

# PROPALMS VPN

---



## Quick Start Guide

---

**Version 3.5**

Rev.06

Last Updated 23-MAR-2010



©1999-2010 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

CONTENTS .....	3
PROPALMS VPN INSTALLATION .....	5
Propalms OS .....	5
Propalms VPN Virtual Appliance .....	5
Steps for Installation of Propalms OS .....	6
Configuration of Propalms OS.....	6
Network Configuration .....	7
System Configuration .....	9
Propalms Administration .....	11
Other Console Options .....	11
PROPALMS VPN CONFIGURATION .....	13
VPN Service States .....	13
Boot strap State .....	13
Configuration State .....	13
Run State.....	13
New VPN Installation.....	14
Bootstrap State .....	14
Configuration State .....	20
Import VPN Certificate (Trusted Root Certification Authorities).....	20
Enroll First Security Officer .....	20
Login to VPN .....	22
Change Password .....	23
Enroll Second Security Officer and Administrators .....	24
APPENDICES.....	25
Appendix A - Procedure to make USB drive bootable with Propalms ISO .....	25
Appendix B - Supported Applications.....	25
Single sign-on for Propalms TSE.....	25

Feature Details .....	25
Other Application Configuration.....	26

# CHAPTER 1

## PROPALMS VPN INSTALLATION

### 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 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.

It is available as a single click integrated installer CD which installs both Propalms OS and Propalms VPN on any custom hardware. The VPN CD installer ISO can be downloaded from Propalms Website (<http://www.propalms.com>).

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

Propalms VPN is available as a virtual appliance as well as a software only VPN.

### PROPALMS VPN VIRTUAL APPLIANCE

Propalms VPN is available as a VMware Virtual Appliance that can be run on VMware Player, VMware WorkStation, VMware Server and VMware ESX/ESXi Servers. The Virtual Appliance is downloadable from Propalms Website (<http://www.propalms.com>). Simply extract the image file and import directly into your VMware environment and you are ready to go.

All the functionalities of the virtual appliance are the same as the software version.

---

## STEPS FOR INSTALLATION OF PROPALMS OS

```
=====
WELCOME TO PROPALMS OS 3.5.0.6 INSTALLATION

[Warning]
THIS CDROM/USB WILL FORMAT ALL DATA ON YOUR HARD DRIVE AND INSTALL PROPALMS OS.

Installation over serial console
-----
To install using a CDROM, enter following command and press enter key:
cdrom console=ttyS0,<baudrate>
To install using bootable USB, enter following command and press enter key:
usb console=ttyS0,<baudrate>

(Baudrate depends upon bios configuration. (2400 to 921600))
Note: If you are installing from a USB drive; Make sure USB drive is detected
      as sdb i.e. plug the drive in first USB port.

Installation over connected monitor
-----
To install using a CDROM, just press "enter" key to start installation.
To install using a USB drive, enter "usb" and press "enter" key.

Default timeout is 60 seconds after which CDROM installation is started.
=====
boot: _
```

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 approximately 10 minutes to complete, depending on hardware.
6. After completion of Installation, remove CD and restart the machine

---

## CONFIGURATION OF PROPALMS OS

After completion of installation and restart you will get a prompt to login to gain access to the Propalms OS Console menu. The account name is 'consoleadmin'. The default password for the account is 'adminconsole'. The administrator has option to change the password for consoleadmin user. Root access to Propalms OS is blocked completely. Once authenticated you will see the following Propalms OS Console screen:

```

-----
Propalms OS 3.5.0.6
Propalms UPN 3.5.0.6
-----
Hostname: propalmsvpn
-----
Ethernet Devices:
eth0 [STATIC]          192.168.1.100
eth1 [DHCP]            10.10.1.34
-----

1) Network Configuration
2) System Configuration
3) Propalms Administration
4) Restart Appliance
5) Shutdown Appliance
0) Go to Shell

Select one of options above (Numerics only): _

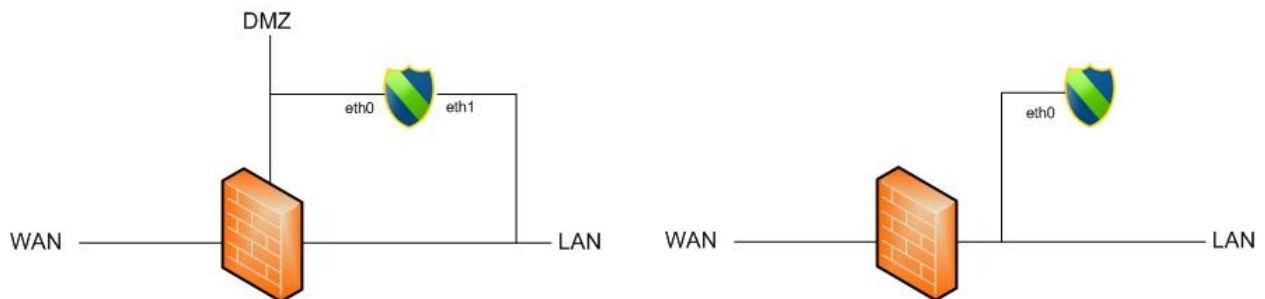
```

Choose a number for the configuration option you require and then type your console administrator password. (Default password is 'adminconsole')

## NETWORK CONFIGURATION

In this screen you can configure the Ethernet devices for your system. Choose option **1** to configure Ethernet interfaces or **2** to restart the network. Type **R** to return to the previous menu options.

The most common configuration scenarios for Propalms VPN are shown below. Depending on your chosen network configuration you will need to setup your network interfaces to suit.



```

-----
NETWORK CONFIGURATION
-----
Ethernet Devices:
eth0 [STATIC]          192.168.1.100
eth1 [DHCP]            10.10.1.34
-----

1) Configure Ethernet Device
2) Restart Network
R) Return to main menu

Select one of options above: _

```

*NB: Propalms VPN installs with a default static IP address of 192.168.1.100.*

*The VPN virtual appliance ships with 2 Ethernet interfaces as standard setting the second NIC as DHCP enabled.*

In the Ethernet configuration screen, select the number of the NIC you wish to configure.

For example:

To configure the **eth1** interface in the screen below simply type **1** then hit return.

```
-----  
ETHERNET CONFIGURATION  
-----  
Following Ethernet devices found on the system.  
eth0   [STATIC]      192.168.1.100  
eth1   [DHCP]       10.10.1.34  
-----  
Enter the device number to configure it (R to return): _
```

Select **1** to manually configure NIC or **2** to configure DHCP option.

```
-----  
ETH1 CONFIGURATION  
-----  
ETH1 DETAILS:  
PROTOCOL: DHCP  
IPADDR: 10.10.1.34  
NETMASK: 255.255.255.0  
  
DEFAULT GATEWAY: 10.10.1.254  
-----  
  
1) Manually configure ETH1  
2) Configure DHCP for ETH1  
R) Return to previous menu  
  
Select one of options above: _
```

Enter the relevant IP information when prompted and choose **y** to apply the configuration. The network service will restart and you will be prompted to press a key to continue when it is finished.

```
-----
                        ETH1 CONFIGURATION
-----
ETH1 DETAILS:

PROTOCOL: DHCP
IPADDR: 10.10.1.34
NETMASK: 255.255.255.0

DEFAULT GATEWAY: 10.10.1.254

-----

                        1) Manually configure ETH1
                        2) Configure DHCP for ETH1
                        R) Return to previous menu

Select one of options above: 1
eth1 ifcfg-eth1

Enter IP address: 10.10.1.100
Enter Netmask: 255.255.0.0
Enter Gateway: 10.10.1.254
Save and apply this configuration? (Y/N): _
```

*NB: Configuring VPN with static IP is always good practice.*

---

## SYSTEM CONFIGURATION

In this screen the administrator can configure the VPN hostname and name resolution configuration.

```
-----
                        SYSTEM CONFIGURATION
-----
Hostname: propalmsvpn
-----

                        1) Set Hostname
                        2) Manage Hosts File
                        3) Configure DNS
                        R) Return to main menu

Select one of options above: _
```

### 1. Set Hostname

Set Propalms VPN Server hostname. To configure the hostname choose option **1** then type the fully qualified domain name that users will use to access this VPN server and press **Enter**. Press any key to continue.

*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. Manage Hosts File

Modify VPN Server local host file for name resolution in case a DNS Server is not available. Type **2** to manage hosts file, then **1** to Add hosts entry or **2** to remove hosts entry.

```
-----
                        HOSTS CONFIGURATION
-----
Current HOSTS FILE:

# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1                propalmsvnpn localhost.localdomain
::1                    localhost6.localdomain6 localhost6
-----

1) Add Hosts
2) Remove Hosts
R) Return to previous menu

Select one of options above: _
```

Enter the **IP Address** <space> **FQDN** <space> **Hostname** and press **Enter**. Type **y** to confirm.

```
Select one of options above: 1
<IP>    <FQDN>  <HOSTNAME>
Enter Hosts entry in above format (R to return): 10.10.1.100 webvnpn.propalms.com
webvnpn_
```

To remove Host entries simply type the line number you wish to delete and confirm.

### 3. Configure DNS

If your DNS servers have not been picked up by DHCP you can add them here. Type **1** to Add DNS server and **2** to delete a DNS server. To add type the **IP address** of the DNS server and press **Enter**. To remove a DNS server, choose the line number for the DNS server entry you wish to remove and press **Enter**.

```
-----
                        DNS CONFIGURATION
-----
Current DNS Configuration:

-----

1) Add DNS Servers
2) Remove DNS Server
R) Return to previous menu

Select one of options above: _
```

---

## PROPALMS ADMINISTRATION

In this section the administrator can perform certain system/account recovery options for Propalms VPN.

```
-----  
PROPALMS ADMINISTRATION  
-----  
1) Reset Administrator Account  
2) Change Console Administration Password  
3) Reinstall Firmware  
R) Return to main menu  
  
Select one of options above: _
```

### 1. Reset Administrator Account

This feature resets the Security Officer / Administrators certificate on VPN management console and sends a new passphrase to the registered email ID of the account. This feature can be used in case where administrator certificate is lost or a user forgets their password.

### 2. Change Console Administration Password

Propalms VPN ships with a default console account of 'consoleadmin' and password 'adminconsole'. The administrator is strongly advised to change this generic password to something secure.

### 3. Re-install Firmware

Choose this option to reset your Propalms VPN installation to factory defaults.

---

## OTHER CONSOLE OPTIONS

### 4. Restart Appliance

Choose this option to restart the Propalms VPN server.

### 5. Shutdown Appliance

Choose this option to shutdown the Propalms VPN server.

### 0. Go to Shell

Go to Linux shell for advanced administration or troubleshooting.

*Important: Propalms VPN does not require the administrator to have root access to the underlying operating system. All installation and configuration can be performed using both the Propalms OS Console (shown above) or through the web based management console. Propalms Support team may require shell access for advanced troubleshooting but this is not common.*



# CHAPTER 2

## PROPALMS VPN CONFIGURATION

### VPN SERVICE 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 System Configuration state, also known as boot-strap state. During this stage, admin configures the system settings, including network, license and certificate settings.

During this stage the first security officer account is created.

---

#### CONFIGURATION STATE

In this state, the VPN service is in configuration mode. VPN service will not accept connections 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.

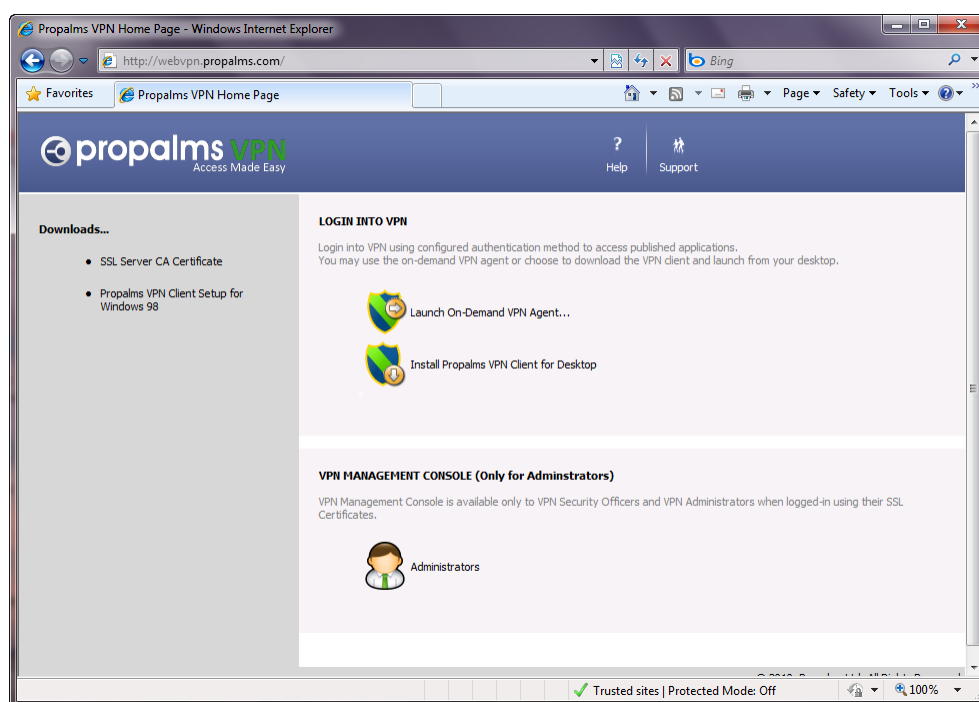
VPN service does not move automatically from configuration state to run state after a fresh configuration. For VPN service to go from Configuration state to Run state, you should go to VPN Status > VPN Server State page in the management console and switch to Run State.

## NEW VPN INSTALLATION

### BOOTSTRAP STATE

After a new installation of Propalms VPN, the VPN service is running in bootstrap mode. The first screen you see in this mode is the System Configuration page where you can configure network and license settings. 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/) or [http://<vpn\\_hostname>/](http://<vpn_hostname>/)
2. Click on link **Administrators** link under section VPN Management console



3. Read and click the box to accept the Software License Agreement.
4. The Propalms VPN – System Configuration screen appears where you can specify network and license settings.
5. 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.

**Propalms VPN: System Configuration**

**Host Configuration**

Host name:  Please enter proper hostname. You'll not be able to edit after the installation.

Default Gateway:

Primary DNS:

Secondary DNS:

**Interface Configuration**

Interface Name	IP Address	Subnet Mask	Gateway
eth0	<input type="text" value="192.168.1.100"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="NONE"/>
eth1	<input type="text" value="10.10.1.34"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="10.10.1.254"/>

**Date and Time settings**

Date:   2010

Time:

Time Zone:

**VPN License**

Company Name:

Use System Default License Provides evaluation license for 5 concurrent users for 30 days

Use New License Key

© 2010, Propalms Ltd. All Rights Reserved.

Trusted sites | Protected Mode: Off | 100%

6. 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.*

7. 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.

## 8. Configure VPN License

**VPN License**

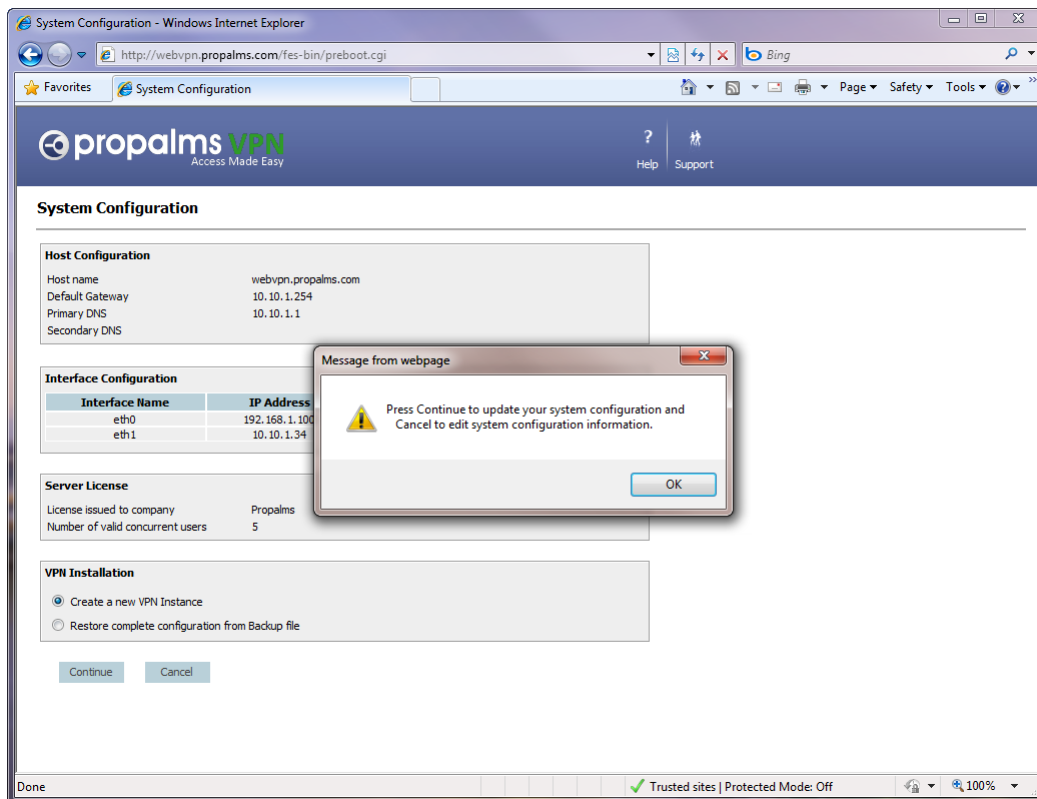
Company Name

Use System Default License Provides evaluation license for 5 concurrent users for 30 days

Use New License Key If you need a New License Key, please send this Product ID '3428650928985632' to [info@propalms.com](mailto:info@propalms.com)

-----

- a. Type your **company name** in the Company Name field.
  - b. Use System Default License. This is an evaluation license which allows 5 users for 30 days.
  - c. Use New License Key. Choose this option if you have purchased a license for your VPN Server. You are required to email the generated product ID to [info@propalms.com](mailto:info@propalms.com) in order to receive your license key.
9. Click **Submit** to save the configuration details or click cancel to go back.
10. On clicking the Submit button, the following confirmation screen appears, displaying the entered values.



11. At this stage you can either **Create a New VPN Instance** for when you are installing a new VPN server or if you have a previous system backup from which you wish to recover then select **Restore complete configuration from Backup file** then Click **Continue**.

On completion of System Configuration, the VPN continues through Bootstrap stage, 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.

1. Once all of the internal tasks have been completed you will be redirected to the Certificate Authority screen.



2. In the Certificate Authority Mode section, the **Default Propalms Internal CA** field is chosen by default. This enables the VPN internal Certificate Authority and the VPN server becomes the Certificate Authority. Choose **External CA** if you wish to use a 3<sup>rd</sup> Party Certificate Authority.
3. Click the **Submit** button to save the changes made. On clicking the Submit button, the Certificate Authority page appears as shown below depending on which option you selected.

### Certificate Authority Information

Accepted Certificate Formats : RSA

CA Certificate	<input type="text"/>	<input type="button" value="Browse..."/>
CA Private Key	<input type="text"/>	<input type="button" value="Browse..."/>
CA Private Key Password	<input type="text"/>	

- a. For External CA provide CA Certificate path, CA Private Key path and CA Private Key Password.
- b. For Propalms Internal CA fill out the required fields

### Certificate Authority Information

Company Name	<input type="text"/>
Country	<input type="text" value="Select Country"/>
State	<input type="text"/>
City	<input type="text"/>
Validity (days)	<input type="text"/>

### Security Officer Account

Name	<input type="text"/>
Email	<input type="text"/>
User ID	<input type="text"/>
Password	<input type="text"/>

Please specify an SMTP server that accepts anonymous email forwarding.  
If you are not sure please keep the default settings as shown below.  
The Passphrase information will be displayed on the screen also.

SMTP Server	<input type="text" value="127.0.0.1"/>
SMTP Port	<input type="text" value="25"/>

4. You also need to create the Security Officer account on the VPN. This account provides administrator access to the VPN management console where further accounts can be created. See table below for description of each field.

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>	Temporary password for this account. Security Officer will specify their own password on enrollment.
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.

5. On clicking the Submit button, the following screen confirming the registration will appear after a short while. Propalms VPN Server emails Root Certificate (cacert.cer) and a Passphrase to the first Security Officer's e-mail address. You can also copy the passphrase from the registration screen shown below.



First Security Officer Sec1 registered successfully.  
The Passphrase is **38U9G3FC3G125UJ8**

Please follow these steps:

1. Download the Propalms VPN Client from VPN home page.
2. Enroll yourself with the help of the Passphrase provided above.
3. Login into Propalms VPN.
4. Open the VPN Management Console.
5. Change the VPN server state to "RUN" mode at 'Server Configuration' -> 'Server State'.

---

## 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 can 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 to avoid seeing warnings when authenticating.

---

## 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://<vpn\\_hostname>/](http://<vpn_hostname>/) 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.

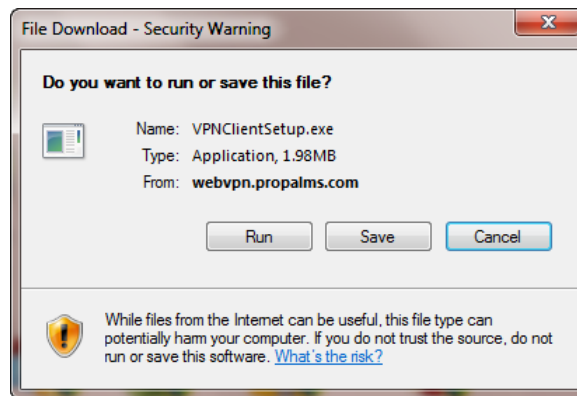
1. Open your web browser and browse to [http://<vpn\\_hostname>](http://<vpn_hostname>/)

2. In order to enroll a user you must install the VPN client or login using the 'On-Demand VPN Agent' (Clientless ActiveX control).

To download and install the VPN client, click on the link **"Install Propalms VPN client for desktop"**. You will need to download and run the Windows Client to login using certificate based authentication for Administrator access.

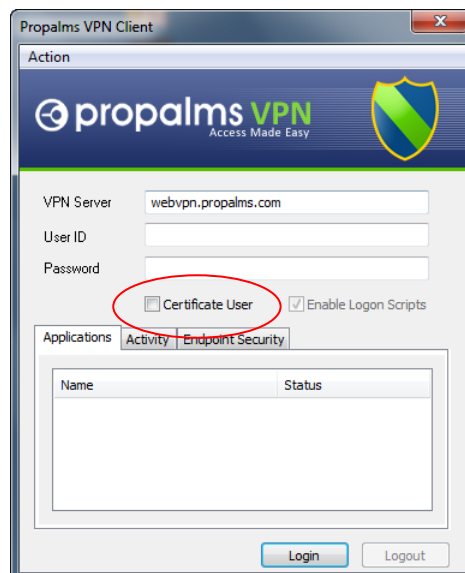


Click **"Run"** on the following screen and complete the installation of client.

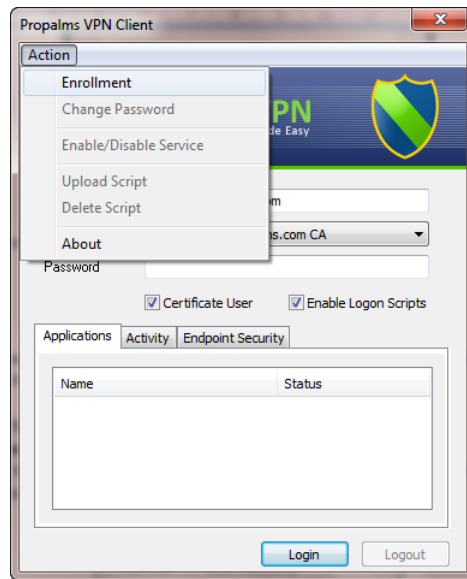


3. Double click the desktop icon for **Propalms VPN Client** and start the client. In the Server box type the **name of your VPN server** and choose **"Certificate User"**.

If you are using the 'On-demand VPN agent' the server value does not appear.



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

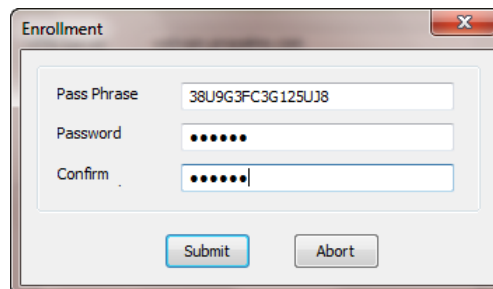


5. In the Pass Phrase field, type the **Passphrase** you received in the e-mail (if you prefer copy and paste the Passphrase from the e-mail to this field).

In the **Password** field, type a password for your 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.



*NB: you may see a security warning if you are you using the Internal CA and have not imported the Root Certificate into the Trusted Root Certificate store on this machine. You can proceed and login without doing this.*

---

## LOGIN TO VPN

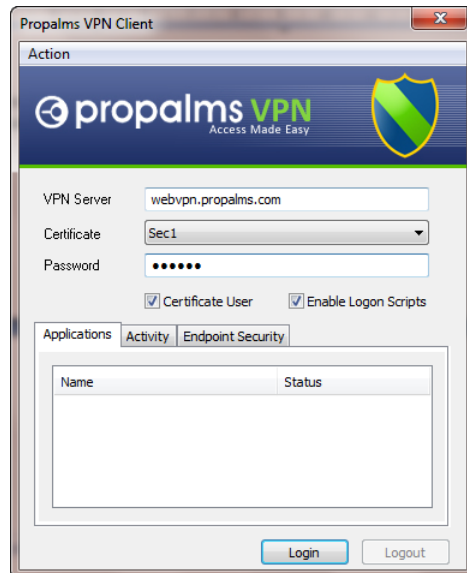
Propalms VPN supports two types of Authentication Mechanisms to access services over the network:

- **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 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 system tray as an icon.



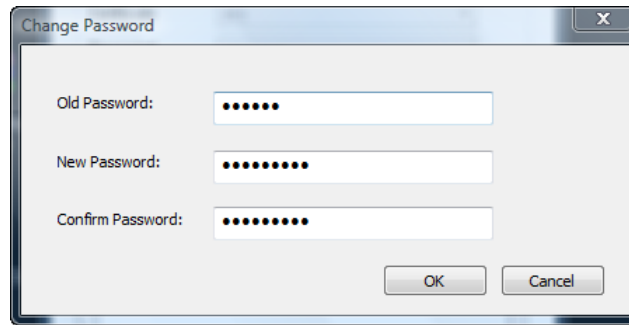
## CHANGE PASSWORD

You are recommended to change your password.

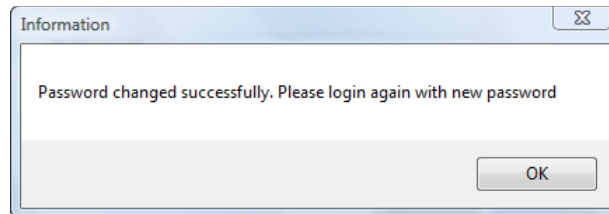
Your password must be between six and 15 characters long and can contain alphanumerical characters

You can change password expiry settings from Administrator portal. (For more details Please refer “User management” chapter)

Return to the VPN login screen. On the Action menu, click Change Password. The Change Password screen appears.



Click on OK to save the changes made and click cancel to exit the screen without making any changes in the password. The following screen will appear after you have changed the password.

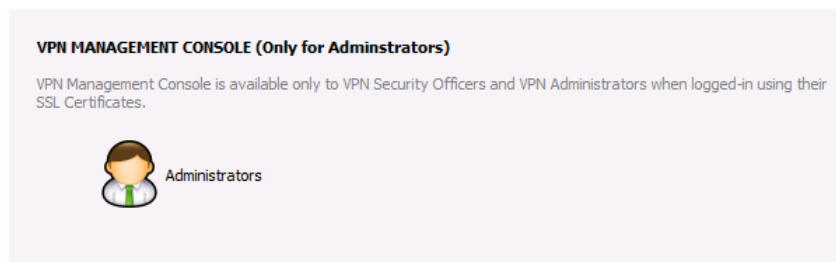


Click the OK button and the user needs to login again using the new password, to continue using VPN.

*Important: If you accidentally lose your password, contact your VPN Administrator.*

You can now access the VPN Management Console by browsing to [http://<vpn\\_hostname>](http://<vpn_hostname>)

Choose the “**Administrators**” link under VPN 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 a 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*

# CHAPTER 3

## APPENDICES

### APPENDIX A - PROCEDURE TO MAKE USB DRIVE BOOTABLE WITH PROPALMS ISO

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

Click on the following link to read instructions on how to make a USB bootable for installing Propalms VPN ISO image.

<https://fedorahosted.org/liveusb-creator/>

### APPENDIX B - SUPPORTED APPLICATIONS

#### SINGLE SIGN-ON FOR PROPALMS TSE

Once a user logs into VPN, if there is a Propalms TSE LaunchPad application available, the LaunchPad portal will be automatically launched using the credentials provided to login to VPN.

#### FEATURE DETAILS

VPN identifies the Propalms TSE LaunchPad application with application name. So for VPN client to be able to launch the TSE portal automatically after logon, create an application with name "PropalmsTSELaunchPad". Specify the hostname as the TSE server running the web server role. Specify port as 80 and specify the "Web Url" as the full URL of the Propalms TSE LaunchPad which should be <http://tse-web-server/launchpad>. Assign this application to respective user group.

When a user connects they will automatically launch the TSE LaunchPad and their credentials will be passed through from the VPN.

## OTHER APPLICATION CONFIGURATION

APPLICATION	PROTOCOL	STATIC/ DYNAMIC	PORT	REMARKS
WWW	TCP	Static	80	Kiosk
FTP	TCP	Dynamic	20,21	Kiosk
SSH	TCP	Static	22	Kiosk
TELNET	TCP	Static	23	Kiosk
ECHO	TCP	Static	7	
ECHO	UDP	Static	7	
VNC	TCP	Static	5900	Kiosk
WINDOWS TERMINAL SERVICE	TCP	Static	3389	Kiosk.
POP3	TCP	Static	110	
LDAP	TCP	Static	389	
IMAP	TCP	Static	143	
IMAP3	TCP	Static	220	
TIMBUKTU	TCP	Static	407	
SMTP	TCP	Static	25	
FILESHARE	TCP	Static	139	Kiosk
PRINT SHARE	TCP	Static	445	Kiosk
SAMBA SHARE	TCP	Static	139	Kiosk
SMB SHARE/ NETBIOS OVER TCP/IP	TCP	Static	139	Kiosk
CITRIX ICA CLIENT	TCP	Dynamic	1494	> 1023
CITRIX ICA CLIENT	UDP	Dynamic	1604	>1023
SQL SERVER	TCP	Static	1433	
SQL MONITOR TOOL	TCP	Static	1434	
MYSQL SERVER	TCP	Static	3306	
ORACLE	TCP	Static	1521	
DB2	TCP	Static		
LOTUS NOTES	TCP	Static	1352	
TFTP	UDP	Static	69	
RADIUS SERVER	TCP	Static	1812	
DNS SERVER	TCP	Static	53	
DNS SERVER	UDP	Static	53	
PC ANYWHERE	TCP	Static	5632	
PC ANYWHERE DATA	TCP	Static	5631	
TACACS	TCP	Static	49	
TACACS	UDP	Static	49	
ORACLE SQL * NET	TCP	Static	66	
BOOT PS	TCP	Static	67	
BOOT PS	UDP	Static	67	
KERBEROS	TCP	Static	88	
KERBEROS	UDP	Static	88	
NNTP	TCP	Static	119	
NNTP	UDP	Static	119	
INGRES-NET	TCP	Static	134	
INGRES-NET	UDP	Static	134	

APPLICATION	PROTOCOL	STATIC/ DYNAMIC	PORT	REMARKS
HTTPS	TCP	Static	443	
CVS	TCP	Static	2501	
Exchange Server -				
DEC Endpoint Resolution, also known as RPC Endpoint Mapper	TCP	Static	135	
Network Time Protocol-NTP	TCP	Static	123	
Kerberos authentication	TCP	Static	88	
LDAP to global catalog servers	TCP	Static	3268	
REQUIRED FOR WINDOWS LOGIN	TCP	Dynamic	1026	
IMAP	TCP	Static	143	
Messenger service through Exchange	TCP	Static	1863	



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.