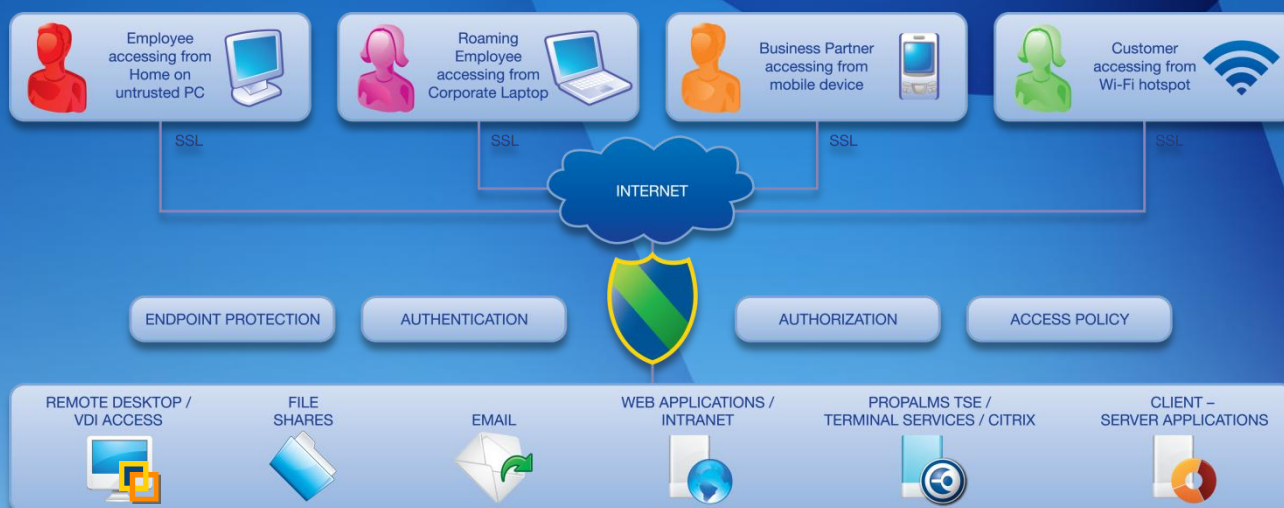




Propalms VPN

Propalms VPN is an easy-to-use, secure remote access solution (SSL VPN)



Today, organizations of all sizes face the pressure to be able to deliver applications and data to ever increasing numbers of mobile workers. Whether this is home users, roaming users, customers or even business partners the need for a Secure Remote Access solution that is easy to use and yet secure is the key requirement; this is where Propalms VPN can help.

When implementing a VPN it is important for organizations to consider the VPN technology. Current VPNs whether IPsec or SSL VPNs rely on layer 2 VPNs to provide seamless access to applications. This creates a security hole in perimeter security deployed at the corporate network level and opens up the network to unknown vulnerabilities generated from unmanaged desktop machines. It should be noted that the requirement is to deliver the application and network services to end-users rather than necessarily bridging unknown endpoints to corporate networks at untrusted locations.

Propalms VPN is an application gateway that provides secure access to the applications using standards based SSL encryption. Propalms VPN enables access to specified applications only, rather than bridging end-user's machines with the corporate network, while still maintaining full application compatibility. Propalms VPN comes with unique network obfuscation feature which hides the internal network details from intentional or unintentional exploitation by a user or hacker.

Propalms VPN brings together the performance, management and functionality required for enterprise remote access and reduces costs traditionally associated with other VPN solutions due to the simplicity and ease of use of our solution united with our low license costs.



SPAN TECHNOLOGY

Propalms SPAN (Secure Private Application Network) technology enables a completely secure access method over any kind of network and devices. With SPAN technology, Propalms VPN can make applications available without bridging client device's network with the corporate network. Other VPN solutions require a network adaptor with virtual IP Address for full functioning of client-server applications. SPAN technology has following salient features:

- Secure remote access without creating unsecured holes in the network's perimeter security.
- Makes application access possible without a virtual adaptor or routing changes on endpoint machine.
- Network information obfuscation. User can never find the actual IP address of hostname of the internal servers.
- Administrator can control each application available over VPN rather than opening up the whole network/subnets.

SECURE AUTHENTICATION

Propalms VPN uses standards-based SSL/TLS Security. Users can be authenticated by methods such as Active Directory, LDAP, and RADIUS or local database. Fully integrated client-certificate based two factor authentication with automatic certificate provisioning is in built in to the VPN. Configurable Authentication and Authorization servers mean that users can login using multiple methods and still have resources assigned by group or role.

ACCESS YOUR APPLICATIONS

Access all of your Applications, including all TCP and UDP applications such as HTTP/S and FTP based apps, RDP, Email, Windows File sharing and Propalms TSE and VDI. Even custom or proprietary applications and protocols are supported by Propalms VPN. In-built application templates help administrator create standard applications as well as define additional parameters.

WEB PORTAL

Users login to a customized Web Portal which displays the applications available to them along with admin messages, VPN client status, endpoint security result and change password options. Administrators can now customize the VPN portal directly from the 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.

HARDENED PROPALMS OS

The VPN application runs on Propalms OS 3 which is a security hardened, enterprise class Linux Distribution derived from CentOS. Propalms OS hosts the required services for running Propalms VPN and is maintained by Propalms Support Team.

32-BIT & 64-BIT VERSIONS

The VPN ISO based on CentOS is available for both 32bit as well as 64bit hardware platforms. The ISO for 32bit hardware can be installed on 64bit hardware. With support for 64bit platform a large amount of RAM and CPU power can be made available to VPN gateway for scalable deployments.

VPN APPLICATION LAUNCHER

The VPN Application launcher is a simple user interface for users to launch their applications when logging in through the VPN desktop client. After login, the Application Launcher is shown to the user with the list of applications the user has access to. The following applications can be displayed:

- Propalms TSE applications
- Virtual desktops from Propalms VDI
- Web applications
- Remote Desktop Connections (MyDesktop)
- Remote Meeting

VPN PORTAL – KIOSK MODE

Kiosk mode allows users to access certain applications without requiring any client software. Propalms VPN web portal delivers a set of Java applications enabling access to:

- Remote Desktop Connections
- File Transfer Protocol Applications
- VNC Applications
- File share Application
- Telnet Application
- Propalms VDI/TSE
- Citrix Web (including Citrix ICA)
- Remote Meeting

MY DESKTOP

MyDesktop feature provides direct access to your office PC via Propalms VPN. Administrator can create a 'MyDesktop' application type and upload a list of usernames along with their desktop hostnames/IP addresses. When users login into VPN an application with the name 'MyDesktop' is displayed on the VPN Portal. User can access their desktop by simply clicking the icon in the VPN Portal or Application Launcher.

PROPALMS TSE INTEGRATION

Propalms VPN works in conjunction with Propalms TSE solution to deliver a highly efficient application delivery solution to enterprises. Propalms TSE provides presentation virtualization and VPN provides secure remote access. Propalms VPN enables single sign-on, Web Portal & Desktop integration features for Propalms TSE enabled applications.

PROPALMS VDI INTEGRATION

Propalms VPN integrates with Propalms VDI to deliver a seamless access mode to VDI managed virtual desktops. VPN administrator can publish the Propalms VDI setup for roaming users by simply creating an application with a target as the Propalms VDI connection broker. Propalms VPN talks to the Propalms VDI connection broker and publishes user's allocated virtual desktop on the Propalms VPN portal.

REMOTE MEETINGS

The remote meetings feature offers authorized VPN users the ability to perform remote web meetings for the purpose or sharing presentations, text chat, file transfer or just use as a helpdesk facility. Remote meeting feature is available in both VPN Portal and VPN desktop 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.

ENDPOINT SECURITY

Enforces access restrictions based on customizable policies such as Anti-virus, Anti-spyware and firewall status ensuring devices are 'safe' for connection to the network. IP and Mac address restrictions can also be enforced.

GRANULAR ACCESS CONTROL

Administrators can create policy based access controls for restricting users to specific applications and resources and preventing unauthorized access. Access controls are based on device identity and profile, user authentication method and role with time-based restriction policies for further lockdown capabilities.

SITE TO SITE ACCESS

Propalms VPN provides a unique Site-to-Site access feature where it is possible to chain the Propalms VPN gateway and access applications across sites. Other VPNs either provide IPsec based site to site or their SSL based Site-to-Site is layer 2 tunnel which suffer from poor performance because of too much packet loss. (Read 'TCP-over-TCP meltdown').

EASY MANAGEMENT

Web based Management Interface with real-time dashboard updates and in-line help make administration simple. Delegated administration and secure, certificate based login for Administrators ensures that the VPN is protected against unauthorized admin access.

DEPLOYMENT

Install in minutes using a simple, integrated installer or save even more time by downloading the Propalms VPN Virtual Appliance and import it directly into your VMware infrastructure or your other chosen virtualization platforms.

ONLINE LICENSE SERVICE

Online licensing portal allowing customers to login and manage their licenses and activate them. Activation can also be performed directly from the VPN management console further simplifying the whole process.

HIGH AVAILABILITY & PERFORMANCE

Scalable to thousands of users with built-in Load Balancing, Propalms VPN can automatically distribute application network traffic among multiple VPN Servers with integrated failover to available servers.

CLIENT ACCESS

Propalms VPN supports Windows, Mac OS X and Linux platforms. Users can access the VPN either through a Web Portal (Java), On-demand VPN Agent (ActiveX) or locally installed Desktop Client.

iPAD & ANDROID SUPPORT

Propalms VPN provides access to business applications and desktops from iPad and Android based tablet devices. The Propalms Universal Client available from the Apple App Store and Android Market allows access to both TSE and VDI applications via the VPN.

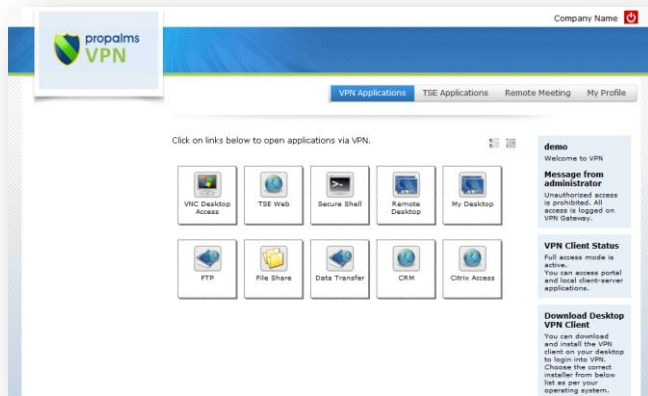
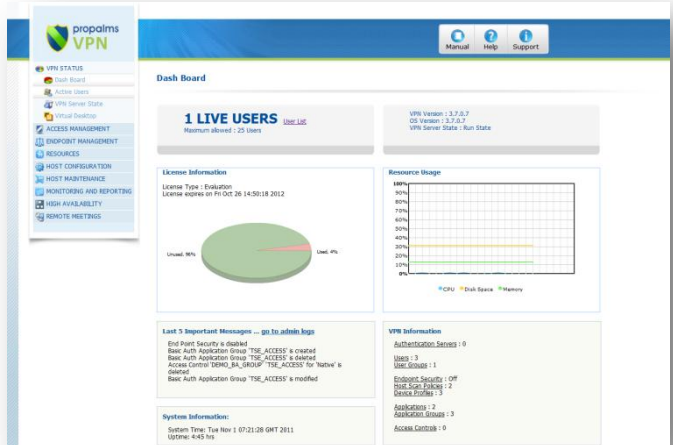


Web Based Management

The Propalms VPN solution has an intuitive, easy to use web interface with graphical dashboard allowing administrators to deploy, configure and monitor the VPN server from any web browser. Administrators can login using high-security, certificate based authentication providing an extra level of security.

Administrators can perform tasks such as:

- Create/add users (native, LDAP, Active Directory).
- Create applications (application templates included)
- Create user and application groups for defining access to applications.
- Control device access using endpoint policies and zones.
- Enable high availability.
- Configure remote meeting and view live sessions.
- Specify time-based access restrictions.
- View reports and manage current sessions.
- And more...



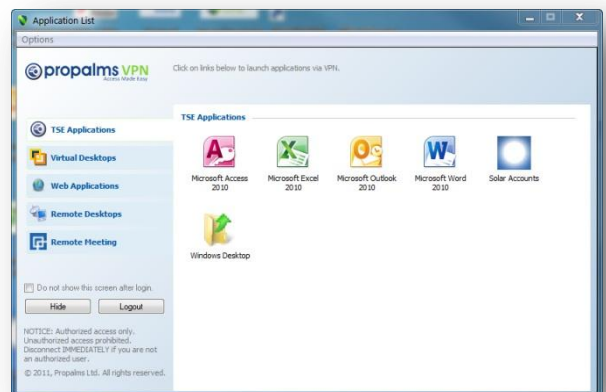
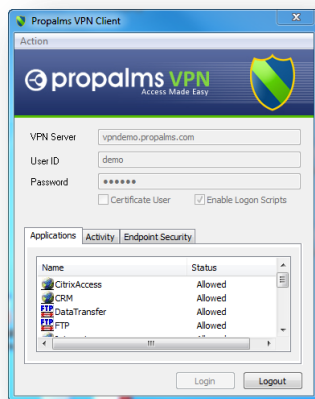
VPN Web Portal...

The VPN Web Portal enables web based access to standard applications such as HTTP/S, RDP, VNC, FTP, Fileshare and terminal resources Telnet and SSH. Users can browse to the portal and login with their username and password to get access to their authorized applications and resources. The VPN client is downloaded on demand and any updates are applied automatically easing the management and support overhead. Once authenticated through the portal, users can access all client-server applications published to them not just the application types that appear on the portal.

The portal also integrates with Propalms TSE and Propalms VDI providing secure, seamless access to remote desktop applications and hosted desktops respectively. User can also collaborate with other users using the Remote Meeting feature.

...VPN Desktop Clients

Propalms VPN has client support for Windows, Mac OS X and Linux. Simply open the VPN portal website and click on the client that you require and installation will happen instantly. The desktop clients remove the need for VPN users to have to login to the Web Portal each time in order to access their corporate applications and resources. The desktop client includes the VPN Application Launcher, a quick access area for launching Web Applications and TSE/VDI sessions through VPN.



...and iPad / Android Access

Propalms Universal Client provides access to applications and windows desktops from your iPad or Android tablet device whether you are in the office, at home or mobile. The universal client connects to Propalms TSE, VDI and VPN solutions offering the ability to use business applications such as Microsoft Office running from Remote Desktop Services or Virtual Desktops hosted on hypervisors such as VMware and Parallels.





<p>MANAGEMENT</p> <ul style="list-style-type: none"> • Web based management console • Dashboard with graphical reporting • Menu driven console interface for system configuration • Wizard driven installation procedure • Self-signed certificate generation • CLI • Delegated administration • Certificate based strong authentication for administrators • Auto checking for configuration errors • Online License service 	<p>APPLICATION SUPPORT</p> <ul style="list-style-type: none"> • All web based, TCP and UDP based client-server applications • Windows file shares and drive mapping • Dynamic port based applications • Special support for RDP virtual channels • Application load balancing • Session caching for load balanced applications • Per application based compression switch • MyDesktop for direct desktop access • Propalms TSE hosted applications • Propalms VDI hosted desktops 	<p>ACCESS SECURITY FEATURES</p> <ul style="list-style-type: none"> • SSL 3.0 and TLS 1.0 • Encryption: Strongest available: DES, 3DES, AES(256), RC4 • Authentication: MD-5, SHA-1, RSA 1024, RSA 2048 • Internet network masking and IP address/hostname mangling • Application level gateway and not layer 2 bridging • Hardened gateway operating system
<p>AUTHENTICATION FEATURES</p> <ul style="list-style-type: none"> • Authentication based on user identity, endpoint identity, endpoint trust level • Multiple user authentication options: static passwords, client certificates, external two factor authentication solutions • Local database with full customization per user, password policies, password reset support • Fully integrated client-certificate based two factor authentication server with automatic CA and certificate provisioning • Email based user provisioning • Authentication method based application access control • Integrates with AD/LDAP/RADIUS • Automatic fetching of group information from AD/LDAP/RADIUS • Support for multiple authentication servers with cascading mode • Support for external authorization servers 	<p>AUTHORIZATION FEATURES</p> <ul style="list-style-type: none"> • Publish applications rather than subnet or network • Simple access control mechanism • Access control based on <ul style="list-style-type: none"> ◦ Device identity and profile ◦ User Authentication method ◦ User Role • Dynamic policy evaluation based on run time information about device, authentication method and user role • Display of allowed applications and availability of the application server to users • Time based restriction policies • Auto-detection of applications running in corporate network • Scheduled account expiry • Block specific groups 	<p>AUDITING FEATURES</p> <ul style="list-style-type: none"> • Complete reporting of user logons and activity • Information logged includes <ul style="list-style-type: none"> ◦ Time of access ◦ Username ◦ MAC Address of endpoint ◦ IP address of endpoint ◦ Application accessed ◦ Device profile • Logging of endpoint security scans • Detailed logging per device scans including <ul style="list-style-type: none"> ◦ Policies evaluated for user sessions ◦ Current profile of endpoint ◦ List of failed policies ◦ List of policies for which remediation information is sent to user • Extract logs in CSV format for feeding to third part report generation • Auto-archiving of logs • Monitor and disconnect live users
<p>ENDPOINT MANAGEMENT</p> <ul style="list-style-type: none"> • Support for checking for antivirus, firewall and antispayware products • Real time status check for <ul style="list-style-type: none"> ◦ Last update time ◦ Real time protection check • Support for checking for MAC ID and IP address • Application control based on device profile • Mandatory profile for non-avoidable policy checks on all endpoints • Quarantine profile for devices that fails all other profile • Option to block endpoints that fails to comply to required policies or option to allow them to login by putting them in quarantine profile 	<p>ACCESS MODES</p> <ul style="list-style-type: none"> • Multiple access modes: <ul style="list-style-type: none"> ◦ VPN portal with java applications ◦ ActiveX browser agent for quick access ◦ Full access client for desktops • No configuration required on end user machines • Client platforms supported <ul style="list-style-type: none"> ◦ Windows 98/XP/Vista/Windows7 ◦ Windows server 2003/2008 ◦ Linux OS ◦ MAC OS X PPC/Intel 10.4 and above ◦ iPad / Android Access • Site to site access 	<p>DEPLOYMENT SCALABILITY</p> <ul style="list-style-type: none"> • Scalable to thousands of users • Active-Active N+1 cluster • VPN connections load balancing, multiple algorithms • Application connection load balancing can distribute the connection for a specific application across multiple app servers in the LAN based on round robin function • Session persistence: Users do not need to re-authenticate • 64-bit hardware support
	<p>GATEWAY FEATURES</p> <ul style="list-style-type: none"> • Runs on hardened Linux based platform • Menu driven console interface for easy configuration • Can run on any standard or custom hardware • Runs on virtualization platforms from VMware, XenServer, Hyper-V 	<p>COMING SOON...</p> <ul style="list-style-type: none"> • Layer 3 VPN mode • Integrated 2 factor authentication feature for OTP and SMS based authentication • VPN Portal for Linux and MAC OS X

Propalms Ltd

EMEA / APAC
Email: sales@propalms.com
Tel: +44 (0)1904 428760
Fax: +44 (0)1904 428701

USA
Email: sales@propalms.com
Tel: +1 407 571 6827
Fax: +1 407 571 6801

INDIA
Email: indiasales@propalms.com
Tel: +91 22 4090 7360
Fax: +91 22 4090 7340

