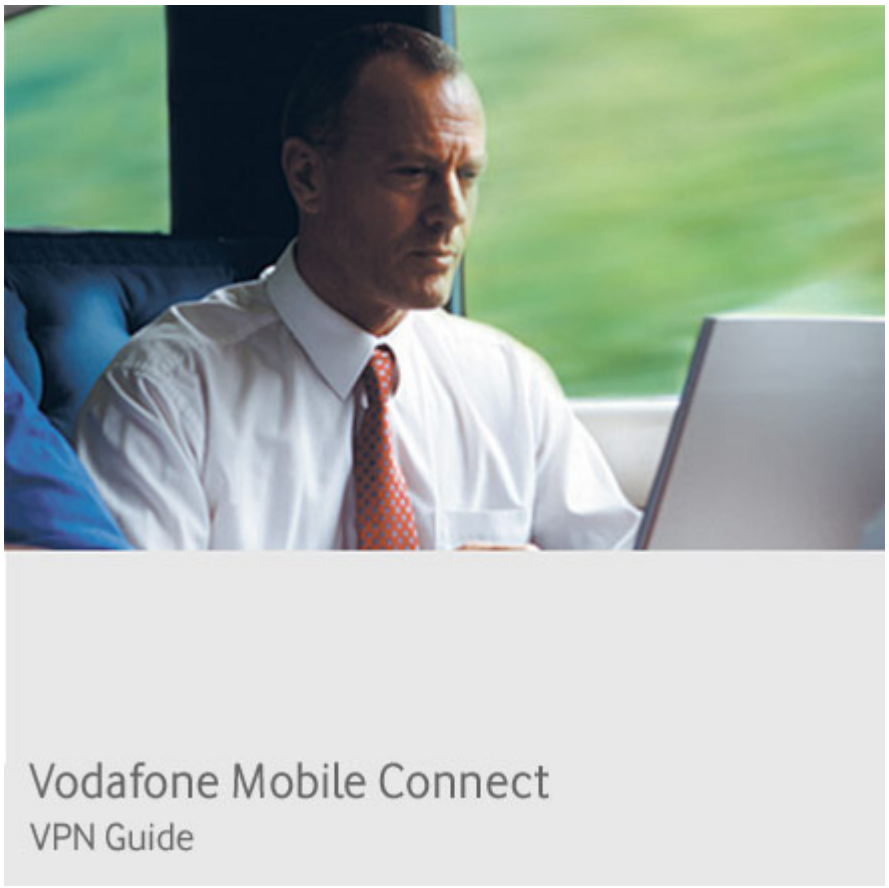
# VPN End to End – Cisco 3005 – Appendix

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

# Contents



# 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

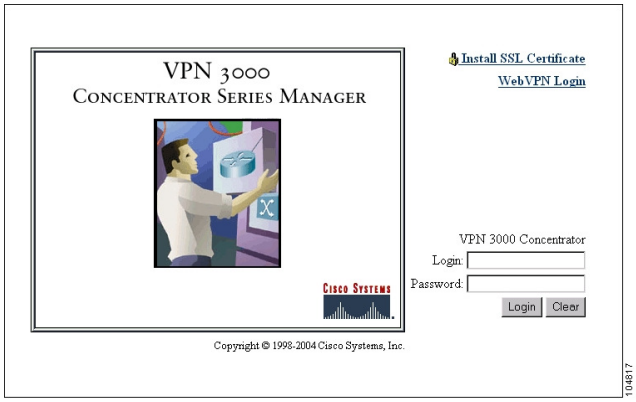
After unpacking the Concentrator install the device in your office environment with connecting power, internal and external network connections – and the console cable to your PC.

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)

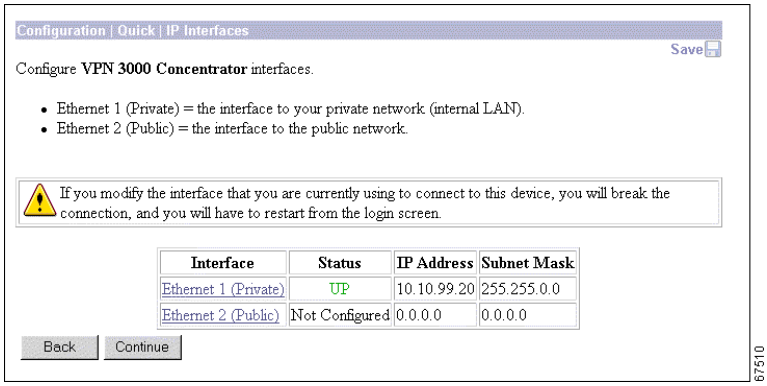
## 2.2 Using the web-based Concentrator manager

- 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.

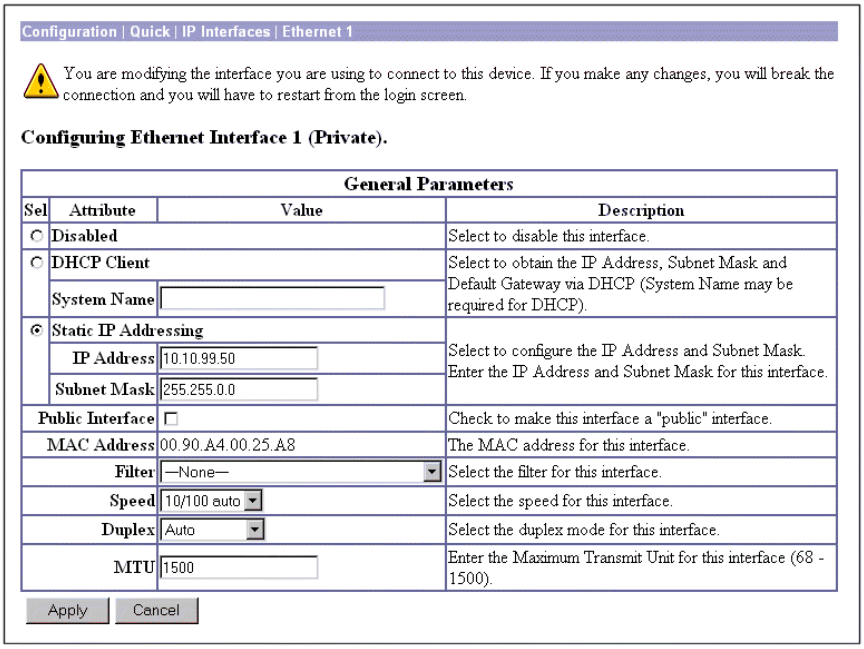



- The following screen appears only the first time you are logging in and offers the Quick Configuration option. If you do not see this screen please navigate through the configuration menus by clicking the Explorer-style tree on the left-hand side. The relevant branch for the basic setup is “Configuration”.

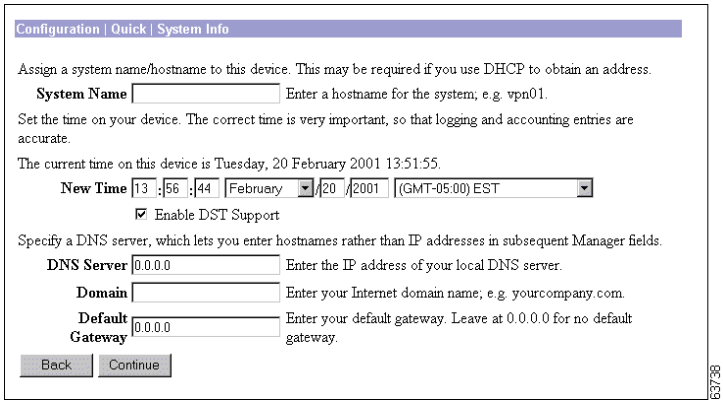

- We continue with Quick Configuration dialog. The next screen lets you configure the VPN Concentrator Ethernet interfaces. The Model 3005 comes with two Ethernet interfaces. Models 3015-3080 come with three Ethernet interfaces.



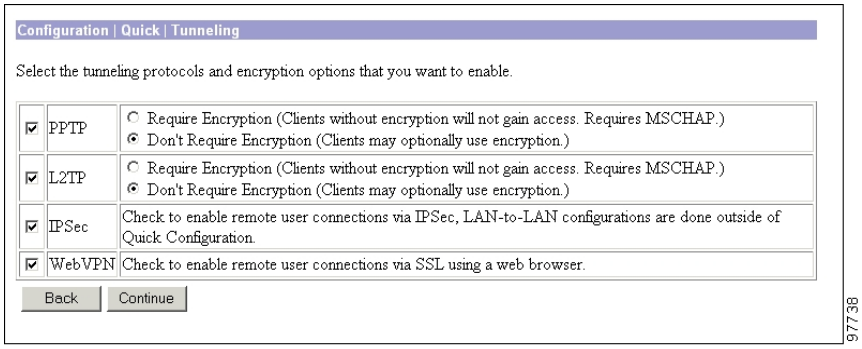

- Configure the external/public IP address. Any changes to your internal/private address terminates the admin session. To configure click on Ethernet 2 and the following screen appears. To make this interface a public interface that is facing to the internet, check the Public Interface check box. Make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



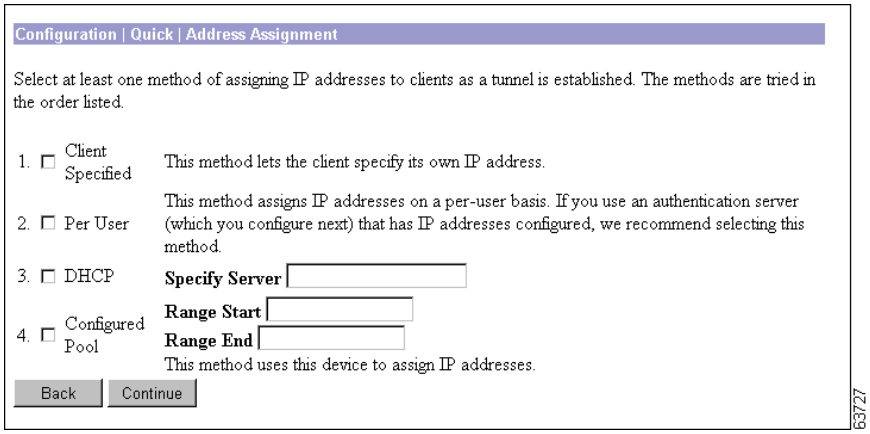

- To configure basic information that identifies your VPN Concentrator on the network you will see the following “System Info” screen. Enter a system name, the current time, DNS Server Address, Domain name and the default gateway – your next hop to the internet. (DST = Daylight-Saving Time)




- 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

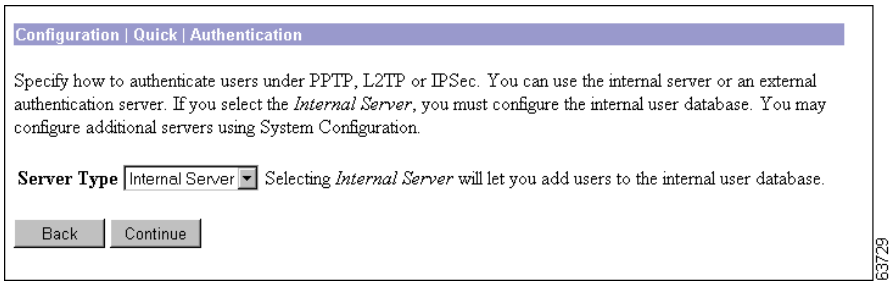



- Check Configured Pool to enable this method, which lead the VPN Concentrator to assign IP addresses from an internally configured pool. Enter the starting and ending IP addresses available in the initial pool, in the Range Start and Range End fields. Enter these addresses in dotted decimal notation;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

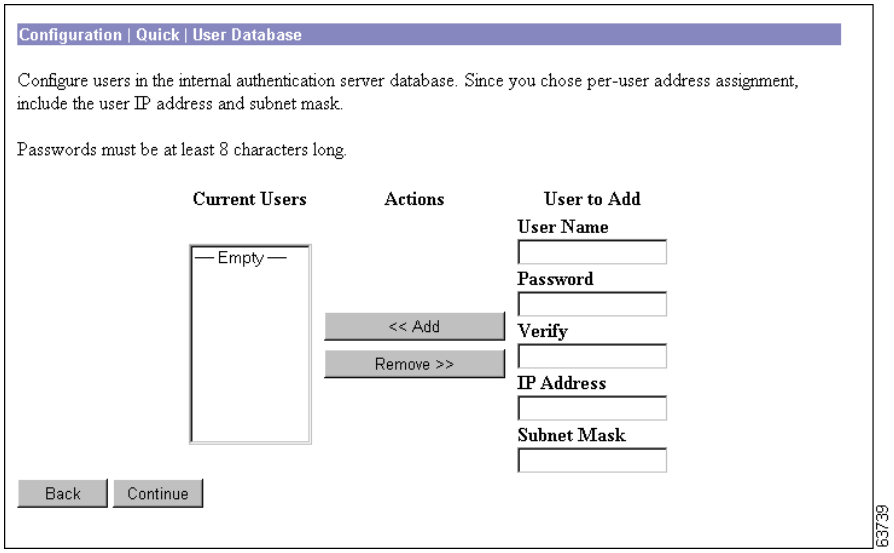



- On the following screen you can choose how to authenticate users. You can select the VPN Concentrator internal server or one of three external server types. We use the default “internal server” that does support up to 100 groups and users (combined). The following selection is possible:

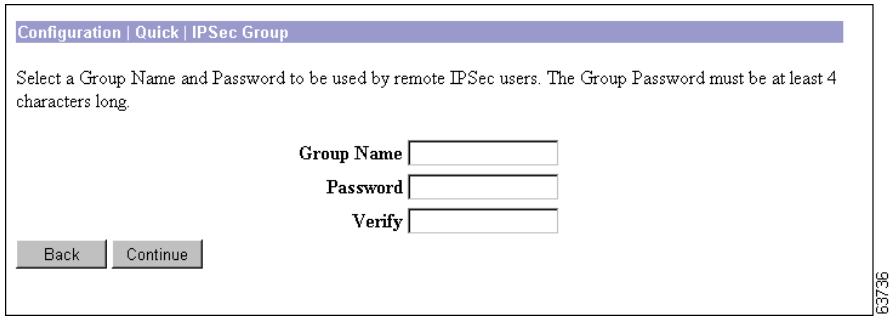
- Internal Server — the internal VPN Concentrator authentication server. (This is the default selection.)
- RADIUS — an external Remote Authentication Dial-In User Service server.
- NT Domain — an external Windows NT Domain server.
- SDI — an external RSA Security Inc. SecurID server.
- Kerberos/Active Directory—An external Windows/Active Directory server or a UNIX/Linux Kerberos server

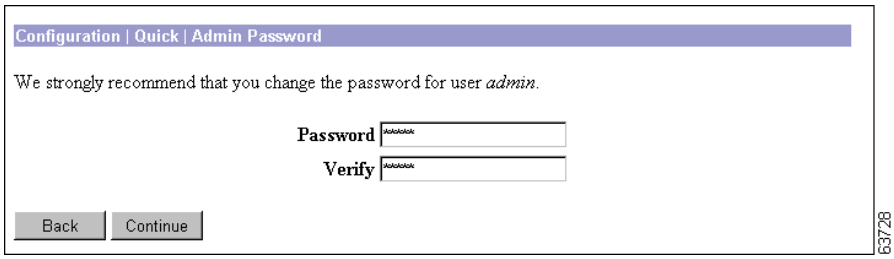



- On the next screen you have to configure at least one user. Unless you choose an address pool like before you can assign IP addresses to a specific user. In our example we leave the address field blank.




- 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

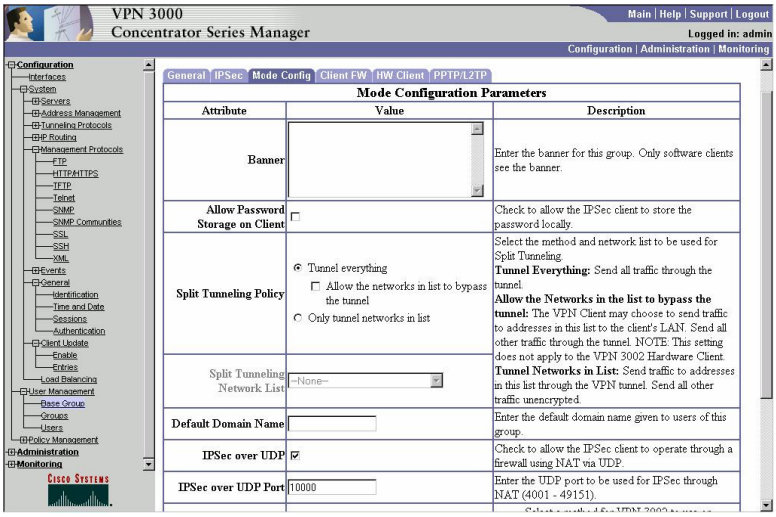




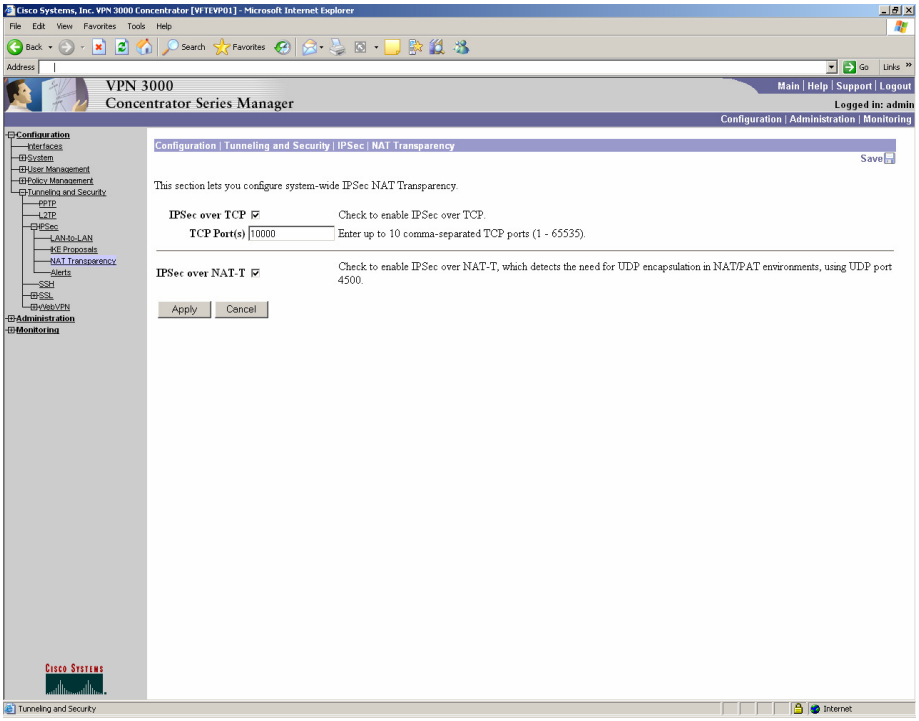

- After done you need to save all changes into the NVRAM of the Concentrator by clicking the “Save Needed” icon. Now you’ve finished the base configuration. For using with Mobile Connect Cards over the Vodafone UMTS/GPRS infrastructure you need to do some advanced settings.

## 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.

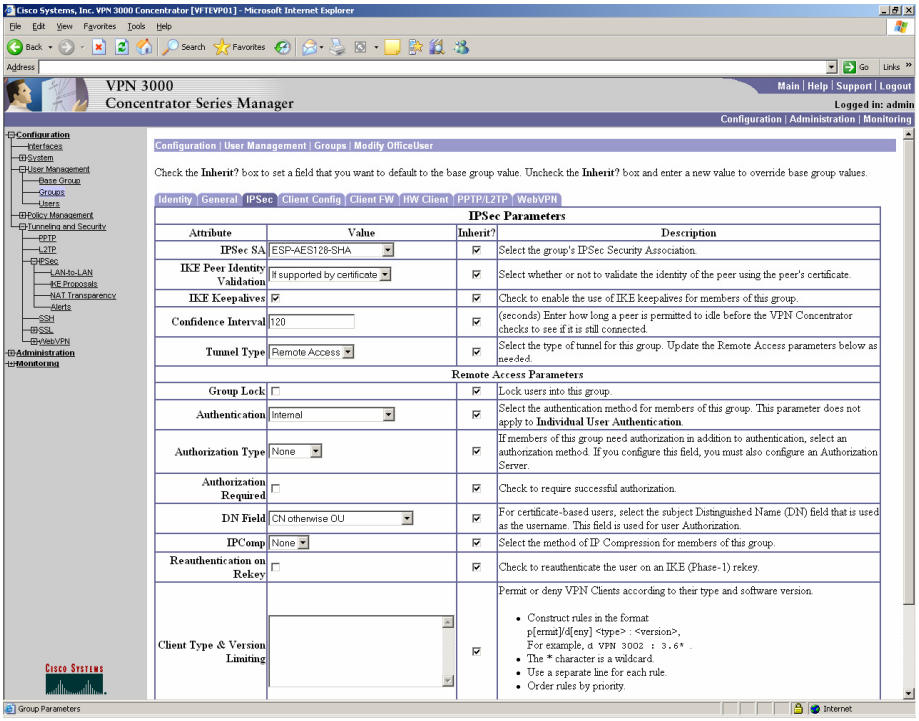



- As an alternative you can use the IETF draft NAT-T implementation. To enable this option go to the menu Configuration | Tunnelling and Security | IPSec | NAT Transparency screen and enable **IPSec over NAT-T.**

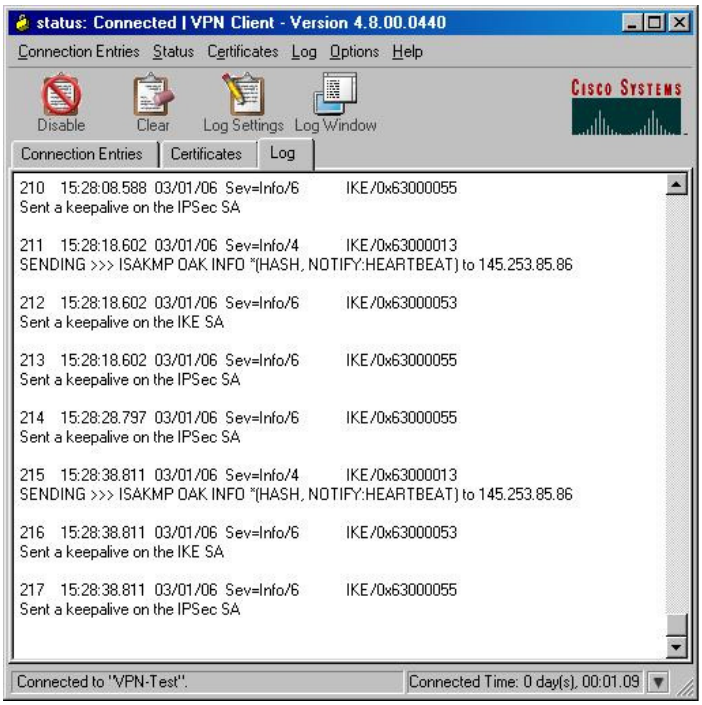



## 2.4 IKE keep alive

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.

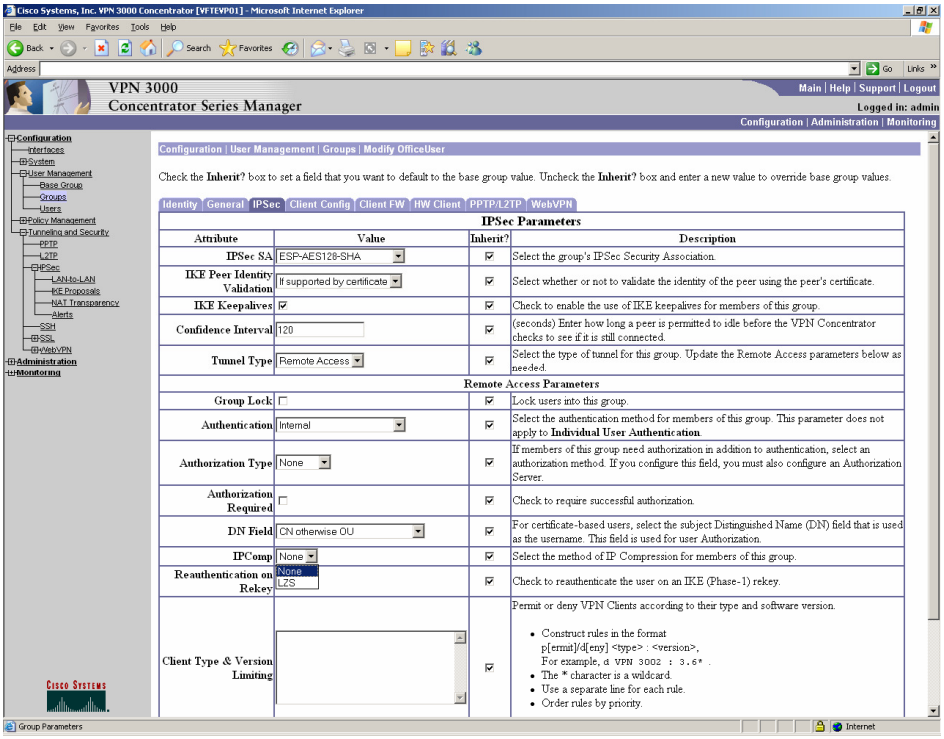



On the Client side you can see the “keep alive” messages on the local log window



## 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.



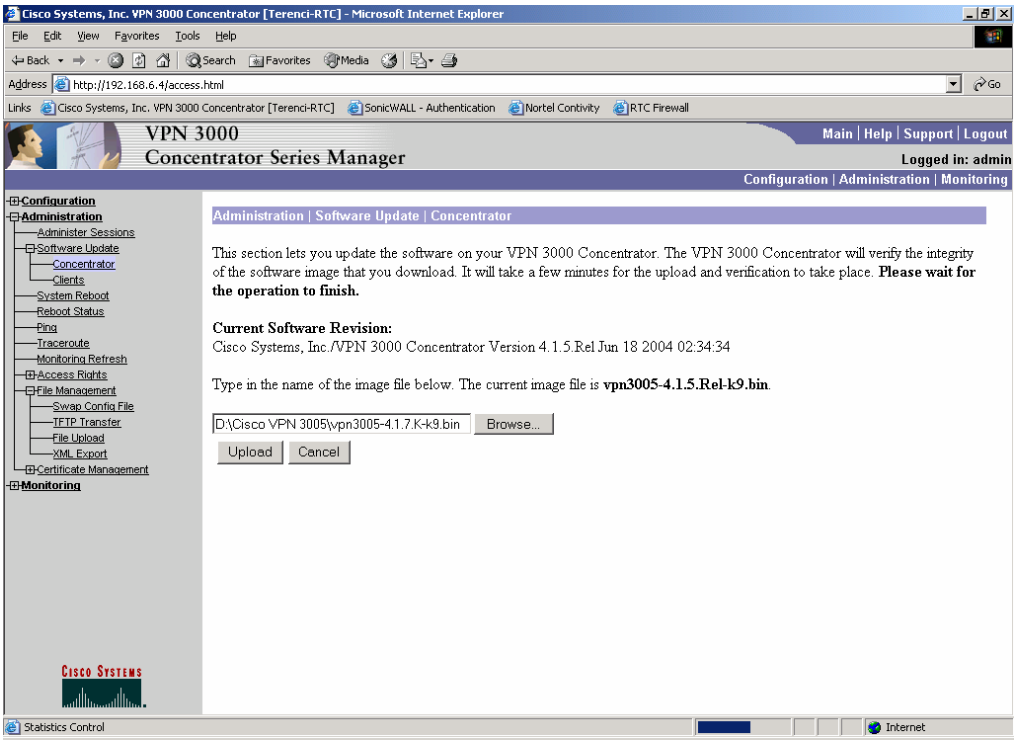

Note that software compression was shown to have little benefit for most environments. The benefit of compression should be reviewed in light of the cost of processor load for both the client and server.

# 3 Update procedure

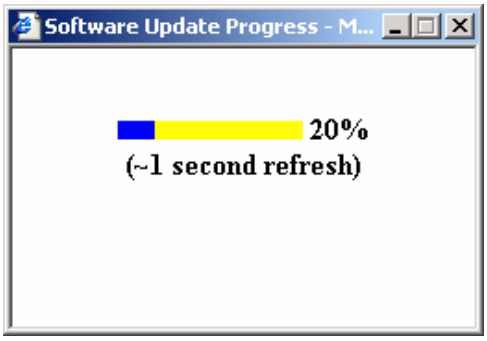
This process uploads the executable system software to the VPN Concentrator, which then verifies the integrity of the software image.

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.

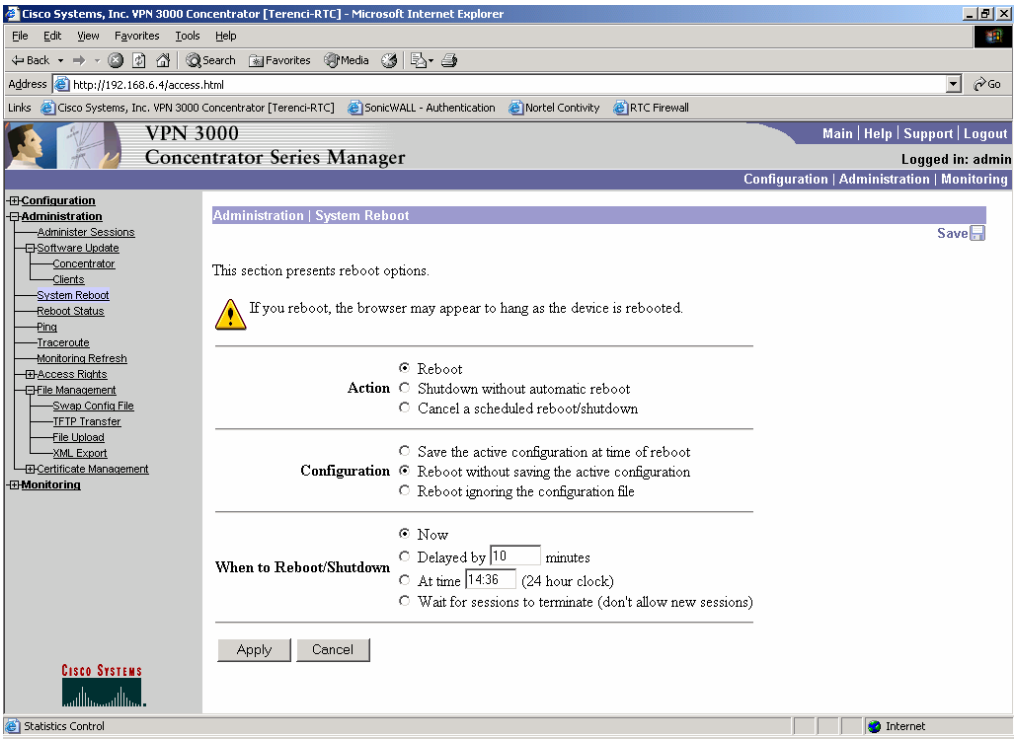



It takes a few minutes to upload and verify the software, and the system displays the progress. It refreshes the number of bytes transferred at 10-second intervals. Please wait for the operation to finish.



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.

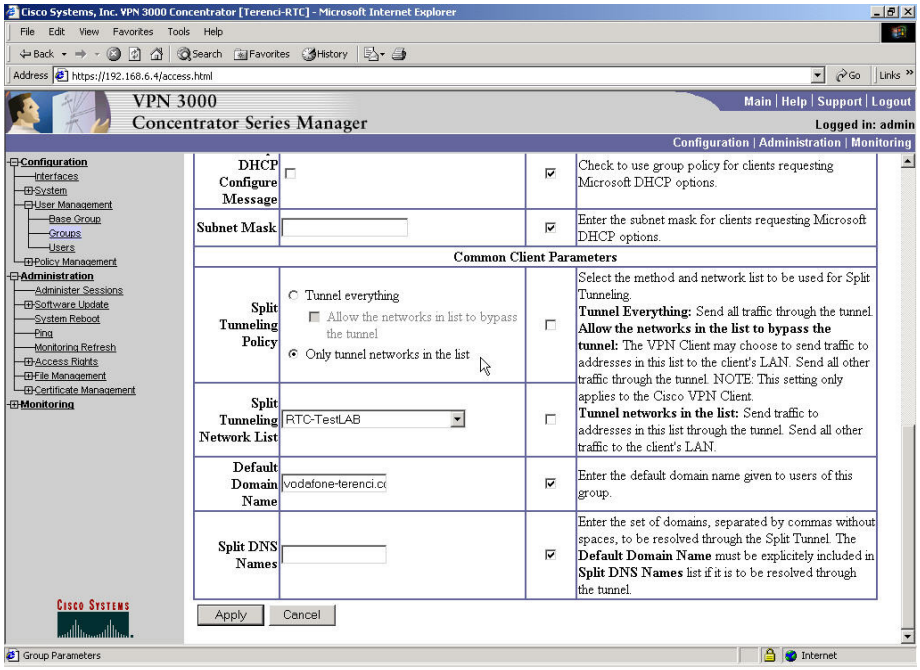

Cisco Systems, Inc. VPN 3000 Concentrator [Terenci-RTC] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.6.4/access.html
Links Cisco Systems, Inc. VPN 3000 Concentrator [Terenci-RTC] SonicWALL - Authentication Nortel Contivity RTC Firewall
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
Concentrator
Clients
System Reboot
Reboot Status
Ping
Traceroute
Monitoring Refresh
Access Rights
File Management
Swap Config File
TFTP Transfer
File Upload
XML Export
Certificate Management
Monitoring
Administration | System Reboot
Save
This section presents reboot options.
If you reboot, the browser may appear to hang as the device is rebooted.
Action
Reboot
Shutdown without automatic reboot
Cancel a scheduled reboot/shutdown
Configuration
Save the active configuration at time of reboot
Reboot without saving the active configuration
Reboot ignoring the configuration file
When to Reboot/Shutdown
Now
Delayed by 10 minutes
At time 14:36 (24 hour clock)
Wait for sessions to terminate (don't allow new sessions)
Apply
Cancel
Cisco Systems
Statistics Control
Internet

# 4 Configuration of Split Tunnelling

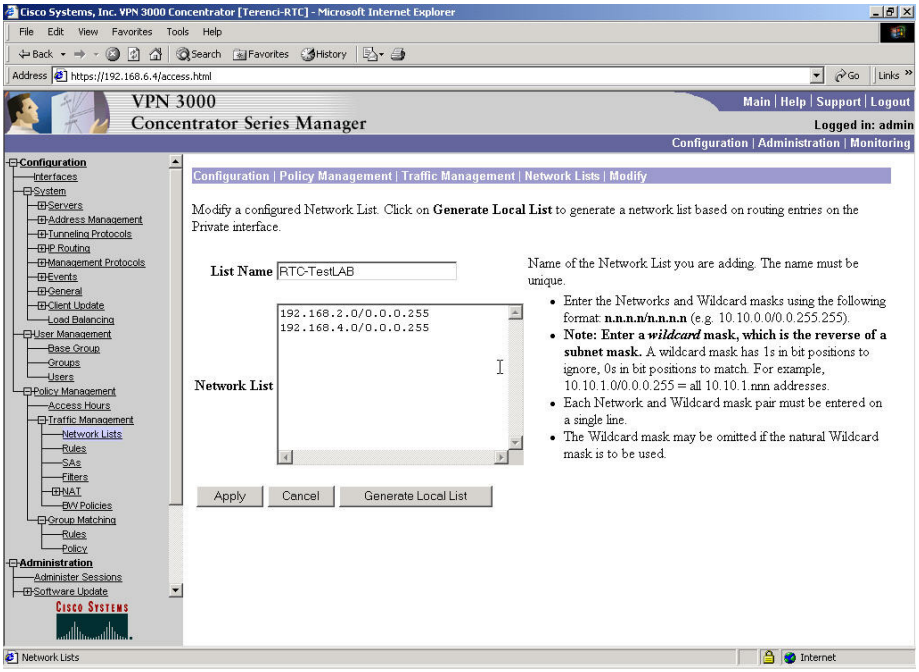
Split Tunnelling is supported and will be negotiated within connection phase by server push and is enabled by default. The user cannot override server settings.

Enabling or disabling split tunnelling 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 tunnelling is NOT recommended as it is a security vulnerability.



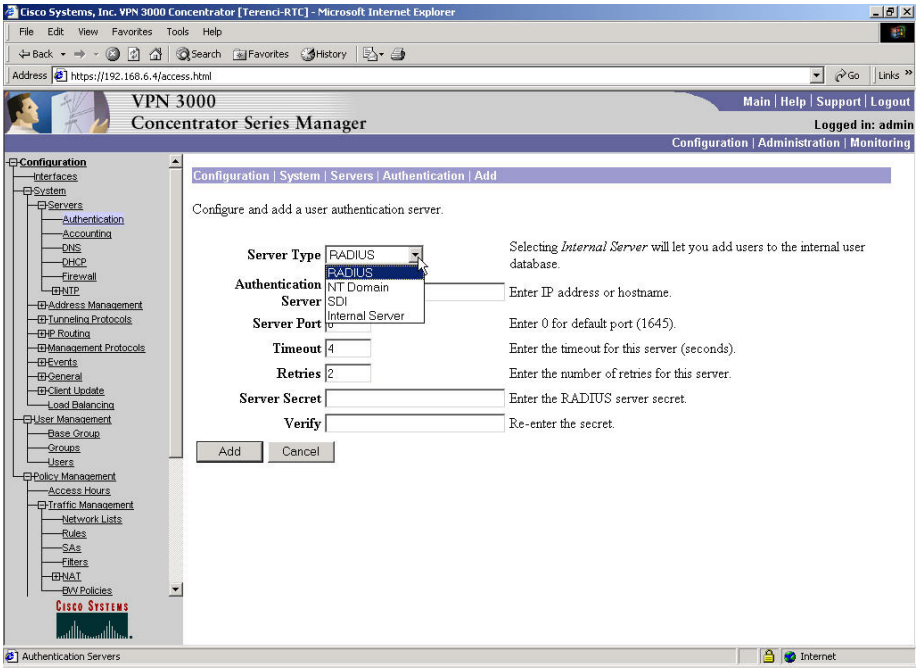

If split tunnelling is enabled by choosing “Only tunnel networks in the list” a network list has to be created in the Policy Management / Traffic Management menu.



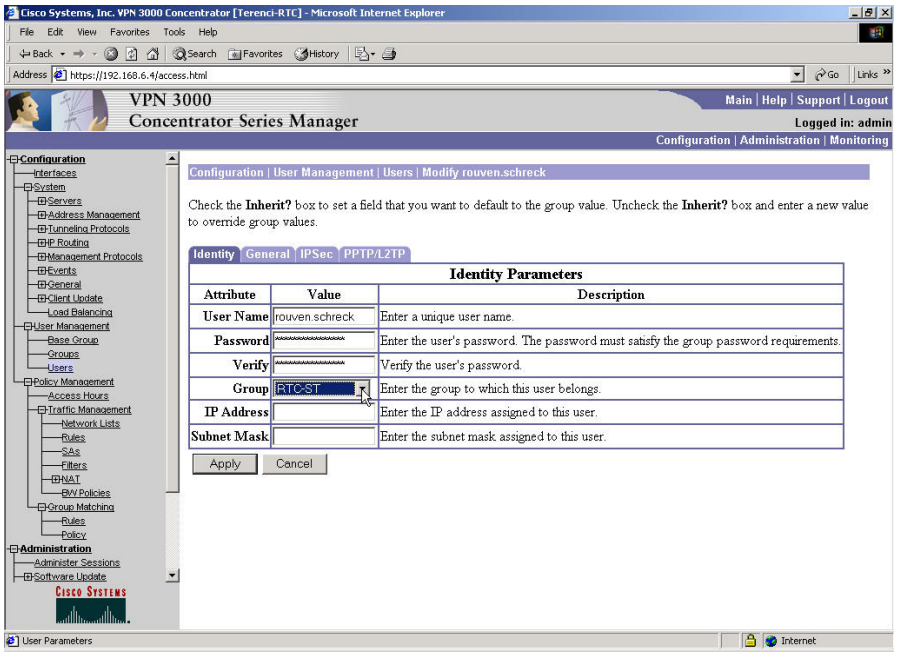

If split tunnelling is disabled by choosing the option “Tunnel everything” the internet connection can be established using an internal proxy or directly from internal network through the Firewall.

# 5 User Management and Profile Handling

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

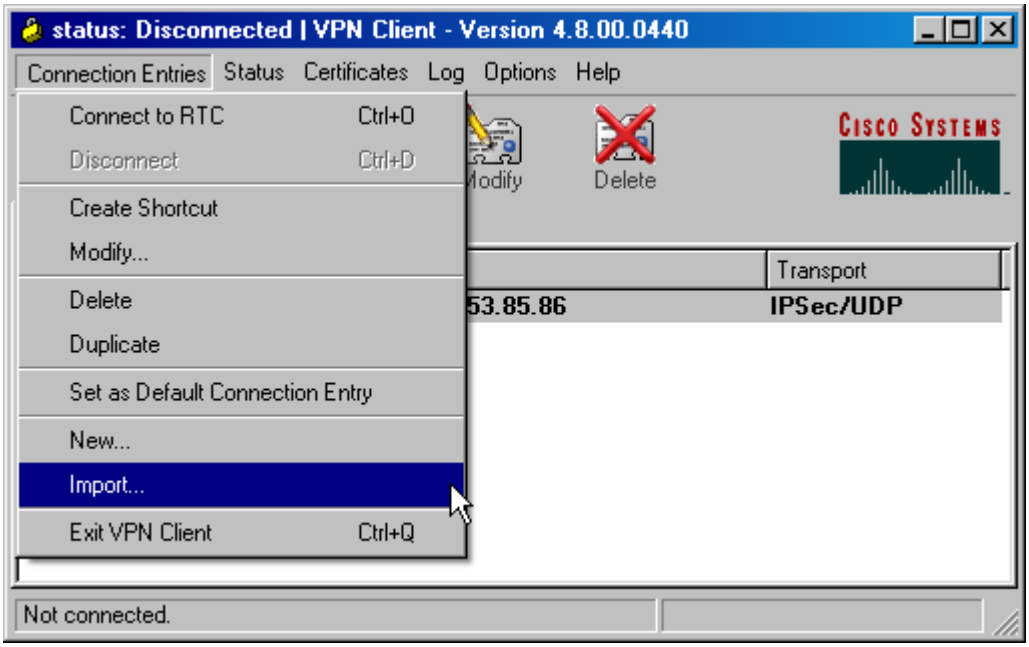



Group profiles with different configuration are supported, but each user can only be a member of one group. From the pull-down menu for the group membership you can select only one group.




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.

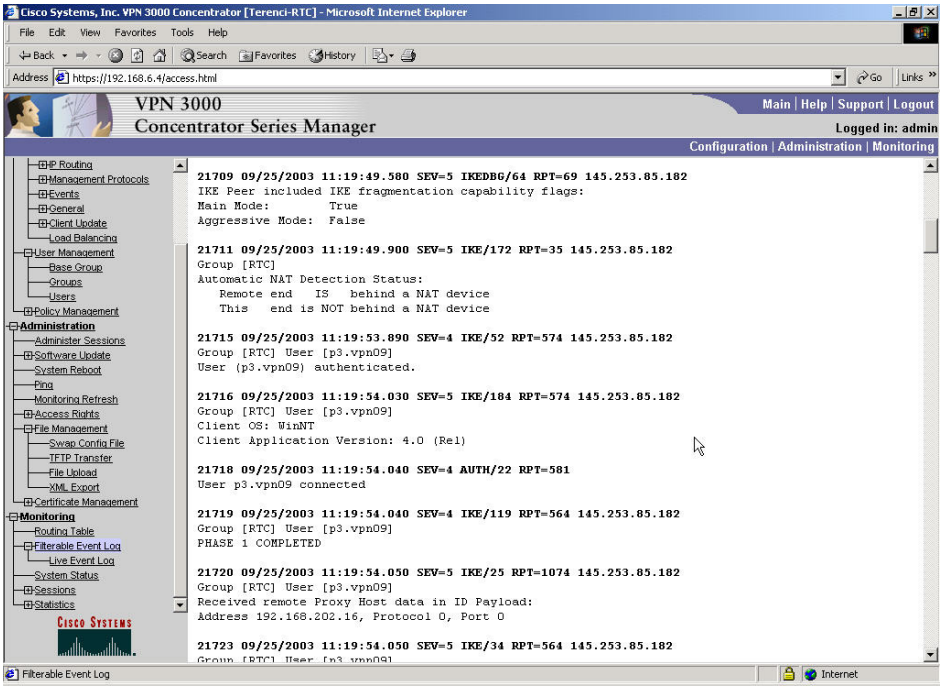
Cisco VPN Client 4.8.00.0440



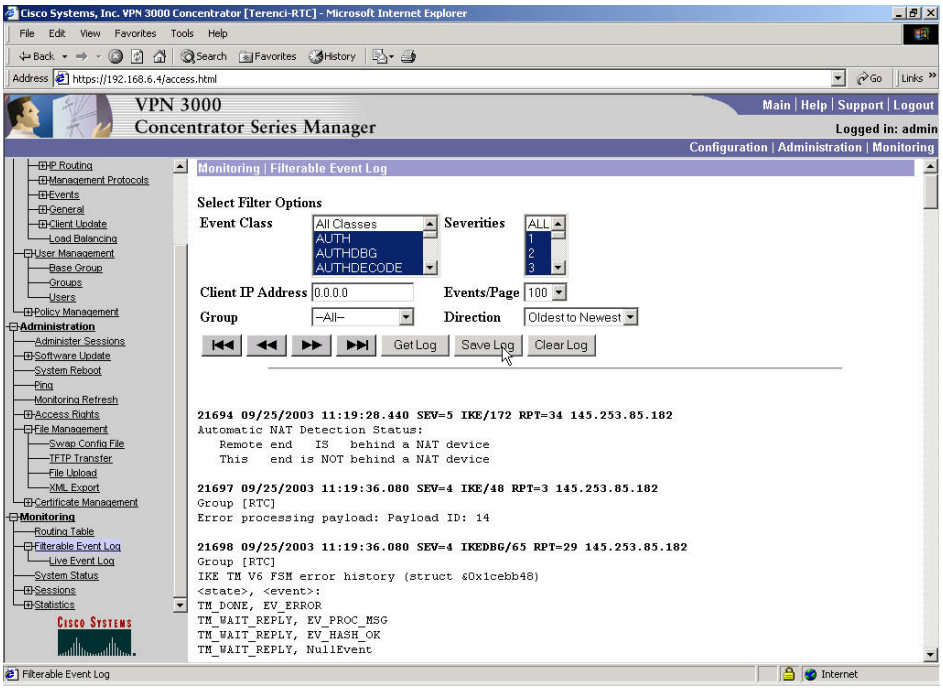

Profile configuration file (.pcf file) is placed in “C:\Program Files\Cisco Systems\VPN Client\Profiles”.

# 6 Logging

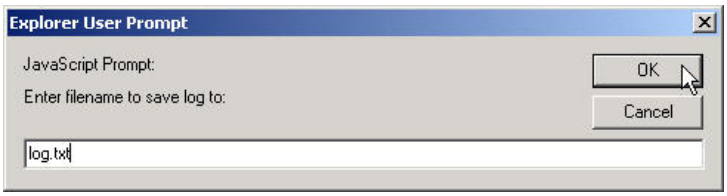
Event logging is available on the Monitoring / Filterable Event Logs screen. This screen shows the events in the current log file, lets you filter and display events by various criteria, and lets you manage the event log file.



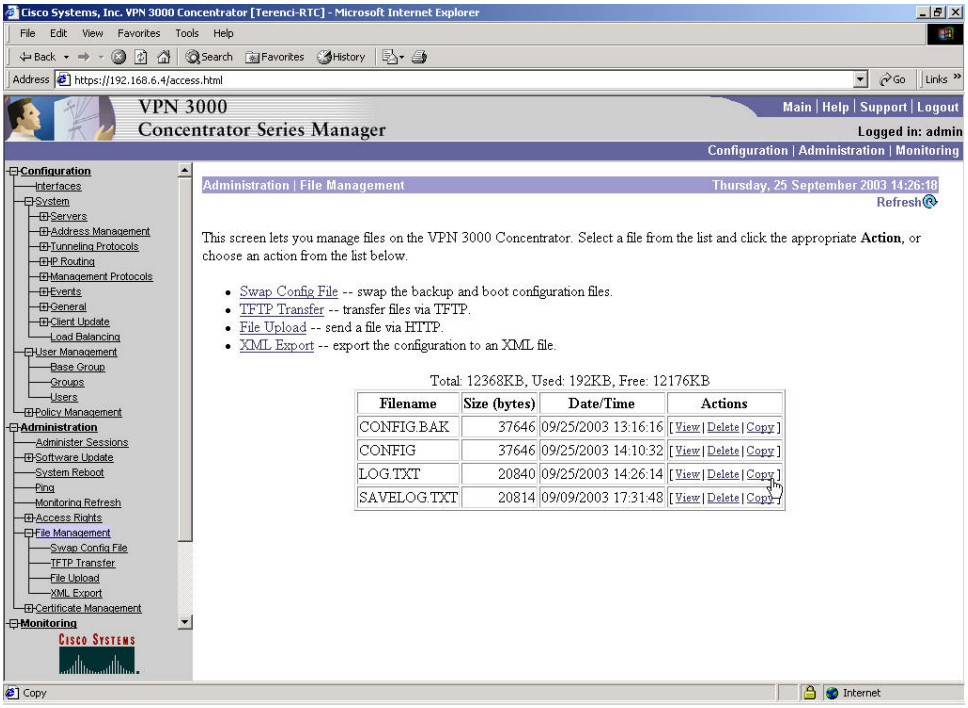

To save a copy of the current event log as a file on the VPN Concentrator, click the “Save Log” button.




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

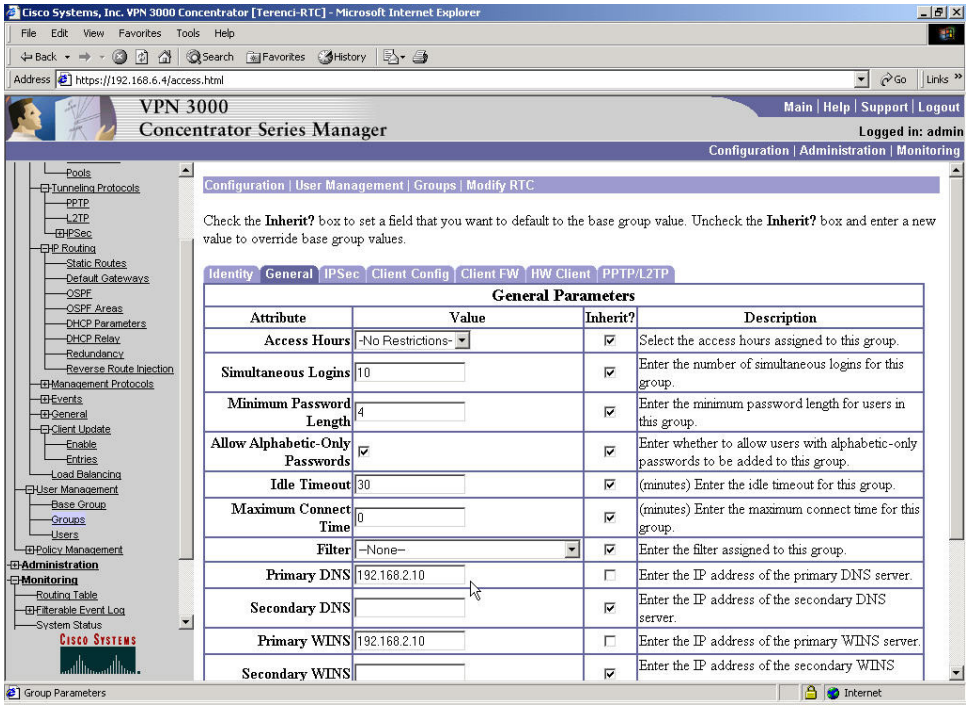



To view, delete or copy files on the VPN Concentrator, see the Administration / File Management screen.


Cisco Systems, Inc. VPN 3000 Concentrator [Terenci-RTC] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://192.168.6.4/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
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
Ping
Monitoring Refresh
Access Rights
File Management
Swap Config File
TFTP Transfer
File Upload
XML Export
Certificate Management
Monitoring
Cisco Systems
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
[ View | Delete | Copy ]
CONFIG
37646
09/25/2003 14:10:32
[ View | Delete | Copy ]
LOG.TXT
20840
09/25/2003 14:26:14
[ View | Delete | Copy ]
SAVELOG.TXT
20814
09/09/2003 17:31:48
[ View | Delete | Copy ]
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.




*** End of Document ***