



Release Notes

Propalms VPN v3.5 Release 3.5.0.6

March 18, 2010

© 2010, Propalms Ltd. All Rights Reserved.

Table of Contents

1	Introduction	4
1.1	Getting v3.5.0.6 Virtual Appliance or v3.5.0.6 ISO	4
1.2	Installing Propalms VPN v3.5.....	4
1.3	Upgrading Propalms VPN v3.5.0.4 to v3.5.0.6	4
1.4	Upgrading Propalms VPN v3.4.0.X to v3.5	4
1.5	Prerequisites	5
2	Changes in v3.5.0.6	6
2.1	EULA Page Added Before Preboot.....	6
2.2	Changes on Preboot page	6
2.3	Change on Full Restore From Backup page.....	6
2.4	VPN OS Shell Changes	6
2.5	VPN ISO Installation Changes.....	6
3	Issues of 3.5.0.4 Fixed in v3.5.0.6.....	8
3.1	Upgrade Appliance Feature Not Working in 3.5.0.4	8
3.2	EPS Detailed Log Page Reports Internal Server Error	8
3.3	Reset Passphrase Feature Fails to Send Email Out	8
3.4	Dashboard shows wrong values of CPU Utilization	8
3.5	Authentication server list was not visible on VPN domain page	8
3.6	Network Configuration on Preboot stage does not apply the IP Address.....	9
3.7	“Reset Passphrase” option shows mail related error when the user is not enrolled.....	9
4	New Features in v3.5.0.4.....	10
4.1	Improved Management Console Interface	10
4.2	Inline Help on Management Console	10
4.3	Dashboard on Management Console	10
4.4	Multiple Authentication Server and Authentication Cascading	10
4.5	External Authorization Server	10
4.6	Block Groups	10
4.7	Global VPN Domain Settings.....	11
4.8	New Product Licensing	11
4.9	Configuration Backup and Restore Options.....	11
4.10	Administration Logs	12
4.11	Reset Security Officer Account.....	12
4.12	Network Settings Configuration	12
4.13	Route Configuration.....	13
4.14	Reboot and Shutdown Options	13
4.15	Scheduled Expiration of Local User Accounts	13
4.16	Detecting Application Creation Errors.....	13
4.17	VPN Client for Linux OS and MAC OS X	13
4.18	Single Sign ON for Propalms TSE for certificate users.....	14
4.19	Endpoint Security Configuration Checks	14
4.20	Re-issue Certificates to Certificate Users	14
4.21	Propalms OS Console Menu Authentication.....	14
4.22	Endpoint Security Product Support Updates.....	15
4.23	AD/LDAP Server: Default Group.....	15
4.24	Windows VPN Client: Progress Bar	15
4.25	Non 443 Port for VPN Gateway.....	15
5	Issues Fixed in v3.5.0.4.....	16
5.1	Random hang issue on Windows Vista and Windows 7.....	16
5.2	Web applications sometimes report disconnected	16
5.3	VPN Client does not work with PPP adaptors on Vista	16
5.4	Auto-Configuration of application on Management Console fails.....	16

5.5	Password Change not working for AD/LDAP	16
5.6	Hostname dependencies removed	16
5.7	Failure Deleting Second Security Officer or Administrator	17
5.8	Incorrect tabbing on management console.....	17
6	Open Issues in v3.5.0.4	18
6.1	File Share/Drive Mapping Support on Vista/Windows 7	18
6.2	Outlook Exchange Randomly Fails to Connect.....	18

1 Introduction

This release notes document describes the features introduced and issues fixed in Propalms VPN v3.5.0.6

1.1 Getting v3.5.0.6 Virtual Appliance or v3.5.0.6 ISO

Propalms VPN 3.5.0.6 virtual appliance and ISO can be downloaded from Propalms website www.propalms.com. Follow this link to download page and select appropriate product to download.

<http://www.propalms.com/download/productdownloads.php>

1.2 Installing Propalms VPN v3.5

Propalms VPN 3.5 is available as an integrated installer in form of an ISO that can be burned on a CD/DVD ROM or can be installed via a USB drive.

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).

For online help, please visit Propalms Support Portal: <http://support.propalms.com/> .

Visit <http://www.propalms.com/download/documentation.php> for downloading documentation.

Please contact vpnsupport@propalms.com for any other support requirements.

1.3 Upgrading Propalms VPN v3.5.0.4 to v3.5.0.6

Due to an issue in upgrade functionality of v3.5.0.4, v3.5.0.4 VPN gateway cannot be upgraded to v3.5.0.6. If a customer wants to upgrade to v3.5.0.6, they need to follow this procedure:

1. Take full system backup of VPN from management console HOST MAINTENANCE -> BACKUP AND RESTORE -> Backup Whole System
2. Install new v3.5.0.6 virtual appliance or reinstall VPN using v3.5.0.6 ISO.
3. During preboot stage, select option to restore VPN from a backup file.
4. On the restore screen, select the v3.5.0.4 backup file.
5. Your new v3.5.0.6 VPN is ready with same certificates and all the configuration.

Important Note: For full system backup to work, the hostname should not change across backup and restore.

1.4 Upgrading Propalms VPN v3.4.0.X to v3.5

Though Propalms VPN 3.4 has option to upgrade the firmware from management console, there is a migration module to be released along with v3.5 that will upgrade v3.4 configuration to v3.5. Customers

Release notes: Propalms VPN v3.5 - 3.5.0.6

running v3.4 will have to use the migration platform if the configuration settings need to be restored. The migration module will be released in May 2010.

1.5 Prerequisites

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

2 Changes in v3.5.0.6

2.1 EULA Page Added Before Preboot

Details;

An End User License Agreement page is added before pre-boot stage. User must accept it to continue the VPN setup wizard.

2.2 Changes on Preboot page

- Secondary DNS is now not mandatory on Preboot page
- Changed location of "Restore from Backup" option to Confirm Preboot stage
- System Date and time is automatically filled in
- At least one interface should be assigned a valid IP address. If more than one interface is present other ones can be assigned "NONE" or a valid IP addresses
- Net mask: Net mask cannot be "NONE" for a valid IP Address
- Default Gateway can be "NONE" or a valid IP Address
- Look and feel changes for better classification of controls
- "Commit" button is renamed to "Continue" on "Confirm System Configuration" page

2.3 Change on Full Restore From Backup page

- Link added on the "Restore From backup" page to cancel restore operation and continue with new VPN Instance installation
- On full system restore user will be informed about hostname change for VPN gateway, if required. Now Hostname will be modified to the same as the hostname of the gateway from which backup was taken.

2.4 VPN OS Shell Changes

- VPN OS Shell menu interface is redesigned for easy working over Serial Console Redirection. The current menu is not very friendly when redirecting VPN console over a serial cable and working over a simple text based terminal.
- Wherever applicable, the default account name and default password for VPN OS Shell is displayed.

2.5 VPN ISO Installation Changes

- Serial Console options are shown for both the CD-ROM and USB Installations.

For CDROM based installations where a monitor is connected to VPN gateway machine, user can press "Enter" key to continue installation.

In this case, the installation messages and the full boot messages will always go to monitor.

For CDROM based installation with serial console, user need to enter following command to start installation

```
cdrom console=ttyS0,<baudrate>
```

e.g. `cdrom console=ttyS0,9600`

In this case, all installation messages will go to serial console only. After VPN installation, boot messages still go over serial console. But after bootup, linux shell will be available over serial console as well as monitor.

For bootable USB based installation where a monitor is connected to VPN gateway machine, user need to type "usb" and press enter to start installation
In this case, the installation messages and the full boot messages will always go to monitor.

For bootable USB based installation over serial console, user need to enter following command to start installation

usb console=ttyS0,<baudrate>

e.g.

usb console=ttyS0,9600

In this case, all installation messages will go to serial console only. After VPN installation, boot messages still go over serial console. But after bootup, linux shell will be available over serial console as well as monitor.

3 Issues of 3.5.0.4 Fixed in v3.5.0.6

3.1 Upgrade Appliance Feature Not Working in 3.5.0.4

Issue:

The upgrade appliance feature does not upgrade the appliance. Hence customers who have installed 3.5.0.4 version can not upgrade to 3.5.0.4 and can not apply any patches.

Workaround:

Customers must use the ISO and reinstall the whole platform to upgrade to 3.5.0.6. To restore the settings, customers can follow this step:

1. Take full system backup from 3.5.0.4.
2. Install VPN using 3.5.0.6 ISO
3. Restore the VPN using backed up settings

Resolution;

The issue is fixed in 3.5.0.6. This means 3.4.0.6 installations can be upgraded to newer versions via management console.

3.2 EPS Detailed Log Page Reports Internal Server Error

Issue:

With endpoint security ON, if the administrator tries to view scan details on endpoint security log page, the details pop-up reports "Internal Server Error". Hence administrator can not view the details of a scan for a user.

Resolution:

The issue is fixed in 3.5.0.6

3.3 Reset Passphrase Feature Fails to Send Email Out

Issue:

If the administrator wants to reset passphrase of her or other administrator via the VPN shell menu item, the user never receives the email.

Resolution:

The issue is fixed in 3.5.0.6.

3.4 Dashboard shows wrong values of CPU Utilization

Issue:

The CPU utilization value on Dashboard is averaged to 5 seconds. Because of this the minor variations in CPU usage are not visible.

Resolution:

The issue is resolved. The CPU value is displayed at the instance of the data collection. The value is no more averaged to 5 seconds.

3.5 Authentication server list was not visible on VPN domain page

Issue:

When using Internet Explorer v8, not all authentication servers are visible on the VPN domain page. It is possible to add new authentication servers though.

Resolution:

The issue is fixed in 3.5.0.6.

3.6 Network Configuration on Preboot stage does not apply the IP Address

Issue:

On Preboot page, changing the IP Address from 192.168.1.100 to any other IP, "IP already exists in the network" error is thrown in random cases.

Resolution:

The issue is fixed in 3.5.0.6.

3.7 "Reset Passphrase" option shows mail related error when the user is not enrolled

Issue:

On resetting Certificate user's passphrase who is not yet enrolled into VPN from VPN Shell Console throws email delivery related error.

Resolution:

The issue is fixed in 3.5.0.6. The message "The user with the email ID is not enrolled yet" will be displayed.

4 New Features in v3.5.0.4

4.1 Improved Management Console Interface

Feature Details

The VPN management console GUI is simplified and improved now. The left navigation tree has a new organization with more logical grouping of configuration screens.

4.2 Inline Help on Management Console

Feature Details

Context sensitive help is added to management to facilitate quick reference to configuration options

4.3 Dashboard on Management Console

Feature Details

A new dashboard is added to management console showing live users, license usage, resource usage and important VPN information.

4.4 Multiple Authentication Server and Authentication Cascading

Feature Details

It is now possible to add and use more than 1 external authentication servers. There is a new authentication server management screen where multiple servers can be configured. These servers can be then configured in cascading mode. This means, if user can not be found in highest priority server, the user is will searched in the lower priority servers also.

4.5 External Authorization Server

Feature Details

In case the authentication server can not provide role/group information for an incoming user, a separate authorization server can be specified which will be used to provide user role information. Authentication servers like OTP tokens or RSA SecureID servers may not provide role information to VPN gateway. VPN gateway requires user's role to assign applications to the user. With such servers an additional external authentication server or native groups can be used to decide the role of the user. The authentication is done with the external authentication server and then the username is searched in the configured external authorization server

4.6 Block Groups

Feature Details

Administrator can specify a list of native/local groups that are not allowed to login into the VPN gateway. This feature can be used when the external authentication server cannot provide any role information and VPN local groups need to be used to put users into particular roles. In that case specific local groups can be blocked to login into VPN.

4.7 Global VPN Domain Settings

Feature Details

A new screen is added to management console to define the authentication and authorization scheme for the VPN, termed as VPN domain. In future versions, it will be possible to add multiple VPN domains each with own AAA scheme.

The global authentication scheme includes the authentication servers to be used for authentication, any external authentication server(s) and group list which needs to be denied login to VPN

4.8 New Product Licensing

Feature Details

The licensing mechanism is improved to include a system default license, endpoint security feature control based on license as well as making the license key tied to a particular hardware.

VPN gateway can run in 3 license states:

1. System default (5 users for 30 day evaluation)
2. Evaluation license (time bound)
3. Production license

A newly installed VPN gateway can be started in system default license which is valid for 5 concurrent users for 30 days. Alternatively administrator can choose to put a license key at the time of pre-boot stage.

A license key can be added from management console after the VPN is configured.

To get a license key, administrator must send the "product key" displayed on management console to info@propalms.com. The new license key will be valid only for the hardware from which product key was taken.

The new license can enable endpoint security feature on the appliance.

The VPN gateway will send notification emails to all registered security officers and administrators before 5 days and 2 days from expiry of the license. The VPN gateway will send a last notification email 24 hours before expiry of the license.

4.9 Configuration Backup and Restore Options

Feature Details

With v3.5, administrators can backup the configuration and restore the same in case of a disaster.

The backup file is stored on administrator's desktop which can be uploaded back to gateway for restoration.

There are two back options available: User settings backup or full system backup.

User Settings Backup:

This backup will export the settings configured by administrator to the desktop.

This backup enables administrators to regularly back the settings and use them in case the administrator needs to revert back to old state or the old system has to be replicated to a new one.

The backup includes following settings:

Local Users: Only basic authentication users

Local Groups

Applications

Application Groups
Access Control
Authentication servers
VPN Domain
Endpoint Security configuration
Host Scan Policy
Device Profiles

This backup does not include any certificate and system information hence is portable across various VPN gateways located at difference locations.

Full System Backup:

This backup exports everything including the certificates related configuration. This backup is useful to rebuild a whole system by reinstalling the firmware and then restoring it to the last backed-up state again.

This backup includes following information:

- All the user settings as in "User settings backup" above.
- SSL and Certificate authority certificates
- User certificates

It is important to make sure the hostname of the system should be set to same as what it was when the backup was taken from the system. If the hostname is different, an error will be prompted to the administrator. It will also give the name of the expected hostname.

This backup type can be used to restore a whole system.

In both cases, VPN must be in configuration state and the VPN services will restart after restore process is over.

4.10 Administration Logs

Feature Details

All the administration changes are logged and viewable through management console. The logs are achieved on the gateway with capacity to store more than 200,000 log entries.

4.11 Reset Security Officer Account

Feature Details

An option is added to VPN console to reset security officer/administration's account. The feature resets the administrator's certificate on VPN management console and sends a new passphrase to the registered email ID of the administrator. This feature can be used in case administrator's certificate is lost or administrator forgets her password.

4.12 Network Settings Configuration

Feature Details

A new option is added to management console so that IP address, DNS and host file modifications can be done from management console. Administrators can change IP address related settings as well as configure the DNS options. It is also possible to create host file entries on VPN gateway to resolve the names.

4.13 Route Configuration

Feature Details

A new option is added to management console so static route configuration can be done from management console.

4.14 Reboot and Shutdown Options

Feature Details

A new option is added to management console to reboot and shutdown the appliance.

4.15 Scheduled Expiration of Local User Accounts

Feature Details

At the time of creating local user accounts, administrator can set a date when the account will automatically expire. After the given date the user account is set to "disabled". This option is applicable only for basic authentication and certificate users. This option is not applicable to security officers and administrators.

4.16 Detecting Application Creation Errors

Feature Details

While creating new application, it is common to set a hostname for Application server or the URL which is not resolvable from VPN gateway. This can happen either the hostname typed is not correct or the DNS server is not configured correctly or there is no DNS server at all. In v3.5 when creating application, the VPN will check if the hostname specified as Application Server hostname and the hostname/domain name in the Web URL is resolvable from VPN gateway or not. An error is thrown if the name cannot be resolved. Administrator can fix the hostname or they can create host file entry for the hostname.

4.17 VPN Client for Linux OS and MAC OS X

Feature Details

VPN Clients for Linux and MAC OS X are now available for download from VPN portal. Users can choose to download the correct VPN client for their platform.

For Linux, a RPM based installer is available for Fedora, Redhat and Suse distributions. A Deb based installer is available for debian flavor of platforms like Ubuntu. Same installers can be used irrespective of release versions of Linux. The command to install the rpm is:

```
rpm -ivh --nodeps <rpm file name>
```

The command line for installing using deb is:

```
Dpkg -i <deb package name>
```

Administrative rights are required for installation of the client.

VPN Client for MAC OS X is supported from version 10.4 and above version. The VPN client is not yet tested on 10.6 version. The MAC OS X installer is a compressed file (.tgz file). After downloading the compressed installer, user should double click to extract and then double click to start the installer.

Administrative rights are required for installation of the client.

4.18 Single Sign ON for Propalms TSE for certificate users

Feature Details

Till version 3.4, SSO for Propalms TSE was supported only for basic authentication users. In v3.5, SSO is supported for users authenticating with certificate also. The username is fetched from the client certificate's 'issued to' field. The user must have same username and password on the Propalms TSE server also.

4.19 Endpoint Security Configuration Checks

Feature Details

Following restrictions are added to endpoint security configuration:

Endpoint security cannot be turned ON unless there is a device profile present.

A Device profile cannot be added unless a Host scan policy is already present.

A Mandatory Device Profile cannot be created unless at least one more device profile exists.

A Quarantine Device Profile cannot be created unless at least one more device profile exists.

4.20 Re-issue Certificates to Certificate Users

Feature Details

It is now possible to reissue certificates to users by resetting their certificate from management console.

On the "Users" screen a button "Recover passphrase" is added to reset the user's current certificate and generate a new passphrase. The new passphrase will be sent to user's registered email ID.

4.21 Propalms OS Console Menu Authentication

Feature Details

In v3.5, when using Propalms OS Console menu, user needs to authenticate to console using a built-in account. The account name is 'consoleadmin'. The password for the account is 'adminconsole'.

Administrator has option to change the password for consoleadmin user.

Root access to Propalms OS is blocked completely.

4.22 Endpoint Security Product Support Updates

Feature Details

Endpoint security product support is upgraded to version 3.4.5.1.

4.23 AD/LDAP Server: Default Group

Feature Details

An option is added while creating access control for AD/LDAP server to include all groups of the AD/LDAP server.

While creating access control, select the AD/LDAP server to fetch the group list. The first item in the group list is a special group named "All Groups". If this group is selected, the access control is applicable to all groups of AD/LDAP. This will enable easy deployment in cases of large AD/LDAP deployment and where most of the groups must be given access to VPN. This feature can also be used when there is no group categorization done on AD/LDAP server.

4.24 Windows VPN Client: Progress Bar

Feature Details

Progress bars are added at time of login, logout and while downloading the new upgrade installer.

4.25 Non 443 Port for VPN Gateway

Feature Details

VPN Client now can connect to VPN Gateway running on ports other than standard HTTPS port 443. In the "VPN server" field specify the port as : "VPN gateway FQDN:Port No".

e.g. remote.company.com:444

Note: currently VPN gateway cannot be run on ports other than 443, though the VPN gateway can be NATTED behind a router/firewall on ports other than 443.

5 Issues Fixed in v3.5.0.4

5.1 Random hang issue on Windows Vista and Windows 7

Issue:

The Windows client hangs randomly on Windows Vista and Windows 7 platforms.
The issue is fixed in v3.5.

5.2 Web applications sometimes report disconnected

Issue:

With Windows client, the web applications sometimes failed with error "page cannot be displayed".
The issue is fixed in v3.5.

5.3 VPN Client does not work with PPP adaptors on Vista

Issue:

Windows client won't connect through a PPP adaptor based Internet connection like mobile based modems. This issue happens only on Windows Vista.
The issue is fixed in v3.5

5.4 Auto-Configuration of application on Management Console fails

Issue:

With Firefox, the auto-configuration of application option on "Create Application" screen fails with Internet Server Error.
The issue is fixed in v3.5

5.5 Password Change not working for AD/LDAP

Issue

Password cannot be changed for an AD/LDAP account if CA authority of the directory server is not a known authority.

The issue is resolved in v3.5.

5.6 Hostname dependencies removed

Issue

It is now not mandatory for the users to be able to resolve the hostname of VPN gateway. The the hostname dependencies are resolved.

5.7 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.

Issue is fixed in v3.5

5.8 Incorrect tabbing on management console

Issue:

The tab order changed randomly on management console. The issue is fixed now.

6 Open Issues in v3.5.0.4

6.1 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.

6.2 Outlook Exchange Randomly Fails to Connect

Issue:

If the user is using MS Exchange over VPN, sometime the outlook application will get into disconnected mode. At this time outlook fails to connect through VPN.

Resolution:

Logout from VPN and login again. This issue will be resolved and will be available as a hot fix.