SDS
2.0

Smart Digital Systems

User Guide for CX Hub | Account Management

✳ **ST Engineering**

Table of Contents

ST Engineering

FortiClient VPN

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

ST Engineering

ST Engineering

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
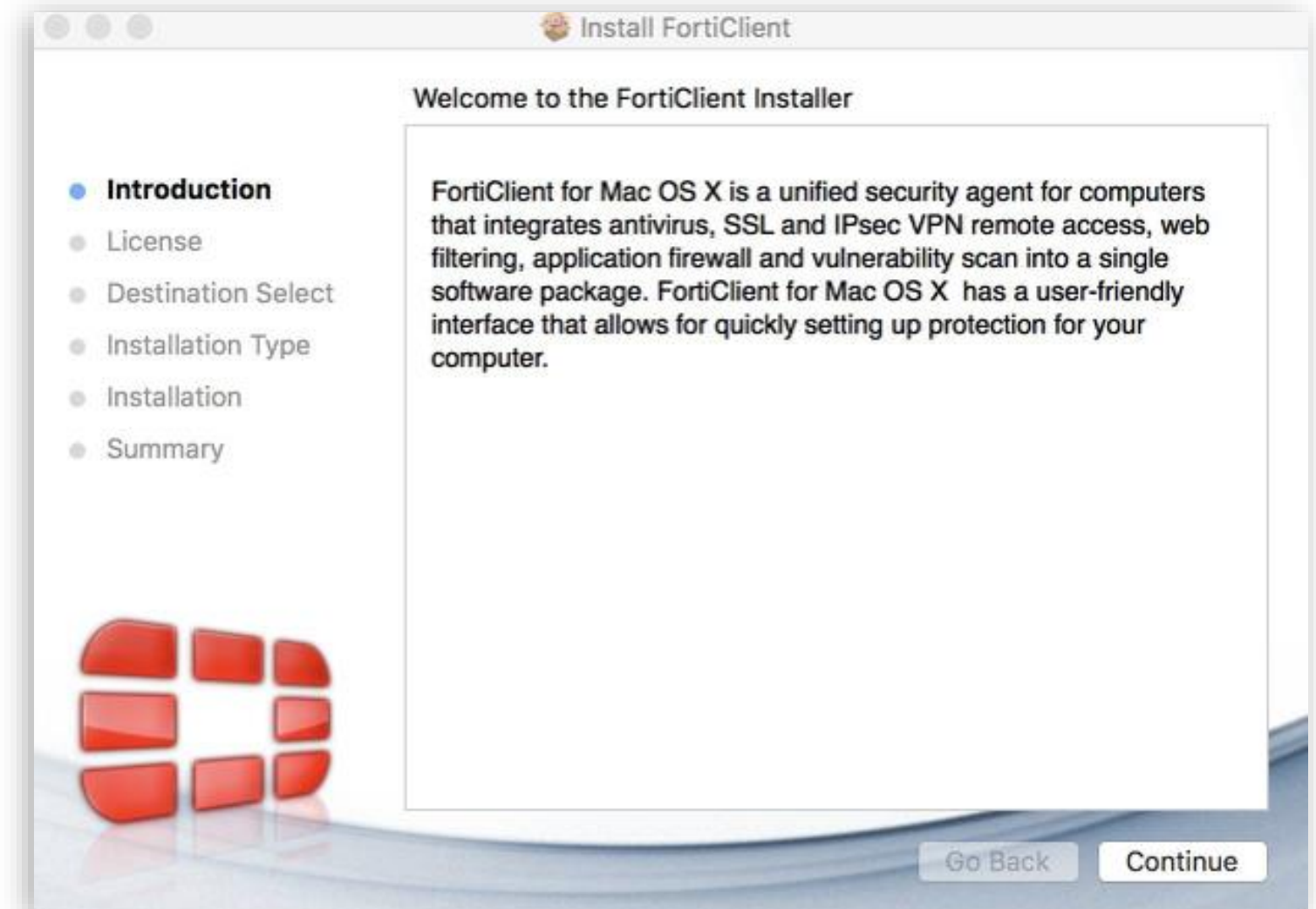
DOWNLOAD

Download VPN for Android

DOWNLOAD

Download VPN for Linux

DOWNLOAD .deb

ST Engineering
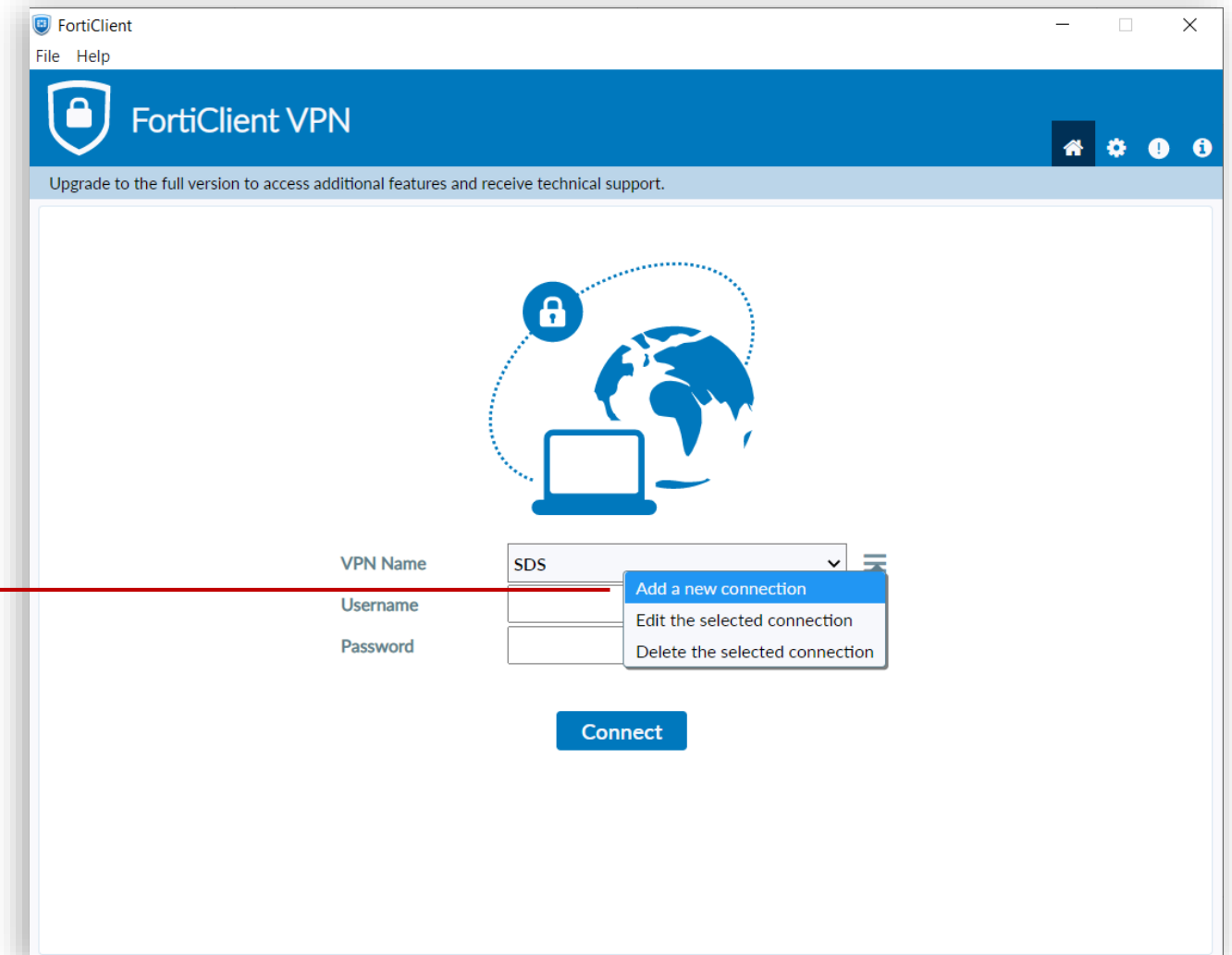
Installation

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

ST Engineering

Creating a new VPN Connection

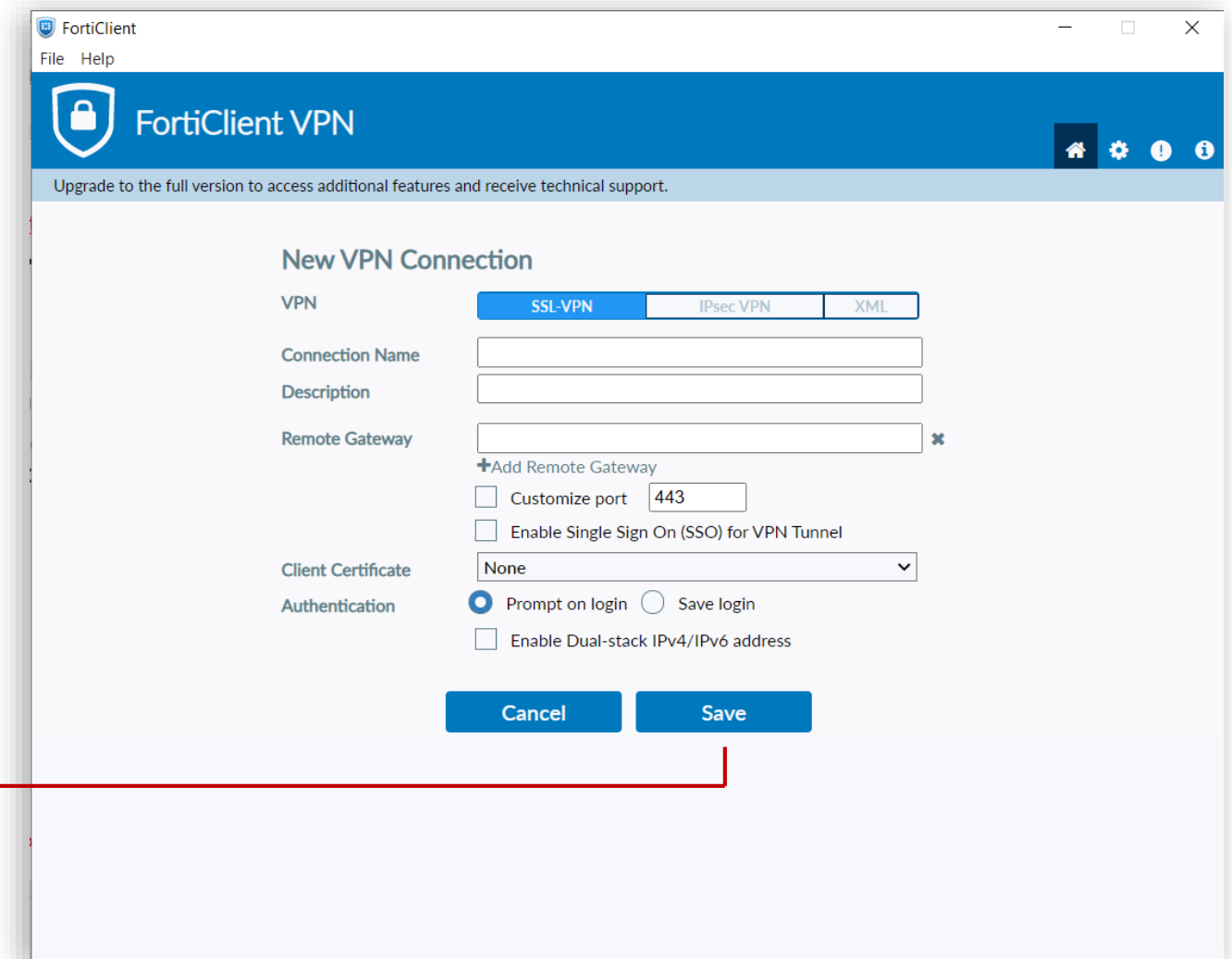Launch the FortiClient VPN software and tap on the menu bar. ☰

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

ST Engineering

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]**.
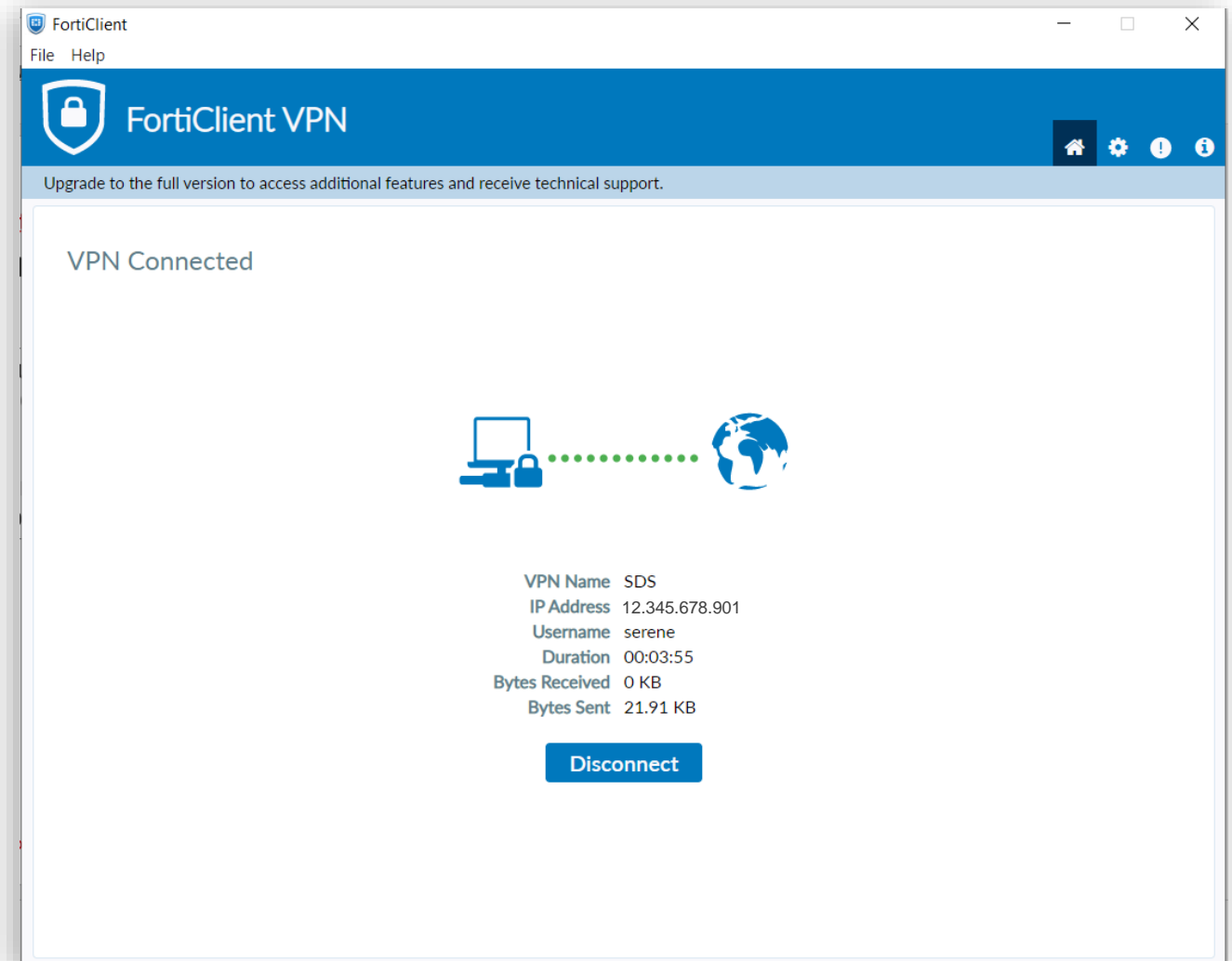
![ST Engineering logo]

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.

ST Engineering
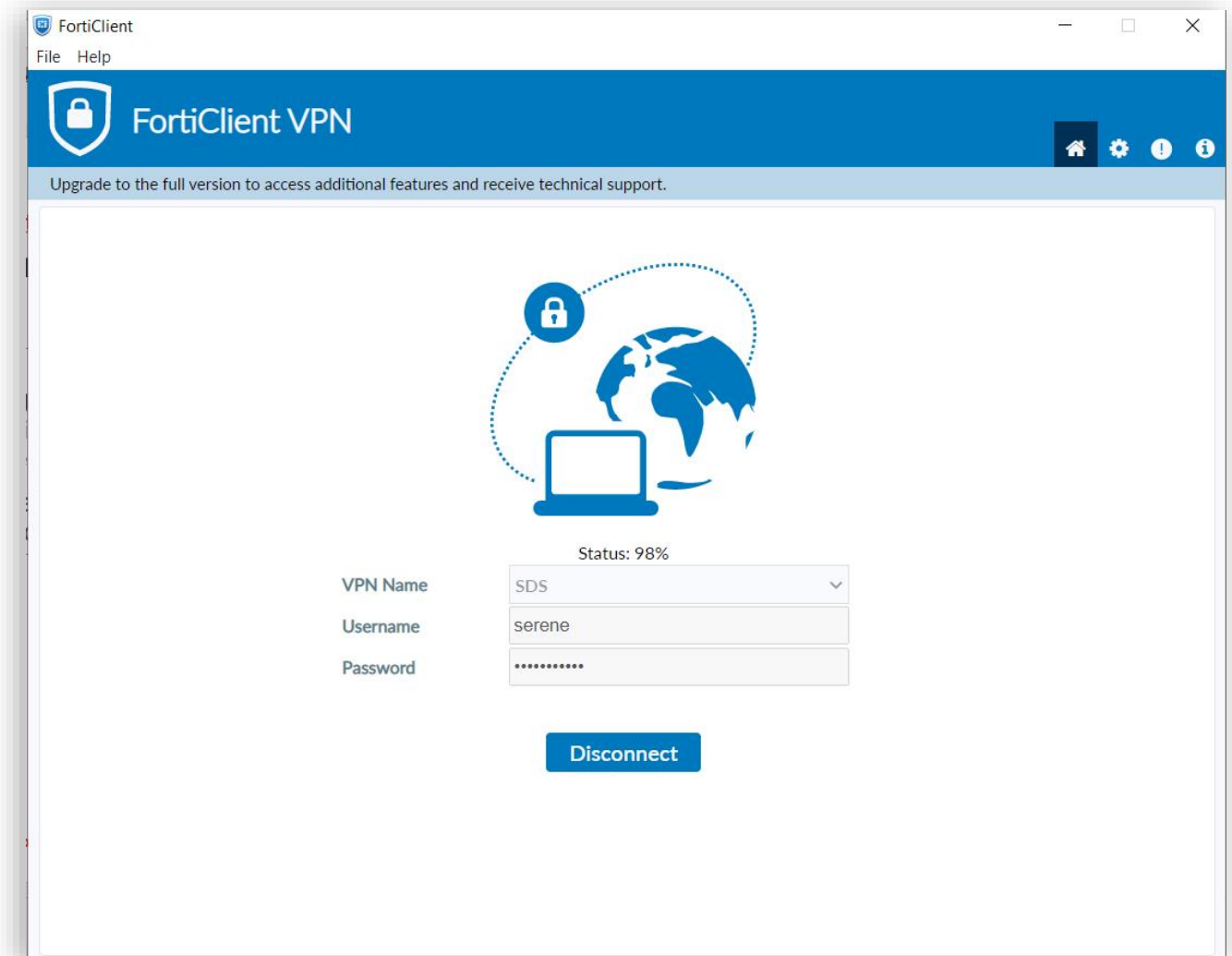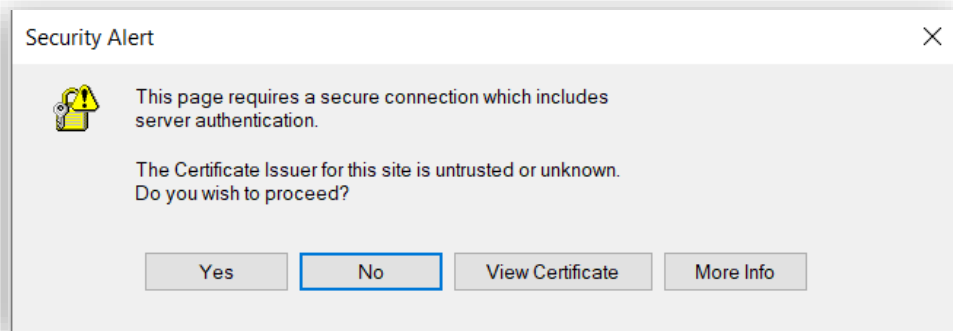
Connecting to FortiClient VPN

It will inform you when the VPN is

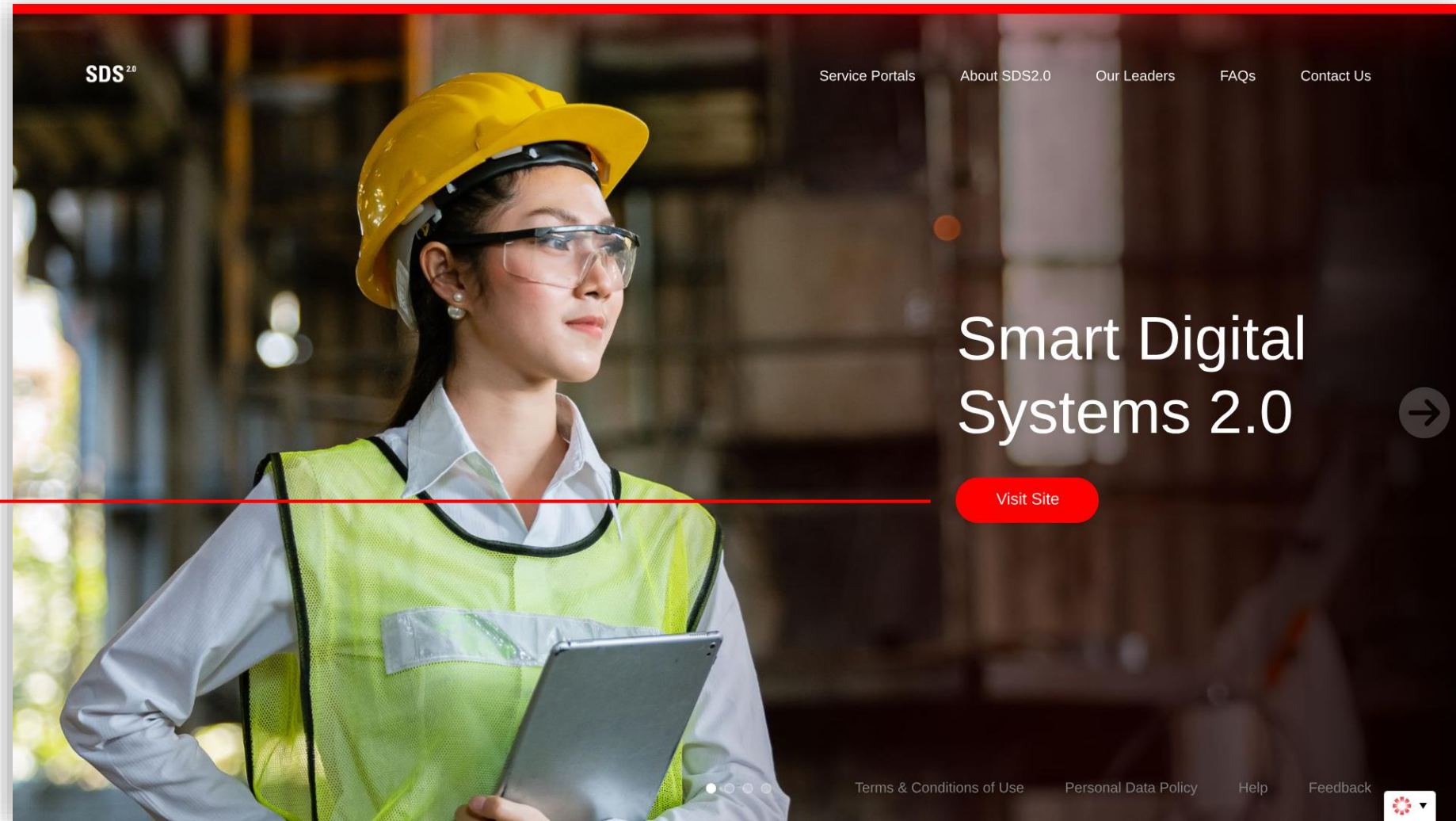successfully connected to the IP Address.

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

✤ ST Engineering

Admin Console Login (1)

ST Engineering

To access SDS2.0:

https://sds.stengg.com

Then select **Visit Site**

SDS 2.0

Service Portals   About SDS2.0   Our Leaders   FAQs   Contact Us

Smart Digital
Systems 2.0

Visit Site

Terms & Conditions of Use   Personal Data Policy   Help   Feedback

Admin Console Login (2)
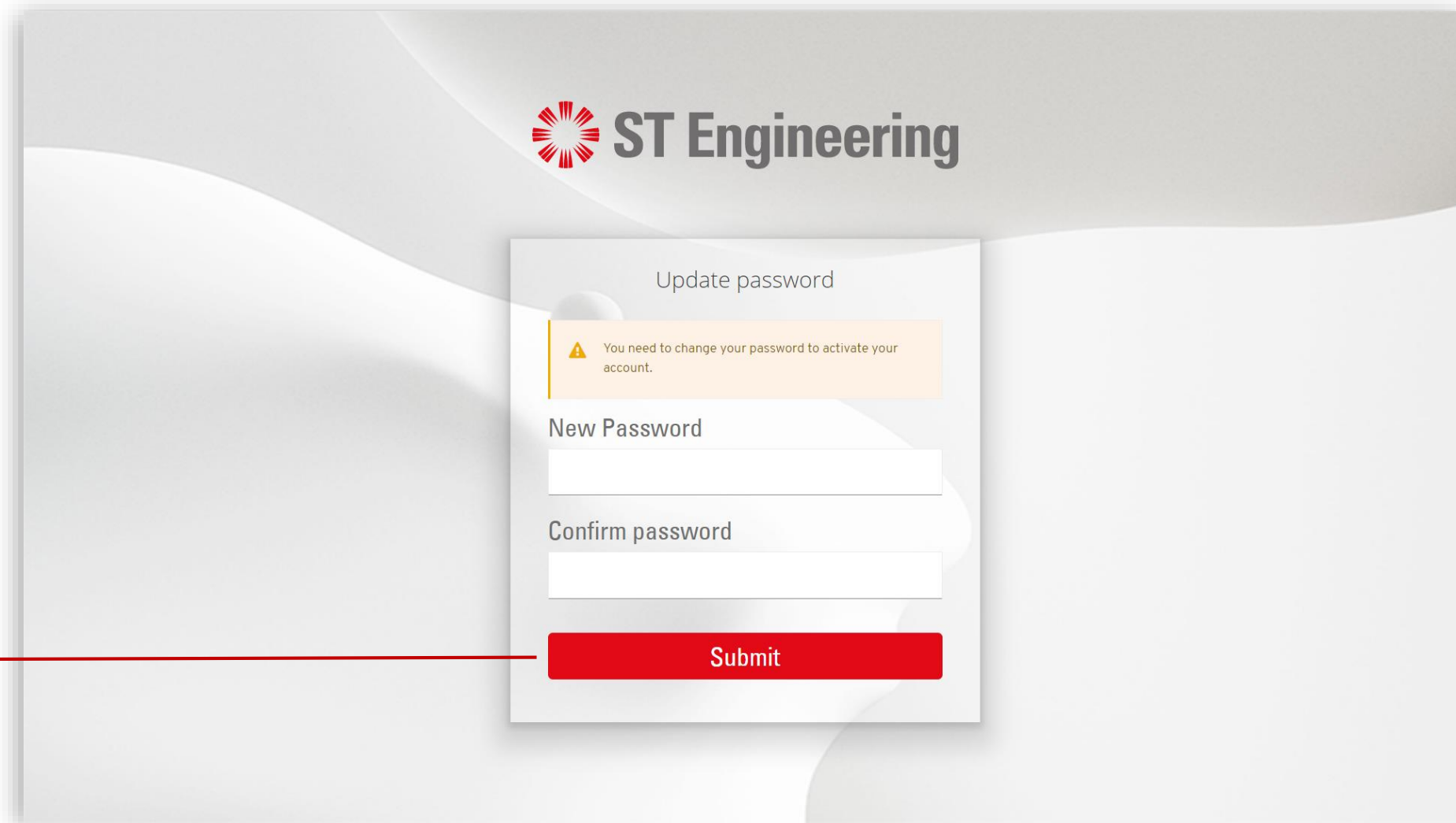
Enter your username and Password here and click **Sign In**.

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]**

Password Policies
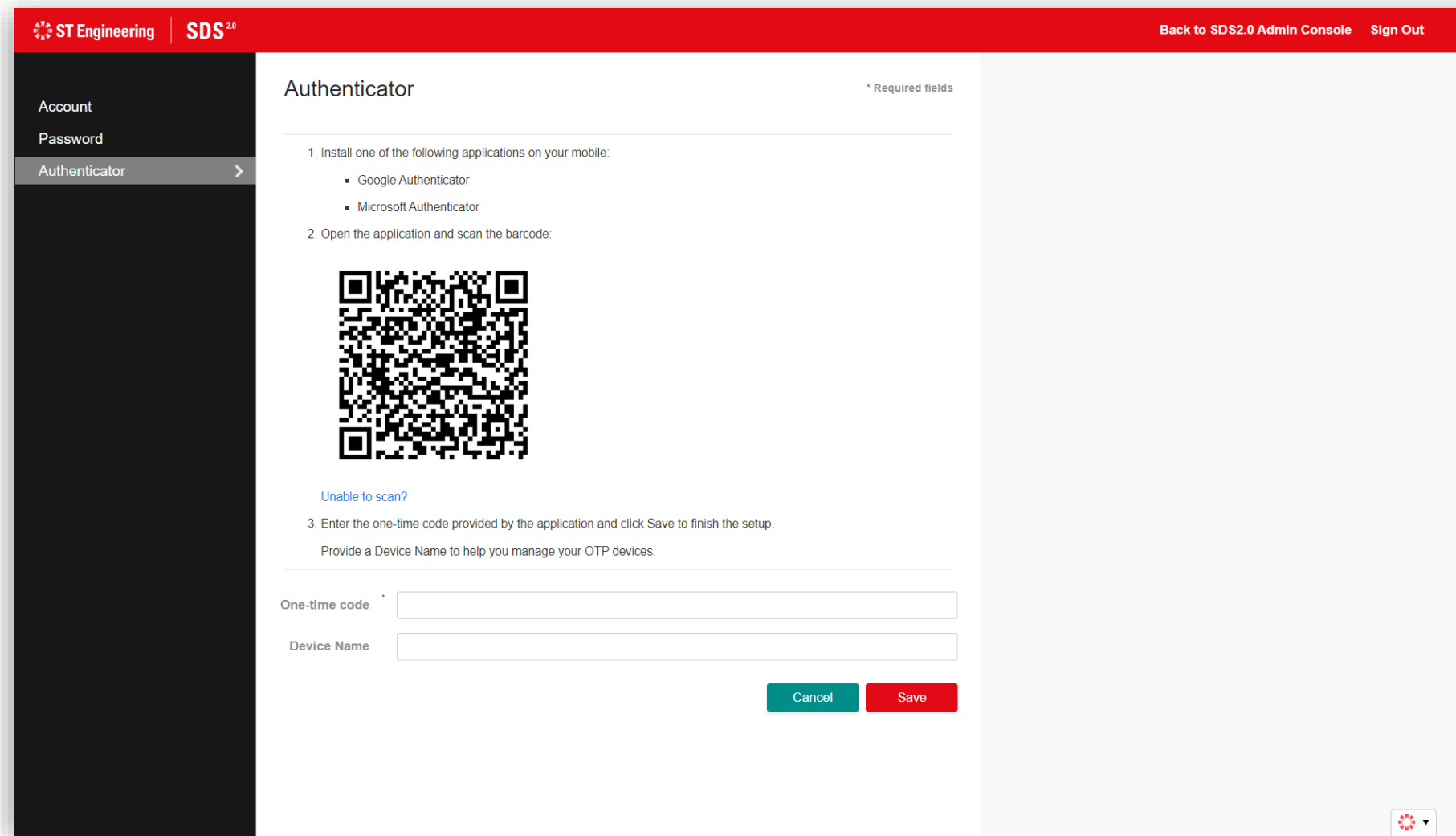
Ensure your password have:

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
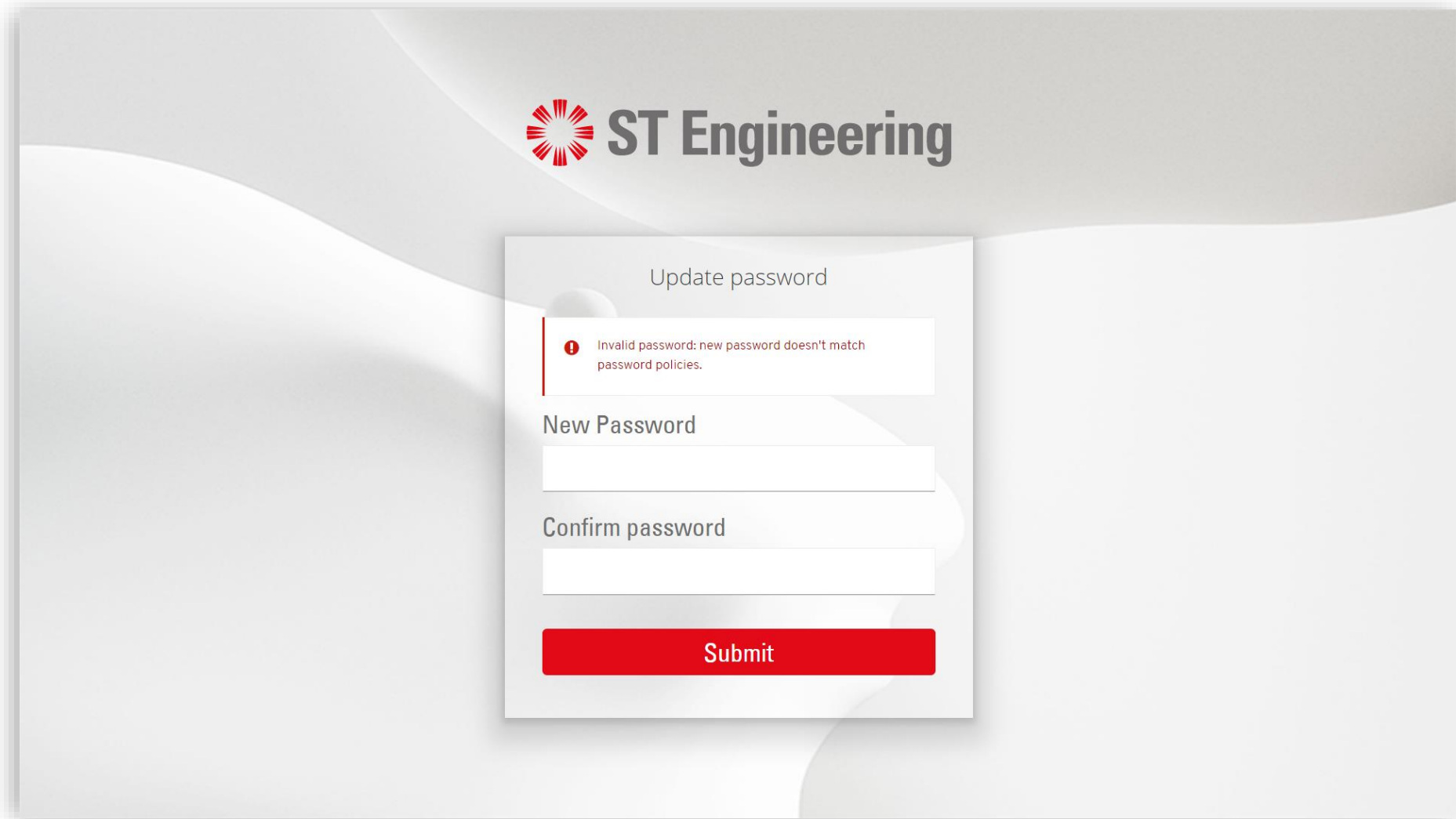
Setting up OTP Token (1)

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.

ST Engineering

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.

Google Authenticator

Google LLC   Tools   ★ ★ ★ ★ ★ 388,786 👤

3+

Add to Wishlist   Install

Google Authenticator generates 2-Step Verification codes on your phone.

2-Step Verification provides stronger security for your Google Account by requiring a second step of verification when you sign in. In addition to your password, you'll also need a code generated by the

ST Engineering
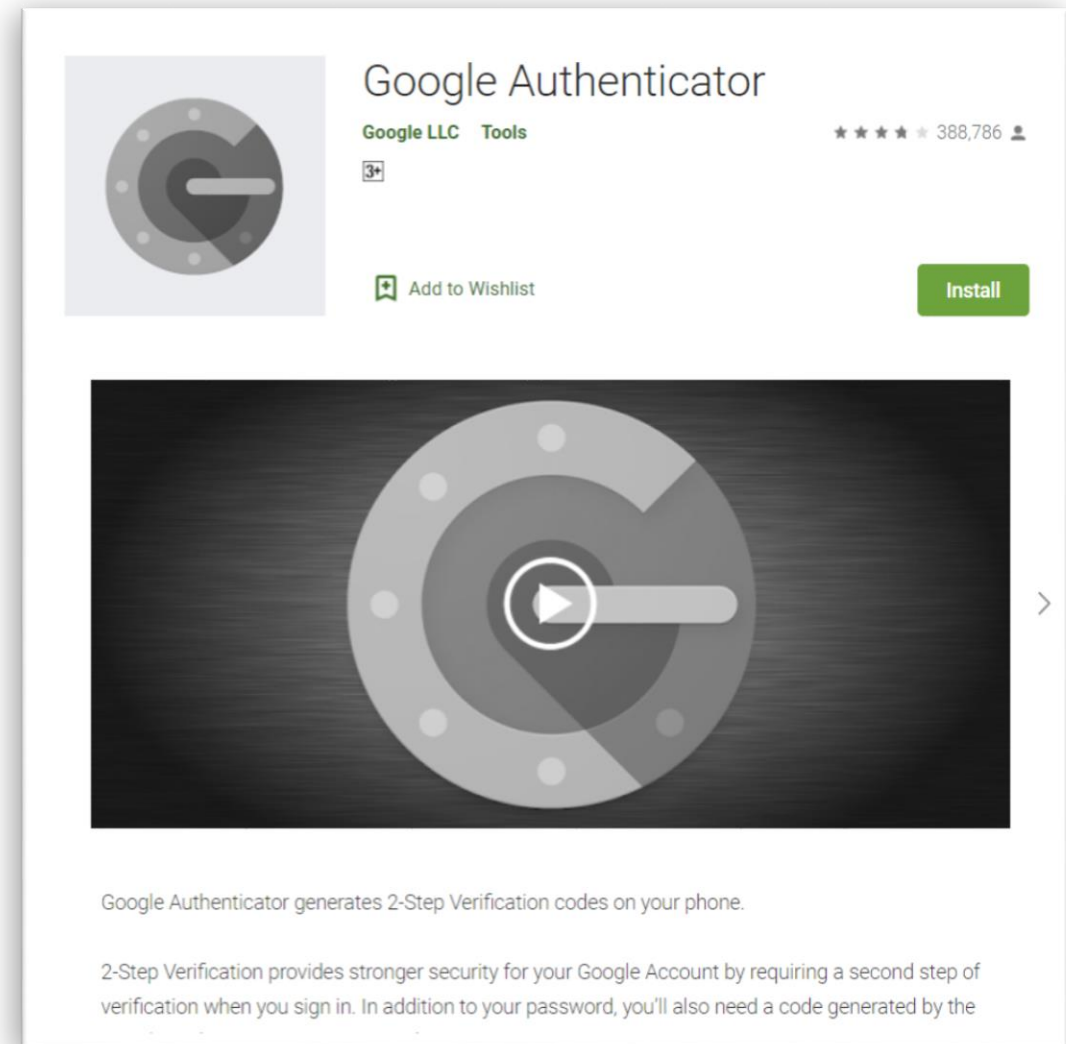
Using Google Authenticator

You can choose to scan your QR code displayed on your Authenticator page or enter a setup key.
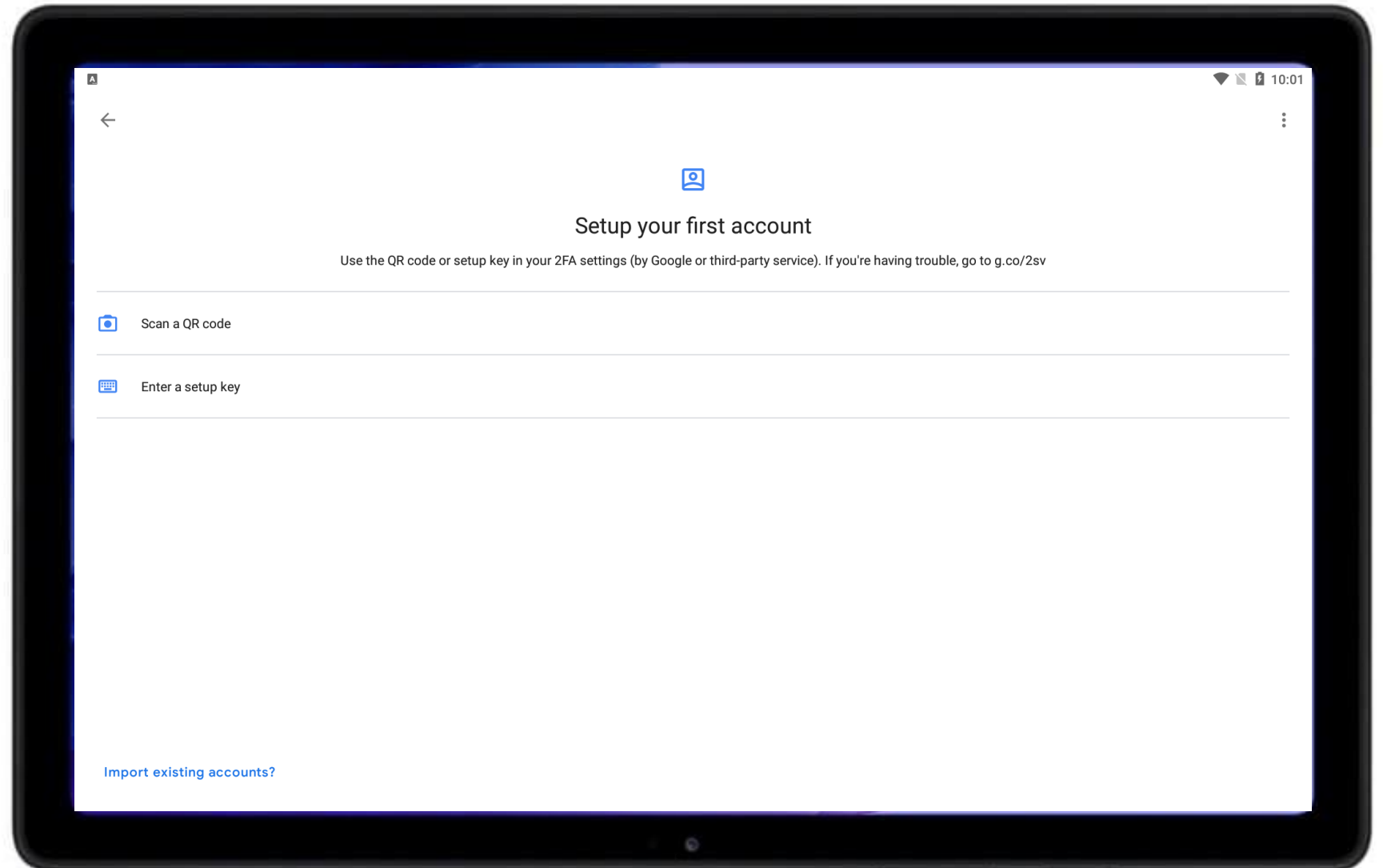
Scan a QR Code
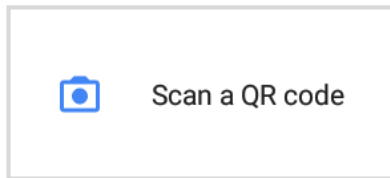
If you have selected **[Scan a QR code]**, your device camera will be activated for scanning.

Scan the QR code shown on Authenticator page.

Then go to to complete your OTP setup.

ST Engineering
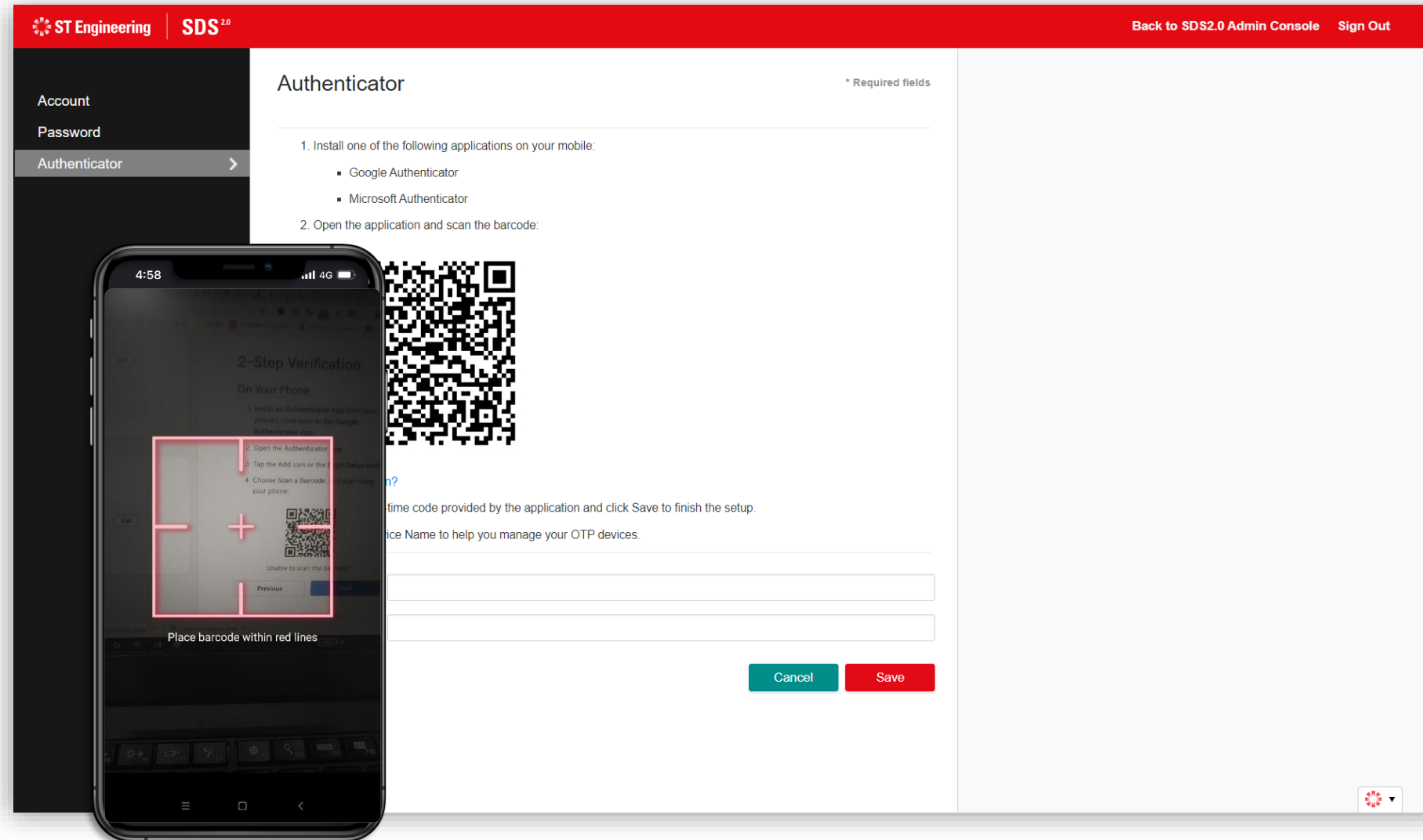
Enter a Setup Key
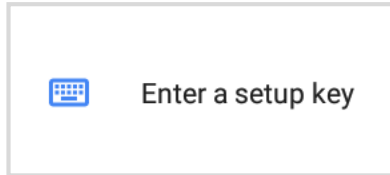
Enter a setup key

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.

← Enter account details

Account name
My Authenticator for SDS2.0

Your key
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEF

Type of key
Time based

Add

Where to find Setup Key

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]**.

Completing OTP Setup

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

Change OTP Token

Select the delete button to remove your old device.
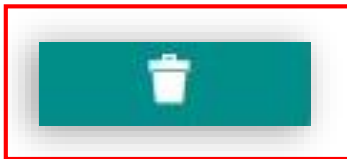
Once removed, you can setup a new OTP token (Refer to slide 14-21).
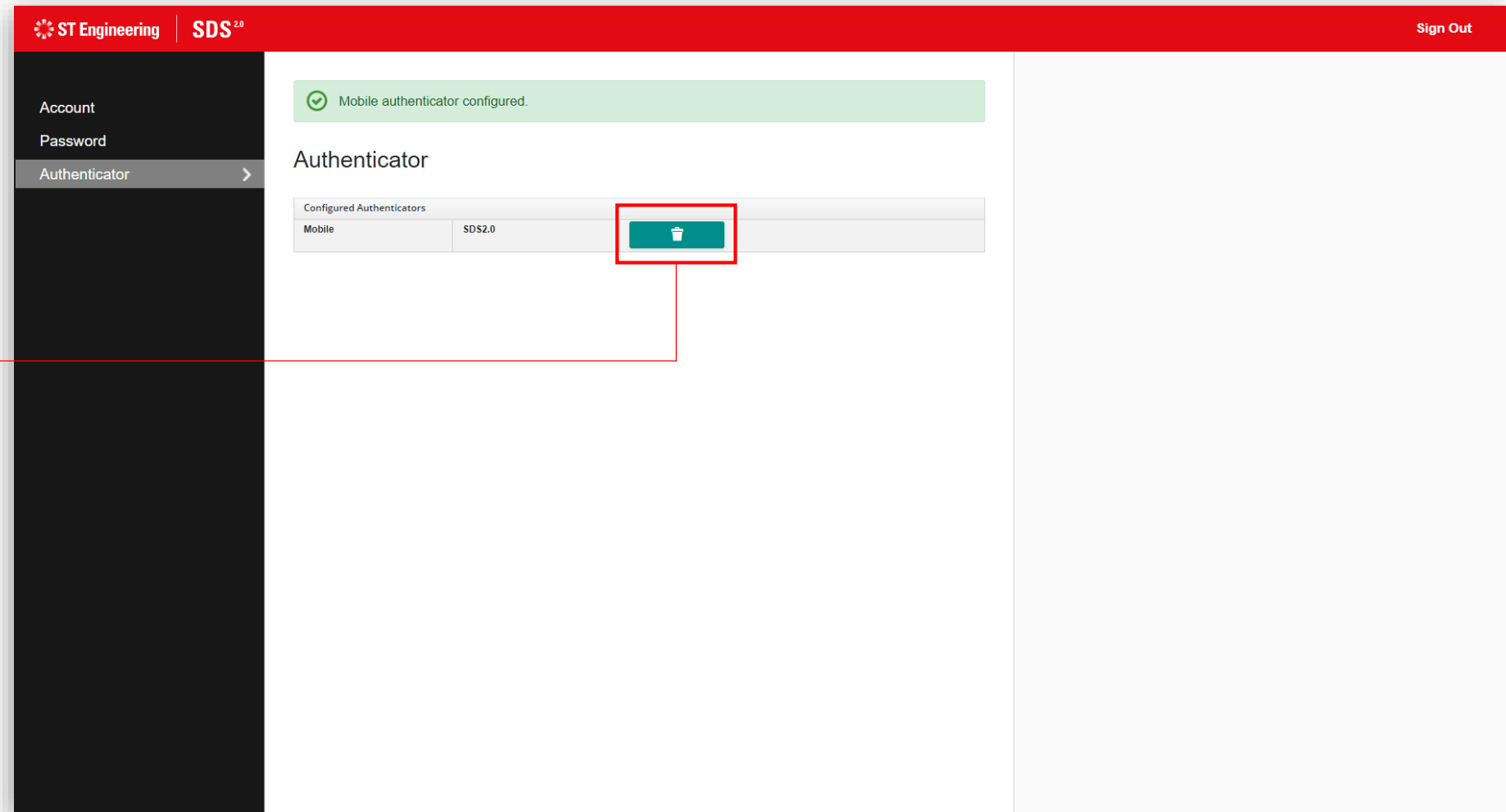
Forget or Lost Physical OTP Device
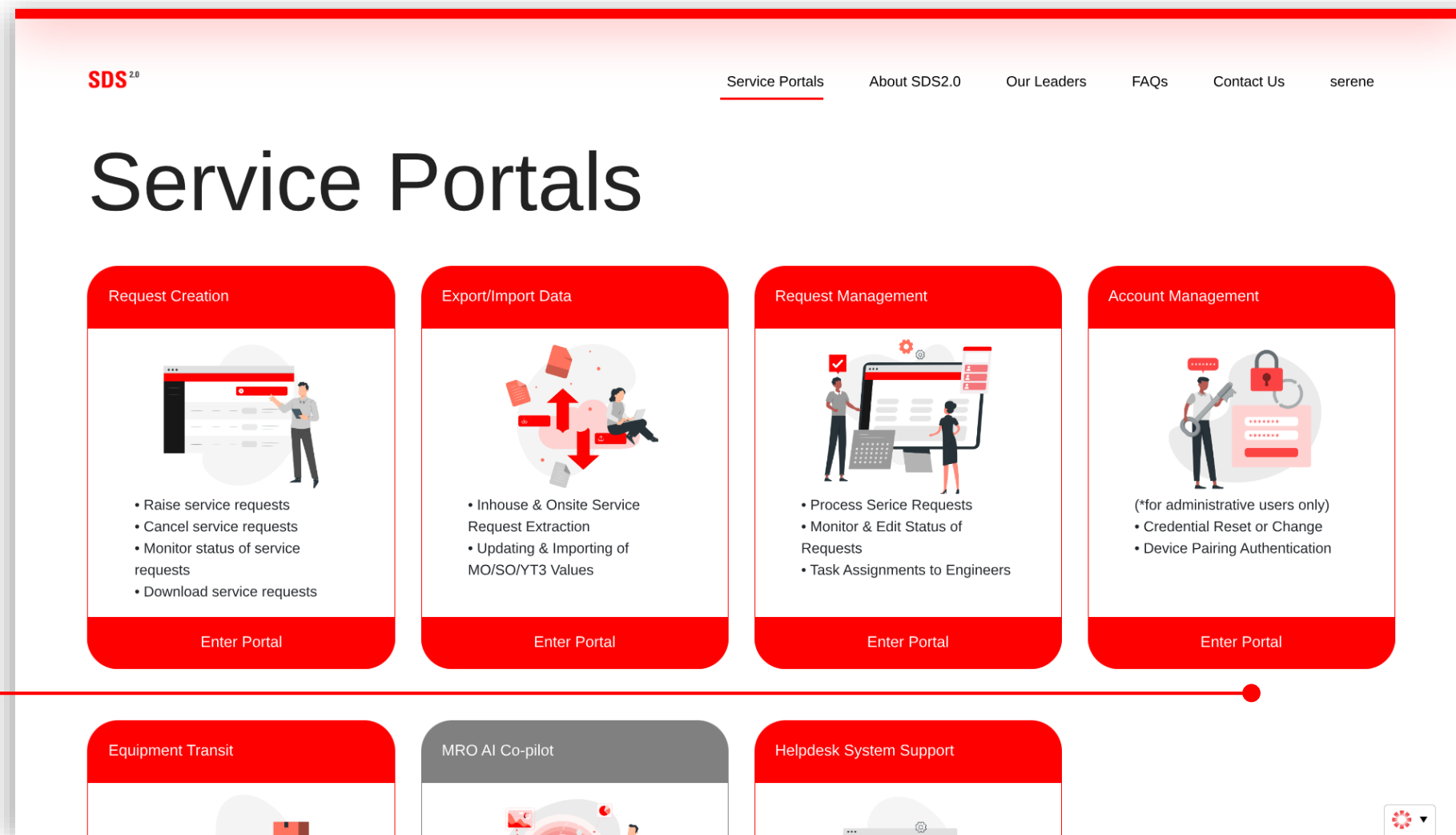
If you have forgotten to bring your physical OTP device, or lost it (E.g., smartphone), **you will need to request help internally (CX Hub)** to reset your OTP token setup.
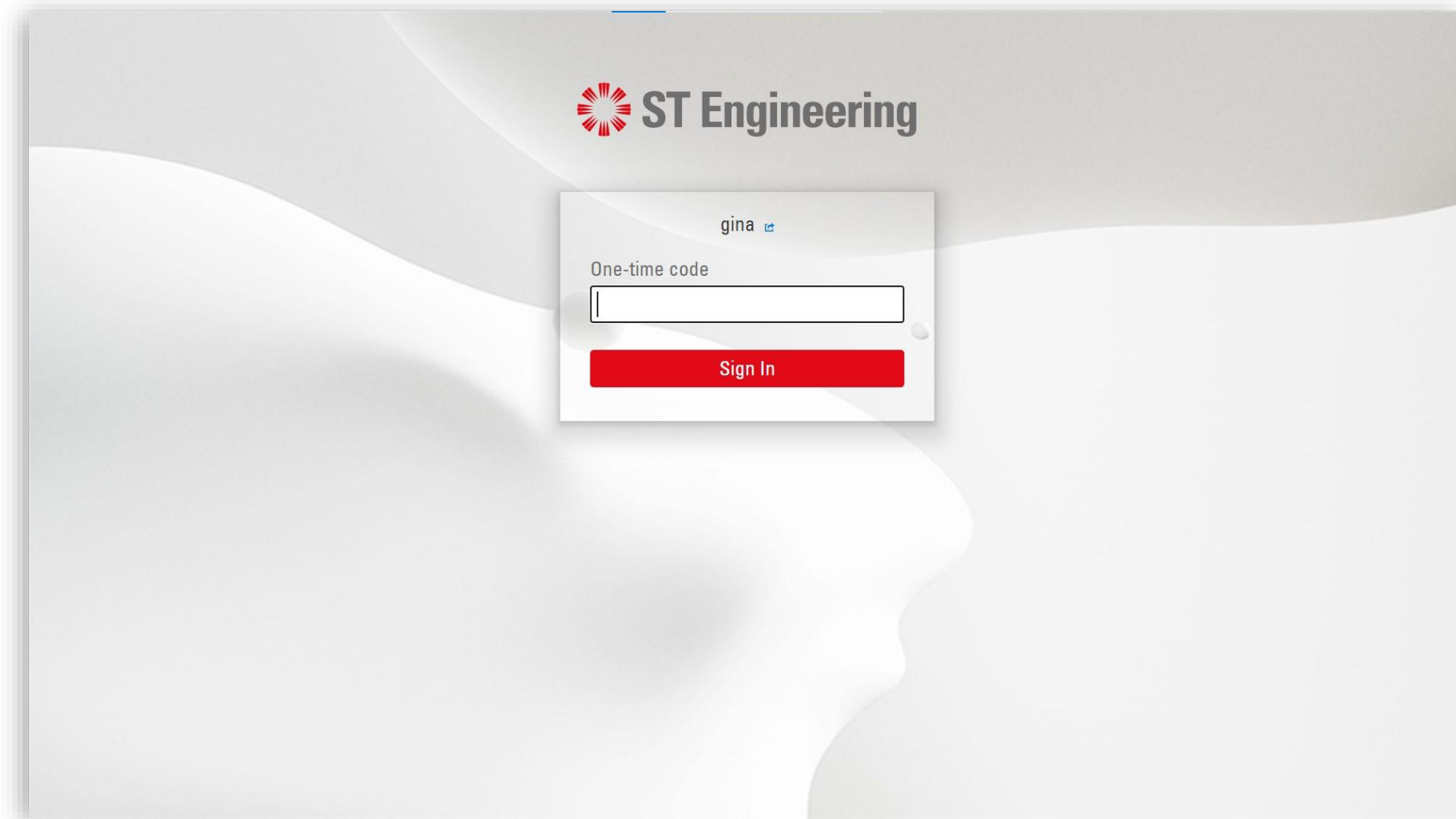
Account Management

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

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

Service Portals   About SDS2.0   Our Leaders   FAQs   Contact Us   serene

Service Portals

Request Creation
- Raise service requests
- Cancel service requests
- Monitor status of service requests
- Download service requests

Enter Portal

Export/Import Data
- Inhouse & Onsite Service Request Extraction
- Updating & Importing of MO/SO/YT3 Values

Enter Portal

Request Management
- Process Serice Requests
- Monitor & Edit Status of Requests
- Task Assignments to Engineers

Enter Portal

Account Management
(*for administrative users only)
- Credential Reset or Change
- Device Pairing Authentication

Enter Portal

Equipment Transit

MRO AI Co-pilot

Helpdesk System Support

Update My Account

To update your account information, tap on your name (i.e., Serene Loh) and select **[My Account]**.
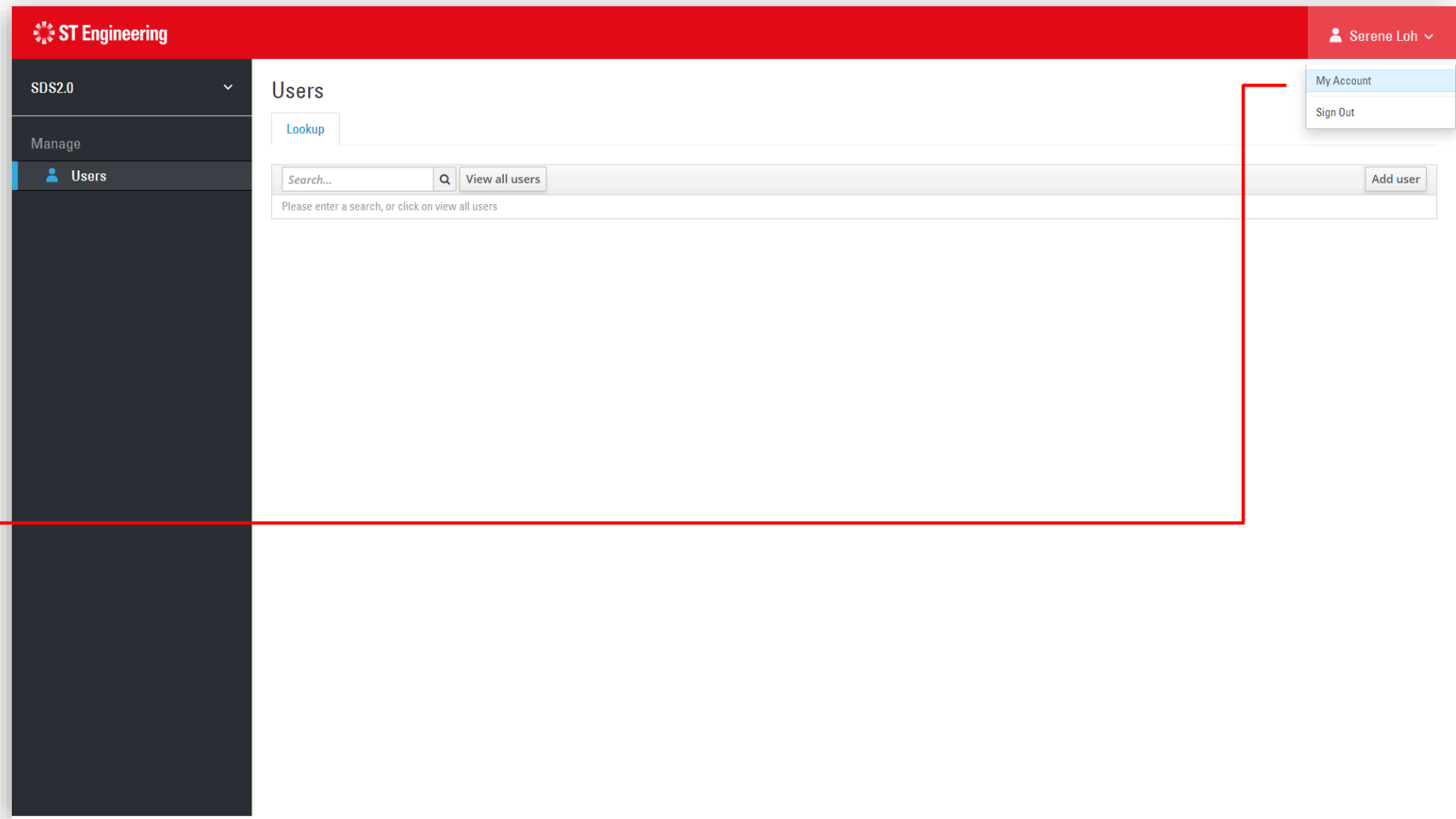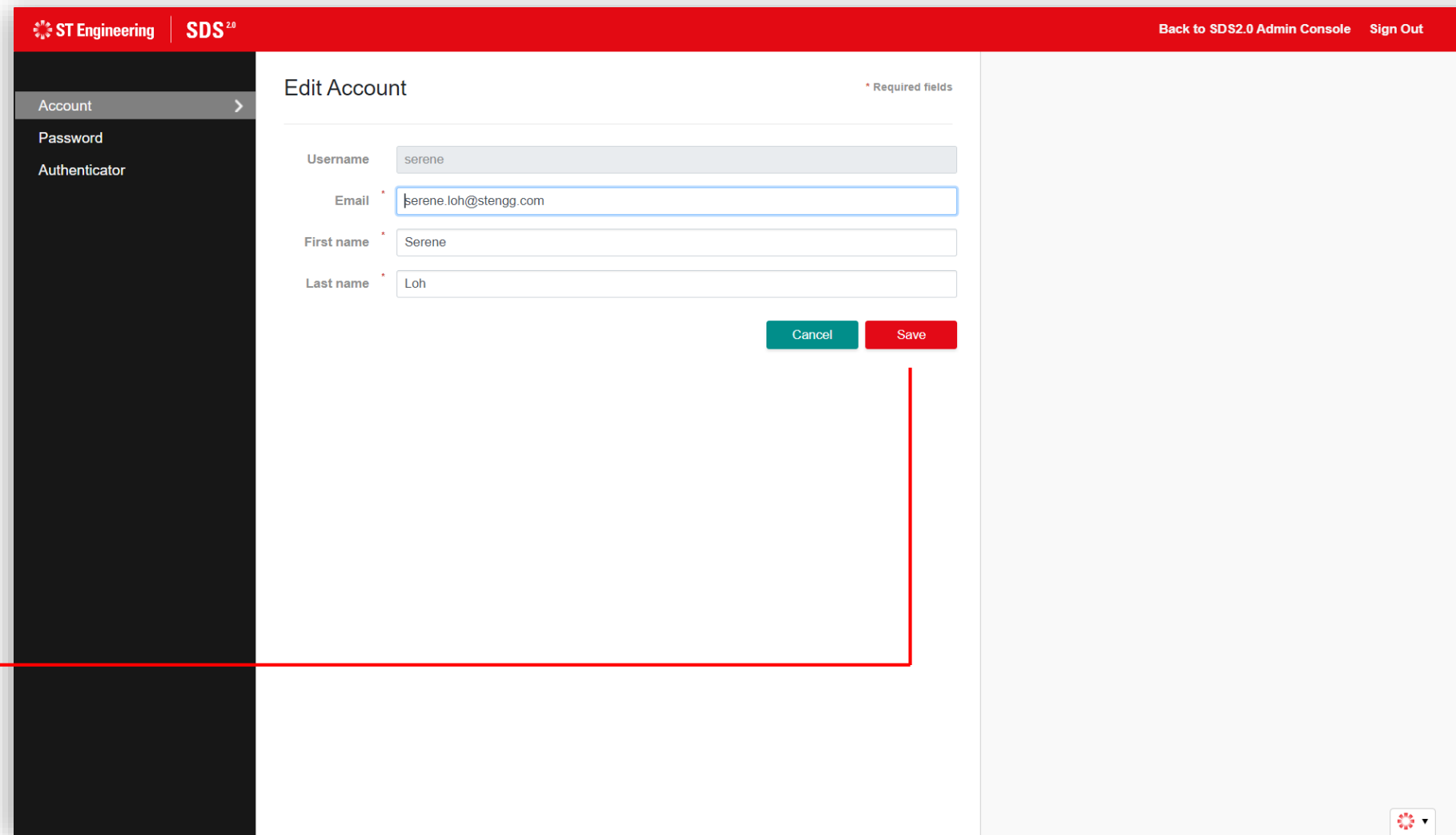
Update Account Information (1)

On the Account page, update your details:

- Email

- First Name

- Last Name

Tap **[Save]** to update your details.
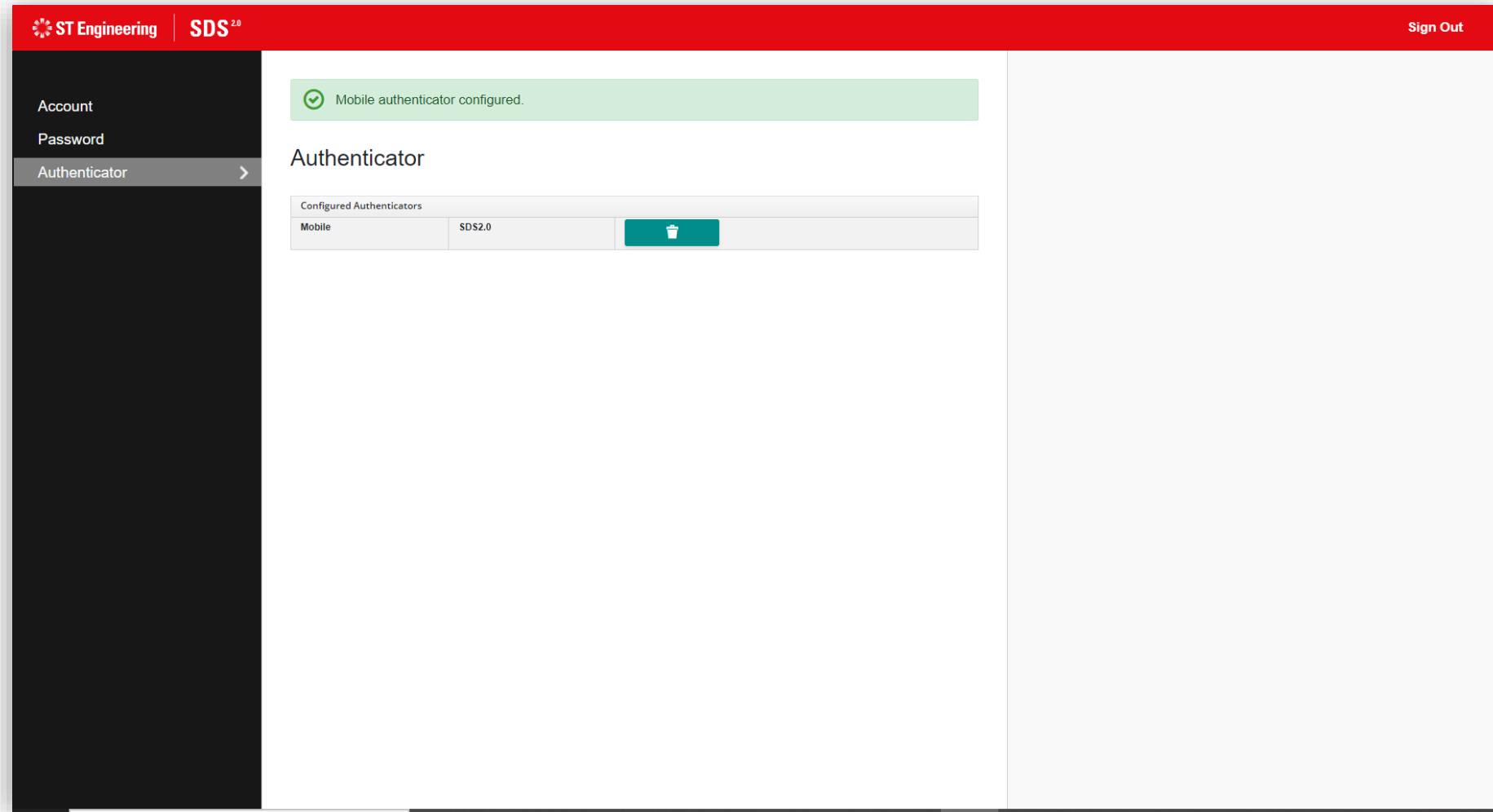
Update Account Information (2)

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

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

ST Engineering | SDS 2.0

Back to SDS2.0 Admin Console   Sign Out

Account >
Password
Authenticator

Edit Account

* Required fields

Username	serene
Email *	serene.loh@stengg.com
First name *	Serene
Last name *	Loh

Cancel   Save

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.
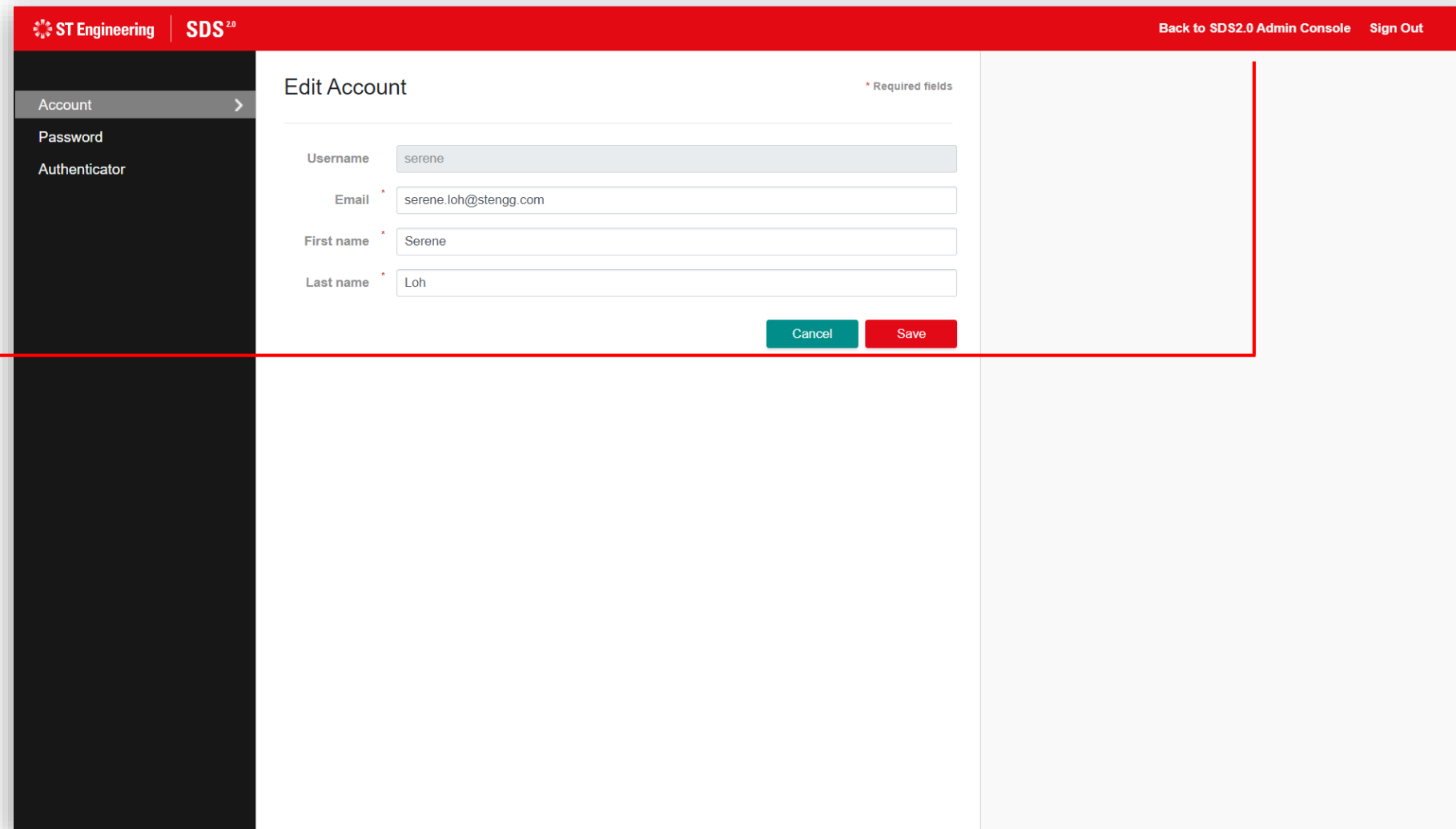
Sign Out of Admin Console

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).
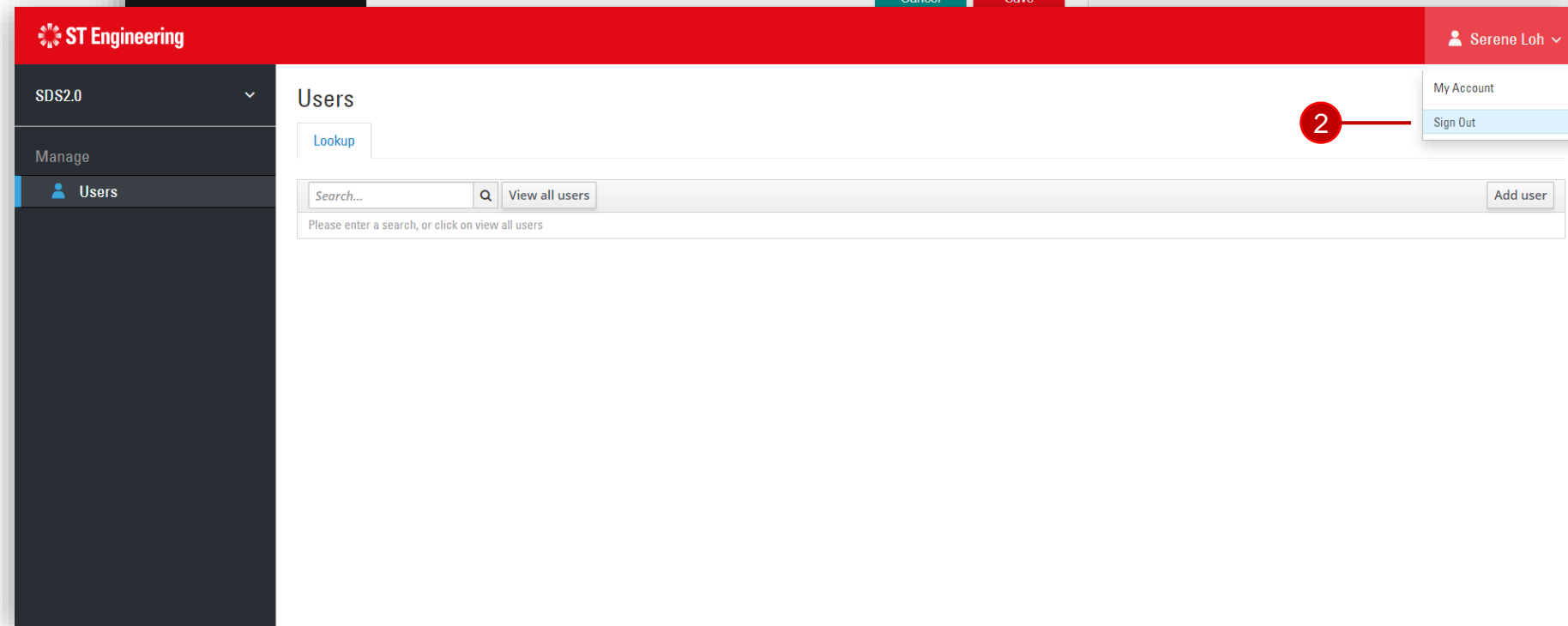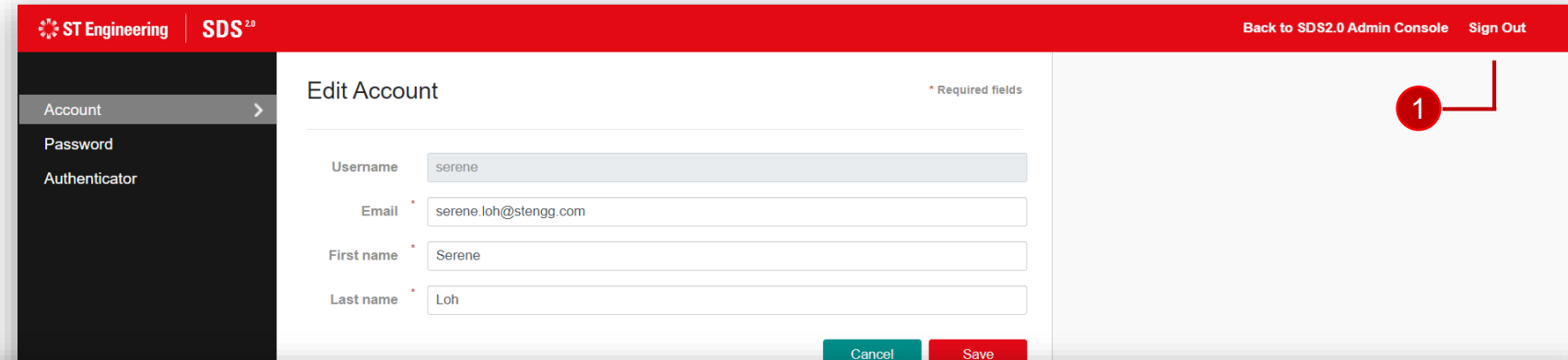
User Account Management

- User Accounts
- Account Creation
- Update/Edit Account Details
- Reset Password

- Reset OTP Token
- View OTP Algorithm
- Sessions
- Delete User

ST Engineering

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

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

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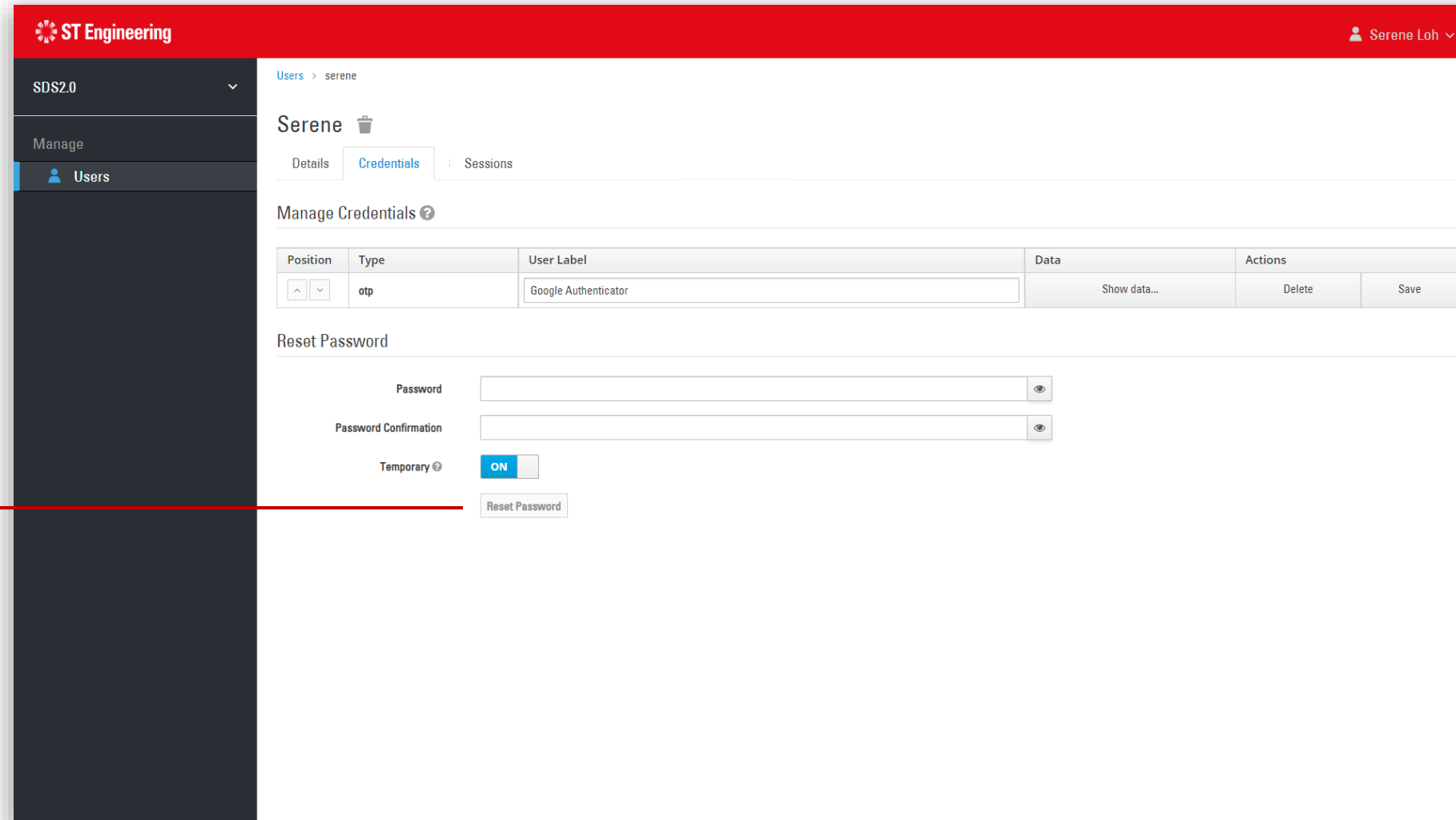
OR from Users page, tap **[Edit]** to edit the user.
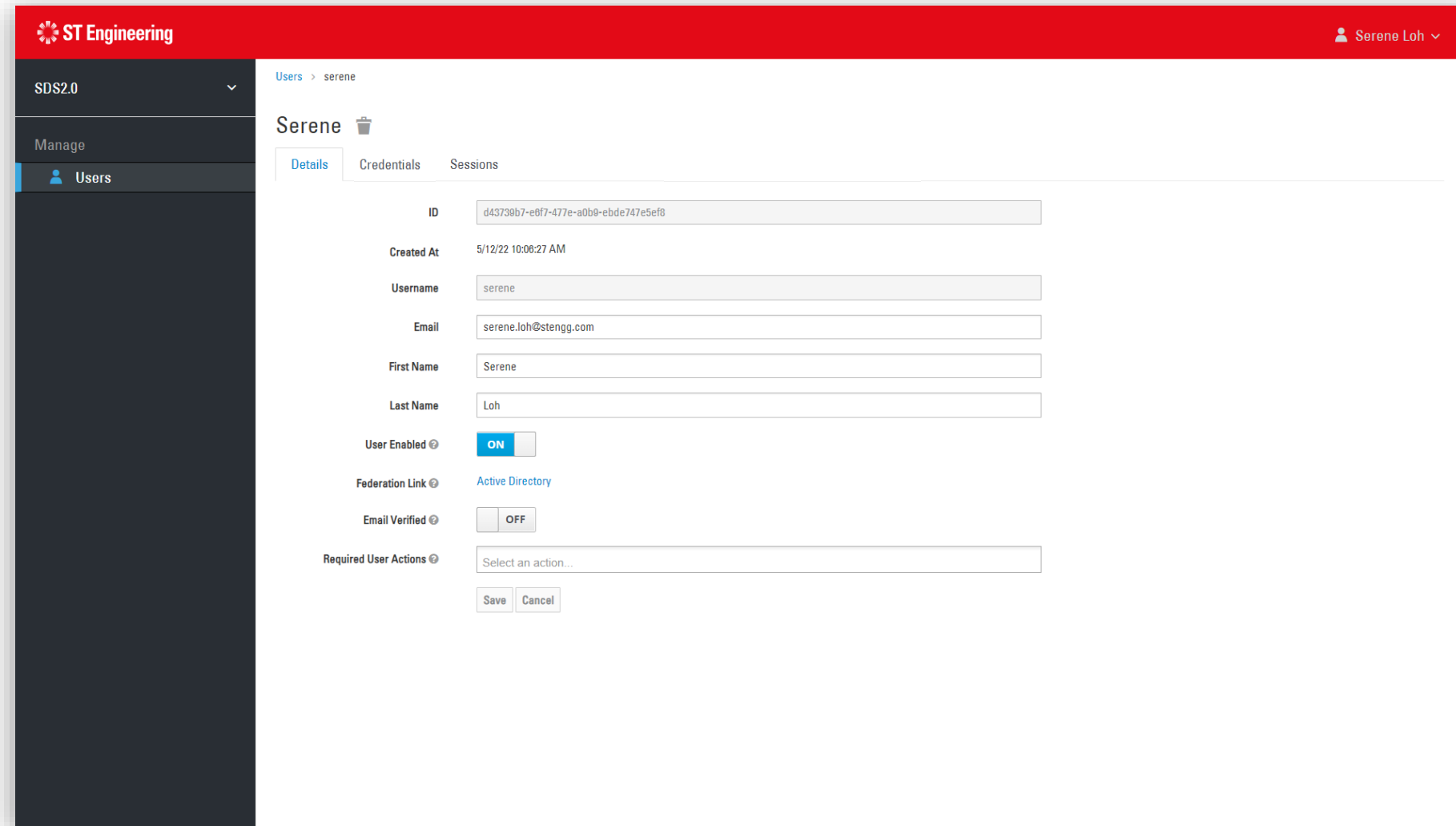
Reset Password

Administrator can reset user's password under Credential Tab.

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

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.
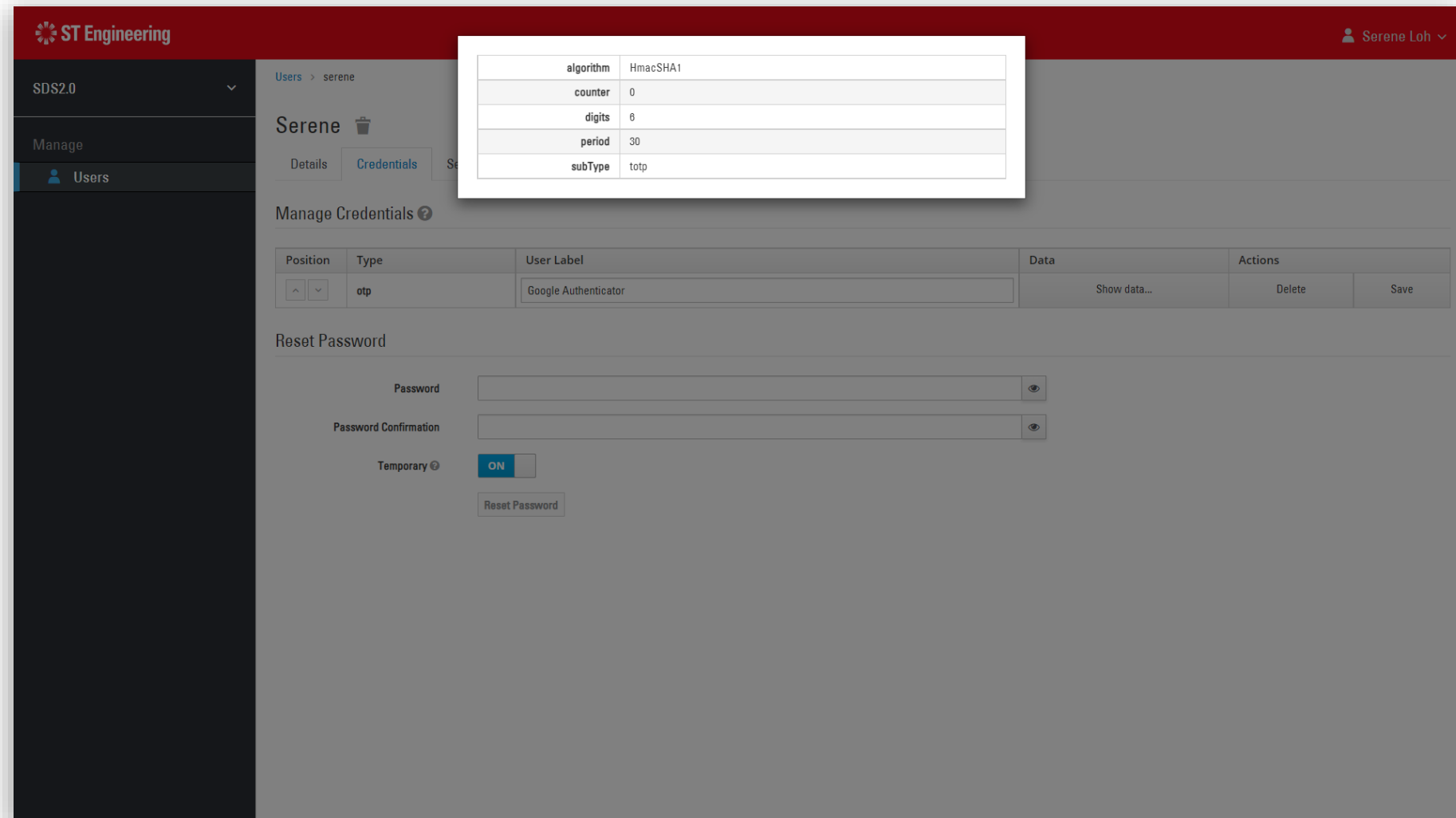
View OTP Algorithm

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…]**.

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]**.

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

Thank you

ST Engineering