OneLab Documentation

Waters™ | Andrew Alliance™

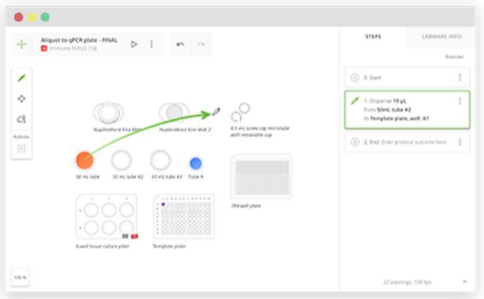
Version	*Date*	*Author*	*Rationale*
1	03/24/2020	A. Pegaz-Blanc	First version
2	04/07/2021	A. Pegaz-Blanc	Update Enterprise deployment section and requirements
3	06/10/2021	A. Pegaz-Blanc	Add data information and update requirements
4	07/07/2021	A. Pegaz-Blanc	Update Enterprise deployment section and requirements
5	12/14/2021	A. Pegaz-Blanc	Update Enterprise deployment section and requirements
6	05/10/2022	A. Pegaz-Blanc	Update network requirements

1. Presentation

A unique browser-based software environment enabling researchers to design, and share, their own protocols, through a highly intuitive graphical interface that can then be executed step-by-step, from any PC or tablet.

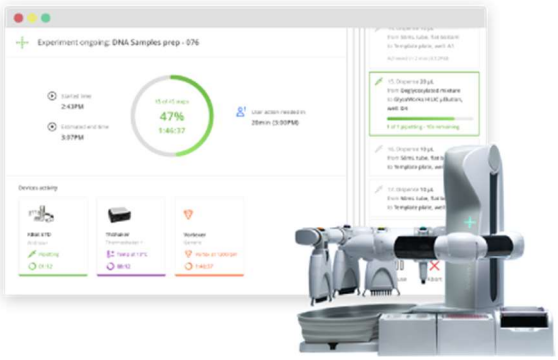
Design protocols

- Intuitive graphical drag-and- drop design interface.
- Eliminate error-prone calculations for serial dilutions and concentration normalizations.
- Accelerate collaboration and training by easily sharing protocols with other researchers.



Execute experiment

- Ensure correct manual execution of protocols, with your current set-up.
- Guarantee reproducibility with secure communication of protocols to OneLab compatible device(s).
- Connectivity with Andrew+ and Pipette+, or any other connected device, enabling researchers to achieve the highest levels of repeatability and productivity, with the added advantage of full traceability.



OneLab is free-to-use on onelab.andrewalliance.com but can also be deployed privately according to your needs (Enterprise or Standalone deployment)

More information on the website: https://www.andrewalliance.com/laboratory-software/ and on the Help Center: https://help.andrewalliance.com/

2. Server deployments

2.1. SaaS: Public cloud

Description

OneLab is deployed as a multi-tenant SaaS (Software-as-a-Service) application, on an AWS Amazon server, public and free-to-use.

OneLab is maintained and supported by Andrew Alliance.

Installation

No installation. The server is already up and running on https://onelab.andrewalliance.com

Updates

OneLab is automatically updated with every new version (major and minor).

Before each update, the users will be notified through Intercom at least one week in advance.

The release notes are available on the Help Center: https://help.andrewalliance.com/

Requirements

OneLab instance must be reachable by the connected devices and by the user's computers according to the following requirements:

- Between OneLab SaaS and User's computers

Service	Source	Destination	Port	Type	Protocol	Direction
OneLab	User's PC	onelab.andrewalliance.com (52.72.22.49)	443	HTTPS	TCP	Outbound
HelpCenter	User's PC	help.andrewalliance.com (52.72.22.49)	443	HTTPS	TCP	Outbound
reCAPTCHA	User's PC	*.gstatic.com	443	HTTPS	TCP	Outbound
	User's PC	*.recaptcha.net	443	HTTPS	TCP	Outbound
Intercom	User's PC	*.intercom.io	443	HTTPS	TCP	Outbound
	User's PC	*.intercomcdn.com	443	HTTPS	TCP	Outbound
	User's PC	static.intercomassets.com	443	HTTPS	TCP	Outbound

- Between OneLab SaaS and connected devices:

Service	Source	Destination	Port	Type	Protocol	Direction
OneLab	Device	onelab.andrewalliance.com (52.72.22.49)	5671	AMQPS	TCP	Bidirectional*
	Device	onelab.andrewalliance.com (52.72.22.49)	443	HTTPS	TCP	Outbound

* The data exchange is bidirectional (inbound and outbound traffics) but the communication with OneLab server is always started by the device (outbound connection).

Additional information

- OneLab SaaS is always up-to-date, which may require the upgrade of the connected device firmware
- Multi-tenant and shared platform (even if the data are properly isolated and segregated in the database)
- No custom integration

2.2. Enteprise: On-premise

Description

OneLab Enterprise deployment is a private on-premise deployment on a cloud or private server, allowing an access for only specific users and connectivity with external services to process your data.

OneLab is maintained and supported by the customer.

Installation

OneLab is installed on your private server by your IT team with the Andrew Alliance support.

Andrew Alliance provides resources, release notes and assistance if needed.

Updates

You will be notified for every new version (major and minor), and you have full control on the OneLab updates. We let you decide if you want to update (or not) according to your needs and your internal processes.

Andrew Alliance provides resources, release notes and assistance if needed.

Requirements

- Supported distributions:
  - Ubuntu 16.04, 18.04 or 20.04
  - CentOS 7 or 8
  - RedHat 7 or 8
  - Debian 10
  - Fedora 33 or 34

- Minimal technical requirements
  - Min. 8 GB of RAM (depends on the # of users and the scalability policy)
  - Min. 64 GB of hard drive space (depends on the # of users and the scalability policy)

- Pre-installed dependencies/tools requirements
  - Docker CE (min. 20.10.0) & docker-compose
    - https://docs.docker.com/engine/install/ubuntu/)
  - Ansible (min. 2.9.6)
    - Installing Ansible — Ansible Documentation)

- Resources
  - Public or Internal DNS domain (required for HTTPS configuration)
  - SSL certificates (required for HTTPS configuration)
    - Public .crt, private .key and fullchain.pem files
  - SMTP server access (optional, only if you want email notifications)
  - reCAPTCHA account (optional, only if you want to enable external registration)

OneLab instance must be reachable by the connected devices and by the user's computers according to the following requirements:

- Between OneLab server and User's computers

Service	Source	Destination	Port	Type	Protocol	Direction
OneLab	User's PC	Private OneLab server DNS/IP	443	HTTPS	TCP	Outbound
HelpCenter	User's PC	help.andrewalliance.com (52.72.22.49)	443	HTTPS	TCP	Outbound
reCAPTCHA (optional)	User's PC	*.gstatic.com	443	HTTPS	TCP	Outbound
	User's PC	*.recaptcha.net	443	HTTPS	TCP	Outbound
Intercom (optional)	User's PC	*.intercom.io	443	HTTPS	TCP	Outbound
	User's PC	*.intercomcdn.com	443	HTTPS	TCP	Outbound
	User's PC	static.intercomassets.com	443	HTTPS	TCP	Outbound

- Between OneLab server and connected devices:

Service	Source	Destination	Port	Type	Protocol	Direction
OneLab	Device	Private OneLab server DNS/IP	5671	AMQPS	TCP	Bidirectionnal*
	Device	Private OneLab server DNS/IP	443	HTTPS	TCP	Outbound

* The data exchange is bidirectional (inbound and outbound traffics) but the communication with OneLab server is always started by the device (outbound connection).

OneLab server should also be allowed to communicate with the external OneLab repository to get the latest versions and resources in case of update.

The restriction could only be allowed for the updates.

- Between OneLab server and Internet:

Service	Source	Destination	Port	Type	Protocol	Direction
OneLab Repository	OneLab	hub.andrewalliance.com	443	HTTPS	TCP	Outbound
Docker Repository	OneLab	hub.docker.com	443	HTTPS	TCP	Outbound

2.3. Standalone: Local hardware

Description

The deployment of OneLab is delivered on a physical server provided with Wi-fi APN and Ethernet connectivity for connected devices.

This deployment of OneLab allows having:

- A single user (administrator)
- Up to 5 connected devices

Installation

No installation is required. OneLab is already up and running on the hardware.

Updates

No automatic update. The system can be updated with a fee by shipping it to our repair center.

Requirements

- OneLab Standalone may require an Ethernet switch in case more than 1 devices must be connected to the server using Ethernet connection.

Additional information

- HTTP communication only
- No real-time support chat with Andrew Alliance team (Intercom)
- The version of OneLab is frozen: updates are possible with an extra fee
- Single OneLab user (administrator)
- Maximum number of connected devices: 5

3. Client requirements

OneLab is a web-based app and accessible from any modern web browser.

The supported browsers are:

- Chrome (v77 or newer)
- Firefox (v65 or newer)
- Edge (v44 or newer, but v80 or newer are recommended)
- Safari (v13 or newer)

OneLab is optimized for a minimal resolution of 1280px x 720px.

4. Security & Data management

OneLab is a connected software environment ensuring security of your lab protocols through secure user identification and access control.

All data exchanges are secure using SSL/TLS encryption (RSA 512 & 256).

OneLab stores data in a consistent way for future analysis, traceability, and data validation. Sensitive data are also encrypted in database.

User information which are stored by OneLab:

- Full name
- Work email
- Encrypted password
- IP and User agent for each session
- Login and logout activities

OneLab stores data related to:

- Configuration information: devices, labware, dominos, reagents, licenses,...
- Protocols describing the actions in the methods.
- Experiment reports documenting an execution of a defined protocol: sample names and IDs, sample tracking, dilution calculations, review and approval signatures.

5. Device management

Each device requires to be paired and activated in OneLab before to be operational.

The pairing is done via a web-based app accessible from a web browser on PC, Smartphone or Tablet equipped with Wi-Fi connection.

The device can be connected either with an Ethernet cable or through Wifi. The captive portal authentication system (or similar using username/password credentials) is not supported.

After few HTTPS calls in order to obtain the device credentials, which will be stored on the device, the device will be paired and accessible in OneLab.

The device activation will require a License and an Activation key (obtainable with Andrew Alliance support) and can be performed directly in OneLab.

Afterward, the device communicates with OneLab in real-time through AMQPS protocol (no polling).

The data exchange is bidirectional (inbound and outbound traffics) but the communication with OneLab server is always started by the device (outbound connection).

OneLab and the device only exchange data about:

- Device authentication
- Device status
- Experiment data and scheduling