Pulseway

Security White Paper

November 2015

Table of Contents

1. Introduction

Information security is an essential consideration for all IT organizations around the world. Security is always the first priority for our product and it's constantly improved by ensuring that up-to-date technologies are used and that security policies are enforced for both staff and end-users. Pulseway utilizes industry standard encryption, attacks protection systems, security policies and multi-factor authentication mechanisms to ensure security compliance.

2.1 Transport Encryption

Pulseway uses end-to-end encryption, which ensures that your private infrastructure information stays private and unauthorized access is prevented. All connections to Pulseway services are done with a fully encrypted communication based on RSA public/private key exchange and AES (256 Bit) session encoding. This is the current industry standard encryption algorithm used worldwide.

2.2 Message Encryption

All communication messages are encrypted with AES (256 Bit) symmetric keys, which are sent via RSA public/private key exchange mechanism to guarantee that in the unlikely event of transport encryption failure, privacy is not compromised. Keys are automatically rotated on a controlled interval to prevent brute-force attacks also adding an extra layer of security against man-in-the-middle attacks.

3. Brute-Force Protection

A brute-force attack is a trial-and-error-method used to guess account passwords. With the growing computing power of standard computers, the time needed for guessing long passwords has been increasingly reduced. Pulseway defends from brute-force attacks by increasing the timeout between failed requests.

4. DigiCert Code Signing Certificate

The agent software is signed via DigiCert Object Code Signing to guarantee that the code has not been altered or compromised by a third party.

5. Datacenter & Network

We host our servers on US East Coast data centers providing high redundancy and lower latency.

The Datacenter is compliant with US federal regulations and industry standards - ISO Certification, LEED Certification, and Uptime Institute.

6. Device Access Control Lists

For enhanced security on the Pulseway mobile apps you can setup:

- PIN code mobile authentication (and Touch ID where supported) to prevent unauthorized access to the monitored systems.

- Centralized device access control lists with the ability to remotely disable mobile devices.

- Default device access control list that will be used for newly added systems which allows you to deny access for all systems until you explicitly approve the new device.

- Agent device access whitelist to only allow commands from explicitly allowed devices.

7. Two-Step Authentication

Users can enable two-step authentication at any time on their accounts, which sends an OTP (One Time Password) via email to the account owner whenever you try to access sensitive account information such as Device Polices, remotely provisioning computer settings or connecting to a system via Pulseway Remote Desktop.

8. IP Address Filters

Pulseway Web Application respects IP Address filters configured on each account which can be used to restrict access to monitored systems to the intranet or VPN networks for increased security.

9. Auditing

All Pulseway commands are locally logged in the Application Windows Event Log and in the Pulseway Enterprise Server database for auditing reasons. The account owner is notified via email every time a new mobile device or a web browser instance is registered on the account.

Contact Information

Do not hesitate to get in touch with our team for any queries or questions relating to the Pulseway Security White Paper.

Email: support@pulseway.com
Phone: +353 16190234