

# PROPALMS VPN

---



## Propalms VPN Installer Quick Start Guide

---

Version 3.4



©1999-2009 Propalms Ltd. All rights reserved.

The information contained in this document represents the current view of Propalms Ltd. on the issues discussed as of the date of publication. Because Propalms Ltd. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Propalms Ltd., and Propalms Ltd. cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. PROPALMS LTD. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Propalms Ltd.

Contact Propalms Ltd.

Unit 4, Park Farm Courtyard,  
Easthorpe, Malton,  
North Yorkshire,  
YO17 6QX,  
UK  
Email: [info@propalms.com](mailto:info@propalms.com)  
Call: +44 (0)1653 696060

## Contents

PROPALMS OS.....	4
Steps for Installation of Propalms OS .....	4
Configuration of Propalms OS.....	5
VPN STATES.....	10
Boot strap State .....	10
Configuration State .....	10
Run State.....	10
NEW VPN INSTALLATION .....	11
BOOTSTRAP STATE.....	13
CONFIGURATION STATE.....	16
Import VPN Certificate (Trusted Root Certification Authorities).....	17
Enroll First Security Officer .....	17
Login to VPN.....	19
Enroll Second Security Officer and Administrators.....	21
Appendix A - Procedure to make USB drive bootable with Propalms ISO .....	22

## PROPALMS OS

Propalms OS is a Linux 2.6 kernel based hardened platform which hosts the required services for running Propalms VPN. Propalms OS is a customized Fedora 9 distribution and is maintained by Propalms Support Team.

When installed, Propalms OS has a small menu driven interface to manage host configuration like network settings modifications or reinstallation of firmware.

Propalms OS comes on an integrated installer CD or bootable USB drive. The integrated installer is a single click OS installer which also installs the VPN software.

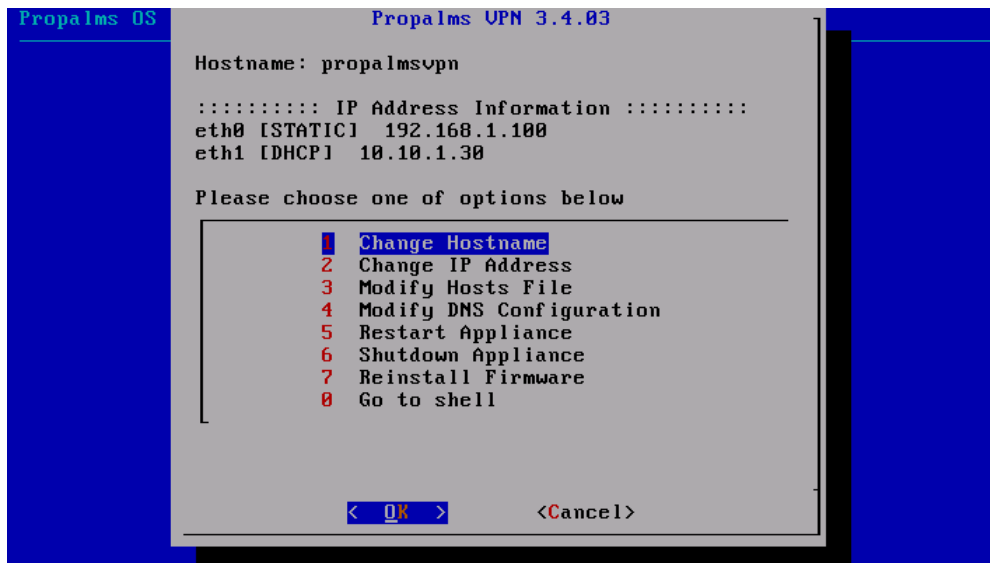
*NB: Installing the Propalms OS will erase all existing data off your system without asking about details of partition.*

### Steps for Installation of Propalms OS

1. Make your system's first bootable device USB or CD
2. Insert Propalms VPN OS installer CD / USB
3. The installer screen will appear. If you are installing through usb, type usb
4. Installation procedure starts. Next few steps will ask about OS language and keyboard layout
5. Installation will start automatically and will take up to 10-15 minutes to complete.
6. After completion of Installation, remove CD and restart the machine

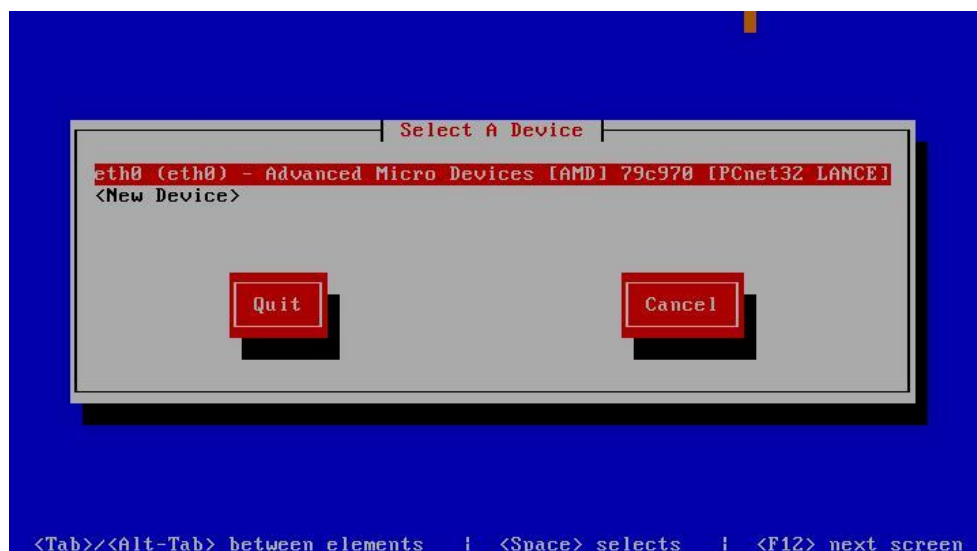
## Configuration of Propalms OS

After completion of successful installation and restart you will get a blue setup screen with following options:-



1. Change Hostname - Set Propalms VPN Server hostname  
*Important: Propalms VPN resolves requests only through hostname. VPN hostname should set before starting VPN configuration. If you are changing hostname after configuration of VPN box, this will affect your whole VPN set up and need to re-configure existing VPN setup.*
2. Change IP Address - Change IP Address and net mask of your VPN Server.

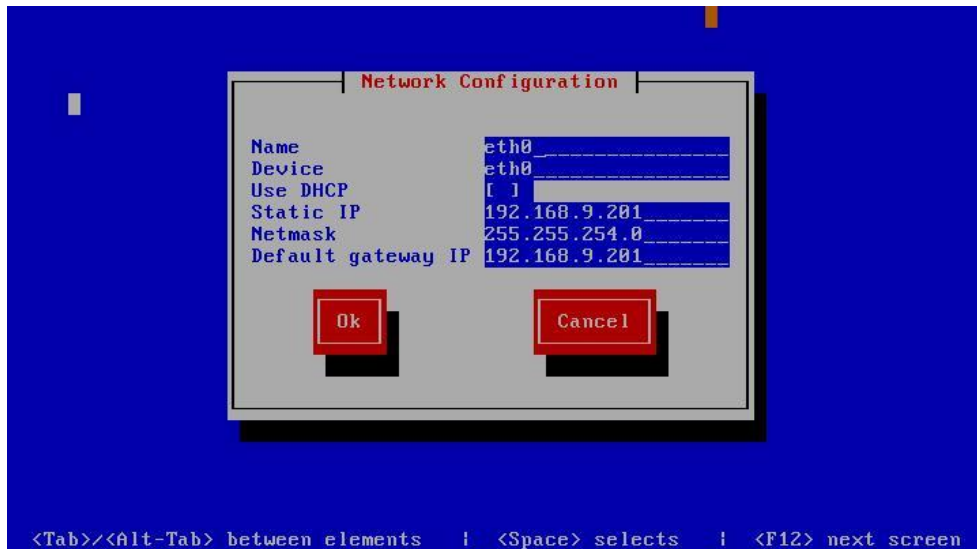
This will show available Ethernet cards in the system. We set default IP address 192.168.1.100. For changing this select the menu Item (use **UP** and **DOWN** arrow keys) and press **Enter**.



Enter new static IP, network mask address and gateway of the network.

*NB: Keeping VPN device with static IP is always a good practice*

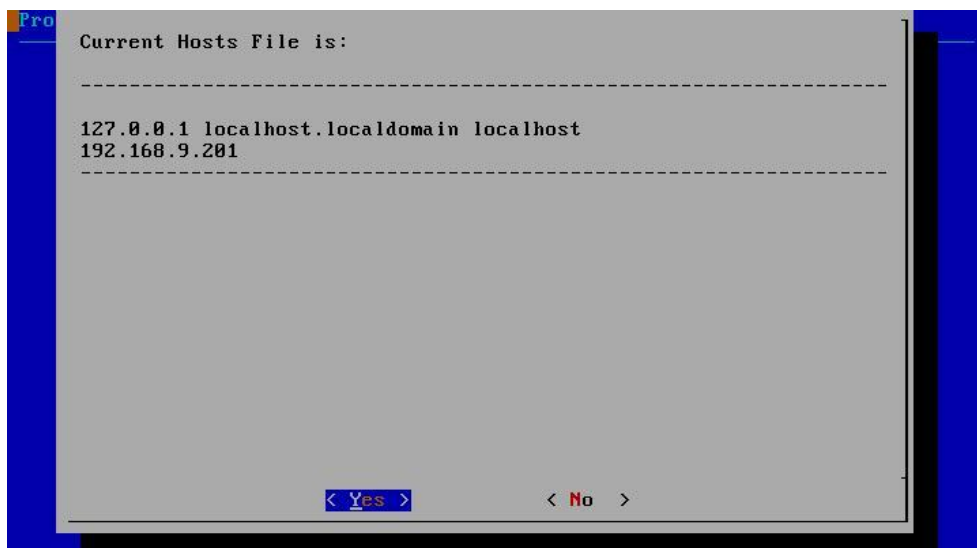
Navigate using arrow keys, select **OK** and press **Enter**. This will redirect you to previous menu (Network device). Select **quit** button and **Enter**. VPN network service will restart.

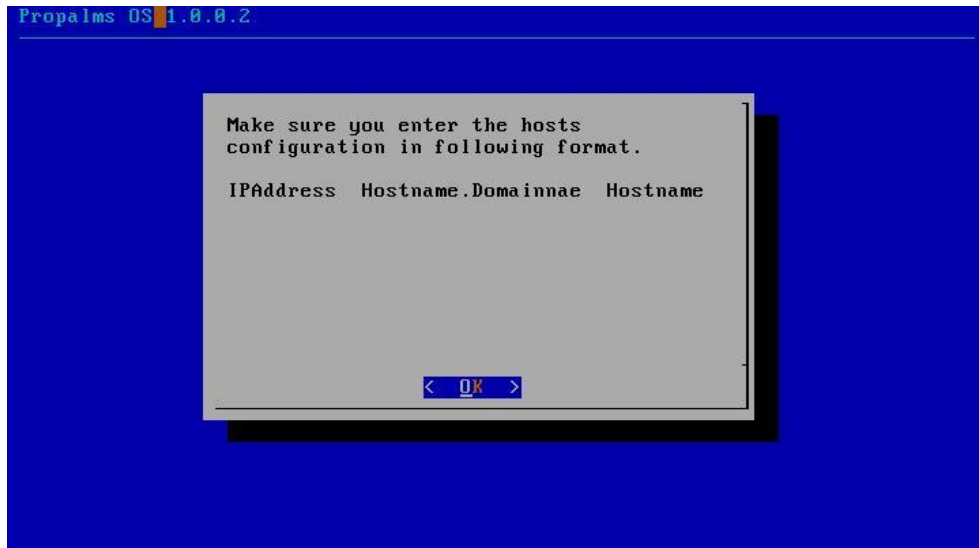


3. Modify Hosts File - Modify VPN Server local host file for name resolution in case a DNS server is not available

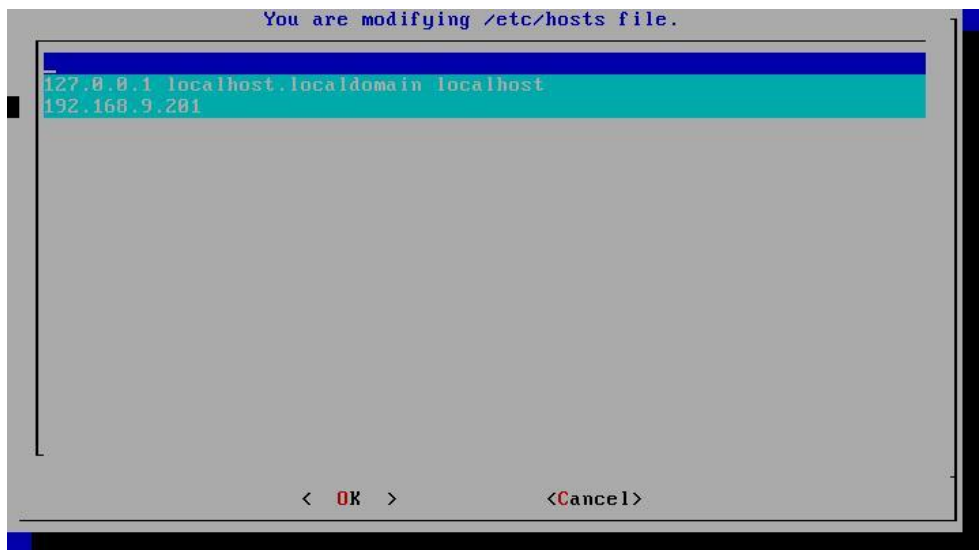
This menu will be useful sometimes for accessing VPN application through application name. For modifying VPN device host file entry, select option 3 Modify host file and press **Enter**.

Navigate using arrow keys then select **Yes** then **OK**





Edit host file and press **OK**.



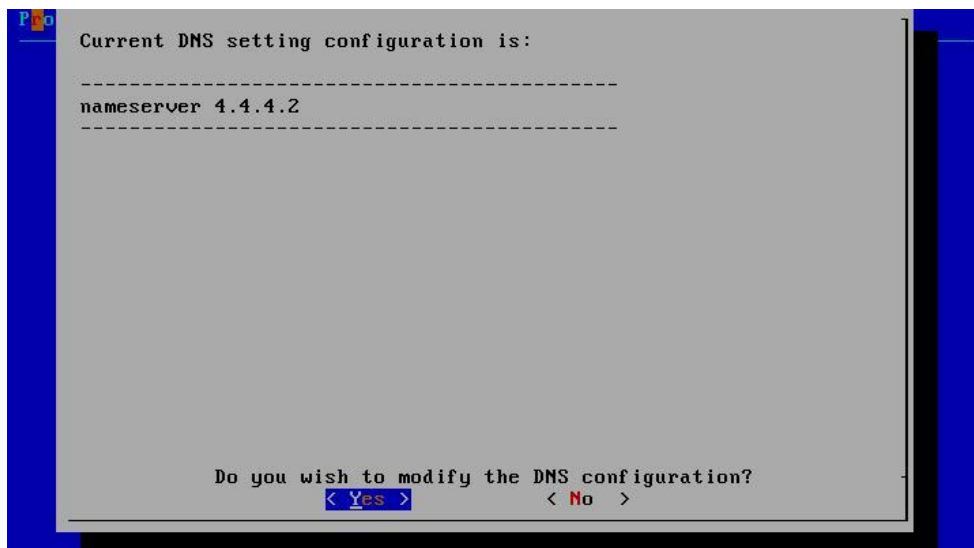
A confirmation window appears



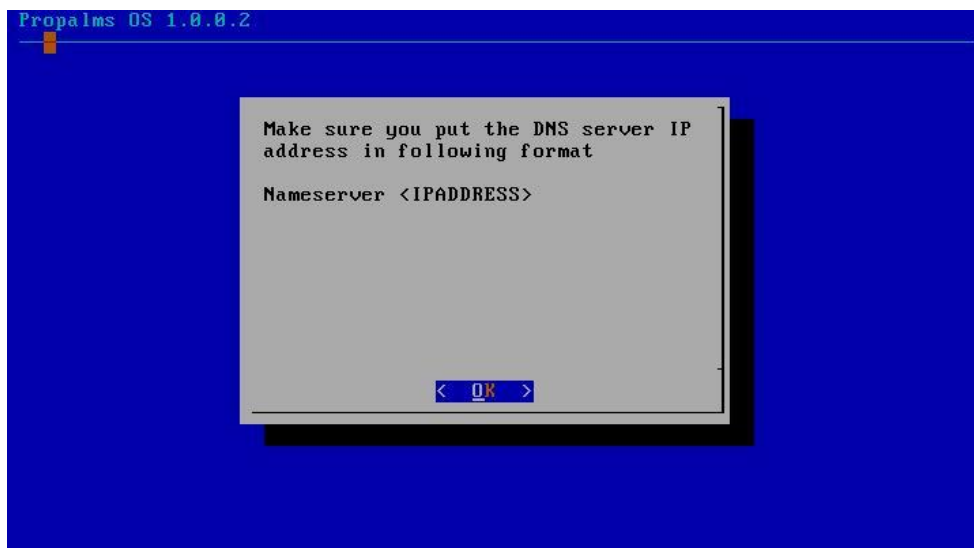
4. Modify DNS Configuration - Select the DNS Servers your Propalms VPN will use

Select Menu item and press **Enter**

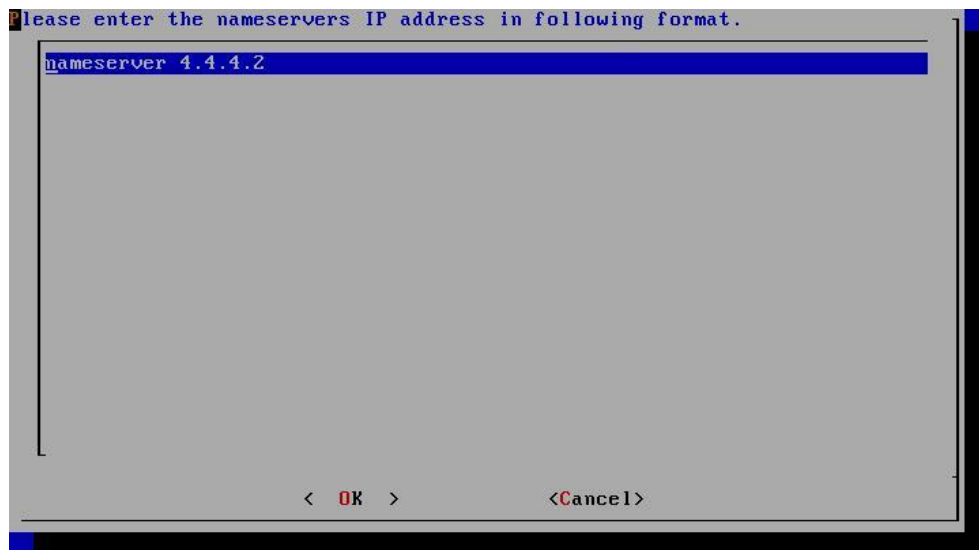
Select **Yes** button and press **Enter**. Information about DNS entry details will appear



Click **OK** to edit



Add your DNS Server details and click **OK**



A confirmation screen will appear



- 5. Restart Appliance - Choose this option to restart your Propalms VPN appliance
- 6. Shutdown Appliance - Choose this option to shutdown the Propalms VPN
- 7. Re-install Firmware - Allows to reinstall the VPN software on the appliance
- 0. Go to Shell - Go to Linux shell for advanced administration

## VPN STATES

The VPN service has three states:-

1. Boot strap
2. Configuration
3. Run

### Boot strap State

On a freshly installed VPN installation, the VPN service is in boot-strap state. During this stage, admin configures the system settings, including network, license and certificate settings.

During this stage first security office account is created.

### Configuration State

In this state, the VPN service is in configuration mode. VPN service will not accept connection from any user other than Security Officers and Administrators.

Once bootstrap state is complete, the VPN service automatically moves to Configuration state.

Administrators can bring the VPN service from run state to configuration state from administrator console for doing system wide changes.

### Run State

In this state, the VPN service is fully functional. No critical system wide changes can be performed on VPN system during run state.

VPN service does not move automatically from configuration state to run state after a fresh configuration. For VPN service to go from Configuration state to Run state, you should go to Server Configuration>Server State and switch to Run State.

## NEW VPN INSTALLATION

After a fresh installation of VPN OS and VPN service, the VPN service is running in boot strap mode. Follow these steps to complete bootstrap stage.

1. Launch the web browser and go to URL [http://vpn\\_gateway\\_ip\\_address/](http://vpn_gateway_ip_address/)
2. Click on link “**Administrator**” under section Management console
3. On the next page click on “**click here**” to go to pre-boot page to do network settings and license settings.
  - a. This will open the SYSTEM CONFIGURATION screen.

Network Configuration - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail Web Services Bluetooth

Address http://demo.propalmsvpn.com/fes-bin/preboot.cgi

propalms VPN  
Access Made Easy

Close Help Support

VPN Management Console

Propalms VPN: System Configuration

**Host Configuration**

Host name

Default Gateway

Primary DNS

Secondary DNS

**Interface Configuration**

Interface Name	IP Address	Subnet Mask	Gateway
eth0	<input type="text" value="192.168.9.201"/>	<input type="text" value="255.255.254.0"/>	<input type="text" value="NONE"/>

**Date and Time setting**

Date

Time

Time Zone

**Server License**

License Key

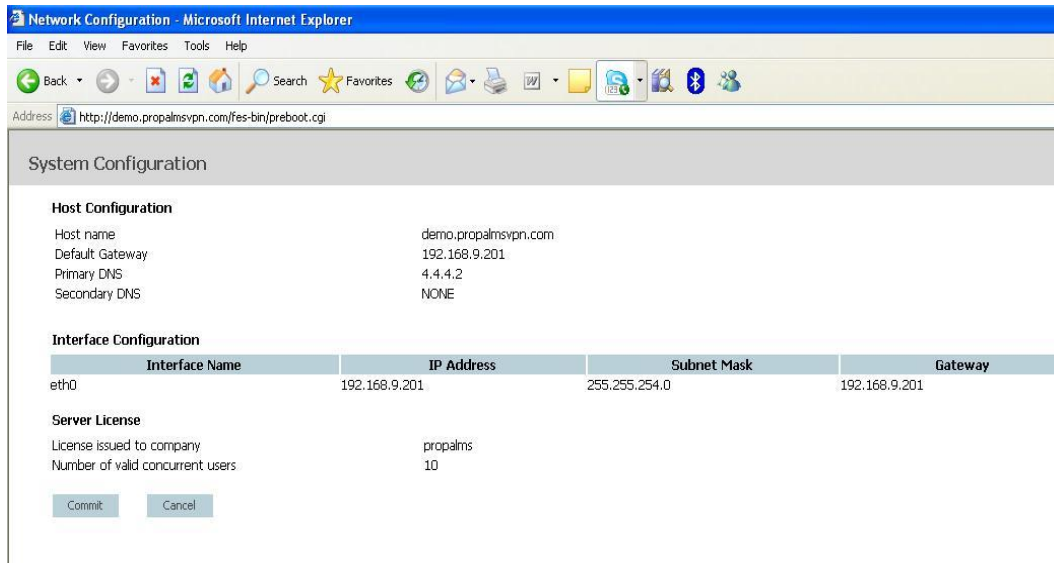
Company Name

4. In the Host Configuration section, enter the following information to configure the host settings.
  - a. Type the **server name** in the Host Name field.
  - b. Type the **default gateway** in the Default Gateway field.
  - c. Type the **primary DNS address** in the Primary DNS field.
  - d. Type the **secondary DNS address** in the Secondary DNS field.

5. In the Interface Configuration section, enter the following information to configure the interface settings.
  - a. The interface name will be displayed by default in the Interface Name field, based on the number of network cards in the system. For example, if there is only one network card in the system, the interface name will be displayed as “eth0”, if there are two network cards, the interface name will be displayed as “eth1” and so on.
  - b. Type the **IP address** in the IP Address field.
  - c. Type the **subnet mask** in the Subnet Mask field.
  - d. Type the **gateway** in the Gateway field.

*NB: If the IP address and gateway is set at the time of installation of Linux in the system before the VPN installation, these values will be displayed in the Host name, Default Gateway, Primary DNS, Secondary DNS, IP Address, Subnet Mask and Gateway fields by default. You can edit the values if required.*

6. In the Date and Time setting section, enter the following information to configure the date and time settings.
  - a. To set the date, click on the drop-down arrows and select the **Date, Month, and Year** from the list, corresponding to the Date field.
  - b. To set the time, click on the drop-down arrows and select the **Hours and Minutes** from the list, corresponding to the Time field.
  - c. Click on the drop-down arrow corresponding to the Time Zone field and select the applicable **time zone** from the list.
7. In the Server License section, enter the following information for license verification.
  - a. Type the **Propalms VPN license key** (received with the server box) in the License Key field.
  - b. Type your **company name** in the Company Name field.
8. Click **Submit** to save the configuration details or click reset to clear the fields.
9. On clicking the Submit button, the following confirmation screen appears, displaying the entered values.



10. Click **Commit** to save the details or click Cancel to change the System Configuration values.

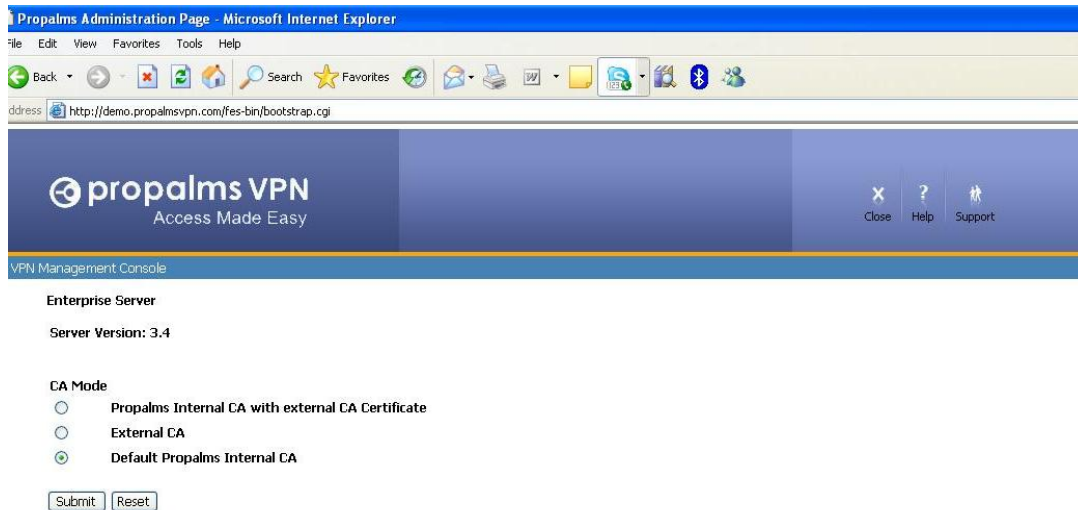
## BOOTSTRAP STATE

On completion of System Configuration, VPN moves into Bootstrap State, and is ready for a one-time registration process. In Bootstrap State, first Security Officer Registration, SMTP Server configuration, Database User configuration, and several others tasks are completed, including:

- Register first Security Officer
- Create Root Certificate Authority (CA) Certificate
- Register SSL Certificate for VPN
- Create Signer Certificate
- Create Verifier Certificate
- Create VPN database and database tables
- Register VPN Ports and Apache Ports (port 80/443, 4001, and 4002)
- Create Configuration files
- Enter Configuration State (this change occurs automatically after the Bootstrap process is complete)

The tasks such as creating CA certificate, Signer Certificate, Verifier Certificate, and many others take place internally when you register the necessary details with VPN during server Bootstrap.

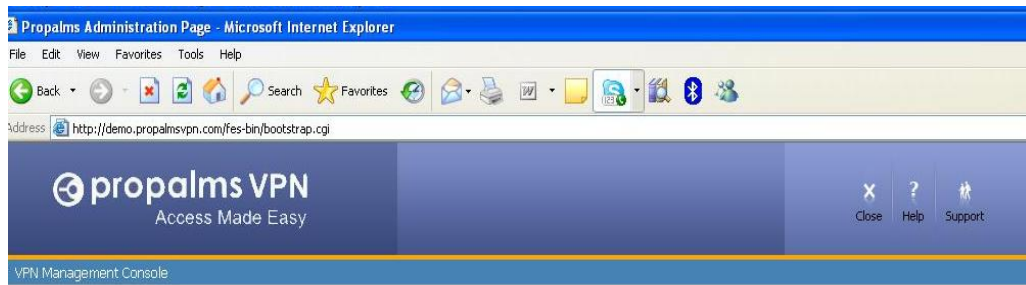
After the details have been saved, a redirection screen will appear which redirects you to the Enterprise Server screen.



In the CA Mode section, the Default Internal CA field is chosen by default. This enables the VPN internal Certificate Authority and the VPN server becomes the Certificate Authority.

Click the **Submit** button to save the changes made and click Reset to cancel the changes made to the page.

On clicking the Submit button, the Bootstrap page appears as shown below.



Certificate Authority Information

Company Name

Country

State

City

Validity (days)

Security Officer Account

Name

Email

User ID

Password

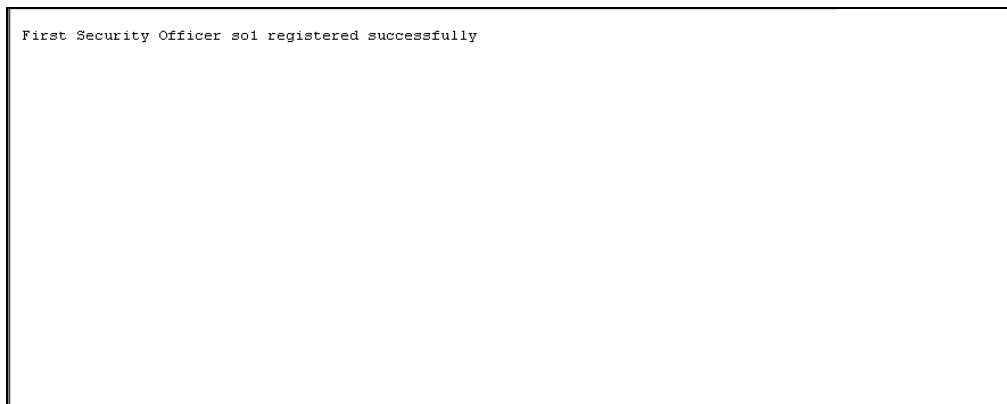
Biometric data required

SMTP Server

SMTP Port

Click **Submit** to register the data, or click Reset to clear all data from this screen.

After clicking the Submit button, the following screen confirming the registration will appear.



*NB: If the message given in the above screen does not appear, please check your Bootstrap registration data carefully.*

VPN Server emails Root Certificate (cacert.cer) and a Passphrase to the first Security Officer's e-mail address.

*Important: The first Security Officer must download the Root Certificate and import it to the browser in the list of Trusted Root Certification Authorities.*

FIELD	VALUE	DESCRIPTION
<b>Certificate Authority Information</b>		
Company Name	<Company Name>	Name of the company to which Certificate will be issued.
Country	<Country Name>	Name of the country where Certificate will be issued.
State	<State Name>	Name of the state where Certificate will be issued.
City	<City Name>	Name of the city where Certificate will be issued.
Validity (days)	<No. of Days>	Validity period for the Certificate.
<b>Security Officer Account</b>		
Name	< First Security Officer Name>	Full name of First Security Officer.
Email	<Username@domain name>	Email ID of First Security Officer.
User ID	<User Name>	Basic Authentication Login ID for First Security Officer.
Password	<Password>	Password for this account.
Biometric data required		Check this field to enable biometric authentication for the First Security Officer.
SMTP server	<SMTP Server Name>	SMTP server address to route emails generated by VPN. It should be FQDN.
SMTP port	25	Port number on which SMTP service is configured to listen.

## CONFIGURATION STATE

Upon successful completion of Bootstrap State, VPN automatically moves into Configuration State. The following tasks are completed in Configuration State:

- Enroll First Security Officer
- Move VPN from Configuration State to Run State

*NB: User Registration and User Enrollment are two different processes. During the User Registration process, the User Name and User E-mail Address are registered with VPN and a Passphrase is generated. During the User Enrollment process, the Passphrase and a Password, supplied by the User, are registered with VPN, and a user Certificate file (.cer) is generated.*

Applications can be added to the server when VPN is in Configuration State. However, users cannot access applications until VPN is in Run State.

VPN sends an email to the first Security Officer account, as registered on the Enterprise Server page, containing a Root Certificate, Passphrase, and a link to the VPN home page. The Security Officer must save the Root Certificate file (cacert.cer) in a local folder and import it to the list of Trusted Root Certification Authorities in the browser.

## Import VPN Certificate (Trusted Root Certification Authorities)

The Root Certificate (cacert.cer) file can be downloaded by either of the two methods:

1. Download and open the file included in the e-mail , or
2. Launch your web browser and type the URL <http://<IP address of VPN>> to access the VPN landing page.  
Click **Server Certificate** from the 'To Download' section of the VPN page and open the root certificate.

Click "**Install Certificate**" Button and follow instructions making sure to install the Certificate in "**Trusted root Certificate**" store location.

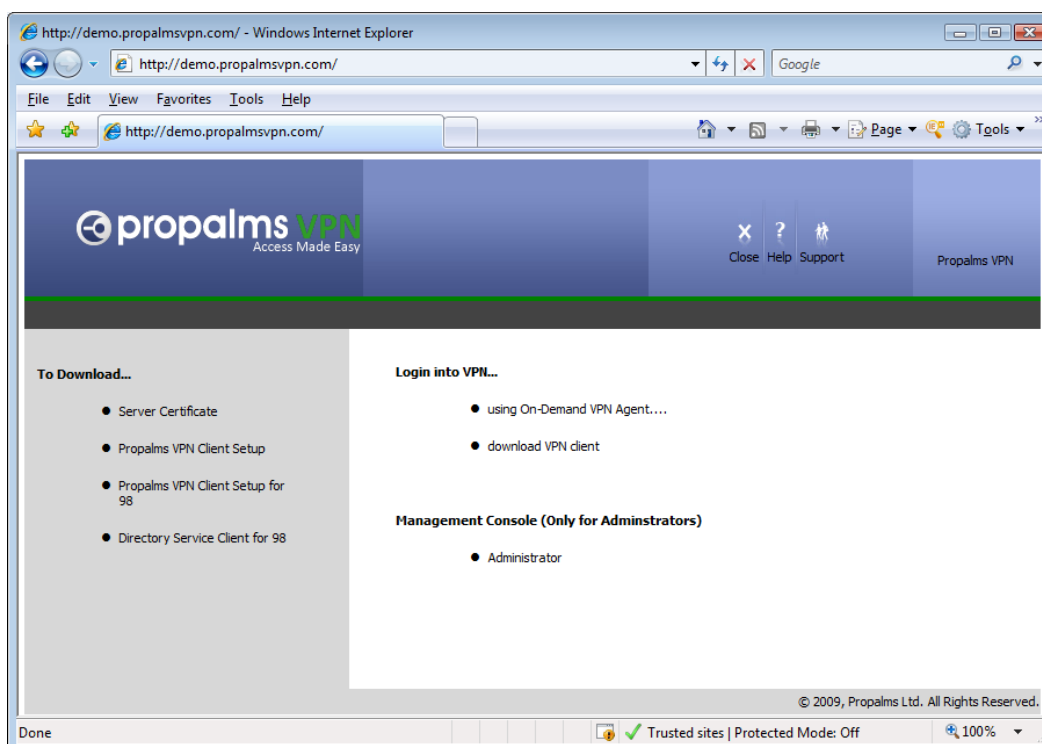
If the Certificate is properly installed, you can see installed Certificate in the Trusted Root Certification Authorities list in IE. To view go to Tools menu, click Internet Options. Click on the Content tab, click Certificates, and then click on the Trusted Root Certification Authorities tab.

## Enroll First Security Officer

The first Security Officer, whom you registered in the VPN Bootstrap State section earlier, must now be enrolled using the Passphrase available in the e-mail generated automatically and sent to the first Security Officer account. The password required must be supplied by the first Security Officer. When the Security Officer is successfully enrolled, a user Certificate is imported to the local personal certificate store.

1. Open your web browser and browse to <http://<IP address of VPN>>

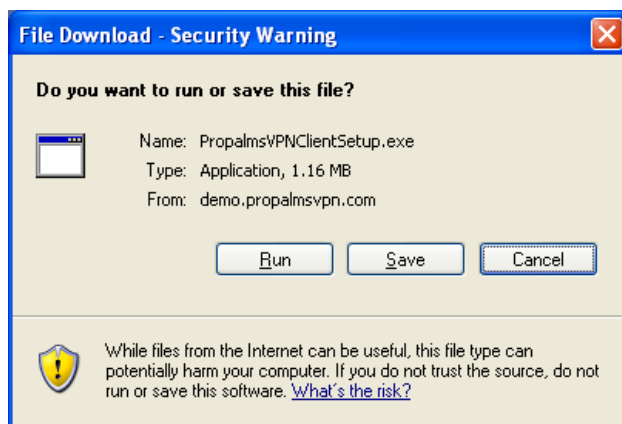
The following landing page should open...



2. In order to enroll a user you must install the VPN client.

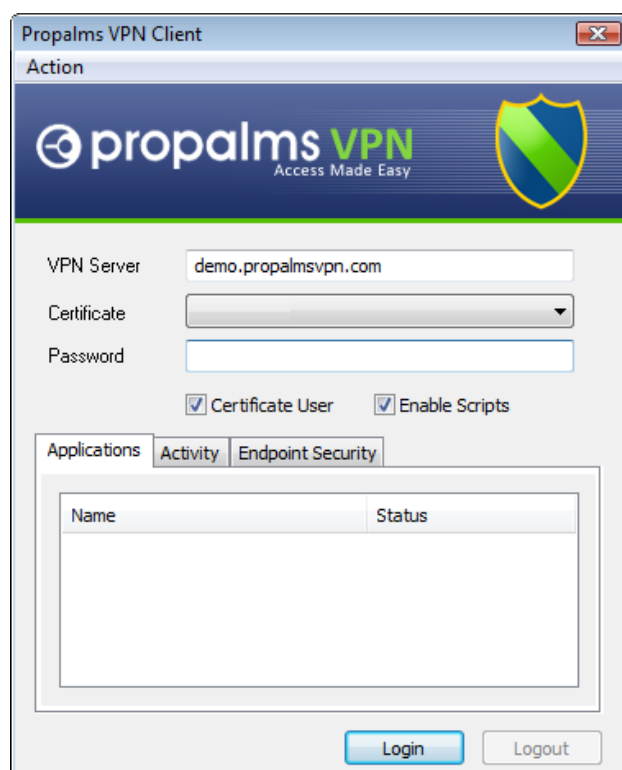
To download and install the VPN client, click on the link “**download VPN Client**” from the right side screen or click on “**Propalms VPN Client Setup**” link in the left side panel.

Click “**Run**” on the following screen and complete the installation of client.

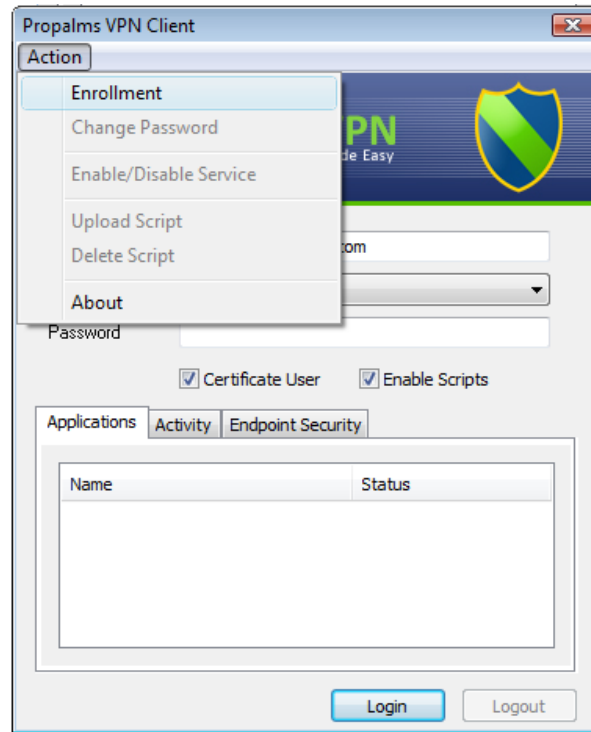


3. Double click the desktop icon for **Propalms VPN Client** and start the client.

In the Server box type the **name of your VPN server** and choose “**Certificate User**”



4. On the Action menu choose **Enrollment**.

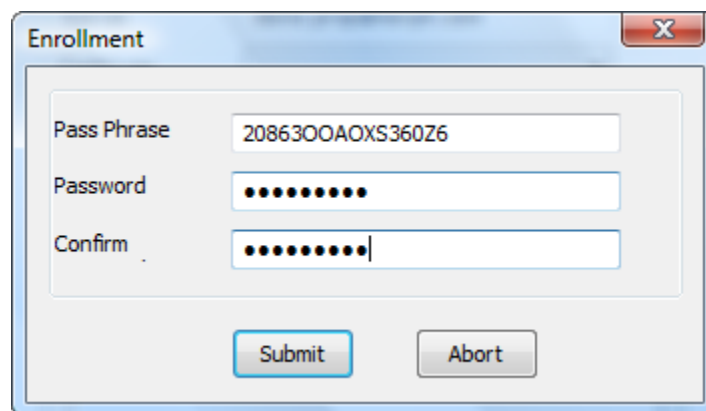


5. In the Pass Phrase field, type the **Passphrase** you received in the e-mail (if you prefer copy and paste the Passphrase from the e-mail to this field).

In the **Password** field, type the password you set for the first Security Officer Account

In the **Confirm Password** field, retype the password for confirmation.

Click on **Submit** to submit the enrollment information and click on **Abort** to exit from this screen without saving the changes.



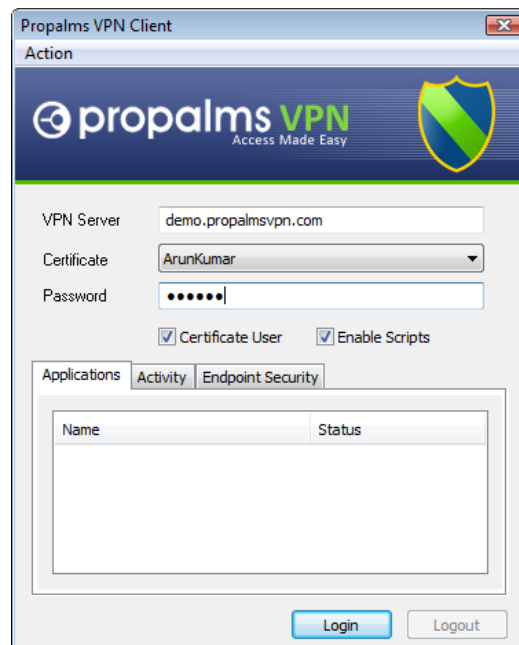
## Login to VPN

Propalms VPN supports two types of Authentication Mechanisms to access services over the network:

- Basic Authentication: This is a weaker authentication mechanism. Users log on using User ID and Password. The Low Security Users are authenticated with this mechanism.
- Certificate Authentication: This is a stronger authentication mechanism. Users log on with Certificate and Password. Security officers and Administrators are also authenticated with this mechanism.

To login as a Security Officer, choose “**Certificate User**” and use the dropdown list under certificates to choose the certificate imported during the Enrollment phase.

Type the **password** for the first Security Officer Account and click **login**.



The details of the applications and the activities available for this certificate user will be displayed in the **Applications** and **Activity** tab screens respectively, and the VPN moves to the systray as an icon.



You can now access the VPN Management Console by browsing to <http://<IP address of VPN>>

Choose the “**Administrator**” link under Management Console to administer the VPN.

## **Enroll Second Security Officer and Administrators**

After the first Security Officer is successfully enrolled, he or she can register the second Security Officer and any Administrator accounts.

Once registered, the second Security Officer and the Administrators must enroll themselves, following the steps above, substituting the second Security Officer and Administrator data accordingly.

***Important: Please read the Propalms VPN Administrator Guide for more information on VPN Management***

## Appendix A - Procedure to make USB drive bootable with Propalms ISO

*NB: If your installation media is CD drive, please ignore following steps*

1. Connect the USB drive to Linux system and format it with following command. Make sure you modify the device accordingly.

```
mkfs.vfat /dev/sdb1
```

2. Make the USB bootable with the Propalms ISO build.

```
livecd-iso-to-disk --noverify --reset-mbr <path to iso>/PropalmsVPN-1.0.0.2.iso /dev/sdb1
```

If it fails with parted error, run following commands to write the mbr of USB drive.

```
parted /dev/sdb [replace the device accordingly]
```

```
toggle 1 boot
```

```
quit
```

3. Mount the USB drive.

```
mount /dev/sdb1 /mnt/disk
```

4. Copy the ISO to USB drive.

```
cp <path to iso>/PropalmsVPN-1.0.0.2.iso /mnt/disk
```



Propalms, Inc. is a leading global provider of application delivery solutions for Terminal Services and Virtual Desktop Infrastructures. Delivering to Enterprises of all sizes we offer reliable, scalable and affordable solutions that simply work. Our belief is that application delivery solutions should be flexible, dynamic and above all, simple to use.