Pulseway

Security White Paper

Version 6.0
Last updated October 2023

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 has been designed with security at its core and utilizes industry standard encryption, attacks protection systems, security policies and multi-factor authentication mechanisms to ensure security compliance.

2. Encryption

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 (TLS 1.2).

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 blocking multiple failed requests and by increasing the timeout between failed requests. We have recently introduced the ability to define minimum password standards to further increase the protection to the product.

4. Code Signing

All the Pulseway Windows and macOS agents and applications are signed using a Code Signing certificate to guarantee that the binaries have not been altered or compromised by a third party.

5. Datacenter & Network Security

We offer SaaS customers the choice of having their instances hosted on dedicated servers in either North American or European data centers.

Our North American data center is situated on the US East Coast providing high redundancy and lower latency.

This Datacenter is compliant with US federal regulations and industry standards such as the NIST Cybersecurity framework, LEED Certification, SOC 2, and Uptime Institute.

Our European data center is situated within the EU and is also optimized for high redundancy and low latency.

This data center is compliant with all local regulations and standards including GDPR. It is also ISO 27001, ISO 9001, ISO 22301 certified.

The Pulseway agents and client software do not require the opening of any inbound network ports. The solution only requires the HTTPS (TCP 443) outbound port to be available.

Customers hosting an on-premise Pulseway server should ensure that only the TCP 443 port is opened in inbound to reduce the risk of attacks on other services running on the server.

6. Device Access Control Lists

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

- PIN code mobile authentication (and Touch ID / Face 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.

7. Two-Factor Authentication

Two factor authentication (2FA) is an additional security layer that will require an additional step to access your account or perform certain operations.

You can opt-in to receive Push notifications on your mobile apps to approve authentication requests or use a TOTP app (Time-based One-Time Passcode) like Google Authenticator, Authy or 1Password.

When setting up 2FA, the system will also generate backup codes that can be used when all the other authentication methods are not available. Each backup code can only be used once.

All Pulseway user accounts are required to have 2FA configured to ensure maximum account protection.

8. IP Whitelisting

We add further access protections by allowing you to define specific IP Addresses that are allowed to access the web application and Rest API. You can also define a session timeout period to define the maximum period of inactivity before a user is logged out.

9. Auditing

All Pulseway commands are locally logged in the Application Windows Event Log and in the Pulseway 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. Audit logs cannot be cleared or altered by Pulseway users.

10. Security Testing

Both Pulseway infrastructure and the Pulseway software is subject to penetration tests performed on a regular basis. The tests are run by our internal SaaS OPS team and also by independent companies, specialized in security testing.

11. Kill Switch

There is a comprehensive incident plan in place that defines stringent internal processes that can be deployed to temporarily disable both SaaS and on-prem services should there be a systemwide breach that could pose a risk to our customers.

Contact Us

Do not hesitate to get in touch with our team for any queries or questions relating to the Pulseway Security White Paper by emailing us at security@pulseway.com.