



Release Notes

Propalms VPN v3.7

Build - 3.7.0.7

November 2011

RELEASE HISTORY

<i>Release Version</i>	<i>Release Date</i>	<i>Type of Release</i>
3.4.0.1	March 21 st 2009	Major Release
3.4.0.2	May 05 th 2009	Minor Release
3.4.0.3	Jun 02 nd 2009	Minor Release
3.4.0.6	September 29 th 2009	Major Release
3.5.0.4	January 31 st 2010	Major Release
3.5.0.6	March 18 th 2010	Bug Fix Release
3.5.3.5	September 10 th 2010	Bug Fix Release
3.6.0.8	January 2011	Major Release
3.7.0.7	November 2011	Major Release

TABLE OF CONTENTS

RELEASE HISTORY	2
INTRODUCTION	5
Getting Propalms VPN 3.7 Virtual Appliance or v3.7 ISO Installer	5
Installing Propalms VPN v3.7 Release.....	5
Upgrading Propalms VPN to v3.7	5
Upgrading Propalms VPN v3.4.0.X to v3.7.....	6
NEW FEATURES IN VERSION 3.7	7
New Application Launcher in VPN Client.....	7
Online License Server	7
Tight Integration with Propalms VDI	8
New Propalms OS 3 (CentOS Distribution).....	9
64-bit Hardware Support.....	9
VPN Portal – Kiosk Mode.....	10
Device Authentication	10
SSO for Citrix XenAPP	11
Virtual IP Address for FTP Application	12
Improved User Interface.....	12
Updated Mac OSX Client	13
Updated Endpoint Security.....	13
File Share Support for Windows 7	13
Secure LDAP Server Support.....	14
Internet Explorer 9.0 Support.....	14
N+1 Clustering Support	14
OPEN ISSUES IN VPN 3.7.0.7	15
Restricted Ports cannot be created	15
VPN Portal does not work on ports other than 443	15

Release notes: Propalms VPN v3.7

VPN Portal cannot close opened windows when working in Internet Explorer 15

After using Remote Meetings, sometimes desktop wallpaper gets removed 15

“Backup and Restore” does not work from non-active load balancers..... 15

Missing Kickstart file error during ISO installation from a USB drive 15

Internal error on Security Officer login 16

File-share application works only on the Domain fileserver 16

All listed selectable SSL Ciphers does not work..... 16

Admin logs are not created for some admin operations..... 16

Error after password change in Mozilla Firefox..... 16

INTRODUCTION

This release notes document describes the features introduced and issues fixed in Propalms VPN v3.7.0.7

GETTING PROPALMS VPN 3.7 VIRTUAL APPLIANCE OR V3.7 ISO INSTALLER

Propalms VPN 3.7 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>

INSTALLING PROPALMS VPN V3.7 RELEASE

Propalms VPN 3.7 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.

The Propalms VPN ISO 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.

UPGRADING PROPALMS VPN TO V3.7

In order for a customer to upgrade to Propalms VPN 3.7 with the new Propalms OS3 a new installation is required. To restore the settings of existing Propalms VPN 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 v3.7 virtual appliance or reinstall VPN using v3.7 ISO.
3. During preboot stage, select option to restore VPN from a backup file.
4. On the restore screen, select the previously created backup file.
5. Your new v3.7 VPN is ready with same certificates and the entire configuration.

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

Release notes: Propalms VPN v3.7

NB: Please contact Propalms VPN support at vpnsupport@propalms.com for assistance if customer requires in-place upgrade from version 3.6 to v3.7 without re-installation.

UPGRADING PROPALMS VPN V3.4.0.X TO V3.7

VPN version 3.4 cannot be migrated directly to version 3.7. Please contact Propalms VPN support at vpnsupport@propalms.com for migrating from v3.4 to v3.7.

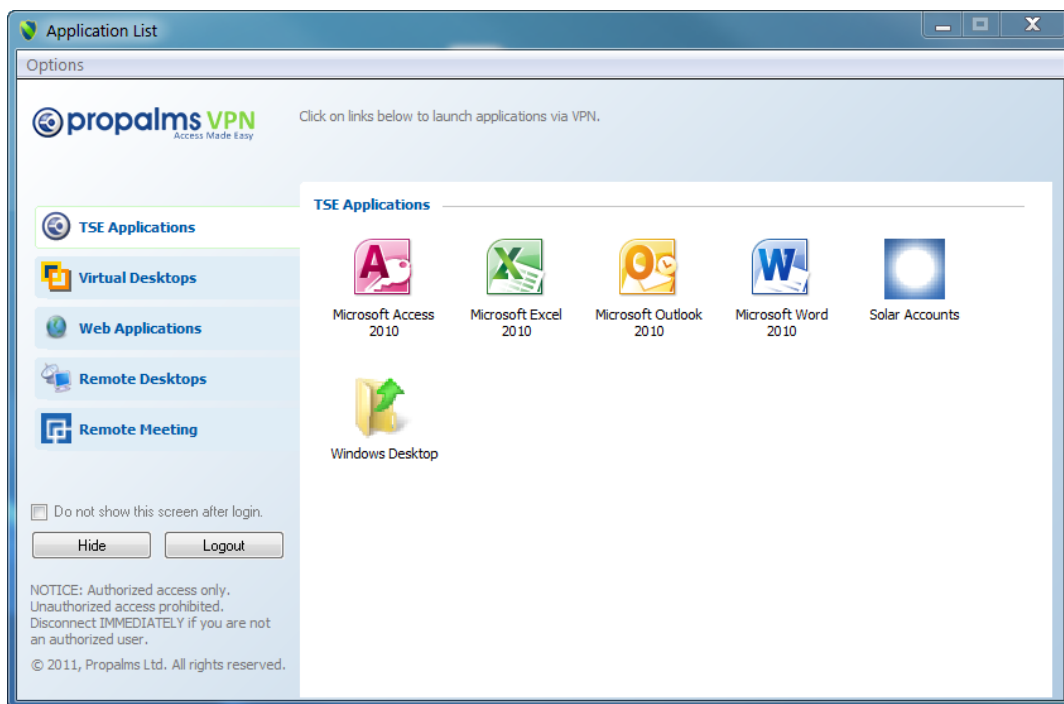
NEW FEATURES IN VERSION 3.7

NEW APPLICATION LAUNCHER IN VPN CLIENT

FEATURE DETAILS

The Application launcher of VPN Client is improved to add more applications with a better user interface. After login, the Application Launcher is shown to the user with the list of applications the user has access to. Following applications are shown to the user:

1. Propalms TSE applications
2. Virtual desktops from Propalms VDI
3. Web applications
4. Remote Desktop Connections
5. Remote Meeting



ONLINE LICENSE SERVER

FEATURE DETAILS

A new online license activation service is added in this release. Now license acquisition is a real time, secure automated system.

With the VPN software image/virtual appliance, the customer will get a Serial Key which will be used to retrieve the actual license. Before the administrator can use the Serial Key to get a new license, the administrator must register himself/herself and the organization with Propalms License Server. After registration is successful, administrator can click on "Retrieve License" to retrieve the license details from Propalms License Server.

Release notes: Propalms VPN v3.7

NB: Please refer to the Propalms VPN Administrator's Guide for more information on how to get and apply licenses from VPN version 3.7 onwards.

License Feature	Details	Status	Expiration Date
Concurrent Users	Production	25 Users	License Never expires.
Endpoint Security	-	License not available	-
Cluster	-	License not available	-
Silver Support	-	License not available	-
Gold Support	-	License not available	-

Get New License Update Profile

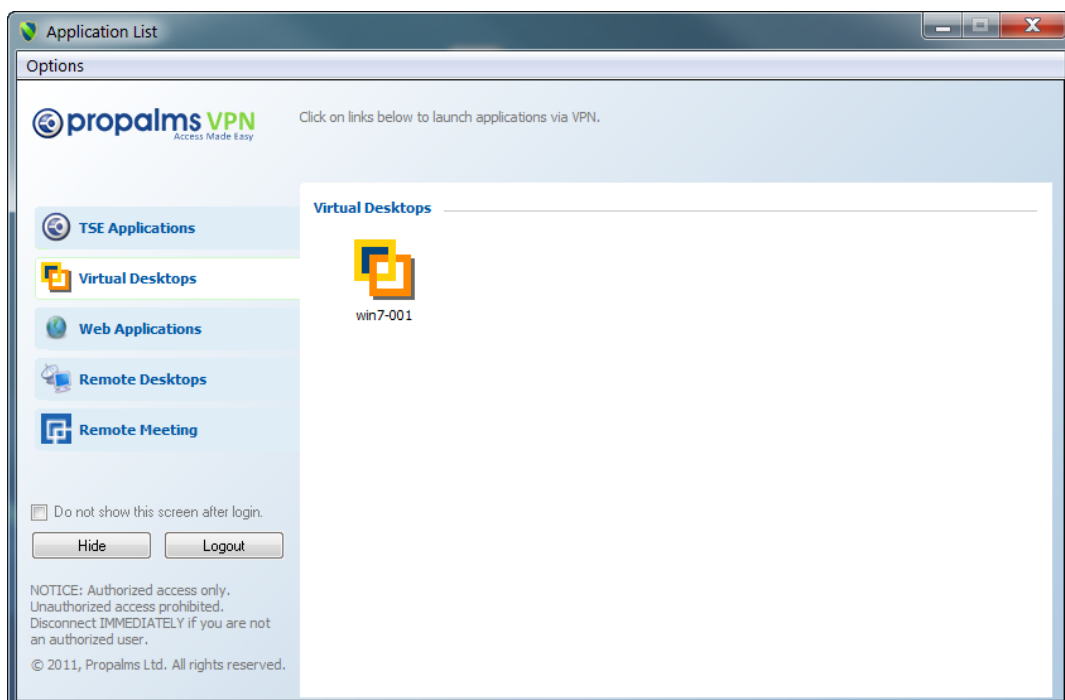
TIGHT INTEGRATION WITH PROPALMS VDI

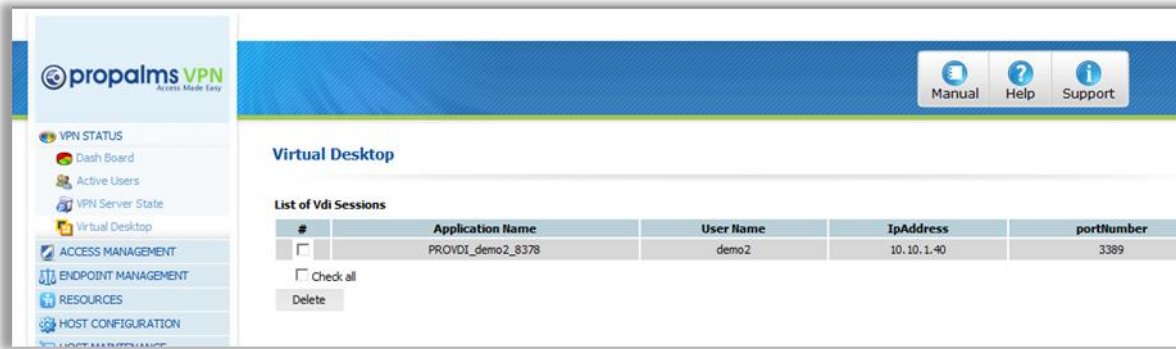
FEATURE DETAILS

In this release, if a user is provisioned a virtual desktop from Propalms VDI he/she can see the virtual desktop directly on VPN Portal and the new application launcher screen. There is no need for any additional VDI client configuration on the users' device as all features are provided by the VPN Portal and the VPN Client.

VPN Administrator must configure an application rule for Propalms VDI access. For single sign-on to work the credentials for VPN must be same as credentials for Propalms VDI for each user. This can be achieved if VPN is configured to use the same domain controller for authentication as VDI.

Administrators can see which virtual machine is assigned to the user on the VPN management console. There is a new screen added under VPN Status section on VPN Management console.





NEW PROPALMS OS 3 (CENTOS DISTRIBUTION)

FEATURE DETAILS

The new VPN runs on CentOS based Linux distribution. CentOS is the most commonly used free distribution derived from RHEL distributions. The new 3.7 VPN ISO contains the new hardened OS with an improved graphical installer.



64-BIT HARDWARE SUPPORT

FEATURE DETAILS

The new VPN ISO based on CentOS is available for both 32bit as well as 64bit hardware platforms. There are two different ISOs available and the customer must install the correct ISO on their specific hardware. The ISO for 32bit hardware can be installed on 64bit hardware though. With support for 64bit platform a large amount of RAM and CPU power can be made available to VPN gateway for scalable deployments.

VPN PORTAL – KIOSK MODE

FEATURE DETAILS

Kiosk mode is a new mode on the VPN portal such that users can access applications without requiring installation of the VPN client which requires user to have admin rights for first time.

Kiosk mode supports following type of applications published over VPN Portal:-

1. Remote Desktop Connections
2. File Transfer Protocol Applications
3. VNC Applications
4. File share Application
5. SSH/Telnet Application
6. Propalms VDI/TSE
7. Citrix Web (including Citrix ICA)
8. Remote Meeting
9. MyDesktop

In current release, after login into VPN, the Portal detects the type of applications user has access to. If user has access to applications supported by Kiosk Mode, then the portal starts working in Kiosk mode. In case user has access to any other application out of those mentioned above, the portal works in full access mode. In that case full VPN client will be downloaded and installed if the latest compatible VPN client is not installed already.

DEVICE AUTHENTICATION

FEATURE DETAILS

Device Authentication is a newly integrated two factor authentication feature in Propalms VPN. Device authentication requires user to register their device with Propalms VPN Gateway. Each user receives an activation code in their email that they can use to register their device. Propalms VPN integrates with EZMCOM authentication server which stores a unique identification of the user device. User must also create a device PIN which user must remember and use again during login process.

During login process, user needs to enter their domain username, domain password and device PIN.

If the device PIN matches with the device PIN created during device registration, the VPN Portal generates a unique one-time-password using the user registration information. The domain username, password and the one-time-password is then sent to Propalms VPN gateway which verifies the details with EZMCOM server. If all the details are correct, user can login.

propalms VPN
Access Made Easy

Welcome to Propalms VPN login

Unauthorized access is prohibited. All access is logged on Propalms VPN Gateway.

Authentication Method: Device Authentication

Username: [Register the Device!](#)

Password:

Device Pin:

Sign In

Welcome to Propalms VPN login

Unauthorized access is prohibited. All access is logged on Propalms VPN Gateway.

Authentication Method: Device Authentication

Username: [Register the Device!](#)

Password:

Device Pin:

Sign In

Register device.

Activation Code: 98384028486081

Device Pin: ●●●●●●

Confirm device Pin: ●●●●●●

[Submit](#) [Cancel](#)

Welcome to Propalms VPN login

Unauthorized access is prohibited. All access is logged on Propalms VPN Gateway.

Authentication Method: Device Authentication

Username: [Register the Device!](#)

Password:

Device Pin:

Sign In

SSO FOR CITRIX XENAPP

FEATURE DETAILS

If there is a Citrix XenApp application published, on user login, Single Sign-on is enabled for Citrix web portal. User need not authentication to Citrix XenApp portal after login into VPN.

VIRTUAL IP ADDRESS FOR FTP APPLICATION

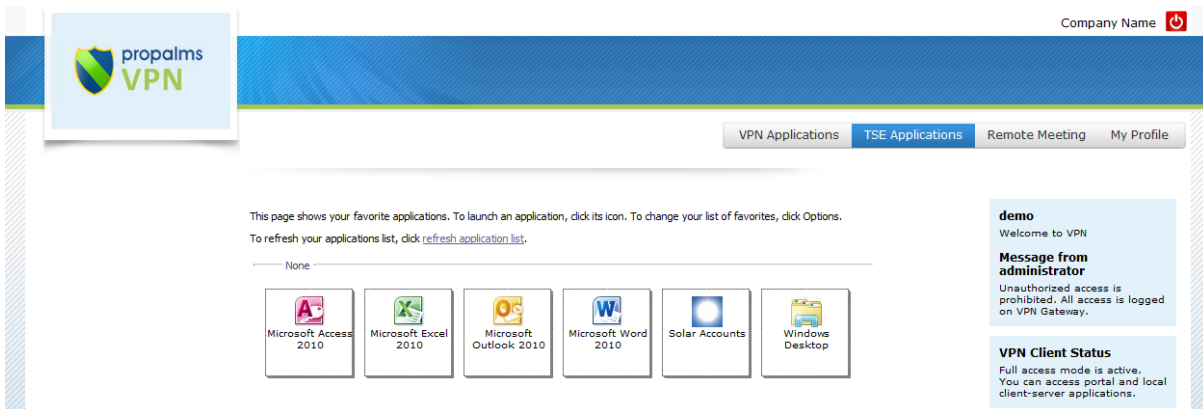
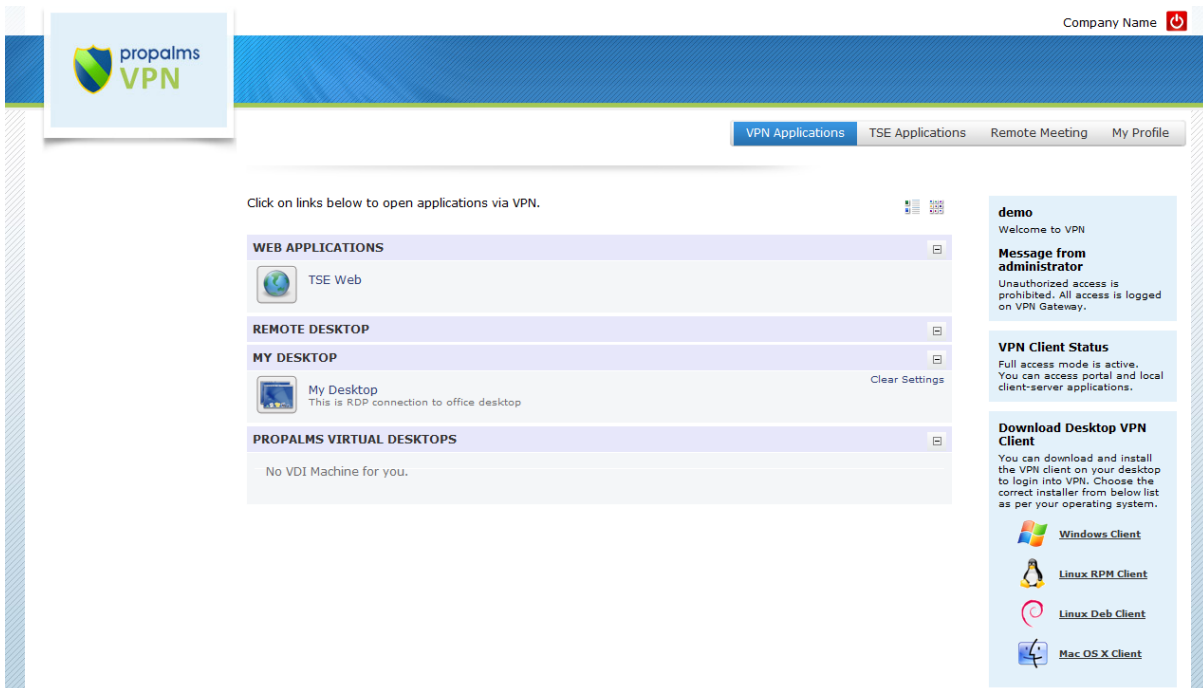
FEATURE DETAILS

In last release, FTP application could not work on Internet explorer 8 when Virtual IP address is enabled for this application. To make FTP application work, we needed to disable the virtual IP address. This release fixes this by implementing an application layer gateway for FTP applications. FTP application can now be accessed with Virtual IP address feature turned on.

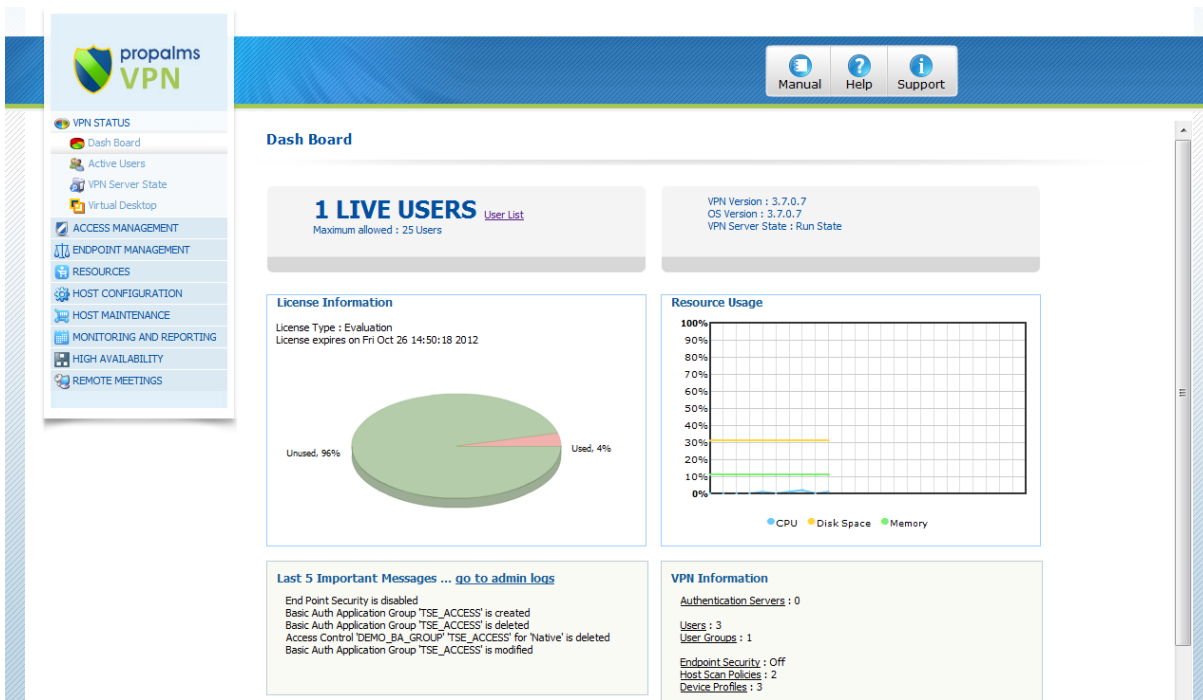
IMPROVED USER INTERFACE

FEATURE DETAILS

The web user interface has been improved across all modules.



Release notes: Propalms VPN v3.7



UPDATED MAC OSX CLIENT

FEATURE DETAILS

The new MAC OSX VPN Client provides tight integration with Propalms TSE and can display the TSE applications directly on Propalms VPN application user interface. The VPN Client installer also includes the latest Microsoft Remote Desktop Client installer such that a user can simply install the VPN client and get TSE as well as RDP applications.

UPDATED ENDPOINT SECURITY

FEATURE DETAILS

The new release includes updated Endpoint Security Modules.

FILE SHARE SUPPORT FOR WINDOWS 7

FEATURE DETAILS

The new VPN client on Windows 7 32bit OS supports drives mapping and shared files and folders. This will enable users to map drives over VPN or use UNC path to access shared files and folders.

Refer to the table below to understand how file sharing is supported.

Operation systems	VPN Portal	VPN Desktop Client
Windows XP 32 bit	Yes	Yes
Windows XP 64 bit	Yes	No
Windows Vista 32 bit	Yes	No
Windows Vista 64 bit	Yes	No
Windows 7 32 bit	Yes	Yes
Windows 7 64 bit	Yes	Next Release
Windows 2003 server SP2 or higher, 32bit	Yes	Yes
Windows 2003 server SP2 or higher, 64 bit	Yes	No
Windows 2008 server 32 bit	Yes	No
Windows 2008 server 64 bit	Yes	No
Windows 2008 server R2 64 bit	Yes	Next Release

SECURE LDAP SERVER SUPPORT

FEATURE DETAILS

VPN Gateway can now talk to LDAP or Active Directory server using secure LDAP protocol. This enables more secure communication between VPN gateway and directory server.

INTERNET EXPLORER 9.0 SUPPORT

FEATURE DETAILS

Microsoft Internet Explorer 9.x browser is now supported for VPN Portal and Administration Console.

N+1 CLUSTERING SUPPORT

FEATURE DETAILS

This release supports more than 2 VPN gateways in a cluster. The N+1 cluster is tested for 8 VPN gateways in a cluster.

OPEN ISSUES IN VPN 3.7.0.7

RESTRICTED PORTS CANNOT BE CREATED

Issue: Restricted ports cannot be created.

Resolution: The issue will be fixed in next service pack release

VPN PORTAL DOES NOT WORK ON PORTS OTHER THAN 443

Issue: If VPN gateway is configured to run on port other than 443, VPN portal does not work correctly

Resolution: This issue will be fixed in next service pack

VPN PORTAL CANNOT CLOSE OPENED WINDOWS WHEN WORKING IN INTERNET EXPLORER

Issue: After user has logged out from VPN portal, the application windows opened from the portal are not closed. This works for Firefox browser though.

Resolution: The issue will be fixed in next service pack release.

AFTER USING REMOTE MEETINGS, SOMETIMES DESKTOP WALLPAPER GETS REMOVED

Issue: On some machines, randomly, the desktop wall paper will get removed and black color would be set as desktop color after a remote meeting session has ended.

Resolution: Restarting the user machine will fix this problem. The issue will be fixed in next service pack release.

“BACKUP AND RESTORE” DOES NOT WORK FROM NON-ACTIVE LOAD BALANCERS

Issue: In a VPN cluster, it's not possible to take backup of VPN settings from a VPN machine which is not running the active load balancer. It is also not possible to restore the configuration.

Resolution: VPN settings backup should be taken only from machine which is running active load balancer. Administrator should login directly into active load balancer to do backup and restore operations. For restoring settings for the whole cluster, restore the settings only on active load balancer. The settings will migrate to the whole cluster automatically within 5 minutes.

MISSING KICKSTART FILE ERROR DURING ISO INSTALLATION FROM A USB DRIVE

Issue: While Installing VPN ISO on some hardware, missing kick start file error is displayed.

Release notes: Propalms VPN v3.7

Resolution: The error is not fatal. Select OK to continue installation. The same error may prompt for 2 or 3 times. Keep clicking OK till the error is gone. If the error does not go, the boot options may not be correct. Check bios if the correct USB bootable options are selected and at the installation boot prompt specify the correct USB install command line.

INTERNAL ERROR ON SECURITY OFFICER LOGIN

Issue: If Security Officer Enrolls through Portal and try to login immediately after enrollment, browser may report and internal error. This happens randomly on Internet explorer and Firefox browsers.

Resolution: Close the Browser and login again.

FILE-SHARE APPLICATION WORKS ONLY ON THE DOMAIN FILESERVER

Issue: File-share Application works only if the target file share server is part of a domain.

Resolution: File-share server should be in a Domain.

ALL LISTED SELECTABLE SSL CIPHERS DOES NOT WORK

Issue: Though several different SSL Ciphers are listed on VPN management console for selection, only following SSL Ciphers work:

TLS_TXT_RSA_RC4_128_MD5

TLS_TXT_RSA_RC4_128_SHA

SSL3_TXT_RSA_RC4_128_MD5

SSL3_TXT_RSA_RC4_128_SHA

Resolution: Select at least one of these ciphers for clients to be able to connect

ADMIN LOGS ARE NOT CREATED FOR SOME ADMIN OPERATIONS

Issue: Admin Logs are not created for Remote Meeting configuration and Cipher selection.

Resolution: Issue will be fixed in next service pack release

ERROR AFTER PASSWORD CHANGE IN MOZILLA FIREFOX

Issue: In Firefox, if user changes the password from VPN Portal and tries to login again without closing the Browser, error is displayed.

Resolution: Close the Browser and login again.