



# What's New in Propalms VPN 3.5?

---

## Contents

Improved Management Console Interface.....	2
Inline Help on Management Console .....	2
Graphical Dashboard on Management Console .....	2
Multiple Authentication Server and Authentication Cascading .....	2
External Authorization Server .....	2
Block Groups .....	3
Global VPN Domain Settings.....	3
New Product Licensing.....	3
Configuration Backup and Restore Options.....	4
Administration Logs .....	5
Reset Security Officer Account .....	5
Network Settings Configuration.....	5
Route Configuration.....	5
Reboot and Shutdown Options.....	5
Scheduled Expiration of Local User Accounts.....	5
Detecting Application Creation Errors .....	6
VPN Client for Linux OS and MAC OS X.....	6
Single Sign ON for Propalms TSE for certificate users .....	6
Endpoint Security Configuration Checks.....	7
Re-issue Certificates to Certificate Users.....	7
Propalms OS Console Menu Authentication.....	7
Endpoint Security Product Support Updates .....	7
Issues Fixed in v3.5.....	8

## **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.

## **Inline Help on Management Console**

### **Feature Details**

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

## **Graphical Dashboard on Management Console**

### **Feature Details**

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

## **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.

## **External Authorization Server**

### **Feature Details**

In case the authentication server cannot 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.

## Block Groups

### Feature Details

The 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.

## 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

## 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](mailto: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.

# Configuration Backup and Restore Options

## Feature Details

With v3.5, administrators can back up 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 up 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 the 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.

## **Administration Logs**

### **Feature Details**

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

## **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.

## **Network Settings Configuration**

### **Feature Details**

A new option is added to the 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.

## **Route Configuration**

### **Feature Details**

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

## **Reboot and Shutdown Options**

### **Feature Details**

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

## **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.

## Detecting Application Creation Errors

### Feature Details

While creating new applications, 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 applications, 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 displayed if the name cannot be resolved. The Administrator can fix the hostname or they can create host file entry for the hostname.

## 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.

## Single Sign ON for Propalms TSE for certificate users

### Feature Details

Until 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.

## 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.

## Re-issue Certificates to Certificate Users

### Feature Details

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

## 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’.

The Administrator has the option to change the password for ‘consoleadmin’ user.

Root access to Propalms OS is blocked completely.

## Endpoint Security Product Support Updates

### Feature Details

Endpoint security product support is upgraded to version 3.4.5.1.

## **Issues Fixed in v3.5**

### **Random hang issue on Windows Vista and Windows 7**

**Issue:**

The Windows client hangs randomly on Windows Vista and Windows 7 platforms.

### **Web applications sometimes report disconnected**

**Issue:**

With Windows client, the web applications sometimes failed with error “page cannot be displayed”.

### **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.

### **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.

### **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.

### **Hostname dependencies removed**

**Issue:**

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

### **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.