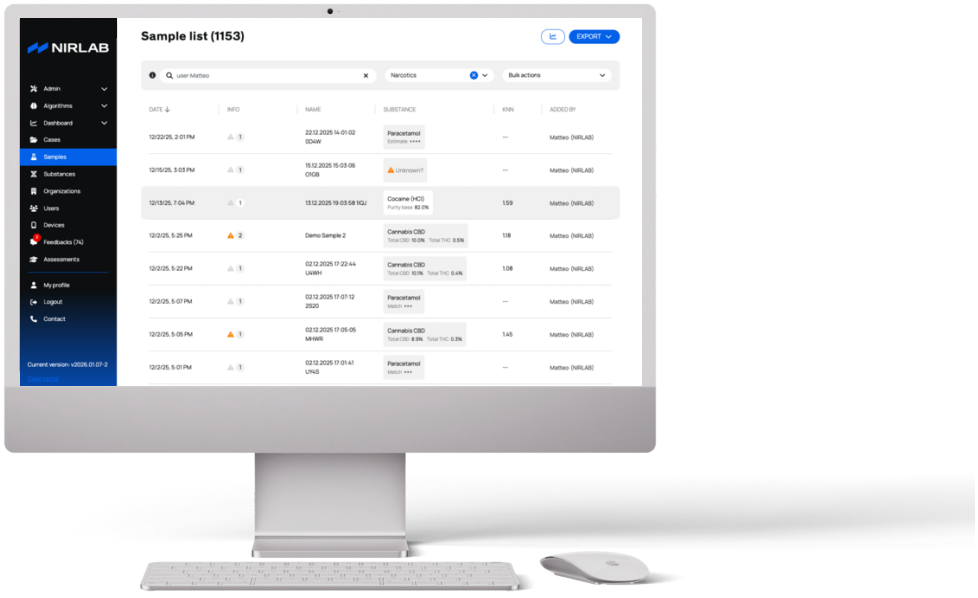
NIRLAB

Administration Guide



General

Version 2.0 - February 2026

TABLE OF CONTENTS

1 Introduction 2
1.1 Purpose of this guide 2
1.2 Organization of this guide 2
2 User management 3
2.1 Initial admin account creation 3
2.2 Creating user accounts 5
2.3 Change and reset passwords 7
2.4 User settings & permissions 10
3 Organization management 12
3.1 Configuring an organization 12
3.2 Creating Teams 14
4 Security and Privacy 15
4.1 General principle 15
4.2 Encryption 15
4.3 Network configuration 16
4.4 Development process 16
4.5 Backup and recovery 16
4.6 Access logs 16
4.7 Infrastructure location 16
5 Appendix 17
5.1 Version History 17

1 INTRODUCTION

1.1 Purpose of this guide

The purpose of this guide is to provide a comprehensive overview and practical instructions for managing and securing your organization within NIRLAB's platform. It aims to equip security teams and administrators with the knowledge and tools necessary to effectively oversee user accounts, manage Teams, and ensure compliance with privacy regulations.

The expected readers of this guide are administrators responsible for managing and securing their organization within NIRLAB's platform, and security experts wishing to assess the security of the NIRLAB products.

1.2 Organization of this guide

The content of this guide covers three main topics.

Section 2 of this guide focuses on user management, detailing how to create user accounts and assign appropriate permissions.

Section 3 covers organization management, detailing how information scoping works across organizations and how Teams can be created and configured to match customer's administrative structures.

Section 4 details data and privacy protection in NIRLAB's platform.

2 USER MANAGEMENT

2.1 Initial admin account creation

New NIRLAB customers will be granted access to an administration account for their organization. NIRLAB will send you an email containing a link to set a password for the admin account. The link will be active for 7 days. This link opens the following page:

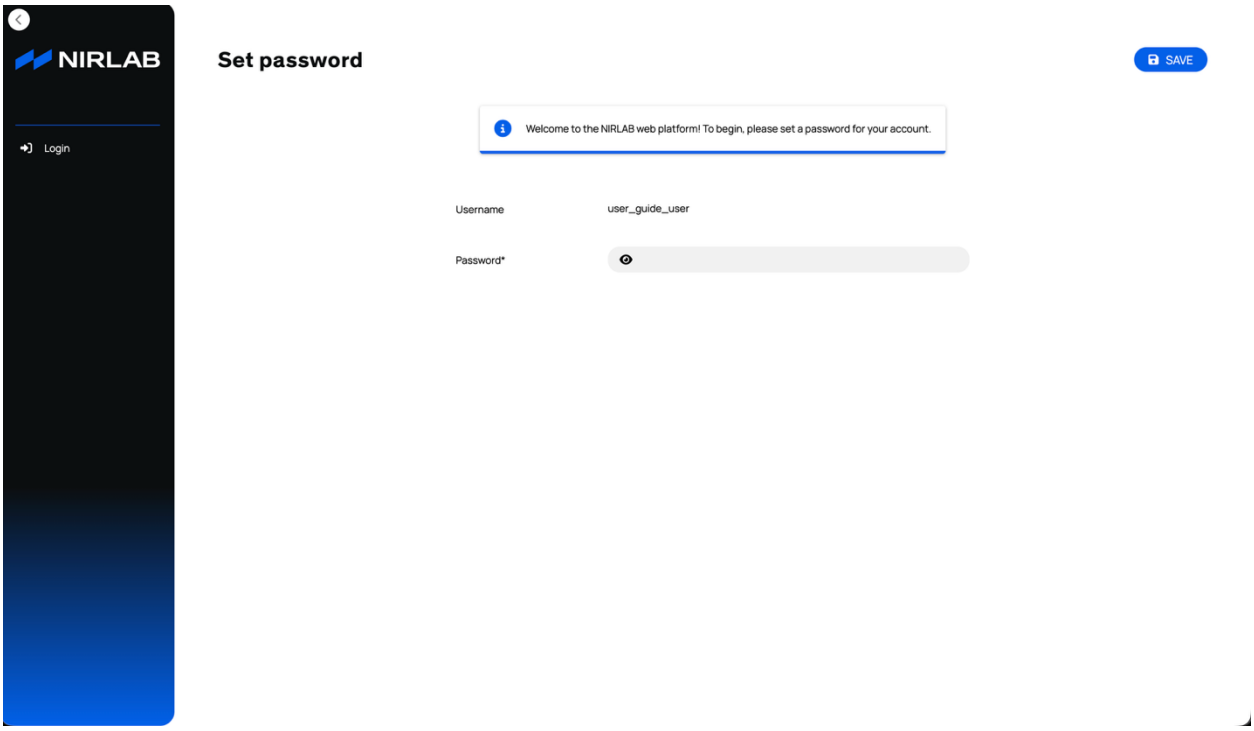


Figure 1: Set password page

First, take note of your username and set a password in the dedicated field and click the “save” button. Passwords must be at least 9 characters long. Other password quality checks may trigger an error. When the password has been set, you will be directed to the login page where you can login with your username and new password.

Note: If your organization has set up single sign-on (SSO) for the NIRLAB web app, please click on “Enterprise Login” and enter your organization’s email address. You will then be redirected to your organization’s login page. SSO access for other services does not automatically apply to NIRLAB.

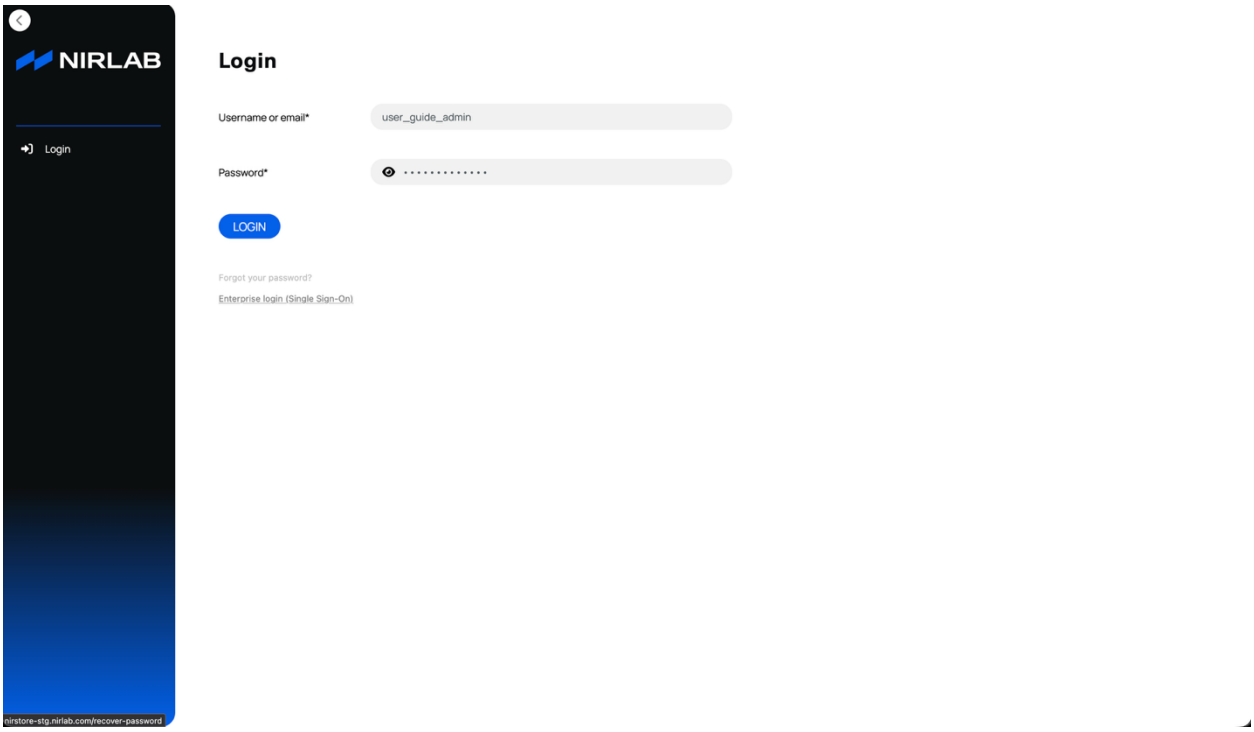


Figure 2: Login page

After logging in, you will be taken to the "**Sample list**" page. You can use the menu on the left to navigate to other sections of the platform.

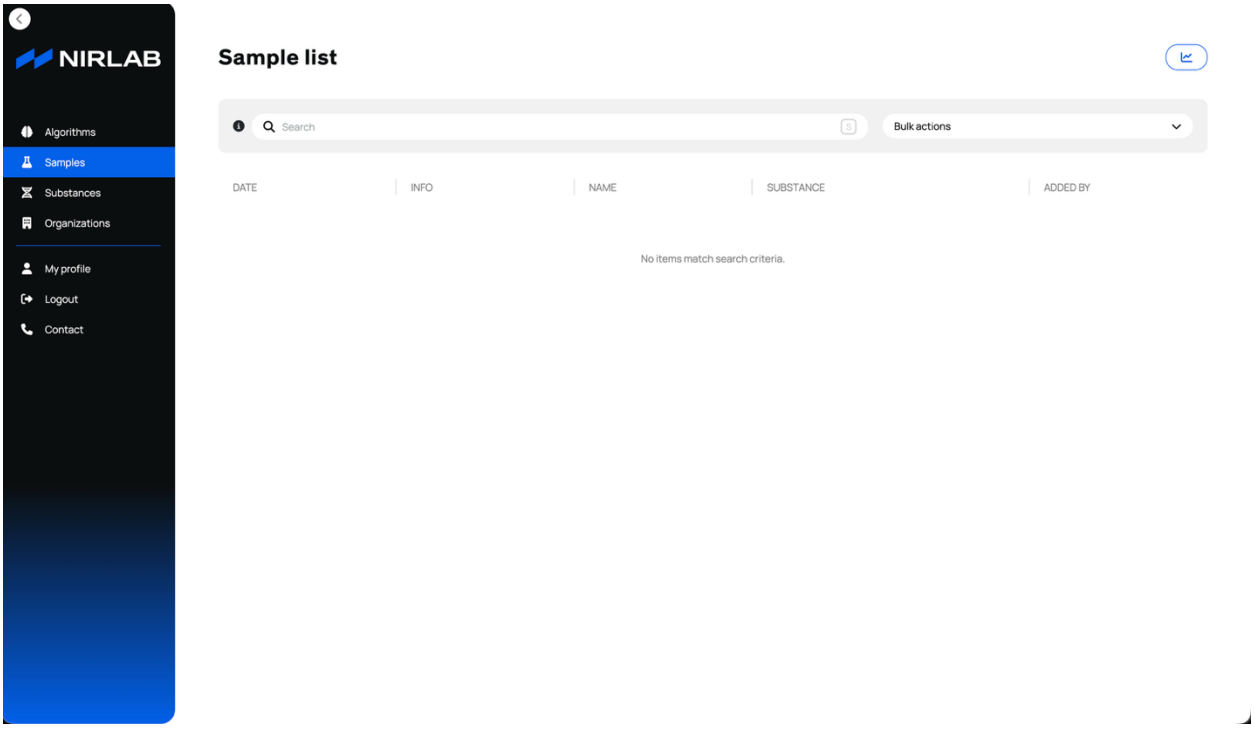


Figure 3: Sample list page

2.2 Creating user accounts

To add users to your organization, first select the "**Organizations**" item in the menu on the left. Then click on your organization in the list to go to the organization detail page.

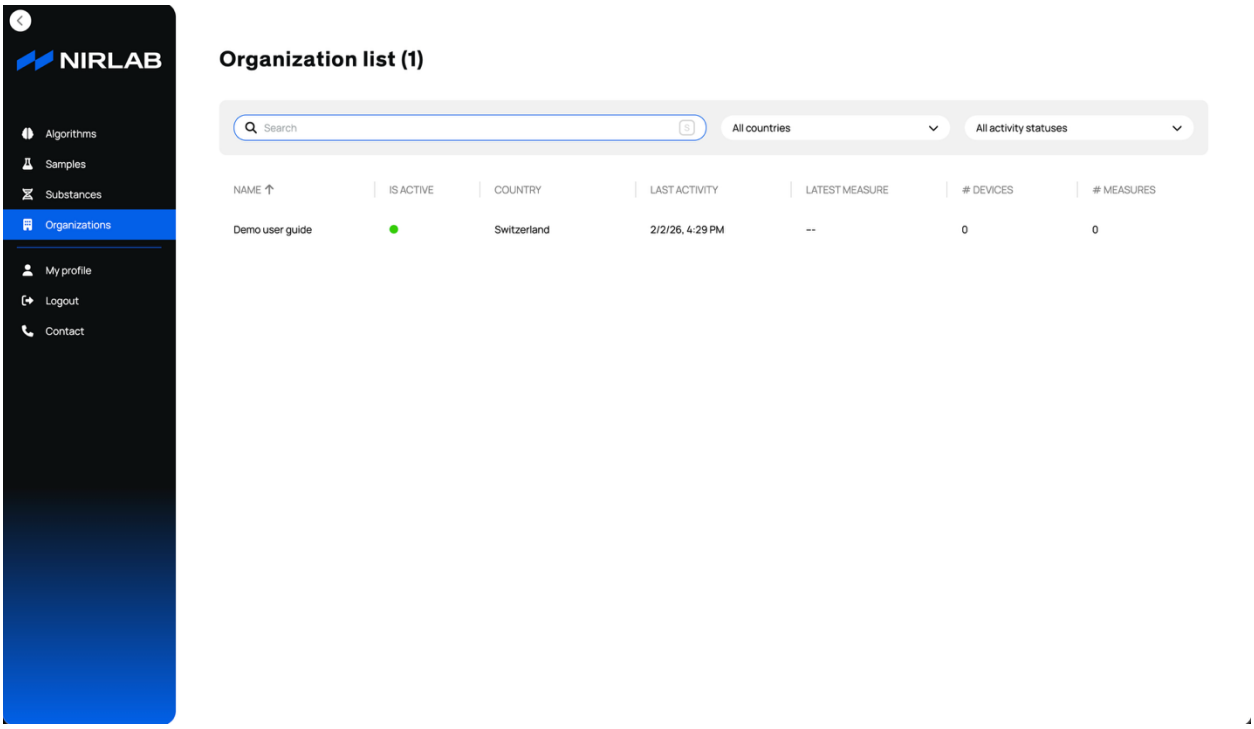


Figure 4: Organization list page

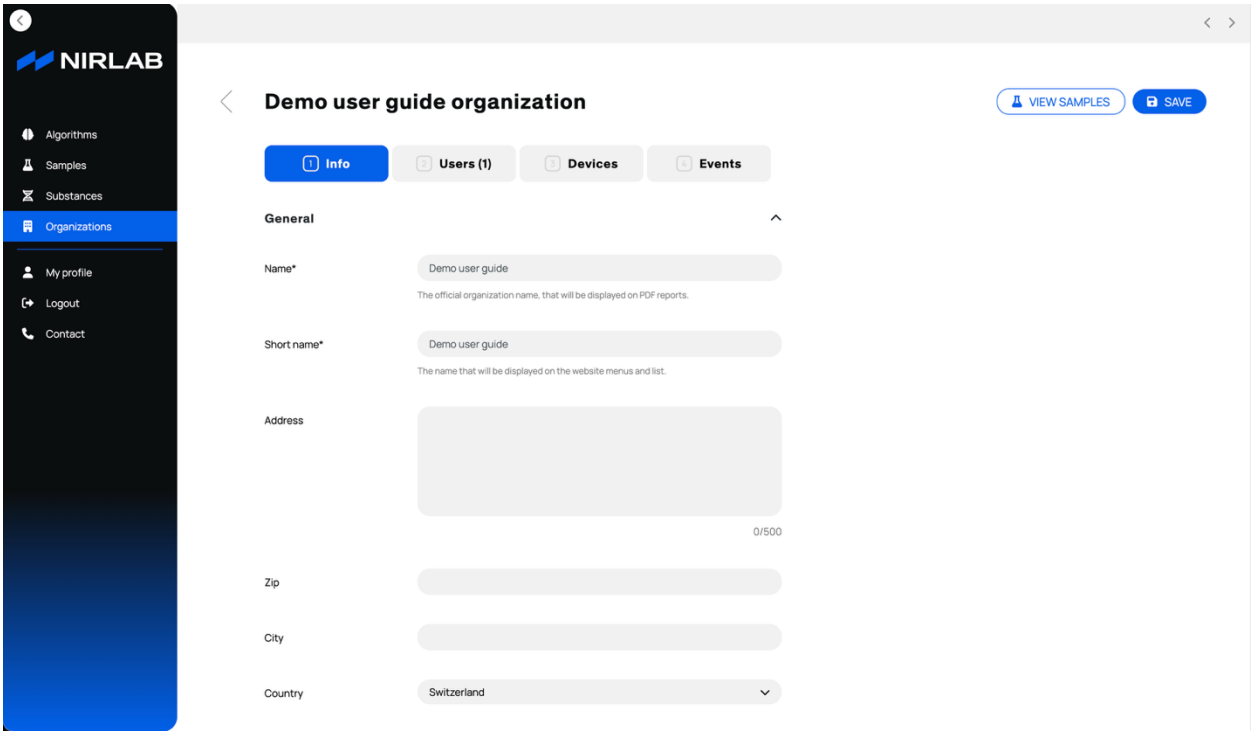


Figure 5: Organization detail page

Go to the organization details page and select the "**Users**" tab. From there, you can add a new user by clicking the "**Add User**" button in the top right corner.

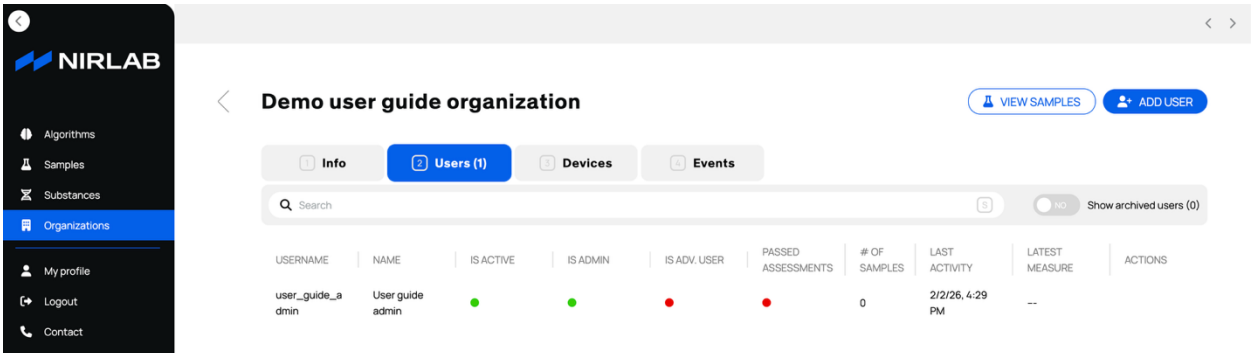


Figure 6: "Users" tab in organization detail page

Clicking the "**Add User**" button opens the user creation page. Here, you need to enter the user's *Username* (lowercase letters only, no spaces or special characters), *display name*, and *email address*. You can also assign organization administrator rights if needed. Once the form is complete, click "**Save**". You will then be asked to confirm the email address to finalize the creation of the user.

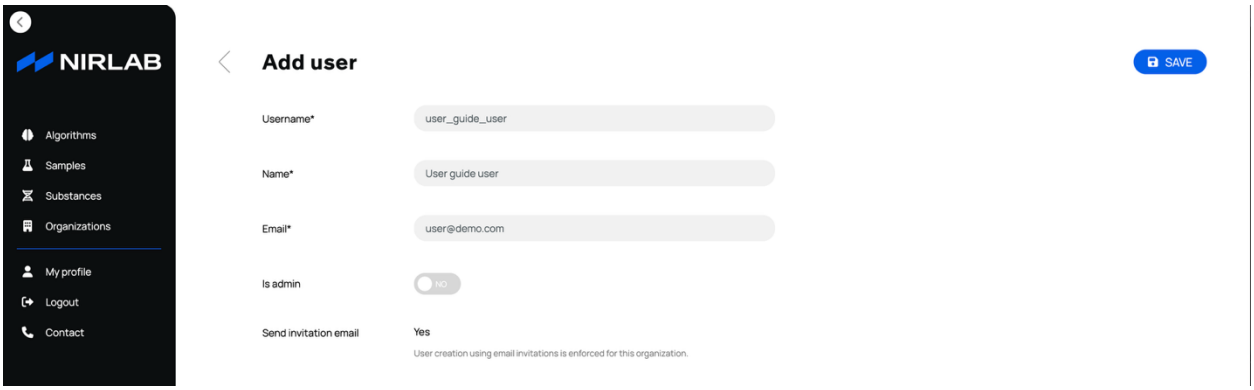


Figure 7: User creation page

After creating the user, an invitation link will be generated. The created user will receive an invitation link by email.

Note: Each email address can only be used for one user; multiple users cannot share the same email address.

You can optionally edit a user's permissions after creation by clicking the "**Edit User**" button. See Section 2.4 for a detailed list of available permissions.

After following the invitation link, the new user will see the user interface described in Section 2.1.

2.3 Change and reset passwords

A user can update his/her own password by clicking the "**My profile**" item in the left menu and then click the "**change password**" button on the top right.

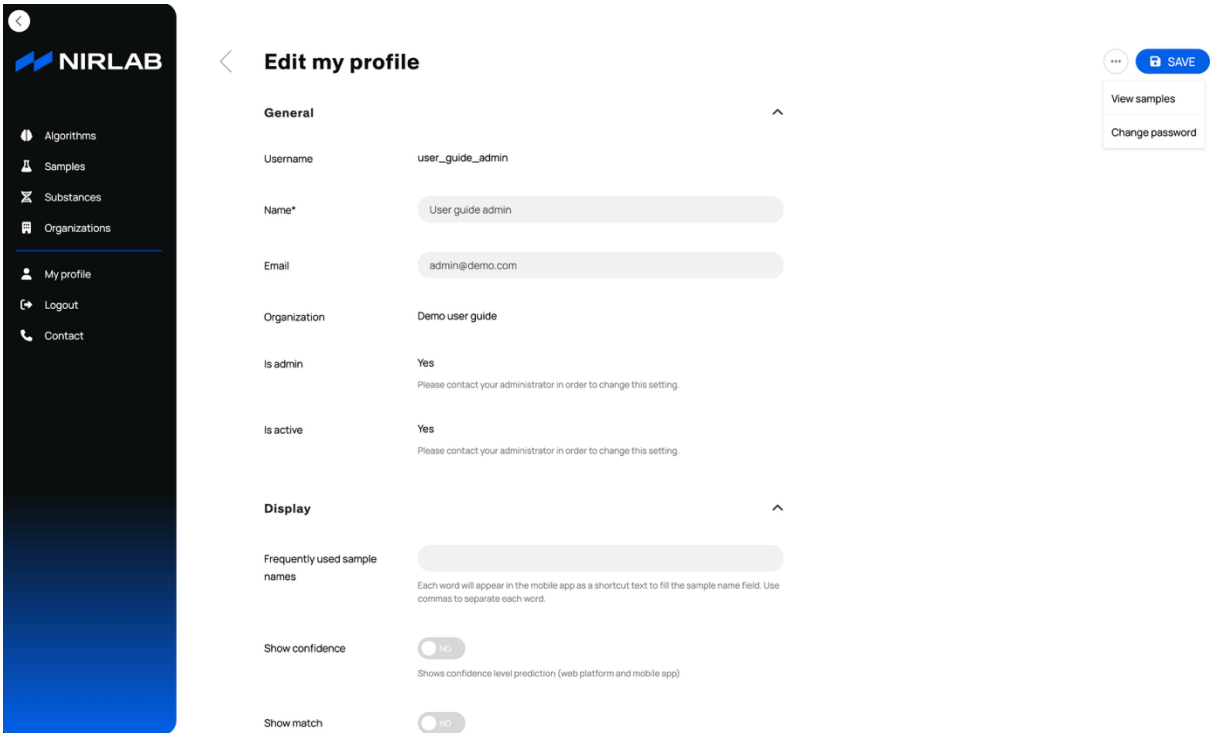


Figure 9: My profile page

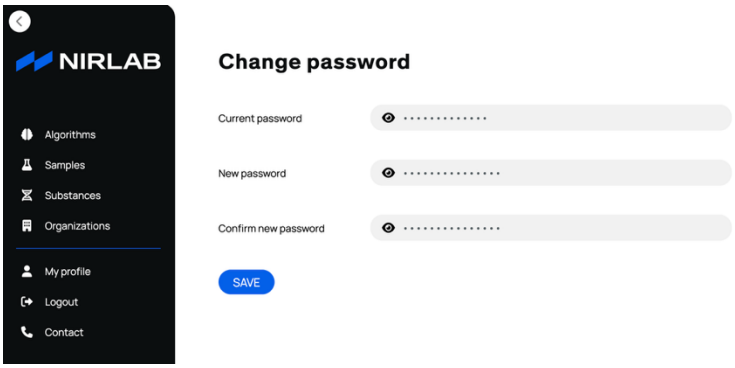


Figure 10: Change password page

An administrator can reset the password of another user by going to the user's organization detail page and clicking the user in the "**Users**" tab (see figure 6) and then clicking the "**Reset password**" button on the top right of the "**user detail page**". This opens the reset password page, where you can choose to log the user out of the NIRLAB mobile app and web platform or not. After confirming password reset, a link to reset the target user password will be shown. You should send this link to the user through a secure communication channel. Note that the NIRLAB platform does not send automatic password reset emails.

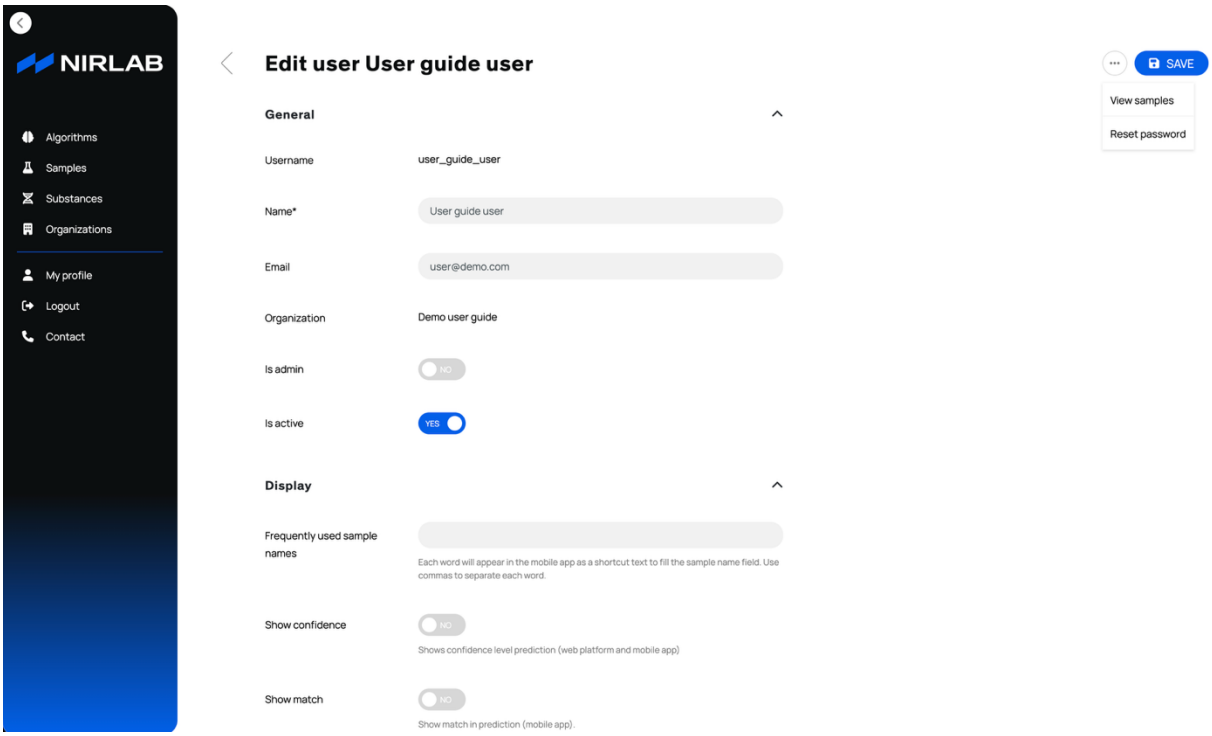


Figure 11: User detail page

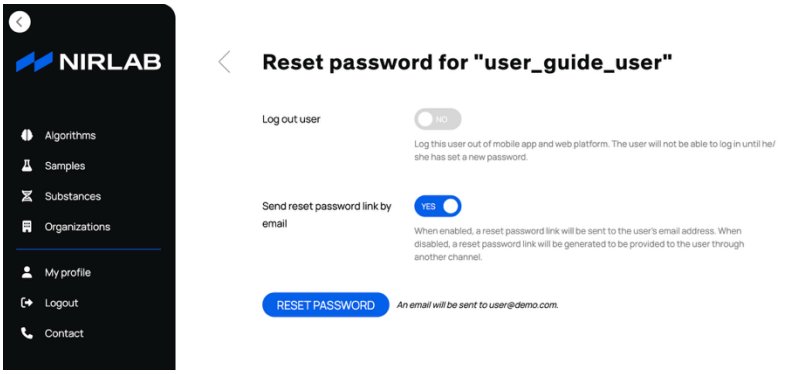


Figure 12: Reset user password page

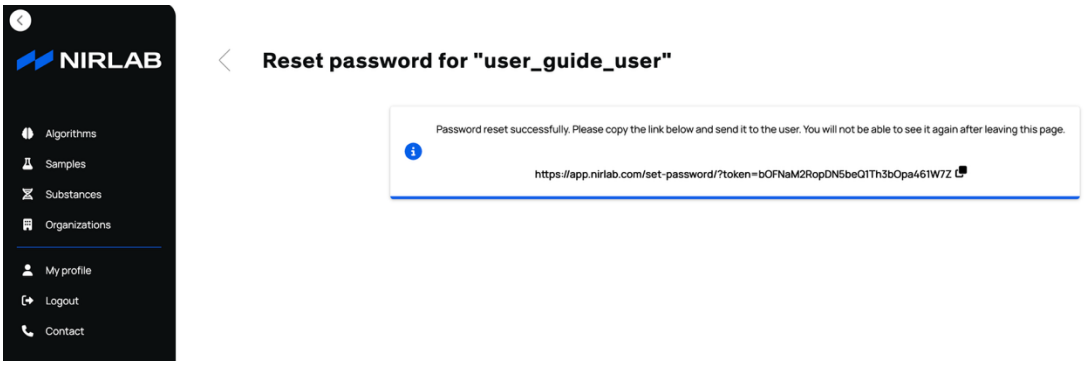


Figure 13: Reset password link after password reset

2.4 User settings & permissions

In the user detail page, which can be accessed by clicking on a user in the "**Users**" section of the "**organization detail**" page (see figure 6), administrators can configure the settings and permissions of a user. The list of permissions is detailed in the table below:

Setting/permission	Description
Is admin	Defines if the user is an administrator of the organization. Administrators can create new users, view all organization measures, create Teams (if the organization is allowed to), view Teams measures, view the organization dashboard.
Is active	Defines if the user is active. When set to false, this user will no longer be able to log in. For example, when an employee leaves the organization.
Frequently used sample names	This optional setting can contain a comma separated list of commonly used sample names that will be displayed in the mobile app to ease sample name entry in the sample scan mode.
Show confidence	Defines if a confidence level value is displayed in the mobile app when showing analysis results and in PDF reports. This setting is not recommended for general use and should only be enabled for advanced users.
Show match	Defines if a match level value is displayed in the mobile app when showing analysis results. This setting is not recommended for general use and should only be enabled for advanced users.
SNV spectra first	Defines if the spectrum displayed by default after a measurement in the mobile app should be normalized with the SNV method or should be the raw absorbance spectrum. Users can always switch between SNV and raw spectra in the mobile app.

Show warning banner on PDF reports	Defines if a warning banner stating that results are for internal use only should be displayed in PDF reports when generated by this user.
Show only regressor of detected chemical form	Defines if quantitative results (e.g. purity of sample) should be displayed for all chemical forms of the substance (e.g. base and HCl for cocaine), or only in the chemical form of the analysed sample.
Show deleted objects	Defines if deleted measures are displayed in the sample detail page.
Is advanced user	Defines if the user can access advanced features on the prediction results in the measurement detail page.
Can see organization measures	Defines if the user can see all organization measures or only the measures performed by himself/herself.
Can export spectra	Defines if the user can export spectral data as a CSV file.
Can access dashboard	Defines if the user can view the organization dashboard. Admin users can always see the dashboard regardless of this setting.

3 ORGANIZATION MANAGEMENT

3.1 Configuring an organization

Organization administrators can edit their organization data by selecting it in the "**organization list"** (see figure 4) and using the form in the organization detail page (see figure 5). The list of fields that can be edited is described in the table below:

Field	Description
Name	Name of the organization that will be displayed in PDF reports.
Short name	Name of the organization that will be displayed in the web platform and mobile app.
Address	Street address of the organization.
Zip	Zip code part of the organization full address.
City	City part of the organization full address.
Country	Country part of the organization full address.
Currency	Currency that the organization uses for payments.
Image	Logo of the organization that will be displayed in PDF reports.
Support name	Name of the support service that will be displayed in the mobile app and on the contact page for organization users. If left blank, the name will default to the value of the organization's retailer.
Support phone number	Phone number of the support service that will be displayed in the mobile app and on the contact page for organization users. If left blank, the name will default to the value of the organization's retailer.

Support email	Email address of the support service that will be displayed in the mobile app and on the contact page for organization users. If left blank, the name will default to the value of the organization's retailer.
Can record geolocation	If enabled, users will be able to choose whether to send geolocation with measurements in the mobile app settings. If disabled, geolocation will never be sent with measurements from the mobile app.
Geolocation required	If enabled, geolocation will always be sent with measurements from the mobile app. If disabled, users will be able to choose whether to send geolocation with measurements in the mobile app settings. Note that in any case, measures may be sent without geolocation information if the user's phone is not able to provide location data.
Allow sample grouping by case	If enabled, samples can be grouped in the "Cases" list and detail pages using a defined regular REGEX expression. This only works for structured naming schemes.
Allow retailer view	If enabled, the retailer of the organization will be able to see the samples analyzed by this organization. If disabled, only members of the organization will be able to see the measures.
Algorithms	The list of algorithms (substance libraries) to which the organization has access.
Default lab	Default laboratory that will be pre-selected when adding lab results. Leave blank to not prefill the field. New labs can only be added by NIRLAB. Please reach out to NIRLAB if you would like to add a lab.

In addition to the organization data form, the organization details page also displays a list of its users and the spectrometers associated with the organization. These can be accessed by clicking the tabs below the page title (see figures 6, 14 and 15).

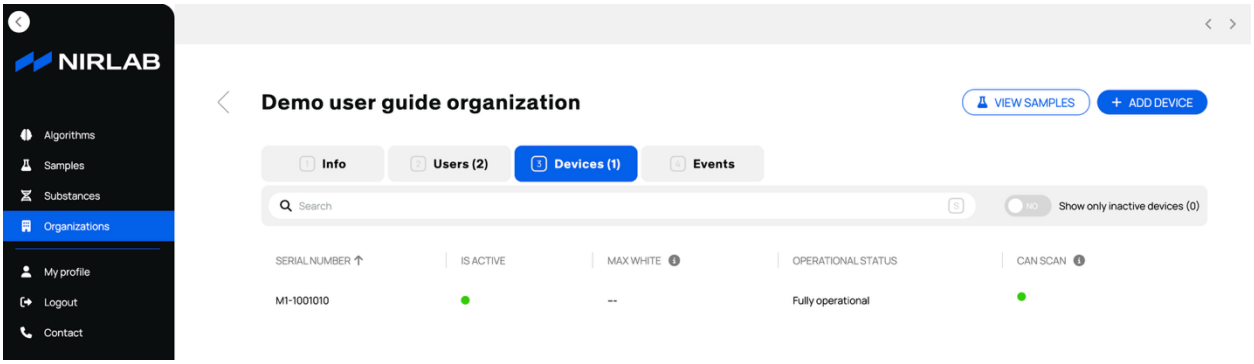


Figure 14: Devices tab in organization detail page

3.2 Creating Teams

Organizations can create **Teams**, which act as sub-organizations within a larger organization. Teams are particularly useful when multiple departments use NIRLAB products but should not share data with each other, while still allowing administrators to view all measurements and perform analytics across departments. This feature is also well suited for large organizations with multiple devices deployed across different sites, as well as organizations with complex administrative structures.

To enable the Teams feature for your organization, please contact the NIRLAB support team.

Once activated, organization administrators can create Teams by navigating to the **"Teams"** tab on the organization details page and clicking the **"Add Team"** button.

Note: A user can only be part of one team at the time.

Please also take a moment to review the user permissions and sample visibility for each user.

4 SECURITY AND PRIVACY

4.1 General principle

As a NIRLAB customer, you can rely on the expertise of our dedicated team to protect your data with the greatest care. Since NIRLAB products are cloud based, you do not need to manage complex technical issues, and can confidently delegate this task to our team of experts that has an intimate knowledge of our products and their configuration. For the sake of transparency, this chapter of the administration guide thoroughly describes how NIRLAB secures your data.

NIRLAB's information security approach starts with one core principle: to collect and store only the minimal necessary information to provide our services, without sharing data with third parties. This principle guides the development of every NIRLAB product, and it is possible to use them without storing any personal information by using user and sample names that are not related to actual names. Sensitive data collection (e.g. measure location) is always optional.

The exhaustive list of collected data and collection purpose is available in the "NIRLAB – Collected user data" document.

In addition to this minimal data collection principle, NIRLAB takes technical and organizational measures to ensure that information security is always guaranteed. These measures are described in the following sections.

4.2 Encryption

All communications between clients (web and mobile app) and NIRLAB servers are encrypted using state-of-the-art protocols (TLS 1.2/1.3 with an up-to-date cipher suite).

Data at rest is not encrypted to support application functionality (search, analytics, etc.).

Passwords are stored using a state-of-the-art method, PBKDF2 (Password-Based Key Derivation Function 2).

4.3 Network configuration

Restrictive firewall access rules are maintained by NIRLAB's IT team. Administrative server access is secured with individual ED25519 or RSA 4096 bits ssh keys. Cloud administration interfaces are accessed by individual, two-factor authenticated accounts.

4.4 Development process

All NIRLAB products follow a strict development process to ensure the highest quality.

- Every change of NIRLAB's products code is reviewed by a at least one other developer.
- Automated tools enforce high code quality standards.
- Automated tests minimize the risk of bugs.
- Automated deployment process ensures high reactivity in case of problems.
- Regular dependency updates minimize the attack surface.
- Automated vulnerability scans ensure that our servers are always secure.

4.5 Backup and recovery

NIRLAB's systems are regularly backed up, with snapshots for fast recovery and with long term archives hosted on a dedicated system.

4.6 Access logs

Access, modification and deletion of important data is logged by our systems. These logs are not accessible to customers, but NIRLAB can provide extracts upon legitimate request.

4.7 Infrastructure location

NIRLAB's cloud platform is hosted at two different locations, depending on the application domain. Data of customers using NIRLAB's Narcotics analysis solution is hosted in the datacenter of the University of Lausanne, located in Lausanne, Switzerland. Data of customers of other NIRLAB products is hosted in the Amazon Web Services datacenter in Paris. Analysis of spectral data is always done on a dedicated server in the datacenter of the University of Lausanne, but no data is stored by this server.

5 APPENDIX

5.1 Version History

Version	Date	Major changes
2.0.0	04.02.2026	Rebranding
1.0.0	07.06.2024	Initial version