



Release Notes

Propalms VPN v3.5

January 27, 2010

© Copyright 2010, Propalms Ltd. All Rights Reserved.

© Copyright 2010, Propalms Ltd. All Rights Reserved.

1	Introduction.....	4
1.1	Installing Propalms VPN v3.5	4
1.2	Upgrading Propalms VPN v3.4.0.X to v3.5.....	4
1.3	Prerequisites	4
2	New Features in v3.5.0.4	5
2.1	Improved Management Console Interface.....	5
2.2	Inline Help on Management Console.....	5
2.3	Dashboard on Management Console.....	5
2.4	Multiple Authentication Server and Authentication Cascading	5
2.5	External Authorization Server	5
2.6	Block Groups.....	5
2.7	Global VPN Domain Settings	6
2.8	New Product Licensing.....	6
2.9	Configuration Backup and Restore Options	6
2.10	Administration Logs.....	7
2.11	Reset Security Officer Account	7
2.12	Network Settings Configuration	7
2.13	Route Configuration	8
2.14	Reboot and Shutdown Options.....	8
2.15	Scheduled Expiration of Local User Accounts.....	8
2.16	Detecting Application Creation Errors.....	8
2.17	VPN Client for Linux OS and MAC OS X.....	8
2.18	Single Sign ON for Propalms TSE for certificate users	9
2.19	Endpoint Security Configuration Checks	9
2.20	Re-issue Certificates to Certificate Users	9
2.21	Propalms OS Console Menu Authentication	9
2.22	Endpoint Security Product Support Updates	10
2.23	AD/LDAP Server: Default Group	10
2.24	Windows VPN Client: Progress Bar	10
2.25	Non 443 Port for VPN Gateway	10
3	Issues Fixed in v3.5	11
3.1	Random hang issue on Windows Vista and Windows 7	11
3.2	Web applications sometimes report disconnected	11
3.3	VPN Client does not work with PPP adaptors on Vista	11
3.4	Auto-Configuration of application on Management Console fails	11
3.5	Password Change not working for AD/LDAP	11
3.6	Hostname dependencies removed	11
3.7	Failure Deleting Second Security Officer or Administrator.....	12
3.8	Incorrect tabbing on management console	12
4	Open Issues in v3.5.....	13
4.1	File Share/Drive Mapping Support on Vista/Windows 7	13
4.2	Outlook Exchange Randomly Fails to Connect	13
4.3	Random VPN Client hang on logout	13
4.4	Endpoint Security IP Address Policy Checking Failed	13
5	Features included in 3.4.0.6.....	14
5.1	Endpoint Security Zones Renamed to Device Profiles	14
5.2	Application Assignment to Device Profiles Improved	14
5.3	Mandatory Profile: New System Default Profile.....	14
5.4	New Endpoint Security Policy Types Added: MAC ID and IP Address.....	14
5.5	Automatic Remediation for Failed Endpoint Security Policies	15
5.6	Cache Wiper and Basic Data Protection Feature Included.....	15
5.7	Detailed Endpoint Security Scan Logs	15
5.8	Passphrase Available on Management Console	15

5.9	Support For External CA Certificate.....	16
5.10	Logging Improvements.....	16
5.11	Launch Propalms TSE Portal Automatically.....	16
5.12	Network Obfuscation Support in Windows Vista/Windows 7.....	16
5.13	Improved VPN Home Page.....	16
5.14	Support for Windows 7.....	16
5.15	DNS Related Issues Fixed.....	17
5.16	Upgrade Appliance option added.....	17
5.17	Special Characters Allowed in Password During Cert Enrollment.....	17
5.18	Vista Access Made Seamless – Trusted Sites Management.....	17
6	Features included in v3.4.03.....	18
6.1	Branding Changes.....	18
6.2	Endpoint Security – Host Scan Policy Checks.....	18
6.3	Default Security Officer and Administrator count.....	20
6.4	Host name dependency for certificate users removed.....	20
6.5	Default Client Idle Timeout.....	20
6.6	Clientless VPN for Vista OS.....	20
6.7	VPN ActiveX uninstaller.....	21
7	Features included in 3.4.02.....	22
7.1	Support for Vista OS.....	22
7.2	On-Demand VPN Agent – ActiveX VPN.....	22
7.3	Support for non-admin users.....	22
7.4	Branding fixes.....	22
8	Features included in 3.4.01.....	23
8.1	Single Sign-ON for Propalms TSE User Portal.....	23
8.2	Support for client login using un-trusted SSL server certificate.....	23
8.3	Integrated VPN installer with Propalms OS.....	23
8.4	Propalms OS.....	23
8.5	New management console.....	24
8.6	New user portal and improved client interface.....	24
8.7	RADIUS Support Bug Fix.....	24

1 Introduction

This release notes document describes the features introduced and issues fixed in Propalms VPN v3.5.0.4.

1.1 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).

Please contact vpnsupport@propalms.com for detailed instructions.

1.2 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 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 Feb 2010.

1.3 Prerequisites

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

2 New Features in v3.5.0.4

2.1 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.

2.2 Inline Help on Management Console

Feature Details

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

2.3 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.

2.4 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.

2.5 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

2.6 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.

2.7 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

2.8 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.

2.9 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.

2.10 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.

2.11 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.

2.12 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.

2.13 Route Configuration

Feature Details

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

2.14 Reboot and Shutdown Options

Feature Details

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

2.15 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.

2.16 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.

2.17 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.

2.18 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.

2.19 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.

2.20 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.

2.21 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.

2.22 Endpoint Security Product Support Updates

Feature Details

Endpoint security product support is upgraded to version 3.4.5.1.

2.23 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.

2.24 Windows VPN Client: Progress Bar

Feature Details

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

2.25 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.

3 Issues Fixed in v3.5

3.1 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.

3.2 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.

3.3 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

3.4 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

3.5 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.

3.6 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.

3.7 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

3.8 Incorrect tabbing on management console

Issue:

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

4 Open Issues in v3.5

4.1 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.

4.2 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.

4.3 Random VPN Client hang on logout

Issue:

Sometimes, logging out from VPN hangs the Windows VPN client. In this case, client application needs to be terminated from task manager

Resolution:

Kill the VPN Client process from task manager. This issue will be resolved and will be available as a hot fix.

4.4 Endpoint Security IP Address Policy Checking Failed

Issue:

For an endpoint security policy of type IP address with IP address configured for "allow" or "block" for "active ip address", then only the first IP address is evaluated against the IP address of the user endpoints. IP addresses after the first IP addresses are not considered during policy evaluation. To reproduce the issue, create an endpoint security policy for IP address, select "allow" or "block" on Add ip address list page. Select option "allow if active IP address matches" and specify more than 1 IP addresses.

When the policy is evaluated only the first IP address is taken into account and not the rest of the IP addresses in the specified list.

Resolution:

This issue is fixed post 3.5.0.6 release. The fix will be available as a hot fix over 3.5.0.6.

5 Features included in 3.4.0.6

5.1 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.

5.2 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.

5.3 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

5.4 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.

5.5 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.

5.6 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.

5.7 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.

5.8 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.

5.9 Support For External CA Certificate

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

5.10 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

5.11 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.

5.12 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

5.13 Improved VPN Home Page

The VPN home page is improved to include icons.

5.14 Support for Windows 7

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

5.15 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.

5.16 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.

5.17 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.

5.18 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.

6 Features included in v3.4.03

6.1 Branding Changes

Feature Details

Propalms VPN product has got a new icon now.

6.2 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 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-polocy
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"

6.3 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.

6.4 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.

6.5 Default Client Idle Timeout

Feature Details

Default client idle timeout is changed to 30 minutes.

6.6 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

6.7 VPN ActiveX uninstaller

Feature Details

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.

7 Features included in 3.4.02

7.1 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`"

7.2 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.

7.3 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.

7.4 Branding fixes

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

8 Features included in 3.4.01

8.1 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.

8.2 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.

8.3 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.

8.4 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 v3.5 (3.5.0.4)

- 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

8.5 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.

8.6 New user portal and improved client interface

Feature Details

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

8.7 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.