



SecurLogin User Guide

Document Version: 76.1

Date: 31 March 2022

Copyright © 2021 i-Sprint Innovations. All rights reserved.

Neither the whole nor any part of the information contained in this document may be adapted or reproduced in any material or electronic form without the prior written consent of the copyright holder.

TRADEMARK INFORMATION and DISCLAIMER

i-Sprint Innovations Pte Ltd, i-Sprint, i-Sprint Innovations, enterprise services manager are registered trademarks of i-Sprint Innovations Pte Ltd in Singapore. AccessMatrix™, Universal Sign On™, Enterprise AdminGuard™ are worldwide trademarks of i-Sprint Innovations.

All other trademarks are the property of the respective trademark holders.

Information in this document is subject to change without notice.

i-Sprint Innovations makes no warranty of any kind with regard to this information, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

i-Sprint Innovations shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

Table of Contents

- 1. Preface 5
 - 1.1 Purpose 5
 - 1.2 Terms 5
- 2. Overview 6
- 3. Enterprise User Registration & Login 7
- 4. Dashboard 9
 - 4.1 Devices Overview 9
 - 4.2 Authentication World Map 9
 - 4.3 Authentication Log 9
- 5. Policies 10
 - 5.1 User Policy 10
 - 5.2 Network Policy 11
 - 5.3 Authentication Restrictions-This controls the usage of the 2FA Methods 11
- 6. Applications 12
- 7. User Store 15
- 8. Users 20
 - 8.1 Users 20
 - 8.2 New User 21
 - 8.3 Import User 21
- 9. 2FA Devices 23
- 10. Groups 24
 - 10.1 Groups 24
- 11. Administrators 25
- 12. Settings 26
 - 12.1 General 26
 - 12.2 Email Templates 26
- 13. Billing 27
 - 13.1 Bill Info 27
 - 13.2. Plan List 27
 - 13.3 Balance Recharge 28
 - 13.4 Recharge Records 28
 - 13.5 Monthly Statement 29
- 14. Client App 2FA Authentication 31
 - 14.1 Push Login Message 31
 - 14.2 OTP by Virtual Token 32



Date: 30 Jan 2018

©2002-2018 i-Sprint Innovations. All rights reserved.

Neither the whole nor any part of the information contained in this document may be adapted or reproduced in any material or electronic form without the prior written consent of the copyright holder.

1. Preface

1.1 Purpose

SecurLogin enterprise user guide includes functions instruction of SecurLogin enterprise administrator user account, and some enterprise user working flow or operations.

To apply 2FA authentication methods to enterprise users for login to target apps, enterprise administrator has to create desired target app under Applications, and to integrate the target app with SecurLogin using the application key and secure key from the created target app of SecurLogin.

1.2 Terms

2FA: Second Factor Authentication.

Protect an Application: To add 2FA authentication for an application.

Application Key: A key used for generation of signature's password, and the signature is used when the third-party calls SecurLogin.

Secure Key: A key used for generation of signature's password, and the signature is used when the third-party calls SecurLogin.

2. Overview

Today, password alone is no longer sufficient to guard against unauthorized access to companies' network and applications. To address this security challenge, SecurLogin offers real time Second Factor Authentication (2FA) service on the Cloud to help companies to deploy 2FA solution rapidly across their organization to strengthen their login process.

SecurLogin supports multiple 2FA login methods to protect and assure users' digital identity:

- 1) Instant authorization login via mobile push notification
- 2) One Time Password via SMS/ email
- 3) One Time Password via mobile token software
- 4) One Time Password via telephone call
- 5) One Time Password via hardware token
- 6) Facial authentication via mobile devices

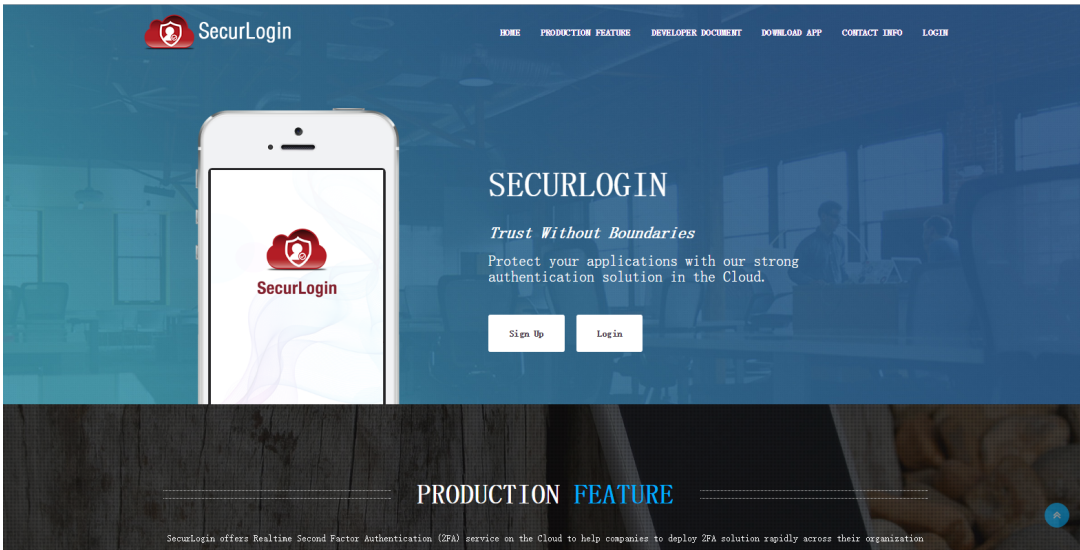
Protecting your users and your company's digital assets, SecurLogin is your 2FA login solution.

Function Models

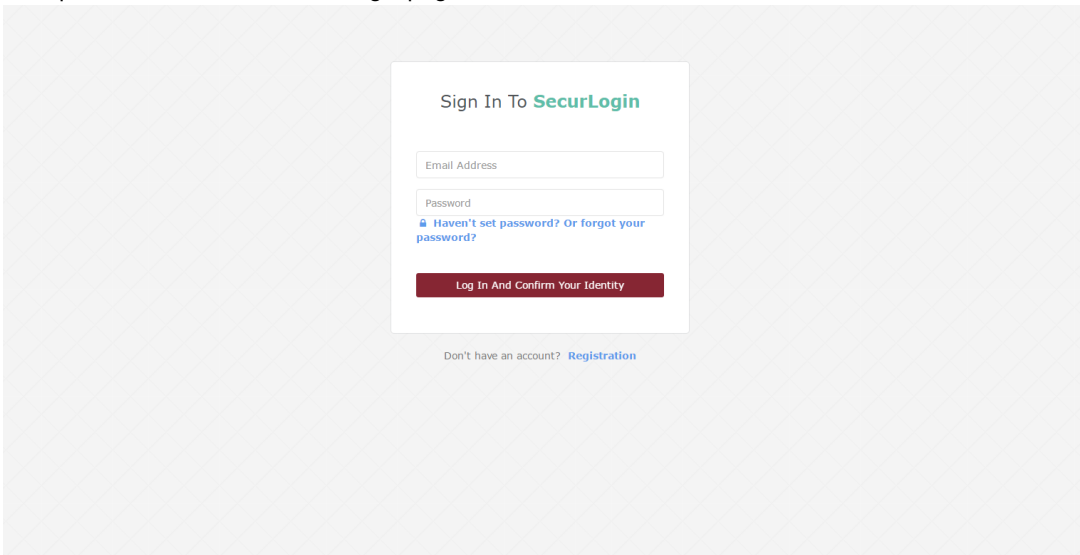
Model	Functions
Dashboard	Devices Overview
	World Map
	Authentication Log
Polices	User Policy
	Network Policy
	Authentication Log
Applications	SDK Application
	VPN Application
User Store	User Store Management
Users	Users
	New User
	Import Users
2FA Devices	2FA Device Management
Groups	Group Management
Administrators	Administrator Management
Settings	General
	Email Templates
Billing	Billing Info
	Plan List
	Recharge Balance
	Recharge Record
	Monthly Statement

3. Enterprise User Registration & Login

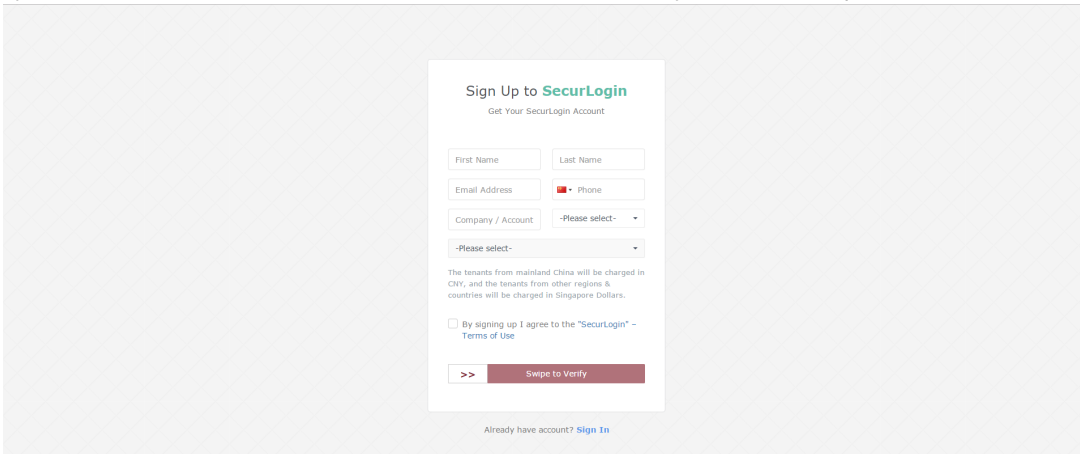
Open a browser and visit the SecurLogin website (English: www.securlogin.com, Chinese: cn.securlogin.com). Click the Login button that on the top right or next to the mobile image to go to login page.



Enterprise administrator account login page:



Enterprise administrator account registration flow: click the Registration button as shown at above image, fill the required info; the system will send an activation email to the email address filled by user; user set password, and download a token.



Sign Up to SecurLogin
Get Your SecurLogin Account

Step 1Step 2Step 3

Set password

Email Address

First Name Last Name

Password

Password 4 to 20 characters (contains at least one digit), case sensitive.

Continue

i-Sprint Innovations © 2016

Step 1Step 2Step 3



Activate

SecurLogin offers Realtime Second Factor Authentication (2FA) service on the Cloud to help companies to deploy 2FA solution rapidly across their organization to strengthen their login process. In addition to verify by user name and password, SecurLogin also requires identity verification by mobile device or email.


SecurLogin is a best authentication solution for iOS or Android device. No iPhone or Android device?

SKIP THIS STEP

1. Launch the app store on your phone and search for "SecurLogin". Install the app. While installing, please tap "OK" to enable push notifications.
2. Or click the following links to download mobile app.

 Available on the APP STORE Download ANDROID APK

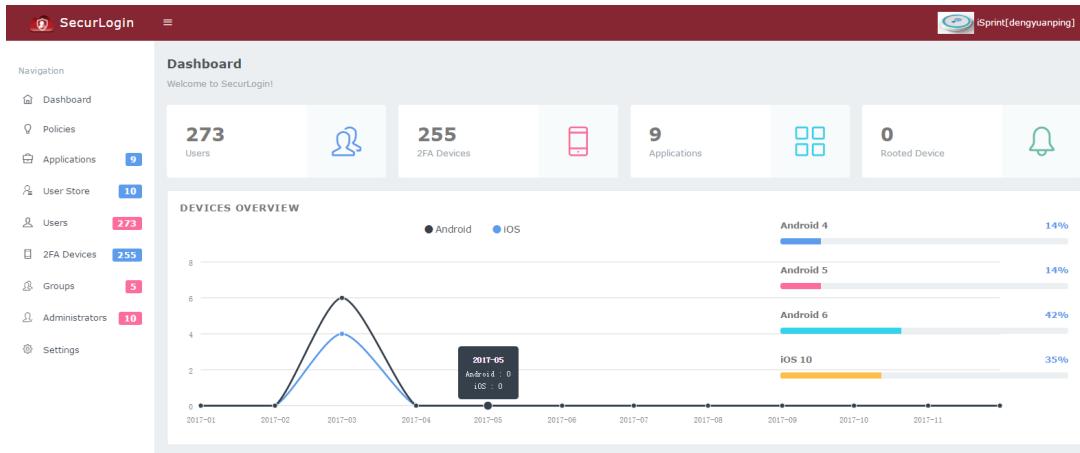
3. Launch SecurLogin, tap "Add Account", and then tap "Scan QR Code" to scan the following QR code:



4. Dashboard

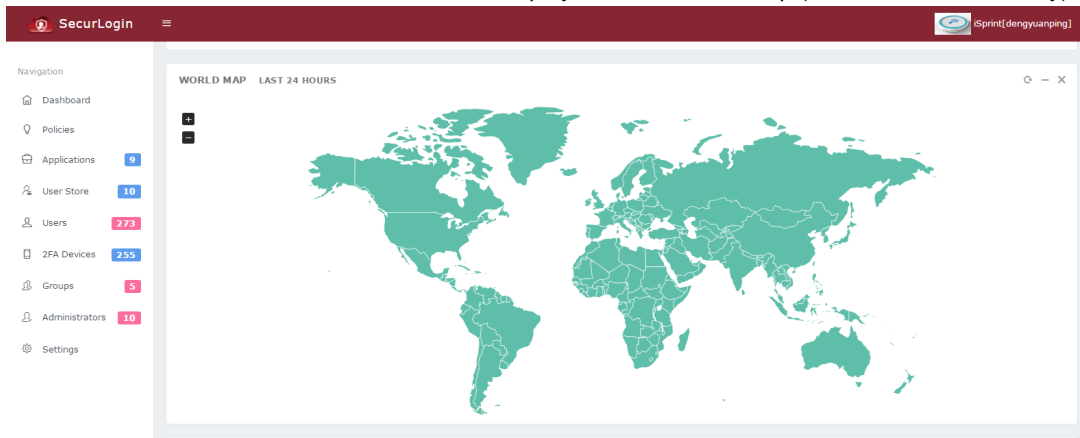
4.1 Devices Overview

Upon successful login, administrator user can view the info relative to enterprise account, such as user quantity, device quantity, etc.



4.2 Authentication World Map

The successful authentication locations will be displayed on the World Map (within last 24 hours only).



4.3 Authentication Log

Authentication log is for normal users only; and it excludes administrator logs. It includes login time, application name, device info, 2FA method and result as below. Such log is comprehensive and ready for audit.

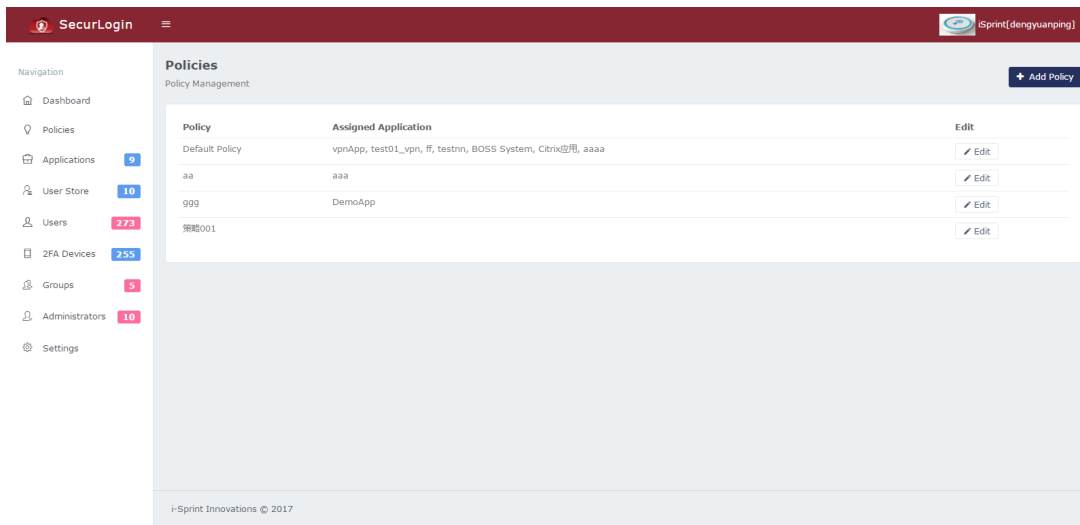
The **AUTHENTICATION LOG LAST 24 HOURS** section includes a search bar and a table with the following columns:

ID	When	User	Application Name	Result	Device	2FA Method
No matching records found						

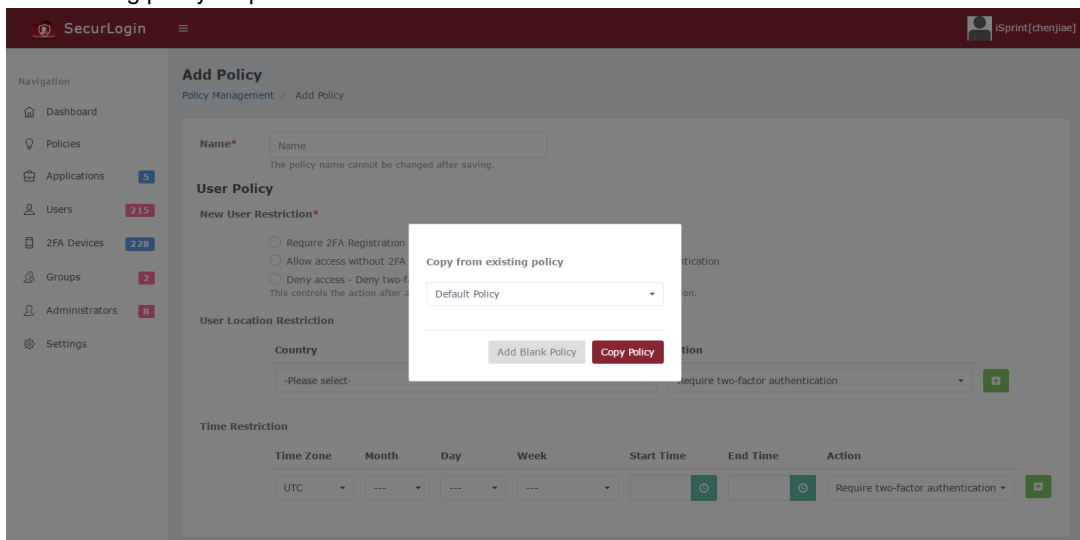
The footer of the interface reads: i-Sprint Innovations © 2017

5. Policies

Policies includes different login polices info, such as status. Polices are applied to groups to control the login of group members, such as available 2FA methods.

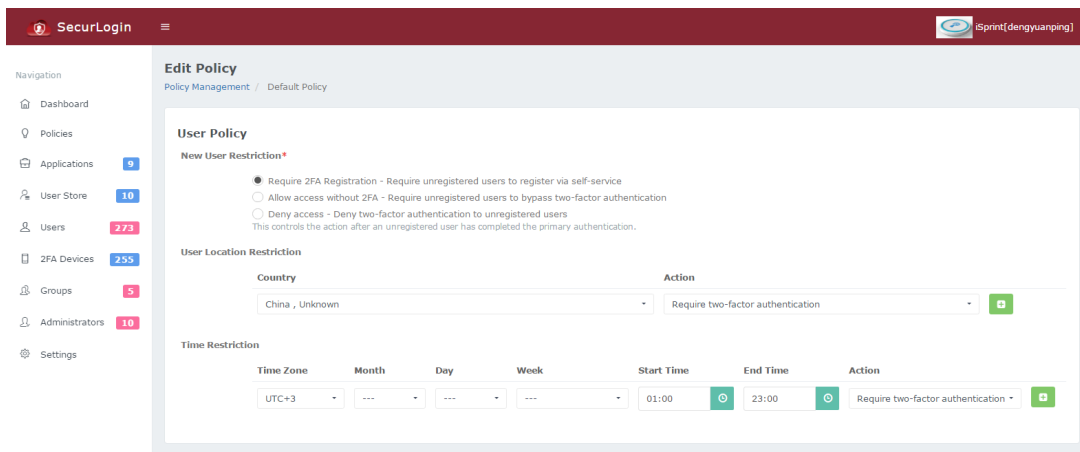


Click +Add Policy button, and select Add Blank Policy or Copy Policy; Copy Policy means user need to select a policy from Copy from existing policy drop down list.



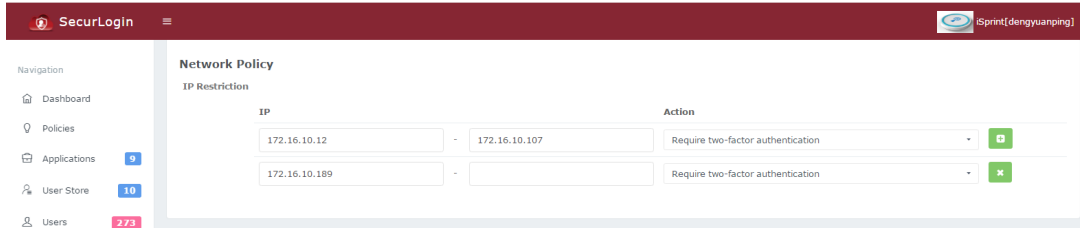
5.1 User Policy

User Policy is composed by New User Restriction, User Location Restriction and Time Restriction. User Policy can be used to determine second authentication for login is needed or not, or deny access.



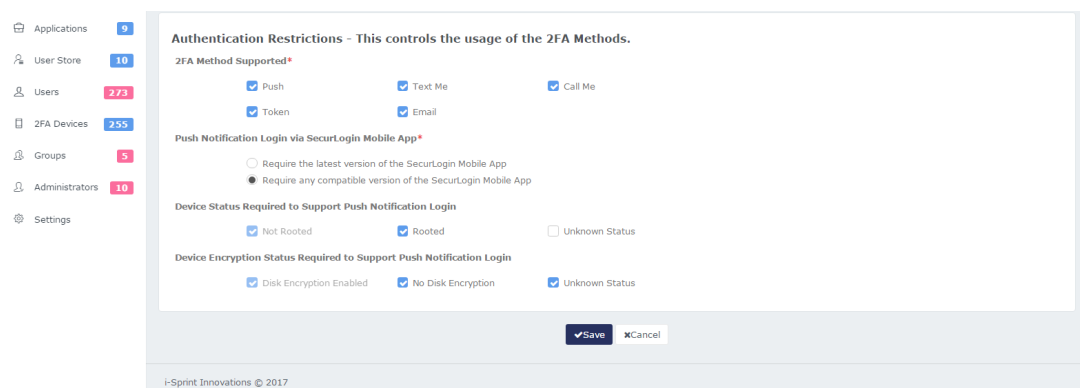
5.2 Network Policy

Network Policy determine the network arrange that user can login from by setting up valid IPs.



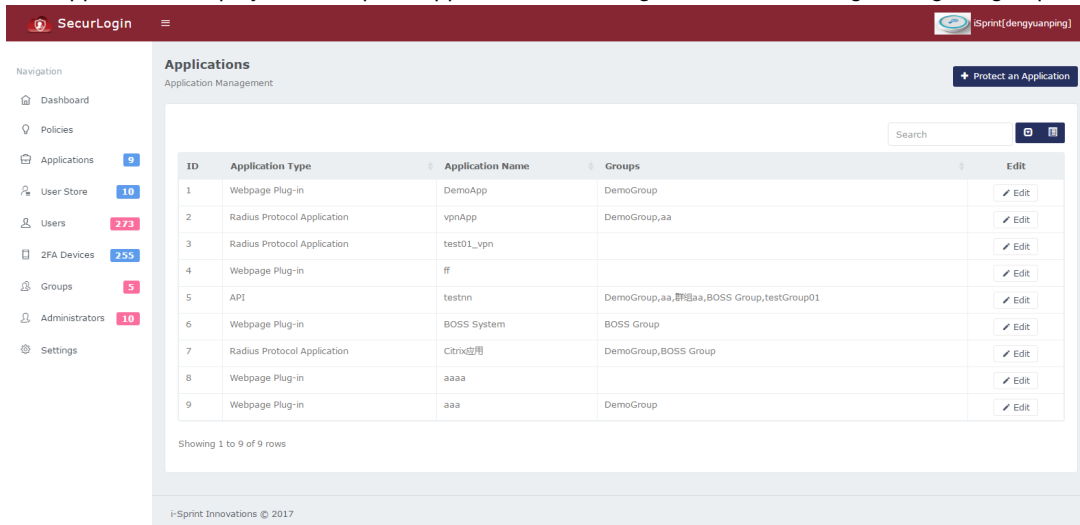
5.3 Authentication Restrictions-This controls the usage of the 2FA Methods

Authentication Restrictions includes 2FA Method Supported, Push Notification Login via SecurLogin Mobile App, Device Status Required to Support Push Notification Login and Device Encryption Status Required to Support Push Notification Login. Check the options below 2FA Method Supported, and client App user can select from the checked methods to complete login to the app that the policy is applied to. The other 3 settings are about SecurLogin Mobile App push login, and they determine the SecurLogin Mobile App version, 2FA device OS status and device encryptions status.

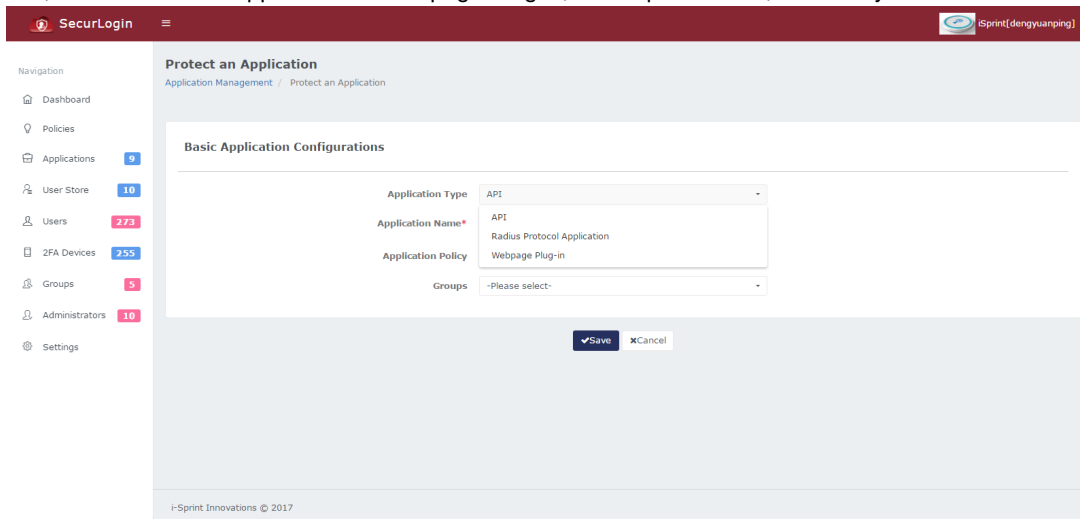


6. Applications

The Applications display the enterprise applications that integrated with SecurLogin/assigned groups.



Click + Protect an Application as shown above to go to Protect an Application page. User needs to select application type from API, Radius Protocol Application or Webpage Plug-in, fills required fields, and finally click Save button.



User can click Edit button of desired application to edit info, such as groups that can access this app, and reset secure key. Different type of application's edit page various accordingly. User can click the Delete Application at the right upper corner to delete.

Edit Application
Delete Application

Application Management / Edit Application

Basic Application Configurations

Application Type*

Application Name*

Application Policy

Groups

Application Key

Secure key Reset Secure Key

Don't write down your secret key or share it with anyone.

Save
Cancel

Edit Application
Delete Application

Application Management / Edit Application

Basic Application Configurations

Application Type*

Application Name*

Application Policy

Groups

Application Key

Secure key Reset Secure Key

Don't write down your secret key or share it with anyone.

Download Webpage Plug-in Download

Save
Cancel

For Radius Protocol Application, SecurLoginProxy need to be installed at the same time. Refer to: [SecurLogin Proxy Deployment Guide](#) - RADIUS Authentication Proxy Service.

For Radius Protocol Application, both two factor authentications will be applicable when Yes Use 1FA Configurations is checked, and user account and static password will be the IFA factor; Checked method of 2FA Method will be the only authentication factor when No Don't Use IFA Configuration is checked as below.

Edit Application
Delete Application

Application Management / Edit Application

Basic Application Configurations

Application Type*

Application Name*

Application Policy

Groups

2FA Method* Push Token Email Text Me Call Me

Use 1FA Configurations* No Don't Use 1FA Configurations Yes Use 1FA Configurations

Application Key

Secure key

Don't write down your secret key or share it with anyone.

Radius Protocol Configurations

Radius Shared Secret*

Radius Port*

1FA Configurations

AD Address*

Use SSL* Yes Use SSL No Don't Use SSL

AD Account*

AD Password*

AD User Id Attribute*

AD Search Context*

Backup AD Address

Backup AD Address Using SSL Yes Use SSL No Don't Use SSL

Backup AD Account

Backup AD Password

Group DN

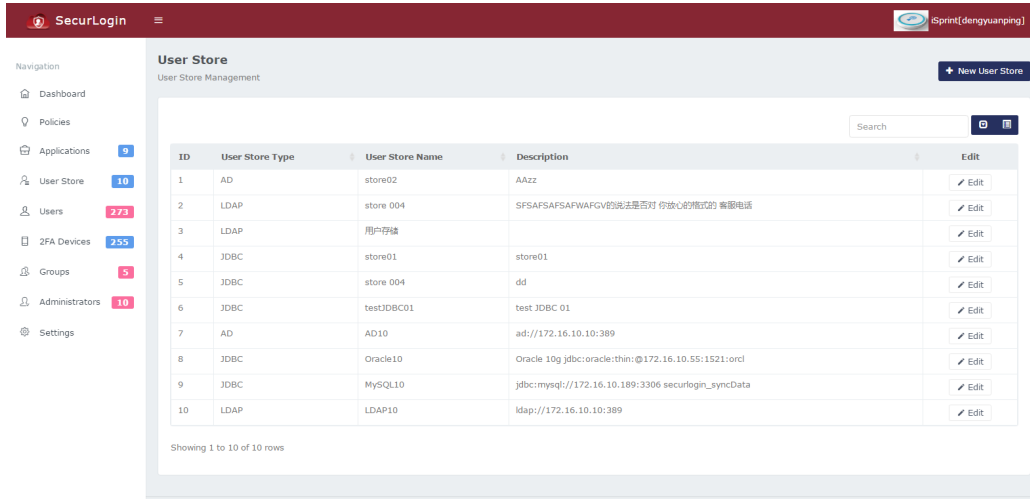
7. User Store

Enterprise users can manage user store info on User Store, i.e. view, add, edit and delete user store.

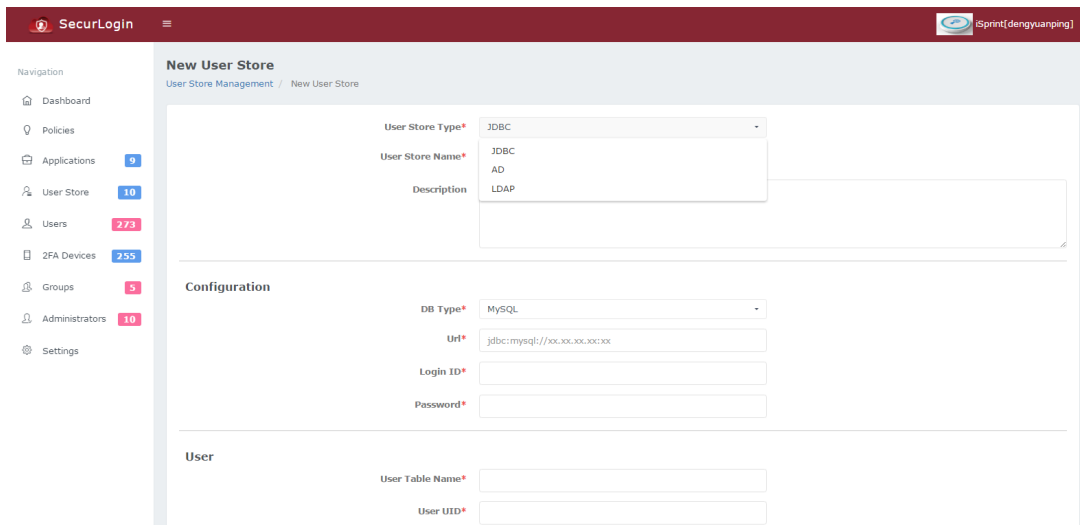
For User Store, SecurLoginProxy need to be installed at the same time. Refer to: [SecurLogin Proxy Deployment Guide](#) - User Reconciliation Proxy Service.

User Reconciliation Proxy Service:

- It is a one-way synchronization: it will only be synchronized from the client's user store database to the SecurLogin server.
- When users deleted manually from client's user database, it won't be synchronized up to SecurLogin server
- Users deleted manually from the web portal only affects SecurLogin, no user will be deleted from the client's user store database that was uploaded from the SecurLogin Proxy. SecurLogin Proxy will only synchronize users to SecurLogin server that was updated from the client's user store database.



Click +New User Store on the top right corner to display New User Store page, and select the desired User Store Type: AD, JDBC or LDAP.



Fill in the fields of the selected user store type, and fields with "*" are required. Note: different user store types may include different fields that need to be filled as below.

New User Store
User Store Management / New User Store

User Store Type* AD
User Store Name*
Description

Configuration

URI* ad://xx.xx.xx.xx:xx
Use SSL false
NT Domain*
User Search Filter* (&(objectClass=user)((objectClass=Computer)))
Login ID*
Password*

User

User UID*
User Search Context
User Attributes Mapping* [Edit](#)

Group

Group DN
Group Attributes Mapping [Edit](#)

[Save](#) [Cancel](#)

New User Store
User Store Management / New User Store

User Store Type* JDBC
User Store Name*
Description

Configuration

DB Type* MySQL
URI* jdbc:mysql://xx.xx.xx.xx:xx
Login ID*
Password*

User

User Table Name*
User UID*
User Attributes Mapping* [Edit](#)

Group

Group Table Name
Group UID
Group Attributes Mapping [Edit](#)

[Save](#) [Cancel](#)

i-SPRINT INNOVATIONS © 2017

New User Store
User Store Management / New User Store

User Store Type* LDAP
User Store Name*
Description

Configuration

URI* ldap://xx.xx.xx.xx:xx
Use SSL false
NT Domain*
User Search Filter* (&(objectClass=user)((objectClass=Computer)))
Login ID*
Password*

User

User Search Context*
User Attributes Mapping* [Edit](#)

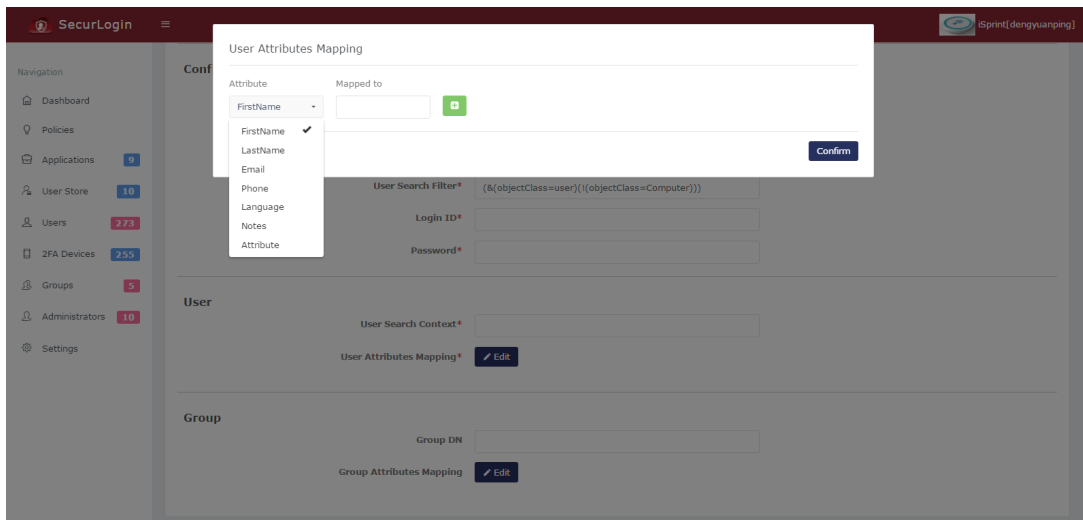
Group

Group DN
Group Attributes Mapping [Edit](#)

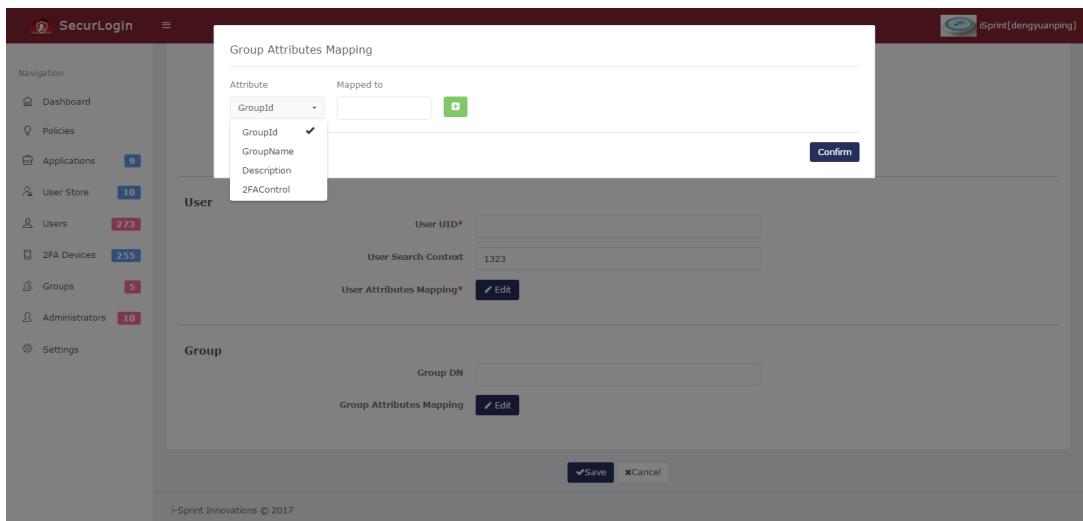
[Save](#) [Cancel](#)

i-SPRINT INNOVATIONS © 2017

Click Edit button next to User Attribute Mapping on User to display User Attribute Mapping page. The Attribute pull-down list includes FirstName, LastName, Email, Phone, etc. Email is required. Fill in Mapped to with desired value.

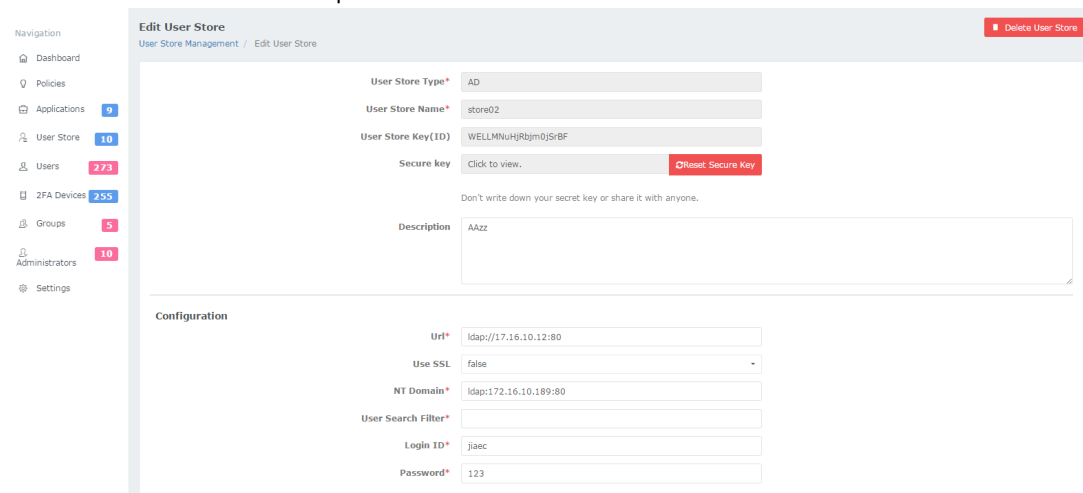


Click Edit button next to Group Attribute Mapping on Group to display Group Attribute Mapping page. The Attribute pull-down list includes GroupId, GroupName, etc. Fill in Mapped to with desired value.



Go to User Store page, click Edit button of desired user store type to display Edit User Store page, and modify required info. Click Save to complete the operation. Click Delete User Store on the top right corner to delete the current user store.

Edit User Store AD 2 screen captures are as below.



Edit User Store JDBC 2 screen captures are as below.

Edit User Store LDAP 2 screen captures are as below.

The screenshot displays a web-based user management interface. On the left, a sidebar contains navigation options: 'Administrators' with a red notification badge showing '10', and 'Settings'. The main content area is divided into two sections: 'User' and 'Group'.
Under the 'User' section, there is a 'User Search Context*' field containing the value '123', and a 'User Attributes Mapping*' field with an 'Edit' button.
Under the 'Group' section, there is a 'Group DN' field and a 'Group Attributes Mapping' field with an 'Edit' button.
At the bottom of the main content area, there are 'Save' and 'Cancel' buttons. The footer of the interface reads 'i-Sprint Innovations © 2017'.

8. Users

8.1 Users

All enterprise users are listed on Users > Users. Administrators can search users' info by User Store Name, User ID, Name, etc. on Search Criteria as below. Click Delete User on the top right corner to delete one or more users' info of current page. Click Batch Import User Data to import users, please refer to 8.3 Import User. Click to select one or more users that need to send enrollment Email, and click Batch Send Enrollment Email to finish sending.

The screenshot shows the SecurLogin Users Management interface. The top navigation bar includes 'SecurLogin' and 'i-Sprint[dengyuanping]'. The left sidebar contains navigation options: Dashboard, Policies, Applications (9), User Store (10), Users (273), 2FA Devices (255), Groups (5), Administrators (10), and Settings. The main content area is titled 'Users' and 'User Management'. It features a 'Search Criteria' section with fields for User Store (Internal User), User ID, User Email, Name, Group (-Please select-), and Creation Time. A 'Search' button is located to the right. Below the search criteria is a table with columns: User Store Name, User ID, Name, Email, Group, Attribute, Creation Time, and Edit. The table contains 10 rows of user data.

User Store Name	User ID	Name	Email	Group	Attribute	Creation Time	Edit
	rita	wangrita	729145014@qq.com	Default Group	-	2017-03-31 14:57:11	Edit
	U14902511697701511	fsdffdsa	afdsaf@fdsaf.fds	BOSS Group	-	2017-03-23 14:39:30	Edit
	18465486	asdfsadf	18465486@qq.com	DemoGroup	-	2017-03-22 19:22:22	Edit
	U14901685936041369	zz chen	zhanze.chen@axbsec.com	BOSS Group	-	2017-03-22 15:43:14	Edit
	1472540764196	UserEDemoE	testE1@axbsec.com	Default Group	-	2017-03-13 13:41:33	Edit
	jae	chenjae	jae.chen@axbsec.com	BOSS Group	-	2017-03-08 16:16:23	Edit
	U14889433068828653	asdf51as	test001@163.com	BOSS Group	-	2017-03-08 11:22:00	Edit
	U14889430408048564	Ktommy	tommyk@dd.com	BOSS Group	-	2017-03-08 11:17:22	Edit

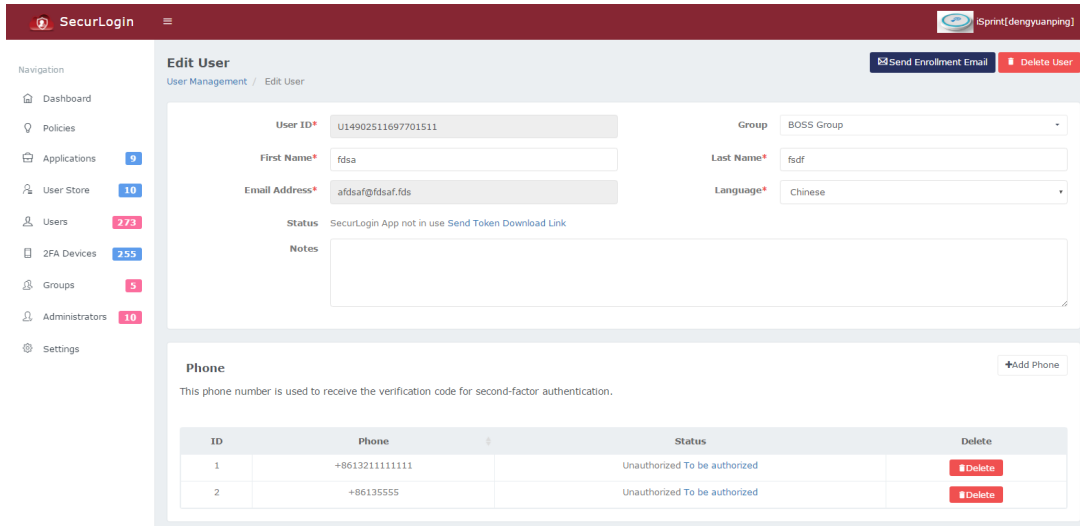
To assign user to desired group, go to Users > Users, check the desired user, and click ~~Add to Group~~ as shown below, select desired group, click Confirm on the prompt message.

The screenshot shows the SecurLogin Users Management interface with the 'Add to Group' dropdown menu open. The dropdown menu lists several groups: DemoGroup, aa, aa, BOSS Group, and testGroup01. The table below the dropdown shows the same user data as the previous screenshot, but with the 'Add to Group' dropdown menu open over the first few rows. The table has columns: User Store Name, User ID, Name, Email, Group, Attribute, Creation Time, and Edit. The table contains 10 rows of user data.

User Store Name	User ID	Name	Email	Group	Attribute	Creation Time	Edit
	wangrita	729145014@qq.com	Default Group	-	2017-03-31 14:57:11	Edit	
	11697701511	fsdffdsa	afdsaf@fdsaf.fds	BOSS Group	-	2017-03-23 14:39:30	Edit
	5	asdfsadf	18465486@qq.com	DemoGroup	-	2017-03-22 19:22:22	Edit
	U14901685936041369	zz chen	zhanze.chen@axbsec.com	BOSS Group	-	2017-03-22 15:43:14	Edit
	1472540764196	UserEDemoE	testE1@axbsec.com	Default Group	-	2017-03-13 13:41:33	Edit
	jae	chenjae	jae.chen@axbsec.com	BOSS Group	-	2017-03-08 16:16:23	Edit
	U14889433068828653	asdf51as	test001@163.com	BOSS Group	-	2017-03-08 11:22:00	Edit
	U14889430408048564	Ktommy	tommyk@dd.com	BOSS Group	-	2017-03-08 11:17:22	Edit
	U14888761213196330	Jtommy	tommyj@dd.com	BOSS Group	-	2017-03-07 16:42:01	Edit
	U1488868494408796	asdfsadf	asdfsadf@163.com	BOSS Group	-	2017-03-07 14:40:49	Edit

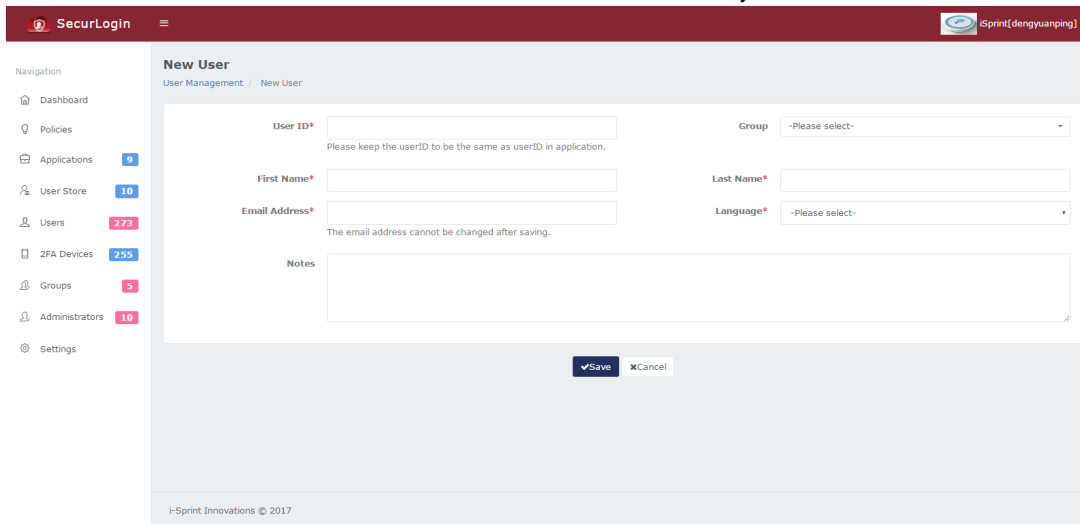
Showing 1 to 10 of 273 rows | 10 records per page

Click the Edit button of desired user to go to Edit User page. Then administrator can modify user info (e.g. phone number), or Send Enrollment Email to user by clicking the button at the right upper corner of page. From the Phone section, administrators can click +Add Phone or Delete to add or delete users' phone number. The new added phone number will be Unauthorized, so user needs to click To be authorized to enroll the phone number according by following the steps from enrollment email. Phone numbers can be used for 2FA authentication only upon successful enrollment.



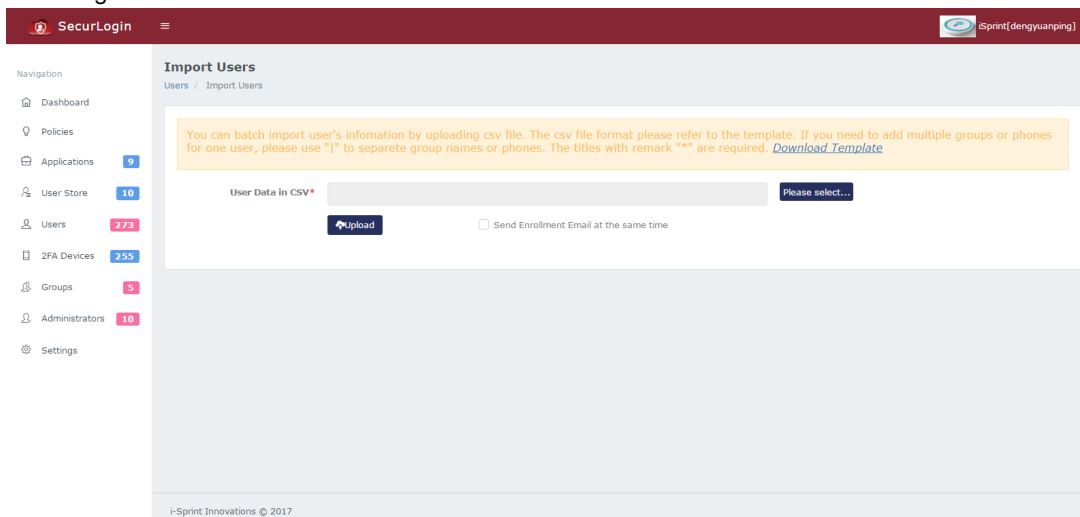
8.2 New User

Clicking Users > New User, or clicking the +New User at the right upper corner of Users page to display New User page. Administrator can fill user info and click Save to create a user manually.



8.3 Import User

Clicking Users > Import Users to go to Import Users page. Click Download Template, and fill the desired user info, and click Save. Back to this page, and click Please select... to located filled template file, and click Upload. The system will send registration email if user checks Send Enrollment Email at the same time next to Upload button. Remark: please create the group inside SecurLogin, and the fill the created group name on the template. The import will be failed if there no such group in SecurLogin.



The import result will display upon running the import task, and it includes successful imported user list, failure list and reason.

Import Users
Users / Import Users

You can batch import user's information by uploading csv file. The csv file format please refer to the template. If you need to add multiple groups or phones for one user, please use "|" to separate group names or phones. The titles with remark "*" are required. [Download Template](#)

User Data in CSV* ImportUsers_CN.csv Please select...

Send Enrollment Email at the same time

SUCCESSFUL IMPORT LIST

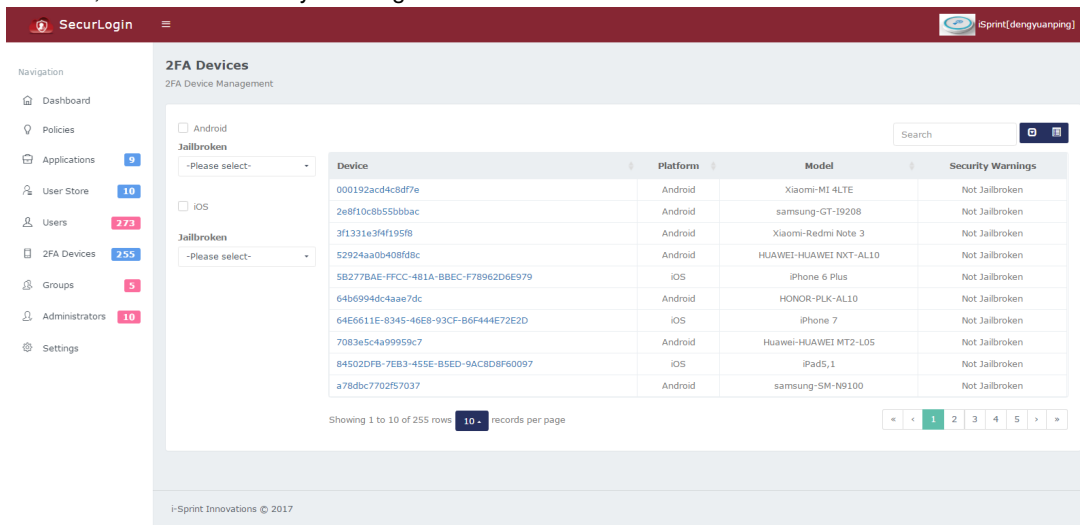
User ID	First Name	Last Name	Email
No matching records found			

IMPORT FAILED LIST

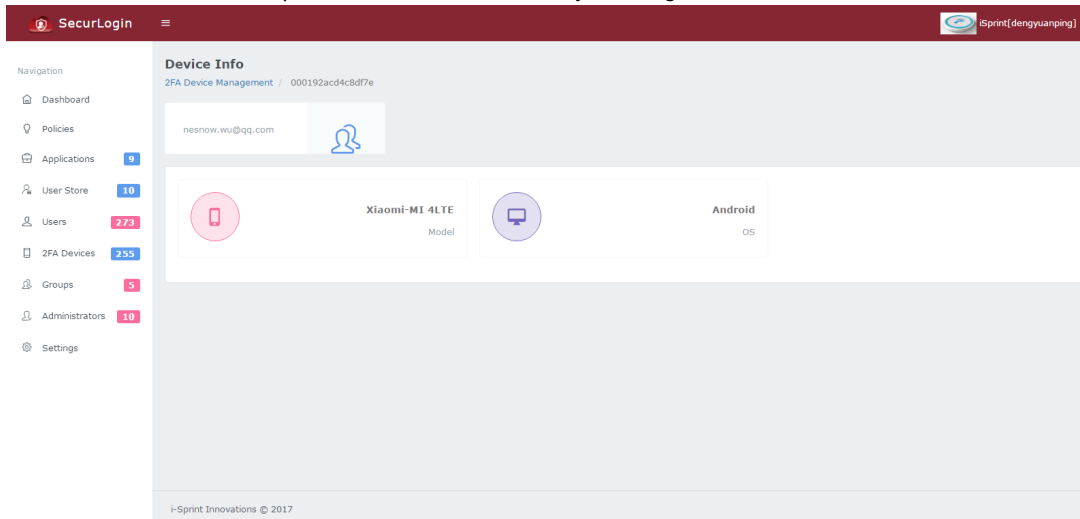
User ID	First Name	Last Name	Email	Cause of Failure
No matching records found				


9. 2FA Devices

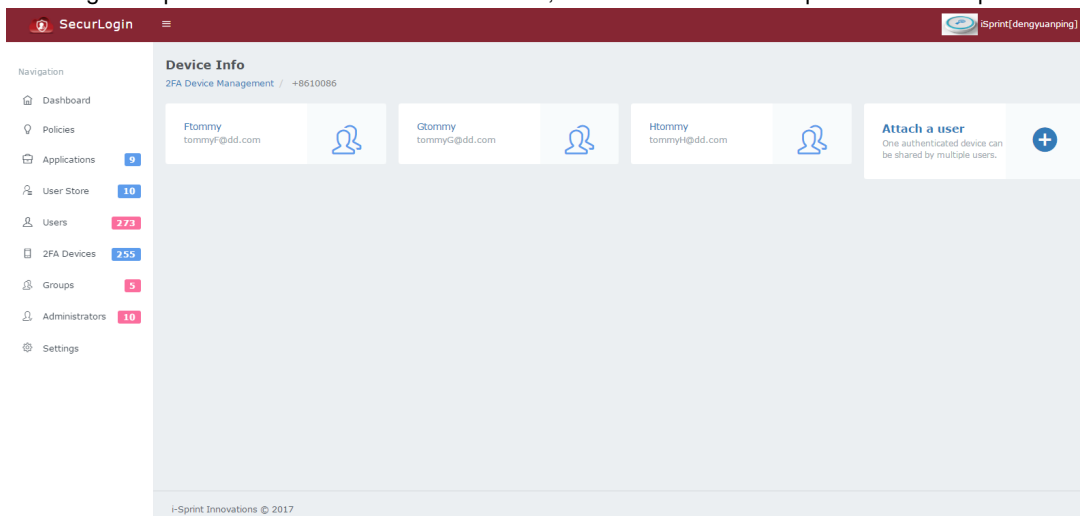
Administrator can view all enterprise user devices info upon user installed SecurLogin mobile app and download a token, such as Platform, Model and Security Warnings info.



Click a device ID that has platform, model, and security warning info on Device to view device info.



Click a phone number that does not have platform etc. from Device to view associated users' info. Click  icon to attach a user, i.e. assign this phone number for more users to use; users can use the new phone number upon successful enrollment.



10. Groups

10.1 Groups

Click Groups to view all the groups.

The screenshot shows the 'Groups' management interface. On the left is a navigation menu with items like Dashboard, Policies, Applications, User Store, Users, 2FA Devices, Groups, Administrators, and Settings. The main content area is titled 'Groups' and contains a table with the following data:

ID	User Store	Group UUID	Group Name	Description	2FA Control	Edit
1		9d6f29b6-2595-4156-8ee2-98657e1b33bc	DemoGroup		By Pass	Edit
2		e58fa129-0db7-4d21-98f9-a33e4e2b5349	aa		Activated	Edit
3		c8cd0cf4-1ec4-46ee-a79d-394255f3dc15	群组aa		Activated	Edit
4		1dcdde062-afbc-4d37-b1e6-758cb1b95ed0	BOSS Group	用于Boss系统的二次认证	Activated	Edit
5		6dee389b-5dc0-41f9-976c-a62bc497d38e	testGroup01	testGroup01	Activated	Edit

Below the table, it says 'Showing 1 to 5 of 5 rows'. At the bottom left, there is a copyright notice: 'i-Sprint Innovations © 2017'.

Click the Edit button of desired group to modify the group login policy or delete the group.

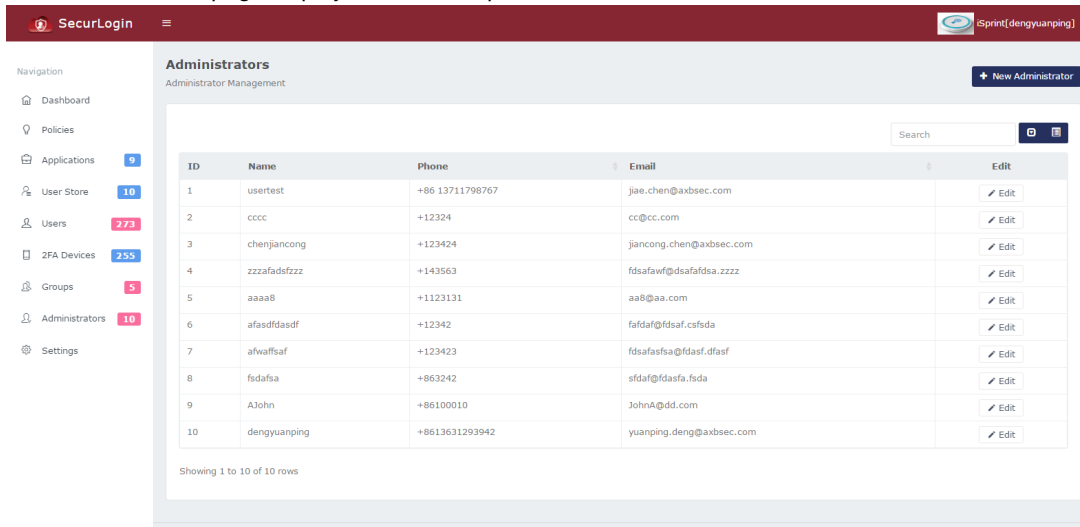
The screenshot shows the 'Edit Group' page. The navigation menu is the same as in the previous screenshot. The main content area is titled 'Edit Group' and contains a form with the following fields:

- Group UUID:** 9d6f29b6-2595-4156-8ee2-98657e1b33bc
- Group Name:** DemoGroup
- Description:** (Empty text area)
- 2FA Control:**
 - Activated: Require two-factor authentication
 - By Pass: Skip two-factor authentication
 - Disabled: Automatically deny access

Below the 2FA Control section, there is a note: 'This 2FA control applies to all of the users in this group.' At the bottom of the page, there is a 'Users' section with a search bar.

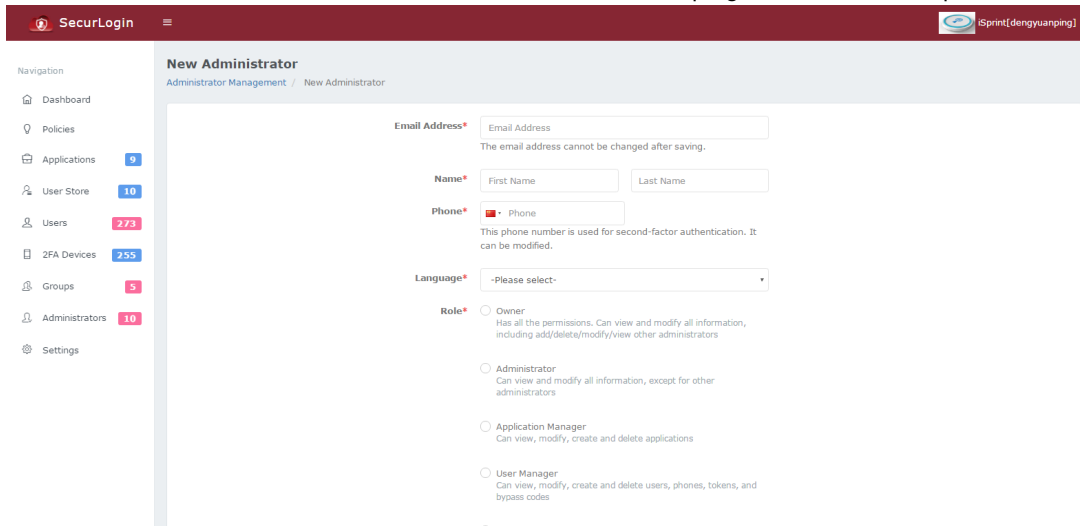
11. Administrators

The Administrators page displays all the enterprise administrator info.



Click the Edit button of desired administrator to modify info or delete it.

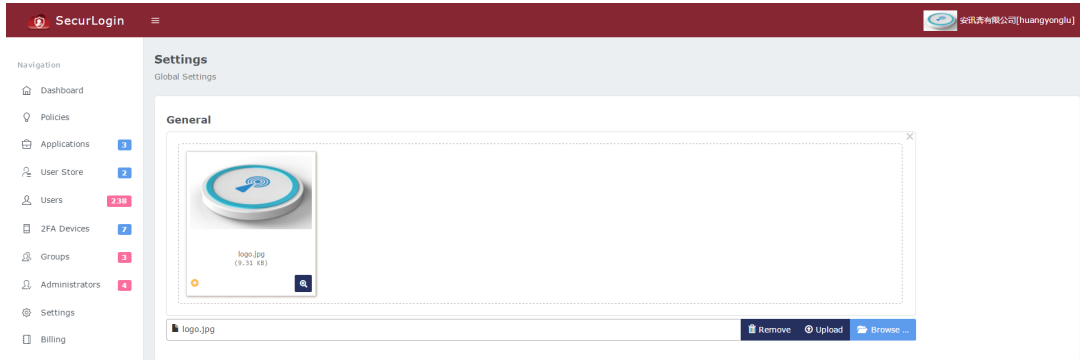
To create an administrator, click the + New Administrator at the top right corner, fill the required fields, and click Save finally.



12. Settings

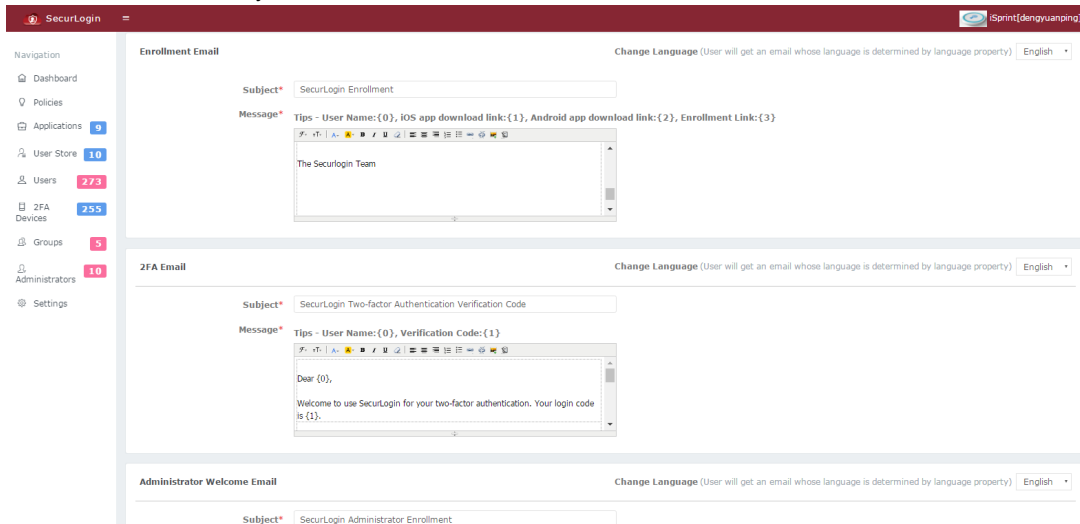
12.1 General

Administrator can add enterprise logo by Settings > General. Click Please select... button, locate desired logo in PNG format, and click Open. The logo will display at the top right corner.



12.2 Email Templates

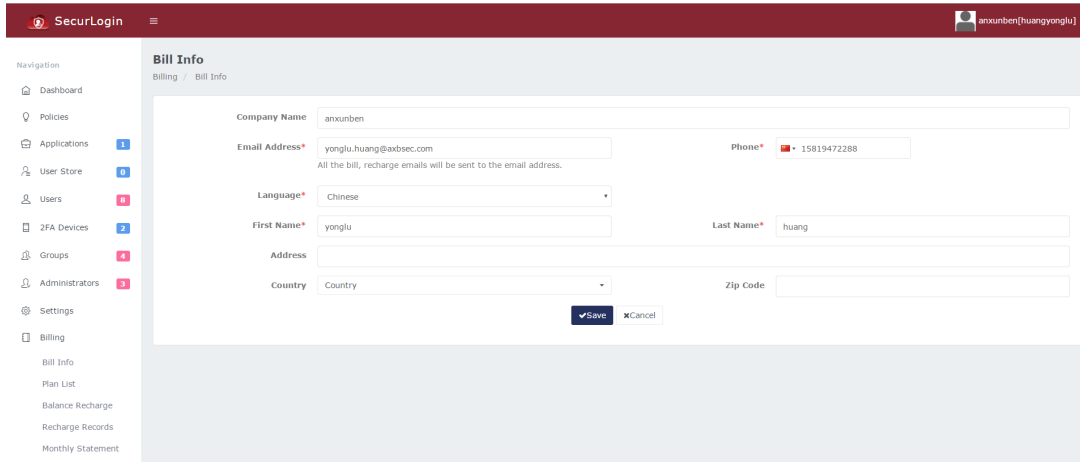
Below the General setting, there are email templates, i.e. Enrollment Email, 2FA Email and Administrator Welcome Email. Administrator can modify them if needed.



13. Billing

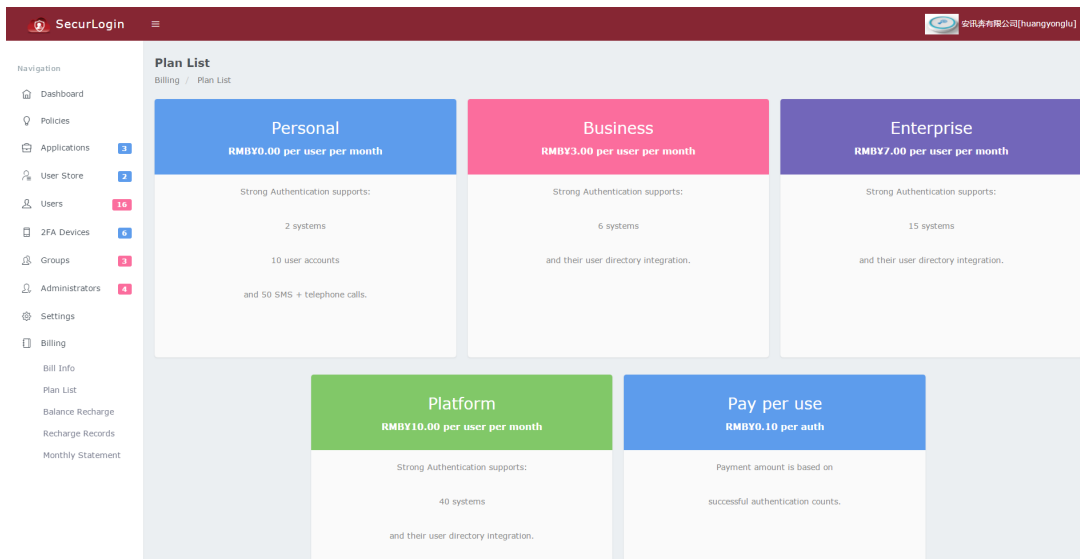
13.1 Bill Info

Administrator can go to Billing > Bill Info to view company basic info.

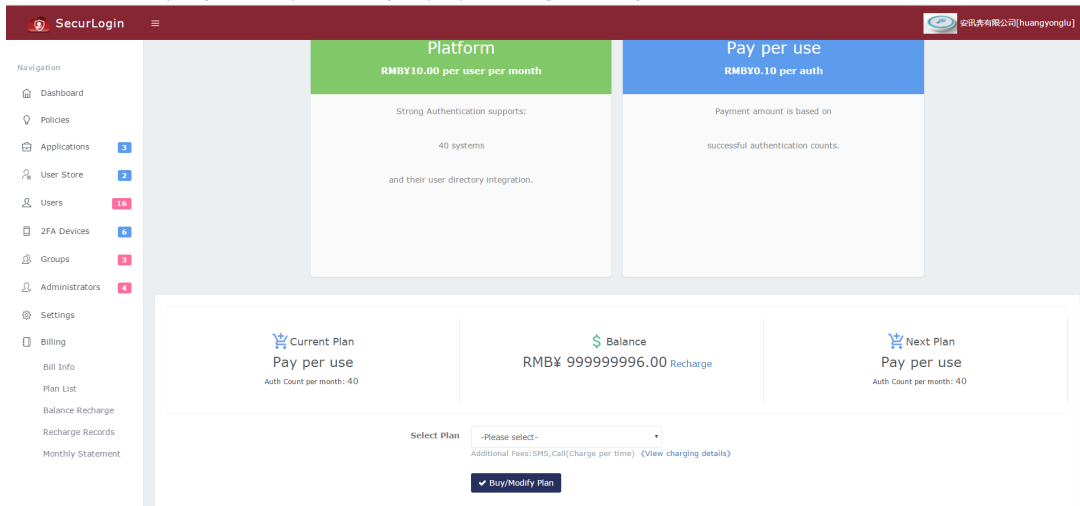


13.2. Plan List

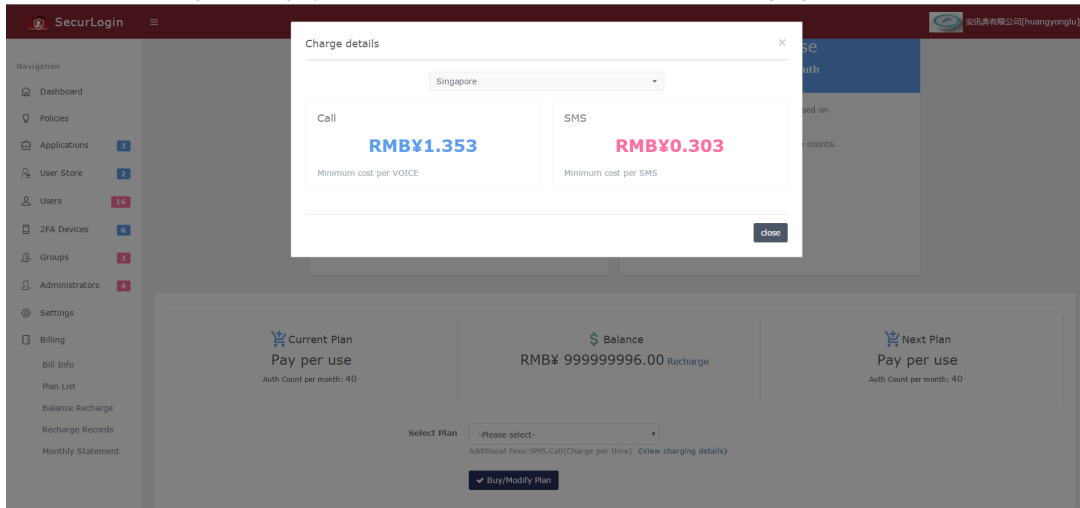
Administrators can go to Plan List page by Billing > Plan List. There are different payment plans for 2FA, and administrator can select a desired one.



Select or modify a plan for your company by clicking the drop-down list of Select Plan at the bottom of page.

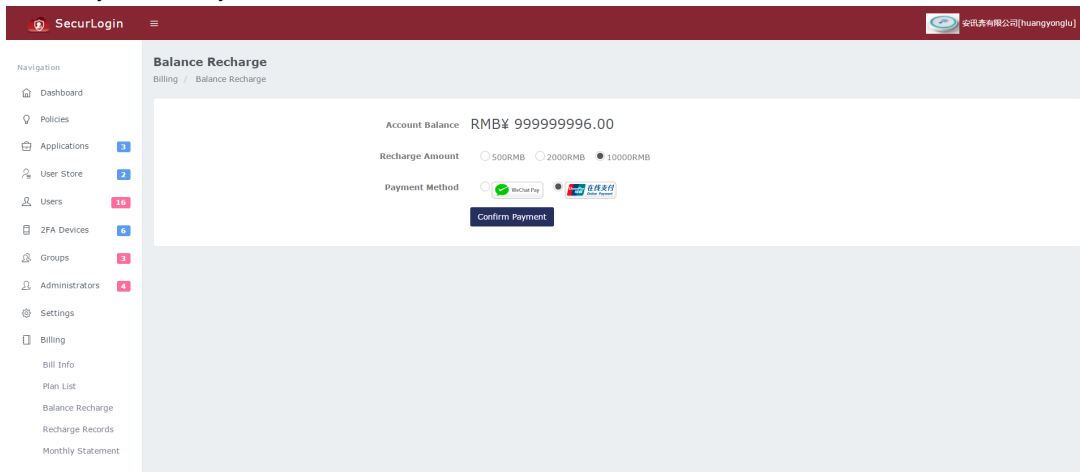


Users are also required to pay for the SMS and Call fee. Click View charging details to view SMS and Call payment info.



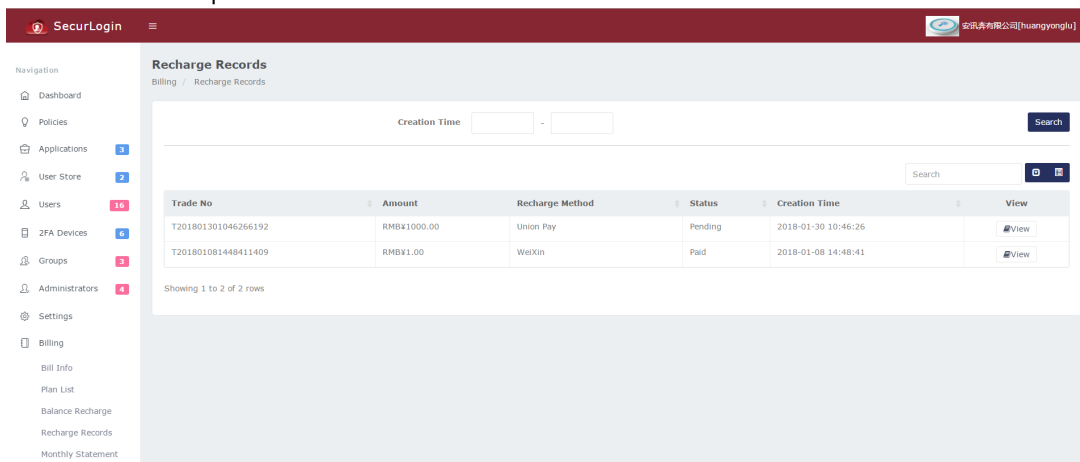
13.3 Balance Recharge

Go to Balance Recharge page by clicking Billing > Balance Recharge, and user can view Account Balance and recharge. There are three recharge amounts, i.e. 5000RMB, 2000RMB and 10000RMB, and the Payment Method can be WeChat Pay or China UnionPay Online Payment.

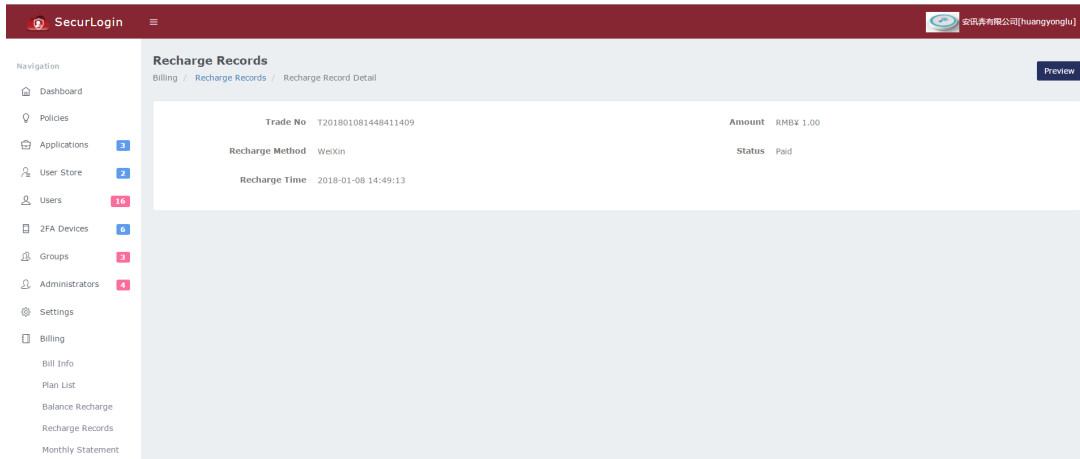


13.4 Recharge Records

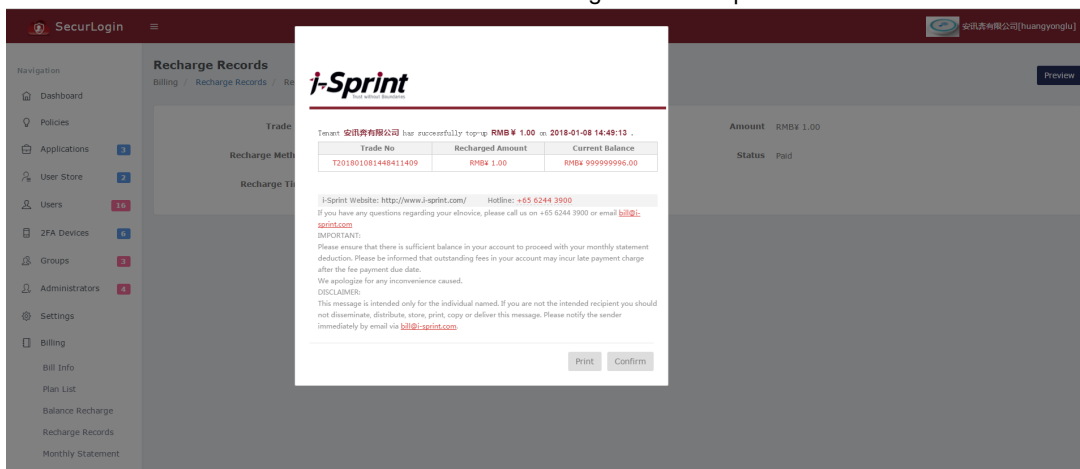
Administrators can view all recharge records by Billing > Recharge Records. Enter or select certain Creation Time to view the records within the specified time.



Select a desired recharge record and click View button to view the details. There will be a Continue Payment button at the right hand corner of the details page if the recharge status is Pending.

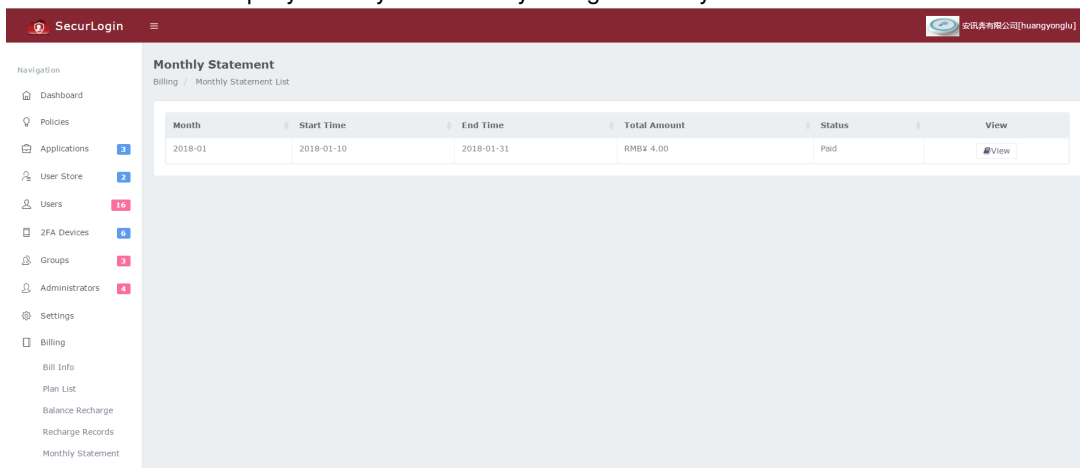


On the detail page of recharge record whose status is Paid, click Preview button at the upper right corner to view the Recharge Amount and Current Balance. Click Print button at the right bottom to print it.

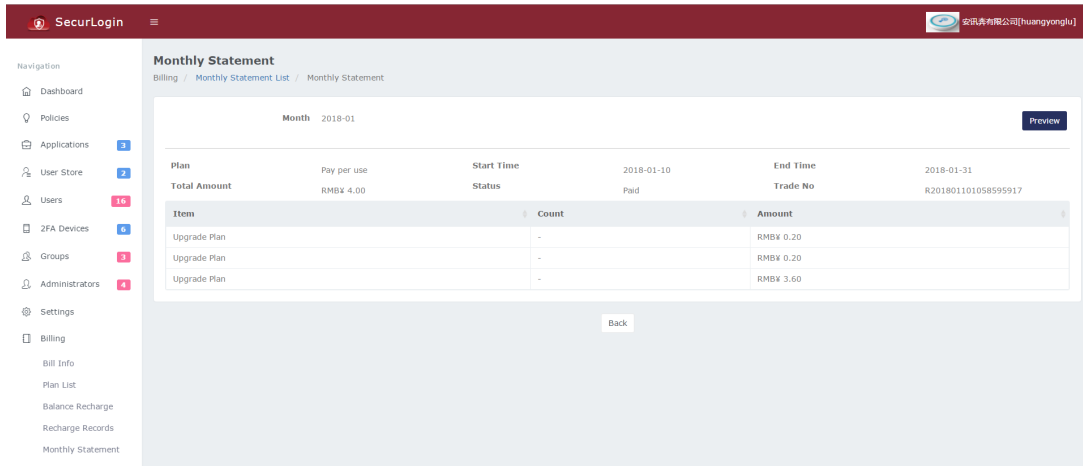


13.5 Monthly Statement

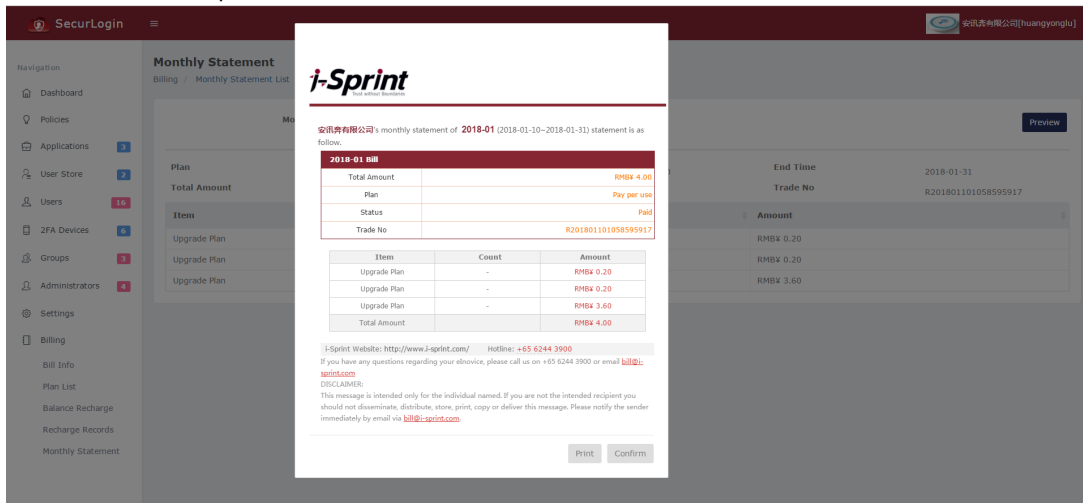
User can view the company monthly statement by Billing > Monthly Statement.



Click View button to view the monthly statement details. Click Preview button to display charging details for the monthly statement.



Click Print button to print it.



14. Client App 2FA Authentication

14.1 Push Login Message

SecurLogin client app user can click Confirm of the push login message to complete 2FA authentication upon successful installation of SecurLogin mobile app.



Login

Login Time: 2018-01-30 15:05:50

User: demoUser

Application: Demo Application

Location: China

Confirm

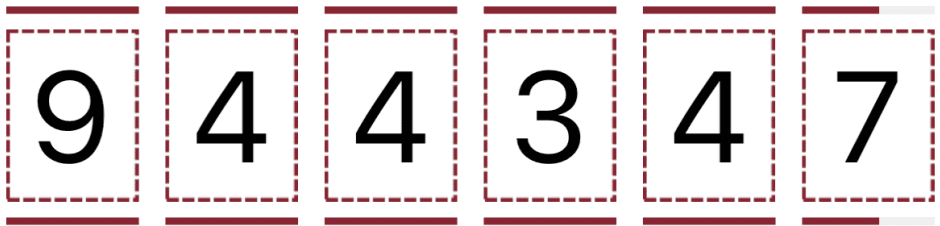
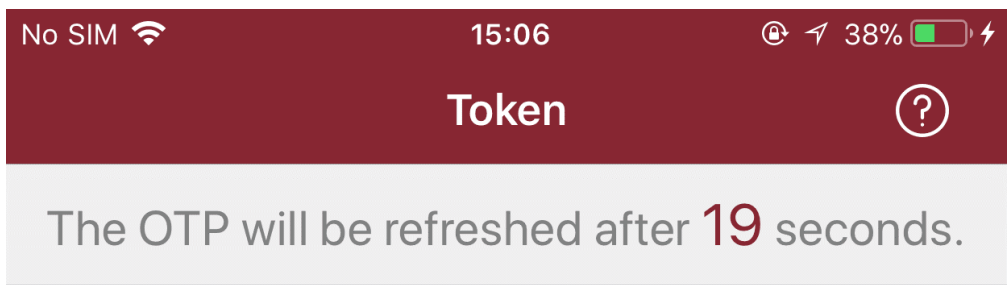
Reject



Close

14.2 OTP by Virtual Token


Upon complete first factor authentication, to use virtual token of SecurLogin to complete 2FA authentication, user need to click the token of SecurLogin mobile app, enter the code to target app/system. User can use virtual token to generate new OTP any time when needed, and it can work without Internet.





SecurLogin Supports


2FA authentication for various VPN devices, web apps
and local apps.


Register a SecurLogin enterprise account now
to protect your assets and users securely.


Token


Apps


QR


History


Me