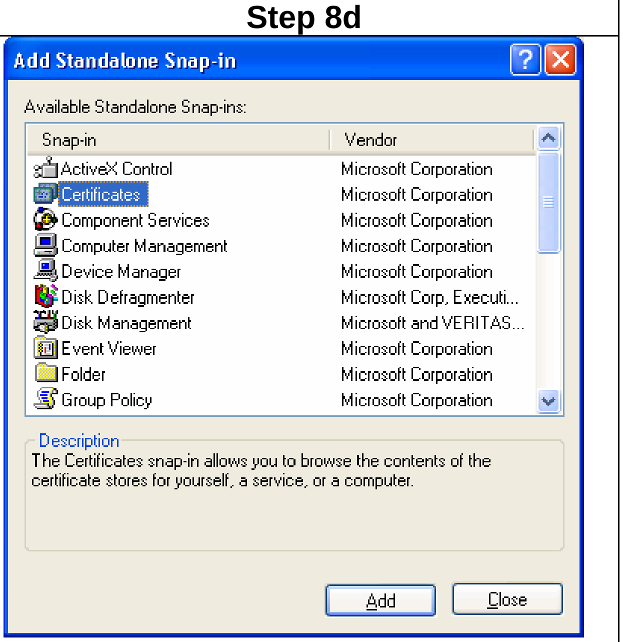
Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Description

Click “Add”.

Step 8d



Add Standalone Snap-in

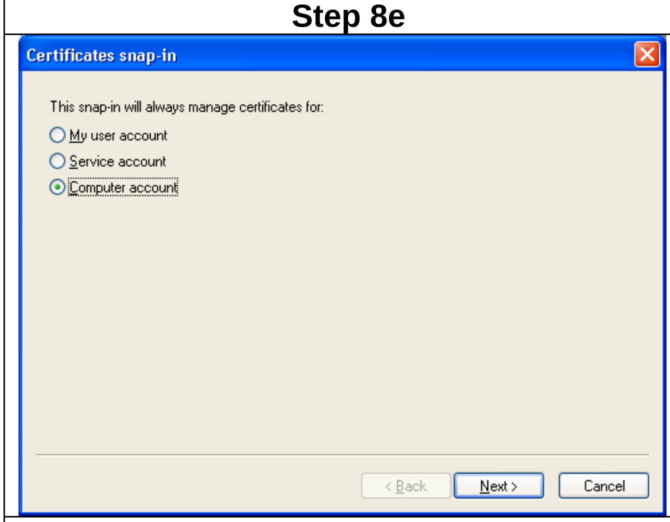
Available Standalone Snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Executi...
Disk Management	Microsoft and VERITAS...
Event Viewer	Microsoft Corporation
Folder	Microsoft Corporation
Group Policy	Microsoft Corporation

Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Select Certificates and click Add.

Step 8e



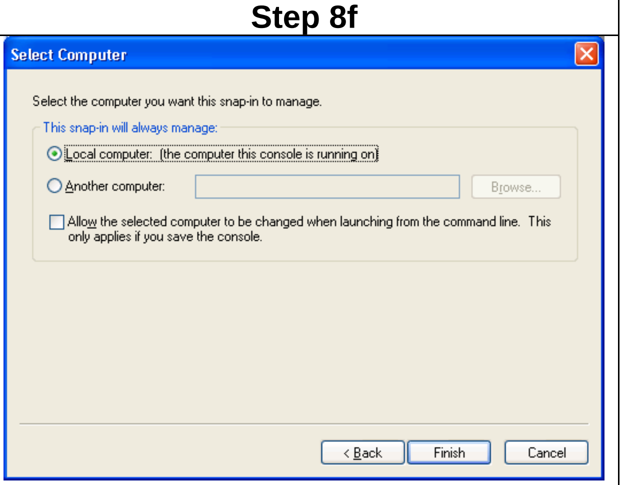
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Select Computer account and click Next.

Step 8f



Select Computer

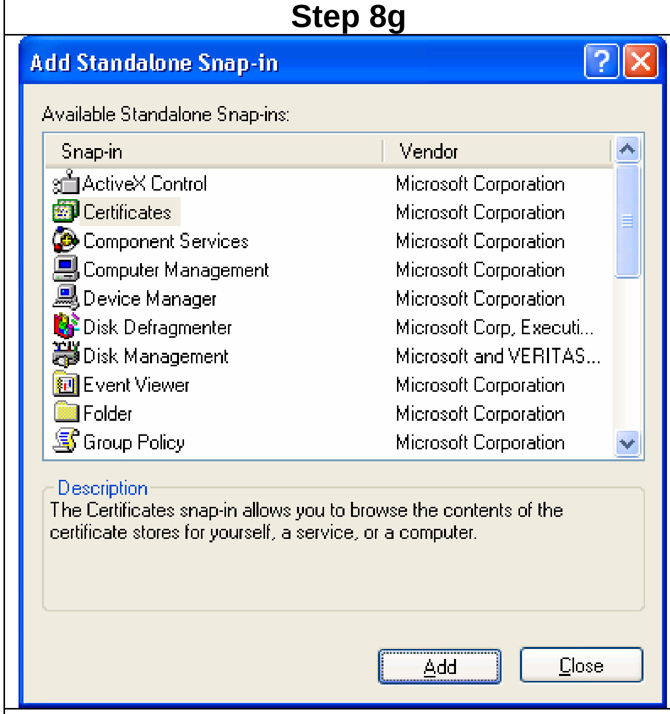
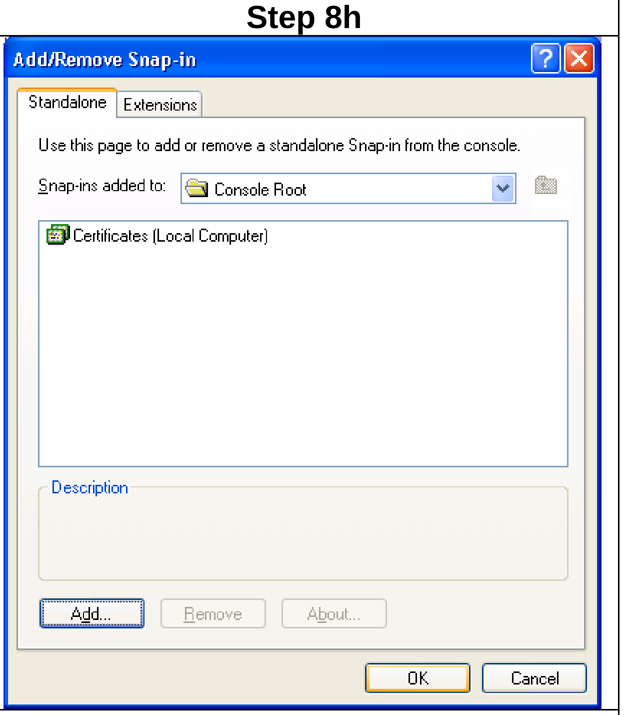
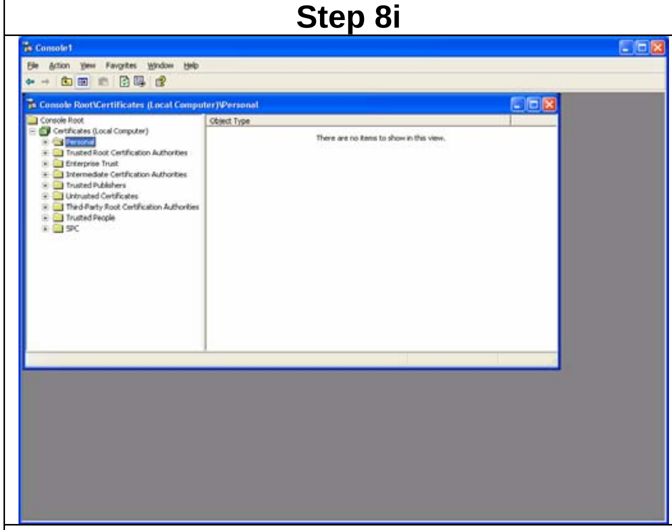
Select the computer you want this snap-in to manage.

This snap-in will always manage:

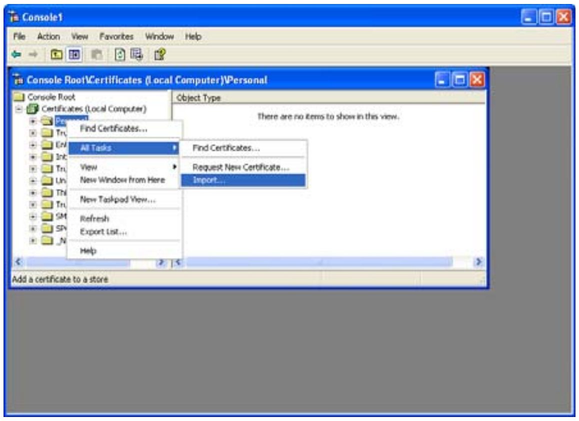
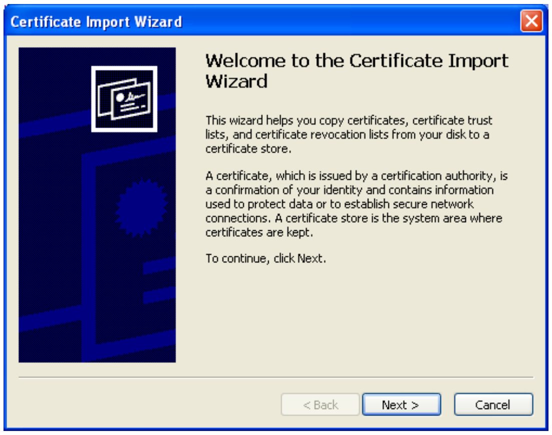
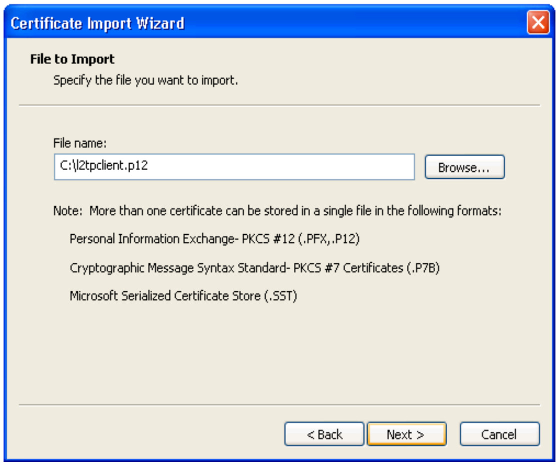
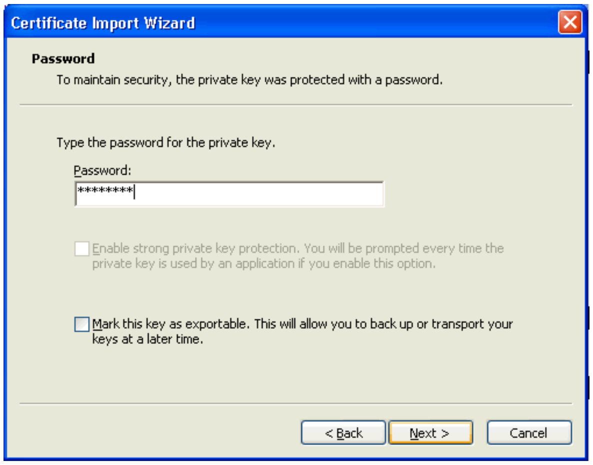
● Local computer: (the computer this console is running on)
○ Another computer:

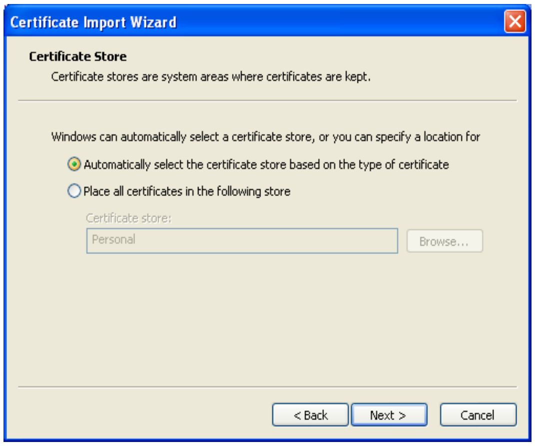
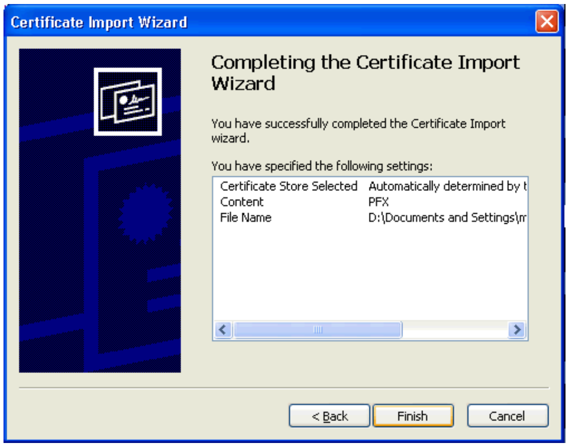
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Leave Local Computer selected and click Finish.

Step 8g	**Step 8h**
Add Standalone Snap-in Available Standalone Snap-ins: Snap-in Vendor ActiveX Control Microsoft Corporation Certificates Microsoft Corporation Component Services Microsoft Corporation Computer Management Microsoft Corporation Device Manager Microsoft Corporation Disk Defragmenter Microsoft Corp, Executi... Disk Management Microsoft and VERITAS... Event Viewer Microsoft Corporation Folder Microsoft Corporation Group Policy Microsoft Corporation Description The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer. 	Add/Remove Snap-in Use this page to add or remove a standalone Snap-in from the console. Snap-ins added to: Console Root Certificates (Local Computer) Description
Click Close.	Click OK.
Step 8i	
Console1 Console Root\Certificates (Local Computer)\Personal Console Root Certificates (Local Computer) Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted People SPC Object Type There are no items to show in this view.	
To save this console, on the File menu, click Save.	

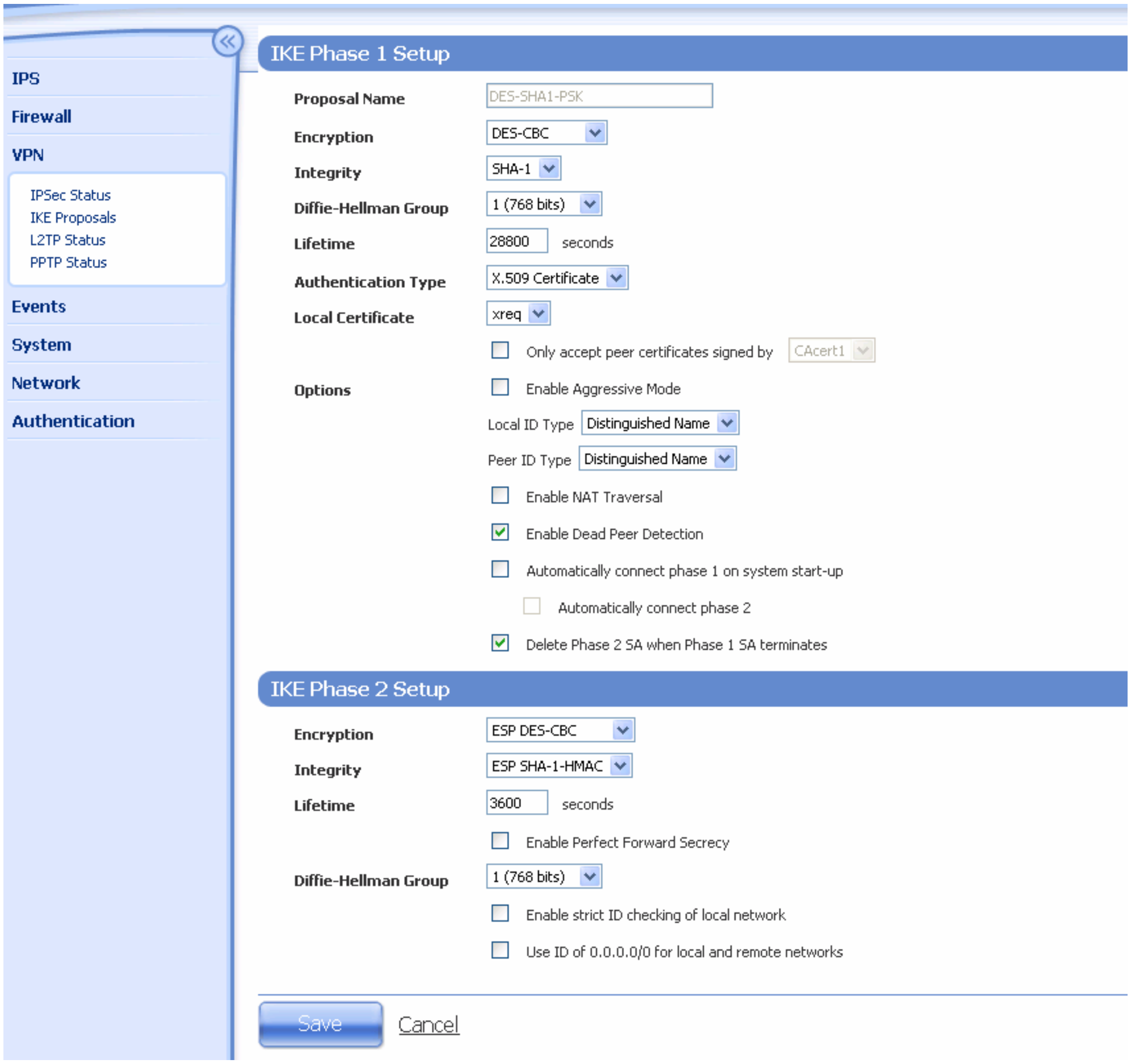
1) Use the MMC Certificates Snap-in to import the CA certificate as a Trusted Root Certificate and the local certificate as a Personal certificate.

Step 2a	**Step 2b**
 Console1 File Action View Favorites Window Help Console Root\Certificates (Local Computer)\Personal Console Root Certificates (Local Computer) Object Type There are no items to show in this view. Find Certificates... All Tasks View New Window from Here New Taskpad View... Refresh Export List... Help Find Certificates... Request New Certificate... Import... Add a certificate to a store	Certificate Import Wizard Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.
Open the Certificates folder and right click Personal, go to All Tasks then click Import	The Certificate Import Wizard starts.
Step 2c	**Step 2d**
Certificate Import Wizard **File to Import** Specify the file you want to import. File name: C:\l2tpclient.p12 Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST) 	Certificate Import Wizard **Password** To maintain security, the private key was protected with a password. Type the password for the private key. Password: ******** □ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. □ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Browse to locate the certificate file and click Next. Ensure you set the filename type mask to .p12 to see your certificate.	Enter the password used when the PKCS#12 certificate was created. Click Next.

Step 2e	Step 2f
 **Certificate Store** Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for ● Automatically select the certificate store based on the type of certificate ○ Place all certificates in the following store Certificate store: Personal 	 Completing the Certificate Import Wizard You have successfully completed the Certificate Import wizard. You have specified the following settings: Certificate Store Selected Automatically determined by t Content PFX File Name D:\Documents and Settings\m
Select where to store the certificate in the store and click Next. Select “Automatic” to place the CA in the Trusted Root Certificates Authority store, and the local certificate in the Personal store. This is necessary. Do *not* use "Place all certificates in the following store: Personal”.	Complete the Certificate Import Wizard by clicking Finish.

5.3 Configuring the X-Family VPN to use the Certificate.

1) Configure the X-Family for Pre-Shared Key as shown in Section 4.
2) Edit the IKE proposal.
    h) Navigate toVPN > IKE Proposals.
    i) Click the pencil icon next to the IKE Proposal used for the Default SA.
    j) Change the "Authentication Type" pulldown to "X.509 Certificate" and select the imported certificate name. (There will only be one certificate in the list.)



IKE Phase 1 Setup

Proposal Name: DES-SHA1-PSK
Encryption: DES-CBC
Integrity: SHA-1
Diffie-Hellman Group: 1 (768 bits)
Lifetime: 28800 seconds
Authentication Type: X.509 Certificate
Local Certificate: xreq

☐ Only accept peer certificates signed by CAcert1

Options
☐ Enable Aggressive Mode
Local ID Type: Distinguished Name
Peer ID Type: Distinguished Name
☐ Enable NAT Traversal
☑ Enable Dead Peer Detection
☐ Automatically connect phase 1 on system start-up
☐ Automatically connect phase 2
☑ Delete Phase 2 SA when Phase 1 SA terminates

IKE Phase 2 Setup

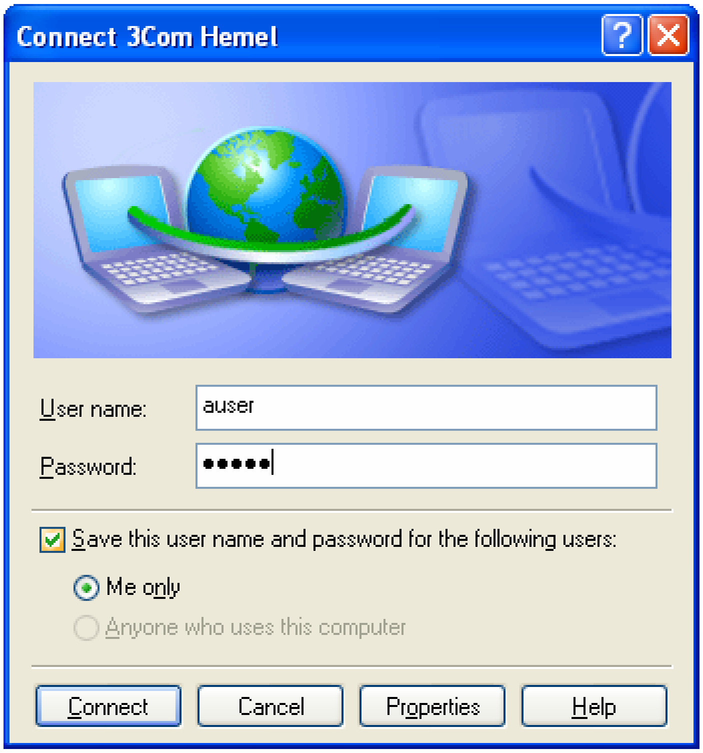
Encryption: ESP DES-CBC
Integrity: ESP SHA-1-HMAC
Lifetime: 3600 seconds
☐ Enable Perfect Forward Secrecy
Diffie-Hellman Group: 1 (768 bits)
☐ Enable strict ID checking of local network
☐ Use ID of 0.0.0.0/0 for local and remote networks

Click "Save".

The X-family device is now ready to use certificates.

5.4 Configuring the Windows XP PC to use Certificates

1) Configure the Windows XP PC L2TP/IPSec client as shown in Section 4, but do not perform step 3c. (i.e. Do not enable the checkbox “Use pre-shared key for authentication” nor enter the pre-shared key.)
2) Click OK to get back to the username/password prompt. Enter the user details configured on the X-family for the local user - this must match Step 8 where the local user name and password were configured on the X-family. ***Note: Remember both username and passwords are case sensitive***


Connect 3Com Hemel

User name: auser

Password: ●●●●●

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

Connection to X-family should now be established.

6 Troubleshooting L2TP Tunnels

The following is a list of things to check if the L2TP tunnel cannot be established or does not operate correctly:

a) On the X-family – ensure that the Strong Encryption package has been loaded (this shows on the LSM home screen as "Encryption: 256 bit" at the bottom of the Product Specification column.

b) On the X-family - ensure that the default IPSec SA is set to:
 - SA enabled
 - Enable GRE and L2TP
 - Phase 1 and 2 encryption set to 3DES (or AES 128)
 - Phase 1 and 2 authentication set to SHA1
 - Phase 1 Diffie-Hellman set to 2
 - Phase 2 PFS **not** enabled.

c) If using RADIUS, check the separate RADIUS Technical Note.

d) Check the firewall policy rules allow:

- Service IPSec from the WAN zone to this-device.
- Service L2TP from the zone configured in L2TP Server to this-device.
- From this-device to ANY for ANY service. (There is an implicit "hidden" rule for this so no explicit rule is required unless an explicit deny rule has been added to the table).

It is worth checking the Block Log on the X-family to see if the connection is being refused. This may require you to enable "Logging" on the Block rules in the firewall that you suspect may be blocking the request.

If you are using Pre-Shared Key:

a) Ensure that the X-family is using exactly the same Shared-Secret/Pre-Shared Key character string as the XP PC. Shared-Secrets/Pre-shared Keys on the X-family must be at least eight characters long.

If you are using X.509 certificates:

a) On X-family - ensure that the correct certificate name is selected on the IKE proposal.

b) On both - ensure that the certificate is signed by a trusted CA. Failure to do this will result in Windows XP refusing to use the certificate for L2TP/IPSec connections.