



Food and Beverage

The Oenoflow™ PRO Filtration System Data Security and Frequently Asked Questions



Contents

Pall Oenoflow PRO Service — Meeting the demands of the modern wine industry	3
Customer Requirements for Installation	3
The Oenoflow PRO System Architecture	4
Frequently Asked Questions	4
Pall Secure Computing Environment Security Summary	5
References	6

Pall Oenoflow PRO Service – Meeting the Demands of the Modern Wine Industry

IoT (Internet of Things) enabled devices are becoming more ubiquitous in businesses across all sectors. By 2020, the installed base of these devices is forecast to grow to almost 31 billion worldwide, increasing to over 75.4 billion devices by 2025.¹ Agriculture, and in particular the wine industry, are no exceptions to this trend. Many wineries already have a substantial number of devices that are IoT enabled. As increasingly significant amounts of data are moved from internal winery operations to the internet, it is vital that every step of the system is secure.

The Oenoflow PRO service allows users to connect their new or current Oenoflow filtration system to Pall's servers. Through this connection, Pall provides updates and access to its Oenoflow PRO Optimizer algorithm and Pall servers gather data used to populate its customer facing Oenoflow PRO apps and dashboards.

Oenoflow PRO Service

Feature	Feature Description	Benefits
Oenoflow PRO Optimizer	Algorithm that controls the Oenoflow PRO system during filtration	Manages filtration without operator input once system is started Delivers measurable OPEX improvements Reduces waste and lowers the environmental impact of filtration
Oenoflow PRO Online and Mobile Apps	Enterprise dashboarding	View all machines belonging to a single customer. Data can be aggregated for the whole group or shown for each individual machine or site.
	OPEX dashboard	Visualize savings achieved with Oenoflow PRO Optimizer algorithm.
	Reporting	Customizable detailed reports on OPEX alarms production data
	Real time system status	View current machine status at a glance.
	Push notifications	Receive alerts for machine alarms and production status changes.
	Batch traceability	Batch records for traceability and to meet future compliance needs.
	Live production data	View a simulated system HMI (Human Machine Interface) for detailed live process information.
	Maintenance dashboard	Track life and use of wear items for preventative maintenance scheduling.
	Documentation vault	Location of all system documentation for easy access. Users can also upload their own documents.
Remote connection for Pall technicians	Allows remote diagnosis to minimize downtime and reduce maintenance costs	

Customer Requirements for Installation

Customers with Oenoflow PRO equipped systems should arrange for access to the internet via one of the following scenarios. This should be available on the first day of system commissioning.

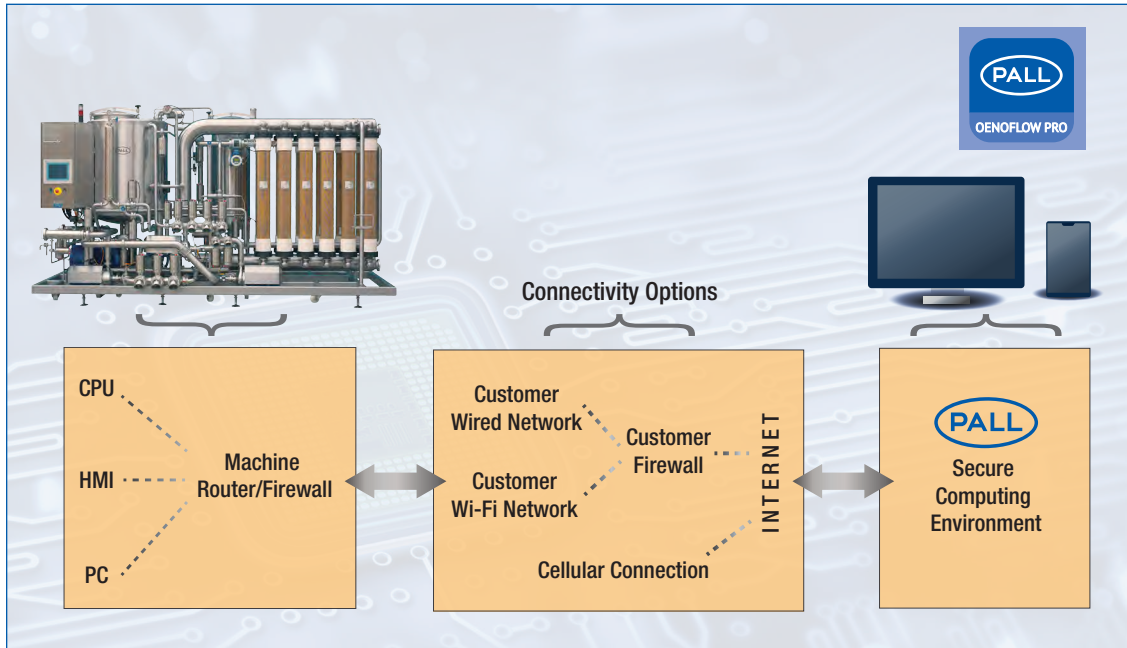
1. Shielded ethernet cable connected to the customer's network.
2. Access via customer's WiFi network.
3. To access the Internet, any customer network firewall that the system is connected to should permit outbound Internet access for TCP on port 443 in order to support the connectivity services.
4. If firewalls are an issue, then cellular data service SIM cards are suitable for local high-speed data service.

The Oenoflow PRO System Architecture

The Oenoflow PRO Service is hosted within the Pall Secure Computing Environment.

Figure 1 provides an overview of the Oenoflow PRO system architecture, highlighting the unidirectional flow of data. Users do not have the ability to change any of the data at the server but do have the ability to view the generated reports.

Table 1: Example architecture of an Oenoflow PRO system.



Frequently Asked Questions

Who can remotely access or control my Oenoflow PRO system?

- A firewall is built into the machine to protect from unauthorized access.
- Only users with authorized login credentials can access an Oenoflow PRO system features that are hosted in the Pall Secure Computing Environment.
- There are three types of users:
 - **Site Supervisor**, defined at initial commissioning of the system
The Site Supervisor manages access credentials for all Site Operators.
 - **Site Operator**
 - **Pall Technician**
- The “System Pause” function is the only command that is available remotely.
 - It can be accessed by Site Operators as designated by the Site Supervisor.
 - Pall Technicians do not have access to it.
 - This feature can be disabled upon request.

Can the machine access anything else in my facility?

- No, any connection to local networks is solely used for outbound internet access. Pall has specific connection guidelines to minimize the interaction between the machine and your local networks implemented during system commissioning.

How is the machine protected from malware or security vulnerabilities?

- The Oenoflow PRO system has antivirus protection installed and enabled at time of manufacture. Antivirus update and software patches are delivered over-the-air via the connection between the Pall Secure Computing Environment and the Oenoflow PRO system.

How is the machine's software kept up-to-date?

- Updates are provided for systems that have active service subscriptions.

How is the data protected as it moves from my machine to the Pall Secure Computing Environment?

- The connectivity software uses TLS and HTTPS to ensure that data being transmitted is encrypted as per industry standards.

How is access controlled to the data in the Pall Secure Computing Environment?

- Only users with valid user credentials can access data.
- Only customer defined users and Pall administrators have access.

What personally identifiable information is collected and how is it used?

- Access to iOS and Android apps require email, phone number and mobile device identifying information. These are used only to contact the user as needed to provide service (e.g. operations alerts and emailed reports). This data is not given or sold to any other parties.

What happens when the Oenoflow PRO platform experiences a connectivity outage?

- Oenoflow PRO is supplied as a standalone hardware system. If connectivity is lost the Oenoflow PRO Optimizer algorithm will still operate normally. Once connectivity is re-established, the algorithm will upload its data to Pall servers and any updates needed will be downloaded to the machine if a valid license is in place.

Pall Secure Computing Environment Security Summary

Security controls applied within machine

- All connections to the Pall Secure Computing Environment are initiated from the machine, outbound connections only.
- All connections to the Pall Secure Computing Environment use commercial best practice encryption to protect the connection – HTTPS and TLS.
- The PC installed in the machine is configured by Pall to allow the least privileged access needed to operate needed software, and is hardened per CIS standards.
- The machine incorporates a router with firewall capability, preventing inbound access to any equipment within the machine.
- The router and PC equipment have been penetration tested, allowing Pall to mitigate security findings as exposed.
- The PC software has the ability to receive operating system and application software patches from the Pall Secure Computing Environment, allowing Pall to deploy verified updates.
- The PC has virus scanning protection enabled and kept up to date.
- The PC has an audit log enabled with logs backed up to the Pall Secure Computing Environment on a regular basis.
- The remote access software installed on the PC uses industry best-practice controls for connection protection as well as user authentication and authorization.

Security controls applied in Pall Secure Computing Environment

- All data stored within the environment is encrypted at rest and while in transit.
- All data access methods use APIs protected by HTTPS and require user authentication and authorization following industry best-practice.
- User logins enforce password complexity rules ensuring strong passwords.
- User logins are forced to log out after a period of inactivity.
- Successful and failed login attempts are logged for all users.
- “Superuser” access to the environment is controlled with 2-factor authentication and all administrative accesses are logged. Role-based access control is used to restrict access to environment data and services.

References

- 1: Statista, Spending on the Internet of Things worldwide by vertical in 2015 and 2020 (in billion U.S. dollars)



Pall Food and Beverage

25 Harbor Park Drive
Port Washington NY 11050
+1 516 484 3600 telephone
+1 866 905 7255 toll free US

foodandbeverage@pall.com



Visit us on the Web at www.pall.com/foodandbev

Pall Corporation has offices and plants throughout the world. For Pall representatives in your area, please go to www.pall.com/contact

Please contact Pall Corporation to verify that the product conforms to your national legislation and/or regional regulatory requirements for water and food contact use.

Because of technological developments related to the products, systems, and/or services described herein, the data and procedures are subject to change without notice. Please consult your Pall representative or visit www.pall.com to verify that this information remains valid.

© Copyright 2020, Pall Corporation. Pall, (PALL), and Oenoflow are trademarks of Pall Corporation.
® Indicates a trademark registered in the USA. *Filtration. Separation. Solution.sm* and BETTER LIVES. BETTER PLANET are service marks of Pall Corporation.