



Sara Alert TM
Secure monitoring and reporting for public health

User Guide for Administrators

Release 1.14
October 13, 2020

Table of Contents

Table of Contents.....	ii
1 ABOUT SARA ALERT™.....	3
1.1 Concept of Operations.....	3
1.2 SMART on FHIR API.....	4
1.2.1 Get Started Using the API.....	4
1.2.2 Supported Workflows	4
1.3 Sara Alert™ Record Retention	5
2 ADMINISTRATOR ROLE OVERVIEW	5
2.1 Record Access	5
3 GETTING STARTED.....	5
3.1 Logging In.....	6
4 ADMINISTRATOR ROLE CAPABILITES.....	8
4.1 View List of Users	8
4.2 How to Add a New User	9
4.3 How to Export the User List	10
4.4 How to Edit User Account Information.....	11
4.5 How to Lock or Unlock User Accounts.....	12
4.6 How to Reset User Passwords	13
4.7 How to Manage Two-factor Authentication (2FA)	14
4.7.1 View Status of 2FA Configuration	14
4.7.2 Resetting Two-Factor Device Pairing	15
4.8 Enabling API Access.....	16

1 ABOUT SARA ALERT™

Sara Alert™ serves as a force multiplier that supports governmental public health response to emerging disease threats, including active monitoring of home quarantine and isolation for disease containment or mitigation. This open source tool allows public health resources to be directed where they are most needed.

Sara Alert™ enables public health officials to enroll individuals at risk of developing a disease of interest (“monitorees”), for example COVID-19. Once enrolled, individuals can report their (and their household members’, if applicable) symptoms daily through multiple platforms (e.g., mobile, desktop, text-based, voice), providing public health departments improved situational awareness. If a monitoree reports any symptoms or does not submit a daily report, the record is flagged by the system so that public health can quickly and efficiently identify monitorees requiring follow-up for care coordination or non-response follow-up.

Sara Alert™ also enables public health officials to enroll cases who require monitoring to determine when it is safe to discontinue home isolation. Once enrolled, individuals can report their symptoms daily through multiple platforms (e.g., mobile, desktop, text-based, voice), providing public health departments improved situational awareness. If a monitoree reports meets a recovery definition or does not submit a daily report, the record is flagged by the system so that public health can quickly and efficiently identify monitorees requiring follow-up to verify that it is safe to discontinue home isolation or non-response follow-up. The concept of operations and high-level workflow are shown below in **Figure 1**.

1.1 Concept of Operations

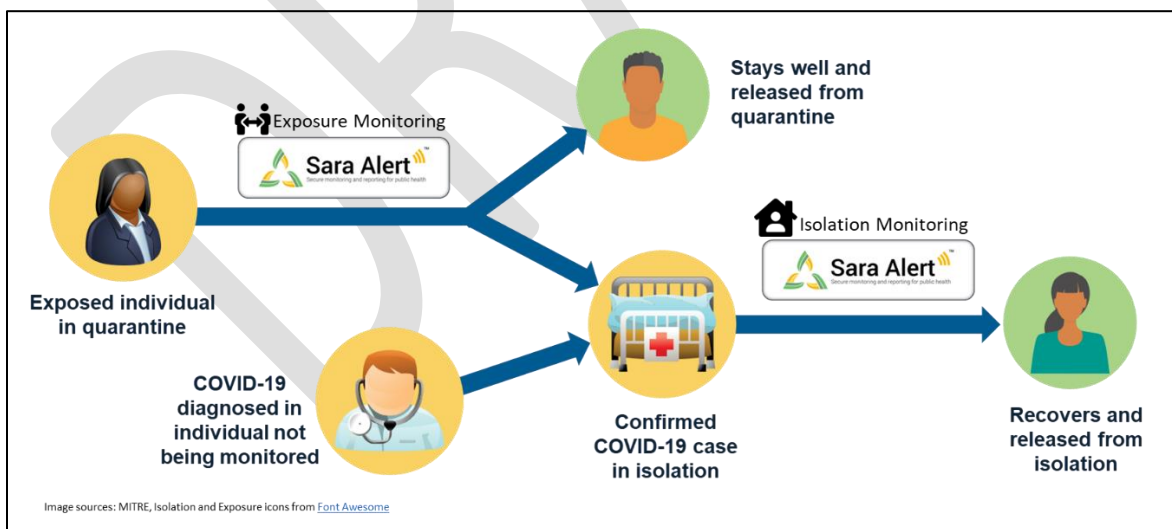


Figure 1: Sara Alert™ Concept of Operations

Visit saraalert.org for more information about Sara Alert, including FAQs, tutorial videos, and fact sheets. To send questions, comments, or other feedback related to Sara Alert, email sarasupport@aimsplatform.com.

1.2 SMART on FHIR API

The Sara Alert™ system has an Application Programming Interface (API) written to SMART on HL7 Fast Healthcare Interoperability Resources (FHIR) standards to support the exchange of information with state systems.

Recommended resources to support use of the API are listed below:

- [FHIR](#), its components, and specifications
- [SMART docs](#)
- [SMART application launch framework](#)
- C# FHIR [library](#)

The Sara Alert™ API documentation is available to users on GitHub [here](#).

1.2.1 Get Started Using the API

No matter the workflow, in order to use the Sara Alert™ API and ensure security of application data, the client must go through a three-step process before reading or writing any data.

1. **Registration:** Register as a Client Application with Sara Alert™ (one-time step) by emailing sarasupport@aimsplatform.com to request access. The registration process allows Sara Alert™ to pre-authorize and curate the clients that will be using the Sara Alert™ API. Registration is a manual step, as is [traditional](#).
2. **Authorization:** Go through an authorization process to obtain access token for API requests.
3. **Authentication:** Use obtained access token to make API requests to Sara Alert API.

1.2.2 Supported Workflows

Sara Alert currently supports two different workflows for API use. Both of these workflows are [SMART-on-FHIR standards](#).

1. [SMART on FHIR App Launch Framework "standalone launch"](#). This expects and requires a user in the loop. For Sara Alert™, this means that a user must be logged in to the Sara Alert™ User Interface, which requires 2 factor-authentication to have been completed (See **page 11**). After an application is authorized, users must individually be given "API access" by their local jurisdiction administrators. Please contact your local administrator to be granted this access.
2. [SMART on FHIR Backend Services](#). This is complementary to the above flow, and does not require a user in the loop.

2 ADMINISTRATOR ROLE OVERVIEW

An administrator is a trusted user who can view and manage Sara Alert™ users within their jurisdiction. Administrators are the only user type with the ability to add, modify, and view system users.

TIP: See the [Quick Start Guide for Administrators](#)

Table 1. Functional Role Summary

Role	Enroll New Exposed Monitoree	Enroll New Case	View/Modify Enrollment Details	View Monitoring Line Lists	View/Modify Monitoring Actions	View/Add/Modify Symptom Reports	View/Add Lab Reports	Transfer Records	View History/Add Comments	Import records	Export Records	View and export analytics	Add/modify system users	View list of system users	Record Access
Administrator													✓	✓	None

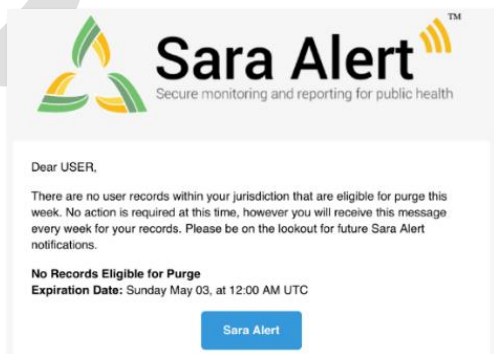
2.1 Record Access

An administrator cannot see individual monitoree record details or the analytics summary. Administrators are only able to see and modify user accounts within their assigned jurisdiction.

2.2 Sara Alert™ Record Retention

To minimize the amount of identifiable information stored on the production servers, Sara Alert™ will **purge records of identifiers** if there have been no changes to a record for a defined time period, provided that a monitoree is no longer being actively monitored. For COVID-19, the time has been configured for 14 days after the last record update (e.g., an update includes any action on the record, including adding comments or updating any fields).

On **Thursdays at noon UTC**, the system will flag all records that are forecasted to be eligible to be purged of identifying information on Saturday at 11:59 pm UTC (i.e. records that at Saturday 11:59 UTC would have not been updated for 14 days). **An email notification will be sent to administrators indicating how many, if any, purge-eligible records are in the administrator's jurisdiction.** Local administrators will need to coordinate with a public health user to export records for retention before purge if necessary. If a jurisdiction would like to retain the records, public health users will need to select **“Export for Purge Eligible Monitorees”**.



TIP: Use an online converter to convert UTC to your local time zone.

Figure 2: Sample notification to administrators

The system will purge records flagged Thursday on **Saturday at 11:59 pm UTC**. If a record flagged for purge is updated before Saturday at 11:59 pm UTC, the record will not be purged.

3 GETTING STARTED

3.1 Logging In

1) Open Sara Alert™ in a web browser. Compatible web browsers include Chrome, Microsoft Edge, Microsoft Internet Explorer 11, Mozilla Firefox, and Safari. If using Microsoft Internet Explorer 11, you may need to turn off compatibility mode.

2) Log in using your credentials.

If this is your *first login attempt*, use the temporary password you were issued; you will be prompted to change it. Temporary passwords **expire after 72 hours**. If your temporary password has expired, contact your jurisdiction administrator for a password reset.

TIP: If you are having difficulty logging in with the temporary password, manually type it in instead of using cut and paste



Figure 3: Log in screen

3) Register for two-factor authentication (2FA) by providing a phone number. (**NOTE:** this is only required the first time you use Sara Alert™). This is how you will receive your 7-digit 2FA token number. Once you have entered your phone number and country (for the country code), click “**Register**”. See **page 14** for more information about 2FA.

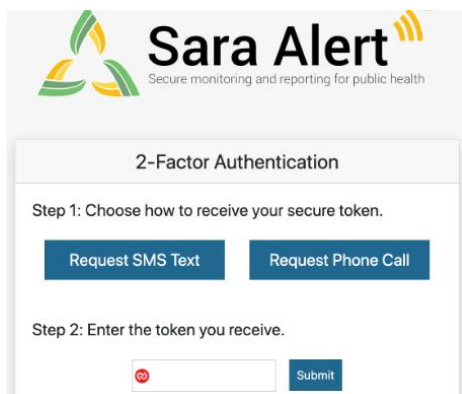


Figure 4: Enter your phone number

GETTING STARTED

4) For all login attempts after initial registration, you will be prompted to choose how to receive the 7-digit 2FA token (i.e., SMS/Text or through a phone call).

- Select your preferred method to receive the 2FA token
- Enter the 7-digit token when you receive it and click “Submit”

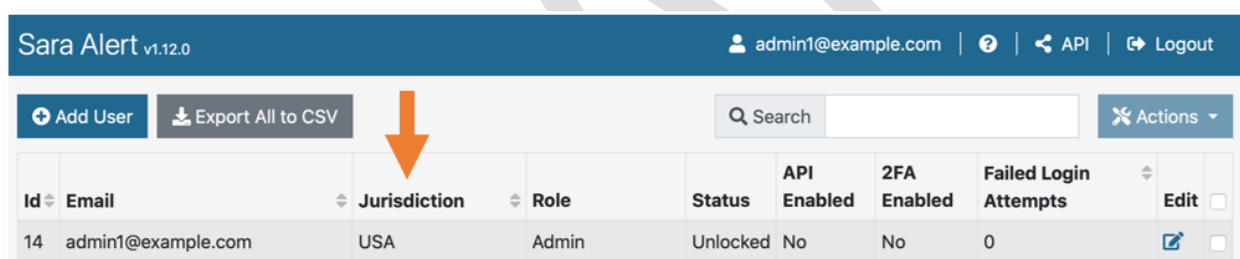


The image shows the Sara Alert 2-Factor Authentication interface. At the top is the Sara Alert logo with the tagline 'Secure monitoring and reporting for public health'. Below the logo is a box titled '2-Factor Authentication'. Inside this box, 'Step 1: Choose how to receive your secure token.' is followed by two buttons: 'Request SMS Text' and 'Request Phone Call'. 'Step 2: Enter the token you receive.' is followed by a text input field with a red circular icon on the left and a 'Submit' button on the right.

Figure 5: Choose your 2FA method

5) You will be taken to the Admin Panel.

6) Your assigned jurisdiction is listed next to your email, under the Jurisdiction column in the admin panel. You are only allowed to see users within your own jurisdiction.

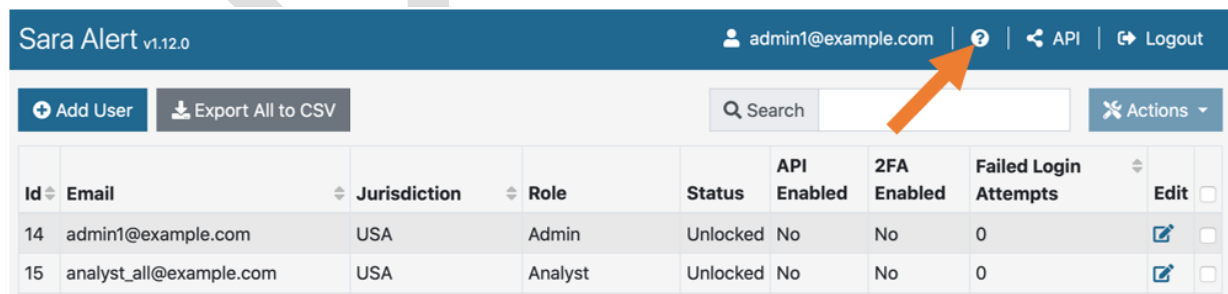


The image shows the Sara Alert v1.12.0 Admin Panel. The top header bar is blue and contains the text 'Sara Alert v1.12.0', the user 'admin1@example.com', a help icon, an 'API' link, and a 'Logout' button. Below the header is a toolbar with 'Add User' and 'Export All to CSV' buttons, a search bar, and an 'Actions' dropdown. The main content is a table with columns: Id, Email, Jurisdiction, Role, Status, API Enabled, 2FA Enabled, Failed Login Attempts, and Edit. An orange arrow points to the 'Jurisdiction' column header. The table contains one row for the user 'admin1@example.com' with jurisdiction 'USA'.

Id	Email	Jurisdiction	Role	Status	API Enabled	2FA Enabled	Failed Login Attempts	Edit
14	admin1@example.com	USA	Admin	Unlocked	No	No	0	

Figure 6: Your Sara Alert™ jurisdiction

7) The “**Help**” button provides links to the User Guide, User Forum and other helpful resources, including how to contact the Sara Alert™ team for help.



The image shows the Sara Alert v1.12.0 Admin Panel, similar to Figure 6, but with an additional row for user 'analyst_all@example.com'. An orange arrow points to the help icon in the top header bar.

Id	Email	Jurisdiction	Role	Status	API Enabled	2FA Enabled	Failed Login Attempts	Edit
14	admin1@example.com	USA	Admin	Unlocked	No	No	0	
15	analyst_all@example.com	USA	Analyst	Unlocked	No	No	0	

Figure 7: Access to Sara Alert™ resources

8) To end the session, click “**Logout**”. Users should log out of the system when they are not using it.

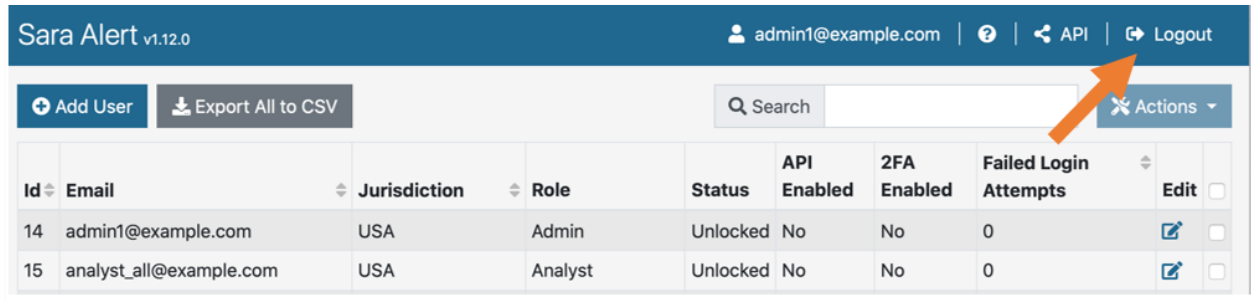


Figure 8: The logout button

4 ADMINISTRATOR ROLE CAPABILITIES

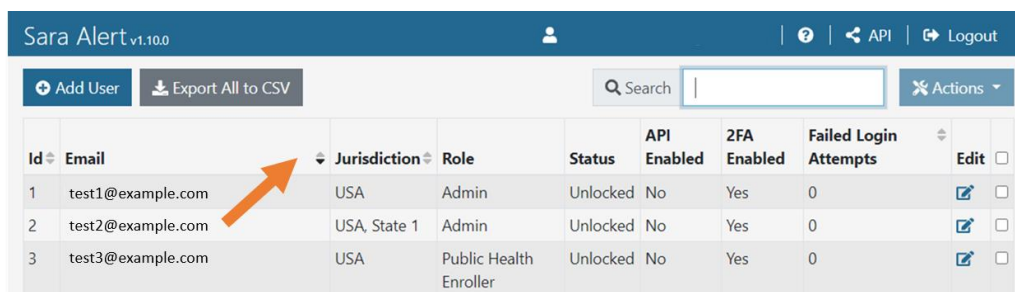
Administrators are responsible for managing Sara Alert™ Users. Local administrators can only manage users within their assigned jurisdiction. If a local administrator needs assistance with managing their users, please contact the Sara Alert™ Help Desk.

4.1 View List of Users

The Administrator role shows the list of current users in their assigned jurisdiction with the following associated information:

- **ID:** Shows the unique system ID associated with the user. Jurisdictions may use this number for the assigned user field, but there is no automatic linkage between this ID and the “Assigned User” field in a monitoree’s record.
- **Email:** User’s email address.
- **Jurisdiction:** Shows the complete access hierarchy for the user. Users (including Administrators) have access to all data (specific to their role) for their jurisdiction and all sub-jurisdictions. Administrators can only assign users to jurisdictions and sub-jurisdictions within their assigned jurisdiction.
- **Role:** User’s role in the system (enroller, public health, public health enroller, analyst, or admin). User roles are linked to a unique email address, so a user may only be assigned one role, unless a user has more than one unique email address.
- **Status:** Whether the user’s account is locked or unlocked (see **page 12**).
- **API Enabled:** Whether the user has access to the API. A local administrator must have approval to access the API from the system administrator before they can enable it for users. For more information on the API, see **SMART on FHIR API** on **page 4**.
- **2FA Enabled:** Whether the user has configured their accounts required 2-factor authentication. Two-factor authentication provides a second layer of security to protect a user account by sending a token for login to their phone through call or text. If a user has not yet configured their 2FA, they will be prompted to do so the first time you log into the system.
- **Failed Login Attempts:** The number of consecutive failed login attempts since the last successful login. The system will automatically lock a user’s account after 5 failed login attempts. Unlocking an account will clear this number.

Click on headers to sort based on that column.

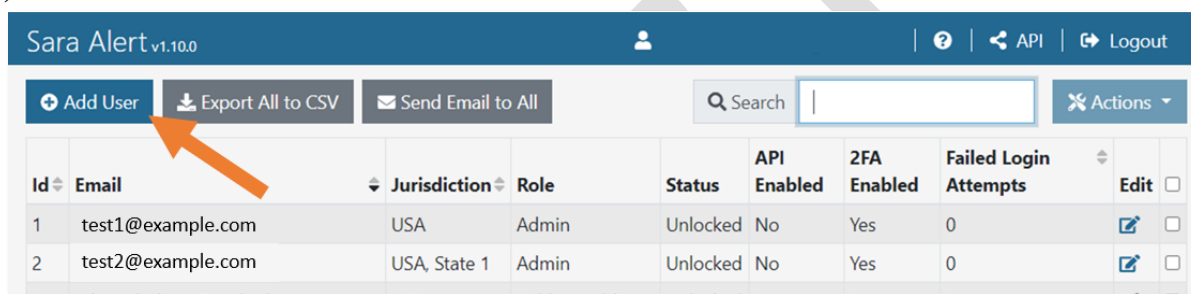


Id	Email	Jurisdiction	Role	Status	API Enabled	2FA Enabled	Failed Login Attempts	Edit
1	test1@example.com	USA	Admin	Unlocked	No	Yes	0	
2	test2@example.com	USA, State 1	Admin	Unlocked	No	Yes	0	
3	test3@example.com	USA	Public Health Enroller	Unlocked	No	Yes	0	

Figure 9: Click the column header to sort that column

4.2 How to Add a New User

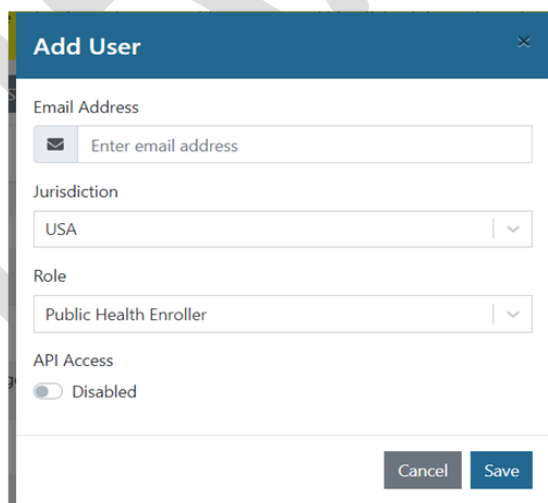
1) Click the “Add User” button.



Id	Email	Jurisdiction	Role	Status	API Enabled	2FA Enabled	Failed Login Attempts	Edit
1	test1@example.com	USA	Admin	Unlocked	No	Yes	0	
2	test2@example.com	USA, State 1	Admin	Unlocked	No	Yes	0	

Figure 10: Add a new user

2) Enter the new user’s email address, select their jurisdiction and role from the drop-down lists, and toggle their API access. Click “Add Save” to complete the process. The user will receive a welcome email with a temporary password they can use to log into the system, change their password, and register for two-factor authentication.



Add User

Email Address

Jurisdiction

Role

API Access
☐ Disabled

Cancel Save

Figure 11: Complete new user entry

4.3 How to Export the User List

To export a list of users for your jurisdiction, click the “**Export to CSV**” button.

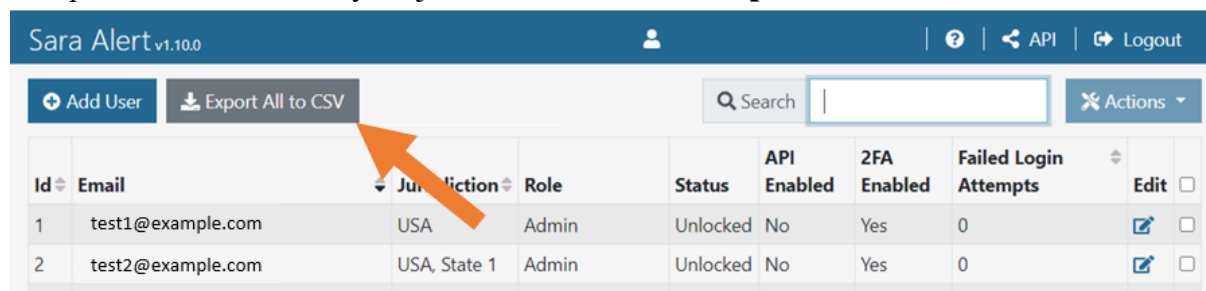


Figure 12: Export a list of users

The CSV file will appear in your browser window. Click the notification to view the export, including all line list information.

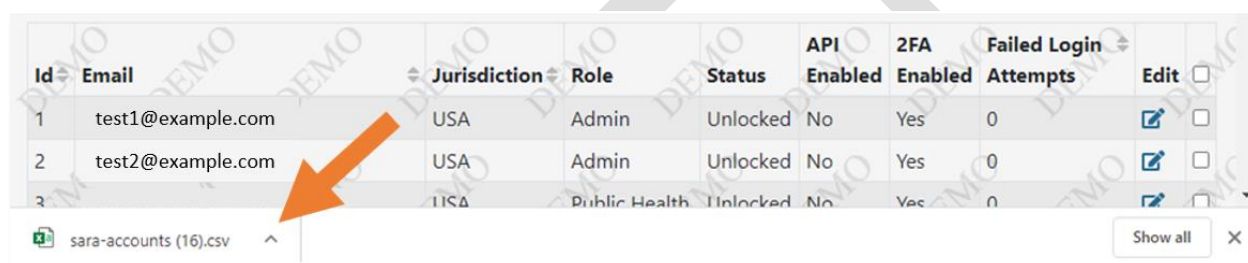


Figure 13: Click the notification in your browser to open the file

	A	B	C	D	E	F	G	H
1	id	email	jurisdiction_path	role_title	is_locked	is_api_enabled	is_2fa_enabled	num_failed_logins
2	1	test1@example.com	USA	Admin	FALSE	FALSE	TRUE	0
3	2	test2@example.com	USA	Admin	FALSE	FALSE	TRUE	0
4	3	test3@example.com	USA	Public Health Enroller	FALSE	FALSE	TRUE	0
5	4	test4@example.com	USA	Public Health Enroller	FALSE	FALSE	FALSE	0
6	5	test5@example.com	USA, State 3	Public Health Enroller	FALSE	FALSE	FALSE	0
7	6	test6@example.com	USA, State 50	Public Health Enroller	FALSE	TRUE	TRUE	0
8	7	test7@example.com	USA	Admin	TRUE	FALSE	FALSE	0
9	8	test8@example.com	USA	Admin	FALSE	FALSE	TRUE	0
10	9	test9@example.com	USA	Admin	FALSE	FALSE	TRUE	0
11								

Figure 14: CSV line list export

4.4 How to Edit User Account Information

User information can be edited one record at a time on the admin panel. As an administrator, you can edit each user's email address, Jurisdiction, role, access status, and API access.

1) To edit a user's information, first click the **"Edit"** icon for that user.

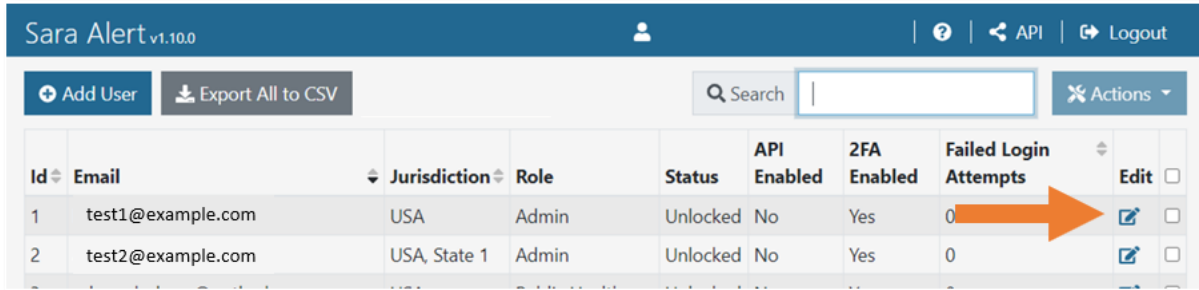


Figure 15: Click the "Edit" icon

2) This will open the "Edit User" window. You can edit the user's Email Address, Jurisdiction, Role, Locked Status, and API access. Click **"Save"** to confirm your changes.

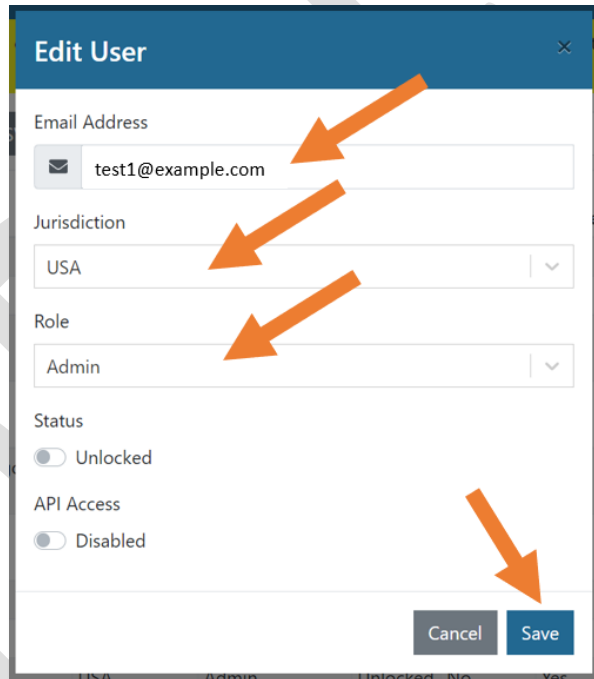


Figure 16: Edit the appropriate fields and click "Save"

4.5 How to Lock or Unlock User Accounts

Sara Alert™ will automatically lock a user’s account after 5 unsuccessful login attempts. This is done as a security measure, but administrators have the ability to unlock an account. You may also lock accounts to prevent a user from accessing the system (ex: if a user is no longer working for your organization).

- 1) To manually lock or unlock a user’s account, first click the “**Edit**” icon for that user

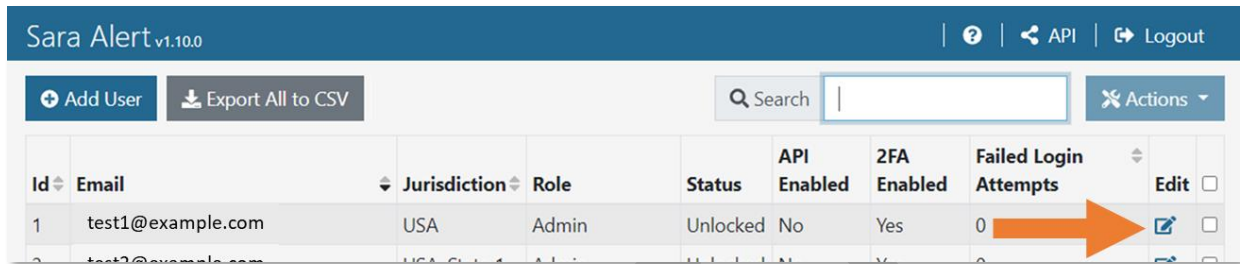


Figure 17: Click the “Edit” icon

- 2) Toggle the “**Status**” switch to lock or unlock the user’s account. Click “**Save**” to confirm.

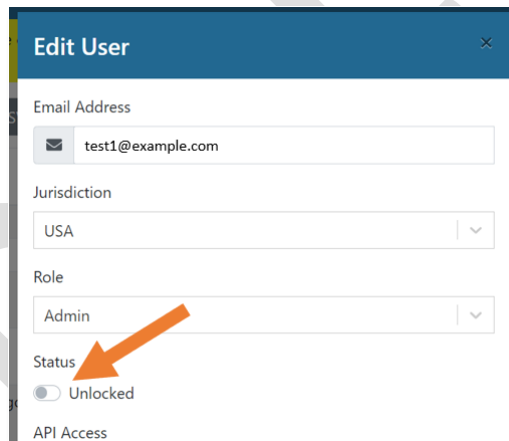


Figure 18: Toggle the “Status” switch to lock or unlock the account

- 3) You can see an account’s status on the user dashboard in the “**Status**” column.

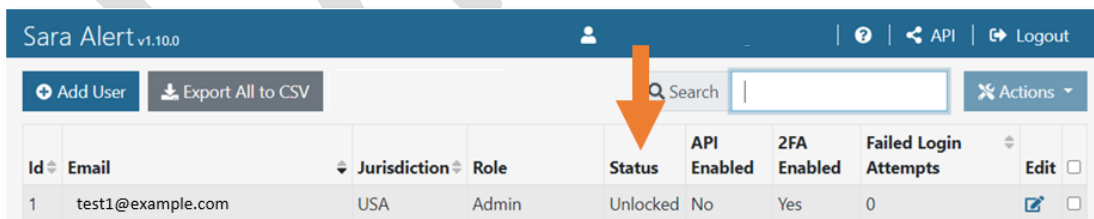


Figure 19: The “Status” column shows if a user’s account is locked or unlocked

4) Users will be unable to log in to a locked account. This error message will appear for users logging in with invalid credentials or attempting to log in to a locked account.

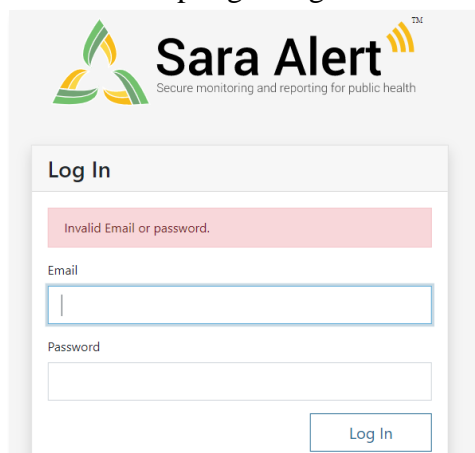


Figure 20: Users cannot log in to a locked account

4.6 How to Reset User Passwords

User passwords can be reset multiple accounts at a time. If you click the select box in the menu header, you can reset passwords for all accounts visible on that page (not all accounts in the system). This feature can be used to reset any forgotten passwords or periodically based on your jurisdiction's security requirements.

1) Sara Alert™ handles password reset requests via email. If one or more of your users requests a password reset, first select the user(s) by clicking the box in the far-right column.

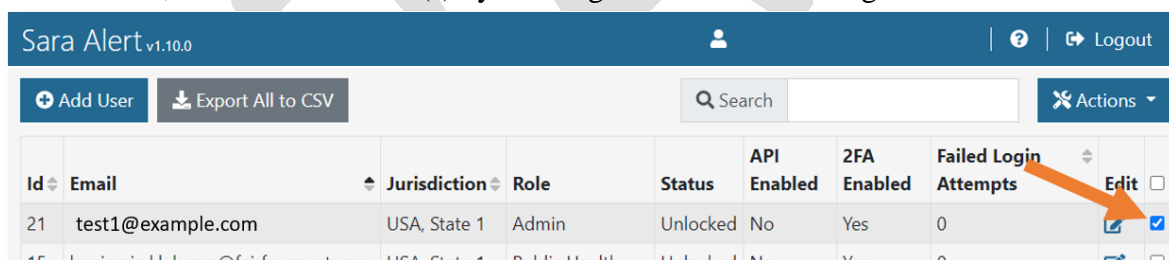


Figure 21: Select the user by clicking the box in the far-right column

2) Clicking the checkbox at the top in the column header will select all users in the current view on the page (not all users in the jurisdiction).

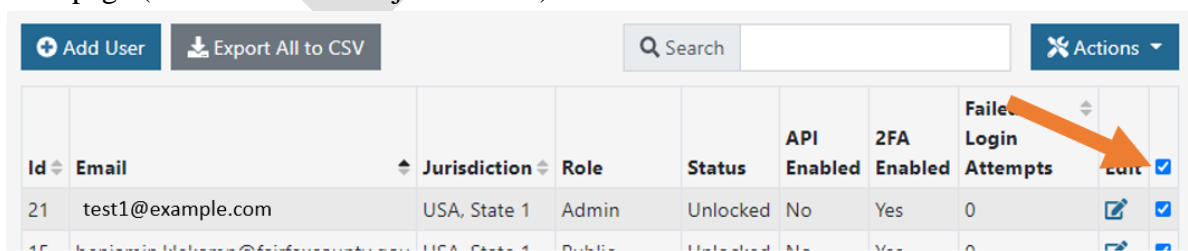


Figure 22: Select all users in the view by clicking the checkbox in the column header

3) Click the “Actions” button and from the drop-down menu, click “Reset Password.”

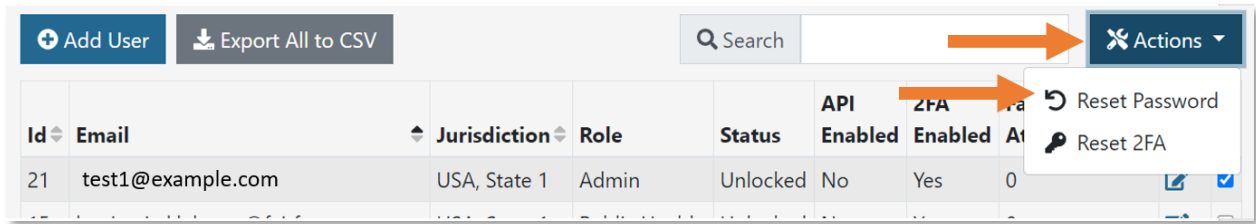


Figure 23: Select “Reset Password” from the “Actions” drop-down menu

4) The user will receive an email with a temporary password. On their next login, they will be prompted to change their password.

NOTE: Temporary passwords expire after 72 hours (and will need to be reissued via another password reset). Temporary passwords should be inputted manually; not through copy and paste.

4.7 How to Manage Two-factor Authentication (2FA)

Two-factor Authentication (2FA) is a security feature that requires two verification methods to confirm a user’s identity. Typically, these methods include a standard password and a second verifier that only the user would have access to (i.e., a message sent to a phone or email address linked to the user’s account). Sara Alert™ uses a 2FA system that requires a user to submit the following on login:

- The user’s password associated with their Sara Alert™ account
- A 7-digit code sent to the user’s phone number associated with their Sara Alert™ account

2FA is a requirement for all Sara Alert™ users (not including monitorees) to help maintain the tool’s security.

4.7.1 View Status of 2FA Configuration

The “2FA Enabled” column shows whether a user has configured their required 2FA. If a user has not configured 2FA, they will be prompted to do so on their next login.

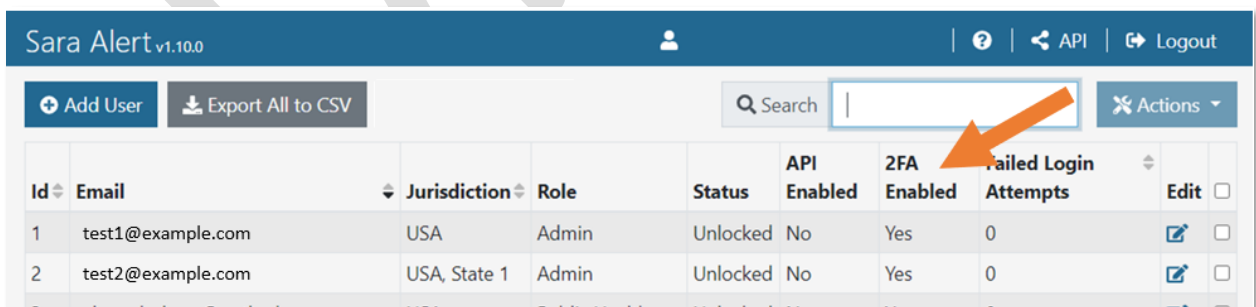


Figure 24: The Administrator Dashboard shows a user’s 2FA configuration status

4.7.2 Resetting Two-Factor Device Pairing

If a user wishes to reset the phone number associated with their Sara Alert™ account (i.e., to change the phone number that will receive the 7-digit 2FA token), they should notify their jurisdiction's Local Administrator.

1) Select one or more user accounts individually by clicking the checkbox in the rightmost column.

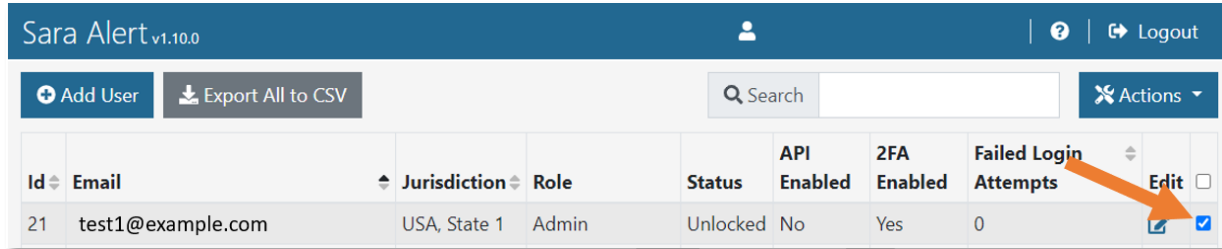


Figure 25: Select an account by clicking the checkbox

2) Clicking the checkbox at the top in the column header will select all users in the current view on the page (not all users in the jurisdiction).

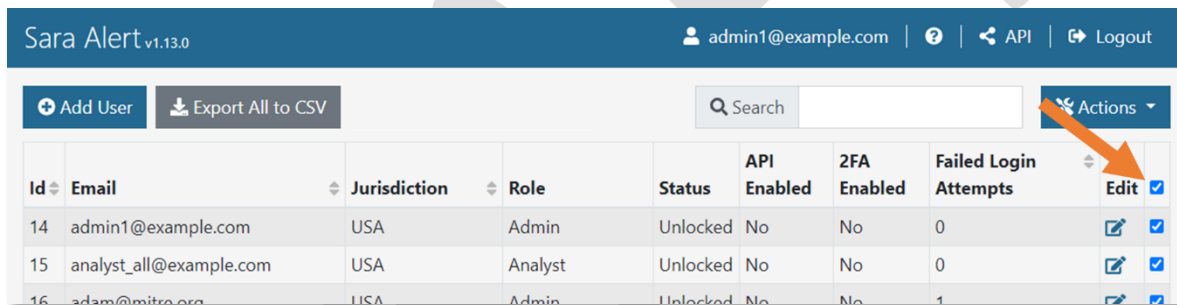


Figure 26: Select all accounts in the current view by clicking the checkbox in the menu header

3) Click “Actions” and select “Reset 2FA” from the drop-down menu

- Once reset, the user's “Configured 2-Factor Auth” status will change to “No” and the selected user(s) will be prompted to register for 2FA on their next login attempt

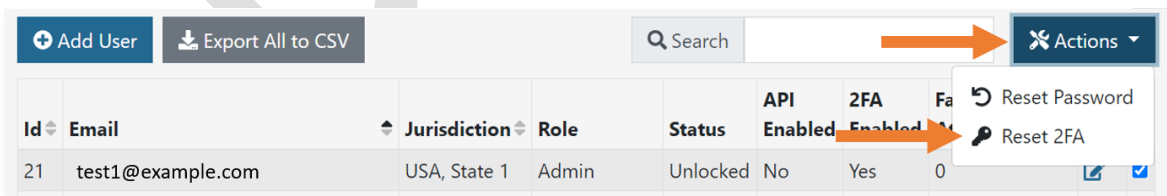


Figure 27: Reset a user's 2FA pairing

4.8 Enabling API Access

Administrator users can provide API access to specific users in their jurisdiction if they have been approved to do so by the system administrators. For more information on how to gain access to the API, see **page 4**.

- 1) To enable API access, first click the “**Edit**” icon for that user

Sara Alert v1.10.0

?

API

Logout

Add User

Export All to CSV

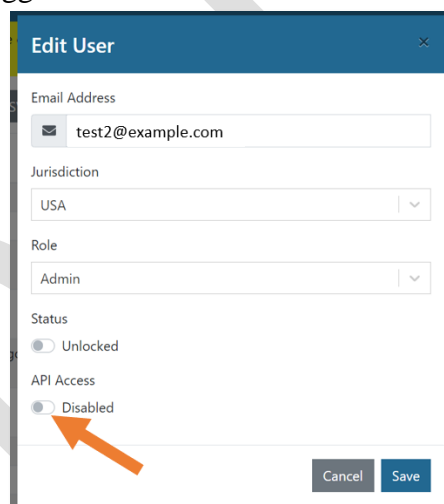
Search

Actions

Id	Email	Jurisdiction	Role	Status	API Enabled	2FA Enabled	Failed Login Attempts	Edit
1	test1@example.com	USA	Admin	Unlocked	No	Yes	0	<div></div>
2	test2@example.com	USA, State 1	Admin	Unlocked	No	Yes	0	<div></div>

Figure 28: Click the “Edit” icon

- 2) In the Edit User window, toggle the **API Access** switch to enable or disable access.



Edit User

Email Address: test2@example.com

Jurisdiction: USA

Role: Admin

Status: ☐ Unlocked

API Access: ☐ Disabled

Cancel Save

Figure 29: Toggle “API Access” to enable or disable access