Pulse Secure®

Pulse One Cloud Release Notes

Supporting Pulse One Cloud 2.0.2003

Product Release	2.0.2003
Published	28 October 2020
Document Version	1.0

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

www.pulsesecure.net

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse One Cloud 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 1
Introduction 1
Managed Appliance Versions Supporting This Release 1
Problems Resolved in This Release 2
Known Issues in This Release 2
Documentation 5
Reporting Documentation Issues 5
Technical Support 5
Revision History 5

Release Notes

- Introduction 1
- Managed Appliance Versions Supporting This Release 1
- New Features 2
- Problems Resolved in This Release. 2
- Known Issues in This Release 2
- Documentation 5
- Technical Support 5
- Revision History 5

Introduction

The Pulse One Cloud enables two capabilities:

1. Pulse One Cloud is a SaaS service that provides unified management of Pulse Connect Secure (PCS), Pulse Policy Secure (PPS) and Pulse Workspace devices, in a single easy-to-use console.

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 Cloud, 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.

Product	Recommended Version	Supported Versions
Pulse Connect Secure (PCS)	9.1R2 or higher.	9.0R3.4 or higher. 9.1R2 or higher.
Pulse Policy Secure (PPS)	9.1R2 or higher.	9.0R3.2 or higher. 9.1R2 or higher.

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-14399	Pulse One displays wrong group status for appliance groups that have deleted members.
POP-14536	Some configuration blocks end up with auto-policies. This fix works in conjunction with *PCS-15717* delivered in 9.1R9.
POP-14663	Administrator has a provision to reset the web user password.
POP-14714	Analytics Device OS graph does not show information for Windows 10 OS. This is tied to PCS *PRS-389456* due in 9.1R10.
PRS-380404	Unable to publish config when "userattr.url" attribute is used as the host for terminal services profile for the master appliance.
PRS-380576	Unable to publish configuration when Citrix storefront web profile is created.
PRS-388525	Fix browser caching vulnerabilities to avoid information exposure.
PRS-388528	Implement input validation for ASP.Net configuration.
PRS-388534	Input neutralization during web page generation to avoid cross site request forgery.
PRS-388870	Services will not restart after demoting and upgrading.
PRS-390359	Admin UI shows "publish required" until the page is refreshed.
PRS-392509	Increase SSH server public key length.
PRS-392838	Cross site request forgery checks for X-Frame-Options HTTP header.
PRS-392847	Remove deprecated cryptographic settings.
PRS-393707	Unable to create new appliance group.
PRS-394343	User cannot add new PWS workspace for iOS devices,

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.
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.

Report Number	Description
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-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-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.
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-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.
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-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-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.

Report Number	Description
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.
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-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.

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.

Reporting Documentation Issues

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, please send your comments to: techpubs-comments@pulsesecure.net. Include a full description of your issue or suggestion and the document(s) to which it relates.

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	28 October 2020	First release.