Sara Alert™

Secure monitoring and reporting for public health

User Guide for Administrators

Software Version 1.38

November 2, 2021

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

Table of Contents

1 ABOUT SARA ALERT™ 1

2 ADMINISTRATOR ROLE OVERVIEW 2

2.1 Record Access 3

2.2 Saving Records Before a System Purge 3

3 GETTING STARTED 4

3.1 Logging In 4

4 ADMINISTRATOR ROLE CAPABILITES 7

4.1 View List of Users 7

4.2 How to Add a New User 8

4.3 How to Export the User List 9

4.4 How to Edit User Information 10

4.5 How to View and Audit User Account Events 11

4.6 How to Lock and Unlock User Accounts 12

4.7 How to Reset User Passwords 14

4.8 How to Manage 2-Factor Authentication 15

4.9 How to Use the Sara Alert™ API 17

4.10 How to Enable API Access 18

Appendix A Assigning User Roles A-1

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

1 ABOUT SARA ALERT™

Sara Alert™ is a standards-based, open-source tool that automates the process of public health monitoring and reporting of individuals exposed to or infected with COVID-19 or any infectious disease. The tool was developed by public health experts for public health. Sara Alert is available in the public domain, free of charge to public health agencies. As an open-source tool, Sara Alert is available for public and private use and is easily integrated into other tools.

Sara Alert enables public health officials to enroll individuals ("monitorees") at risk of developing a disease of interest, for example COVID-19. Once enrolled, monitorees 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. If a monitoree 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 follow-up to verify that it is safe to discontinue home isolation or perform non-response follow-up. The concept of operations is shown below in **Figure 1**.

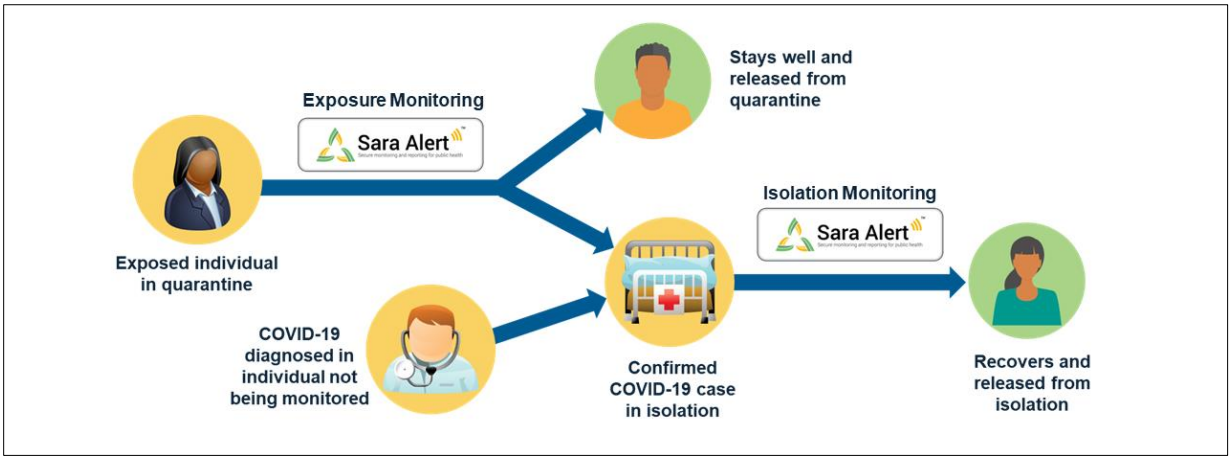


Figure 1: Sara Alert™ concept of operations

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

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

2 ADMINISTRATOR ROLE OVERVIEW

As an Administrator, you manage users' (those assisting public health monitoring) access to Sara Alert™. You are responsible for managing users in your jurisdiction (the area that your public health organization serves). Those with Administrator access can:

TIP: See the **Quick Start Guide for Administrators**

- Add new users to Sara Alert
- Change a user's information, including resetting their password, changing their role, and giving them access to certain tools and features in Sara Alert
- See your users' work history, including days, times, and actions in the system
- See a list of users

Administrators manage these kinds of Sara Alert users:

- **Enrollers.** These users enroll monitorees in Sara Alert. A monitoree is someone who has or may have been exposed to or has a case of the disease of interest. Enrollers can:
  - Enroll new monitorees
  - View and change details they enter for the monitorees
  - View summary information about the monitorees they enter
  - In some cases, assign monitorees to another jurisdiction
- **Public Health Enrollers.** These users have full access to monitoree records. They can:
  - Enroll new monitorees
  - View and manage workflows and line lists. Workflows in Sara Alert are the Exposure Workflow for monitorees who have been exposed to the disease of interest and the Isolation Workflow for monitorees who have symptoms of the disease of interests. Line lists are monitorees grouped by certain descriptors, like symptom status or reporting status.
  - Import, export, and transfer monitoree records
  - View analytics (data reports)
- **Public Health Users.** These users have full access to Sara Alert monitoree records. They cannot enroll new monitorees, but they can:
  - View and manage line lists and workflows
  - Import, export, and transfer monitoree records
  - View analytics (data reports)
- **Contact Tracers.** These workers find and contact people who have been exposed to or have symptoms of the disease of interest. They can:
  - Enroll new monitorees
  - View and manage line lists and workflows
- **Super Users.** These users can do the same things in Sara Alert as Public Health Enrollers and Administrators. They can:
  - Enroll new monitorees
  - View and manage line lists and workflows
  - Import, export, and transfer monitoree records

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

  - View Analytics (data reports)
  - View and manage all Sara Alert users

- **Analysts.** These users are only able to view high-level analytics (data reports) for their jurisdiction. They cannot view individual monitoree data or see user information.
- Administrator users can also manage other **Administrators.**

2.1 Record Access

Information about a monitoree in Sara Alert™ is called a record. As an Administrator, you cannot see individual monitoree records or analytics reports for your jurisdiction. You can only see and change **user** accounts in your jurisdiction.

2.2 Saving Records Before a System Purge

The Sara Alert™ system stores (keeps) information about thousands of monitorees. To reduce the amount of stored information, Sara Alert purges (deletes or gets rid of) information for monitorees who have not been monitored by Sara Alert for a while. These monitorees are called "purge-eligible." The system deletes these records if **both** of the following are true:

- The monitoree is no longer being actively monitored.
- The information in a record has not been edited or updated for a specific period (for COVID-19, this period is 14 days). An update is any action or change in the record, including adding comments.

Sara Alert uses UTC to schedule purges. UTC stands for Coordinated Universal Time. It is what countries around the world use to set time.

The following days and times are important to know for the weekly Sara Alert purge:

- **Each Thursday at 12:00 noon UTC:**
  - At this time, Sara Alert flags all records likely to be purged that week. These are records of monitorees that, by Saturday at 11:59 p.m. UTC, will meet both deletion requirements listed above unless they are edited.
  - Sara Alert also sends you an email telling you the number of records from your jurisdiction that are scheduled to be deleted on Saturday. If there are no records that are scheduled to be purged, the email will look like the example below:

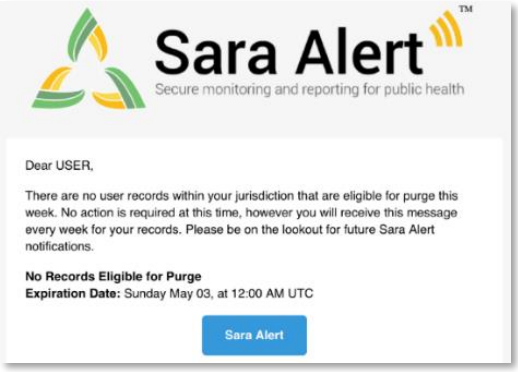


Figure 2: Sample email to administrators

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

- If you need to keep any of the records that have been flagged for deletion, ask a Public Health, Public Health Enroller, or Super User to export and save the records by exporting the **"Excel Export for Purge-Eligible Monitorees"** export format. To save the records, the export must happen **before 11:59 p.m. UTC on Saturday**. If your jurisdiction would like to retain all records that are scheduled for purge, you should coordinate with a Public Health, Public Health Enroller, or Super User to perform this export regularly.

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

- **Each Saturday at 11:59 p.m. UTC (just before midnight):** Sara Alert deletes purge-eligible records. If a user updates a record **before Saturday at 11:59 p.m. UTC**, the system does not delete the record.

Use the table below to find out when **Saturday at 11:59 p.m. UTC** is in your time zone. To prevent records from being deleted, a Public Health, Public Enroller, or Super User must export and save the records before this time. If you are on Daylight Saving Time where you work, be sure to see that time in the chart. Time zones that do not use Daylight Saving Time have "none" in the chart. Many places use Daylight Saving Time during the summer.

Table 1: Saturday, 11:59 p.m. UTC in U.S. and Freely Associated State Time Zones

Time Zone	Standard Time	Daylight Time
Alaska Time	Saturday, 2:59 p.m. AKST	Saturday, 3:59 p.m. AKDT
Arizona Mountain Time	Saturday, 4:59 p.m. MST	None
Atlantic Time	Saturday, 7:59 p.m. AST	Saturday, 8:59 p.m. ADT
Central Time	Saturday, 5:59 p.m. CST	Saturday, 6:59 p.m. CDT
Chamorro Time	Sunday, 9:59 a.m. ChST	None
Eastern Time	Saturday, 6:59 p.m. EST	Saturday, 7:59 p.m. EDT
Hawaiian-Aleutian Time	Saturday, 1:59 p.m. HAST	Saturday, 2:59 p.m. HADT
Mountain Time	Saturday, 4:59 p.m. MST	Saturday, 5:59 p.m. MDT
Pacific Time	Saturday, 3:59 p.m. PST	Saturday, 4:59 p.m. PDT
Palau Time	Sunday, 8:59 a.m. PWT	None
Samoa Time	Saturday, 12:59 p.m. SST	None

3 GETTING STARTED

3.1 Logging In

1) Open Sara Alert™ in a web browser. Browsers that work with Sara Alert™ are Chrome, Microsoft Edge, Microsoft Internet Explorer 11, Mozilla Firefox, and Safari. If you are using Microsoft Internet Explorer 11, you should turn off compatibility mode.

2) Log in using your credentials.

If this is your *first time logging in*, use the temporary password you received in the email from Sara Alert. The system will ask you to change the password to something you can remember on

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

your own. Temporary passwords **expire after 72 hours**. If your temporary password has expired, contact your jurisdiction Administrator to reset it.

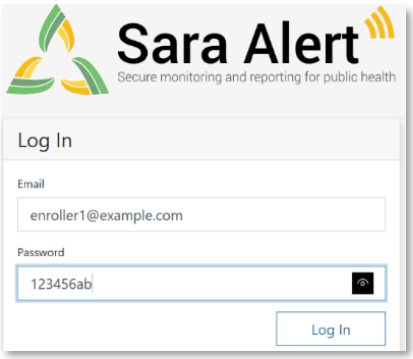


Figure 3: Log In screen

1) Register for 2-factor authentication (2FA) by entering your cell or landline phone number.

This registration is only required the first time you use Sara Alert. This is how you register to receive your seven-digit 2FA token number for future logins. Enter your phone number and country and click "**Register.**" See **page 15** for more information about 2FA.

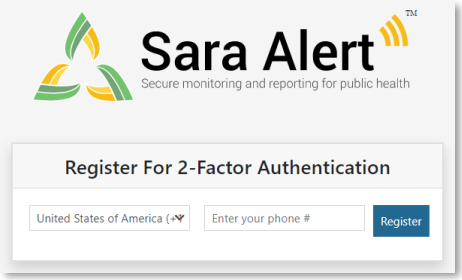


Figure 4: Register for 2-factor authentication

2) After your first log-in, the system asks you how you want to receive the 2FA token number. You can receive it by SMS text or by an automated phone call. Do not select the SMS text option if your 2FA phone number is a landline.

- Choose how you want to receive the 2FA token number.
- Enter the token number you receive and click **"Submit."**

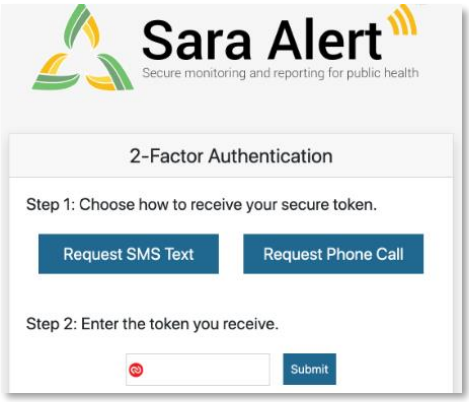


Figure 5: Choose your 2FA method.

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

3) After you enter your 2FA token, you will go to the Admin Panel. This is the main screen for Administrators where you can manage your users.

4) Your username and user role are listed in the upper right corner of the screen.

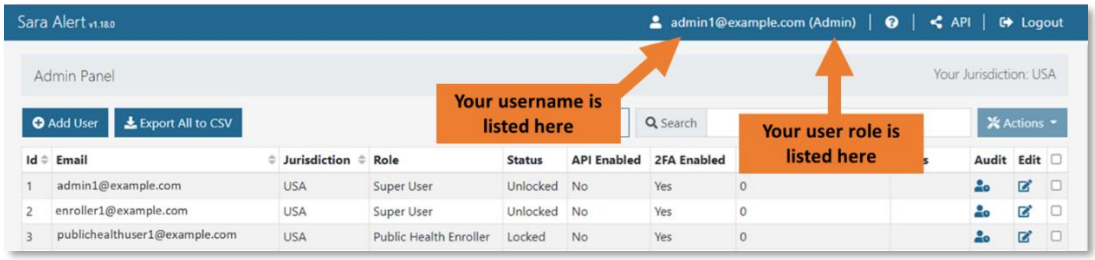


Figure 6: Your Sara Alert™ username and user role

5) You can also see your assigned jurisdiction listed in upper right corner of the screen. You can only see users within your own jurisdiction.

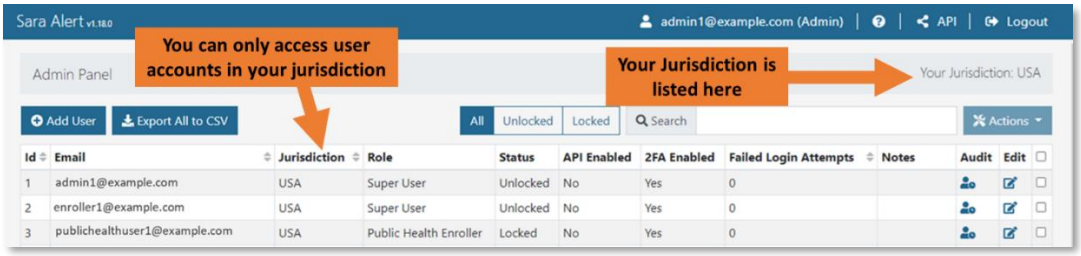


Figure 7: Your Sara Alert™ jurisdiction

6) Click the "**?**" (Help) button for links to the User Guide, User Forum, and other helpful resources, including how to contact the Sara Alert team for help.

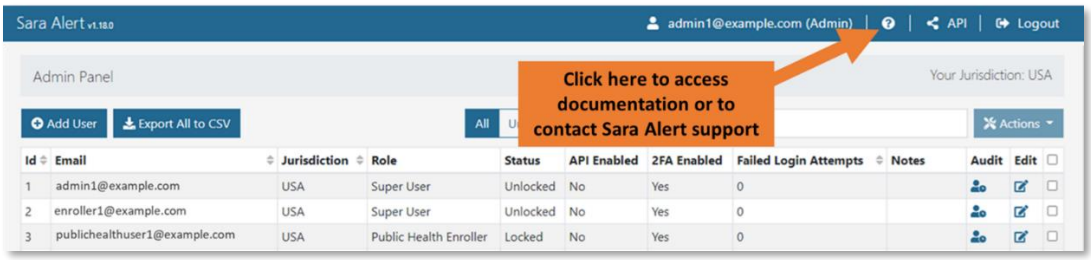


Figure 8: Access to Sara Alert™ resources

7) To end the session, click "**Logout.**" Be sure to log out of the system when you are not using it.

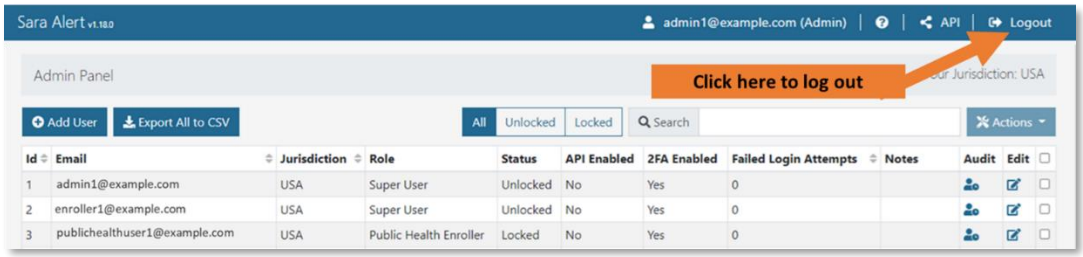


Figure 9: The logout button

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

4 ADMINISTRATOR ROLE CAPABILITES

As an Administrator, you manage Sara Alert™ users in your jurisdiction. If you need help using Sara Alert or managing users, contact the help desk at sarasupport@aimsplatform.com.

4.1 View List of Users

The **Admin Panel** shows a list of all users in your jurisdiction. These are the users you manage. You can see the following information about each one:

- **ID:** User identification (ID) number in your list of users. The ID is a unique number for each user, generated by Sara Alert, and is not linked to any other information in the system.
- **Email:** User's email address.
- **Jurisdiction:** Highest-level jurisdiction for a user. For example, the highest-level jurisdiction could be a state or county. Based on their role, a user has access to information for their jurisdiction and all sub-jurisdictions. For example, if a user's jurisdiction is "USA, State 1" they would have access to information for all counties and local jurisdictions within State 1. You can assign users to jurisdictions and sub-jurisdictions within your jurisdiction.
- **Role:** User's role in the system (Enroller, Public Health, Public Health Enroller, Contact Tracer, Analyst, Administrator, or Super User). The role is linked to a user's email address and the email address can link to only one role. If an individual needs to have multiple roles in Sara Alert, they will need two different Sara Alert accounts, each with its own email address. See **page A-1** for a list of user roles and their tasks in Sara Alert.
- **Status:** Whether the user's account is locked or unlocked (see **page 11**).
- **API Enabled:** Whether or not the user has access to the API (Application Programming Interface). If you are a local Administrator, you need approval from the system Administrator to access the API. With this approval, you can enable the API for a user. See **page 17** for more information about the API.
- **2FA Enabled:** Whether or not the user has configured their account for 2-factor authentication (2FA). 2FA is a security feature for Sara Alert™. It sends a 7-digit number (called a token) to a user's phone through call or text. The user enters the token to log in to Sara Alert. Users set up their 2FA the first time they log in. See **page 15** for more information.
- **Failed Login Attempts**: The number of consecutive (back-to-back) failed login tries since the last time a user logged in successfully. The system automatically locks a user's account after five failed login attempts. You can unlock an account to clear the number back to zero.
- **Notes**: Displays any notes that have been entered for a user. Any Administrator or Super User can see the notes for users in their jurisdiction.

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

You can sort the user list by the ID, Email, Jurisdiction, or Role columns. Click the arrow in the column header to sort that column.

Figure 10: Click the arrow in the column header to sort that column

4.2 How to Add a New User

1) On the **Admin Panel**, click the "**Add User**" button.

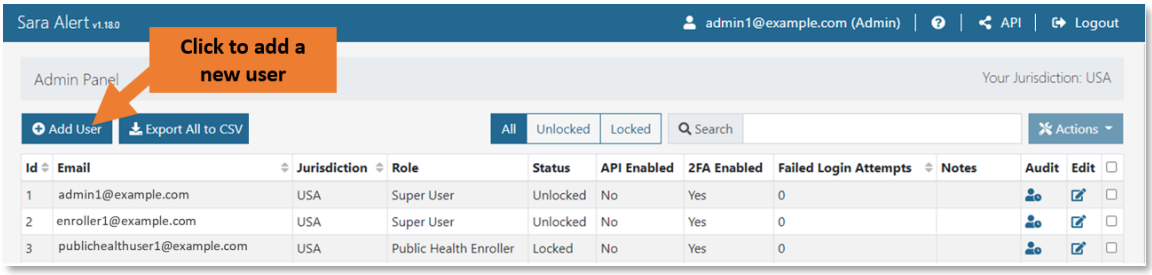


Figure 11: Add a new user

2) The "**Add User**" window opens. In this window:

a. Enter the new user's email address.
b. Select the jurisdiction and role from the drop-down lists.
c. For some users: set the API Access button to "Enabled" or "Disabled" (see **page 17** for more information about the API). This button will default to "Disabled."
d. Add comments in the Notes section, if needed.
e. Click **"Save."**

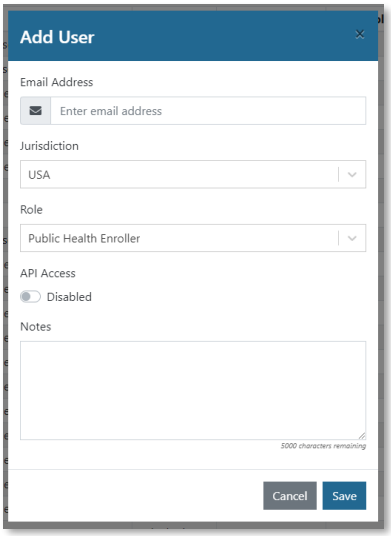


Figure 12: Add a new user

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

Once you click save, the user receives a welcome email with a temporary password that they can use to log into the system. When they log in, they can change their password and register for 2FA.

4.3 How to Export the User List

1) To export a list of users for your jurisdiction for reference or data retention, go to the **Admin Panel** and click the "**Export All to CSV**" button. This will export the information in a CSV format (a spreadsheet).

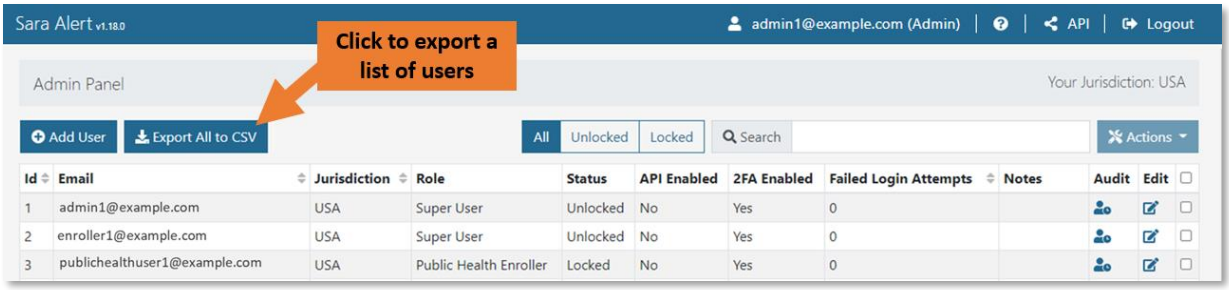


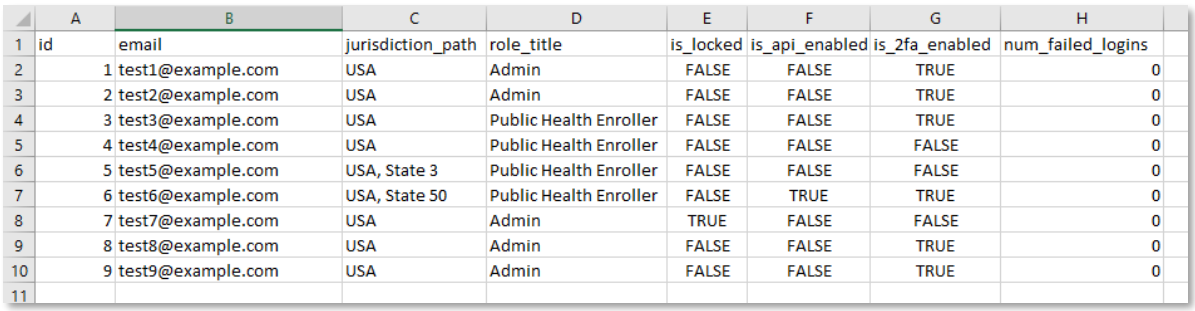
Figure 13: Export a list of users

2) The CSV file appears as a downloaded file in your browser. For example, the file may be in the lower-left corner or the upper-right corner of your browser window. Click the downloaded file name to see the export. This download includes all Admin Panel information.

NOTE: The exact style and location of the downloaded file depends on the browser you are using.

Figure 14: Click the downloaded file in your browser to open it

3) The exported Admin Panel opens in Excel or in the application you use to view CSV files. The exported file is a spreadsheet.



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

Figure 15: CSV Admin Panel export

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

4.4 How to Edit User Information

On the **Admin Panel**, you can edit (change) user information one user at a time. You can edit the following information about a user:

- Email address
- Jurisdiction
- Role
- Access status
- API access
- Notes

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

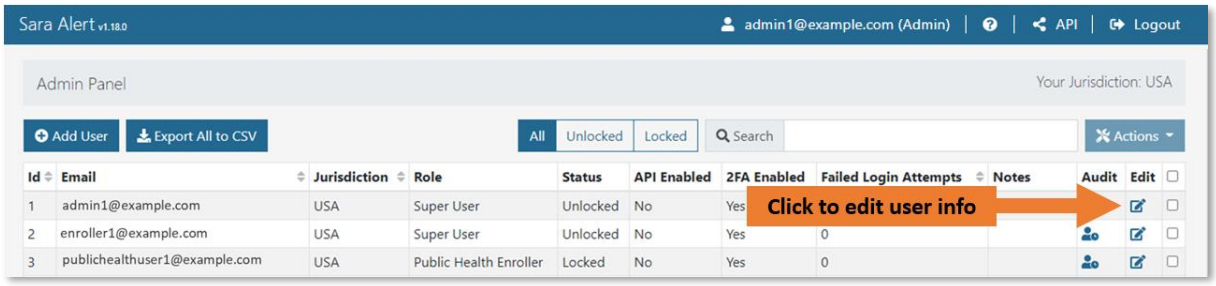


Figure 16: Click the "Edit" icon

4) The **"Edit User"** window opens. Edit the user information. When you are done, click **"Save."**

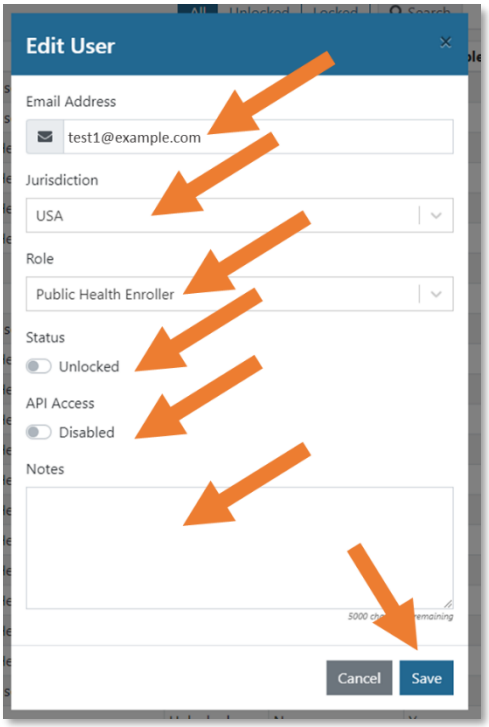


Figure 17: Edit user and click "Save."

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

4.5 How to View and Audit User Account Events

Administrators and Super Users can view user account events that happened after December 17, 2020 (which is when this feature was added to Sara Alert™). A user account event is an action that a user takes in Sara Alert. User account events include:

- When that user logs into Sara Alert
- If an Administrator or Super User makes changes to any field in the Admin Panel for that user
- If that user's password is changed
- If that user's 2FA is reset

1) To view a user's event history (list of events), click the "**Audit**" icon for the user.

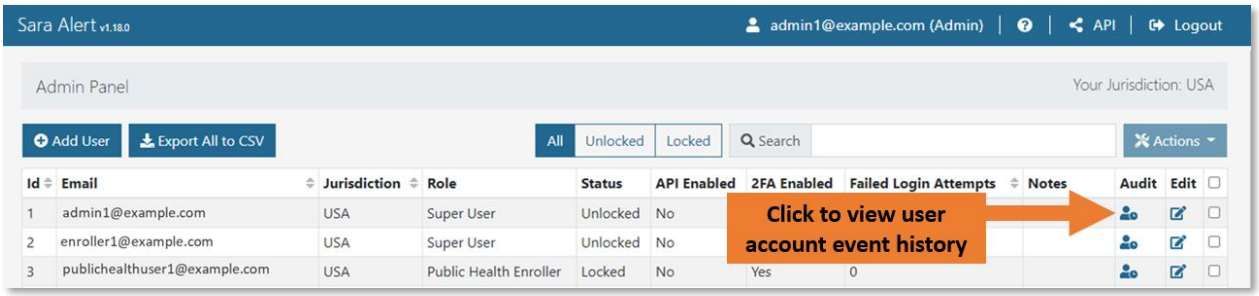


Figure 18: Click the "Audit" icon

2) The "**Audit Events**" window opens with the audited user's email address at the top. The window shows a table that gives you three kinds of information about each user event:

1. **Triggered by:** Shows the email address of the user who performed the action
2. **Action:** Describes the user's action (user account event)
3. **Timestamp:** Gives the day and time of the user's action

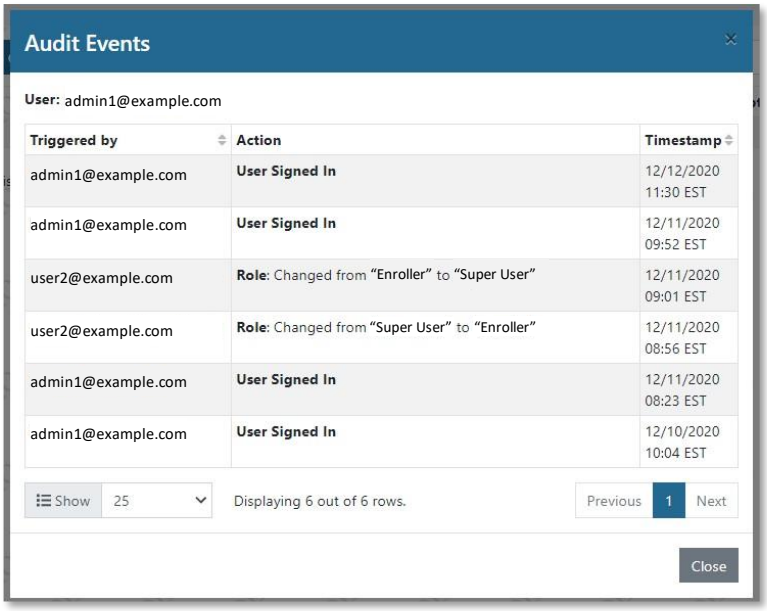


Figure 19: Audit results

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

In the **"Audit Events"** window, you can:

- Scroll through a user's actions so you can see what they have done in the system.
- Choose the number of rows of information you see on the screen.
- Use the "**Previous"** and "**Next"** buttons to move forward and backward in the list.
- Click **Close** when you are done.

4.6 How to Lock and Unlock User Accounts

Sara Alert™ automatically locks a user account after five failed login attempts to help keep the system secure. As an Administrator, you can:

- Unlock a user account that is locked
- Lock an account to keep a user from getting into the system. For example, you may need to lock an account if a user is no longer working for your organization.

1) To lock or unlock a user's account, on the **Admin Panel** click the "**Edit**" icon for the user.

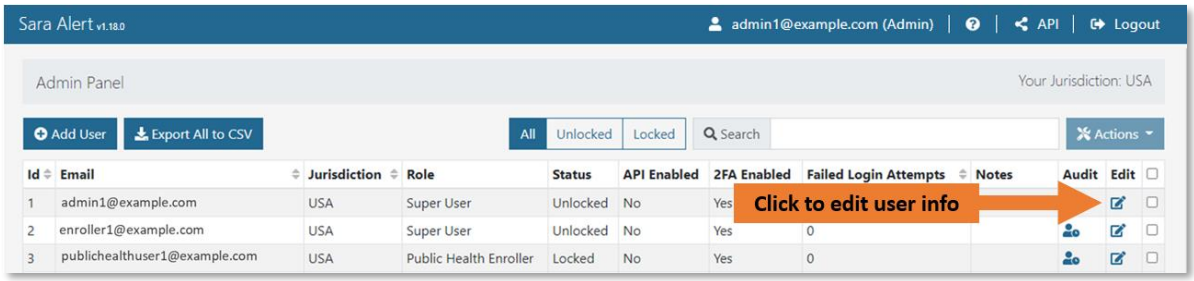


Figure 20: Click the "Edit" icon.

2) Change the "**Status"** switch to Locked or Unlocked. Then, click "Save."

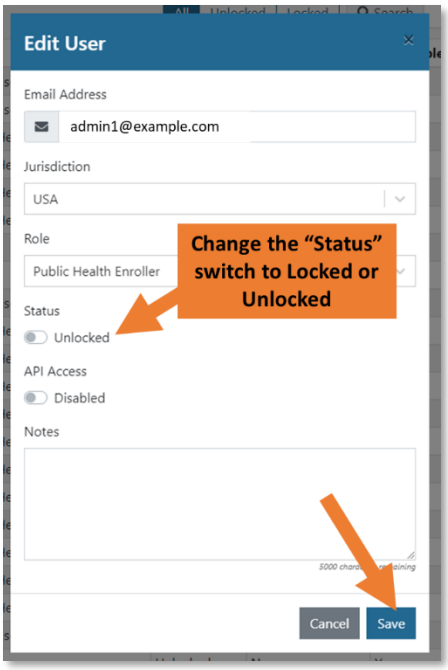


Figure 21: Change the "Status" switch to Locked or Unlocked and click "Save"

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

3) To check the account, see the **"Status"** column on the Admin Panel.

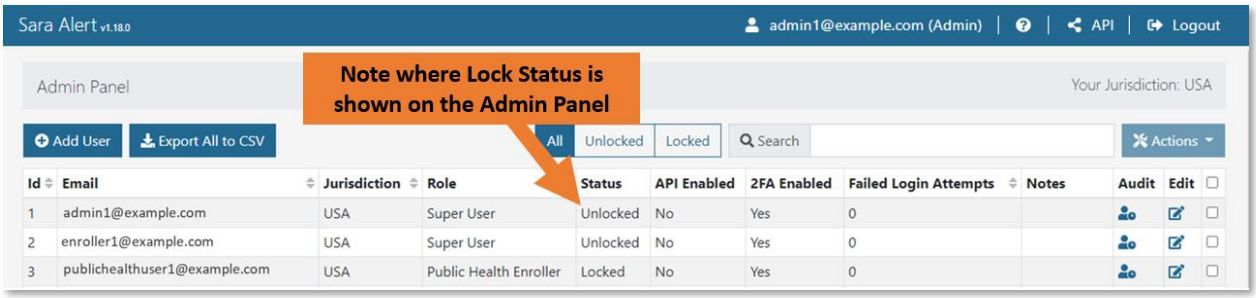


Figure 22: The "Status" column shows if a user's account is locked or unlocked

4) On the **Admin Panel**, you can use the filter buttons to show:

- All users
- Only unlocked users
- Only locked users

Figure 23: Use the filter buttons to show users by locked or unlocked status.

If a user's account is locked, they cannot log in to Sara Alert. If they try to log in, they get an error message that says, "Invalid Email or password."

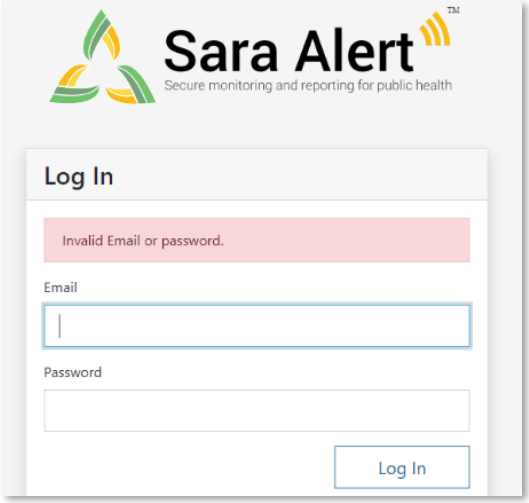


Figure 24: Log In error message for a locked account

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

4.7 How to Reset User Passwords

If a user needs their password reset, they will need to notify their local administrator through another method outside of Sara Alert™. Users may need to have their passwords reset if:

- They forget their password.
- Their jurisdiction requires them to reset their password after a set amount of time. For example, they may need to reset their password every 30 or 60 days. Not all jurisdictions require regular password updates.

You can reset passwords one user at a time or for many users at once. You may need to reset passwords for more than one user if your jurisdiction has regular scheduled resets. When a user's password is reset, Sara Alert sends an email to the user with a temporary password and a prompt to change the password to something they can remember on their own.

1) You can send password reset emails to **users who request a password reset (forgotten password):** Click the checkbox in the last column of the user's row. Check all the users who have requested a password reset.

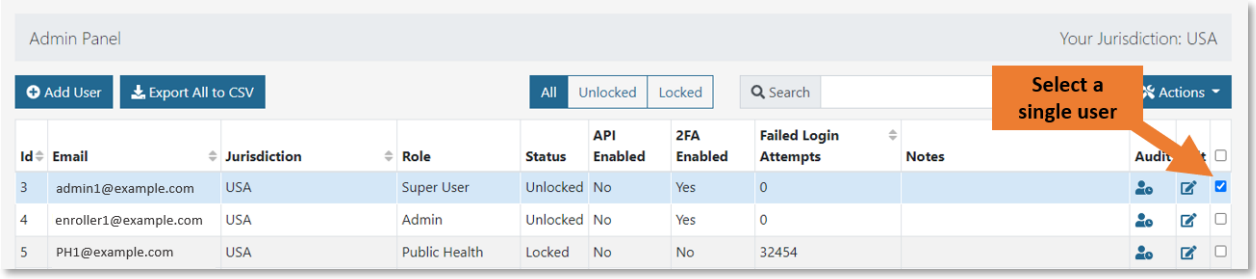


Figure 25: Select the user by clicking the checkbox in the last column

2) If all users in the view require a password update: Click the checkbox in the last column of the header row (next to "Edit"). This selects all the rows in the current view on the screen. It does not select all the rows in the entire list of users. To reset the password of all users in a jurisdiction, you will need to repeat this process across all views (pages).

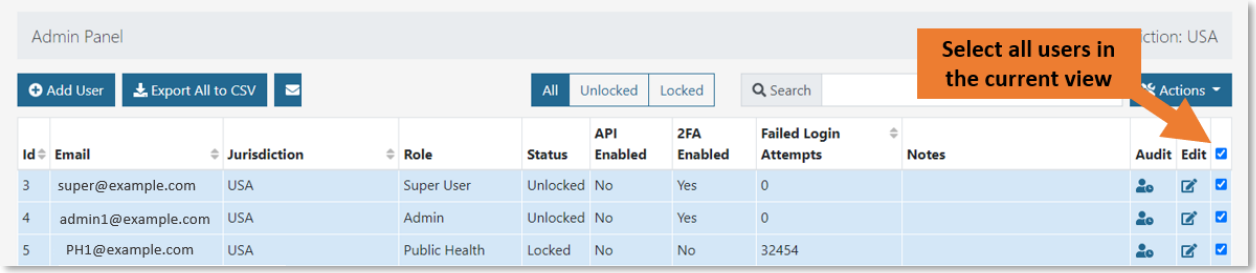


Figure 26: Select all users in the view by clicking the checkbox in the last column of the header row

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

3) Click the **"Actions"** button. In the drop-down menu, click **"Reset Password."**

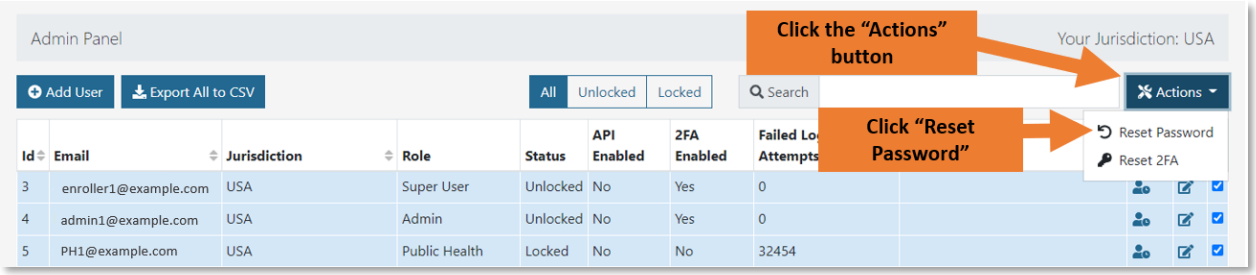


Figure 27: Click the "Actions" button and select "Reset Password" from the drop-down menu.

4) The user receives an email that includes a temporary password. On their next login, they are prompted to change their password. **NOTE:** Temporary passwords expire after 72 hours. If a user does not use the temporary password in 72 hours, you can send another password reset email. You should advise users to enter temporary passwords manually and not copy and paste them.

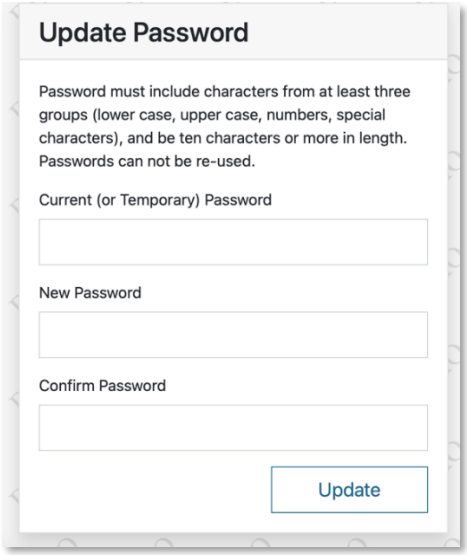


Figure 28: Users create and confirm a new password after a password reset

4.8 How to Manage 2-Factor Authentication

Sara Alert™ uses a 2-factor authentication (2FA) system that requires a user to give the following information when they log in:

- The user's Sara Alert password
- A seven-digit number (called a token) sent to the user's phone from Sara Alert

2FA is a requirement for all Sara Alert users to help maintain the tool's security and keep monitoree information safe.

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

4.8.1 View 2FA Status

On the **Admin Panel**, the "**2FA Enabled**" column shows if a user has enabled (set up) 2FA. If a user has not enabled 2FA, the system prompts them to register for 2FA on their next login.

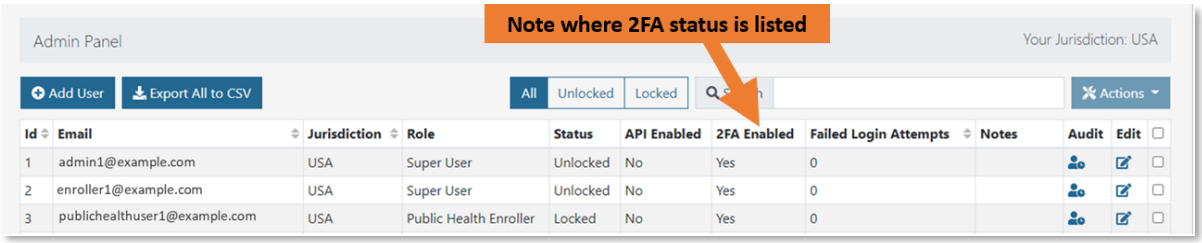


Figure 29: 2FA status

4.8.2 Resetting 2FA

If a user needs to change the phone number that they use for 2FA, they should let their jurisdiction's local **Administrator** or **Super User** know. If they change their phone number, they will also need to reset their 2FA.

To change a user's phone number and reset their 2FA:

1) In the **Admin Panel**, select the user requesting the change. Do this by clicking the checkbox in the last column of the user's row. You can select more than one user if more than one user is changing their number.

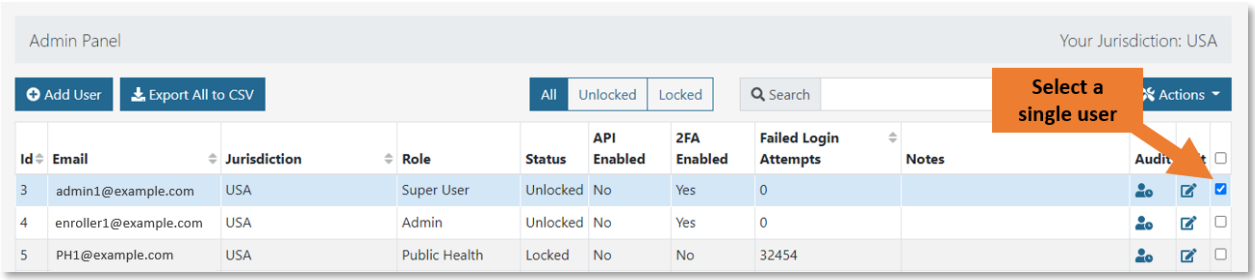


Figure 30: Select the user by clicking the checkbox in the last column

2) Click **"Actions"** and select **"Reset 2FA"** from the drop-down menu.

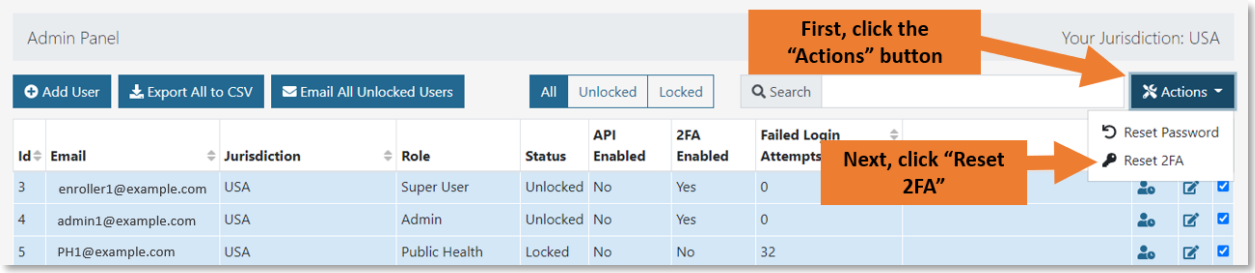


Figure 31: Reset a user's 2FA

The user's 2FA column changes to "No." Sara Alert™ prompts the user to start 2FA on their next log in.

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

4.9 How to Use the Sara Alert™ API

Your jurisdiction can use the Sara Alert Application Programming Interface (API) to connect to exchange monitoree data between other data systems you may use with Sara Alert. The API allows the other software systems to read (request) specific monitoree data from Sara Alert, and to write (putting new data into the system) monitoree data to Sara Alert. To learn about what an API is, what the Sara Alert API does, or how to use the Sara Alert API in your jurisdiction visit https://saraalert.github.io/SaraAlert/api/api-getting-started.

Sara Alert's API uses Sustainable Medical Applications, Reusable Technologies (SMART) on HL7 Fast Healthcare Interoperability Resources (FHIR) API standards and specifications.

Additional standards used to support the API include:

- FHIR Release 4 (R4), its components, and specifications
- SMART application launch framework
- C# FHIR library
- OAuth 2.0

Sara Alert also provides the ability to export monitorees from Sara Alert in the Public Health Document Container (PHDC) format to support interoperability with jurisdictions that use NBS.

The Sara Alert™ API documentation is available to users on GitHub here.

4.9.1 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**: Email sarasupport@aimsplatform.com to register a Sara Alert™ client application for API use. Additional information on the registration process can be found here.
2. **Authorization**: Once registered, you must authorize the client application to use the API and obtain an authorization code, which in turn is used to get an access token. Additional information can be found here.
3. **Authentication**: The obtained access token is then used to make API requests to the Sara Alert API.

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

4.10 How to Enable API Access

If your jurisdiction is **already using the Sara Alert API** to transfer data between a different data system and Sara Alert, you may need to give a user in your jurisdiction API access. You can provide API access to users in your jurisdiction **with the system Administrator's approval.**

1) To change API access for a user, on the **Admin Panel** click the "**Edit**" icon for the user.

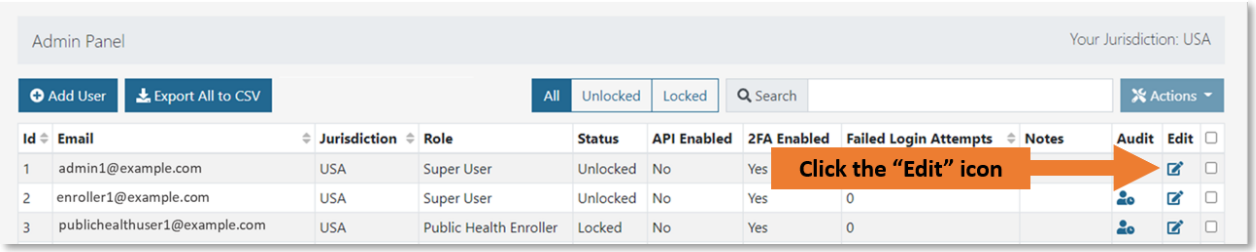


Figure 32: Click the "Edit" icon.

2) In the **Edit User** window, move the **API Access** switch to Enabled or Disabled.

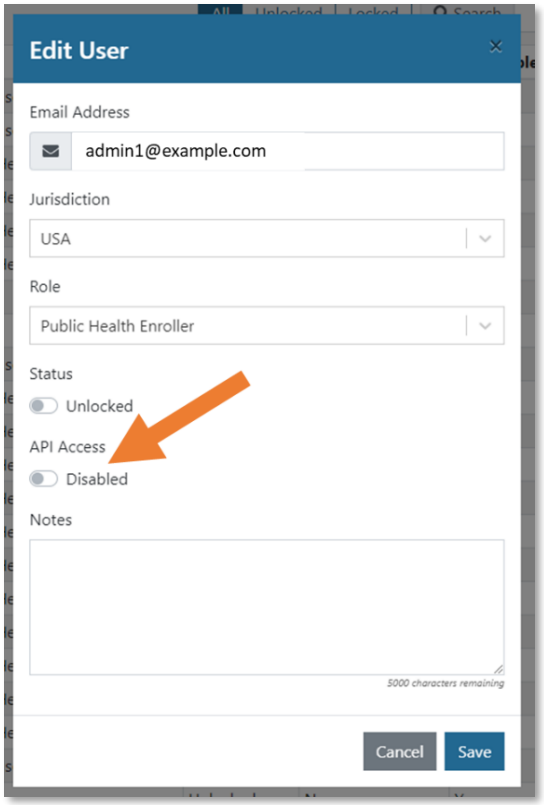


Figure 33: Move the "API Access" switch to Enabled or Disabled

3) Click **"Save."**

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176

Appendix A Assigning User Roles

Table A-1 can help when you are assigning roles to users in your jurisdiction. Assign user roles based on:

- The tasks the user performs
- The records needed to perform the tasks

Table A-1. Functional Summary by Role

Task	Enroller	Public Health	Public Health Enroller	Contact Tracer	Analyst	Adminis-trator	Super User
Enroll New Exposed Monitoree	✓		✓	✓			✓
Enroll New Case	✓		✓	✓			✓
Add Close Contacts		✓	✓	✓			✓
Enroll Close Contacts			✓	✓			✓
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	Only records added by the user	All records in jurisdiction	All records in jurisdiction	All records in jurisdiction	None; View Aggregate Data Only	None; Manage users in jurisdiction	All records and users in jurisdiction

©2021 The MITRE Corporation. All rights reserved.

Approved for Public Release Case #20-1176