



---

## Release Notes

### Propalms VPN v3.4.06

September 29, 2009

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
1.1	Installing Propalms VPN v3.4.06.....	3
1.2	Prerequisites .....	3
<b>2</b>	<b>New Features.....</b>	<b>4</b>
2.1	Endpoint Security Zones Renamed to Device Profiles .....	4
2.2	Application Assignment to Device Profiles Improved .....	4
2.3	Mandatory Profile: New System Default Profile.....	4
2.4	New Endpoint Security Policy Types Added: MAC ID and IP Address.....	4
2.5	Automatic Remediation for Failed Endpoint Security Policies .....	5
2.6	Cache Wiper and Basic Data Protection Feature Included.....	5
2.7	Detailed Endpoint Security Scan Logs .....	5
2.8	Passphrase Available on Management Console .....	5
2.9	Support For External CA Certificate.....	6
2.10	Logging Improvements.....	6
2.11	Launch Propalms TSE Portal Automatically .....	6
2.12	Network Obfuscation Support in Windows Vista/Windows 7 .....	6
2.13	Improved VPN Home Page.....	6
2.14	Support for Windows 7 .....	7
2.15	DNS Related Issues Fixed .....	7
2.16	Upgrade Appliance option added .....	7
2.17	Special Characters Allowed in Password During Cert Enrollment .....	7
2.18	Vista Access Made Seamless – Trusted Sites Management .....	7
<b>3</b>	<b>Open Issues .....</b>	<b>8</b>
3.1	File Share/Drive Mapping Support on Vista/Windows 7 .....	8
3.2	VPN Client Hangs on Vista and Windows 7 .....	8
3.3	Failure Deleting Second Security Officer or Administrator .....	8
<b>4</b>	<b>Features included in v3.4.03.....</b>	<b>9</b>
4.1	Branding Changes .....	9
4.2	Endpoint Security – Host Scan Policy Checks.....	9
4.3	Default Security Officer and Administrator count .....	11
4.4	Host name dependency for certificate users removed .....	11
4.5	Default Client Idle Timeout .....	11
4.6	Clientless VPN for Vista OS .....	11
4.7	VPN ActiveX uninstaller .....	11
<b>5</b>	<b>Features included in 3.4.02.....</b>	<b>13</b>
5.1	Support for Vista OS.....	13
5.2	On-Demand VPN Agent – ActiveX VPN.....	13
5.3	Support for non-admin users.....	13
5.4	Branding fixes .....	13
<b>6</b>	<b>Features included in 3.4.01.....</b>	<b>14</b>
6.1	Single Sign-ON for Propalms TSE User Portal .....	14
6.2	Support for client login using un-trusted SSL server certificate .....	14
6.3	Integrated VPN installer with Propalms OS.....	14
6.4	Propalms OS .....	14
6.5	New management console .....	15
6.6	New user portal and improved client interface.....	15
6.7	RADIUS Support Bug Fix.....	15

# 1 Introduction

This release notes document describes the features introduced and issues fixed in Propalms VPN v3.4.06.

## 1.1 Installing Propalms VPN v3.4.06

Starting from version 3.4.01 onwards Propalms VPN can be installed only using the Propalms Integrated installer. The Propalms integrated installer includes the Propalms OS as well as the VPN software image. The installer is available in form of an ISO which is made available on bootable CD-ROM or bootable USB drive or can be downloaded from Propalms website ([www.propalms.com](http://www.propalms.com)).

Please contact [vpnsupport@propalms.com](mailto:vpnsupport@propalms.com) for detailed instructions.

## 1.2 Prerequisites

Propalms VPN can be installed on a virtualization platform or any custom hardware which is compliant to run Fedora core 9 OS. In future Propalms VPN will be available on a closed hardware platform.

## 2 New Features

### 2.1 Endpoint Security Zones Renamed to Device Profiles

#### Feature Details

The "Endpoint Security Zone" in Propalms VPN Endpoint Security configuration is renamed as "Device Profile". The change is reflected in Endpoint Security Zone creation/modification pages. The change is made to keep the terminology related to calibrating the endpoint devices and putting them in profiles based on their trust level.

### 2.2 Application Assignment to Device Profiles Improved

In version 3.4.06, all applications are allowed for each device profile. Administrator can select to block specific applications to a device profile. This feature should reduce application assignment management for administrator.

#### Feature Details

Currently when a new application is added, admin has to add the application to application groups as well as admin needs to add the application to all configured device profiles (endpoint security zones in previous versions) to allow access to the application.

This becomes error prone and quite a task for every new application to be added. The application assignment to a device profile is changed so that every new application is allowed for every device profile. Admin must go and configure the application as BLOCKED application for the device profiles which restricts access to the application. This way the newly added applications are allowed by default but now can be selectively blocked for a device profile.

### 2.3 Mandatory Profile: New System Default Profile

A new system default device profile is added to Propalms VPN endpoint security features. Mandatory Profile enables administrators to define the least required set of policies that must be complied by all the endpoint devices connecting to VPN gateway. If the endpoint fails to clear all the policies specified in Mandatory Profile, the user is denied to login from this endpoint or network.

#### Feature Details

Currently when a new application is added, admin has to add the application to application groups as well as admin needs to add the application to all configured device profiles (endpoint security

### 2.4 New Endpoint Security Policy Types Added: MAC ID and IP Address

New endpoint policies are added for MAC ID and IP address checks. Admin can upload a list of MAC ID/IP addresses that can be enforced for the connecting device as part of endpoint security host scanning checks. Application access control can be then employed based on the result of the checks.

#### Feature Details

It is now possible to control logon access or application access based on the identity of the machine by matching the machine against the pre-known MAC ID and IP Addresses. Admin can define the known "good" MAC Addresses and/or IP addresses or define known "bad" MAC Addresses and/or IP addresses. When the user tries to login from a specific machine into VPN, the MAC ID of the active network adaptor and the public IP address of the user are evaluated by the VPN gateway against the MAC Address/IP Address policies. Optionally when set, VPN gateway can pass or fail a policy if any of the MAC Address (MAC address of other interfaces on user's machine) or IP address matches the list specified by administrator in VPN configuration. This makes sure that same policy gets enforced on the end user machine irrespective of whether the end user connects using wireless network or wired network.

## 2.5 Automatic Remediation for Failed Endpoint Security Policies

A user is now prompted for the failed policies and an option is provided to the user to fix the failed policies.

### Feature Details

When a user logs into the VPN, the details about failed policies is provided to the user along with option to remediate the policies. User can choose to fix the policies via VPN client or can fix manually. User can also ignore the information and continue with login into VPN. This feature will reduce support calls as it will enable the user to increase the trust level of the machine and get more access to VPN.

## 2.6 Cache Wiper and Basic Data Protection Feature Included

A Cache cleanup feature and basic data protection features are included

### Feature Details

Administrators can now set policies based on device profiles to cleanup following items on user logout:

- Internet Cache
- Cookies
- Browsing History
- Typed URLs
- Desktop Run History
- Recent File History
- Recycle Bin Contents

It is also possible to block the clipboard function so that user cannot perform any cut-copy-paste operation.

## 2.7 Detailed Endpoint Security Scan Logs

The endpoint security scan results are stored on the VPN gateway and can be viewed on management console through a new log viewer. The log viewer gives all details about each policy the user session is evaluated against and the scan result. Administrator can resolve a support call by looking at the logs. It is possible to download a summary of endpoint security scan results in CSV format.

## 2.8 Passphrase Available on Management Console

The passphrase generated for certificate users is now displayed on the management console after creation of the user. This will help to avoid any kind of delay or lost passphrase due to email delivery failures. VPN Administrator can send the passphrase to the users via other means like IM, private emails, etc.

## 2.9 Support For External CA Certificate

It is possible to upload an external CA root certificate while configuring VPN server.

## 2.10 Logging Improvements

General logging features are improved as mentioned below:

1. Option to configure log entries per page
2. Option to clear log files
3. Option to download logs in CSV format with correctly formatted file name
4. Size of the log files is displayed
5. Display of the logs is improved

## 2.11 Launch Propalms TSE Portal Automatically

Once a user logs into VPN, if there is a Propalms TSE launchpad application available, the launchpad portal will be automatically launched.

### 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 "Propalms TSE launchpad". Specify the hostname as the TSE server running the web server role. Specify port as 80 and specify the "Web Uri" as the full URL of the Propalms TSE launchpad which should be <http://tse-web-server/launchpad>. Assign this application to respective user group.

## 2.12 Network Obfuscation Support in Windows Vista/Windows 7

Network obfuscation support is added to Windows Vista and Windows 7. This features provides complete network blinding for internal network. This means for all the published applications, user will see random IP addresses with subnet 16.25.2.X

## 2.13 Improved VPN Home Page

The VPN home page is improved to include icons.

## **2.14 Support for Windows 7**

VPN client and the On-Demand Client are now supported on Windows 7.

## **2.15 DNS Related Issues Fixed**

Some of the client issues related to DNS are fixed. These issues restricted the user from accessing Internet when the user is connected to VPN. This issue happened randomly on Windows XP and Windows 2003 server clients.

## **2.16 Upgrade Appliance option added**

A new option "Upgrade Appliance" is added to "Server Configuration" node on management console so that the installed VPN base can be upgraded online. There is no need to go to Linux console to do any upgrades now. Propalms VPN Support team will provide patch files that can be uploaded using this option on VPN appliance and the firmware will get updated.

## **2.17 Special Characters Allowed in Password During Cert Enrollment**

Special characters are now allowed in the password when enrolling a certificate user. User must use the 3.4.06 VPN client with 3.4.06 gateway. Certificate "enrollment" is no more backward compatible now.

## **2.18 Vista Access Made Seamless – Trusted Sites Management**

For a user to access web applications using Internet Explorer, Propalms VPN site as well as all the web applications must be added to "Trusted Sites" in Internet explorer. Propalms VPN Client will do that automatically now. If an application is created with a "Web URI", the web uri will be added as "Trusted Site" in Internet explorer, on user logon. The user need not add all web applications to trusted sites. If the user is using Propalms VPN on-demand Client, user still need to add Propalms VPN URL as trusted site. Note: user need to add both http and https Propalms VPN site URLs as trusted sites.

## **3 Open Issues**

### **3.1 File Share/Drive Mapping Support on Vista/Windows 7**

**Issue:**

File share/Driver mapping is not supported on Vista and Windows 7

**Resolution:**

It's a work in progress. The feature will be available in next release.

### **3.2 VPN Client Hangs on Vista and Windows 7**

**Issue:**

The VPN Client may hang on Windows Vista and Windows 7. User need to kill VPN client process (vVPNClientExe.Exe) from task manager and re-login to continue.

The issue happens randomly and happens only on machines with special configurations.

**Resolution:**

The issue is being investigated and will be released as a patch once the issue is resolved.

### **3.3 Failure Deleting Second Security Officer or Administrator**

**Issue:**

If created it is not possible to delete security officer and administrator account on VPN if the total count of SO and admin is not maintained as at least 2.

**Resolution:**

If there is a need to delete the second security officer or administrator, create a third security officer or administrator and delete the second account.

## 4 Features included in v3.4.03

### 4.1 Branding Changes

#### Feature Details

Propalms VPN product has got a new icon now.

### 4.2 Endpoint Security – Host Scan Policy Checks

#### Feature Details

Endpoint security policies verify the integrity of the end point machines connecting to corporate network via Propalms VPN. Using Endpoint security checks, administrators can apply granular control over the devices that connects to the network. A device complying to the corporate policies is given highest level of access. A device which fails to comply to corporate policies, access to applications from this device can be restricted.

#### Concepts

Endpoint Security Policy:

An Endpoint Security Policy describes the checks to be performed on end point machine. The checks can be based on one or more Antivirus, Antispyware or firewall products.

Endpoint Security Sub-Policy:

An endpoint security policy can have multiple sub-policies. A sub-policy defines one single product or multiple products with common attributes. For e.g. in an endpoint security policy named "Check for Antivirus", there can be one or sub-policies like "Check for McAfee Antivirus", "Check for Trend Micro AV version 8.0 and above", etc. For an endpoint security to pass, at least one endpoint security sub-policy must pass.

Endpoint Security Zone:

A Zone is a set of endpoint security policies. Administrator can create maximum of 20 zones to create different endpoint device profiles. Administrator needs to specify the applications which are allowed for each device profile. An endpoint will fall into a particular zone, only if all the member policies are successfully cleared.

Quarantine Zone:

It's a no policy zone which is allocated to a device if the device fails to pass all endpoint security checks configured for other zone. Administrator should allow minimum set of applications to Quarantine zone. If such a zone is not specified and user fails to pass sufficient policies to fall into any other zone, the user is denied access to the VPN.

Application Assignment

The net list of applications allowed to the user is a combination of the endpoint security zone the user's machine fall into and the authentication groups the user belongs to. User will get applications which are allowed as per the zone as well as user's group membership.

#### Configuration Method

1. Create applications
2. Assign Applications to Application Groups

3. Create endpoint security policies
4. Create endpoint security zones
5. Assign endpoint security policies and add applications to endpoint security zones
6. Create access control to associate application groups with user groups

Note: Endpoint security needs to be enabled from "Server Configuration" -> "Endpoint Security" page. By default endpoint security is disabled.

### **Endpoint Security Product Definition Update**

Propalms VPN endpoint security definitions are updated in real time every hour. Propalms VPN gateway is configured to check for product updates every hour from site [www.oesismonitor.com](http://www.oesismonitor.com) over a HTTPS connection.

Note: On a freshly installed gateway, there are no product definitions available. Propalms VPN should have access to Internet to update the definitions. The definitions are updated on every reboot and then every hour. If there are no definitions present, the product up to date checks are considered successful.

### **Reporting**

The endpoint security zone to which the endpoint belongs is logged in the user logs. Users can see the zone name on the VPN status window.

### **Remediation**

In this version, user is reported about the policies they need to remediate to get more access. The details are displayed on the browser.

If the endpoint fails to fall into any security zone or falls into quarantine zone, the remediation information is displayed automatically. Alternatively, user can see the remediation information from the system tray menu item "Show Remediation Info". If the endpoint does not need to remediate any policies, the menu item is disabled.

### **Configuration Example:**

Use Case: Endpoint running any Antivirus product and firewall product is allowed to login and should be allowed all applications. The Antivirus must be latest, updated and real time protection must be ON. Firewall must be turned ON. Any endpoint failing these checks should be put in quarantine zone and should be given only web email access.

#### Configuration Steps:

1. Create one endpoint security policy named "Check for AntiVirus".
2. Set policy type to Antivirus
3. Add a sub-policy with name "Any Antivirus".
4. Keep Vendor name as "Any Antivirus Product"
5. Check option "Product upto date"
6. Check option "Real Time Protection Enabled"
7. Click Submit to add sub-policy
8. Click Submit to create endpoint security policy.
9. Create another endpoint security policy named "Check for Firewall"
10. Set policy type to Firewall
11. Add a sub-policy with name "Any Firewall"
12. Keep Vendor name as "Any Firewall Product"
13. Check option "Firewall is Enabled"
14. Click Submit to add sub-policy
15. Click Submit to create endpoint security policy.
16. Create an endpoint security zone named "Trusted Devices"

17. Add the two policies "Check for Antivirus" and "Check for Firewall"
18. Add all applications to the zone
19. Click Submit to create zone
20. Create another endpoint security zone
21. Check option "Quarantine Zone"
22. Add web-based email application to zone
23. Click Submit to create endpoint security zone
24. Make sure endpoint security is turned ON on page "Server Configuration" -> "Endpoint Security"

### **4.3 Default Security Officer and Administrator count**

#### **Feature Details**

From 3.4.03 onwards, there is only one security officer need to be created to bring the VPN server in "RUN" mode. It is not required to create minimum of 2 security officers and 2 administrators.

### **4.4 Host name dependency for certificate users removed**

#### **Feature Details**

It is now no more mandatory for certificate users to login using the hostname of the VPN server. Users can specify the IP address of the VPN gateway. In this case all client SSL certificates are listed in the "Certificate" combo control on the VPN login screen. The CA name is also displayed so that user can select the correct certificate in case multiple certificates with same name exists on the system.

Note: It is advised to always publish the VPN Gateway using the hostname for which the SSL server certificate is generated.

### **4.5 Default Client Idle Timeout**

#### **Feature Details**

Default client idle timeout is changed to 30 minutes.

### **4.6 Clientless VPN for Vista OS**

#### **Feature Details**

Propalms VPN Active-X based clientless VPN is now supported on Vista OS.

Note: Protected Mode of Internet explorer should be disabled for the applications to be accessed via Propalms VPN

### **4.7 VPN ActiveX uninstaller**

#### **Feature Details**

Release notes: Propalms VPN v3.4.03

To uninstall Propalms VPN ActiveX from the end user machine, run the program  
%SYSTEMDRIVE%\Windows\System32\PropalmsVPNActiveXUninstaller.exe.

Administrator rights are required to run this program.

Note: You must reboot the system after uninstalling the VPN ActiveX agent.

## 5 Features included in 3.4.02

### 5.1 Support for Vista OS

#### Feature Details

The Standalone VPN client now supports Vista OS. It has been tested on Vista Ultimate and Vista Home Basic editions. Please read following points to know the limitations of the client:

1. This client only support TCP and UDP applications
2. This client does not support name resolution and DNS resolution. Hence all applications must be accessed using IP address.
3. For web based applications to work through Vista client, the URL must be added as trusted site in internet explorer.
4. The activeX is not yet supported on Vista OS. User must use the client.
5. The Client is not yet tested on Vista 64 bit edition and Windows 2008 server.
6. The VPN client now works for standard users but administrator password is required for installation and un-installation. The client will automatically prompt the user to end the admin credentials when required. Admin rights are also required for first time use of the client.
7. Uninstalling the VPN client does not uninstall the LSP modules on Vista. Please run command "`\"vfvpninstlsp.exe -r\"` from `c:\windows\system32;`

**IMP:**The vista client is based on LSP API on Windows. Propalms VPN client for Vista installs a LSP module which remains installed even across machine reboots. Some of the applications may face conflict with third party LSPs. If any networked application fails to run on your machine, please uninstall LSP using command "`c:\windows\system32\vfvpninstlsp.exe -r`"

### 5.2 On-Demand VPN Agent – ActiveX VPN

#### Feature Details

The VPN ActiveX based client is now restored. It was removed in version 3.4.01 due to technical reasons. It is now back with ver 3.4.02.

### 5.3 Support for non-admin users

The VPN client can now run from standard user accounts also. The local admin rights are required for installation and un-installation of the client.

### 5.4 Branding fixes

The application portal page and one of the access denied page on management console are now converted to Propalms brand.

## 6 Features included in 3.4.01

### 6.1 Single Sign-ON for Propalms TSE User Portal

#### Feature Details

Propalms TSE customers can now deploy Propalms VPN to provide secure access to Propalms TSE servers. User is required to authenticate only once to the VPN. Once the user is logged into VPN, VPN will provide single sign-on feature for Propalms TSE published applications. When user launches the Propalms TSE launchpad, the user will directly see the published application page, rather than the login page.

SSO feature works only for one Propalms TSE web server. In next release support for multiple web servers will be added. SSO is optional and can be turned off. To configure SSO for Propalms TSE webserver, create an application in VPN with application name as "Propalms TSE Launchpad". If the application name is different than this, SSO will not be available.

SSO is only available for Launchpad. It is not available for TSE administrator console.

### 6.2 Support for client login using un-trusted SSL server certificate

#### Feature Details

In older versions, to login into VPN, user must install the VPN server SSL certificate if it is not signed by a already trusted CA. From ver 3.4.01 onwards, VPN client will support login using un-trusted certificates also. Basic Authentication users are not required to install the server's SSL certificate before they login. If the certificate is not issued by a trusted CA, user will be prompted a dialog to accept the server's certificate. Certificate users still need to install the server certificate.

This feature will also enable users to login using IP address of the VPN server.

### 6.3 Integrated VPN installer with Propalms OS

#### Feature Details

Propalms VPN 3.4.01 comes as a integrated installer which installs both the Propalms OS and the VPN. It's a single click, no questions asked installer which installs default setting along with Propalms VPN. The default settings on the appliance are;

Network Settings:

Eth0: 192.168.1.100

Eth1 and all other available interfaces: DHCP

Hostname: PropalmsVPN

The current version of integrated installer is 1.0.0.2.

### 6.4 Propalms OS

#### Feature Details

Propalms OS is based on a customized Fedora core 9 distribution. Propalms OS is a hardened distribution with a menu driven console interface to perform basic operations. Following operations can be performed using the menu driver interface:

Release notes: Propalms VPN v3.4.03

- Change IP address
- Change hostname
- Create host file entries
- Modify DNS settings
- Reinstall firmware
- Go to Linux shell

Propalms OS comes as a part of integrated installer. The current version of Propalms OS is 1.0.0.2

## **6.5 New management console**

### **Feature Details**

Management console is revamped to give it some web 2.0 functionality. It is now easier to navigate with better user experience.

## **6.6 New user portal and improved client interface**

### **Feature Details**

The user portal and VPN client are revamped to give better user experience.

## **6.7 RADIUS Support Bug Fix**

### **Feature Details**

RADIUS support issue in version 3.3 is resolved in ver 3.4.01. In version 3.3, RADIUS functionality was not working.