



Cyberoam IPSec VPN Client Configuration Guide

Version 4

Document version 1.0-410003-25/10/2007

IMPORTANT NOTICE

Elitecore has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

LIMITED WARRANTY

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and the performance thereof is under warranty provided by Kaspersky Labs. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In the event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose. In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

Copyright 2000 Elitecore Technologies Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Elitecore Technologies Ltd. Information supplies by Elitecore Technologies Ltd. Is believed to be accurate and reliable at the time of printing, but Elitecore Technologies assumes no responsibility for any errors that may appear in this documents. Elitecore Technologies reserves the right, without notice, to make changes in product design or specifications. Information is subject to change without notice

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
eLitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-26400707
Email: support@cyberoam.com
Web site: www.cyberoam.com

Visit www.cyberoam.com for the regional and latest contact information.

Typographic Conventions

Material in this manual is presented in text, screen displays, or command-line notation.

Item	Convention	Example
Server		Machine where Cyberoam Software - Server component is installed
Client		Machine where Cyberoam Software - Client component is installed
User		The end user
Username		Username uniquely identifies the user of the system
Part titles	Bold and shaded font typefaces	Report
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold & Black typefaces	Notation conventions
Navigation link	Bold typeface	Group Management → Groups → Create it means, to open the required page click on Group management then on Groups and finally click Create tab
Name of a particular parameter / field / command button text	Lowercase italic type	Enter policy name, replace policy name with the specific name of a policy Or Click Name to select where Name denotes command button text which is to be clicked
Cross references	Hyperlink in different color	refer to Customizing User database Clicking on the link will open the particular topic
Notes & points to remember	Bold typeface between the black borders	Note
Prerequisites	Bold typefaces between the black borders	Prerequisite Prerequisite details

Table of Contents

Introduction.....	6
VPN Configuration.....	7
Create VPN tunnel.....	8
Phase 1 configuration	8
Phase 2 configuration	14
Global Parameters.....	16
Manage Tunnels/Connections.....	18
Console	19
Configuration Management	20
Import VPN configuration.....	20
Export VPN configuration.....	21

Introduction

Welcome to the Cyberoam's – IPSec VPN Client Configuration Guide.

Cyberoam VPN client is IPSec VPN Client that allows to establish secure connections over the Internet usually between a remote worker and the Corporate Intranet.

It supports following Windows versions:

- Windows 98
- Windows Millennium
- Windows 2000. Win2000 all service packs
- Windows NT4
- Windows XP, WinXP all service packs, including SP2
- Windows Vista

IPSec is the most secure way to connect to the enterprise as it provide strong user authentication and tunnel encryption with ability to cope with existing network and firewall settings.

The two endpoints in Cyberoam IPSec VPN Client are referred to as:

Local - First endpoint is the local machine itself

Remote - Second endpoint is the remote peer - the machine you are trying to establish a VPN connection to, or the machine which is trying to establish a VPN connection with you.

VPN is the bridge between Local & Remote networks/subnets.

Cyberoam automatically encrypts the data and sends to the remote site over the Internet, where it is automatically decrypted and forwarded to the intended destination. By encrypting, the integrity and confidentiality of data is protected even when transmitted over the untrusted public network. Cyberoam uses IPSec standard i.e. IPSec protocol to protect traffic. In IPSec, the identity of communicating users is checked with the user authentication based on digital certificates, public keys or preshared keys.

Cyberoam can be used to establish VPN connection between sites, Road Warrior, Net-to-Net and Host-to-Host connection.

VPN Configuration

Cyberoam IPSec VPN Client connects a user to a corporate network.

The user connects to a local Internet Service Provider (ISP). Then, using the VPN client connects to the VPN Gateway to create a secure tunnel for passing IP packets to the corporate network.

The VPN client encapsulates the data in a routable IP packet and encrypts it using the IP Security (IPSec) Protocol. The corporate server authenticates the connection, decrypts and authenticates the IPSec packet, and translates the source address in the packets to an address recognized on the corporate network. This address is used for all traffic sent from the corporate network to the user for the duration of the connection.

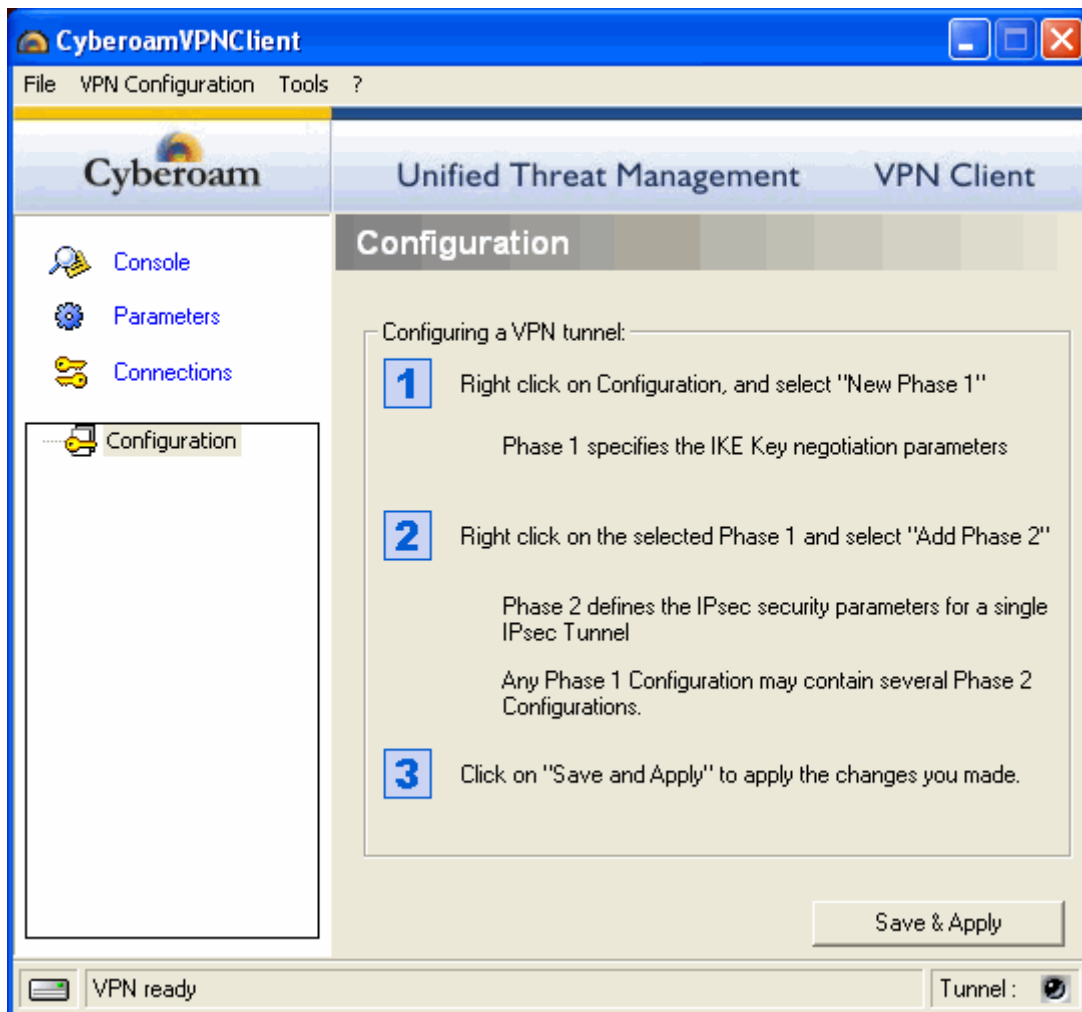
If the Client is successfully installed, you will find application icon on desktop or in system tray.

Create VPN tunnel

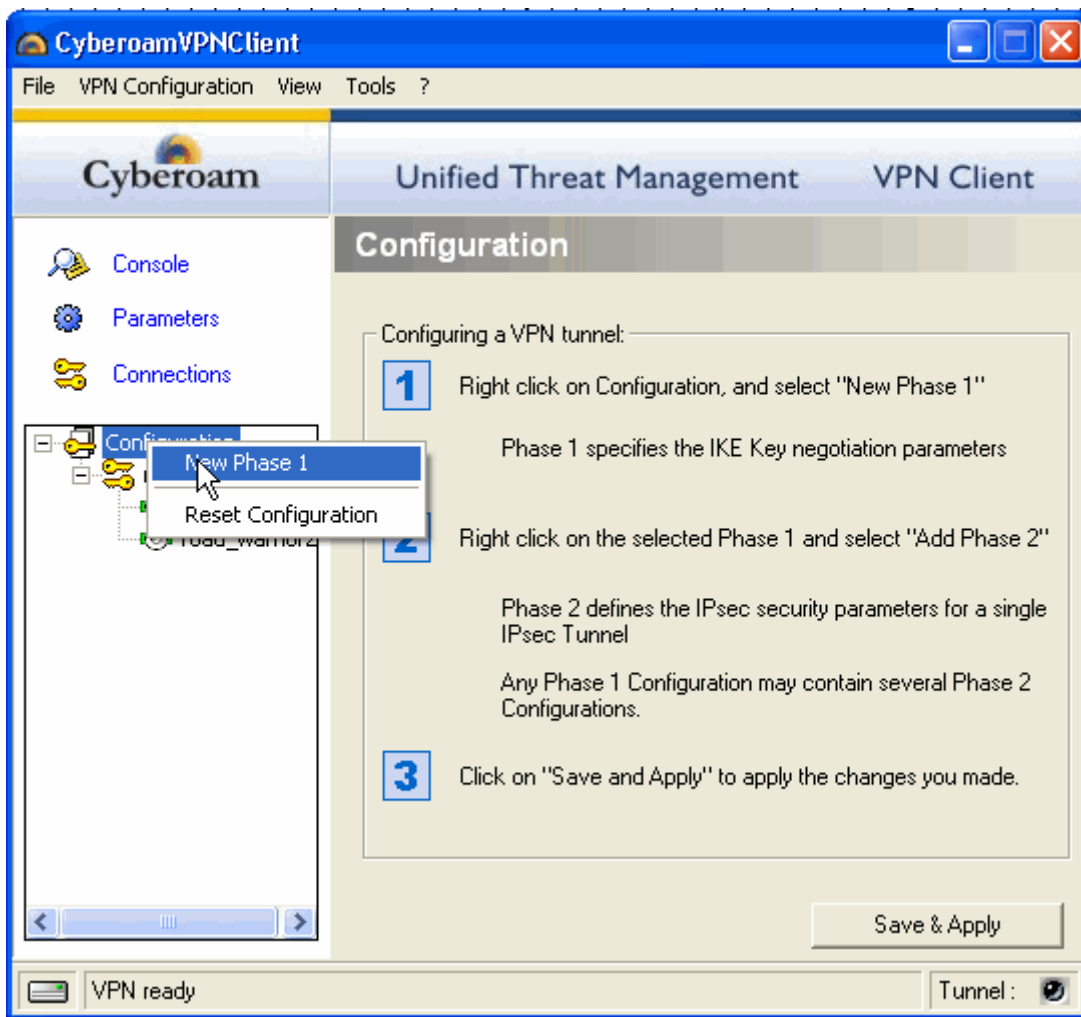
Phase 1 configuration

Double-click the icon to start the application.

The VPN Client window opens with the Configuration page. Configuration page allows creating, modifying and saving the VPN configuration along with the security elements like Preshared keys, Certificates etc. Page also displays configuration steps.



Right click Configuration and click New Phase 1 to configure for phase 1 authentication.

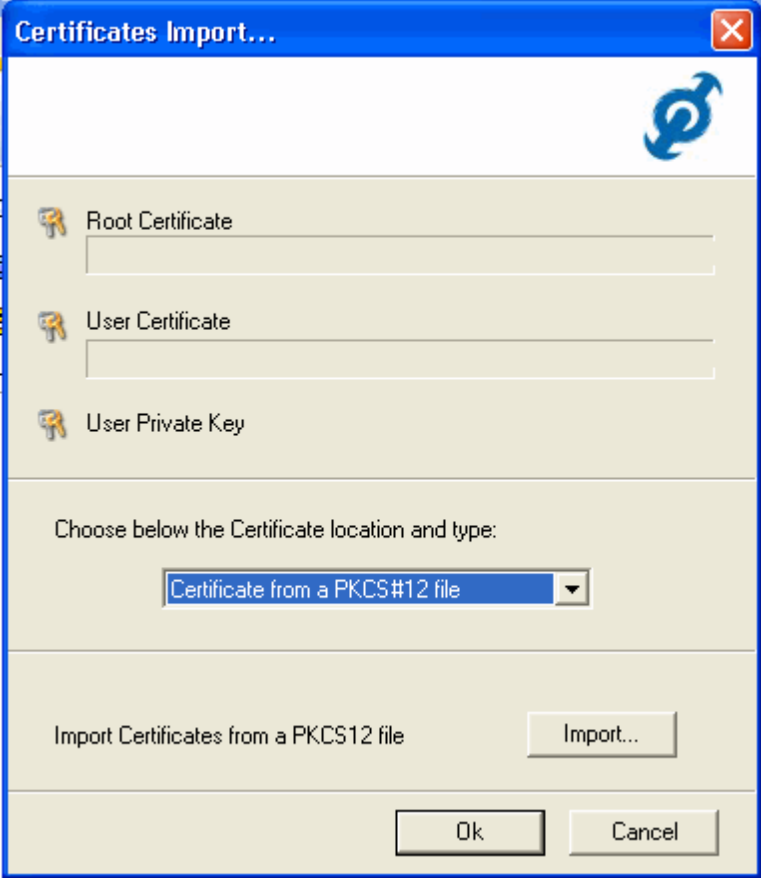


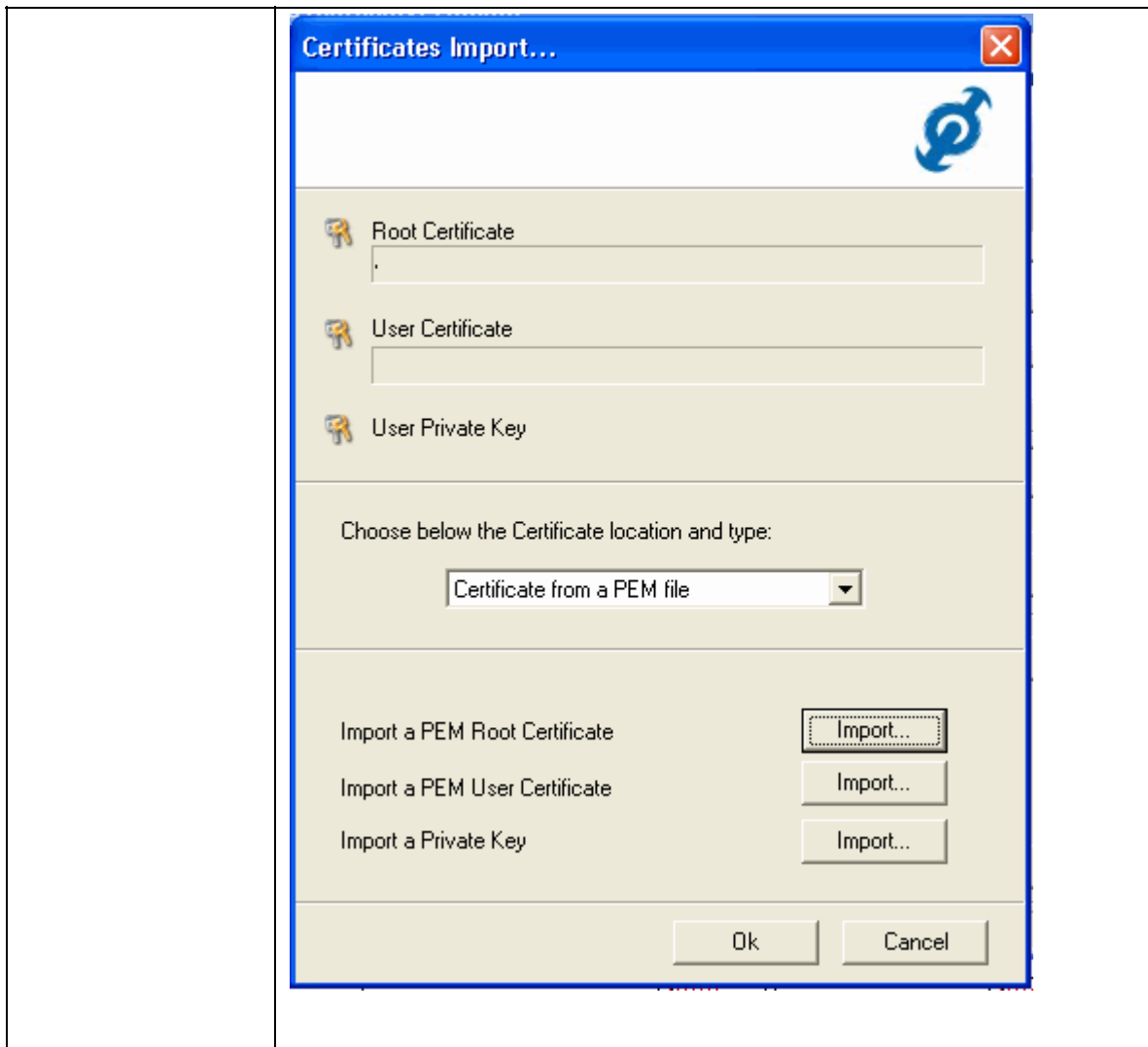
Use Phase 1 (Authentication) window to set Authentication parameters. Also called IKE Negotiation Phase.

Purpose of phase 1 is to negotiate IKE policy, authenticate peers and set up a secure channel between the peers. As part of Phase 1, each peer must identify and authenticate itself to the other.

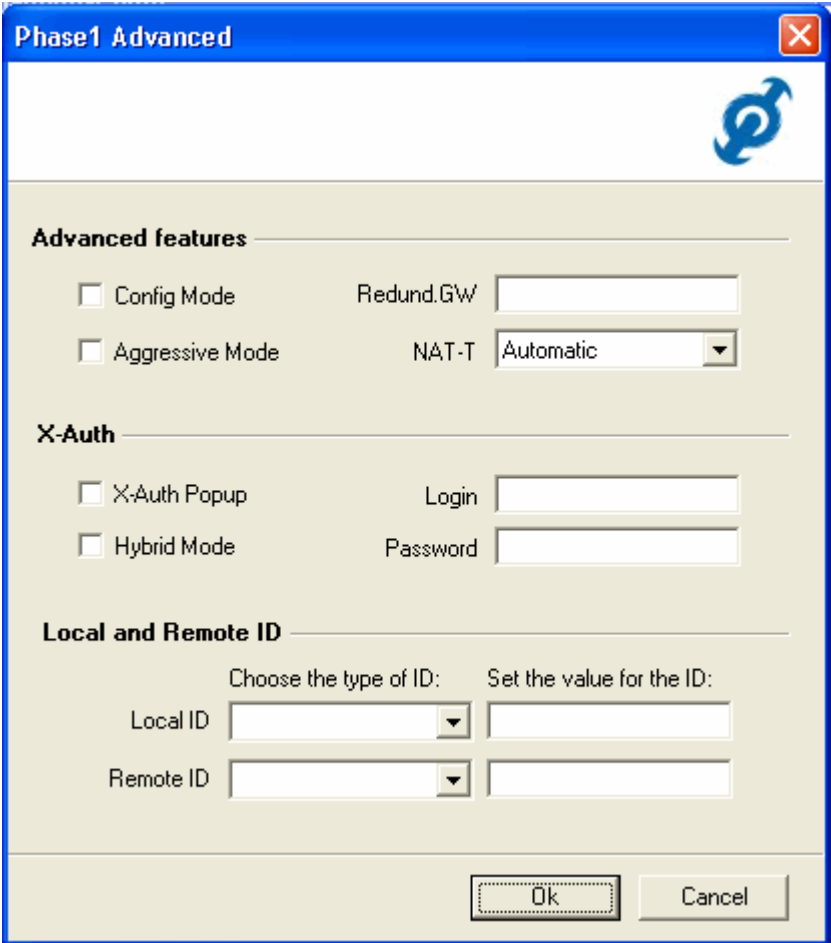


Screen Elements	Description
Name	Specify name for Phase 1. It is possible to change this name at any time. Two Phase 1 cannot have the same name.
Interface	Specify IP address of the network interface through which VPN connection is to be established. OR Specify *, if IP address changes
Remote Gateway	IP address or DNS address of the remote VPN server. If you are trying to establish connection to Cyberoam server then specify WAN IP address of Cyberoam server. IP address should be same as specified in IPsec connection for Local Server. Refer to VPN Management, Defining Connection Parameters for details.
Pre-shared key	Click Preshared key if you want to authenticate user with Preshared key Specify Preshared key as specified on the Server side. The Administrator or the remote end user who wants to establish the connection will have share the key. Preshared key is an authentication mechanism whereby a single key is

	used for encryption and decryption. Both the peers should possess the preshared key. Remote peer uses the preshared key for decryption.
Certificate	<p>Click Certificate if you want to authenticate user with Certificate.</p> <p>The remote end user who wants to establish the connection will share the certificate.</p> <p>If you have imported VPN configuration, VPN Client will automatically upload certificates.</p> <p>Choose appropriate certificate type if you want to manually upload the certificates. Supported certificate types: PKCS, PEM, Smartcard</p> <p>To import certificates, click Certificate Import</p>  <p>Select Root Certificate (.pem file), User Certificate (.pem file) and User Private key (.key file) to be imported.</p>



IKE	
Encryption	Select Encryption algorithm to be used
Authentication	Select Authentication algorithm to be used
Key group	Select Diffie-Hellman key length as specified in Policy configured at server. Group DH Group 1 = DH768 2 = DH1024 5 = DH1536 14 = DH2048 15 = DH3072 16 = DH4096
P1 Advanced button	Click to specify advanced parameters for phase 1 authentication.

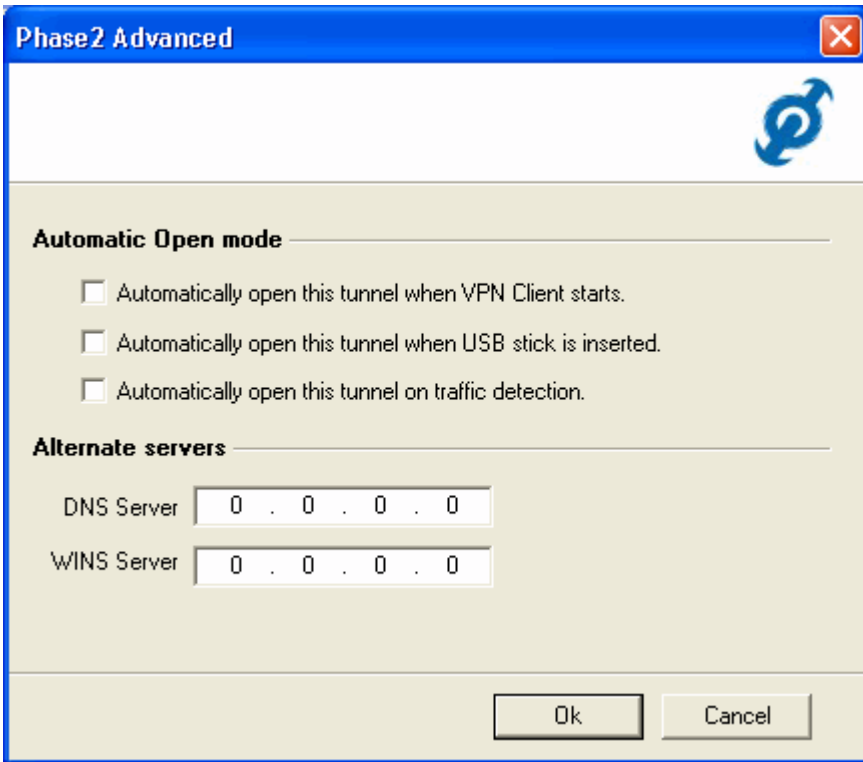
	 <p>Select Automatic for NAT-T</p> <p>X-Auth</p> <p>Enable X-Auth Popup if at the remote end User Authentication is “Enable as server”. This will popup user name and password window when you try to connect.</p> <p>Or</p> <p>Specify Login name and password</p> <p>Do not enable X-Auth Popup or specify Login and Password, if user authentication is “Disabled” at the remote end.</p> <p>Local and Remote ID</p> <p>Local ID – Client ID Remote ID – As specified at the remote end</p> <p>Click OK</p>
Apply Rules button	Click to apply and save the rule

Phase 2 configuration

The purpose of Phase 2 is to negotiate the IPsec security parameters that are applied to the traffic passing through tunnels negotiated during phase 1.



Screen Elements	Description
Name	Specify name for Phase 2. It is possible to change this name at any time. Two Phase 2 cannot have the same name.
VPN Client Address	Specify IP address of the Client side computer. Specified IP address should not belong to the remote LAN. Specify 0.0.0.0, if in Phase 1, Interface is specified as 'Any'
Address type	Specify IP address of the remote peer. Remote peer may be a LAN or a single computer. If it is LAN, click Subnet Mask and specify subnet mask for remote LAN. If at the remote end, Cyberoam is used then specify same address as specified in the connection parameters as Local LAN Address. Refer to VPN Management, Defining Connection Parameters for details.
ESP	

Encryption	Select Encryption algorithm to be used
Authentication	Select Authentication algorithm to be used
Mode	Specify Tunnel
PFS	<p>Click to enable PFS and select DH1024 as Group</p> <p>If at the remote end, PFS group is 'Same as Phase-1' then select same Group as selected in Key Group</p> <p>If PFS is enabled new key will be generated for every negotiation on key expiry. PFS is enabled/disabled from Cyberoam server end from VPN policy defined for connection.</p>
Apply Rules button	Click to save and apply rules
P2 Advanced	 <p>Check "Automatically open this tunnel when VPN client starts" to open tunnel as soon as client starts</p> <p>Check "Automatically open this tunnel when USB stick is inserted" to open tunnel as soon as USB stick is inserted in which certificates etc are stored.</p> <p>Check "Automatically open this tunnel on traffic detection" to open tunnel as soon as traffic to related site found.</p>
Open Tunnel button	<p>Click to open tunnel. Button changes to "Close Tunnel" once tunnel is open.</p> <p>Once the connection is established, the client icon color changes to Red.</p>
Open During Boot	Enable to establish connection automatically on startup of client

Global Parameters

Global Parameters are generic settings that apply to all the created VPN tunnels. You can set global parameters from Parameter tab. Cyberoam uses the default values.



Screen Elements	Description
Lifetime (sec.)	Authentication (IKE) - key life for Phase-I Encryption (IPSec) - key life for Phase-II
Dead Peer Detection (DPD)	Check interval (sec.) - Client will check for server availability e.g. if it is set to 30 sec then Client will check for server availability after every 30 seconds Max number if retries – Client will check for sever availability for specified number of times Delay between retries (sec.) – Client will wait for specified seconds before trying again
Miscellaneous	Retransmissions – Client will send message for the specified number of times Delay between retries – Minimum time before any attempts by user to restart IKE negotiation
Block non-	Check to block any unencrypted connection i.e. only encrypted traffic is

ciphered connection	authorized
------------------------	------------

Manage Tunnels/Connections

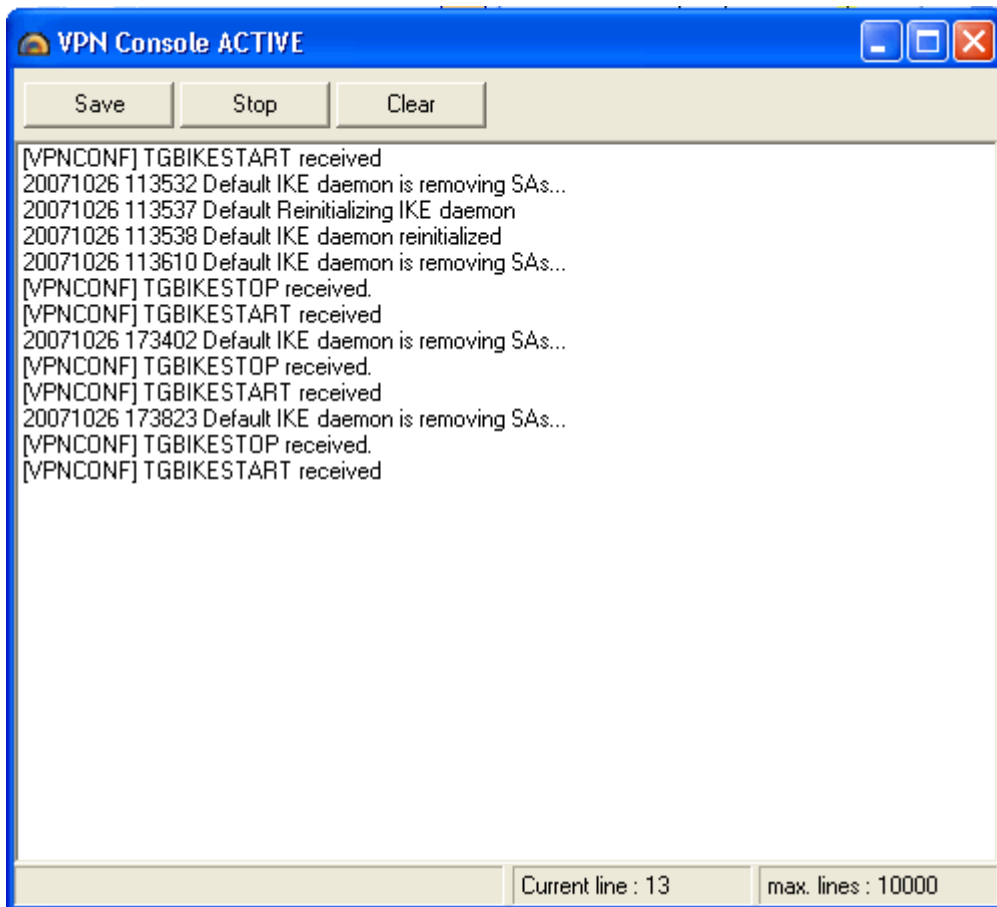
Use Connection tab to view the currently open tunnels/connections and close the tunnel. To stop the connection, click the tunnel and click Delete.

Tunnels can also be opened, viewed or closed using VPN client icon in system tray. If more than one tunnel is open when you stop connection using 'Stop and Quit' option from the client icon, all the open tunnels will be closed. If you want to stop a particular tunnel, use Connection tab.



Console

Use console tab to analyze the connection process. It also provides logs for the refused connection. You can even save the log for future use.



Configuration Management

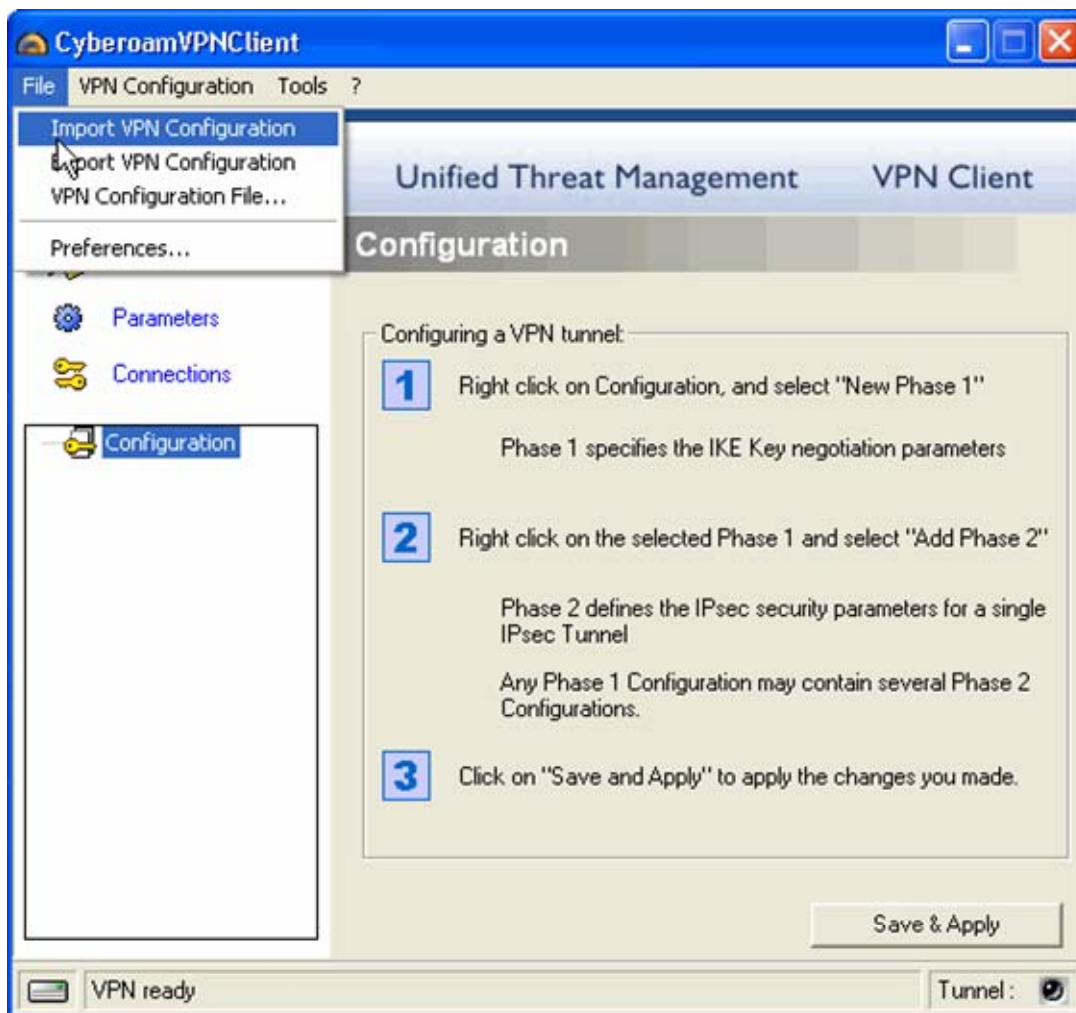
VPN Client can import or export a VPN configuration. With this feature, configuration can be delivered at the remote end or can be saved for the future use.

All the configuration files will have .tgb extension.

Import VPN configuration

Go to File>Import VPN Configuration and upload the .tgb file.

There is no need to upload certificates separately as VPN configuration file created by Cyberoam server includes certificates also.

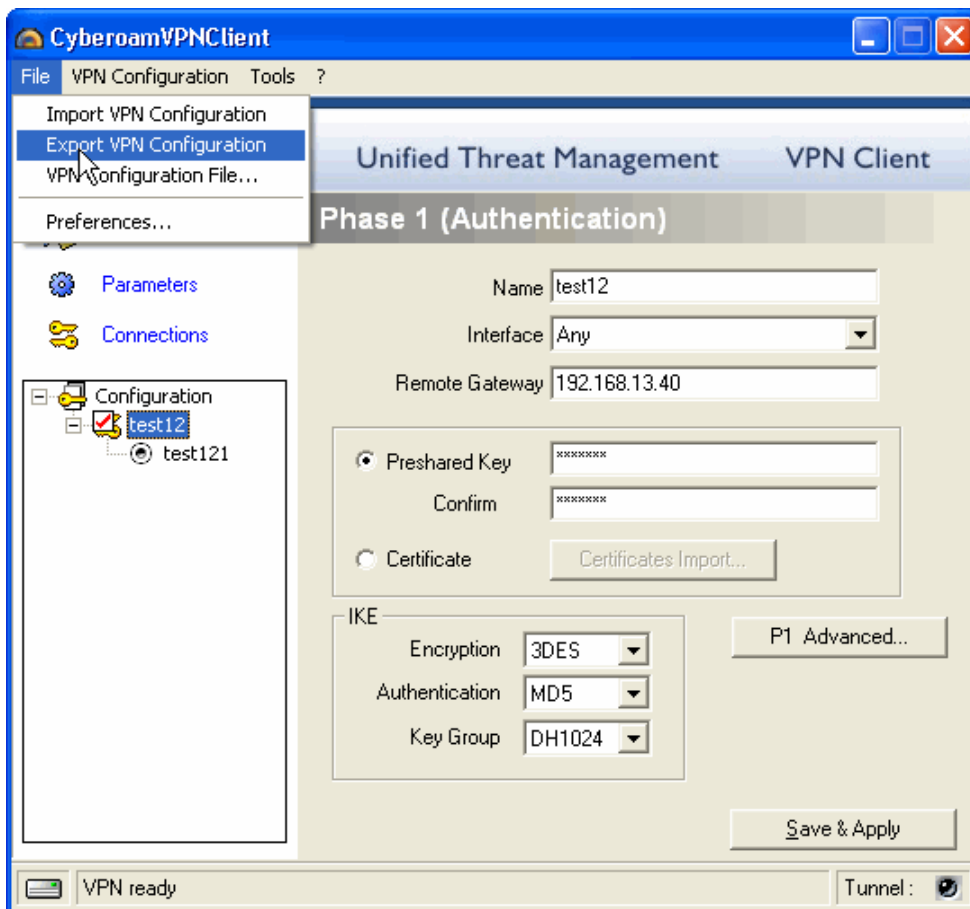


Note

All the existing configurations will be lost. You can save configurations by exporting VPN configurations.

Export VPN configuration

Go to File>Export VPN Configuration



VPN configurations created in VPN Client can be exported as a password protected file also.

When the user wants to export a configuration, a window automatically asks if the VPN configuration file to be exported must be protected with a password or not.

