

SDS
2.0

Smart Digital Systems

User Guide for CX Hub | Account Management



Co-Confidential

6th March 2024, Release 4 v1.0

AGENDA

Table of Contents

1. FortiClient VPN

- Secured Network Access
- Installation
- Creating a new VPN Connection
- Connecting to FortiClient VPN

2. SDS 2.0 Administrator Account

- Admin Console Login
- First-Time Login
- Password Policies
- Setting up OTP Token
- Using Google Authenticator
- Scan a QR Code
- Enter a Setup Key
- Where to find Setup Key
- Setting up OTP via Key Entry
- Completing OTP Setup
- Change OTP Token
- Forget or Lost Physical OTP Device
- Account Management
- Update My Account
- Update Account Information
- Change Password
- Forget Password
- Admin Console Page
- Sign Out of Admin Console

3. User Account Management

- User Accounts
- Account Creation
- Update/Edit Account Details
- Reset Password
- Reset OTP Token
- View OTP Algorithm
- Sessions
- Delete User

FortiClient VPN

- Secured Network Access
- Installation
- Creating a new VPN Connection
- Connecting to FortiClient VPN

Secured Network Access

FortiClient VPN required to be installed and activated on the administrator's computer device to access SDS2.0 Admin Console.

It provides a secure, reliable access to SDS2.0 Admin Console network from any internet connected remote location. Go to <https://www.fortinet.com/support/product-downloads#vpn> to download the latest FortiClient VPN installer for your device.

FortiClient VPN

The VPN-only version of FortiClient offers SSL VPN and IPsecVPN, but does not include any support. Download the best VPN software for multiple devices.

Remote Access

- ✓ SSL VPN with MFA
- ✓ IPSEC VPN with MFA



Download VPN for Windows

DOWNLOAD



Download VPN for MacOS

DOWNLOAD



Download VPN for Linux

DOWNLOAD .rpm



Download VPN for iOS

DOWNLOAD



Download VPN for Android

DOWNLOAD

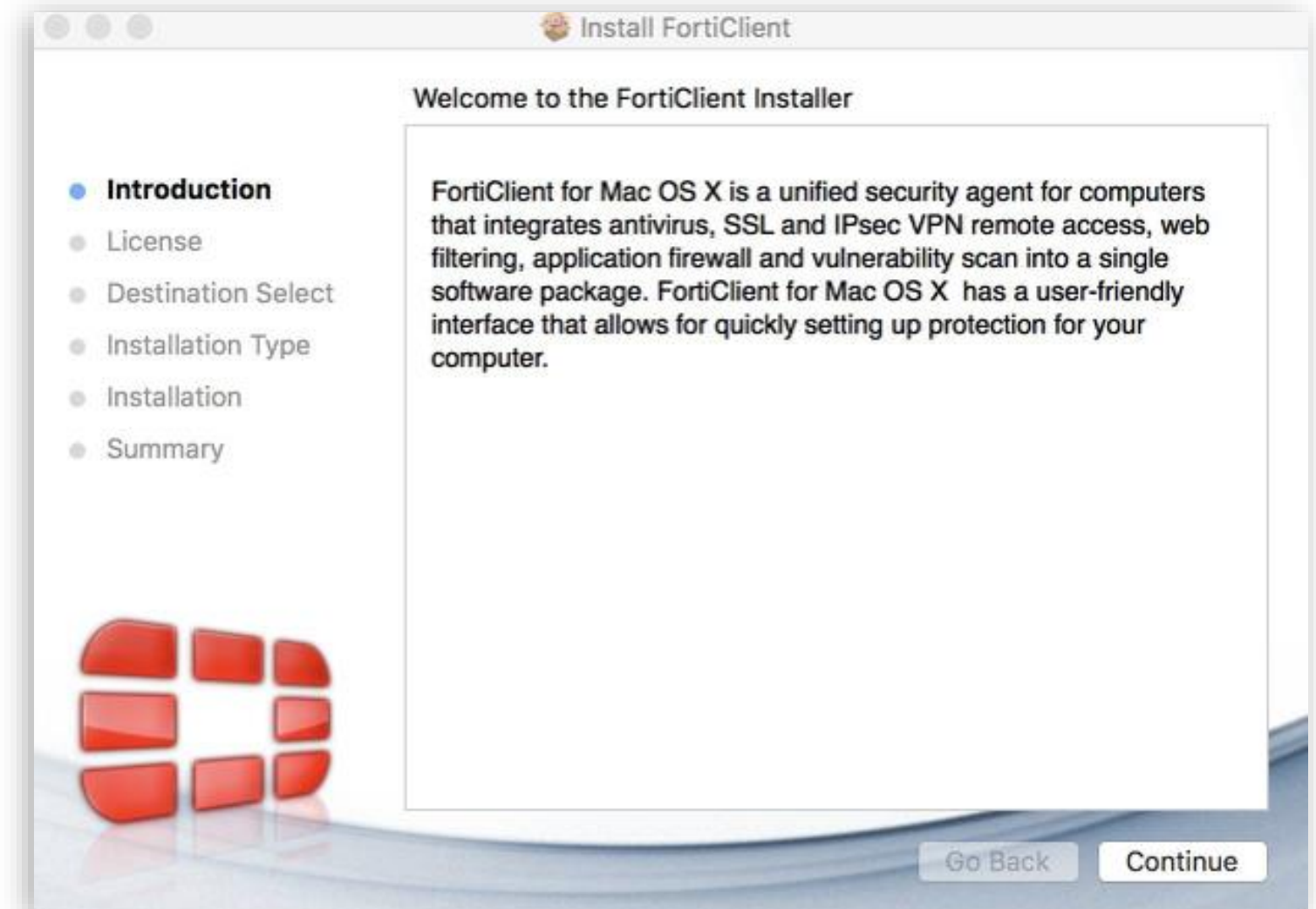


Download VPN for Linux


DOWNLOAD .deb

Installation

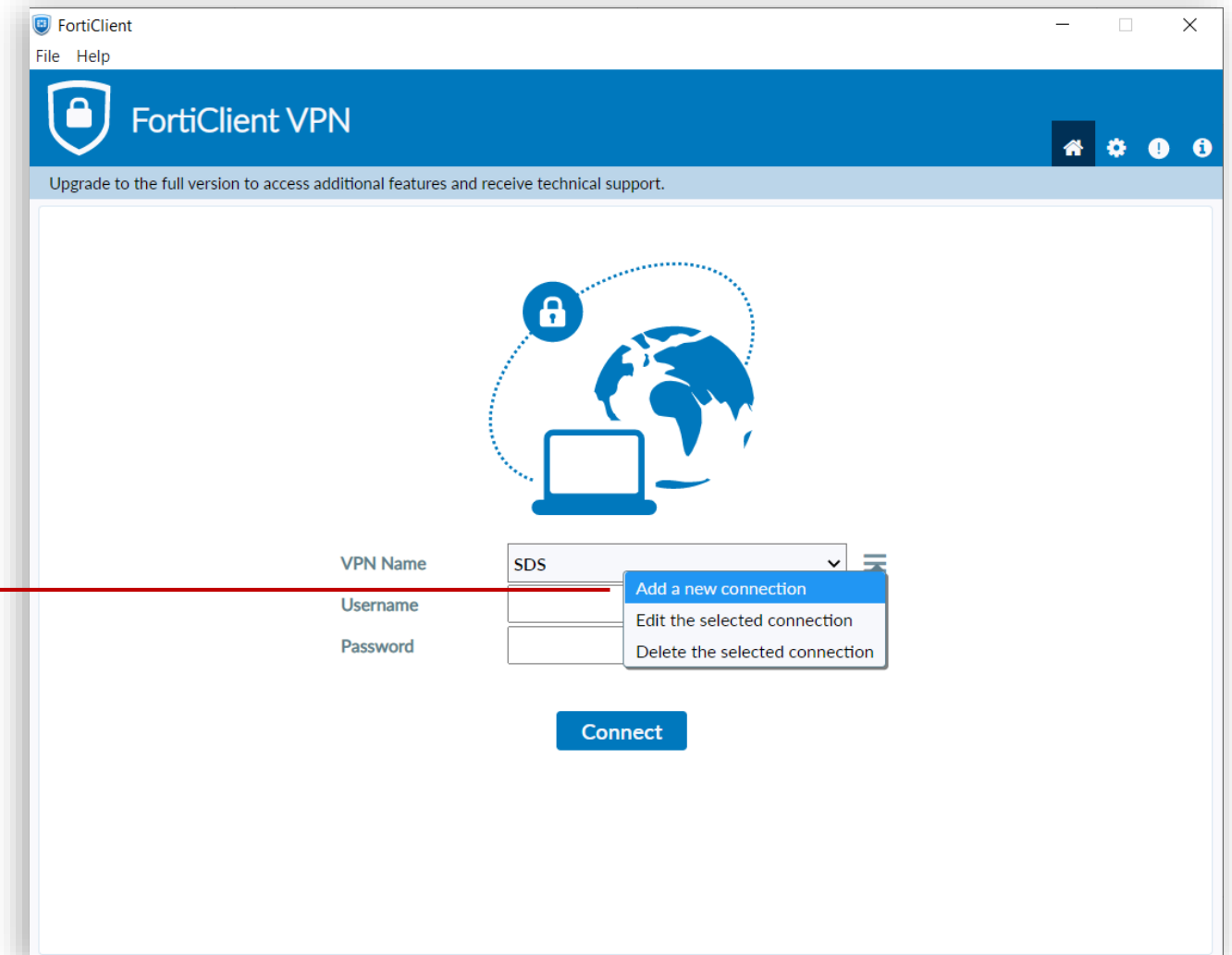
Launch the FortiClient VPN installer and follow the instructions displayed on the screen to install the software successfully.



Creating a new VPN Connection

Launch the FortiClient VPN software and tap on the menu bar. 

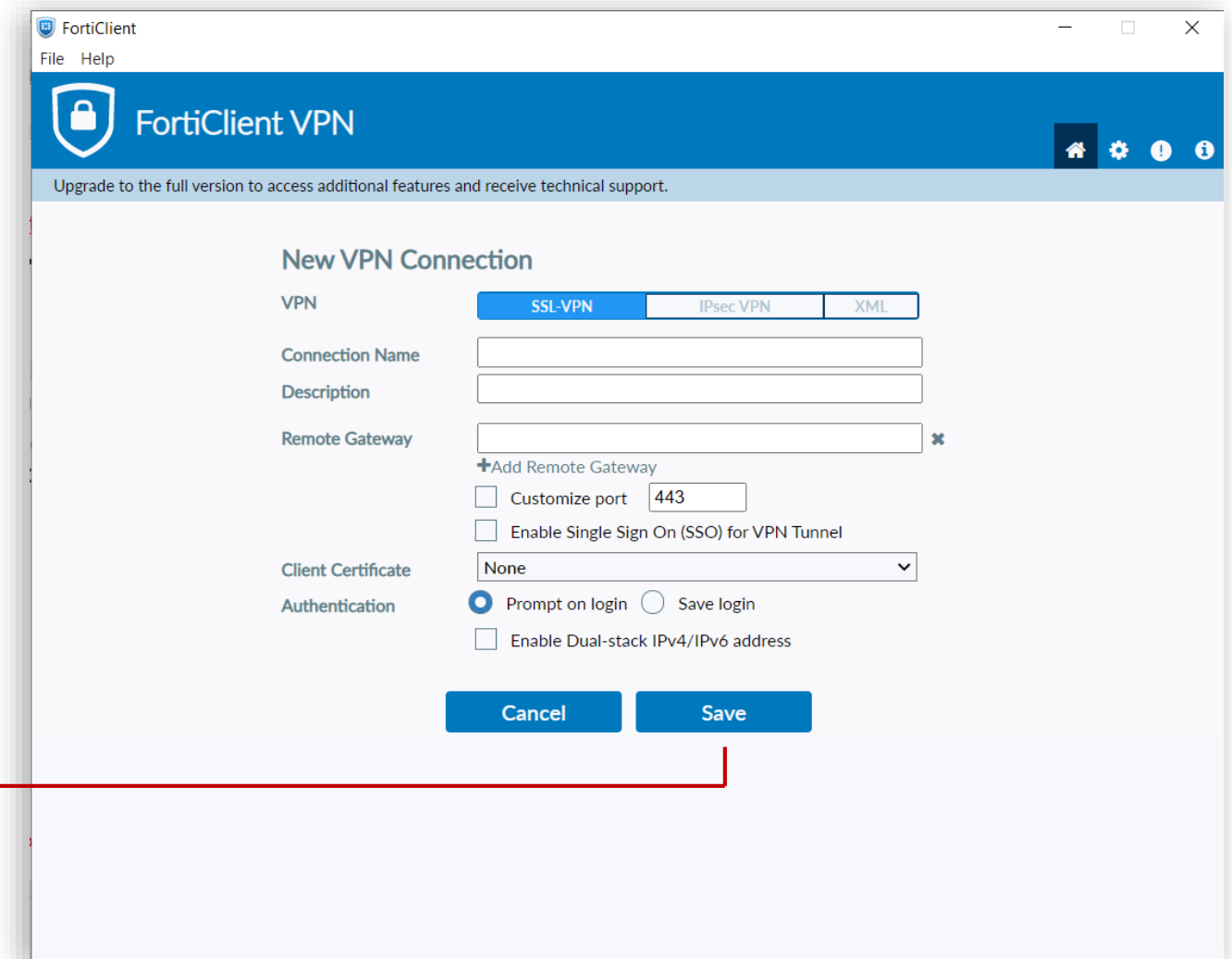
Then select **[Add a new connection]** from the dropdown list.



Creating a new VPN Connection

Information to create a new VPN connection, including the username and password **will be raised in accordance with the escalation matrix** in a separate channel.

Enter the necessary information for the VPN connection and tap **[Save]**.



FortiClient
File Help

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

New VPN Connection

VPN: **SSL-VPN** | IPsec VPN | XML

Connection Name:

Description:

Remote Gateway: ✕

+Add Remote Gateway

Customize port:

Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: ▾

Authentication: Prompt on login Save login

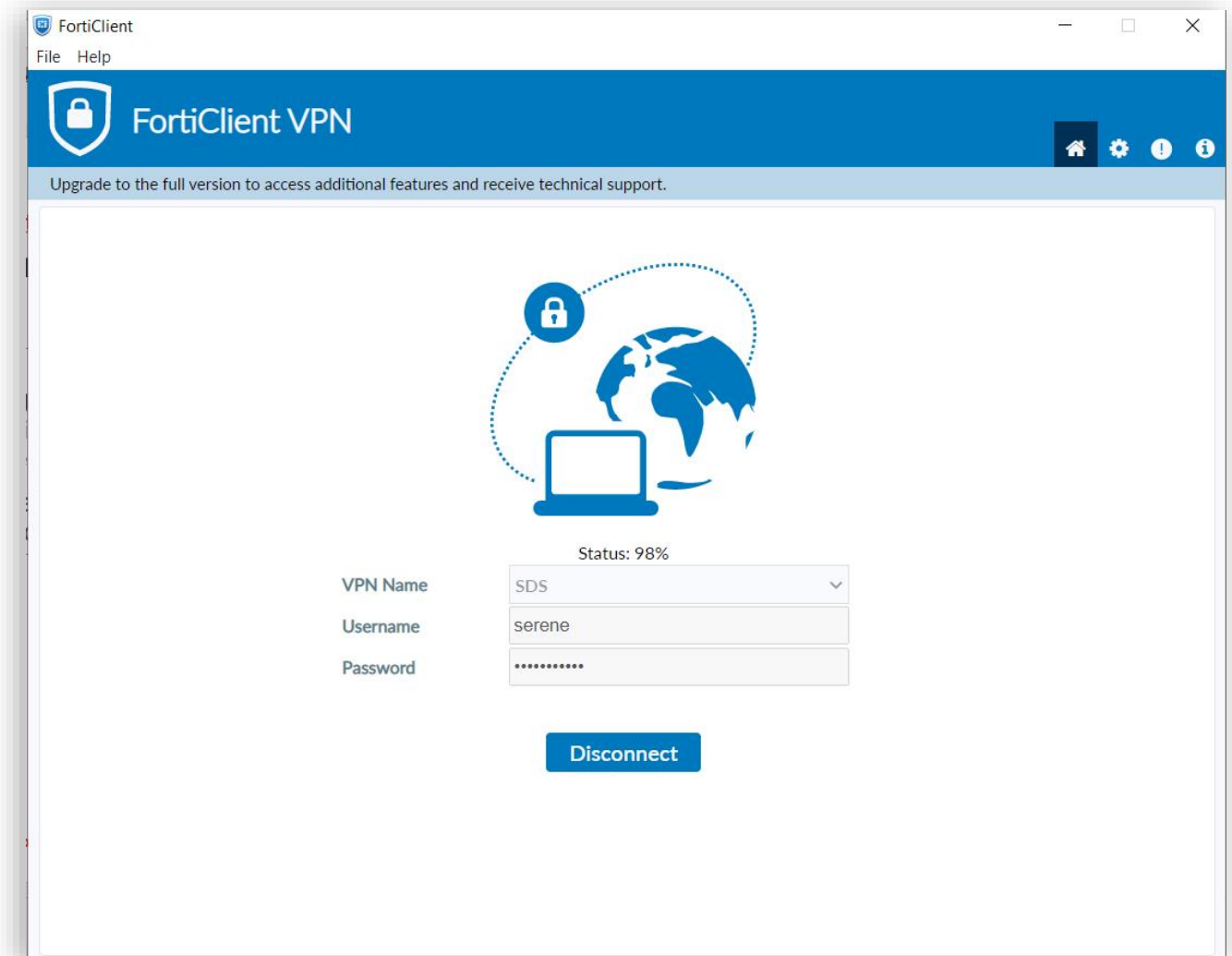
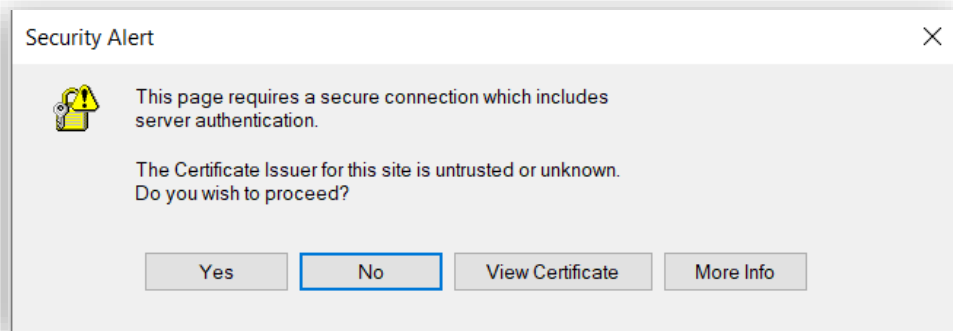
Enable Dual-stack IPv4/IPv6 address

Cancel **Save**

Connecting to FortiClient VPN

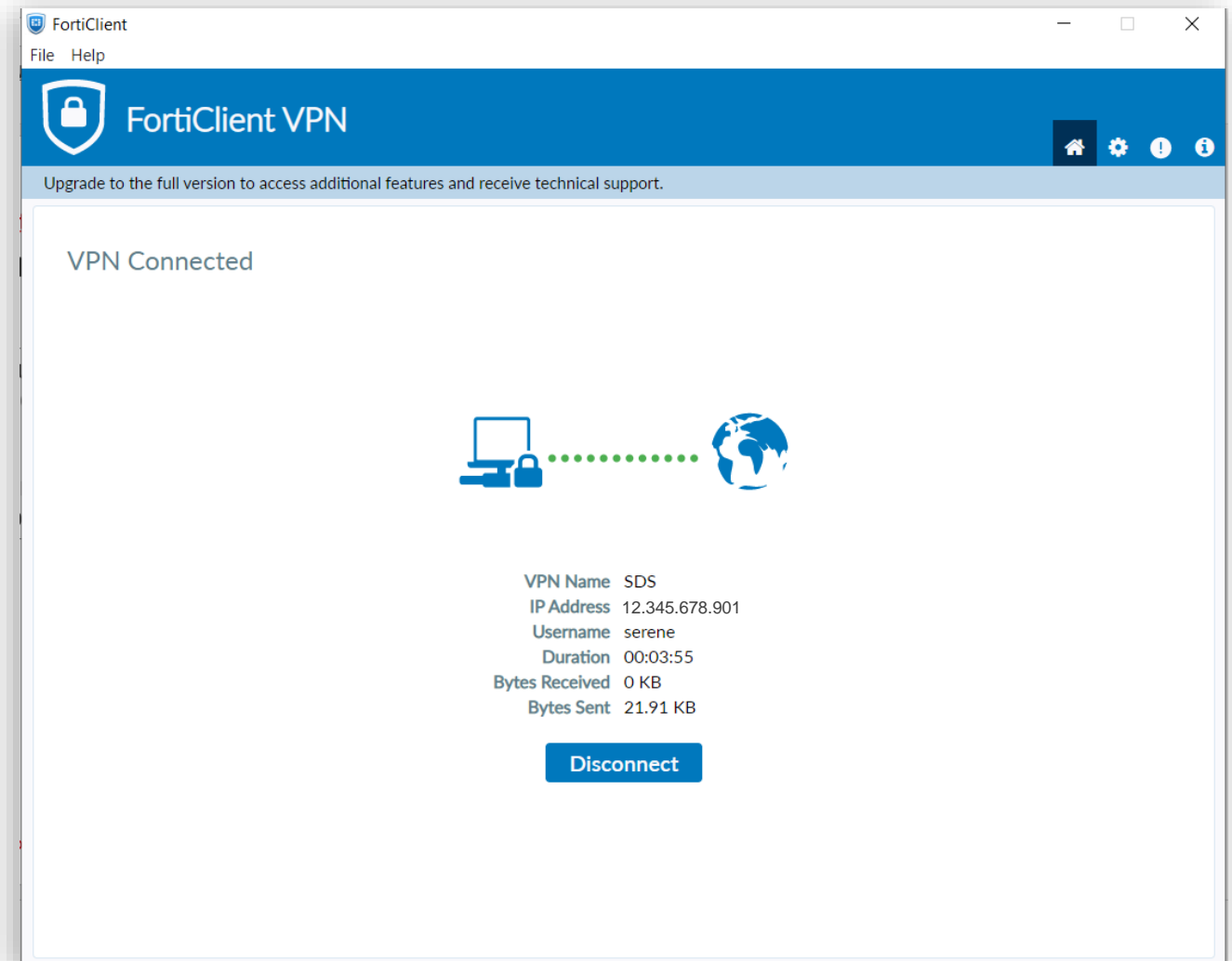
Enter your credential provided by the SDS 2.0 Team and tap **[Connect]**.

Windows may prompt a security alert on server authentication, tap **[Yes]** to proceed with the server connection.



Connecting to FortiClient VPN

It will inform you when the VPN is successfully connected to the IP Address.



SDS 2.0 Administrator Account

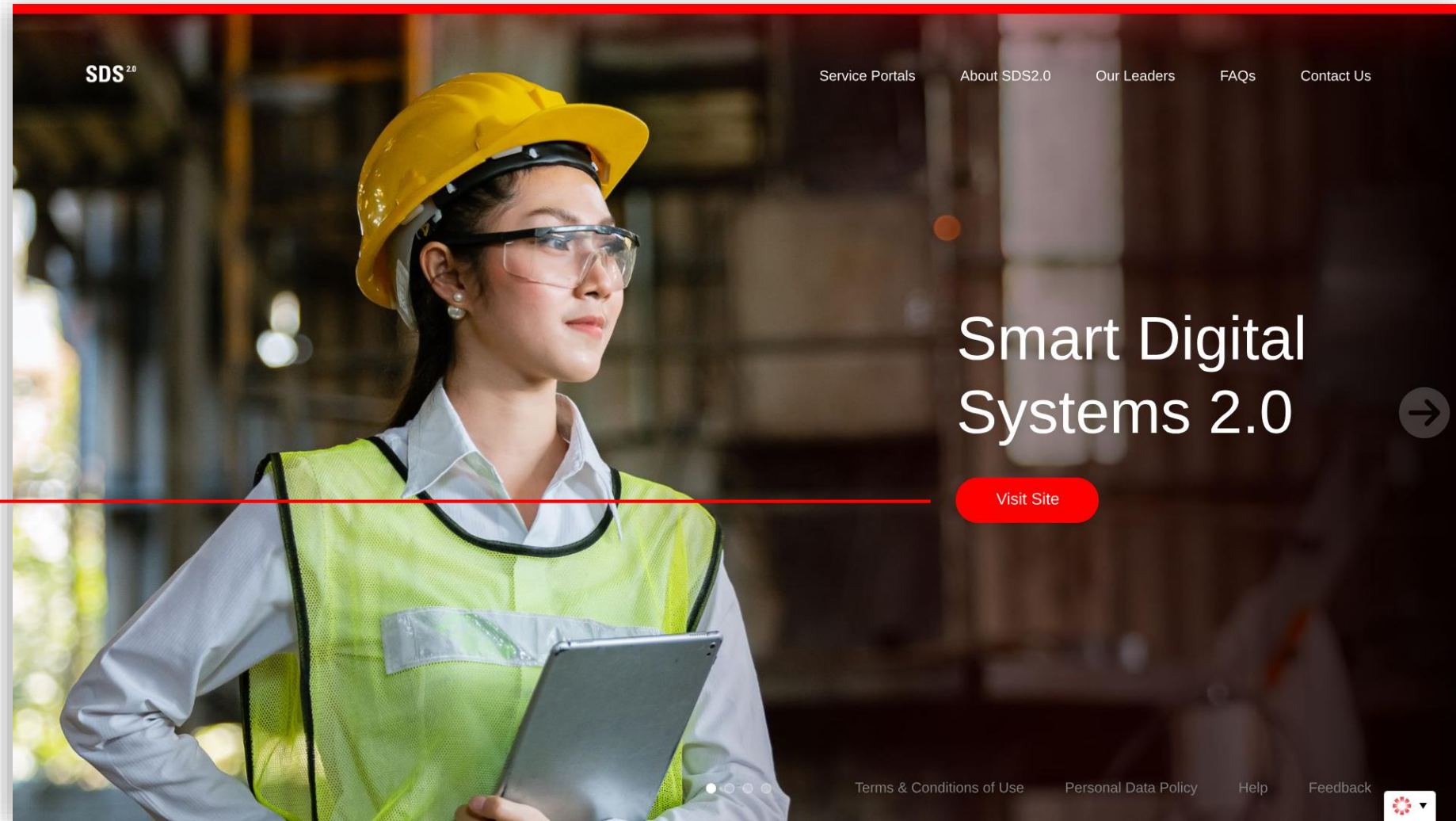
- Admin Console Login
- First-Time Login
- Password Policies
- Setting up OTP Token
- Using Google Authenticator
- Scan a QR Code
- Enter a Setup Key
- Where to find Setup Key
- Setting up OTP via Key Entry
- Completing OTP Setup
- Change OTP Token
- Forget or Lost Physical OTP Device
- Account Management
- Update My Account
- Update Account Information
- Change Password
- Forget Password
- Admin Console Page
- Sign Out of Admin Console

Admin Console Login (1)

To access SDS2.0:

<https://sds.stengg.com>

Then select **Visit Site**



Admin Console Login (2)

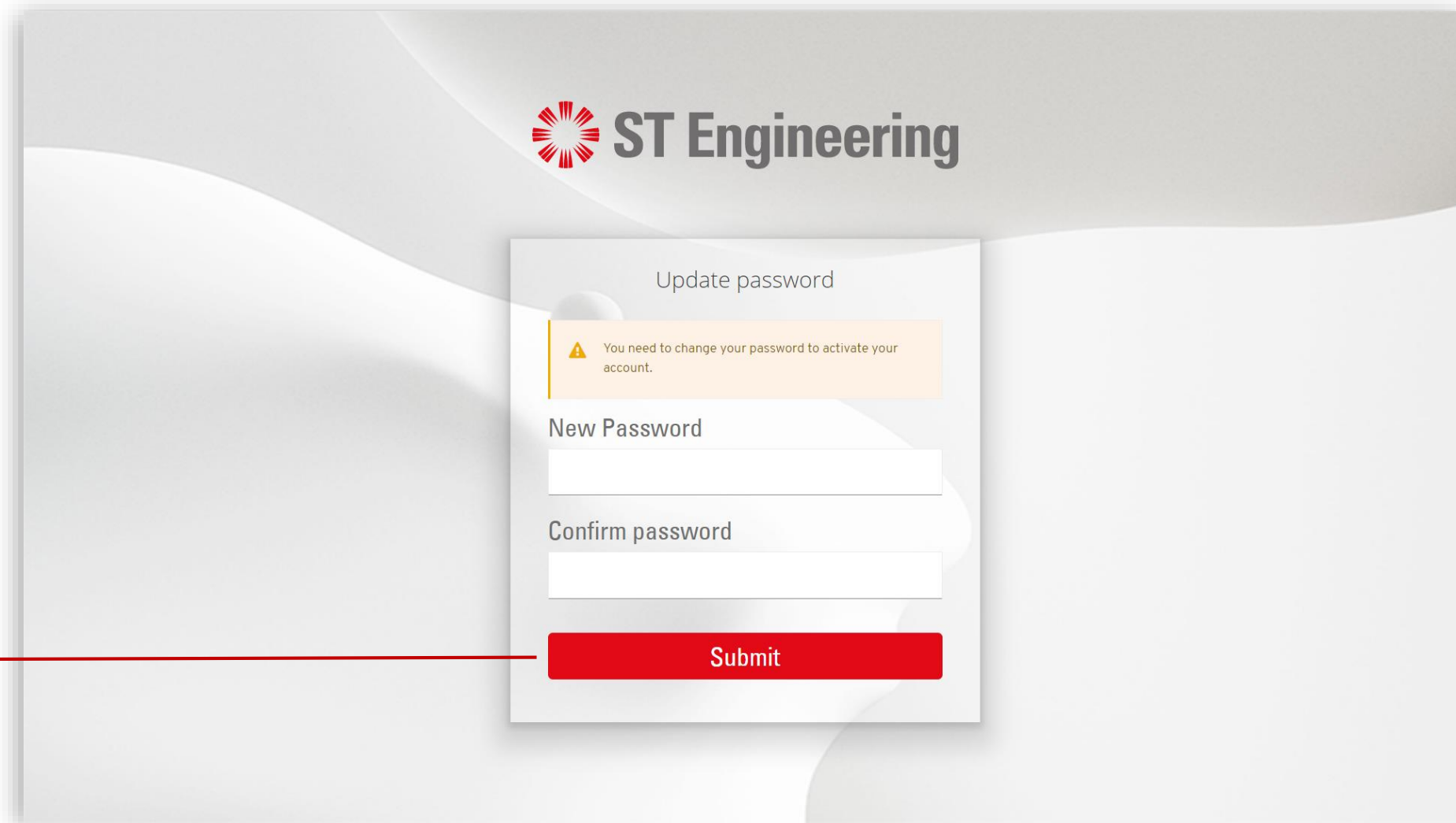
Enter your username
and Password here
and click **Sign In**.




First-Time Login

If it is your first-time login to the system, you will be prompted to change your password.

Enter a new password and re-enter your password to confirm, then tap **[Submit]**



Update password

 You need to change your password to activate your account.

New Password

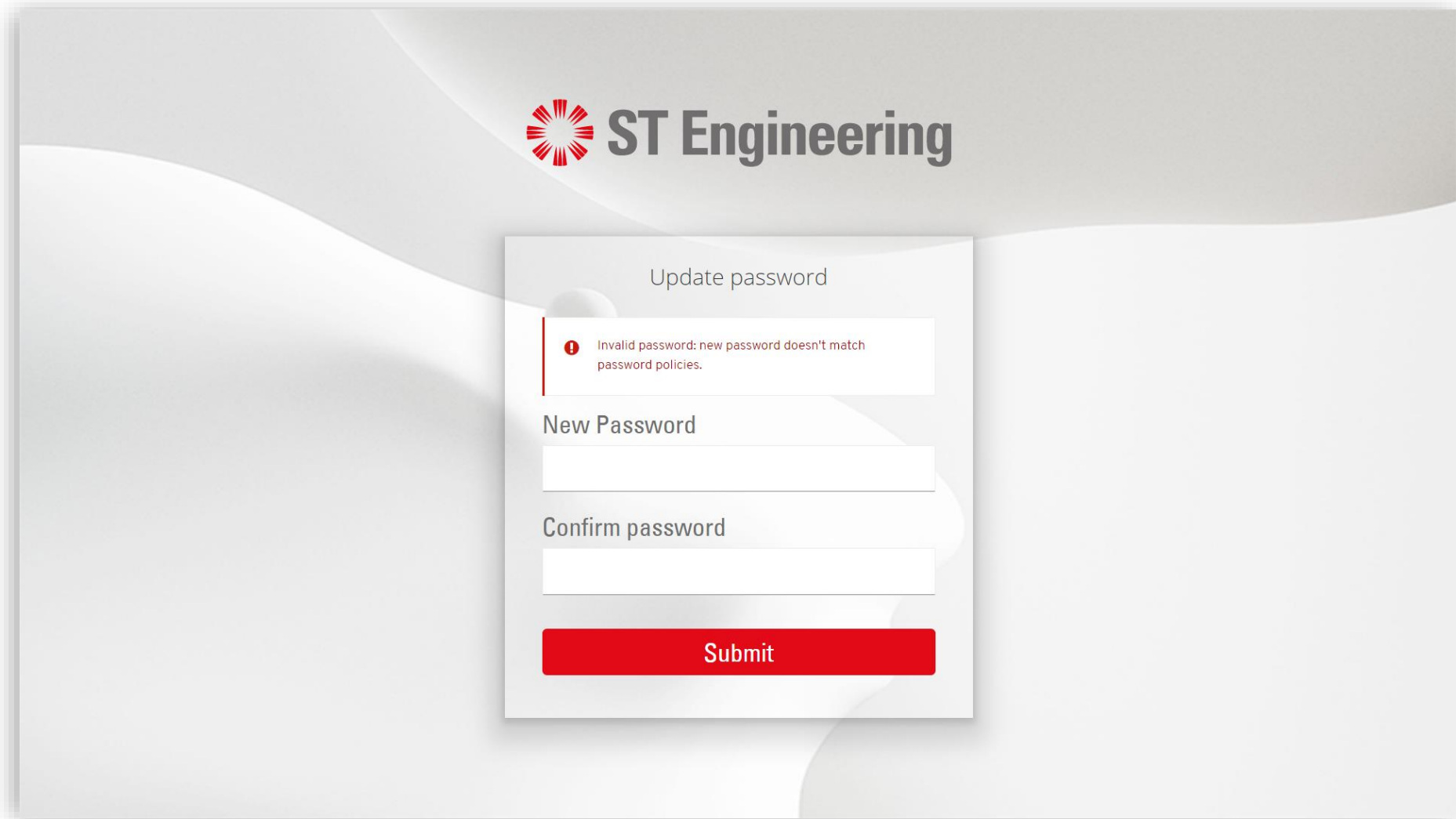
Confirm password

Submit

Password Policies

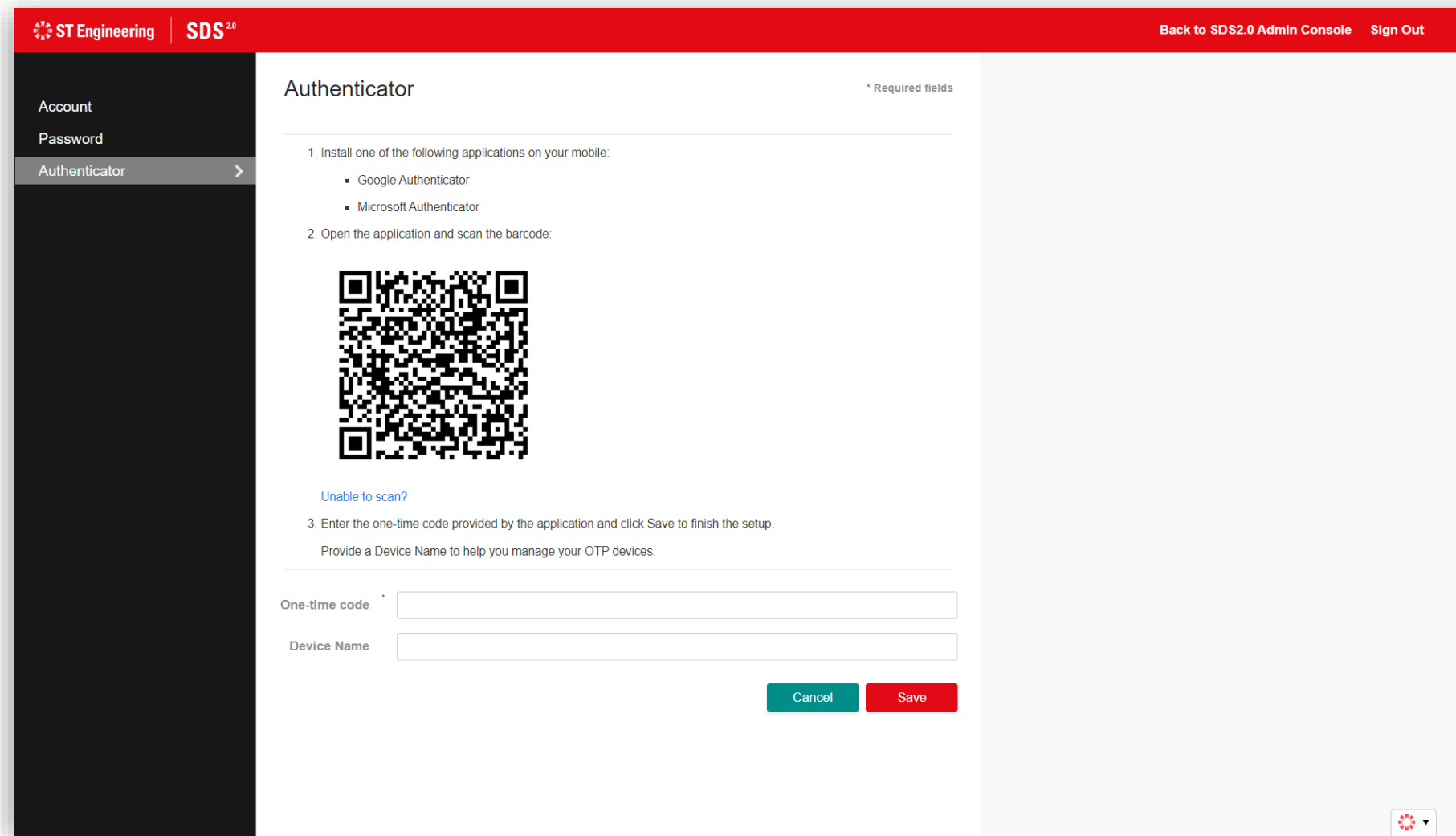
Ensure your password have:

- 1) A min. of 8 characters in length
- 2) At least one upper case and one lower case character
- 3) At least one special character and one numeric character



Setting up OTP Token (1)

For First-Time Login, you will be redirected to the Authenticator Page to setup a **One Time Password (OTP)** linked to your Admin Console account.




The screenshot shows the 'Authenticator' page in the SDS 2.0 Admin Console. The page has a red header with the ST Engineering logo and 'SDS 2.0' on the left, and 'Back to SDS2.0 Admin Console' and 'Sign Out' on the right. A dark sidebar on the left contains navigation links for 'Account', 'Password', and 'Authenticator'. The main content area is titled 'Authenticator' and includes a list of instructions: 1. Install one of the following applications on your mobile: Google Authenticator, Microsoft Authenticator. 2. Open the application and scan the barcode: A QR code is displayed. 3. Enter the one-time code provided by the application and click Save to finish the setup. Below the instructions, there are two input fields: 'One-time code' and 'Device Name'. At the bottom right, there are 'Cancel' and 'Save' buttons.

ST Engineering | SDS 2.0 Back to SDS2.0 Admin Console Sign Out

Account
Password
Authenticator

Authenticator * Required fields

1. Install one of the following applications on your mobile:
 - Google Authenticator
 - Microsoft Authenticator
2. Open the application and scan the barcode:

3. Enter the one-time code provided by the application and click Save to finish the setup.
Provide a Device Name to help you manage your OTP devices.

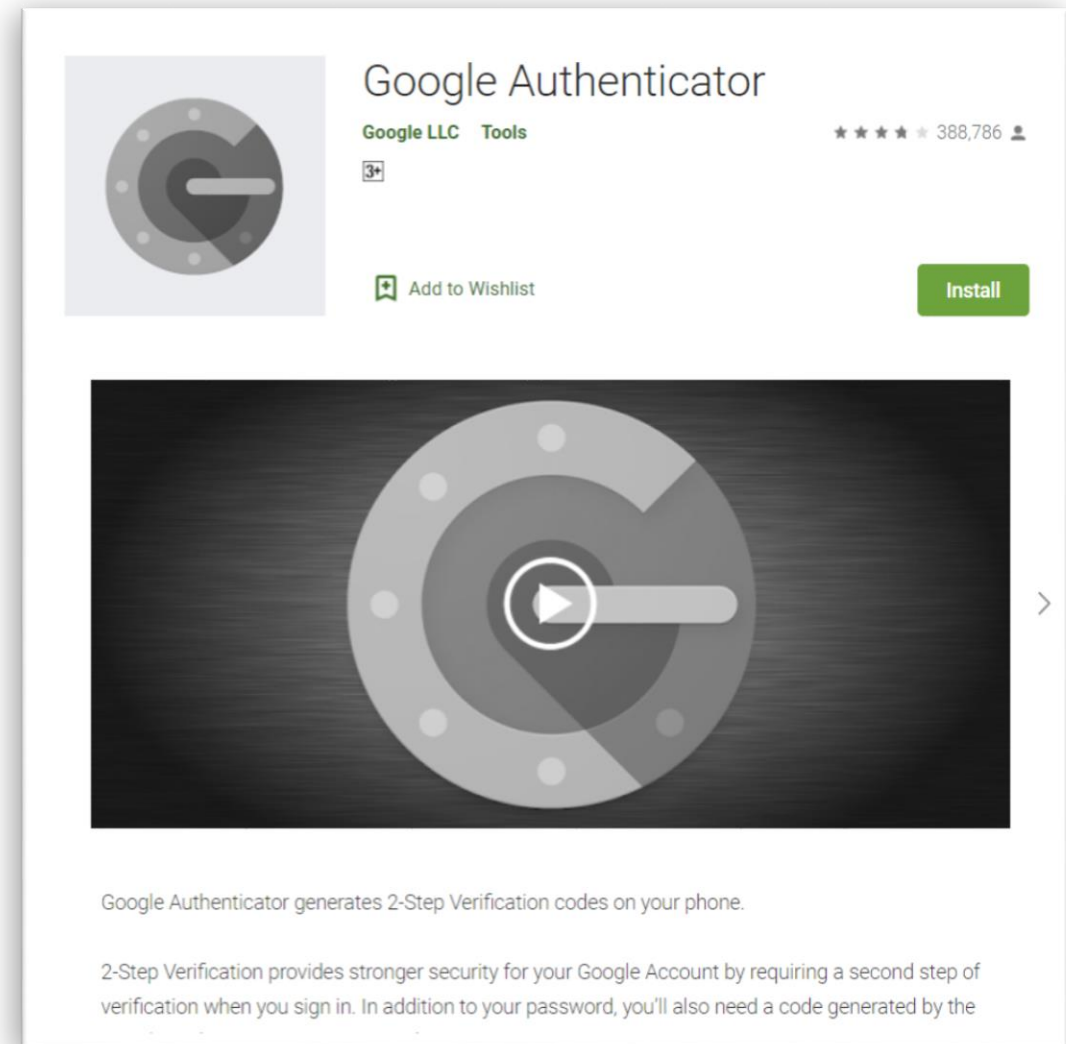
One-time code

Device Name

Setting up OTP Token (2)

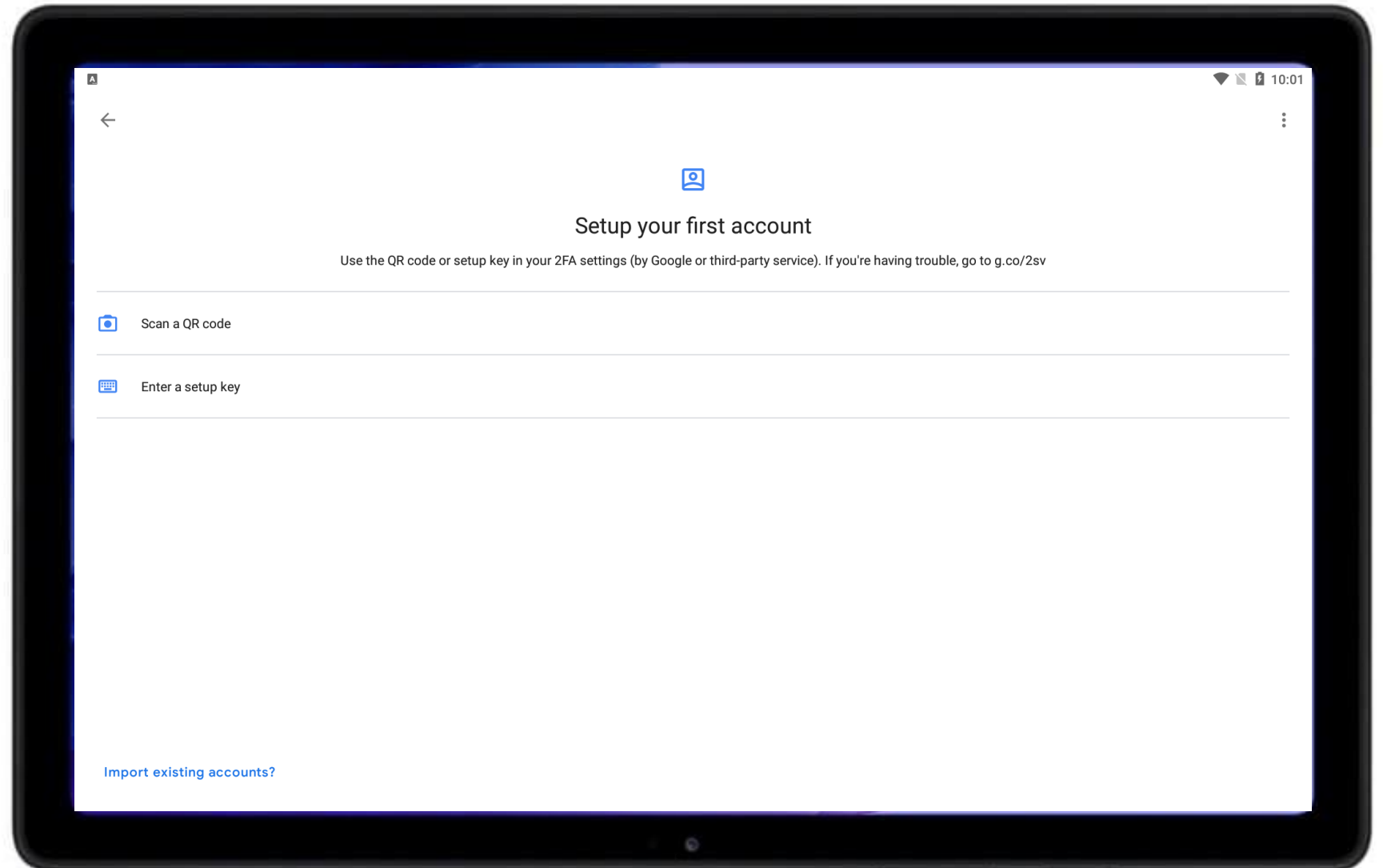
Download **Google Authenticator** app from Google Play Store or App Store.

Note: You can also use **Microsoft Authenticator** App as an alternative app to setup the OTP token.

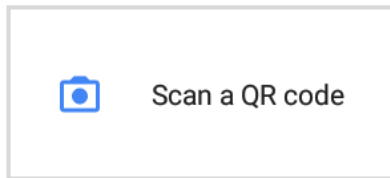


Using Google Authenticator

You can choose to scan your QR code displayed on your Authenticator page or enter a setup key.



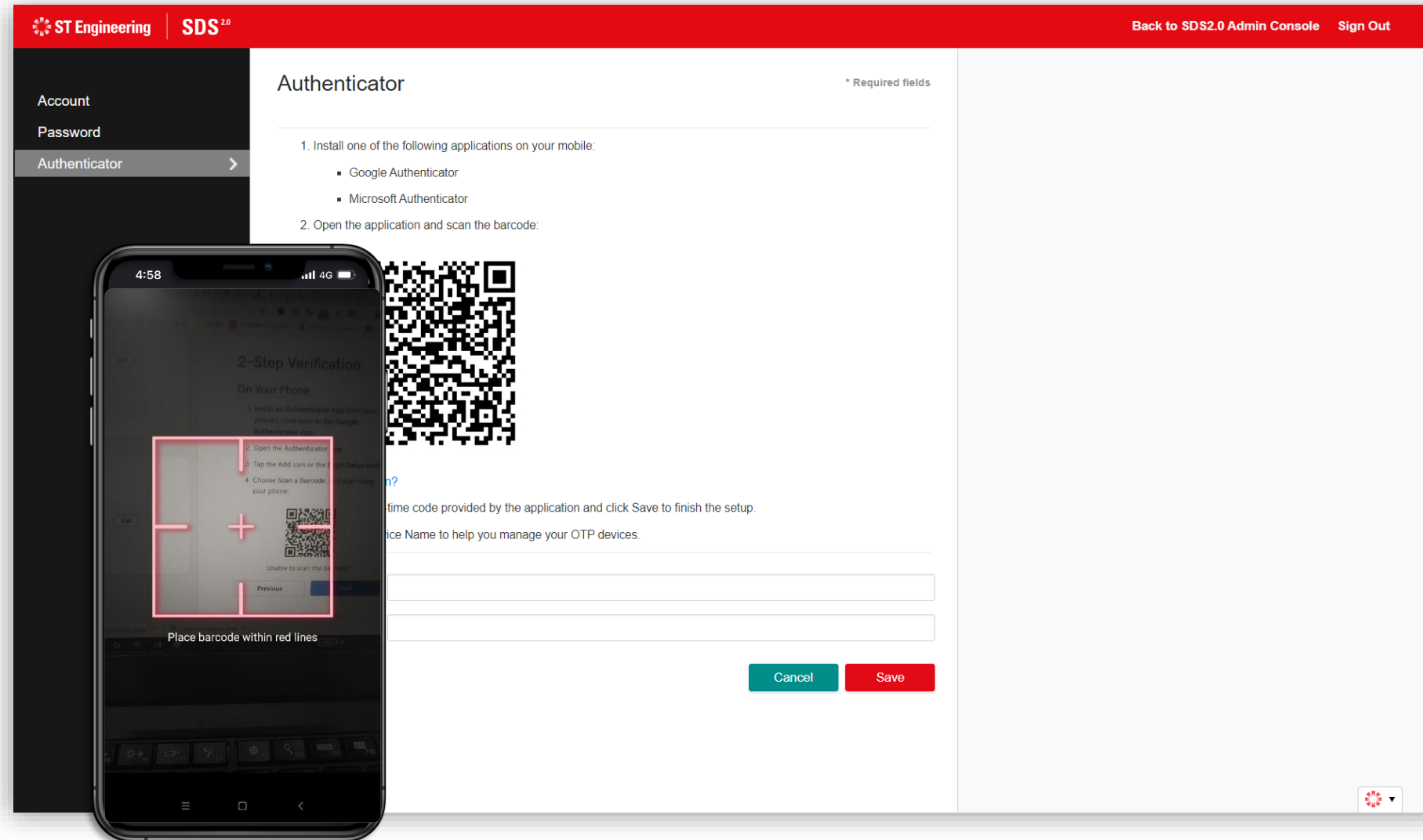
Scan a QR Code



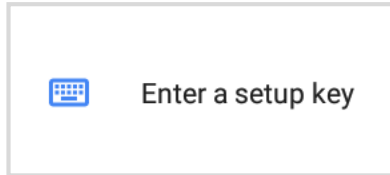
If you have selected **[Scan a QR code]**, your device camera will be activated for scanning.

Scan the QR code shown on Authenticator page.

Then go to [slide 20](#) to complete your OTP setup.

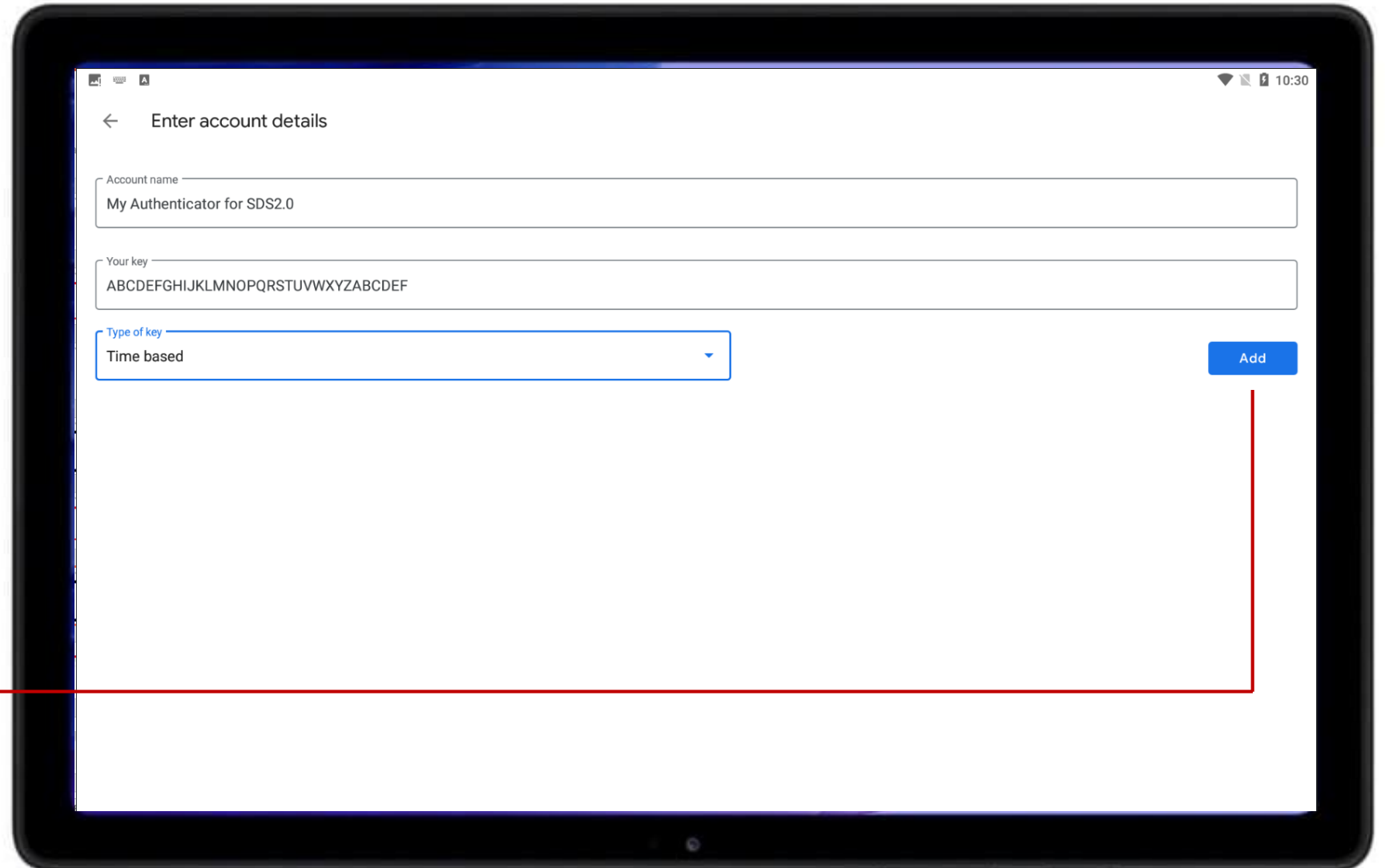


Enter a Setup Key




If you have selected **[Enter a setup key]**, you will need to input an Account name, your setup key, and the type of key.

Then tap **[Add]** to create your OTP token.

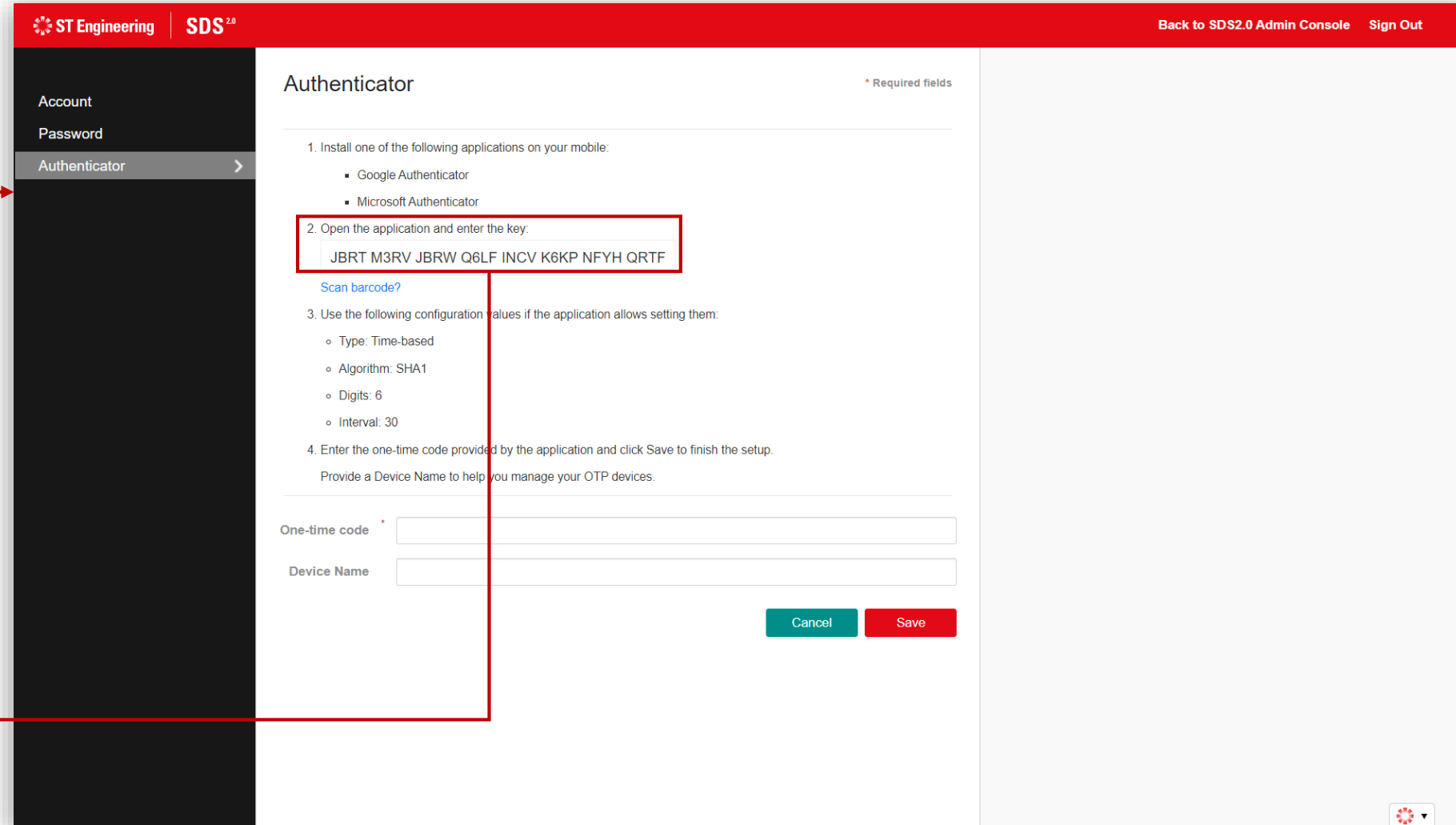


Where to find Setup Key



[Unable to scan?](#)

3. Enter the one-time code provided by
Provide a Device Name to help you m



ST Engineering | SDS 2.0 Back to SDS2.0 Admin Console Sign Out

Authenticator * Required fields

1. Install one of the following applications on your mobile:
 - Google Authenticator
 - Microsoft Authenticator
2. Open the application and enter the key:
3. Use the following configuration values if the application allows setting them:
 - Type: Time-based
 - Algorithm: SHA1
 - Digits: 6
 - Interval: 30
4. Enter the one-time code provided by the application and click Save to finish the setup.
Provide a Device Name to help you manage your OTP devices.

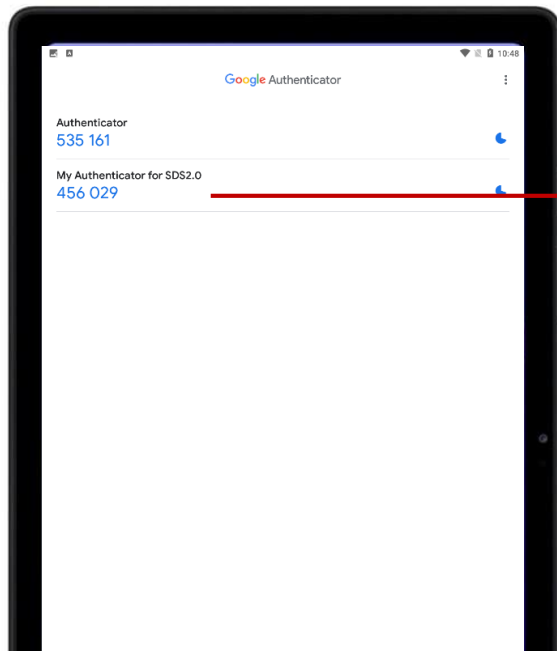
One-time code

Device Name

The setup key is at the Authenticator Page. Tap [\[Unable to scan?\]](#) link below the QR code to view the setup key.

Completing OTP Setup

Enter the one-time code displayed on your mobile and give your device a name, then tap **[Save]**.



ST Engineering | SDS 2.0 Back to SDS2.0 Admin Console Sign Out

Authenticator * Required fields

1. Install one of the following applications on your mobile:
 - Google Authenticator
 - Microsoft Authenticator
2. Open the application and enter the key:

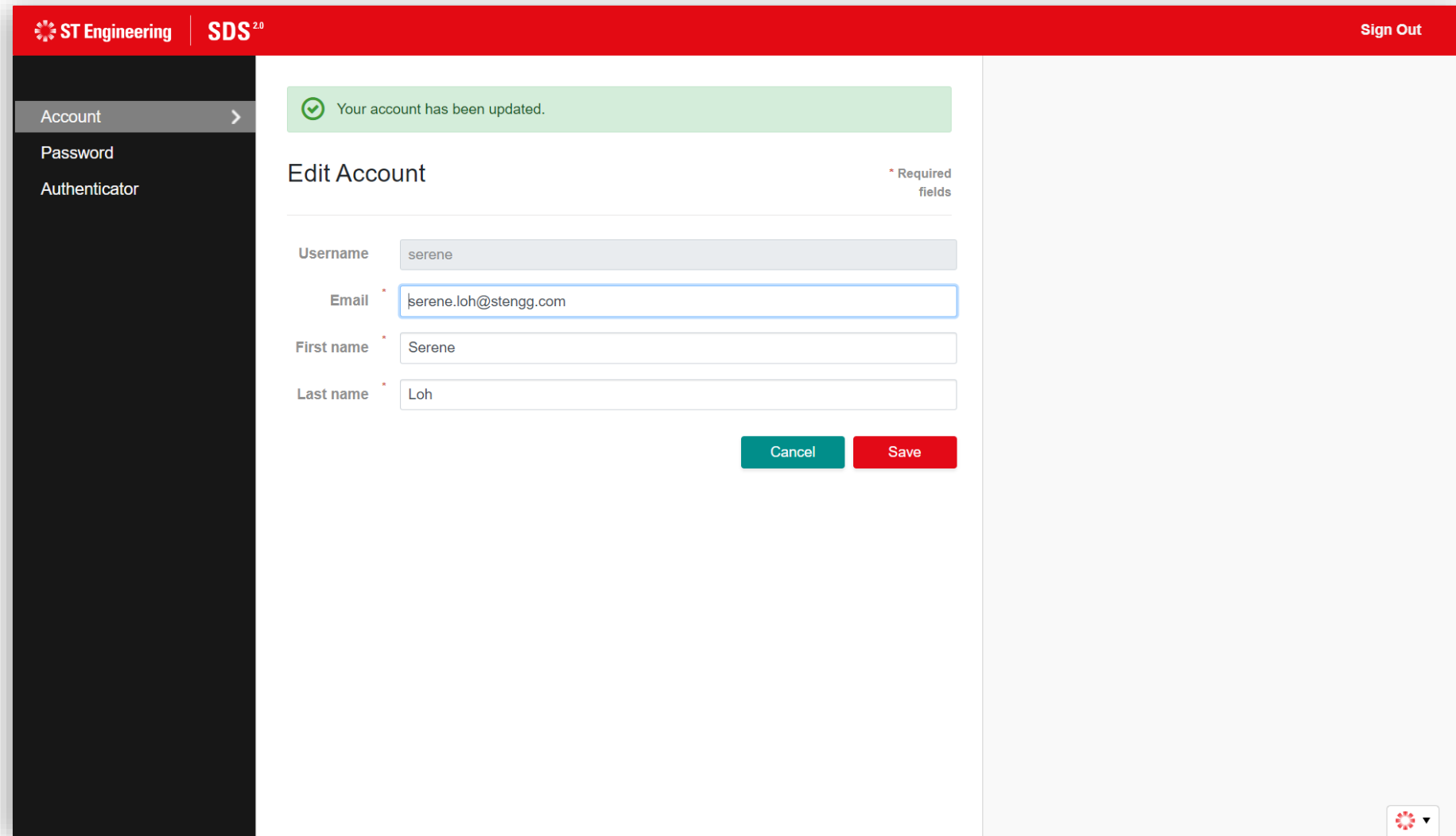
[Scan barcode?](#)
3. Use the following configuration values if the application allows setting them:
 - Type: Time-based
 - Algorithm: SHA1
 - Digits: 6
 - Interval: 30
4. Enter the one-time code provided by the application and click Save to finish the setup.
Provide a Device Name to help you manage your OTP devices.

One-time code

Device Name

Completing OTP Setup

Your authenticator will be created successfully when you followed the steps correctly.



The screenshot displays the 'Edit Account' page in the SDS 2.0 application. At the top, a green notification bar with a checkmark icon indicates 'Your account has been updated.' Below this, the 'Edit Account' form is shown with the following fields:

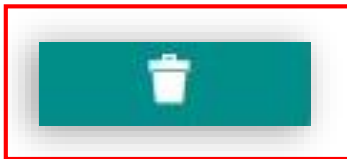
- Username:** serene
- Email:** serene.loh@stengg.com (marked as a required field)
- First name:** Serene (marked as a required field)
- Last name:** Loh (marked as a required field)

At the bottom right of the form, there are two buttons: 'Cancel' and 'Save'. On the left side of the interface, a dark sidebar menu contains the following items: 'Account' (highlighted with a right-pointing arrow), 'Password', and 'Authenticator'. The top navigation bar includes the 'ST Engineering' logo, 'SDS 2.0', and a 'Sign Out' link.

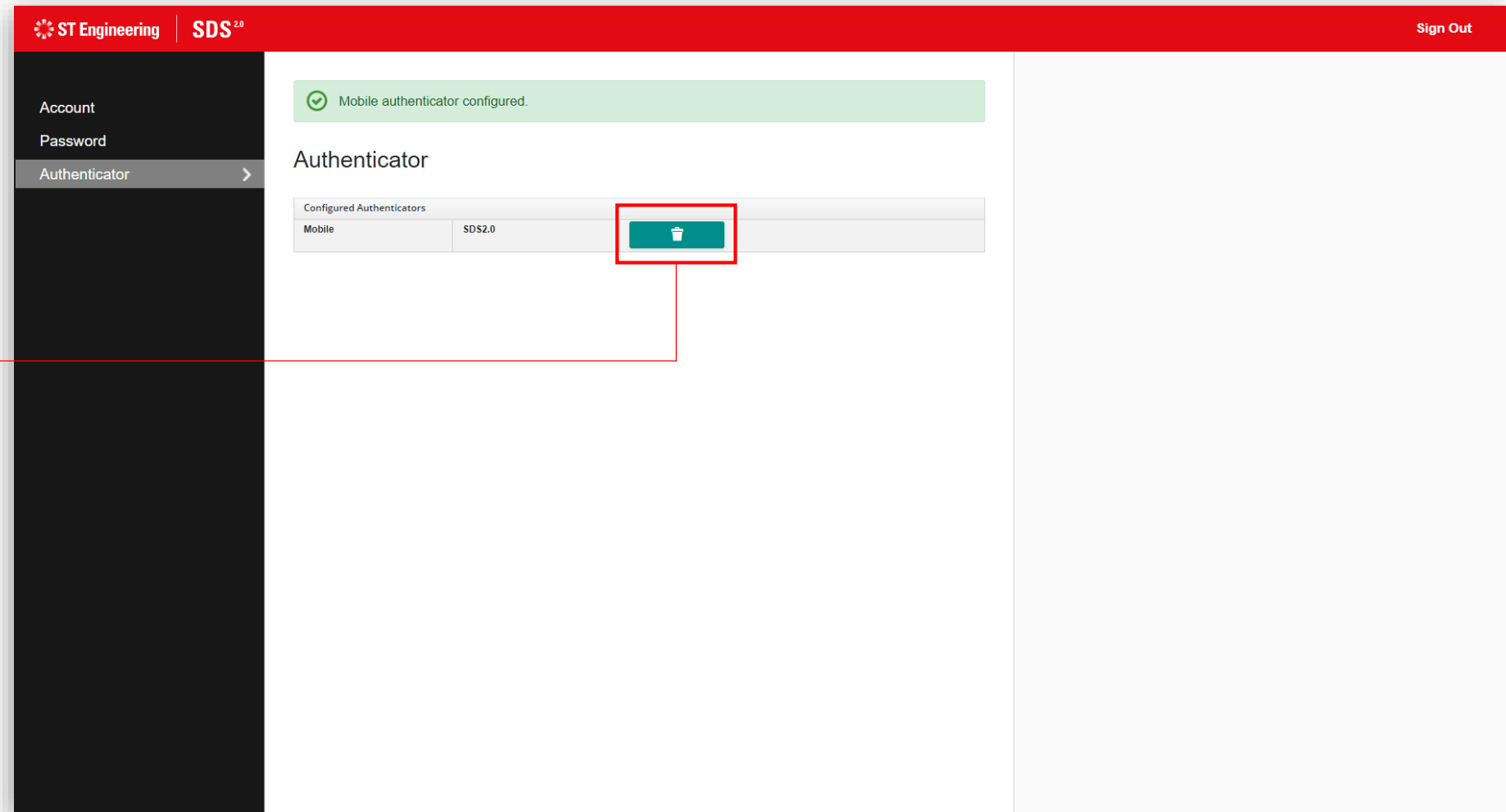


Change OTP Token

Select the delete button to remove your old device.

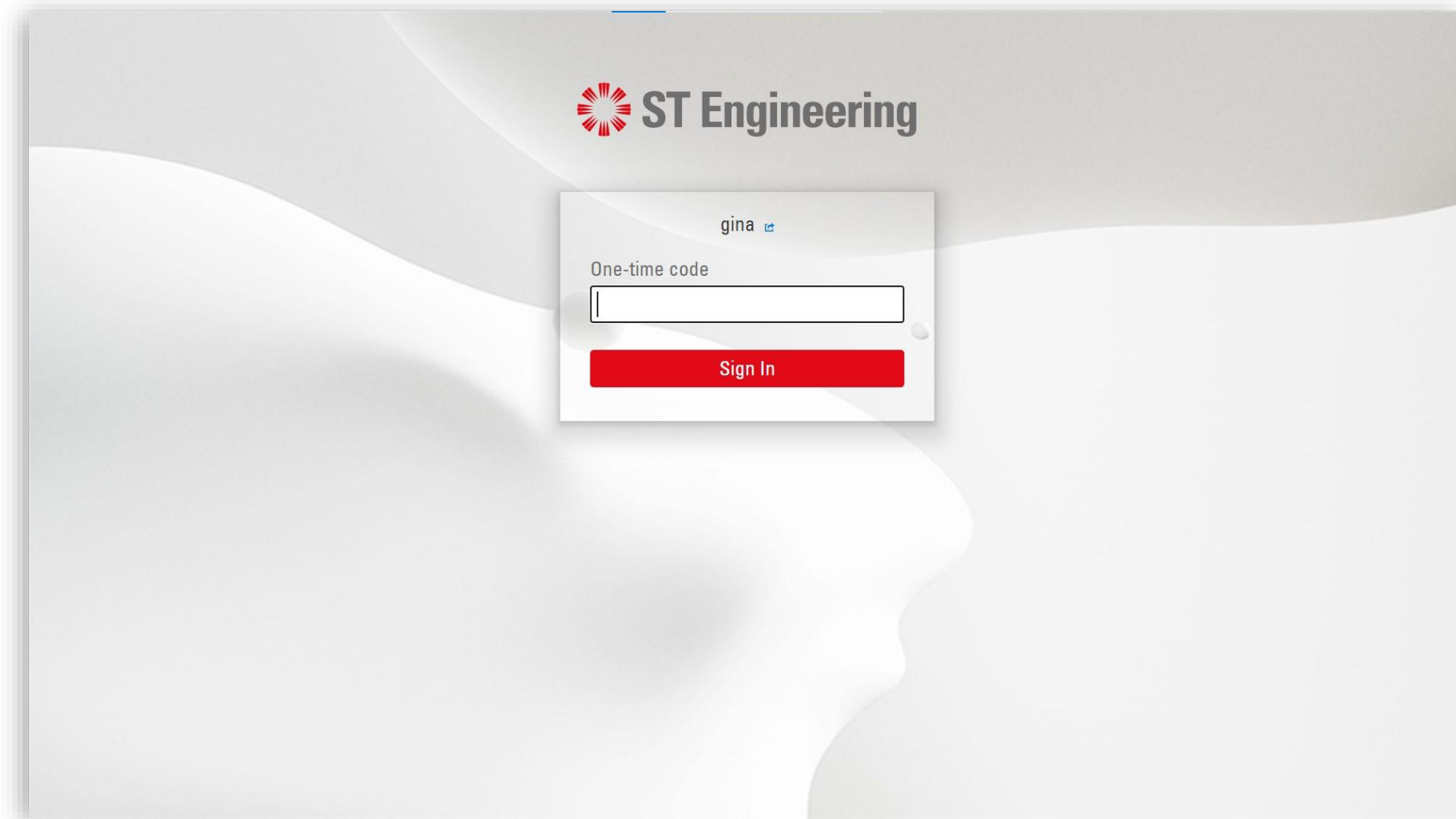


Once removed, you can setup a new OTP token ([Refer to slide 14-21](#)).



Forget or Lost Physical OTP Device

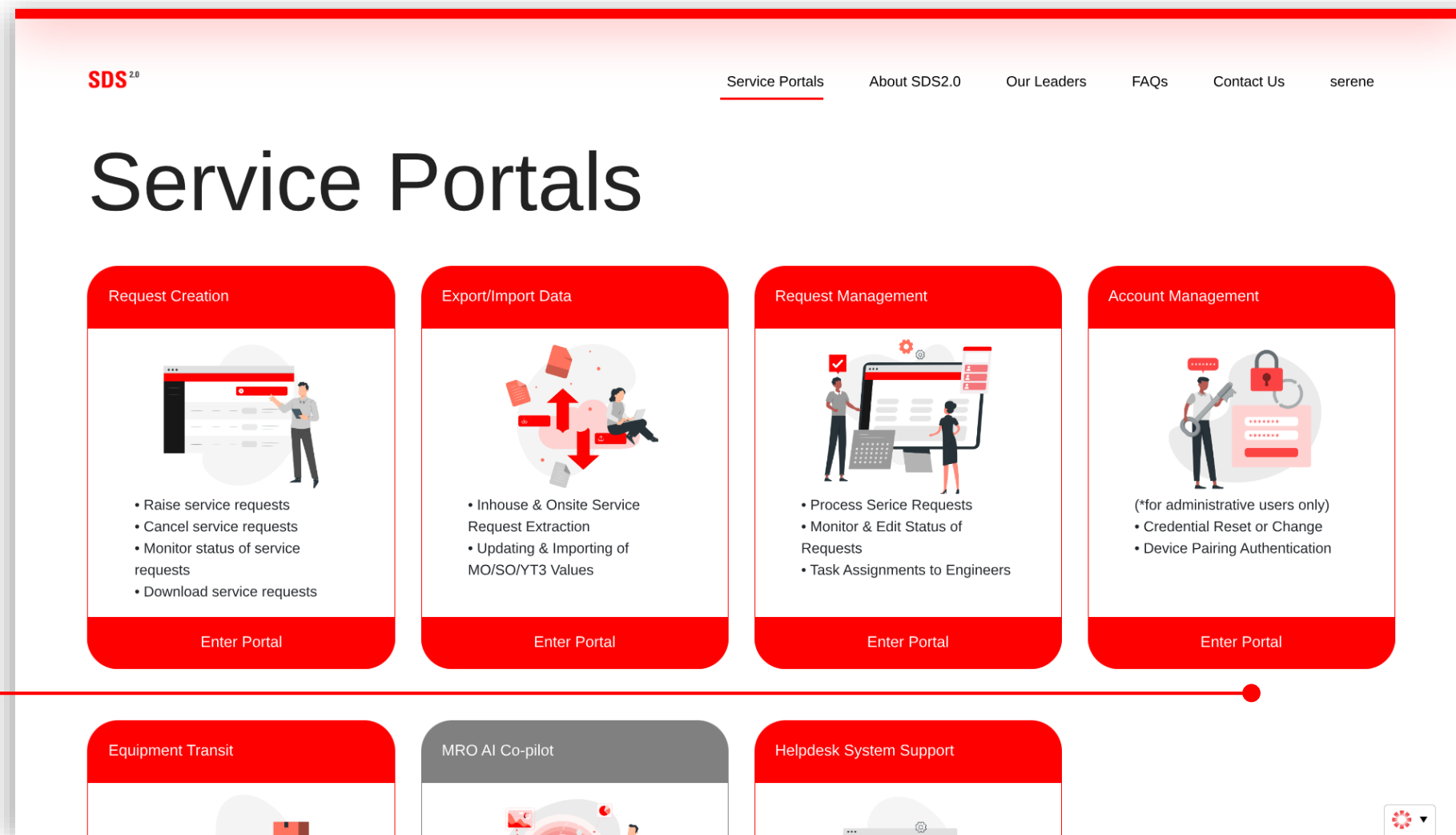
If you have forgotten to bring your physical OTP device, or lost it (E.g., smartphone), **you will need to request help internally (CX Hub) to reset your OTP token setup.**



Account Management

If your account has been setup, your subsequent logins will direct you to SDS2.0 landing page.

Select **Enter Portal** under **Account Management** section.



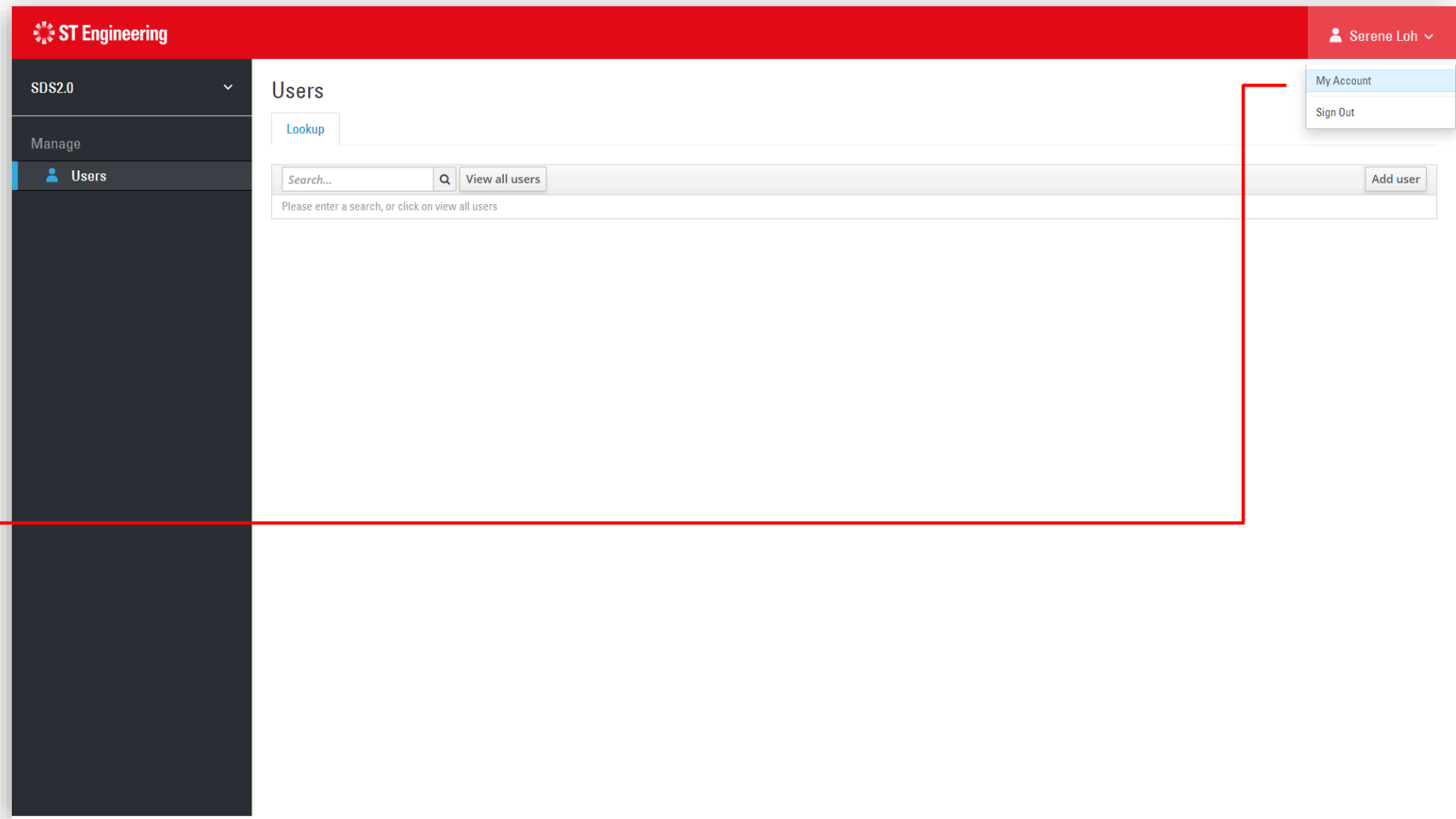
The screenshot shows the SDS 2.0 Service Portals landing page. At the top, there is a navigation bar with the following links: Service Portals (underlined), About SDS2.0, Our Leaders, FAQs, Contact Us, and serene. The main heading is "Service Portals". Below this, there are four main service categories, each with an illustration and a list of features:

- Request Creation**:
 - Raise service requests
 - Cancel service requests
 - Monitor status of service requests
 - Download service requests
- Export/Import Data**:
 - Inhouse & Onsite Service Request Extraction
 - Updating & Importing of MO/SO/YT3 Values
- Request Management**:
 - Process Service Requests
 - Monitor & Edit Status of Requests
 - Task Assignments to Engineers
- Account Management** (*for administrative users only):
 - Credential Reset or Change
 - Device Pairing Authentication

Each category has an "Enter Portal" button at the bottom. Below these are three more categories: Equipment Transit, MRO AI Co-pilot, and Helpdesk System Support.

Update My Account

To update your account information, tap on your name (i.e., Serene Loh) and select **[My Account]**.

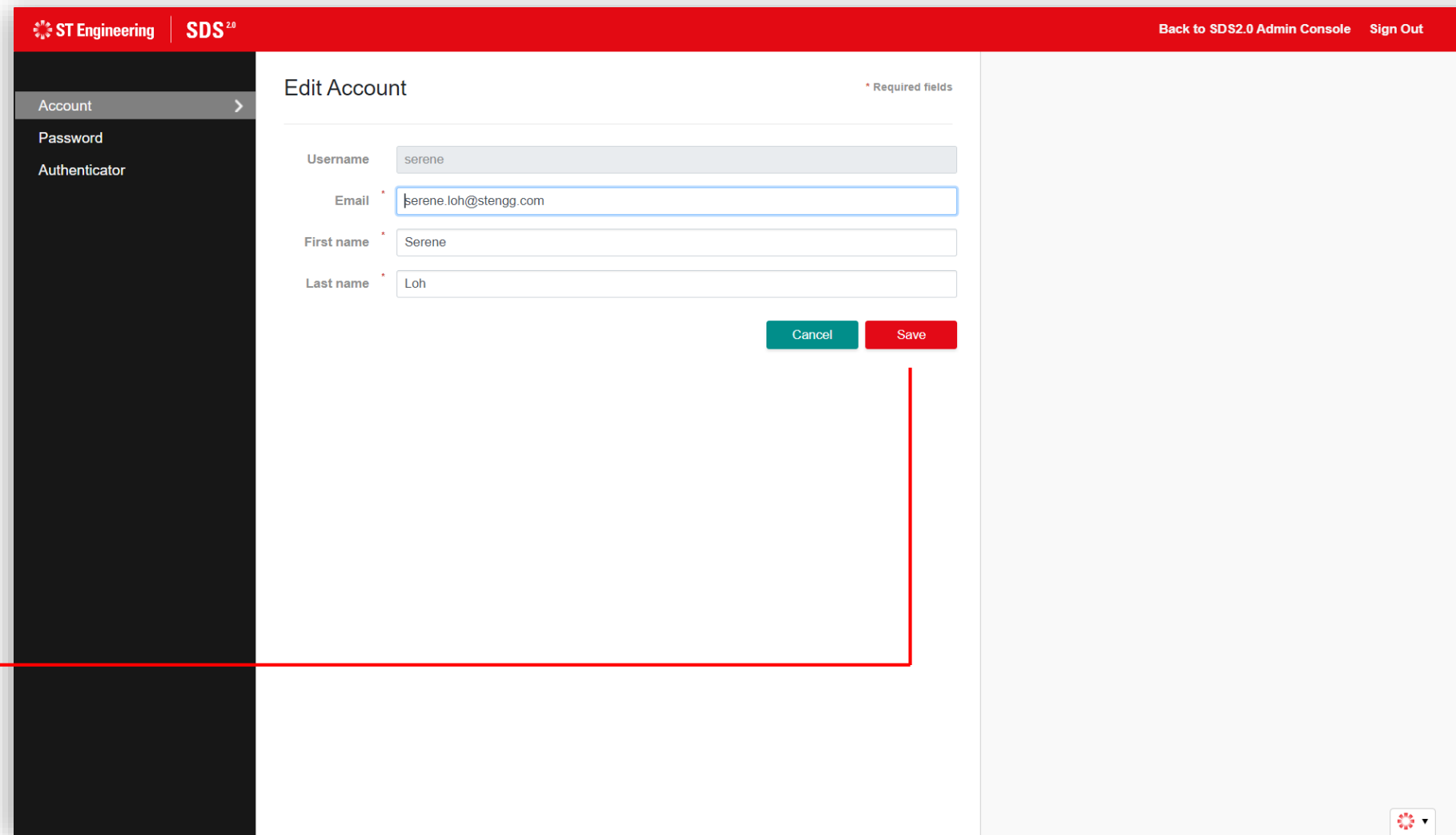


Update Account Information (1)

On the Account page,
update your details:

- Email
- First Name
- Last Name

Tap **[Save]** to update
your details.

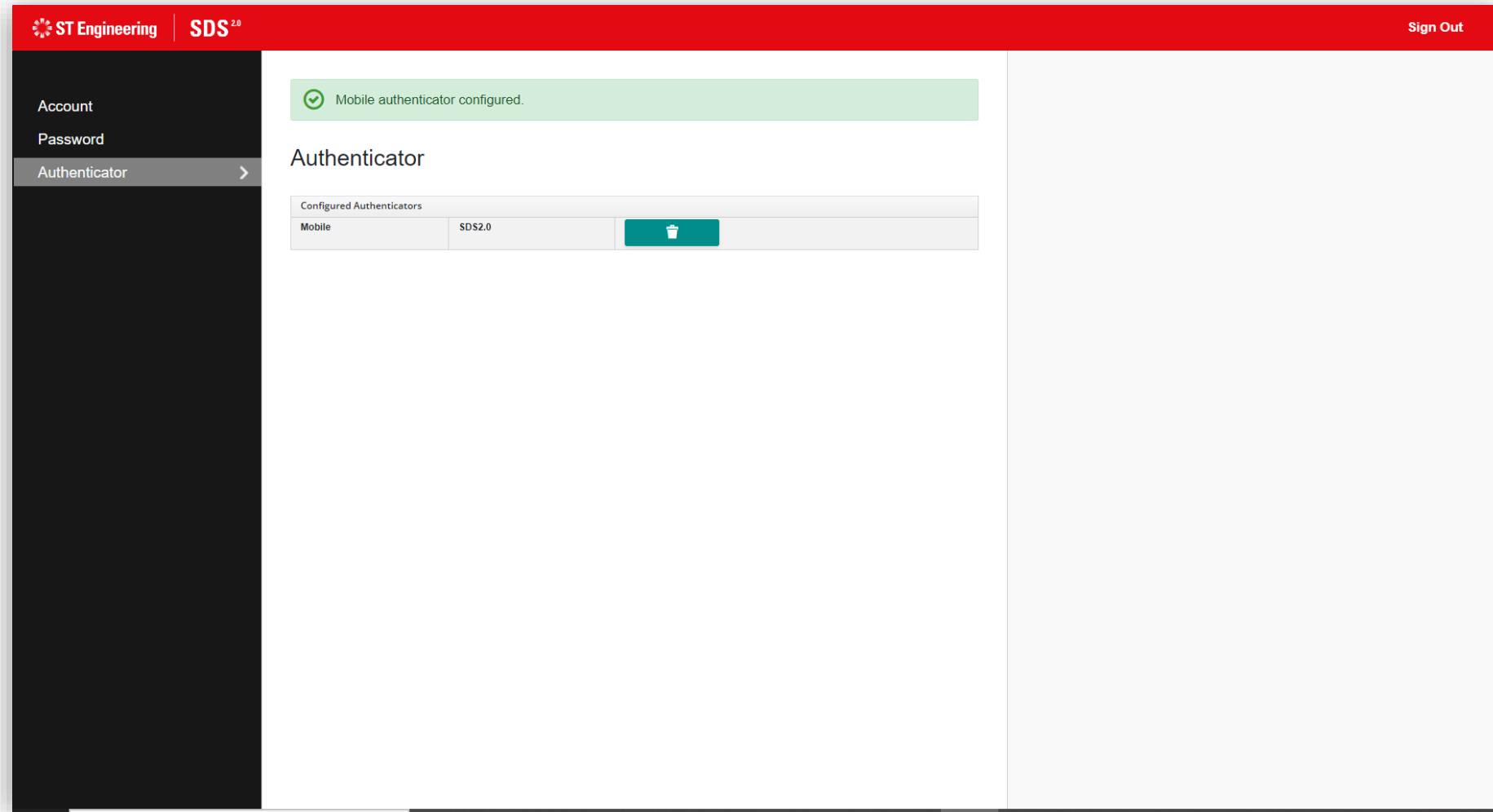


The screenshot shows the 'Edit Account' page in the SDS 2.0 Admin Console. The page has a red header with the ST Engineering logo and 'SDS 2.0' on the left, and 'Back to SDS2.0 Admin Console' and 'Sign Out' on the right. A dark sidebar on the left contains a menu with 'Account', 'Password', and 'Authenticator'. The main content area is titled 'Edit Account' and contains a form with the following fields: 'Username' (value: serene), 'Email' (value: serene.loh@stengg.com), 'First name' (value: Serene), and 'Last name' (value: Loh). There are asterisks next to the Email, First name, and Last name fields, indicating they are required. At the bottom right of the form are two buttons: 'Cancel' (teal) and 'Save' (red). A red line is drawn from the 'Save' button to the text 'Tap [Save] to update your details.' in the text block to the left.

Update Account Information (2)

[Back to SDS2.0 Admin Console](#) [Sign Out](#)

Your account will be updated successfully when all the fields are input correctly.




ST Engineering | SDS^{2.0} [Sign Out](#)

Account
Password
Authenticator >

Mobile authenticator configured.

Authenticator

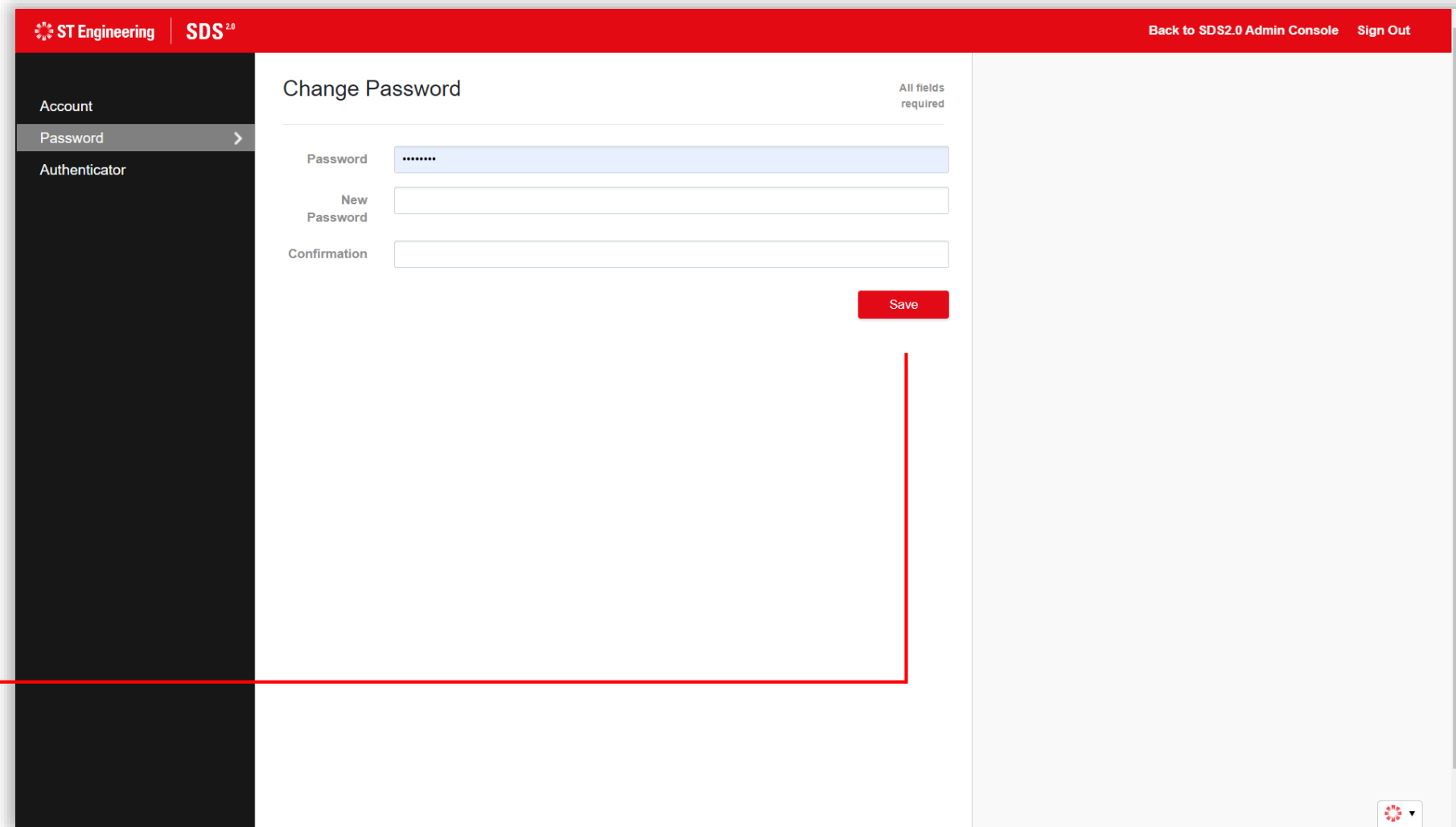
Configured Authenticators		
Mobile	SDS2.0	

Change Password

On the Password Page, change your password with the following input:

- (Current) Password
- New Password
- Confirmation (on New Password)

Tap **[Save]** to update password.



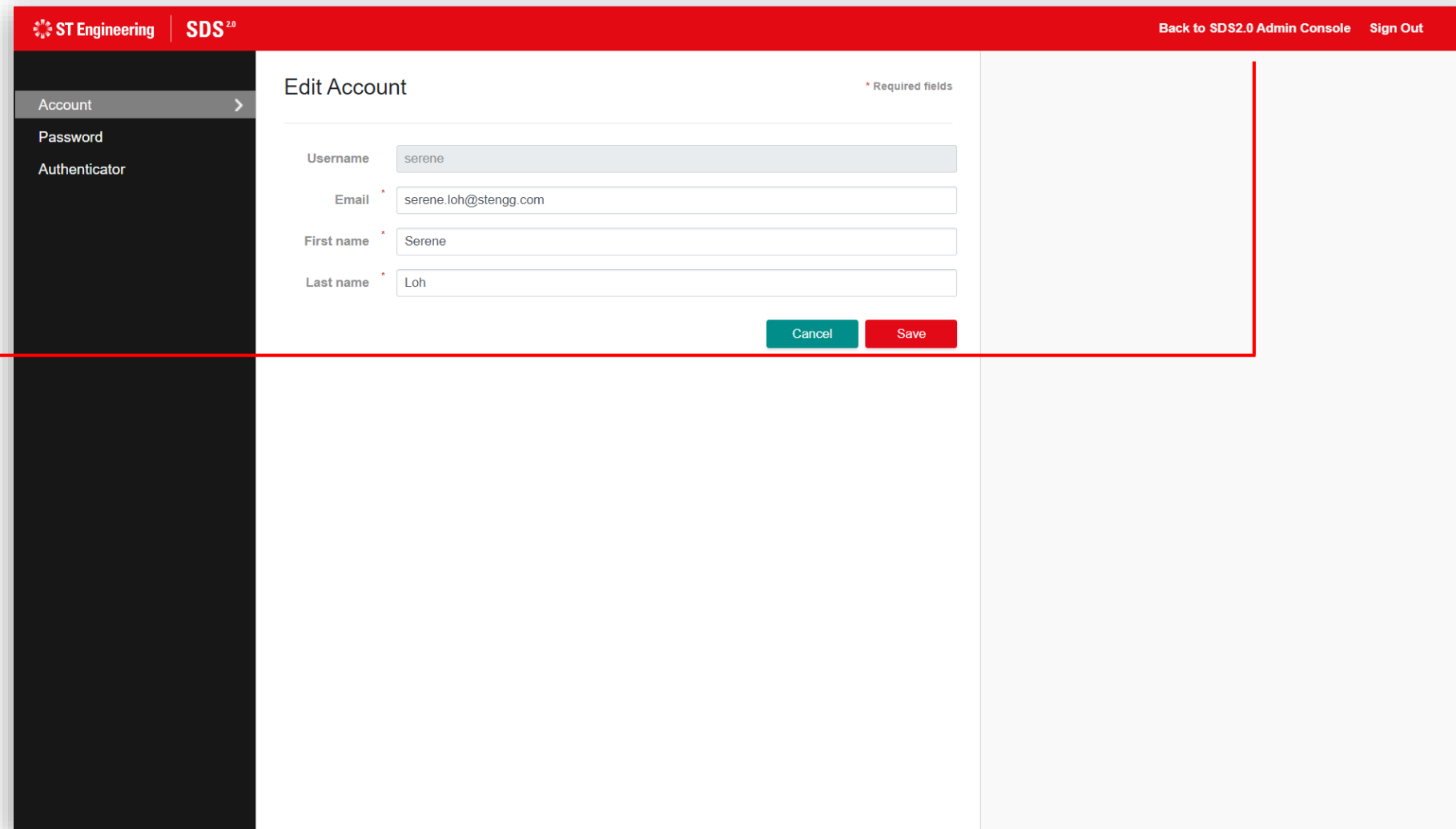
Forget Password

If you have forgotten your password, you **will need to request help internally (CX Hub) to reset your password.**



Admin Console Page

To view or go back to Admin Console page, tap on **[Back to SDS2.0 Admin Console]** at the top-right corner of the navigation bar.

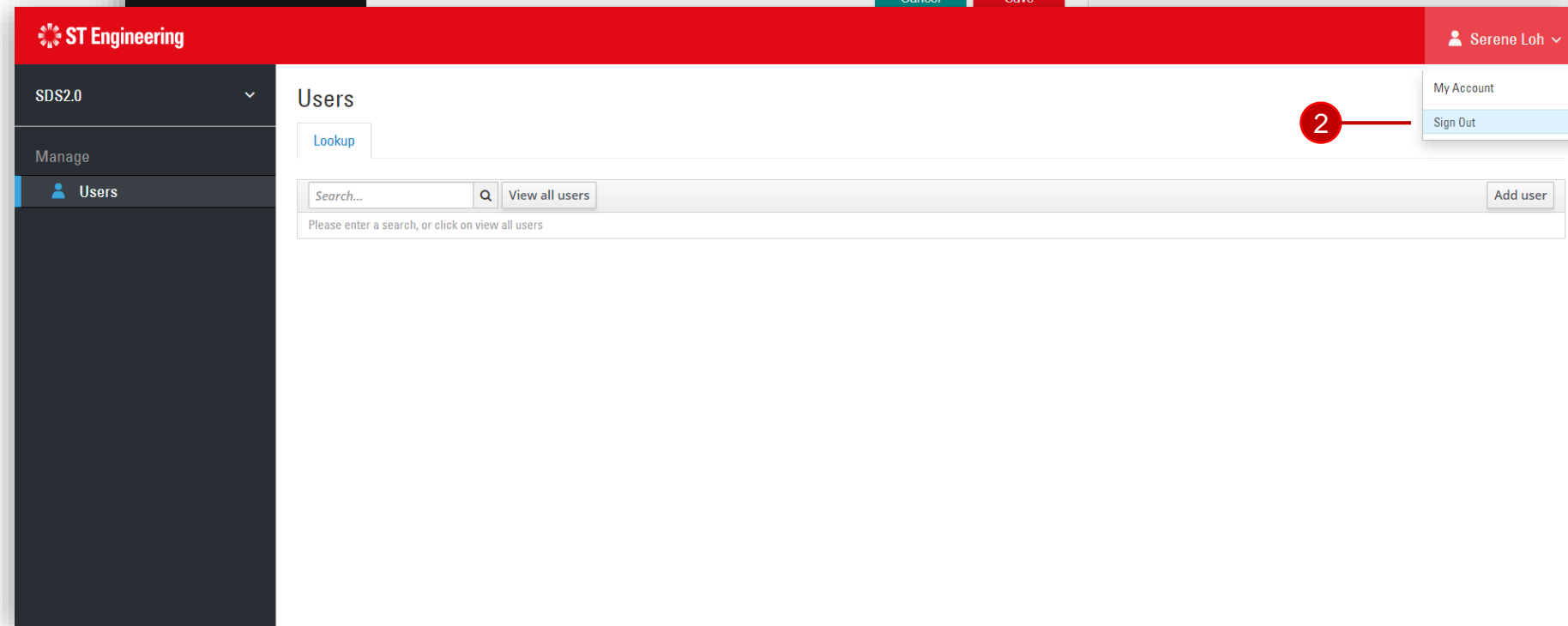
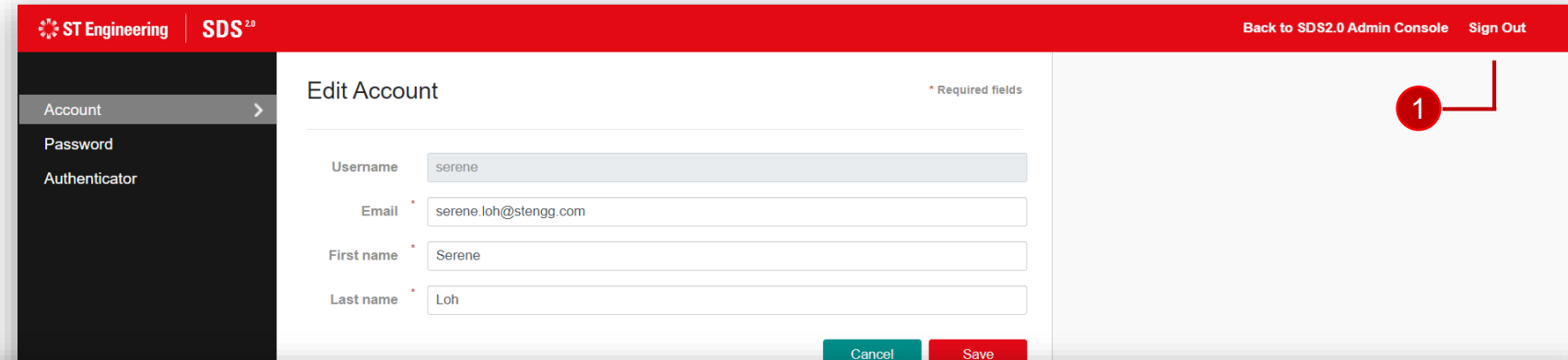


Sign Out of Admin Console

To sign out of your admin account, tap

- 1 **[Sign Out]** if you are at your account page or
- 2 **[Your Name] > [Sign Out]** if you are at admin console page.

It should redirect you back to the login page ([Refer to slide 11](#)).



User Account Management

- User Accounts
- Account Creation
- Update/Edit Account Details
- Reset Password
- Reset OTP Token
- View OTP Algorithm
- Sessions
- Delete User

User Accounts

The administrator can view a list of users from Users menu.

- 1 Quick search function
- 2 Reloads data displayed on the list of users
- 3 Adds a new user
- 4 Edit user information

ST Engineering | SDS 2.0 | Serene Loh

Users

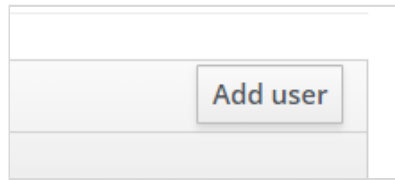
Lookup

Search...

ID	Username	Email	Last Name	First Name	Actions
5c56efc2-cac5-48a2-a826-62...	10000154	tanoh@stengg.com	Tan	Oon Hock	Edit
07962f17-d392-4b4c-910c-65...	10000218		Chong	Lea Ping	Edit
560038f0-54cf-4320-9c61-26...	10000643		Yeo	King Yong	Edit
7aec5745-99f7-4d58-9f7d-33...	10000946		Bok	Wing Chun	Edit
ac252128-a979-4e43-94d2-a...	10001278	tohmy@stengg.com	Toh	Meng Yak Michael	Edit
fb08a21e-bc66-48c3-afc8-94a...	10001423		Driver	Milkrun	Edit
d128d384-8ec4-4128-b3c0-8f...	10001690	soonck@stengg.com	Soon	Chih Kuang	Edit
99cc432d-fdb4-4249-888c-90...	10001730	yapwl@stengg.com	Yap	Willie	Edit
45407de9-9cfe-4d02-9707-1d...	10001993	ericheng@stengg.com	Heng	Cheok Hou Eric	Edit
d9e05164-ce2d-412c-8b4c-65...	10002179	axeltan@defence.stengg.com	Tan	Axel, Hal Lieh	Edit
d94c0586-3f16-4214-a1e9-37...	10002267	lowlk@defence.stengg.com	Low	Lit Keong	Edit
51209a4c-368f-4e33-b702-39...	10002393	leetecksing@defence.stengg...	Lee	Teck Sing	Edit
de3f4e87-c1fc-42d1-b528-be...	10002723	phang.kaibin.kevin@stengg.c...	Phang	Kevin	Edit
7d0552f4-24fc-489b-bbc0-00...	10002771	poh.hweetong@stengg.com	Poh	Hwee Tong	Edit
0eb7a1e7-c828-44bb-b2d1-7...	10003063	vijay.letchumi@stengg.com	D/o Sivanantham	Vijay Letchumi	Edit
49bee619-db29-44f7-b558-91...	10003277	mohamad.zulkiflee@stengg.c...	Bin Mohd Ali	Mohamad Zulkiflee	Edit
79102ee0-ee4e-4737-b507-4...	10003332	quah.yishen@stengg.com	Quah	Yishen	Edit
f7b15fae-9b26-4074-8b1f-c6c...	10003374		Lim	Joel	Edit
2063bd9f-349d-43e0-9c30-8b...	10003497	tang.huizhong@defence.sten...	Tang	Hui Zhong	Edit
8e470a76-abf0-48ec-b67f-53...	10095721	jonathan.js@stengg.com	S/O Joseph Simon	Jonathan	Edit

First Page Previous Page Next Page

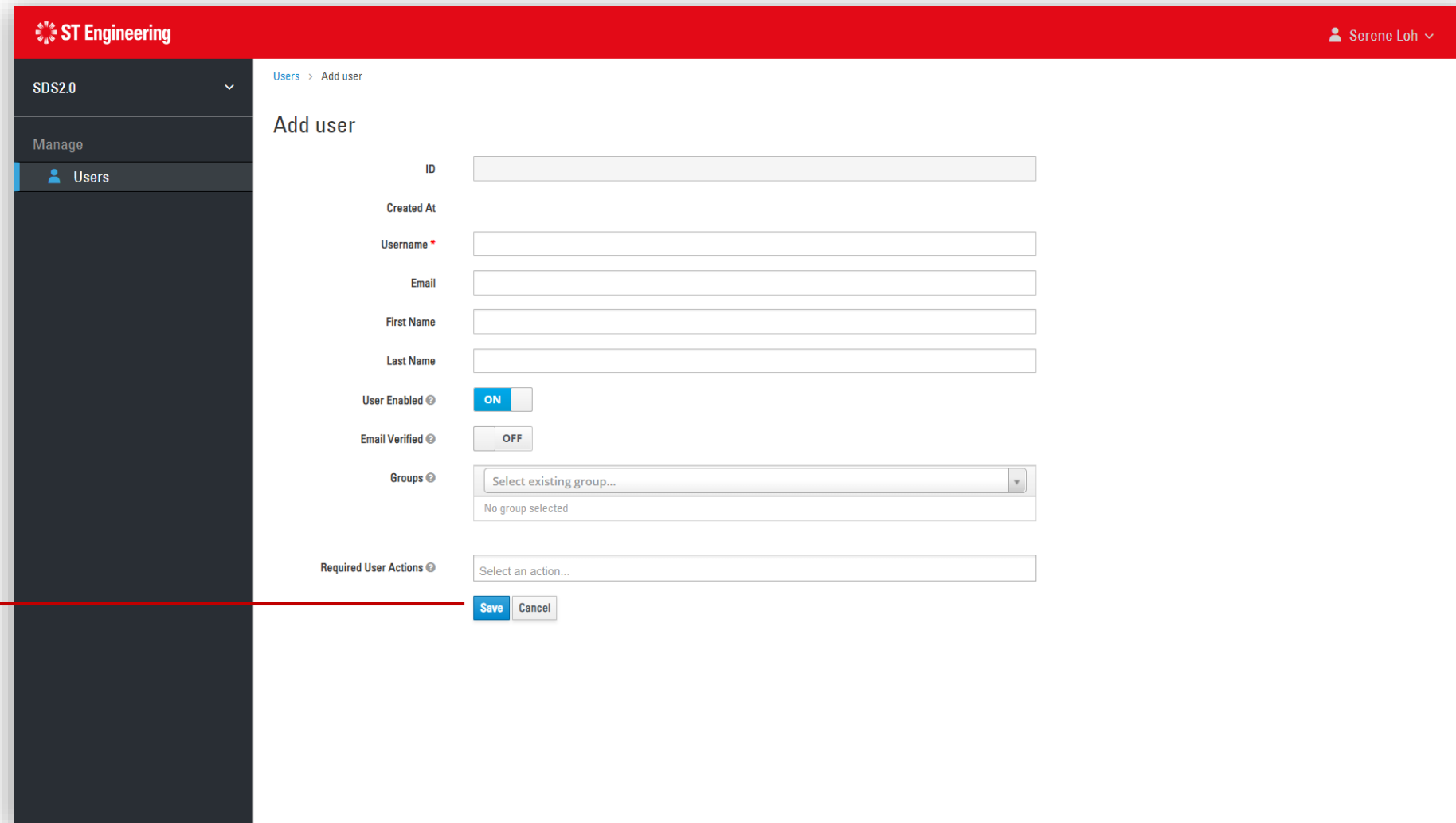
Account Creation



From Users page, tap **[Add user]** button to create a new user.

Input the user information in the given text fields and tap **[Save]** to create.

Note: Username is a mandatory field



The screenshot shows the 'Add user' form in the ST Engineering application. The form is titled 'Add user' and is located in the 'Users' section of the 'Manage' page. The form includes the following fields and controls:

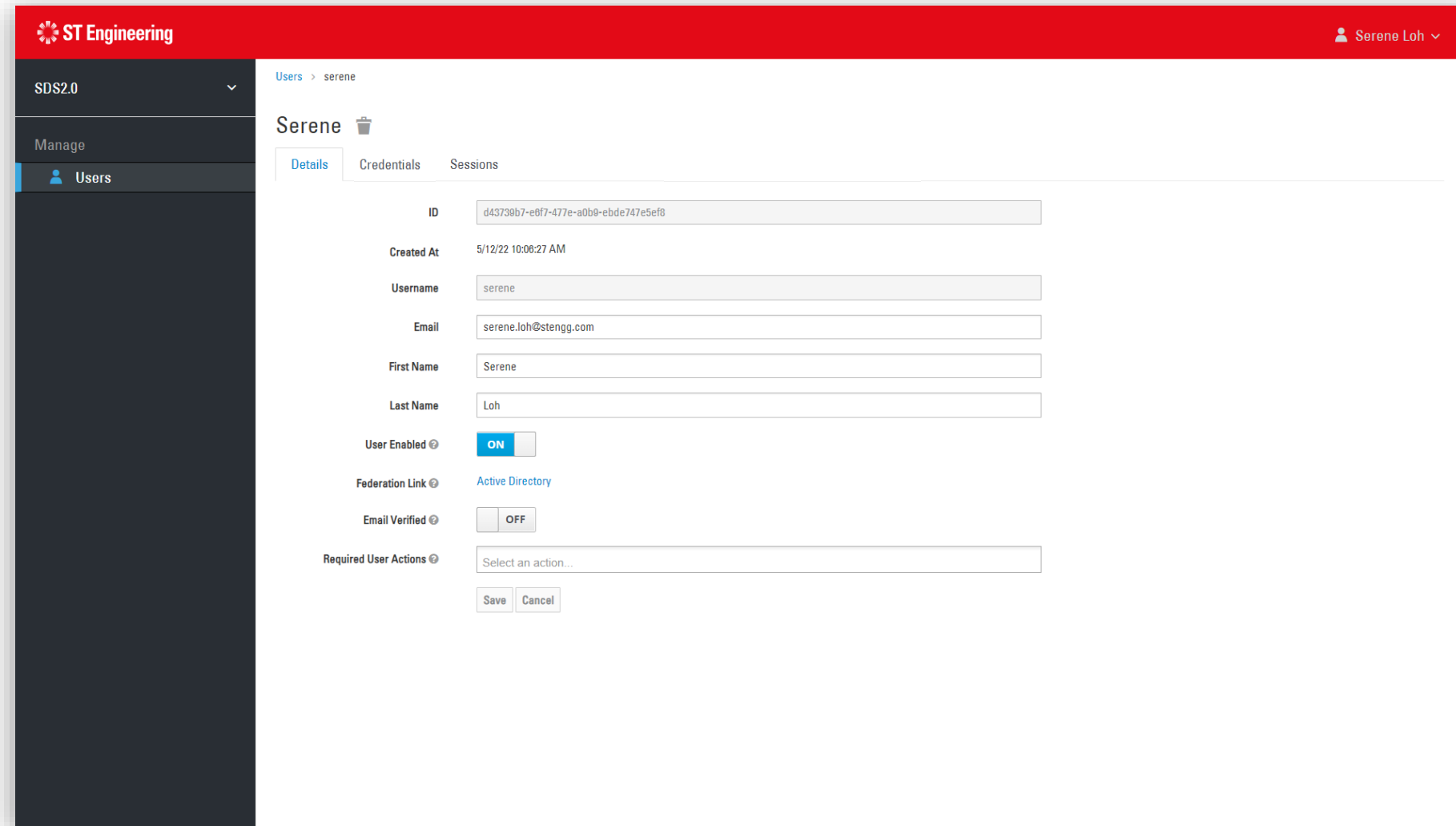
- ID:** A text input field.
- Created At:** A text input field.
- Username:** A text input field with a red asterisk indicating it is mandatory.
- Email:** A text input field.
- First Name:** A text input field.
- Last Name:** A text input field.
- User Enabled:** A toggle switch currently set to 'ON'.
- Email Verified:** A toggle switch currently set to 'OFF'.
- Groups:** A dropdown menu with the text 'Select existing group...' and 'No group selected' below it.
- Required User Actions:** A dropdown menu with the text 'Select an action...'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

Update/Edit Account Details

Once saved, it will auto-generate a User ID and a user page in Details Tab.

Admin can modify and update the changes here.

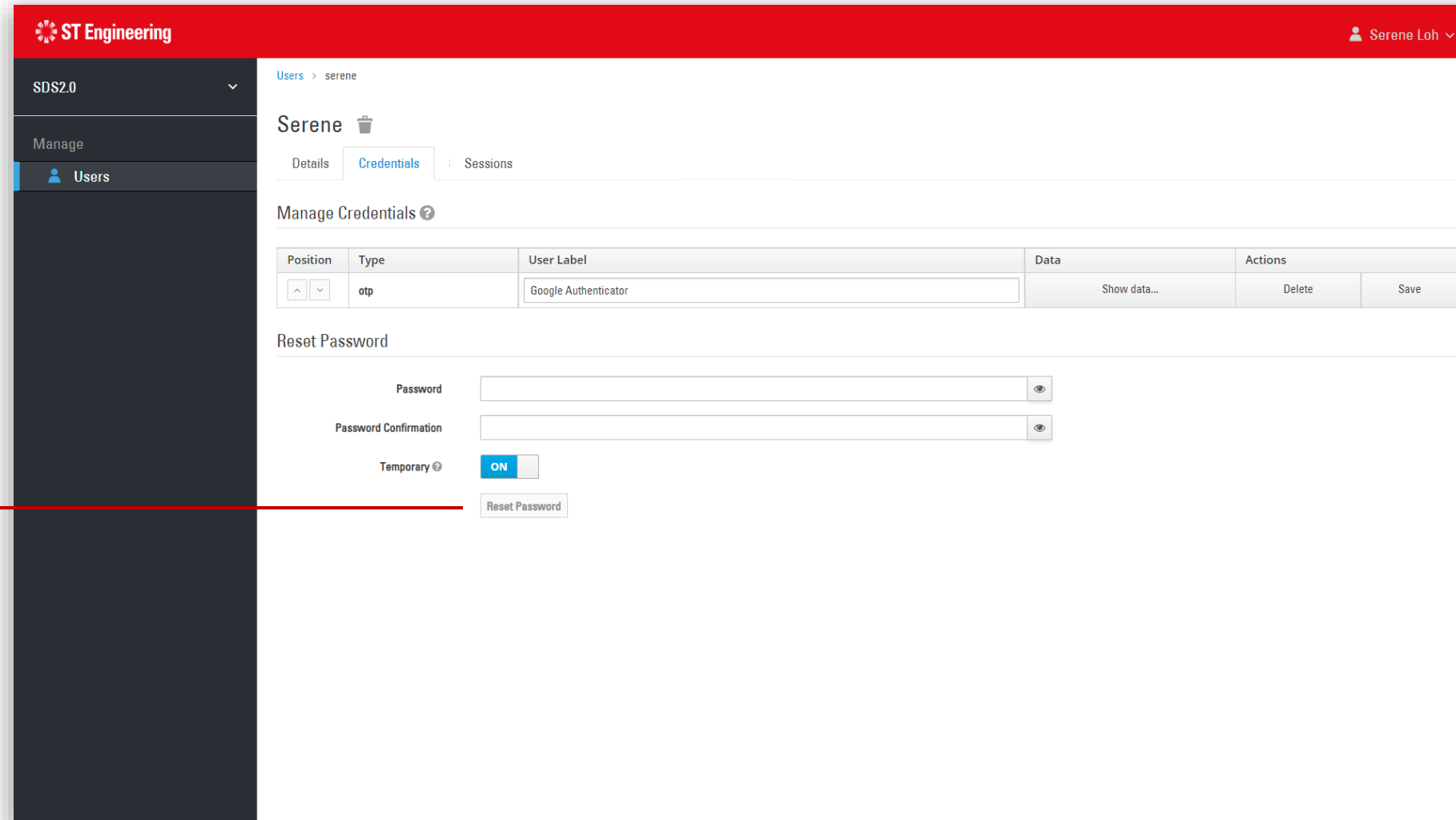
OR from Users page, tap **[Edit]** to edit the user.



Reset Password

Administrator can reset user's password under Credential Tab.

Enter a default password and re-enter password to confirm, then tap **[Reset Password]**.



The screenshot shows the ST Engineering user management interface. The top navigation bar is red with the ST Engineering logo and the user name 'Serene Loh'. The left sidebar shows 'Manage' and 'Users'. The main content area shows the user 'Serene' with tabs for 'Details', 'Credentials', and 'Sessions'. The 'Credentials' tab is active, showing a table with one entry: 'Google Authenticator'. Below the table is the 'Reset Password' form, which includes fields for 'Password', 'Password Confirmation', and a 'Temporary' toggle switch. A red line points from the text 'tap [Reset Password]' to the 'Reset Password' button.

Position	Type	User Label	Data	Actions
	otp	Google Authenticator	Show data...	Delete Save

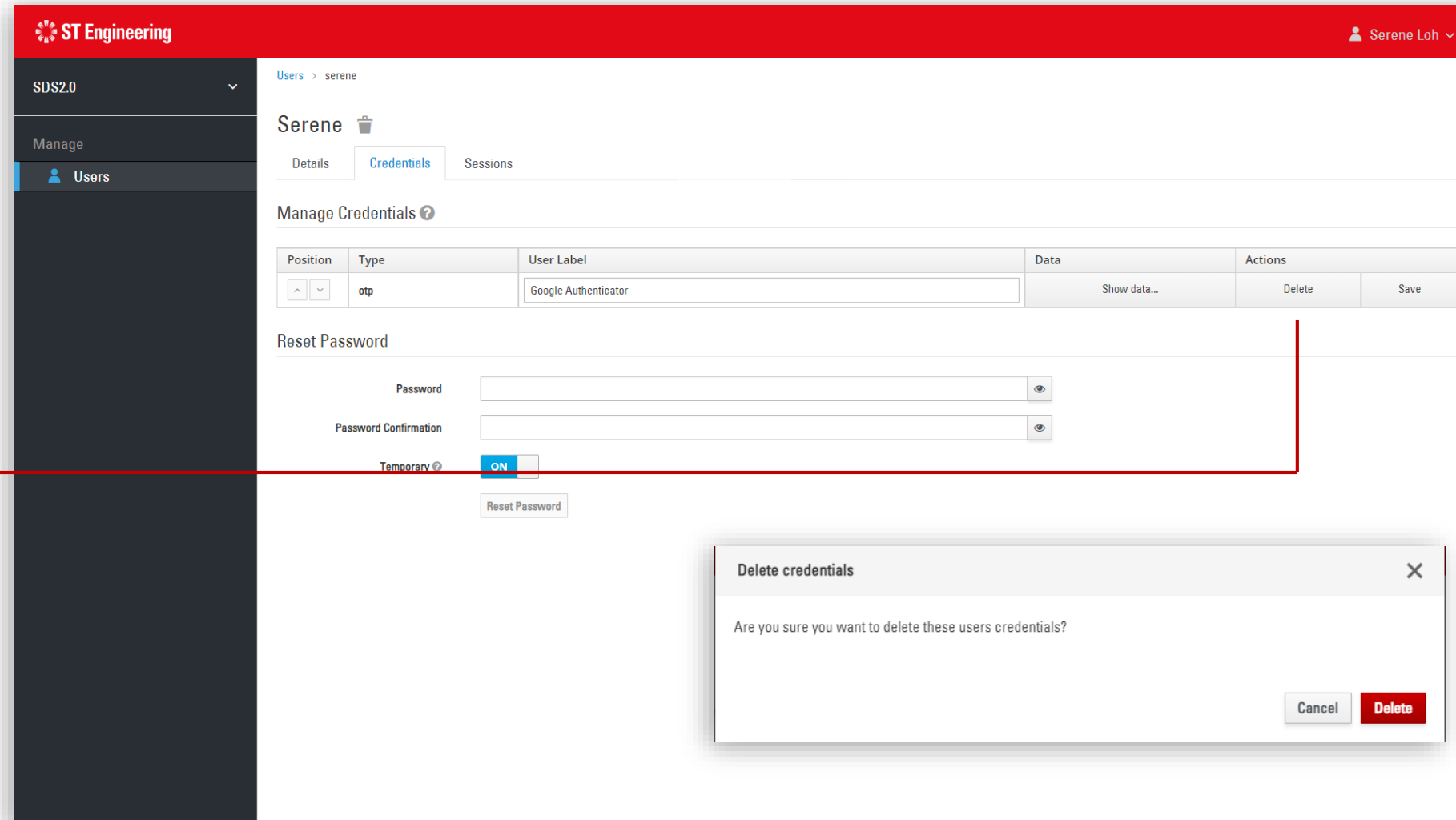
Reset Password

Password
 Password Confirmation
 Temporary ON
 Reset Password

Reset OTP Token

Administrator can reset user's OTP token under Credential Tab.

Under Manage Credentials, tap **[Delete]** and confirm delete to remove the OTP token created by the user.



The screenshot shows the ST Engineering user management interface. The user 'Serene' is selected, and the 'Credentials' tab is active. A table lists the user's credentials:

Position	Type	User Label	Data	Actions
	otp	Google Authenticator	Show data...	Delete Save

Below the table is a 'Reset Password' section with the following fields:

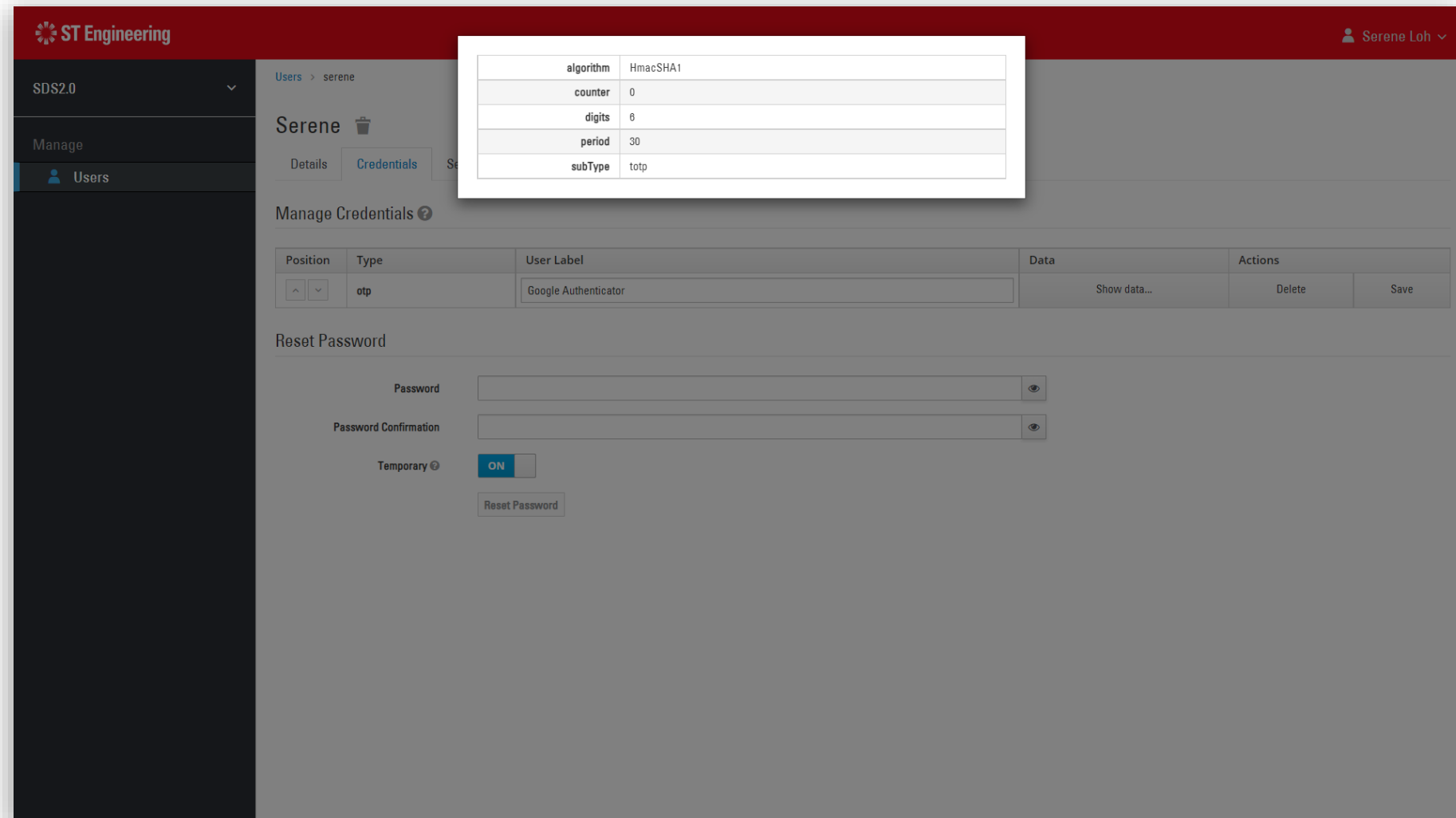
- Password:
- Password Confirmation:
- Temporary:

A red box highlights the 'Delete' button in the table's actions column. A modal dialog titled 'Delete credentials' is shown in the foreground, asking 'Are you sure you want to delete these users credentials?' with 'Cancel' and 'Delete' buttons.

View OTP Algorithm

Admin can check the type of algorithm, subtype, counter, number of digits displayed and reset duration for the user's OTP token. Under Manage Credentials, tap [Show data...].

	Data	A
	Show data...	



The screenshot shows the 'Manage Credentials' interface for user 'Serene'. A modal window displays the following OTP algorithm details:

algorithm	HmacSHA1
counter	0
digits	6
period	30
subType	totp

The background interface includes a table for 'Manage Credentials' with the following data:

Position	Type	User Label	Data	Actions
^ v	otp	Google Authenticator	Show data...	Delete Save

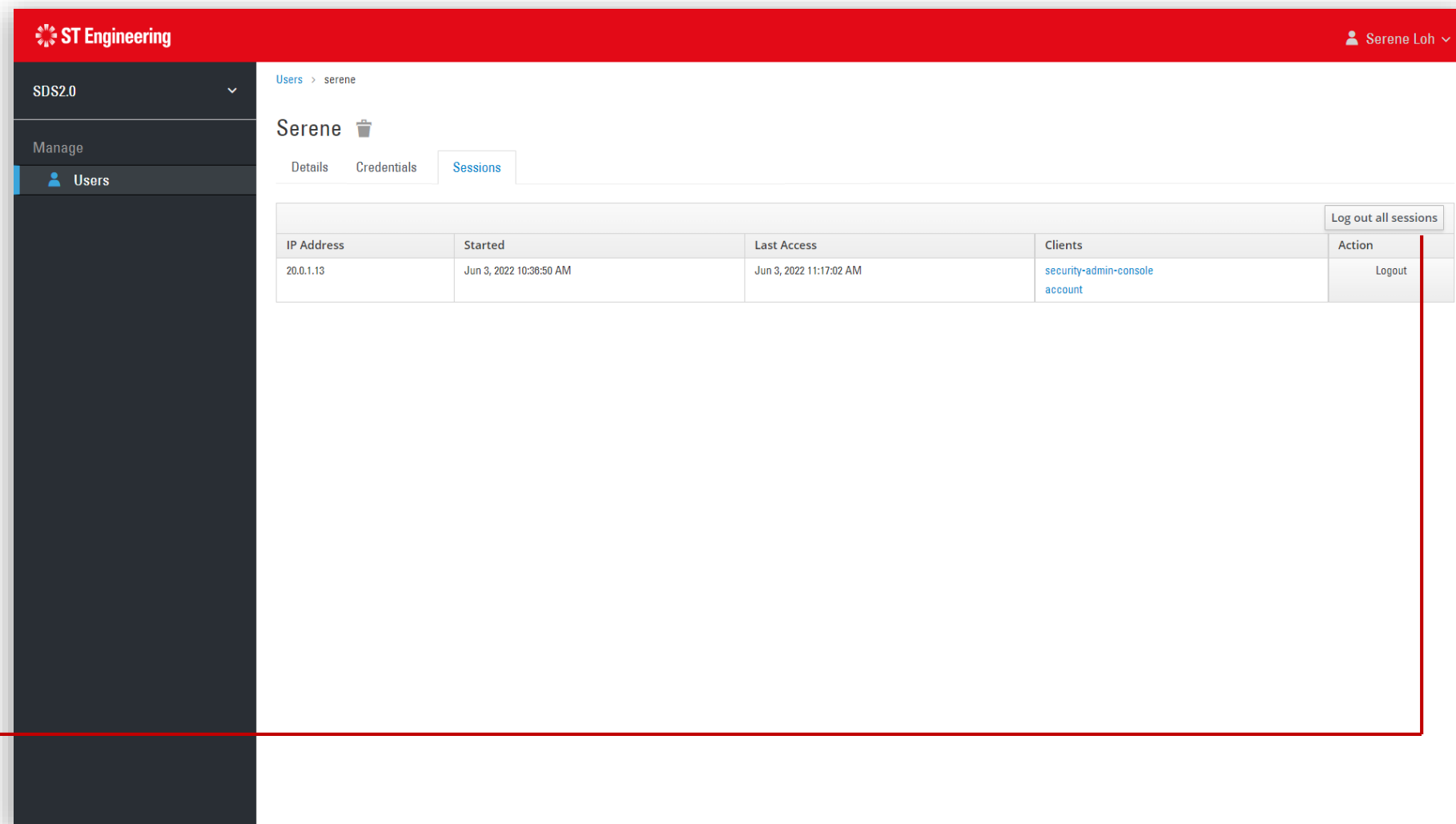
Below the table is a 'Reset Password' section with fields for Password, Password Confirmation, and a Temporary toggle set to ON.

Sessions

User sessions display login activities and web clients of the user.

The sessions will expire and auto-cleared when there is inactivity after some time.

Admin can also end user sessions by selecting **[Log out all sessions]**.



The screenshot shows the ST Engineering user management interface. The user 'Serene' is selected, and the 'Sessions' tab is active. The table below displays the following session data:

IP Address	Started	Last Access	Clients	Action
20.0.1.13	Jun 3, 2022 10:38:50 AM	Jun 3, 2022 11:17:02 AM	security-admin-console account	Logout

A 'Log out all sessions' button is located in the top right corner of the table area.

Delete User

If you want to remove a user from the list permanently, you will need to create a helpdesk request on ITSM at:

<https://itsm.stengg.com>

Users

Lookup

Search...

ID	Username	Email	Last Name	First Name	Actions
5c56efc2-cac5-48a2-a826-62...	10000154	tanoh@stengg.com	Tan	Oon Hock	Edit
07962f17-d392-4b4c-910c-65...	10000218		Chong	Lea Ping	Edit
560038f0-54cf-4320-9c61-26...	10000643		Yeo	King Yong	Edit
7aec5745-99f7-4d58-9f7d-33...	10000946		Bok	Wing Chun	Edit
ac252128-a979-4e43-94d2-a...	10001278	tohmy@stengg.com	Toh	Meng Yak Michael	Edit
fb08a21e-bc66-48c3-afc8-94a...	10001423		Driver	Milkrun	Edit
d128d384-8ec4-4128-b3c0-8f...	10001690	soonck@stengg.com	Soon	Chih Kuang	Edit
99cc432d-fdb4-4249-888c-90...	10001730	yapwl@stengg.com	Yap	Willie	Edit
45407de9-9cfe-4d02-9707-1d...	10001993	ericheng@stengg.com	Heng	Cheok Hou Eric	Edit
d9e05164-ce2d-412c-8b4c-65...	10002179	axeltan@defence.stengg.com	Tan	Axel, Hal Lieh	Edit
d94c0586-3f16-4214-a1e9-37...	10002267	lowlk@defence.stengg.com	Low	Lit Keong	Edit
51209a4c-368f-4e33-b702-39...	10002393	leetecksing@defence.stengg...	Lee	Teck Sing	Edit
de3f4e87-c1fc-42d1-b528-be...	10002723	phang.kaibin.kevin@stengg.c...	Phang	Kevin	Edit
7d0552f4-24fc-489b-bbc0-00...	10002771	poh.hweetong@stengg.com	Poh	Hwee Tong	Edit
0eb7a1e7-c828-44bb-b2d1-7...	10003063	vijay.letchumi@stengg.com	D/o Sivanantham	Vijay Letchumi	Edit
49bee619-db29-44f7-b558-91...	10003277	mohamad.zulkiflee@stengg.c...	Bin Mohd Ali	Mohamad Zulkiflee	Edit
79102ee0-ee4e-4737-b507-4...	10003332	quah.yishen@stengg.com	Quah	Yishen	Edit
f7b15fae-9b26-4074-8b1f-c6c...	10003374		Lim	Joel	Edit
2063bd9f-349d-43e0-9c30-8b...	10003497	tang.huizhong@defence.sten...	Tang	Hui Zhong	Edit
8e470a76-abf0-48ec-b67f-53...	10095721	jonathan.js@stengg.com	S/O Joseph Simon	Jonathan	Edit

First Page Previous Page Next Page



Thank you