

PingPlotter Cloud Security Best Practices

Agent Details:

- Network trace data is collected on agent machines, which closely resembles the data collected via traceroute & ping, collected with ICMP, UDP, or TCP based on configuration. ICMP is the default.
- Web requests made by agents always use HTTPS, with trace data flowing through the WebSocket Secure protocol.
- Agents only need to be able to connect to <https://connect.pingplotter.com>, our server "hub" that sends commands such as the signal to start a trace, and receives agent trace data. Our server does not connect into the agent machine.

Hosting:

PingPlotter Cloud's supporting services are hosted in Microsoft Azure Data Centers.

Read more about Azure's security practices, compliance, and how the Cloud hosting model changes the dynamics of digital security here: <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Logging:

- Web application logs are stored up-to 30 days.
- Logs can be deleted upon request & account deactivation.
- PII is not logged.

Authentication and User Management:

On signup, users are given a temporary password that is emailed to them, with instructions on how to change their password to a non-temporary password.

Once a user has signed up, they should set up 2-Factor Authentication via an authenticator app or device.


When logged in, the user is granted a token, that expires within 31 days. All usage of the PingPlotter Cloud Web Application API requires a user token.




PingPlotter Cloud's Web Application, has a permission-based user system, allowing administrators to configure users with read-only access, and the ability to revoke all access.


Pingman Tools General Practices:

- Principle of Least Privilege - employees are given the minimum amount of access to perform their tasks.
- Use of strong passwords, randomly generated by password management tools.
- Do not collect data outside of what is absolutely **required** for the task performed by our product or systems.
 - When debugging production issues, reach out to collect more data, if needed.
- Respond to security bounty reports, and reward bounties when relevant

If there are any additional questions please contact us at support@pingman.com



Products PingPlotter Cloud Professional Edition Standard Edition PingPlotter Sidekick	Solutions Infrastructure Monitoring End-User Support Network Validation Troubleshooting	Links Download PingPlotter Support Wisdom Account Contact Us	  	Get the latest PingPlotter news <input type="text" value="Enter email address"/> <input type="checkbox"/> You agree to our Privacy Policy . * Join our newsletter!
---	--	--	---	--

 Copyright 1998-2021 Pingman Tools, LLC. All Rights Reserved.