

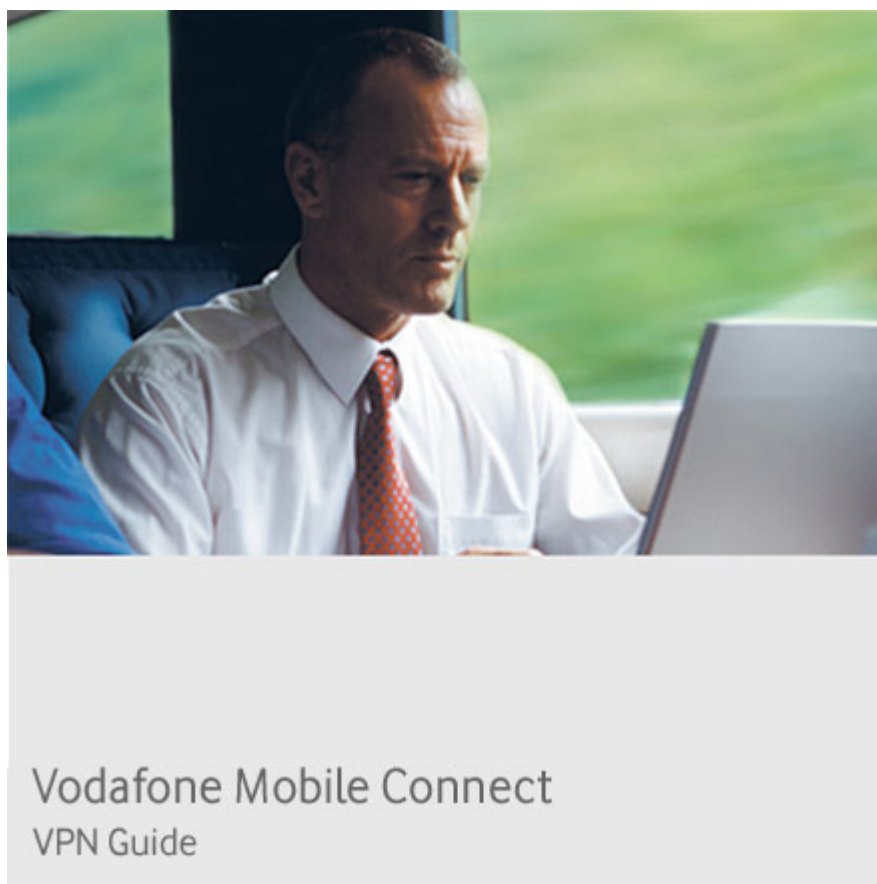
# **VPN End to End – Cisco 3005 – Appendix**

Appendix A: Cisco 3005 VPN Concentrator

Technical Notes for use with Vodafone Mobile Connect services

Date: **3 May 2007**

Revision No: **3.0**



## Scope

This document presents results of installation, configuration, and operations testing of VPN components with the Vodafone Mobile Connect service. The document is not intended to be a tutorial on VPN concepts nor does it supersede or replace the vendor's documentation. The reader is referred to the VPN vendor for definitive guidance on the proper and recommended use of their product. While Vodafone Group has taken care to ensure that the information contained herein is accurate, no responsibility can be accepted for errors, omissions, or inaccuracies.

## Document History

Version	Date	Reason
1.0	October 2003	Initial release using GPRS network. Client documentation included in main document.
2.0	May 2006	Creation of separate document for client configuration. Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Minor edits & upgrades

## File Reference

VPN\_Cisco\_3005\_Appendix\_A\_Concentrator

## Document Authors

Joerg Pfeffer , TECON Terenci

Peter Jaeger, TECON Terenci

Miroslaw Grzesica, TECON Terenci

## Document Distribution

Public via websites of Vodafone, its Affiliates, and its Partner Networks

### © Vodafone Group 2007.

Other than as permitted by law, no part of this document may be reproduced, adapted, or distributed, in any form or by any means, without the prior written consent of Vodafone Group Plc.

# Contents

---

1	Executive summary .....	4
2	VPN Concentrator Installation and Configuration (4.1) .....	5
2.1	Initial setup.....	5
2.2	Using the web-based Concentrator manager.....	5
2.3	Advanced settings.....	10
2.4	IKE keep alive .....	11
2.5	Data compression .....	13
3	Update procedure .....	14
4	Configuration of Split Tunnelling .....	17
5	User Management and Profile Handling .....	19
6	Logging .....	21
7	Name Resolution .....	24

## Tables & Figures

---

Nil

# 1 Executive summary

---

This Appendix is in addition to the detailed document for Cisco 3005 VPN Concentrator and describes the setup and update process in a detailed way with example screen shots taken from the initial processes.

Logging and additional functionality is described in the appropriate chapters.

## 2 VPN Concentrator Installation and Configuration (4.1)

---

The following description is intended for network administrators who are familiar with networking and IP concepts. The Concentrator has to be integrated into the internal company network. The Concentrator setup therefore has to comply with the configuration of the internal networking. This description is intended to allow a network administrator not yet familiar with the Cisco Concentrator to configure a VPN with UMTS/GPRS usage.

### 2.1 Initial setup

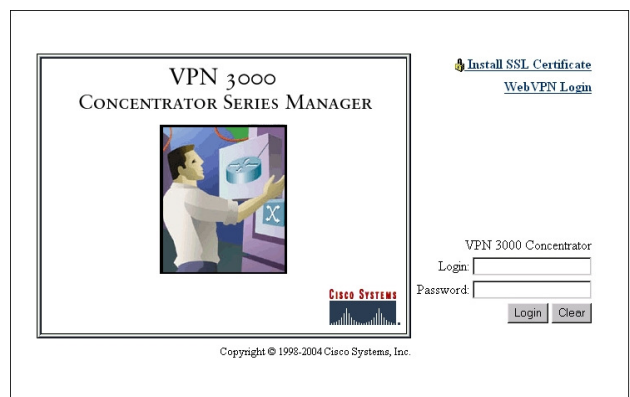
After unpacking the Concentrator install the device in your office environment with connecting power, internal and external network connections – and the console cable to your PC.

Note: You can either place the Concentrator besides or behind your Firewall. We recommend placing it behind the Firewall and opening the appropriate ports for VPN connection to the Concentrator. See the chapter “Which protocols are supported” above for port description.

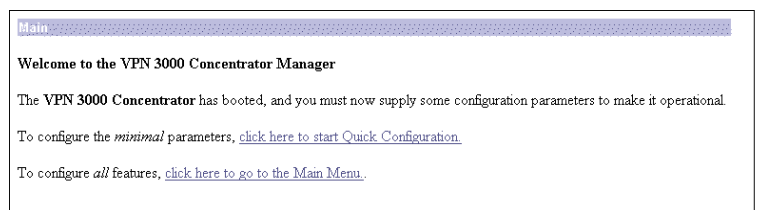
Now configure the VPN Concentrator Ethernet 1 interface to your private network from the console over serial cable and a terminal emulation program, e.g. Hyperterm (9600 Baud, 8Bit data, No parity, 1 stopbit)

### 2.2 Using the web-based Concentrator manager

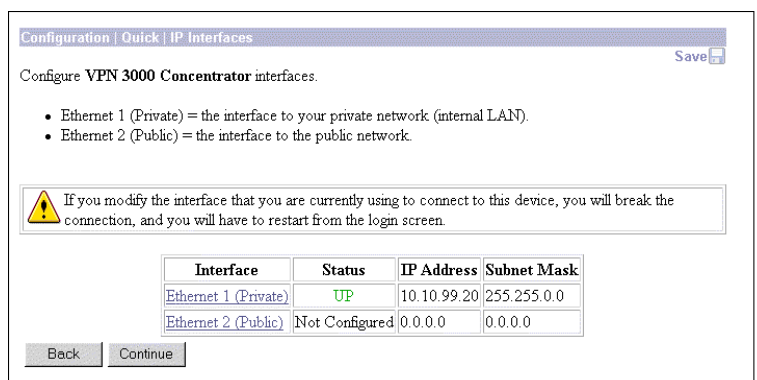
- Use a web browser to contact the VPN Concentrator's internal address. The VPN Concentrator Manager requires one of the following browsers:
- Microsoft Internet Explorer version 6.0 SP1 or higher (Windows) (SP2 required for Windows XP)
- Netscape Navigator version 7.2 or higher (Windows, Linux, or Solaris)
- Mozilla 1.73 or higher (Windows, Linux, or Solaris)
- Firefox 1.0 or 1.5 (Windows, Macintosh, or Linux)
- For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.
- Make sure you have Java script/Active scripting enabled in your browser.
- Note: The web page is only accessible from the internal interface, so you must either be connected to the internal network or logged in via a VPN-Client and a valid VPN user.



- The following screen appears only the first time you are logging in and offers the Quick Configuration option. If you do not see this screen please navigate through the configuration menus by clicking the Explorer-style tree on the left-hand side. The relevant branch for the basic setup is "Configuration".




- We continue with Quick Configuration dialog. The next screen lets you configure the VPN Concentrator Ethernet interfaces. The Model 3005 comes with two Ethernet interfaces. Models 3015-3080 come with three Ethernet interfaces.



- Configure the external/public IP address. Any changes to your internal/private address terminates the admin session. To configure click on Ethernet 2 and the following screen appears. To make this interface a public interface that is facing to the internet, check the Public Interface check box. Make other appropriate changes like speed, duplex etc and finally apply everything.

Configuration | Quick | IP Interfaces | Ethernet 1

 You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

**Configuring Ethernet Interface 1 (Private).**

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP (System Name may be required for DHCP).
	System Name	<input type="text"/>	
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	<input type="text" value="10.10.99.50"/>	
	Subnet Mask	<input type="text" value="255.255.0.0"/>	
	Public Interface	<input type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	<input type="text" value="00.90.A4.00.25.A8"/>	The MAC address for this interface.
	Filter	<input type="text" value="None"/>	Select the filter for this interface.
	Speed	<input type="text" value="10/100 auto"/>	Select the speed for this interface.
	Duplex	<input type="text" value="Auto"/>	Select the duplex mode for this interface.
	MTU	<input type="text" value="1500"/>	Enter the Maximum Transmit Unit for this interface (68 - 1500).

Apply Cancel

78631

- To configure basic information that identifies your VPN Concentrator on the network you will see the following "System Info" screen. Enter a system name, the current time, DNS Server Address, Domain name and the default gateway – your next hop to the internet. (DST = Daylight-Saving Time)

Configuration | Quick | System Info

Assign a system name/hostname to this device. This may be required if you use DHCP to obtain an address.

System Name  Enter a hostname for the system; e.g. vpn01.

Set the time on your device. The correct time is very important, so that logging and accounting entries are accurate.

The current time on this device is Tuesday, 20 February 2001 13:51:55.

New Time  :  :  February  /  (GMT-05:00) EST

☒ Enable DST Support

Specify a DNS server, which lets you enter hostnames rather than IP addresses in subsequent Manager fields.

DNS Server  Enter the IP address of your local DNS server.

Domain  Enter your Internet domain name; e.g. yourcompany.com.

Default Gateway  Enter your default gateway. Leave at 0.0.0.0 for no default gateway.

Back Continue

63736

- After "continue" you are able to configure the tunnelling protocols and encryption options. In our example we are using IPSec connections only, Client-to-LAN. Press "continue" configuring address assignment

Configuration | Quick | Tunneling

Select the tunneling protocols and encryption options that you want to enable.

<input checked="" type="checkbox"/>	PPTP	<input type="radio"/> Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.) <input checked="" type="radio"/> Don't Require Encryption (Clients may optionally use encryption.)
<input checked="" type="checkbox"/>	L2TP	<input type="radio"/> Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.) <input checked="" type="radio"/> Don't Require Encryption (Clients may optionally use encryption.)
<input checked="" type="checkbox"/>	IPSec	Check to enable remote user connections via IPSec. LAN-to-LAN configurations are done outside of Quick Configuration.
<input checked="" type="checkbox"/>	WebVPN	Check to enable remote user connections via SSL using a web browser.

Back Continue

- Check Configured Pool to enable this method, which lead the VPN Concentrator to assign IP addresses from an internally configured pool. Enter the starting and ending IP addresses available in the initial pool, in the Range Start and Range End fields. Enter these addresses in dotted decimal notation; for example, 172.16.100.100 – 172.16.100.200. Click Continue to proceed.

Configuration | Quick | Address Assignment

Select at least one method of assigning IP addresses to clients as a tunnel is established. The methods are tried in the order listed.

- ☐ Client Specified This method lets the client specify its own IP address.
- ☐ Per User This method assigns IP addresses on a per-user basis. If you use an authentication server (which you configure next) that has IP addresses configured, we recommend selecting this method.
- ☐ DHCP Specify Server
- ☒ Configured Pool
 

Range Start 
 Range End 
 This method uses this device to assign IP addresses.

Back Continue

- On the following screen you can choose how to authenticate users. You can select the VPN Concentrator internal server or one of three external server types. We use the default “internal server” that does support up to 100 groups and users (combined). The following selection is possible:
- Internal Server — the internal VPN Concentrator authentication server. (This is the default selection.)
- RADIUS — an external Remote Authentication Dial-In User Service server.
- NT Domain — an external Windows NT Domain server.
- SDI — an external RSA Security Inc. SecurID server.
- Kerberos/Active Directory—An external Windows/Active Directory server or a UNIX/Linux Kerberos server



**Configuration | Quick | Authentication**

Specify how to authenticate users under PPTP, L2TP or IPSec. You can use the internal server or an external authentication server. If you select the *Internal Server*, you must configure the internal user database. You may configure additional servers using System Configuration.

**Server Type**  Selecting *Internal Server* will let you add users to the internal user database.

63729

- On the next screen you have to configure at least one user. Unless you choose an address pool like before you can assign IP addresses to a specific user. In our example we leave the address field blank.

**Configuration | Quick | User Database**

Configure users in the internal authentication server database. Since you chose per-user address assignment, include the user IP address and subnet mask.

Passwords must be at least 8 characters long.

Current Users	Actions	User to Add
<div>— Empty —</div>	<input type="button" value=" &lt;&lt; Add"/> <input type="button" value=" Remove &gt;&gt;"/>	<b>User Name</b> <input type="text"/> <b>Password</b> <input type="text"/> <b>Verify</b> <input type="text"/> <b>IP Address</b> <input type="text"/> <b>Subnet Mask</b> <input type="text"/>

63739

- Later on you can change user parameters on the regular Configuration | User Management | Users screens, but on this quick configuration screen, you can only add and remove users.
- Further you need to configure an IPSec group with a name and a password. We recommend not sharing this password within your organisation for security reasons. Please note: Entries are case-sensitive. Finally you get to the Changing Admin Password-screen. We recommend changing the admin password now

**Configuration | Quick | IPSec Group**

Select a Group Name and Password to be used by remote IPSec users. The Group Password must be at least 4 characters long.

**Group Name**

**Password**

**Verify**

63736

Configuration | Quick | Admin Password

We strongly recommend that you change the password for user *admin*.

Password

Verify

63726

- After done you need to save all changes into the NVRAM of the Concentrator by clicking the “Save Needed” icon. Now you’ve finished the base configuration. For using with Mobile Connect Cards over the Vodafone UMTS/GPRS infrastructure you need to do some advanced settings.

## 2.3 Advanced settings

- Since we are doing IPSec over an address translation we need to enable IPSec over UDP. You enter this in the main configuration under base group or the appropriate group of your users. Please check “IPSec over UDP” and enter a port number within the given range, for example 10000. We recommend further having the split tunnelling Policy with “Tunnel everything”. Otherwise you open serious backdoors over your remote Clients into your private LAN.

VPN 3000  
Concentrator Series Manager

Main | Help | Support | Logout  
Logged in: admin  
Configuration | Administration | Monitoring

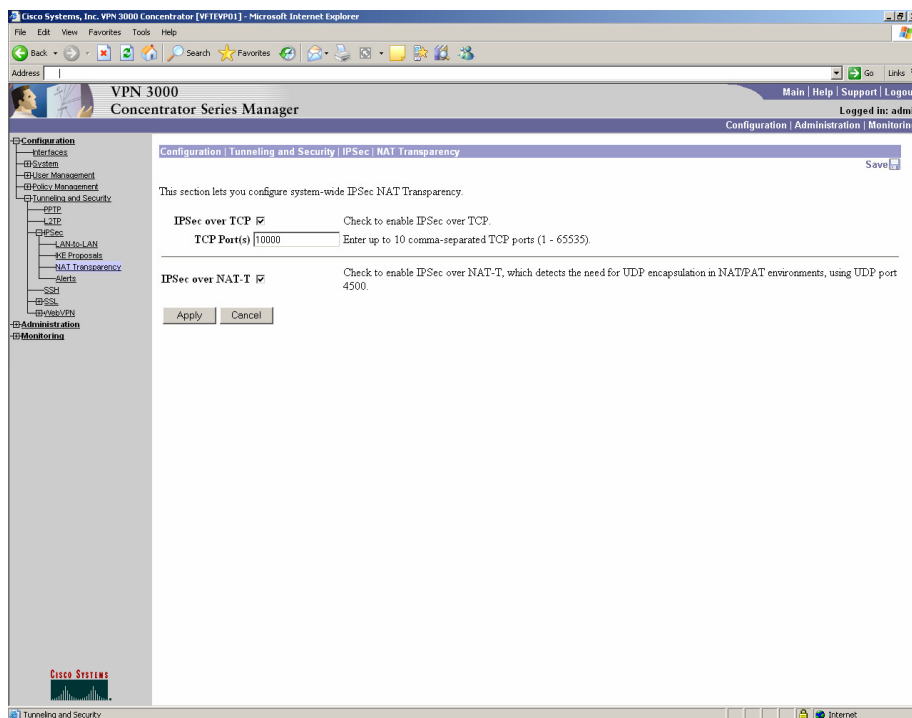
Configuration

- System
  - Server
  - Address Management
  - Tunnelling Protocols
    - IPsec
    - SSL
    - SSH
    - SSL
    - SSL
  - Management Protocols
    - FTP
    - HTTP/HTTPS
    - TFTP
    - Telnet
    - SNMP
    - SNMP Communities
    - SSH
    - SSL
    - SSL
- General
  - Identification
  - Time and Date
  - Sessions
  - Authentication
  - Client Update
  - Enable
  - SSL
  - SSL
- User Management
  - Base Group
  - Users
  - Groups
- Policy Management
- Administration
- Monitoring

General | IPsec | Mode Config | Client FW | HW Client | PPTP/L2TP

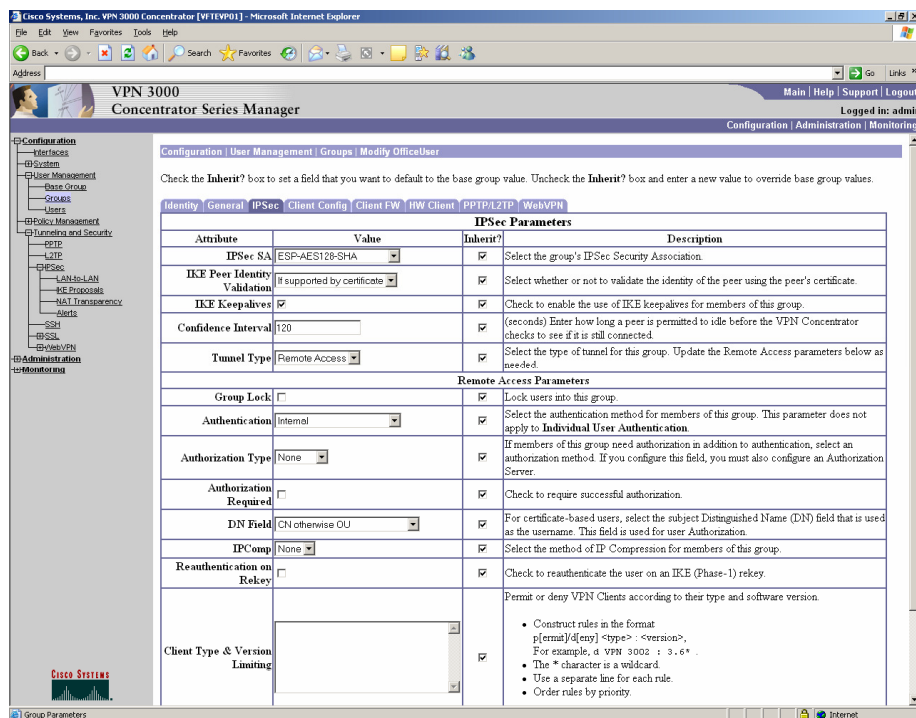
Attribute	Value	Description
Banner		Enter the banner for this group. Only software clients see the banner.
Allow Password Storage on Client	<input type="checkbox"/>	Check to allow the IPsec client to store the password locally.
Split Tunneling Policy	<input checked="" type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel. <input type="radio"/> Only tunnel networks in list	Select the method and network list to be used for Split Tunneling. <b>Tunnel Everything:</b> Send all traffic through the tunnel. <b>Allow the Networks in the list to bypass the tunnel:</b> The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting does not apply to the VPN 3002 Hardware Client. <b>Tunnel Networks in List:</b> Send traffic to addresses in this list through the VPN tunnel. Send all other traffic unencrypted.
Split Tunneling Network List	None	
Default Domain Name		Enter the default domain name given to users of this group.
IPsec over UDP	<input checked="" type="checkbox"/>	Check to allow the IPsec client to operate through a firewall using NAT via UDP.
IPsec over UDP Port	10000	Enter the UDP port to be used for IPsec through NAT (4001 - 49151).

- As an alternative you can use the IETF draft NAT-T implementation. To enable this option go to the menu Configuration | Tunnelling and Security | IPsec | NAT Transparency screen and enable **IPsec over NAT-T**.

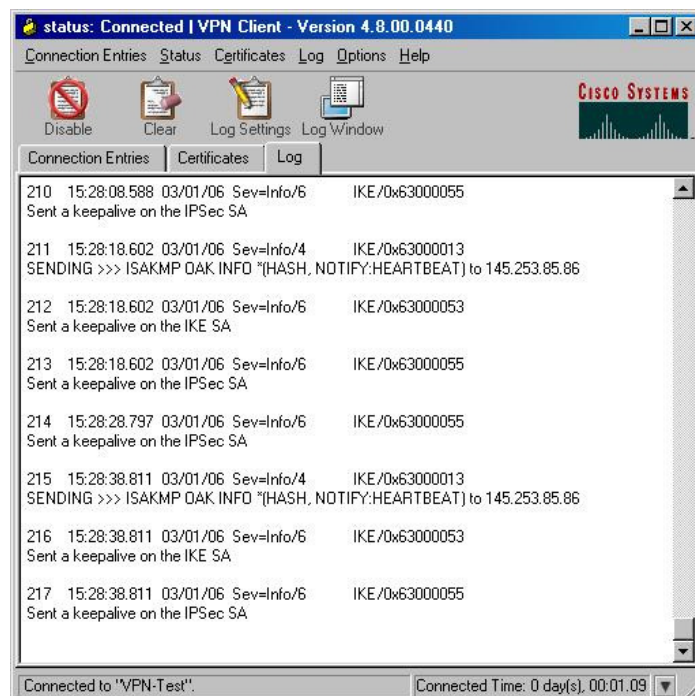


## 2.4 IKE keep alive

Keep alive messages are supported by default and configurable in the IPsec section of a group profile. These messages are sent from Client to gateway, but when the Client is idle, it does not send a keep alive until it sends data and gets no response.



On the Client side you can see the “keep alive” messages on the local log window



## 2.5 Data compression

Data compression using LZS compression algorithm is available and can be enabled in the group profile. Enabling data compression might speed up the data transmission rate of VPN users.

Configuration / User Management / Groups / Modify OfficeUser

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Attribute	Value	Inherit?	Description
IPSec SA	ESP-AES128-SHA	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	120	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
<b>Remote Access Parameters</b>			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input checked="" type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to <b>Individual User Authentication</b> .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	LZS	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Client Type & Version Limiting		<input checked="" type="checkbox"/>	Permit or deny VPN Clients according to their type and software version. <ul style="list-style-type: none"> <li>Construct rules in the format <code>[permit/deny] &lt;type&gt; : &lt;version&gt;</code>. For example, <code>d VPN 3002 : 3.6*</code>.</li> <li>The * character is a wildcard.</li> <li>Use a separate line for each rule.</li> <li>Order rules by priority.</li> </ul>

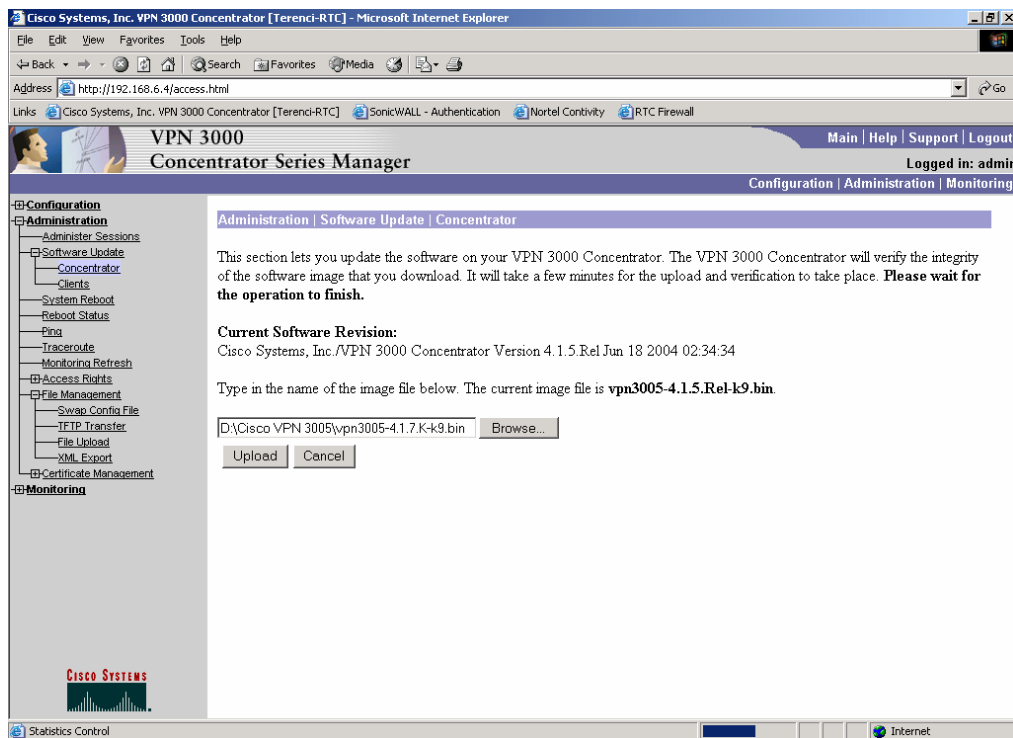
Note that software compression was shown to have little benefit for most environments. The benefit of compression should be reviewed in light of the cost of processor load for both the client and server.

### 3 Update procedure

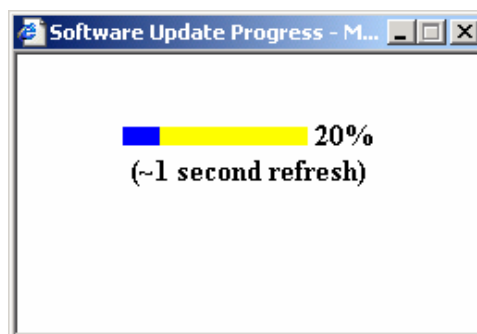
This process uploads the executable system software to the VPN Concentrator, which then verifies the integrity of the software image.

The new image file must be suitable for your specific model of concentrator and accessible by the workstation you are using to manage the VPN Concentrator.

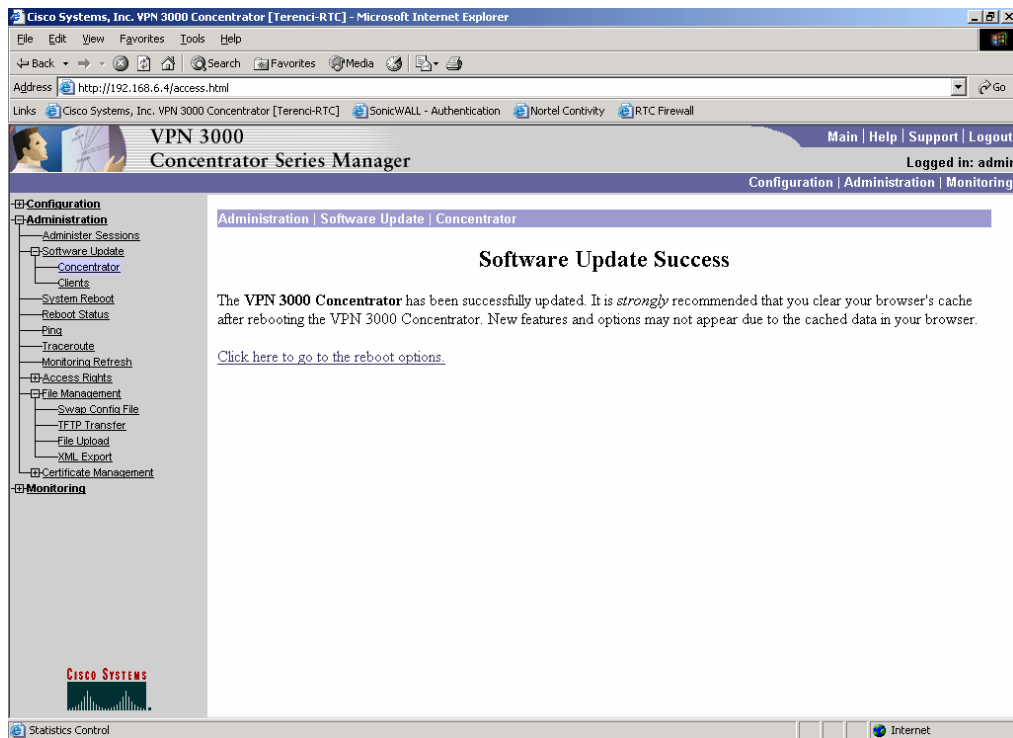
Go to the menu Administration | Software update | Concentrator and browse for the file path. Afterwards click on the “Upload” button.



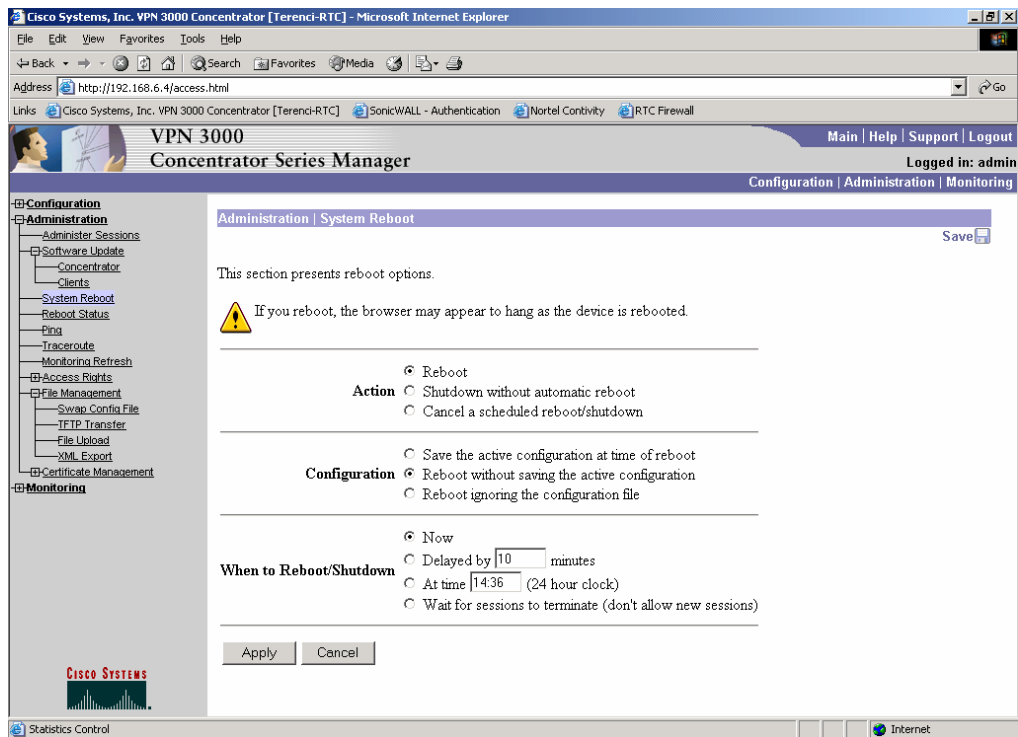
It takes a few minutes to upload and verify the software, and the system displays the progress. It refreshes the number of bytes transferred at 10-second intervals. Please wait for the operation to finish.



To run the new software image, you must reboot the VPN Concentrator. The system prompts you to reboot when the update is finished. Click on the link below the message to open the reboot options page.



Make sure the action “Reboot” is selected on the “System Reboot” page and click on the “Apply” button. After the reboot the new software version is available and can be checked under the menu Monitoring | System status.





## 4 Configuration of Split Tunneling

Split Tunneling is supported and will be negotiated within connection phase by server push and is enabled by default. The user cannot override server settings.

Enabling or disabling split tunneling can be configured in the Group properties. All users assigned to this group will use this setting and it is not possible to change the configuration from within the client.

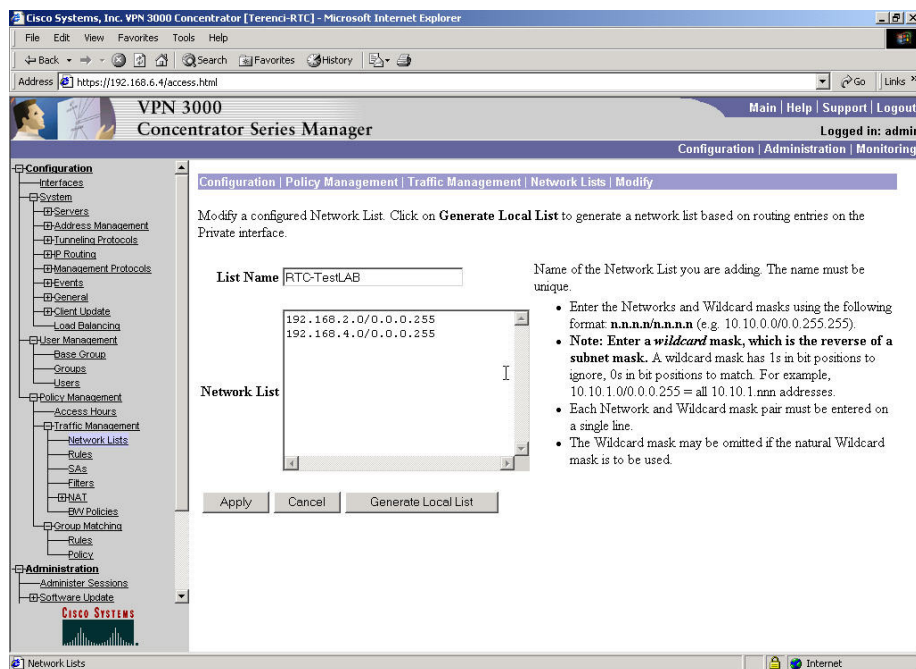
Note that split tunneling is NOT recommended as it is a security vulnerability.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The left sidebar contains a navigation tree with categories: Configuration (Interfaces, System, User Management, Base Group, Groups, Users), Policy Management, Administration (Administer Sessions, Software Update, System Reboot, Ping, Monitoring Refresh), Access Rights, File Management, and Certificate Management. The main content area is titled 'Common Client Parameters' and contains several configuration sections:

- DHCP Configure Message:** A checkbox that is checked, with a description: 'Check to use group policy for clients requesting Microsoft DHCP options.'
- Subnet Mask:** A text input field, with a checked checkbox and description: 'Enter the subnet mask for clients requesting Microsoft DHCP options.'
- Split Tunneling Policy:** Two radio buttons: 'Tunnel everything' (unchecked) and 'Only tunnel networks in the list' (checked). A description explains the settings: 'Select the method and network list to be used for Split Tunneling. **Tunnel Everything:** Send all traffic through the tunnel. **Allow the networks in the list to bypass the tunnel:** The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. **Tunnel networks in the list:** Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.'
- Split Tunneling Network List:** A dropdown menu showing 'RTC-TestLAB'.
- Default Domain Name:** A text input field containing 'vodafone-terenci.c', with a checked checkbox and description: 'Enter the default domain name given to users of this group.'
- Split DNS Names:** A text input field, with a checked checkbox and description: 'Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. The **Default Domain Name** must be explicitly included in **Split DNS Names** list if it is to be resolved through the tunnel.'

At the bottom of the configuration area are 'Apply' and 'Cancel' buttons. The status bar at the very bottom indicates 'Group Parameters' and 'Internet'.

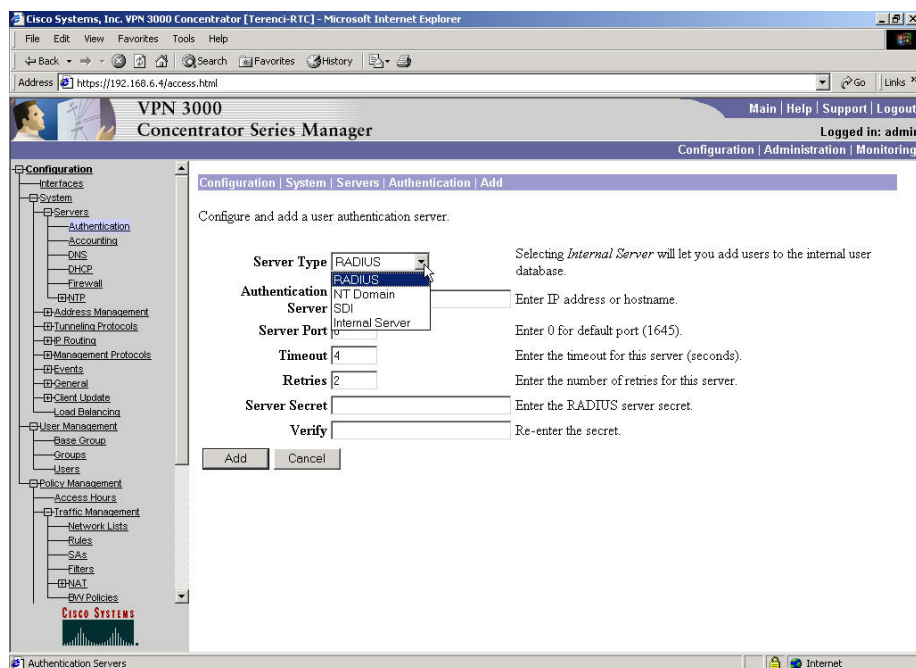
If split tunneling is enabled by choosing "Only tunnel networks in the list" a network list has to be created in the Policy Management / Traffic Management menu.



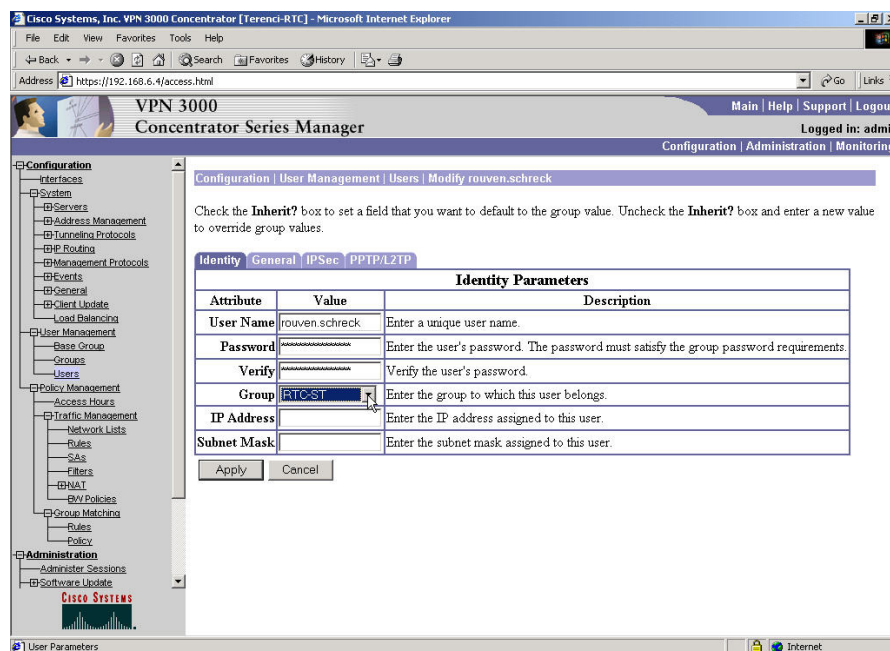
If split tunnelling is disabled by choosing the option “Tunnel everything” the internet connection can be established using an internal proxy or directly from internal network through the Firewall.

## 5 User Management and Profile Handling

Integrated user management and external authentication server such as RADIUS, SDI, NT- or AD-Domain are supported. You can choose it in the Configuration / System / Server / Authentication menu.

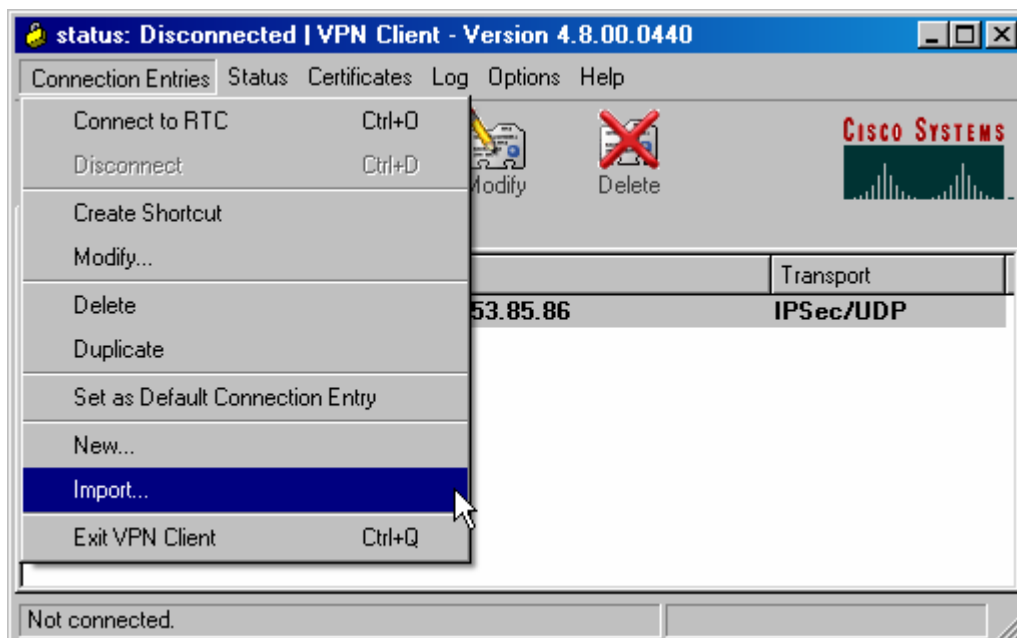


Group profiles with different configuration are supported, but each user can only be a member of one group. From the pull-down menu for the group membership you can select only one group.



The connection profile is for the first time locally configured. After connecting to the Concentrator the profile will be updated automatically each time the Client connects. The Client application offers the possibility to import this profile.

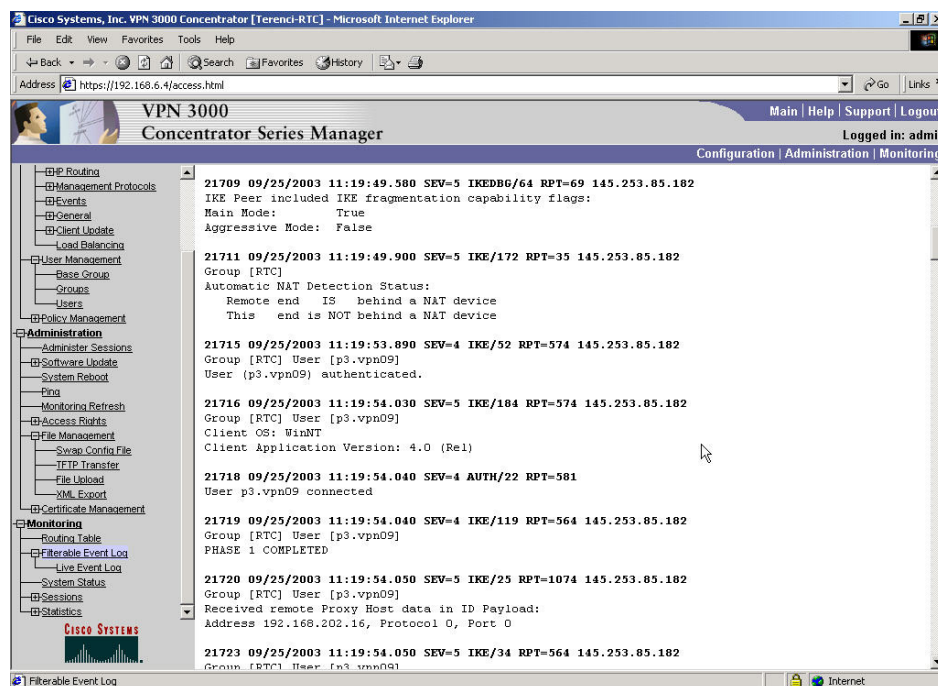
Cisco VPN Client 4.8.00.0440



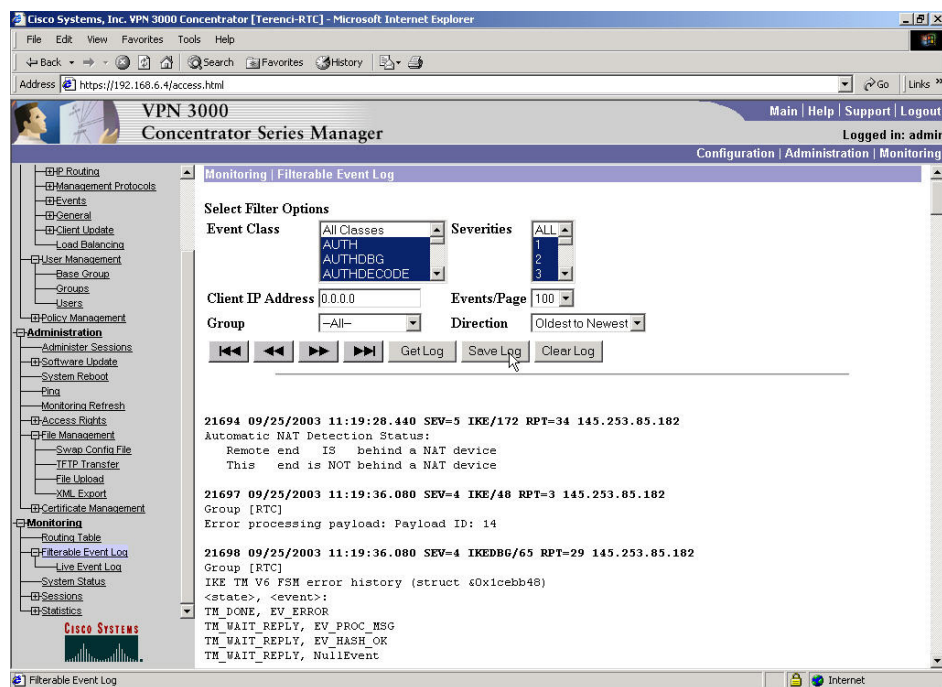
Profile configuration file (.pcf file) is placed in "C:\Program Files\Cisco Systems\VPN Client\Profiles".

## 6 Logging

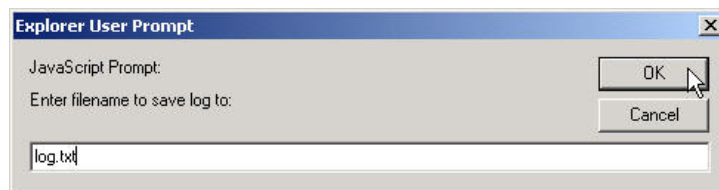
Event logging is available on the Monitoring / Filterable Event Logs screen. This screen shows the events in the current log file, lets you filter and display events by various criteria, and lets you manage the event log file.



To save a copy of the current event log as a file on the VPN Concentrator, click the “Save Log” button.



The browser prompts you for a filename, which must conform to the 8.3 naming convention.



To view, delete or copy files on the VPN Concentrator, see the Administration / File Management screen.

Cisco Systems, Inc. VPN 3000 Concentrator [Terenci-RTC] - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History Links

Address <https://192.168.6.4/access.html> Go

**VPN 3000** Main Help Support Logout  
Concentrator Series Manager

Logged in: admin  
Configuration Administration Monitoring

**Administration | File Management** Thursday, 25 September 2003 14:26:18  
Refresh

This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate **Action**, or choose an action from the list below.

- [Swap Config File](#) -- swap the backup and boot configuration files.
- [TFTP Transfer](#) -- transfer files via TFTP.
- [File Upload](#) -- send a file via HTTP.
- [XML Export](#) -- export the configuration to an XML file.

Total: 12368KB, Used: 192KB, Free: 12176KB

Filename	Size (bytes)	Date/Time	Actions
CONFIG.BAK	37646	09/25/2003 13:16:16	<a href="#">View</a> <a href="#">Delete</a> <a href="#">Copy</a>
CONFIG	37646	09/25/2003 14:10:32	<a href="#">View</a> <a href="#">Delete</a> <a href="#">Copy</a>
LOG.TXT	20840	09/25/2003 14:26:14	<a href="#">View</a> <a href="#">Delete</a> <a href="#">Copy</a>
SAVELOG.TXT	20814	09/09/2003 17:31:48	<a href="#">View</a> <a href="#">Delete</a> <a href="#">Copy</a>

**Configuration**

- Interfaces
- System
  - Servers
  - Address Management
  - Tunneling Protocols
  - IP Routing
  - Management Protocols
  - Events
  - General
  - Client Update
  - Load Balancing
- User Management
  - Base Group
  - Groups
  - Users
- Policy Management

**Administration**

- Administer Sessions
- Software Update
- System Reboot
- Pin
- Monitoring Refresh
- Access Rights
- File Management
  - Swap Config File
  - TFTP Transfer
  - File Upload
  - XML Export
- Certificate Management

**Monitoring**

CISCO SYSTEMS

Copy Internet

## 7 Name Resolution

DNS and WINS configuration is integrated in the group profile. After connection establishment DNS server IP address is assigned by the Concentrator to the Client as primary/secondary DNS server for resolving host names.

The screenshot shows the Cisco VPN 3000 Concentrator Series Manager web interface. The left sidebar contains a tree view with categories like Tools, Tunneling Protocols, IP Routing, Management Protocols, User Management, Policy Management, Administration, and Monitoring. The main content area is titled 'Configuration | User Management | Groups | Modify RTC'. Below this, there is a table for 'General Parameters' with columns for Attribute, Value, Inherit?, and Description. The table contains settings for Access Hours, Simultaneous Logins, Minimum Password Length, Allow Alphabetic-Only Passwords, Idle Timeout, Maximum Connect Time, Filter, Primary DNS, Secondary DNS, Primary WINS, and Secondary WINS. The 'Inherit?' column has checkboxes, and the 'Value' column contains input fields or dropdown menus.

Attribute	Value	Inherit?	Description
Access Hours	No Restrictions	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	10	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	4	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	None	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS	192.168.2.10	<input type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS	192.168.2.10	<input type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.

\*\*\* End of Document \*\*\*