Pulse Secure

Pulse Secure Access Service

Release Notes

Build	**27973**
Published	**June 2015**
Version	**8.0R1**
Revision	**01**

Contents

Introduction

These release notes contain information about what is included in this software release: supported features, changed features, unsupported features, known issues, and resolved issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Hardware Platforms

You can install and use this software version on the following hardware platforms:

- SA2500, SA4500, SA4500 FIPS, SA6500, SA6500 FIPS
- MAG2600, MAG4610, MAG6610, MAG6611, MAG SM160, MAG SM360

To download software for these hardware platforms, go to **http://pulsesecure.net/support**

Virtual Appliance Editions

This software version is available for the following virtual appliance editions:

- Demonstration and Training Edition (DTE)
- Service Provider Edition (SPE)

Table 1 on page 3 lists the virtual appliance systems qualified with this release.

Table 1: Virtual Appliance Qualified Systems

Platform	Qualified System
VMware	• IBM BladeServer H chassis • BladeCenter HS blade server • vSphere 5.1, 5.0, and 4.1

KVM	• QEMU/KVM v1.4.0
	• Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz
	  • NFS storage mounted in host
	  • 24GB memory in host
	  • Allocation for virtual appliance: 4vCPU, 4GB memory and 20GB disk space

To download the virtual appliance software, go to **http://pulsesecure.net/support**

Upgrade Paths

Table 2 on page 4 describes the tested upgrade paths.

Table 2: Upgrade Paths

Release	Description
7.1R16 to 8.0R1	You can upgrade directly to 8.0R1 simply by installing the 8.0R1 update. We have tested this upgrade path.
Earlier than 7.1R16	First upgrade to release 7.1R16 or later; then upgrade to 8.0R1.

Note: If your system is running Beta software, roll back to your previously installed official software release before you upgrade to 8.0R1. This practice ensures the rollback version is a release suitable for production.

New Features

Table 3 on page 4 describes the major new features that are introduced in this release.

Table 3: New Features

Feature	Description
Active Directory integration	Support for AAA with the Active Directory server version released with Windows Server 2008 R2, including support for Samba modules.
	Support for integration with the Active Directory server version released with Windows 2012. Standard configuration procedures apply. No new user documentation. For information on integration with Active Directory, see **Using Active Directory.**
Desktop client environment	Support for Pulse desktop client and browser-based access; Host Checker, JSAM, Pulse Collaboration, and other components; for endpoints running the Apple OS X 10.9 operating system. No configuration required. No new user documentation. See the **Pulse Secure Access Service Supported Platforms Guide** for a list of features compatible with OS X 10.9 endpoints.
Desktop client environment	Support for Pulse desktop client and browser-based access; Host Checker, Network Connect, Terminal Services, WSAM, and other components; for endpoints running the Windows 8.1 operating system. No configuration required. No new user documentation. See the **Pulse Secure Access Service Supported Platforms Guide** for a list of features compatible with Windows 8.1 endpoints.

Table 3: New Features *(continued)*

Feature	Description
Diagnostic tools	Added a diagnostic logging tool for Samba. For information on diagnostic logging tools, see **Using the Samba Diagnostic Log**.
File browsing resource access policy	Support for file browsing resource access policy configuration with the CIFS version released with Windows 2012. Standard configuration procedures apply. No new user documentation. For information on file browsing resource access policies, see **Creating a File Rewriting Resource Profile.**
FIPS	Additional support for FIPS Level 1: • Support of FIPS 140-2 compliant operation mode for desktop Pulse. • TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS cipher suite additions. • Addition of three FIPS-compliant EAP protocols (EAP-TTLS, EAP-PEAP, EAP-TLS) for MAG FIPS with UAC personality. For information on FIPS, see the **FIPS Certification Guide.**
Google Chrome support	Support for endpoint access from a Google Chrome browser. No configuration required. No new user documentation.
Host Checker	Improved logmessageswhen a rulematches. See **Using Host Checker Reports and Logs.**
IPv6	IPv6 support for active/passive clusters. See **Example: Creating an Active/Passive Cluster that Supports IPv6 Client Access.**
	Support for IPv6-in-IPv6 tunnelling. For an overview of IPv6 support, see **Using IPv6.**
Maintenance tools	Enhancements to the automatic version monitoring feature. For information on enabling version monitoring, see **Configuring System Maintenance Options.**
MDM integration	Integration with AirWatch and MobileIron MDMs so that MDM device attributes can be used in role mapping rules. See **Device Access Management Framework Feature Guide.**
RADIUS integration	Support for RADIUS change of authorization disconnect messages. For information on RADIUS server integration, see **Using a RADIUS Server.**
SAML	A new SAML IdP configuration option to improve the rewriter's handling of interactive traffic. It applies to deployments with the Secure Access Service acting as a SAML identity provider (IdP) and the backend resource is protected by a SAML service provider (SP). For information on the SAML IdP configuration, see the **SAML Feature Guide.**

Table 3: New Features *(continued)*

Feature	Description
SAML	A new SAML SP configuration option to support RequestedAuthnContext context class specifications. For information on the SAML SP configuration, see **Using the SAML Server.**
	Support for Pulse client access to Secure Access Service when it is deployed as a SAML SP. Previously, users must use a browser in SAML deployments.
Secure Mail resource profiles	A new feature that enables policy-based access to Microsoft Exchange from iOS mobile devices. For information on Secure Mail resource profiles, see **Configuring Secure Mail.**
VPN Tunneling	Configuration enhancements for the VPN Tunneling split tunneling feature. See Defining **Split Tunneling Network Policies.**
Web application resource policy	Support for Exchange Server and Outlook Web Access (OWA) 2013. Standard configuration procedures apply. No new user documentation. For information on Web application resource policies, see Creating **Resource Profiles Using the Microsoft OWA Template.**
Web compression resource policy	Support for Web compression resource policies (gzip compression) on MAG Series platforms. No new user documentation. For information on Web compression resource policies, see **Writing a Web Compression Resource Policy.**
Reporting	A new dashboard and tabular reports that give details on user access, device access, and endpoint compliance. For information on the dashboard, see the **Dashboard Feature Guide.**
Virtual appliance	New features that enable you to run SA and IC virtual appliances as a guest OS on any Linux machine with KVM Hypervisor support. For information on virtual appliances, see the **Virtual Appliance Deployment Guide.**

Changed Features

Table 4 on page 6 describes changes to features that you might observe when you upgrade.

Table 4: Changed Features

Change	Description
Active Directory integration	Support for AAA with the Active Directory server version released with Windows Server 2008 R2, including support for Samba modules. When you upgrade, you will notice two configuration modes for the Active Directory integration: • Active Directory standard configuration. Supports interoperability with any version of Active Directory, and is the required configuration mode to support authentication using MS-CHAP v2 with Windows 2008 R2 Active Directory Service. Machine authentication, for example, uses MS-CHAP v2.

Table 4: Changed Features *(continued)*

Feature	Description
	• Active Directory Legacy Mode configuration. Supports interoperability with Active Directory versions Microsoft 2003 or earlier. You might choose to use the Active Directory Legacy Mode configuration as your primary configuration if you require role-mapping rules to use "domain local groups" of trusted child domains. The Active Directory standard configuration does not support "domain local groups" for authorization. You can also use an LDAP server as the directory server if you want to use domain local groups in role mapping. For information on integration with Active Directory, see **Using Active Directory**.
Dynamic Policy Evaluation	Please note the following changes to Dynamic Policy Evaluation for this release: • Clients that use Network Communications Protocol (NCP) do not honor policy changes. This includes NC, WSAM, Pulse Collaboration, and WTS/CTS. • NC has a persistent NCP control channel. NC does not get this new policy until NC is disconnects and attempts to reconnect by the user. When NC reconnects via the UI level (NC service reconnect times out), it will obtain the new policy. • WSAM establishes a new NCP tunnel when the protected application opens a new connection, so WSAM establishes new NCP connections frequently. This means WSAM gets the new policy frequently. • Pulse Collaboration has a persistent NCP data channel, so Pulse Collaboration will not get the new policy. The down side of Pulse Collaboration not getting the new policy is not significant because Pulse Collaboration only tunnels its own data traffic. • WTS has a persistent NCP tunnel so it does not get policy changes until the user disconnects and then reconnects.
ForceAuthn Parameter	The ForceAuthn parameter, used by SAML 2, is set to False and is non-configurable.

Unsupported Features

Table 5 on page 7 lists problem reports that are resolved with the conclusion that the product does not support the use case scenario.

Table 5: Unsupported Features

Number	Description
925338	The Pulse Collaboration add-in is not supported on Outlook 2013.
924940	The AAA traffic segregation feature is supported only for the Active Directory legacymode configuration.
920148	On Mac, the Network Connect diagnostic option has been removed. There are no plans to add this back.
914086	Network Connect is not supported on Mac OS X 10.9.

Table 5: Unsupported Features*(continued)*

Number	Description
886797	When using the Google Chrome browse, client certificate authentication fails using ECC certificates. The Google Chrome browser does not support ECC certificates.
883202	Pulse Collaboration sharing features are not supported on Ubuntu 12.04 and Linux OpenSUSE 12.1.
852739	On Mac, with Java 7 and using Hob applet, users cannot type Spanish stress characters. It works if using Java 6.
832033	On Windows XP only, there is an issue with Access SharePoint 2010. In Explorer View, users cannot preview a picture in the Picture Library, and they cannot save a modified picture to a SharePoint server.
831664	On Windows XP only, there is an issue with Access SharePoint 2010. In Explorer View, the Send To option for a document returns an error.
824060	SAML is not supported with ECDSA certificates.
821285	The passthrough-proxy feature does not support EricomAccessnow. It is supported through rewriter.
812100	Rapid configuration of VA-SPE and VA-IC is not supported for IPv6 network configurations.
799312	Citrix Desktop Viewer toolbar is disabled.
744704	Pulse on Macintosh does not support the Safari browser “auto proxy discovery” settings.
680162	Some applications, such as Sticky Notes and Snipping Tool, cannot run inside Secure VirtualWorkspace.
683068	On Mac, the Network Connect client only supports running start / end scripts that are located on the local machine.
460540	On Windows XP, when Internet Explorer 8 is run InPrivate Browsing mode, Host Checker and Cache Cleaner do not function properly. Host Checker and Cache Cleaner do not support InPrivate Browsing mode.

Known Behavior

Table 6 on page 9 lists problem reports that are resolved with the conclusion that product behavior is not regarded as a bug or that the issue will not be addressed.

Table 6: Known Behavior

Number	Description
932856	Premier RDP Applets or HOB Applets with 8-bit color depth do not work on MacBooks with retina displays. This is a third party issue. The workaround is for administrator or user to configure color depth to 16-bit or 32-bit. (A user can configure color depth through RDP launcher.)
932430	Citrix JICA Applets do not have application name, permission, and codebase attributes in the jar manifest file. As a result, customers with Java 7 Update 45 see a warning when launching these applets. Only Citrix can fix this issue.
931408	When Pulse is launched from a Web browser running a version of Java earlier than Java 7 Update 45, Pulse 5.0 client users might be prompted by an additional dialog-box. This problem occurs because Java 7 Update 45 introduced a new security restriction that changes the way Web pages can interact with Java applets. To accommodate this Java Plugin change, the Pulse Desktop Setup Client Java applet manifest file had to change in a way that causes an additional prompt with pre-7.45 versions of Java. This change to Java is described in the following locations: **https://blogs.oracle.com/java-platform-group/entry/liveconnect_changes_in_7u45** **https://blogs.oracle.com/java-platform-group/entry/7u45_caller_allowable_codebase_and** The workaround to avoid the extra prompt is to upgrade the browser Java plugin to Java 7 Update 45 or later.
928210	On Pulse Collaboration, the Give Control option is disabled on attendee user interface if the host assigns the presenter role to an attendee during remote control and the attendee starts presenting.
927228	On the System > Configuration > Licensing page, the expand/collapse button to show and hide licenses stops working after using once. This occurs only with Internet Explorer 11.
922721	An issue was observed on Mac OS X 10.9 and on Mac OS X 10.8.5 with Safari 6.1. For JSAM to launch successfully, the end user must modify Safari preferences for the Java plug-in. In Safari, end users go to the Security tab / Internet plugins: manage website settings, and select the Java plugin. The Secure Access Service URL must be set to **Run in unsafe mode.**
920952	On Windows XP only, after Network Connect is installed with the standalone installer, and Network Connect is launched first time, it exits silently without displaying appropriate error message if the Secure Access Service does not assign an IP address. When NC is launched again, the correct error message is displayed: **The Secure Gateway denied the connection request from the client.**
920939	On Mac, Host Checker components are not loading with Network Connect standalone client. The workaround is to use browser in this situation.
919318	On rare occasions, Secure Virtual Workspace might not launch properly using the Firefox browser. If issues occur, the user receives a message **extracting of file neoSVWDlls.zip failed 32.** The workaround is to use the Task Manager to terminate the process ctfmon.exe.

Table 6: Known Behavior *(continued)*

Number	Description
918392	We have fixed an issue with how session values are set when the user signs into an "auth-only" sign-in page. Previously, the session values were populated with default profile settings. With the fix, the session value are populated with the values configured for the role. On the User Role > Web > Options page, there is an option to Allow browsing untrusted SSL Web servers. You should enable this option for roles allowed access to auth-only URLs to avoid performance impact. The reason is without this option, the Secure Access Service will verify the SSL certificate for each SSL connection that goes to auth-only URL.
918202	Expect the user interface to display over-allocated status if licenses are deleted on the license server. If all the licenses are deleted from the server, the server might display licenses as unavailable when third party subscription licenses are installed. Concurrent user licenses installed after the deletion will be displayed as available.
918003	In rare situations, Secure VirtualWorkspace fails to launch onWindows 7 (64-bit).
915262	On Windows 8, a new Internet Explorer browser window is opened when JSAM launches. This is an Internet Explorer issue.
914556	On Mac, upgrading Network Connect fromthemini browser froma pre-8.0 release to 8.0R1 does not work.
912652	An issue was observed on Mac OS X 10.9 and on Mac OS X 10.8.5 with Safari 6.1. The default action of blocking Java applets prevents the Pulse client from being deployed from the browser.
911545	An issue was observed on Mac OS X 10.9 and on Mac OS X 10.8.5 with Safari 6.1. For Pulse Collaboration to launch successfully, the end user must modify Safari preferences for the Java plug-in. In Safari, end users go to the Security tab / Internet plugins: manage website settings, and select the Java plugin. The Secure Access Service URL must be set to **Run in unsafe mode.**
910920	This is a behavior change in JSAM starting with 8.0. JSAM will not know the change in user session status until it tunnels any application traffic to the Secure Access Service. For example, after a user session has ended, JSAM continues to display status as ok instead of **session expired**. It changes to session expired only after application traffic is sent through JSAM.
907076	From the MobileIron VSP, VPN profiles are not provisioned properly to Mac OS X platforms. On MobileIron VSP, you will see "pending install" status in the device view
899517	An issue was observed on Mac OS X 10.8.5 with Safari 6.1. For Network Connect to launch successfully, the end user must modify Safari preferences for the Java plug-in. In Safari, end users go to the Security tab / Internet plugins: manage website settings, and select the Java plugin. The Secure Access Service URL must be set to **Run in unsafe mode.**
897070	The Secure Mail profile installed from one Secure Access Service system cannot be overwritten by another system. If a user tries to install Secure Mail from a different Secure Access Service system, the profile installation fails. The user must manually remove the mail profile before on-boarding to the other system.

Table 6: Known Behavior *(continued)*

Number	Description
893033	Authentication to Active Directory might fail for up to five minutes after rebooting the system. This is expected behavior while authentication services start up.
892345	E-mails with embedded images (.jpg, .png, etc) are not rendered properly on the iOS mail client. By default, these images are not included in the default set of attachments encrypted for Secure Mail. A workaround exists if using RTF document style (instead of HTML).
889894	If antivirus is configured on a client machine, it might block editing of host file. Therefore, when launching JSAM, you might get an error message like **You don't have permission to change the host file. Please talk to your administrator.**
888799	When using Secure Mail, the iOS mail client might report an error like An error occurred while delivering this message when sending or forwarding emails with large file attachments. This can occur when there is significant network latency between the SA and the back-end Exchange server or O365.
888445	The "Multiple POST" option should be disabled in SSO Form POST policy for OWA 2013. This option is disabled in the OWA 2013 Resource profile by default. If this option is enabled, when the user wants to logout from OWA, then it will SSO into OWA again. In effect, the user will not be able to logout from OWA during SA session.
881503	Using Secure Mail, it has been observed that the native iOS mail client might sometimes not report the correct number of items in the user's mailbox. This has been observed after clicking Block access blocking access and subsequently **Allow access**.
880431	When using Internet Explorer, after a user saves an HTML attachment on OWA 2013 through rewriter, the user will not be able to open the saved file. The workaround is to use Firefox or Chrome.
845980	On Windows 8, the EnableUA value needs to be set to 0 in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System for remediating Windows 8 firewall.
842058	During upgrades/downgrades, IKEv2 might stop working on some interfaces (especially the VIP in an A/P cluster). To resolve this issue, do one of the following: • Make any change to the System > Configuration > IKEv2 configuration. When you save a change to the configuration of a service, the service is restarted. • Go to Maintenance > System > Platform and click the **Restart Services** button. This restarts all system services.
831195	The character '<' when defined as part of the value of a SAML attribute value configured in SAML attribute statements configuration table will not be sent as part of the outgoing SAML assertion. This is because the character '<' has a special meaning and represents beginning of a replaceable token that represents a session or a custom variable. Note that if the attribute statements configuration is based on LDAP attributes, then even if the value fetched from a LDAP query contains a '<' character, it will be sent as is.

Table 6: Known Behavior *(continued)*

Number	Description
829905	When a Secure Access Service system is loaded with large number of tunnels and the authentication configured is RSA ACE authentication, the CPU is likely to spike to 100%. For such an environment, we recommend that you configure RSA ACE as RADIUS and in the Secure Access Service configuration, use a RADIUS server configuration instead of an ACE server configuration.
823456	SNMP GET fails for ifTableLastChange & ifTableLastChange objects.
804342	On Windows 7, a user encounters the Program Compatibility Assistant dialog box when attempting to upload logs. To reproduce, 1. Go to the client Preferences > Advanced page 2. Select Network Connect 3. Click Upload Logs.
750943	When JIS is running and proxy is configured in the browser, after Windows Pulse Collaboration client is installed, the dsCboxBroker.exe process is not running.
749276	Terminal Services is not launched when Internet Explorer is configured to automatically detect proxy settings.
743443	If a Secure Meeting administrator changed a user credential while the user is logged in from Outlook plug-in, the user can still continue to update the meeting information successfully. If user closes Outlook and opens it again, the user is prompted to enter his password again.
741595	On Solaris only, if a Host Checker policy has been configured, youmust run Host Checker each time you sign in.
728182	If Pulse client is not installed on the iOS device, nothing happens when click on a mobile meeting invitation link.
723665	If a user joins a Secure Meeting from an iOS device, the user is removed from the attendee list while the iOS device goes to sleep or locked. The user is added back to the attendee list after iOS devices is active again.
722851	Due to a bug in Windows implementation, client certificate authentication fails when TLS 1.1 or TLS 1.2 is enabled in Internet Explorer Advanced Security Options (Windows 7 only).
722167	When a Windows client starts sharing the desktop, the Closed drawer view is not properly shown on a MAC client viewer window. The Closed drawer is not docked on the left edge.
711948	The Javameeting client is unable to type text onWindows 7 presenter after theWindows 7 UAC prompt.
709402	When Network Connect is running in Linux openSuse, it does not go to reconnecting state when network connectivity is lost.
709157	If a user is logged in to a role with the max session timeout the same as Default Options, and this user later joins meeting and is mapped to a Meeting Users role that has a manually configured shorter max user session value; and if the user has already existed longer than this configured max user session timeout, the user is logged out. This is because role merge always takes the configured value over default options.

Table 6: Known Behavior *(continued)*

Number	Description
709142	If a pre-7.2 Outlook plugin is installed after 7.2 Outlook plugin, the Outlook client crashes when the user clicks **Collaboration**.
704414	Downloading files via aWindows share bookmark does not work.
701757	On Windows, if the host file contains only one entry (127.0.0.1 locahost) and no comments, after launching JSAM, the 127.0.0.1 entry is removed from the host file. The workaround is not to remove the comments from the host file.
691937	If a user logs into the Secure Access Service using Network Connect from a Mac in a realm with host checker policies enabled, when user clocks on the logout button in a Network Connect client, the user session is terminated, but the Host Checker process still runs until the next policy check.
686064	On Lotus Connection 2.5, after uploading a new file successfully, the page is not refreshed with the new file. The workaround is not to have a Caching policy set to **unchanged.**
676831	When no mail ID is configured in the User Preferences page, create a new meeting, and assign a user who does not have a Secure Access Service account the Conductor role, a meeting invitation e-mail is sent out when you click **Save and Previous.**

Open Issues

Table 7 on page 13 lists open issues and provides links to the PR Search portal for more information.

TIP: PR Search requires authentication. Log into the PR Search portal first and then click the links provided in this section.

Table 7: Open Issues

Number	Description
941024	In some cases, after a user disconnects and reconnects to the service with the Pulse client, the dashboard report for the session does not include the realm name.
938069	After an upgrades, the Dashboard active user sessions countmight be inaccurate.
937515	When you click the Help link from the Maintenance > System > Platform page, the system returns a file not found error. The link is broken. You can use the help system table of contents to display the content. You can also find the content on the Pulse Secure web site in the following location: **http://pulsesecure.net/techpubs/**

Table 7: Open Issues *(continued)*

Number	Description
934500	If the admin has disabled uploading attachments on OWA 2013, the user gets a Web page informing him that access to the website is blocked. When using Internet Explorer 11, if the user clicks the Return to previous page link on the Web page, the user sees a Web page expired message.
934431	Uninstalling WSAM from end-user Preferences page using the Firefox browser does not work. The workaround is to use the Internet Explorer browser to perform the uninstall operation.
934428	If a proxy is needed to reach Collaboration server, only the Active-X deployment works as expected. With Java (and Internet Explorer, Firefox, etc.), the client is launched, but it does not connect. A "cannot connect to server" (paraphrase) message is displayed.
933961	Through rewriter, uploading a user profile picture does not work on OWA 2013.
933571	After a login to iNotes 8.5.3 failed, if the user clicks Cancel, the user is redirected back to the iNotes login page.
933408	If the Require secure gateway authentication option is configured (requires all meeting attendees to sign in to the Secure Access Service), an error dialog box is displayed in Outlook when meetings are modified. In some cases the modification is successful.
933343	If the Require secure gateway authentication option is configured, a meeting invitation did not get removed from the end-user meeting page even though user deleted the Outlook meeting.
933303	For Pulse Collaboration Outlook Plug-In, in the modal window for teleconference, there are some extra colons displayed under Moderator and Participant details.
933165	If the system settings configuration from a previous release is imported with the Import everything (except Device Certificate(s)) option in a cluster, the cluster might become unstable after the import operation. To recover the cluster after the import operation, log into each node.
932778	On Windows, auto-uninstalling Network Connect fails if Pulse Secure Installer Service or Pulse Service is installed on the client machine. The workaround is to disable Pulse Secure Installer Service or Pulse Service.
932712	With Secure Mail, it has been observed that a blank login page might appear when clicking the Register button on certain iOS versions. The workaround is to simply click the button again. This behavior has been observed on iOS version 6.1.4 on iPhone 5.
932287	If a user signs into Secure Access Services (SSL-VPN) and then migrates their session to Access Control Service, the Federation-Wide Sessions display on the IF-MAP Federation > This Server > Federation-Wide Sessions page might contain two nearly identical rows for the one session. When the user later signs out of the Access Control Service, a vestigial row remains, with all cells blank except the User cell. These extra rows can be ignored unless thousands of them accumulate. An accumulation might affect the IF-MAP server performance and storage capacity.

Table 7: Open Issues *(continued)*

Number	Description
	To eliminate the extra rows: 1. On the Access Control Service to which the users have migrated, go to the IF-MAP Federation > Overview page. 2. Select **No IF-MAP**. 3. Click **Save Changes**. 4. Select **IF-MAP** client or **IF-MAP server** (whichever was in effect before step 2). 5. Click **Save Changes.** This workaround disrupts user access to protected resources. It should be scheduled during a period when low utilization is anticipated.
932107	On Mac, after a session has expired, user signs in again using the New Window option on JSAM. JSAM continues to display the **Expired** status instead of **OK** status.
931712	If the path provided while transferring snapshot creating via serial console does not exist in the server specified, the error message reported might in some cases be **Unknown** instead of **Incorrect Path**.
931005	On Windows, the upload log button appears in the JSAM applet even though the **Enable upload logs** option is disabled by the admin.
927523	An issue has been reported with Active Directory authentication service (the standard configuration, not the legacy mode configuration). There might be delays processing authentication requests after a certain period. To alleviate this issue, a preventative maintenance task to restart the Active Directory authentication service takes place every 24 hours. To modify the default behavior of this service, refer to Knowledge Base article KB28378: **www.pulsesecure.net/kb/InfoCenter/index?page=content&id=S:KB28378**
927191	In the Dashboard, the legends are not visible for Top Roles chart when using Internet Explorer 11 on Windows 7 during the first login.
927176	On the User Roles >Role > General > Session Options page, under the Roaming Session subsection, the options for **Limit to subnet** are not hidden when **Limit to subnet** option is selected and then unselected. This occurs only with Internet Explorer 11.
927169	If the time zone for the system time is set to **Jerusalem**, the time change on Oct 27, 2014 (to follow DST policies of Israel) will not occur.
927161	On the Citrix client download page under the terminal services options section, the **Enable Remote desktop launcher** radio button is not hidden when we uncheck it. This occurs only with Internet Explorer 11.
927040	A cluster rejoin situation can occur when the network interface used for cluster synchronization is at or very near line-rate for sustained periods of time.

Table 7: Open Issues *(continued)*

Number	Description
926551	If we switch between SNMPv2 and SNMPv3 versions before executing system settings import with **Import everything (except Device Certificate(s))** import option in a cluster, the SNMP trap engine-ids might change on some nodes of the cluster after import.
925097	On Vista and greater OS, when using Pulse Collaboration, there might be two Collaboration processes (dscboxui.exe) present.
923072	If there are more than 300,000 sessions per day, some of the dashboard charts might show erroneous numbers with the 24 hour period is selected.
921904	When configuring TLS syslog servers, use the name with which the server certificate has been created with and not its IP-address. If the TLS syslog server certificate has been issued to an IP address, use that instead of its name.
921424	If an administrator chooses to 'Block Access' when using Authorization-Only Sign-in policy, the email generated to the user is not localized and is only available in English.
920558	With Protection mode enabled in Internet Explorer, the Host Checker remediation tray icon does not display the remediation instructions when connected using VPN Tunneling and UAC is also enabled.
920534	SecureVirtualWorkstation does notwork properlywhen usingAvastAntivirus software. There is noworkaround.
920523	An Active/Passive IPv6 cluster needs to be recreated if any modification is done on the internal port. In some scenarios, it is possible that the IPv6 VIPs will become unreachable after internal port properties are modified.
916286	Date filtering is not working on the System> Log pages.
915501	On Windows, if ActiveX is disabled and Host Checker is enabled in realm/role, Network Connect fails to launch from the mini-browser.
915197	Due to a kernel limitation, the system shows the status of the default IPv6 route as green in the Network Settings > Routes page for the external interface.
912502	If the Device ID or MAC address of the client device cannot be retrieved, the Device Summary report might not show the URL to Single device report.
911705	Syslog over TLS does not work with the STRM syslog server.
911103	After a TCP Dump capture of traffic on the device, when you select SSLDump to view the resulting traffic, application traffic cannot be decrypted if the encryption algorithm is used in GCM mode. As a workaround, install an RSA certificate to another network port (for example, a virtual port). Accessing the device with that network port will negotiate a cipher where the application data can be deciphered.

Table 7: Open Issues *(continued)*

Number	Description
910384	Do not adjust the system time when the system is under heavy load. Some components, including the dashboard, might misbehave, and dashboard charts might not be generated properly.
901628	With the MobileIron MDM, you cannot deploy a Pulse Secure SSL VPN to Android devices. Look to a future MobileIron release for a resolution to this issue.
896345	Due to changes in Microsoft Active Directory 2012, some degradation in authentication performance has been observed.
894118	A virtual appliance instance might exhibit high CPU utilization and loss of throughput, including disruption of existing connections when the system exceeds 5000 tunnels (Network Connect, Pulse ESP/SSL or a combination of both) with 60 Mbps of bidirectional traffic. This issue was reported for a KVM platform with a 4 GB memory and 4 CPU allocation.
893879	WTS bookmarks that were created on a system earlier than 8.0 and configured to use HOB applet might fail to work well on the Secure Access Service 8.0 when a client-side browser is configured to use HTTP proxy with authentication enabled. To work around this issue, under Users > Resource Profiles > Terminal Services > Resource, select the **Configure HTML for the default applet** option. Or add the line **<param name="PROXYMODE" value="NO">** if using a custom HTML page for launching HOB applet.
892749	For Secure Mail, if an administrator configures the option to disable **Allow Outbound E-mail Attachments**, when the end-user forwards an email, the attachments are stripped. iOS clients display a warning message that the attachments have been removed. However, if this mail is using a Windows Outlook client, the warning text shows up as an attachment.
891897	Currently, there is a limitation on the number of different authorization-only sign-in URLs supported. We recommend that you use a single authorization-only sign-in URL. Multiple URLs might be configured provided the back-end Exchange server is the same for all URLs.
890220	In the rare case that Secure Mail settings must be changed (for example, enable/disable attachment encryption), we recommend that you force all devices to onboard again by selecting the devices in the device table and clicking **Force re-onboard.**
800805	Firefox 10 and later with a proxy PAC file is not supported. In these cases, an end user sees an error message that Java is not present while it is actually installed.
880578	The Status button on the Enterprise tab of Pulse Mobile for iOS devices (iPhone and iPad) always shows as Active even though device might have been removed or quarantined.
856402	The MAG chassis SSO works only in one node of a cluster formed by Secure Access Service systems from different MAG Devices.

Table 7: Open Issues *(continued)*

Number	Description
840855	In some scenarios, if the inbound DMI was already enabled on that node before adding it to a cluster, the inbound DMI might have to reenabled again in that node once the cluster is formed.
816309	An active-active cluster cannot be an IF-MAP server. It can be an IF-MAP client. When a cluster member is an IF-MAP client, you want to synchronize user sessions. Navigate to Clustering > Properties and ensure that **Synchronize user sessions** is selected. (It is selected by default.) If you unselect it, only a subset of the local sessions are exported to the IF-MAP server.
804296	On Windows 8, where proxy server with authentication is required, the Pulse Log Upload does not work from the Preferences > Advanced tab.
797412	When a Windows 8 endpoint accesses Sharepoint through the Secure Access Service, the Microsoft office integration functionality (via WebClient service), such as creating new Microsoft documents, editing Microsoft documents (such as Word, Powerpoint, Excel, OneNote in Microsoft Office, opening/editing pictures through Picture Manager) does not work as expected. This is because the WebClient service does not access the Secure Access Service cookie from Internet Explorer persistent cookie store.
795722	On Mac, when an IPv6 endpoint connects to the Secure Access Service, JSAM does not work.
790698	On Windows 8, the usage of FBA might not function properly. Users might see **Access Denied** message when users open a document from a document library.
790347	OnWindows 8, the usersmight not be able to open an explorer view due to the implementation of FBA.
784932	In Pulse Collaboration, if a name of a attendee is more than 18 characters long, the name overlaps with presence indication symbol.
740630	After doing an XML import of the local authentication server configuration on the root and virtual systems, the user full name does not appear in the Full Name field of the user profile for the virtual system. It does appear for the root system.
738793	When a cluster member gets removed from the cluster, the DMI inbound and outbound connection might not get disabled on the removed node. The workaround is to disable the DMI inbound and outbound connection manually on that particular device (removed node).
707130	When deleting a meeting without attendees or an expired meeting from Outlook client that was created using Outlook plug-in, this meeting is deleted from the Outlook client, but it still exist on the Secure Meeting server.
699288	If an older version of Outlook plug-in is installed on client machine, installing version 7.2 Outlook plug-in attempts to uninstall the older outlook plug-in. While the older outlook plug-in client is uninstalled, it prompts user to start the Outlook client with the **Retry** and **Ignore** buttons. Users must click the Ignore button to complete uninstallation. Clicking **Retry** brings user back to the same prompt.

Table 7: Open Issues (continued)

Number	Description
689157	CDL function incorrectly uses authentication server instead of directory server for evaluating customexpressions.
672996	On Chinese OS, there is a problemrendering aWeb page through the rewriter.

Fixed Issues

Table 8 on page 19 lists issues that have been fixed and are resolved by upgrading to this release.

Table 8: Fixed Issues

Number	Description
931822	When launching JSAM, Java update 45 had displayed a warning that the Pulse Secure application will be blocked in a future Java security update because the JAR file manifest does not contain the Permissions attribute.
914557	Virtual Desktop profile did not accept passwords with “>” and “<” symbols.
909640	When generating a new CSR of type ECC with either p-256 or p-384 curves, after clicking on create, the next screen under CSR had incorrectly shown the key size as 1024 bits.
906620	WSAM had not resolved a destination server by FQDN when the option **Resolve only host names with domain suffix in the device DNS** domains was enabled and the network configuration contained two or more domain names, separated with comma and a space.
897498	The French translation of ACE Authentication New Pin Mode text had been incorrect.
897134	The Citrix desktop toolbar had been present when using Citrix listed applications.
895599	TheWebRequestCompleted log had not displayedwhen the server respondswith an HTTP 304 response code.
895263	There had been issues with the filtering option in logs.
894336	When a node with an Active Directory standard configuration was removed from a cluster, the Active Directory authentication server settings had been deleted in some cases.
887021	The iCal attachment in meeting invitations had been off by one hour if the system clock was set to the Atlantic (Canada) time zone.

Table 8: Fixed Issues *(continued)*

Number	Description
886136	PulseCollaboration invitationmails sent usingOutlook plugin had not shown a server-generated password.
881890	On Windows XP endpoints, DNS access had failed for Pulse users when the DNS servers on the virtual IP address are updated.
880902	An e-mail gateway doing MIME verification had rejected the Pulse Collaboration invitation if each line was terminated by \n instead of \r\n.
880539	An attempt to bring up an Network Connect-GINA tunnel would fail if there was a reconnect in the previous Network Connect-GINA tunnel instance.
879345	OnWindows 8, randomdisconnects of CTS had been observed when connected with low wireless signal.
876900	After upgrading to Secure Access 7.4, the e-mail address configured on the Preferences page for the user session was not used when sending meeting invites.
876199	The browsing toolbar had displayed the Pulse Secure logo instead of the logo that is uploaded by the administrator.
875244	Intermittent RADIUS core dumps due to New PIN had been reported.
873149	The virtual appliance had not sent AAA traffic out of the Management Interface when Send AAA traffic via **Management interface** was enabled.
871892	After you performed an XML import of terminal services policy, access had been blocked until you clicked **Save Changes** on the Terminal Services resource configuration page.
869204	When using authorization URL, the back-end server hostname had been truncated when using a nonstandard port.
866782	The Web bookmark page title string was garbled when an “add bookmark” operation is done and the title has multibyte character.
865199	Client certificate authentication had failed with keys larger than 2048 bit on FIPS appliances.
864106	Connecting to a pre-7.2 Secure Access Service with OAC 5.4+ installed had resulted in a **Http:NAR:dsHostChecker.exe - Entry Point Not found** error message.
862628	Had not been able to assign a previously used A/P cluster VIP IP address as Virtual Port IP after deleting the cluster.

Table 8: Fixed Issues *(continued)*

Number	Description
855818	CDATA content had not processed via the rewriter for a customWeb application.
855496	Inside Secure Virtual Workspace, a licensing in terminal server related error had occurred when terminal services tried to connect to the server.
855458	NC diagnostic tool had incorrectly reported that the tunnel is up even when the tunnel is down.
852332	Pulse had not been able to establish the connection to the server when the Pulse Access Control Service performed a dynamic access policy change.
850750	In Pulse Collaboration, MacBooks with retina displays had been unable to share their desktops.
848061	After a TCP Dump capture of traffic on the device, when you select SSLDump to view the resulting traffic, application traffic could not be deciphered with ECDH or ECDHE cipher suites where encryption algorithm is not GCM mode. This issue has been resolved. Application traffic can now be deciphered with ECDH- or DCDHE-based cipher suites where the encryption algorithm is not GCM mode.
843922	In some rare instances, Pulse server side process had crashed during re-keying of Pulse ESP sessions.
843617	An e-mail gateway doing MIME verification had rejected the Pulse Collaboration invitation due to invalid MIME parsing.
842932	Only Windows 8 Professional, intermittently, users had encountered an error **(nc.apps.windows.23712)** while launching Network Connect.
839489	If a bookmark imported through XML import had been duplicated, the new duplicated bookmark had contained the wrong link.
839315	User access logs had not been able to filter a Korean letter for both role and realmname.
837482	Host Checker had failed to reinstall and launch when Pulse Secure SetupDLL.dll was not present in the system.
833417	Virus definition check had failed for certain antivirus products even if the endpoint had virus definition files that were up to date.
830445	Host Checker had prevented Network Connect from closing when the session was terminated via Web on Mac OS X 10.6.
827376	On the iPhone, the username and password fields had been invisible on the secondary login page.

Table 8: Fixed Issues *(continued)*

Number	Description
821438	Sametime instantmessaging with iNotes 8.5.3 FP1 integration had not worked through core access.
799743	The versionInfo.ini file for Network Connect had not been copied during the upgrade process.
783399	Windows 8 endpoints had been unable to save files to Sharepoint when accessing through the Secure Access Service.
553348	When using multivalued attributes for an RDP bookmark, the values had not been received correctly to create unique bookmarks.

Documentation

Table 9 on page 22 describes the documentation set. The documentation is available at **http://pulsesecure.net/techpubs/**

Table 9: Documentation

Title	Description
Release Notes	A release summary, including lists of new features, changed features, known issues, and fixed issues.
Supported Platforms	List of client environments, third-party servers, and third-party applications that have been tested and are compatible with the software release.
What's New	An overview of the key new features in this release.
Getting Started Guide	How to complete a basic configuration to get started using the solution.
Licensing Guide	How to install any licenses thatmight be required.
Virtual Appliance Deployment Guide	How to install, configure, and use the virtual appliance edition.
SA Series to MAG Series Migratio Guide	How tomigrate the systemconfiguration and user data to the newer platform.

Table 9: Documentation *(continued)*

Title	Description
Administration Guides	
Complete Software Guide	The complete collection of user documentation for this release in PDF format.
Administration Guide	How to complete the network and host configuration and how to use certificate security administration, configuration file management, and system maintenance features.
Dashboard and Reports Feature Guide	Describes the dashboard and reports you can use to analyze user and device access.
Monitoring and Troubleshooting Guide	How to usemonitoring and troubleshooting tools.
FIPS Certification Guide	How to enable the systemto be compliant with FIPS Level 1 requirements.
Feature Guides	
User Access Management Framework Feature Guide	An overview of the framework and configuration steps for AAA servers, roles, realms, and sign-in features.
Device Access Management Framework Feature Guide	Provides an overview of the framework, configuration steps, and examples.
Content Intermediation Engine Developer Reference	A reference on content intermediation engine support forWeb content.
Client-Side Changes Installation Reference	List of the files added or settings modified on the client desktop environment after the Pulse desktop client has been installed.
Endpoint Security Feature Guide	Describes Host Checker, Cache Cleaner and Secure VirtualWorkspace settings.
Handheld Devices and PDAs	DescribesWSAM and ActiveSync enabling on PDAs and handheld devices.
Configuring Secure Mail	An overview of the feature and configuration steps.
E-Mail Client Feature Guide	An overview of the feature and configuration steps.
File Rewriting Feature Guide	An overview of the feature and configuration steps.

Table 9: Documentation *(continued)*

Title	Description
Pulse Collaboration Feature Guide	An overview of the feature and configuration steps.
Secure Application Manager Feature Guide	An overview of the feature and configuration steps.
Terminal Emulation Sessions Feature Guide	An overview of the feature and configuration steps.
VPN Tunneling Feature Guide	An overview of the feature and configuration steps.
Web Rewriting Feature Guide	An overview of the feature and configuration steps.
Pulse Client Feature Guide	An overview of the feature and configuration steps. For extensive documentation of Pulse, see the **Pulse desktop client documentation set**.
SAML Sign-On Feature Guide	An overview of the feature and configuration steps.
Solutions	
Instant Virtual System	Describes how to deploy IVS.
IF-MAP Feature Guide	An overview of the feature and configuration steps.
Intrusion Detection and Prevention Sensors	Describes interoperability with IDP.
Developer Reference Guides	
CustomSign-In Pages Developer Reference	A reference on customizing sign in pages.
DMI Developer Reference	A reference on using DMI tomanage systemconfiguration.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@pulsesecure.net.**

Technical Support

When you need additional information or assistance, you can contact "Pulse Secure Global Support Center (PSGSC):

http://www.pulsesecure.net/support

support@pulsesecure.net

Call us at (408) 372-9600

Revision History

Table 10 on page 25
lists the revision history for this document.

Table 10: Revision History

Revision	Description
01/December 2, 2013	Initial publication.