ACCREDITED SOLUTION

SAILOR 250/500 – Cisco Systems VPN Client

Thrane & Thrane A/S · Lundtoftegaardsvej 93 D · DK-2800 Kgs. Lyngby · Denmark
T +45 39 55 88 00 · F +45 39 55 88 88 · info@thrane.com · www.thrane.com

inmarsat
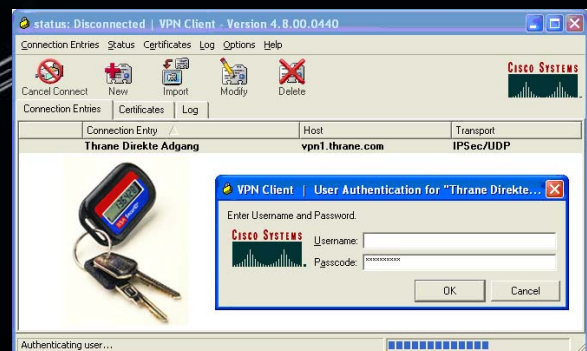
Document Name:	SAILOR 250/500 – Cisco Systems VPN Client	Revision: D

Introduction:	This document describes the Cisco VPN Client solution for use with SAILOR 250 and 500 Fleetbroadband terminals.

Typical Users:	► Ship Managers ► Merchant vessels ► Leisure yachts ► Fishery vessels

Product Description:

The VPN client from Cisco Systems is simple to deploy and operate, the Cisco VPN Client allows organizations to establish end-to-end, encrypted VPN tunnels for secure connectivity for mobile employees or teleworkers. This thin design, IP security (IPSec)-implementation is compatible with all Cisco virtual private network (VPN) products.

The Cisco VPN Client can be preconfigured for mass deployments, and initial logins require little user intervention. It supports the innovative Cisco Easy VPN capabilities, delivering a uniquely scalable, cost-effective, and easy-to-manage remote access VPN architecture that eliminates the operational costs associated with maintaining a consistent policy and key management method. The Cisco Easy VPN feature allows the Cisco VPN Client to receive security policies upon a VPN tunnel connection from the central site VPN device (Cisco Easy VPN Server), minimizing configuration requirements at the remote location. This simple and highly scalable solution is ideal for large remote access deployments where it is impractical to individually configure policies for multiple remote PCs.

The Cisco VPN Client supports Windows 98, ME, NT 4.0, 2000, and XP; Linux (Intel); Solaris (UltraSparc 32- and 64-bit); and Mac OS X, 10.2, 10.3, and 10.4. The Cisco VPN Client is compatible with the following Cisco products:

Cisco 6500 / 7600 IPSec VPNSM and VPN SPA IOS Software Release 12.2SX and later
Cisco VPN 3000 Series Concentrator Software Version 3.0 and later
Cisco IOS Software Release 12.2(8)T and later
Cisco PIX Security Appliance Software Version 6.0 and later
Cisco ASA 5500 Series Software Version 7.0 and higher

The Cisco VPN Client is included with all models of Cisco VPN 3000 Series concentrators and Cisco ASA 5500 Series security appliances, and most Cisco PIX 500 security appliances. Customers with Cisco SMARTnet® support contracts and encryption entitlement may download the Cisco VPN Client from the Cisco Software Center at no additional cost. For customers without Cisco SMARTnet support contracts, a media CD containing the client software is available for purchase.

Benefits:

- Secured access to corporate resources
- Remote PC and handheld protection
- Flexible connectivity options
- Simplified central management for lower total cost of ownership

Note: This version of the VPN client is NOT compatible with the Windows NT 3.x and 4.x operating systems.
If you are using a Windows 95, Windows 98, or Windows NT platform, you must update the VPN Client software manually. Generally, an administrator sends a notification to inform you that you must upgrade.

Cisco Systems contact details:	Support	http://www.cisco.com/web/about/ac49/ac162/about_cisco_customer_service_contacts.html
	Sales	http://www.cisco.com/en/US/ordering/or13/or8/order_customer_help_how_to_order_listing.html
	Web	http://www.cisco.com

Thrane & Thrane contact details:	E-mail	mailto:solutions@thrane.com
	T&T Distributor	http://www.thrane.com/Contact/Distributors.aspx
	Web	http://www.thrane.com

| Tested on products: | SAILOR 250/500 | Software version: 1.04 |
| | Cisco VPN Client | Software version: 4.8.00.0440 |

| Instructions: | It is recommended to remove any old VPN Client software before installing the Cisco VPN Client with MSI. |

1. Install the VPN Client by double-clicking the MSI installer (vpnclient_en.msi). This may take a few minutes as it gathers system information.
2. To continue the installation choose [Next]
3. Accept the license agreement [Next]
4. [Next]
5. [Next]
6. [Finish]
7. Restart your system

After successfully installing the Cisco VPN Client software a New VPN Connection Entry must be imported.

Start up the Cisco VPN Client from Start -> Programs -> Cisco Systems VPN Client -> VPN Client

Your network administrator might have created a connection entry profile for you. To use this profile, you must first import the profile to the Profiles directory on your computer. To import a new connection entry profile from a file, either display the Connection Entries menu and choose Import (as shown below) or click the Import icon on the toolbar above the Connection Entries tab. The VPN Client displays the Import VPN Connection dialog box.
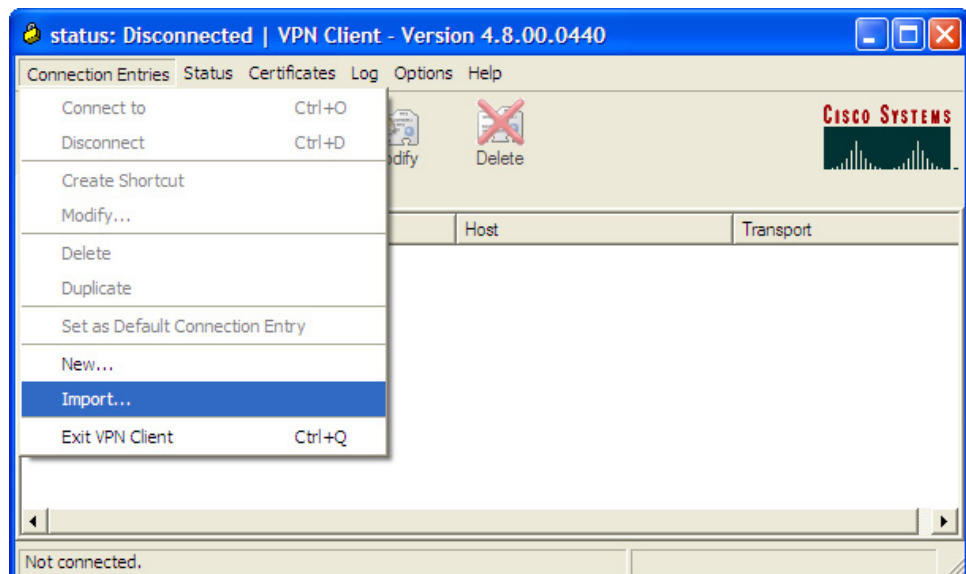
Type the file name (a file with a .pcf extension) in the File Name box or browse to find the file you want to import (see next page).
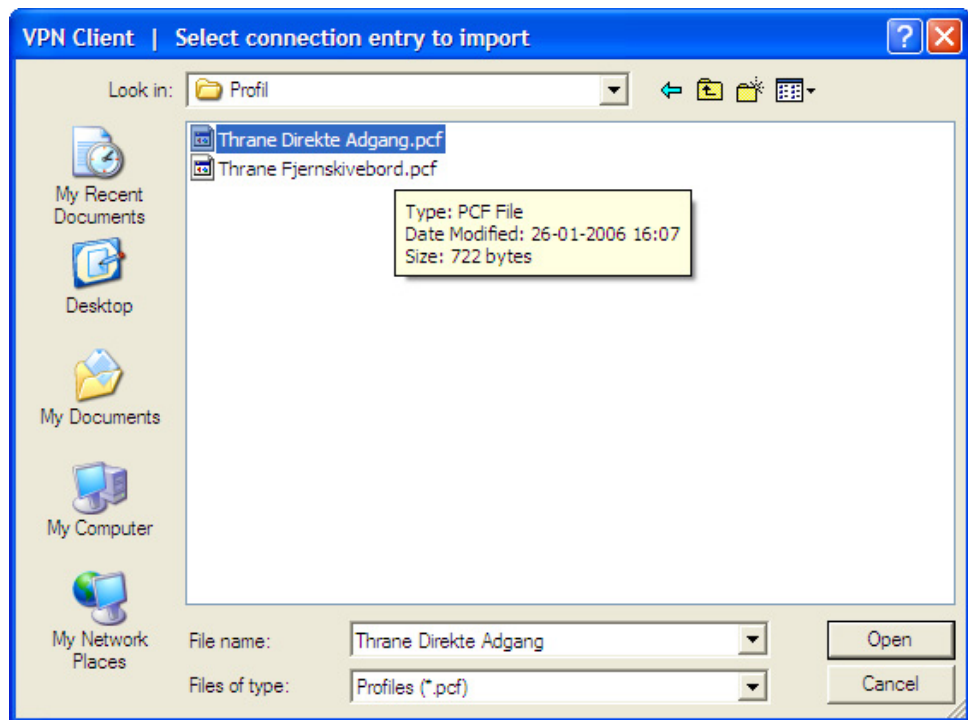
The VPN Client displays a message to let you know that the import action succeeded and places the imported profile in the Cisco Systems\VPN Client\Profiles directory.
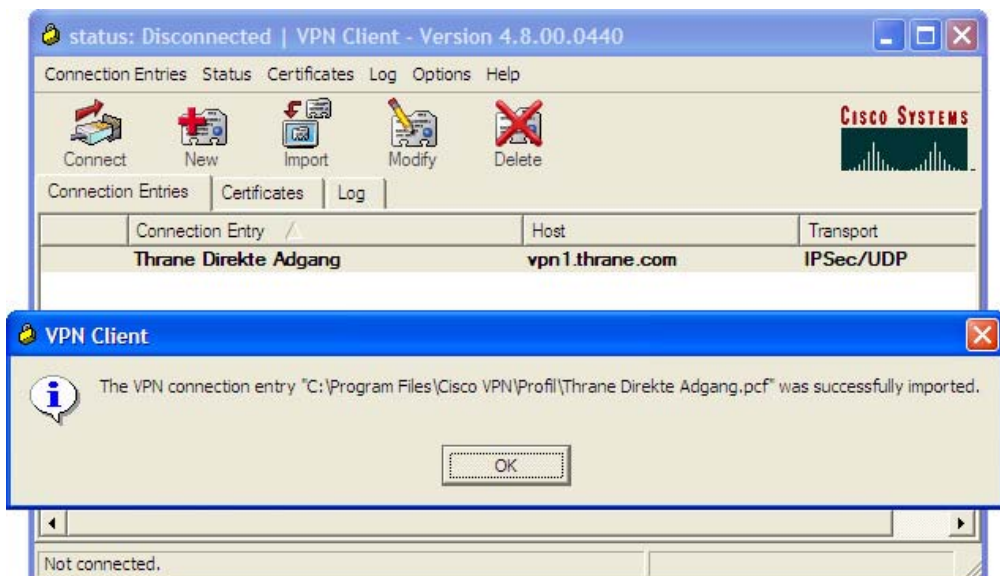

You are now ready to use the Cisco VPN Client.

If your computer is connected to the Internet for instance via SAILOR FleetBroadband terminal, then you can click on the Connect icon or use the menu as shown on next page.
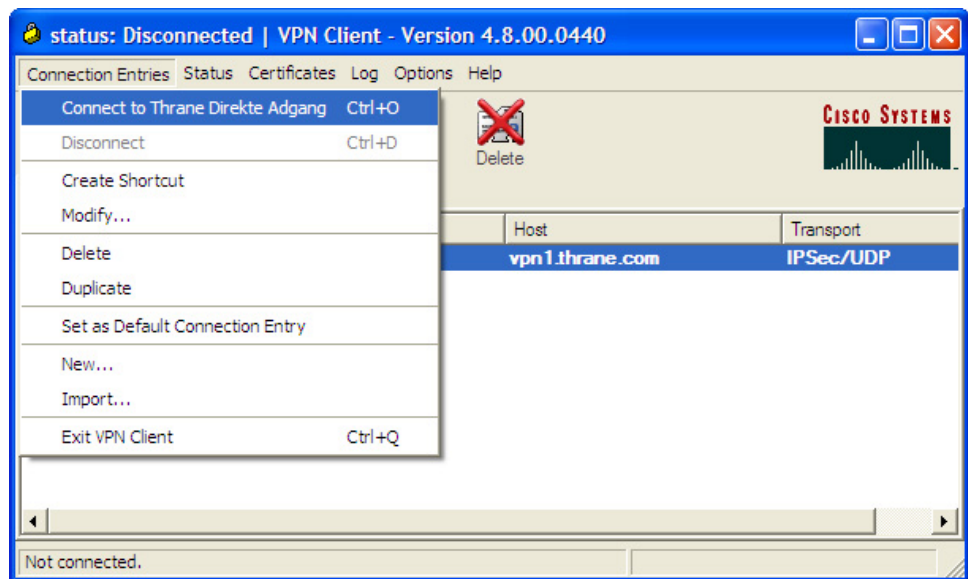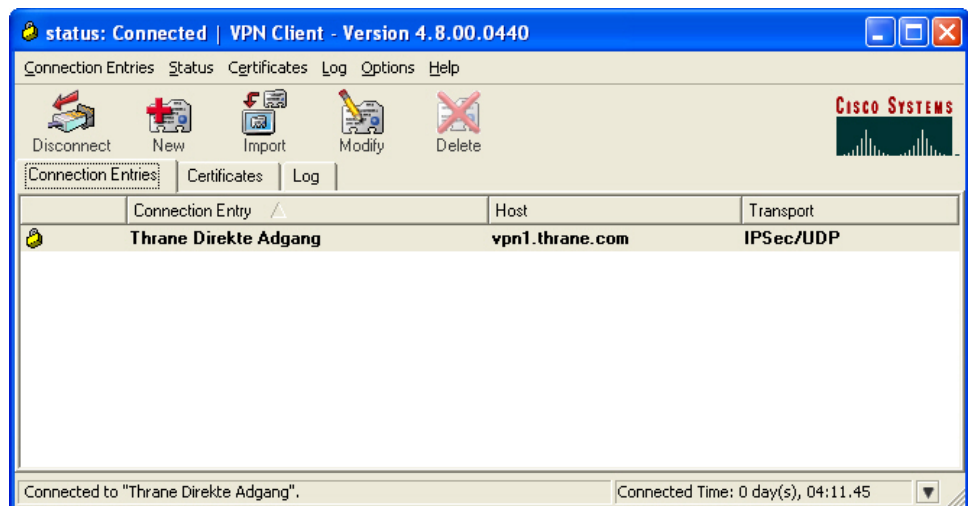
After a few seconds you will be prompted for a username and passcode.

The passcode may be a combination of a personal code and the code generated in the Secure Token similar to the one above. Please check with your IT Administrator.
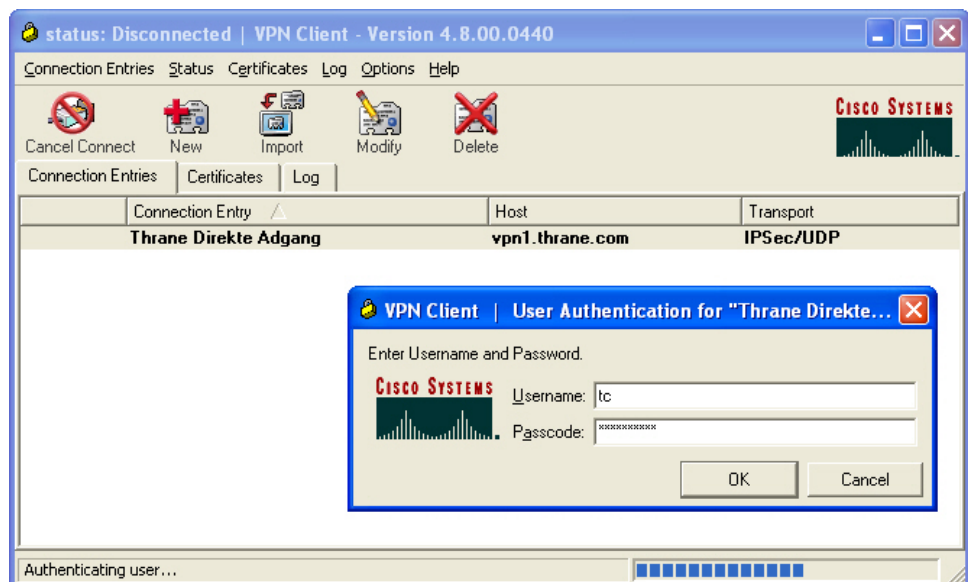
After authentication and exchange of security policies the window will disappear and a small lock will be shown in you status window.

status: Connected | VPN Client - Version 4.8.00.0440

Connection Entries   Status   Certificates   Log   Options   Help

Disconnect   New   Import   Modify   Delete

CISCO SYSTEMS

Connection Entries | Certificates | Log

Connection Entry △	Host	Transport
Thrane Direkte Adgang	vpn1.thrane.com	IPSec/UDP

Connected to "Thrane Direkte Adgang".   Connected Time: 0 day(s), 04:11.45

You are now connected to you corporate network via your Cisco VPN tunnel.

Note: The best performance is achieved by using IPSec and UDP encapsulation.

Tested: Following tests were performed:
#1   Simultaneous Standard Voice and VPN connected via Standard Data connection
#2   Chat using MS Messenger
#3   Connected to MS Exchange Server and send and receive emails
#4   File Transfer using CoreFTP

Remote Satellite Systems
INTERNATIONAL

TOLL FREE 1-888-989-8199

1455 N. Dutton Suite A, Santa Rosa, CA 95401
FAX 707-546-8198 • info@remotesatellite.com
www.remotesatellite.com