**Pulse Secure®**

# Pulse One Cloud

Release Notes

Pulse Secure, LLC

2700 Zanker Road, Suite 200 San Jose, CA 95134

The Pulse Secure Logo, the Pulse logo, and PulseE are trademarks of Pulse Secure, LLC. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899,6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*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 **https://www.pulsesecure.net/support**. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Contents

# 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.

> *i* **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.

Table 1: Appliance Versions

| Product | Recommended Versions | Supported Versions |
|---|---|---|
| Pulse Connect Secure (PCS) | 9.1R1 or higher | 8.3R1-8.3R4, 8.3R6.1 or higher. Please refer to Knowledge Base article KB43861. |
| Pulse Policy Secure (PPS) | 9.1R1 or higher | 5.4R1-5.4R4, 5.4R6.1 or higher. Please refer to Knowledge Base article KB43861. |

# New Features in This Release

The following table lists the new features in this release.

Table 2: New Features in This Release

| Feature | Description |
|---------|-------------|
| Certificate Based Email | This feature enables certificate-based authentication for ActiveSync accounts on mobile devices |
| Workspace Location Enhancements (Android) | Admin can track and plot each Android user's registered Workspace location on the map in their respective Workspace. This included location accuracy, which enables storage of location accuracy data when workspaces report their location to the server. |
| Managed  Client Enrolment (iOS only) | This feature introduces support for PWS provisioning of VPN policy for Mobile client absent of device management. |
| VPN On-Demand (iOS only) | This feature describes functionality provided for on-demand VPN connections. On-demand configuration defines multiple *rules* that dictate to VPN clients automated *actions* to perform when rules are evaluated and conditions are met. |

# Problems Resolved in This Release

The following table describes issues that are resolved in this release.

Table 3: Resolved in This Release

| Problem Report | Description |
|----------------|-------------|
| POP-12754 | After changing the "External Port" configuration in the VPN Provider, VPN Properties values are shown as updated even before clicking on "Update Auto VPN Configuration". |
| POP-12793 | User with Read Only privileges is able to delete the APP VPP token. |
| POP-12884 | Even after enabling the "iOS Allow Cloud Backup" and "iOS Allow Cloud Keychain Sync" property in policy in PWS, in the iOS device, status is still "Off" but are editable now. |

# Known Issues in This Release

The following table describes the open issues in this release, with workarounds where applicable.

Table 4: Known Issues in This Release

| Problem Report | Description |
|---|---|
| POP-2483 | The Group validation status is updated to "Invalid" if a group is added while the LDAP server is not available.<br>**Workaround**: Manually initiate the verification process once the LDAP server is available again. |
| POP-3980 | Pulse One domain UI does not accurately display a locked account. |
| POP-4077 | When a configuration publish is attempted for a Pulse One group containing appliances with different versions, the publish operation fails with some errors. |
| POP-5460 | The endpoint compliance widget 'Logins in Past 24 Hours' in the 'Overall System Health' dashboard does not display the 'non-compliant reason' reasons information correctly. After 24 hours, the data from the previous 24 may still show up. |
| POP-5629 | Search for users based on LDAP group while adding policy lists all users instead of just LDAP group policy users.<br>**Workaround**: Save the policy and reopen 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 Pulse Workspace server.<br>**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.<br>**Workaround:** Do not give edit/delete privileges to custom roles with permissions lower than a Super Admin's unless specifically intended. |
| POP-7860 | When a user uses the time-range selector to select a range that returns more than a 100 data points, the graph may not display correctly. |
| POP-9228 | "Space name" is showing "Unregistered" even after Space state is up-to-date.<br>**Workaround**: If admin refresh the Workspace page, Space name will show correctly. |
| POP-9234 | 'Applying 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.<br>**Workaround**: Click to 'Apply Group Config' on leader or active node of the target cluster. This should automatically get the group back in sync once done. |
| POP-9337 | A group that has no target appliance may sometimes go into an unknown state.<br>**Workaround**: Make changes to the configuration of the master appliance. This should trigger a re-render an 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<br>**Workaround**: Remove appliance from the associated group(s) and add back. |
| POP-10194 | After "Verify Group" for LDAP users, new policy is not pushed in client.<br>**Workaround**: Do policy refresh from the client or Push space in the server will update the newly added group policy. |
| POP-10861 | Apps not installed in BYOD device with Google Accounts Method if we enable "Enforce EMM policies on Android devices" in Google Admin console. |

| Problem Report | Description |
| --- | --- |
| POP-11926 | After issuing Full Device Wipe, UI is not showing the space state info |
| POP-11979 | Pulse Client "Workspace Apps" page stuck with "Error Occurred" for long time after Corporate Owned Provisioning is completed |
| POP-11991 | "System Error" after issuing "Wipe Workspace" if the profile has been removed |
| POP-12399 | After the Volume Purchase Program (VPP) apps are installed on an iOS device, it could take up to 45 mins for the license count based on app usage to be updated accordingly. |
| POP-12775 | When an admin enters an incorrect location API key, the location maps displays no image/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. |
| POP-13225 | Certificate Based authentication for ActiveSync is not working with the certificate generated by the PWS in-built CA Server for both iOS and Android devices.<br>**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.<br>**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-13507 | DEP device gets onboarded as managed device even when managed client option is enabled |
| POP-13556 | App Catalog page is stuck and apps are not visible when uploading an invalid Apple VPP token to Pulse One.<br>**Workaround**: Remove the invalid Apple VPP token, upload the valid token and refresh the App Catalog page. |
| POP-13562 | For the newly created policy, VOD rules are not inherited from global policy.<br>**Workaround**: Configure the VPN On-Demand Rules in the custom policy as well. |
| PWS-3115 | After creating the new user space, Workspace Search box shows unwanted values. |

# Documentation

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

# 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):

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

# Revision History

The following table lists the revision history for this document.

Table 5: Revision History

| Revision | Revision Date | Description |
|----------|---------------|-------------|
| 1.0 | May 15, 2019 | First release. |