Pulse One Appliance Release Notes

Supporting Pulse One Appliance 2.0.1904

Product Release	**2.0.1904**
Published	**29 January 2020**
Document Version	**1.0**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Pulse One Appliance Release Notes

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

Release Notes

Introduction

Pulse One Appliance runs either:

- On PSA7000 hardware, OR
- As a virtual appliance on VMware ESXi, which is hosted within the customer datacentre.

The Pulse One Appliance enables two capabilities:

1. Pulse One Centralized Management: provides unified visibility and management of Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS) in a single easy-to-use console. It provides the ability to aggregate Syslog data from all Pulse Connect Secure and Pulse Policy Secure appliances running in a customer environment. The Pulse One Appliance UI provides an intuitive method to view reports, write custom queries, and troubleshoot issues.
2. Pulse Workspace (PWS) Mobility Management: enterprise mobility management that support BYOD and corporate-owned devices while respecting user privacy and choice. It encrypts all data at rest, controls data sharing between enterprise apps, wipes corporate data without affecting personal information, and connects directly to the enterprise VPN.

These Release Notes highlight the features that have been added and the known issues in this release.

Note: If the information in the Release Notes differs from the information found in the online documentation set, please refer to the Release Notes as the source of the most accurate information.

Managed Appliance Versions Supporting This Release

To use the new features introduced in this release of Pulse One Appliance, you will need to use newer versions of Pulse Connect Secure and Pulse Policy Secure, with the recommended minimum supported version numbers shown in the table below. It is recommended that you upgrade your appliances to these minimum release versions.

The following table lists the revision history for this document.

Product	Recommended Version	Description
Pulse Connect Secure (PCS)	9.1R1 or higher.	Pulse Connect Secure 9.1R1 or higher. Pulse Connect Secure 9.0R4 (or higher & 9.0R3.4 (9.0.3.64053). Pulse Connect Secure 8.3R7.1 or higher. Please refer to Knowledge Base article KB43861.
Pulse Policy Secure (PPS)	9.1R1 or higher.	Pulse Policy Secure 9.1R1 or higher. Pulse Policy Secure 9.0R4 or higher & 9.0R3.2 (9.0.3.51873). Pulse Policy Secure 5.4R7.1 or higher. Please refer to Knowledge Base article KB43861.

Pulse One Release Builds

The following table lists the Pulse One release builds.

Format	Release Build
OVF	Pulse One 2.0.1904-5831 (B39)
Upgrade bundle	Pulse One 2.0.1904-5829 (B114)

New Features

The following table describes the major features that are introduced in this release.

Feature	Description
Whitelist IP by country	Admin wants to configure Pulse One to specify a list of countries from which login to Pulse One is either allowed. • If list is empty, then access allowed from all the countries. • If allowed countries list has some countries, then access from any other countries (except allowed list) will be denied.
User profile and anomaly data on Pulse One for UEBA	UEBA feature requires the profiles of uses to be stored and displayed on Pulse One so that administrator may drill down on any anomalies.
Device profile and anomaly data on Pulse One for UEBA	UEBA feature requires the profiles of devices to be stored and displayed on Pulse One so that administrator may drill down on any anomalies.

Problems Resolved in This Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
POP-11998	Race condition during credential renewal can cause appliance to be unregistered.
POP-14281	Remove basestring usage from pulsesecure.pcsclient.
POP-14323	Incorrect CPE in openssh.yml hides vulnerabilities.
POP-14329	Task status is displaying ESAP uploading when converting to AAA/Gateway.
POP-14337	Admin wants user roles default and global options and admin roles default options to be distributed by Pulse One.
POP-14363	Pulse One started supporting 2 blocks uploading to config History. Right now in Configuration History it is displaying both the Blocks as "Unknown > auth.roles.user-global-options (added)". We should display them as "default > auth.roles.user-global-options (added)".
POP-14375	Enabling enrollment of managed Android clients broken the iOS Managed Device enrollment.
POP-14380	log-aggregator forwarding targets are not synced between Pulse One active and passive nodes.
POP-14400	Display auth.role.user-default-option in Pulse One Configuration History.
POP-14428	Whitelist deletes currently whitelisted IP when user enters a value and hits enter.
POP-14446	Error message is coming in JSON Format and P1 login page is not coming when user is not allowed to access the console for country whitelisting.
POP-14450	SDP profile from managed device enrollment is tagged as per-app VPN and blocks the resource access with gateways.
POP-14457	Hostchecker Anti-virus-rules policy changes results in repeated "Publish Required".
POP-14458	Policy changes with <process-rules> elements results in repeated "Publish Required".
PRS-14321	Vuln_finder not finding linux kernel vulnerabilities: the OSTP yml file for Linux kernel needs a CPE ID.
PRS-385173	Pulse One: Unable to publish Hostchecker policy using config group.

Known Issues in This Release

The following table lists the Known issues in the current release..

Report Number	Description
POP-2483	The Group validation status is updated to “Invalid” if a group is added while the LDAP server is not available. **Workaround:** Manually initiate the verification process once the LDAP server is available again.
POP-3980	The Pulse One domain UI does not accurately display a locked account.

Report Number	Description
POP-4077	The Publish operation fails when a Pulse One group contains appliances with different versions.
POP-5460	The 'Logins in Past 24 Hours' endpoint compliance widget in the 'Overall System Health' dashboard does not display the 'non-compliant reason' information correctly. After 24 hours, the data from the previous 24 may still be visible.
POP-5629	Search for users based on LDAP group while adding a policy lists all users instead of just LDAP group policy users. **Workaround:** Save the policy and re-open the edit screen to see the changes.
POP-5886	Pulse One supports the ability to aggregate up to 90 days of syslogs from Pulse Connect Secure and Pulse Policy Secure appliances that are configured to send their Syslog data to Pulse One. However, an admin is not prevented from configuring more days. **Workaround:** Please specify a maximum of 90 days when configuring this capability.
POP-5888	Pulse One does not prevent an admin from running the 'system destroy' command when an NFS directory is mounted. **Workaround:** Remove the NFS mount before running 'system destroy system-config' on the CLI.
POP-5942	When not successfully mounted, 'log-aggregator show' does not indicate any errors with the mount process. **Workaround:** Please check the NFS share to ensure that the logs are being written there. If not, please retry to mount.
POP-5943	The 'system destroy system-configs' command does not immediately disconnect interfaces. **Workaround:** After using the 'system destroy system-configs' command on the serial console of a Pulse One Appliance, reboot the appliance.
POP-6029	Removed appliance names are no longer displayed in the appliance activities trail.
POP-6166	Send Logs does not upload logs on to the Pulse Workspace server. **Workaround:** Do send log using email address.
POP-6493	A few settings – Licenses, NTP, and so on – are not synched from Active node to Passive node after a cluster is successfully set up.
POP-6660	The 'cluster add' command returns 'ERROR: list index out of range' if the IP address being added is invalid.
POP-6728	If the Active node is shut down and you attempt to run 'cluster status' command on the Passive node, it might take up to 5 minutes for the Passive node to provide a status message.
POP-7559	An admin user having a custom-defined role with delete privileges at the "User" level can edit/delete admins with custom permissions higher than itself. That is, Super Admins, and so on. **Workaround:** Do not give edit/delete privileges to custom roles with permissions lower than a Super Admin's unless specifically intended.
POP-7860	When the use of the time-range selector returns more than a 100 data points, the graph may not display correctly.

Report Number	Description
POP-8091	The 'system destroy system-config' command also deletes all entered licenses when it deletes all other configuration and data. You can re-enter licenses only after the provisioning step has been successfully completed. **Workaround:** Perform 'services restart' after re-entering licenses to make them effective.
POP-8198	Login failure due to a short password configured for the user authentication causes an inaccurate "User Login Failure" count in the User Syslogs Reports feature.
POP-8245	After performing the 'cluster demote' command, the internal interface is disabled, and its IP address removed from the configuration. You need to configure internal interface again prior to invoking subsequent clustering commands.
POP-8313	In the first few minutes after a service start, the 'log-collector' service makes a number of outbound attempts to reach https://versioncheck.graylog.com to check for the newest version available.
POP-8333	The message presented when a 'cluster join' command is run before the external interface is configured is not user friendly: "AttributeError: 'NoneType' object has no attribute 'network for joining the cluster'".
POP-8415	IP subnet 192.170.0.0/24 is used internally by Pulse One. These addresses cannot be used to configure external nor internal interface of the appliance.
POP-9228	"Space name" is showing "Unregistered" even after the Space state is up-to-date. **Workaround:** If the admin refreshes the Workspace page, Space name will show correctly.
POP-9234	Applying a group config to the non-leading node of an AA cluster target or to the passive node of an AP cluster target, causes the group to remain in an infinite publishing state. **Workaround:** Click to 'Apply Group Config' on the leader or the Active node of the target cluster. This should automatically get the group back into sync once complete.
POP-9337	A group that has no target appliance may sometimes go into an unknown state. **Workaround:** Make changes to the configuration of the master appliance. This should trigger a re-render and update the status of the group to 'In-sync'.
POP-9590	Connectivity issues when an interface with DHCP configuration overlaps with the static IP subnets of other interfaces. **Workaround:** If using DHCP, ensure all interfaces are on different subnets. If using static, use only static IPs for all interfaces; do not mix DHCP assigned IPs with static IPs.
POP-9596	SSH connections are not gracefully closed when the IP address of the management interface is modified. **Workaround:** Enter "~." To cleanly exit out of SSH and return to the command prompt.
POP-10189	Appliance groups sometimes display continual rendering state after an upgrade from Pulse One 2.0.1649 to Pulse One 2.0.1834. **Workaround:** Remove appliance from the associated group(s) and add back.
POP-10194	After performing "Verify Group" for LDAP users, a new policy is not pushed in client. **Workaround:** Refresh the policy from the client or push the workspace in the server to update the newly added group policy.

Report Number	Description
POP-10427	Cluster promotion command fails with 'log-indexer' timeout error after 'system destroy data'.
POP-10731	Upgrade fails with 'log-indexer' error when no licenses were added to the system prior to upgrade.
POP-10861	Apps are not installed on BYOD device that use Google Accounts method if "Enforce EMM policies on Android devices" is enabled in the Google Admin console.
POP-11107	When 'services logs' is running in one SSH session, another duplicate SSH session will not be able to kill the first session.
POP-11457	After destroying its config, on-premise appliance gets stuck in MSSP mode.
POP-11484	When a failed Active node comes back online, the Pulse One cluster suffers a split brain. **Workaround:** Once an Active node has suffered outage, remove the IP entry from the DNS to prevent it from hitting this scenario.
POP-11545	Managed appliances will not fail over if an appliance was registered in a release using the registration URL: *api.pulseone.domain* (pre-1743) which is upgraded to a release (post 1723) using registration URL: *hostname.pulsonedomain.com*. **Workaround:** All appliances affected would have to be re-registered.
POP-11885	Before an Active/Passive upgrade, you demote both nodes to standalone. If the cluster's FQDN resolves to both addresses, managed PCS/PPS appliances might connect to either node. This is a split-brain condition. Data will be lost.
POP-11926	After issuing a Full Device Wipe, the UI does not show the Space state info.
POP-11979	The Pulse Client "Workspace Apps" page is stuck (and displays "Error Occurred") for a long time after Corporate-Owned Provisioning is completed.
POP-11991	After issuing "Wipe Workspace", an error appears if the profile has been removed.
POP-12028	The upgrade software option remains enabled when a group is upgrading. If an admin attempts the upgrade again, a conflict message is displayed.
POP-12099	Scheduler fails to create a task if there is already a task of the same type open. Only one task of each type is allowed per appliance (or per group) at any time.
POP-12200	Scheduling an install task with a package version that is not the staged package version initiates the installation on the appliance and upgrades the appliance to the staged package version.
POP-12265	Active/non-leader node of cluster shows a vague error message when the upgrade of a group of clusters fails. **Workaround:** The message may be ignored.
POP-12399	After Volume Purchase Program (VPP) apps are installed on an iOS device, it could take up to 45 mins for the license count to be updated to reflect the app usage.
POP-12775	When an admin enters an incorrect location API key, the location map displays no image or visible errors.
POP-12789	Lost Mode options are not hidden for Unsupervised devices.
POP-12835	Even after the workspace is wiped, Space Actions show "Force Update Cert" button as highlighted. It should be grayed out.

Report Number	Description
POP-13225	Certificate Based authentication for ActiveSync does not work a certificate generated by the PWS in-built CA Server is used. This affects both iOS and Android devices. **Workaround:** Use an external PKI Server for generating ActiveSync certificate using SCEP or CAWE.
POP-13350	Policy publish button is not enabled when OnDemand rules are configured. **Workaround:** After configuring the VPN On-Demand rules, again toggle the VPN OnDemand 'Enabled' property and then publish the policy.
POP-13363	After deleting all the rules/criteria/action parameters, Selected value is still showing '1'.
POP-13505	Profiler data is not received on Pulse One for up to 24 hours after running a 'system destroy data' command.
POP-13546	A user may get an "Unauthorized error" if they try to change their Pulse One password using a browser tab that was previously used for the SDP workflow: **Workaround:** Delete the cached DSID cookie from the browser's cookie settings.
POP-13566	Syslogs are not received on Pulse One for up to 24 hours after running a 'system destroy data' command.
POP-13708	Out of Memory error prevents admin from using SSH to access the Pulse One appliance. **Workaround:** Reboot the appliance.
POP-13777	Workspace device UI should add the ability to display the enrolled workspace as Managed client or Managed Device.
POP-13839	In the Google App search window, each page does not consistently show ten apps in the search results.
POP-13851	Even after supporting pagination for Google App search and removing duplicate search results, I.T. admins cannot search and add the required apps to the App Catalog. **Workaround:** Add the Android apps directly from the Google Play after logging in using the AFW registration account.
POP-13932	For a custom-created policy, web clips present in the Global policy are not shown. **Workaround:** Configure the Web clips in the custom policy also.
POP-14176	When a Pulse One cluster is demoted or promoted, there may be a brief period of time where the node is unavailable from the admin UI. **Workaround:** Restart the services and the system should start working properly again.
PRS-369700	Upgrading using SSH still requires serial console access to complete the process. The user is prompted to reboot the appliance once the upgrade is successful. Over SSH, the session is terminated once the services are stopped and the upgrade process begins.
PRS-368359	PCS appliances with IP addresses in range 172.17.0.0/16 do not register on Pulse One OnPrem appliances. This is because Docker uses the same IP subnet. **Workaround:** Consider moving managed appliances to a different subnet.

Documentation

Pulse Secure documentation is available at https://www.pulsesecure.net/techpubs.

For policy reasons, security issues are not normally mentioned in release notes. To find more information about our security advisories, see the security advisory page on the Pulse Secure website.

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

For additional information or assistance, contact Pulse Secure Global Support Center (PSGSC):

- https://support.pulsesecure.net
- support@pulsesecure.net
- Call 1-844-751-7629 (toll-free USA)

For technical support resources, browse the Pulse Secure Technical Support website https://support.pulsesecure.net.

Revision History

The following table lists the revision history for this document.

Revision	Revision Date	Description
1.0	29 January 2020	First release.