



What's New in Propalms VPN 3.6?

Contents

New VPN Portal.....	2
Application Templates	2
Thin Applications on VPN Portal	2
My Desktop – Personal Desktop Delivery.....	3
Propalms TSE Integration.....	3
VPN Cluster and High Availability	3
Portal Customization.....	4
CSR Generation and SSL Certificate Upload.....	4
Remote Meetings.....	4
PROID Server	4
NTP Settings	5
Network Tools: Ping, Traceroute	5
Change VPN Gateway Port Number	5
Change SSL Ciphers	5
Option to Hide Application Pop-up and Listing	5
Show Real IP Address to User	6
VPN Client Upgrades without Admin Rights	6
VPN Client: Tight Integration with Propalms TSE	7
Issues Fixed in v3.6.....	8

New VPN Portal

Feature Details

Propalms VPN 3.6 gets a new portal for clientless access. Users can use a browser to login into VPN and access the applications listed on the portal. The following types of applications are listed on the portal:

- Web applications: HTTP, HTTPS,
- Java based applications: RDP, VNC, Telnet, SSH, Fileshare
- Integrated Apps: Propalms TSE, Propalms VDI
- My Desktop: Personal desktop access

VPN Portal shows following information to the user:

- List of applications user has access to.
- A logon message by administration on login page
- A welcome message by administration on portal landing page
- Status of VPN client
- Endpoint security result
- Option to change password

Application Templates

Feature Details

New application templates are added on management console to help administrator create standard applications as well as define additional parameters. The following new templates are added:

- HTTP, HTTPS, FTP – Web, FTP - Java
- SSH, Telnet, Microsoft Exchange, Microsoft Fileshare, NFS
- RDP, VNC, My Desktop
- Propalms TSE – Web, Propalms TSE – RDP, Propalms TSE – Print, Propalms VDI
- Citrix Web, Citrix ICA, Web Proxy application

Thin Applications on VPN Portal

Feature Details

VPN Portal comes with a set of Java applications which helps user access applications without requiring client software. Following Java applications are available on the portal:

- Remote Desktop
- File Transfer
- Secure Shell
- VNC
- File Share

My Desktop – Personal Desktop Delivery

Feature Details

MyDesktop provides direct desktop access via Propalms VPN. Administrator can create an application with application type as MyDesktop and upload a list of usernames along with their desktop hostname/IP address. This application can be then assigned to the groups. When users login into VPN an application with name MyDesktop is displayed on the VPN Portal. User can access her desktop using hostname “MyDesktop” or the IP address of her desktop. The MyDesktop application can be accessed from VPN Client also.

When creating a MyDesktop application, administrator can specify which protocol to use for remote desktop session. Two choices are RDP and VNC.

Propalms TSE Integration

Feature Details

Before version 3.6, Propalms VPN and Propalms TSE were only loosely integrated. Propalms VPN could enable single sign for Propalms TSE, but in version 3.6, Propalms VPN and TSE are much more tightly integrated. In 3.6, a user will not need to interact with Propalms TSE LaunchPad to access TSE applications.

When user logs into Propalms VPN Portal or Propalms VPN Client and user has been given access to Propalms TSE team, the Propalms TSE applications will be pulled from TSE server and made available directly on VPN portal and VPN Client LaunchPad.

This feature will provide seamless access to VPN and TSE hosted application, improving user experience to a great extent.

On VPN Portal a new tab is added to display Propalms TSE Applications. VPN Client will also display TSE applications on application LaunchPad.

VPN Portal and client also take care of installing Propalms TSE connection manager client.

VPN Cluster and High Availability

Feature Details

VPN High availability and load balancing feature is required to make VPN service always ON with efficient utilization of hardware resources available, required to support large no. of remote users. The system would enable thousands of remote users to be able to access corporate services with maximum performance. The whole deployment will be fault tolerant and should manage the user load efficiently. The high availability and load balancing system is also referred to as VPN cluster.

Propalms VPN Cluster feature enables organizations to deploy two or more VPN gateways to support large no. of user’s with highly available VPN service.

The cluster will have the following components:

- Load balancer module: At least 1, maximum 2
- High availability module: At least 1, maximum 2
- VPN Gateway module: At least 1, maximum: 256

Refer to the detailed Cluster and High availability FSD document named High Availability and Load Balancer_fsd.docx for more detailed information.

Portal Customization

Feature Details

Customer can now customize the VPN portal directly from VPN management console. It is possible to upload a custom logo and company name and set login and welcome messages to be displayed on VPN portal. It is also possible to hide the Propalms Ltd. Copyright message and hide the VPN client download links.

CSR Generation and SSL Certificate Upload

Feature Details

In VPN 3.6, customers can generate Certificate Signing Request from the VPN directly and send to the CA for getting the SSL certificate. Administrator can upload the new SSL certificates included the intermediate CA certificates from the management console.

Remote Meetings

Feature Details

In Propalms VPN 3.6, a feature is added to VPN such that two VPN users can do remote web meetings for the purpose of sharing presentation, text chat, file transfer or just use as helpdesk. Remote meeting feature is available in both VPN Portal and VPN Client. A user can select “give support” to connect to another VPN user. User can select “get support” to request support from another VPN user.

For connecting to another user, user must enter the username of the partner and the meeting password.

PROID Server

Feature Details

PROID is a two factor authentication solution that provides One Time Passwords delivered via multiple mechanisms including hard tokens, soft tokens, email, SMS, PKI tokens and web tokens. VPN 3.6 can authenticate user’s with PROID server by calling its authentication API running over HTTPS rather than using plain text UDP based RADIUS protocol.

One or more PROID servers can be created and assigned to VPN domain. PROID server only provides authentication services. Authorization service is not provided by PROID server.

NTP Settings

Feature Details

It is now possible to configure Network Time Protocol servers in VPN settings. Setting NTP server configuration helps keeping time on VPN gateway in-synch to the world time.

Network Tools: Ping, Traceroute

Feature Details

New tools are added to help troubleshoot the problems. Ping and traceroute tools are added to VPN gateway.

Change VPN Gateway Port Number

Feature Details

It is now possible to configure a port different than port 443 for VPN gateway. If the VPN port is changed to something other than 443, users can connect to VPN by specifying server address in VPN client as <vpn hostname>:<new port no.>. This option is available under Global VPN settings page on administration console.

Change SSL Ciphers

Feature Details

It is now possible to configure SSL ciphers to be used for SSL tunnels. Both SSL 3.0 and SSL 2.0 ciphers can be configured. Though most of the OpenSSL supported ciphers are listed, only a limited set of ciphers can be configured based on the Cipher support available in most common browsers like Internet explorer and Firefox. If only unsupported Ciphers are selected, the connectivity to the VPN will be lost and the only option will be to manually change the ciphers.

Option to Hide Application Pop-up and Listing

Feature Details

It's now possible to hide application getting listed on VPN Portal and VPN Client. Application can also be hidden from getting listed in activities list on VPN client. Option "Hide application pop-up" will hide the pop-up that comes up on accessing the application.

Show Real IP Address to User

Feature Details

When enabled, user will be able to see the real IP address of the application server. By default the user sees a mangled IP address for the application servers. But some applications like FTP in browser, does not work very well with mangled IP addresses. For support FTP via Internet Explorer 8 and higher, this option should be selected.

VPN Client Upgrades without Admin Rights

Feature Details

VPN client can be now upgraded without requiring administrative rights. In earlier version, user must have administrative rights to both install and upgrade the VPN client. From version 3.6 onwards, installation will require admin rights but further upgrades will happen without requiring admin rights.

VPN Client working from a restricted user account

Feature Details

VPN Client is now fully supported with all functionality in a restricted user account. Following functionalities are enhanced in this version:

- Name resolution when the user is not part of any domain
- Starting of network filter driver on Windows XP
- Adding VPN client to Windows Firewall allowed applications list
- Automatic upgrade of VPN client

New Application Launcher GUI with VPN Client

Feature Details

In earlier versions, VPN client used internet explorer to launch the application portal. Starting this version a new dialog based Application portal is launched. This VPN client application launcher shows a list of web applications and the Administration application if authorized.

VPN Client: Hiding SSL Server Certificate Check Warning Dialog during Login

Feature Details

During login, the VPN client displays a warning dialog if the server certificate does not pass the 3 checks for server's SSL certificate:

- Certificate should be signed by a trusted CA
- Date should be valid
- FQDN specified by user to the client to connect to should match the "Issued To" field in SSL certificate.

If the certificate fails any of these checks, a warning dialog is shown

A new option is added to this dialog to hide this dialog from next login. If user selects this option, the SSL server warning dialog will never be displayed again.

VPN Client: System Tray Menu Changed

Feature Details

The system tray menu now has shortcuts to the VPN Application Launchpad as well as the TSE Web Portal (if access provided).

Now when double clicking the system tray, the VPN application launcher dialog is opened rather than the VPN statistics dialog. This happens only when VPN application launcher is enabled. VPN Application launcher gets enabled when there is a web application available to the user.

VPN Client: Tight Integration with Propalms TSE

Feature Details

VPN Client can now manage Propalms TSE hosted applications, including installation and initialization of Propalms TSE Connection Manager Client. It's no more mandatory to create an application with name PropalmsTSELaunchpad, just that the application type specified should be Propalms TSE – Web. VPN client will try to initialize the Propalms TSE PCM with the URL specified in the VPN application.

If PCM is not installed or an updated version is available with VPN gateway, VPN client can install/update the PCM client after confirming with user. Once ready, VPN client initializes PCM client and lists the TSE hosted applications on Propalms VPN Application launcher dialog.

It is mandatory for Propalms TSE webserver to work on HTTP.

Note: The auto initialization of Propalms TSE apps happens only when an application is published in the VPN for the user and a valid Propalms TSE LaunchPad URL is configured. It is still possible to open Propalms TSE LaunchPad URL in browser by selecting **TSE Web Portal** option in VPN client system tray.

Issues Fixed in v3.6

Security Fix: SSL 2.0 is now disabled

SSL v2.0 is now completely disabled on SSL VPN gateway. SSL 2.0 is known to have cryptographic vulnerabilities that might allow an attacker to decipher the SSL protocol. It is recommended to use SSL 3.0/TLS 1.0 protocol.

Security Fix: ICMP Timestamps are disabled

It was found that it's possible to detect the exact time on VPN gateway by sending and receiving ICMP timestamp control messages. These messages are now blocked on VPN gateway and VPN gateway will not respond to such messages.

Dashboard shows incorrect HDD usage

When disk usage is below 10%, the dashboard does not show the HDD usage correctly on the graph. The disk usage line goes out of the graph. The issue is fixed.

User cannot change password with AD/LDAP server

User is not able to change her password after login using domain credentials. The issue occurred after support for multiple authentication servers is added. The issue is fixed.

User can change password in older versions if the AD/LDAP server enforces password change because of password policies.

Security officer can be denied login if her group is blocked

If the group of security officer is added to blocked groups on VPN Domain configuration screen, the security officer won't be able to login. This can accidentally lock the VPN administrators out. The issue is fixed to allow the security officers login even if their group is blocked.

User Session Lockout issue on using different adaptors

In a very common scenario, a user can forget to logout from one network of the VPN and then move to a different network and try to login from there which can block the user from login. For e.g. a user from his home can login using her wireless network and without logging out of VPN she moves out of home. Now if she tries to login into VPN again but using a mobile network (like GSM/CDMA) using a data card, she won't be allowed to login as she will be using a different network adaptor.

In such case user cannot login even when using the same machine as the older session is still live in pending state. Either the user has to wait for session to expire or call administrator to force fully log her out from VPN.

The issue has been resolved. Now a user can use any type of network and she would be able to login as long as she is using the same machine.

Note: User must have at least 1 ethernet/wireless network interface card on her machine. Without such an adaptor, user will never be able to login into VPN.

Supporting Hardware with 10 or more network interface cards

SSL VPN gateway is not able to support when the no. of network interfaces on the hardware increases to 10 or more. Also if the OS detects the network interface names like eth10, eth11, ...eth24 , etc., the VPN gateway cannot handle such longer names. The issue is resolved to support longer interface names.

Serial Console Redirection of VPN OS Console Menu

The VPN OS Console menu is rewritten from a dialog based menu to a text based menu to support serial console redirection.

VPN Client login is slow when no. of applications is large

When the user has access to large no. of applications, the VPN client takes too much time "Setting up services". The issue is fixed. The VPN Client login time is improved and now it takes few seconds only.

VPN Client: Network Connection Timeout Error

VPN Client would sometime report "Network Connection Timeout" Error. The reason for the problem could be:

- Authentication server taking too much time to authenticate the user
- Slow connectivity to VPN gateway

The VPN Client timeout was set to only 10 seconds. The same has been increased to 90 seconds.

MAC Address for CDMA/GSB Mobile Internet Data cards

The mobile internet data card (GDM/CDMA) does not report unique MAC addresses on different machine. Either such data cards do not have a MAC address or they have a default MAC address as "00:53:45:00:00:00". VPN gateway uses MAC ID of the user to perform some validation. It's required that every user logging into VPN must report unique MAC IDs.

The issue is fixed by using the MAC ID of the first found Ethernet/wireless adaptor on the machine when the user is using such a mobile internet data card.



Propalms Ltd is a global provider of application delivery and secure remote access solutions for Terminal Services and Virtual Desktop Infrastructures. Delivering to Enterprises of all sizes we offer reliable, scalable and affordable solutions that simply work. Our belief is that application delivery solutions should be flexible, dynamic and above all, simple to use.

© 2011 Propalms Ltd. All Rights Reserved. Microsoft®, Windows® are registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.