I.X Trio Administration Guide

Version: 1.09

Contents

Apply Trio Domain

Manage Trio Service for Your Company

Apply Trio Domain

1. Register a new Trio domain

For any enterprise who want to use I.X Trio service, you will need to register a Trio domain. If you have registered trial program on Trio web site, please ignore this section and skip to Manage Trio Service for Your Company. If you haven't registered any Trio domain, please visit the following URL:
https://service.ix-security.com/console/#/signup

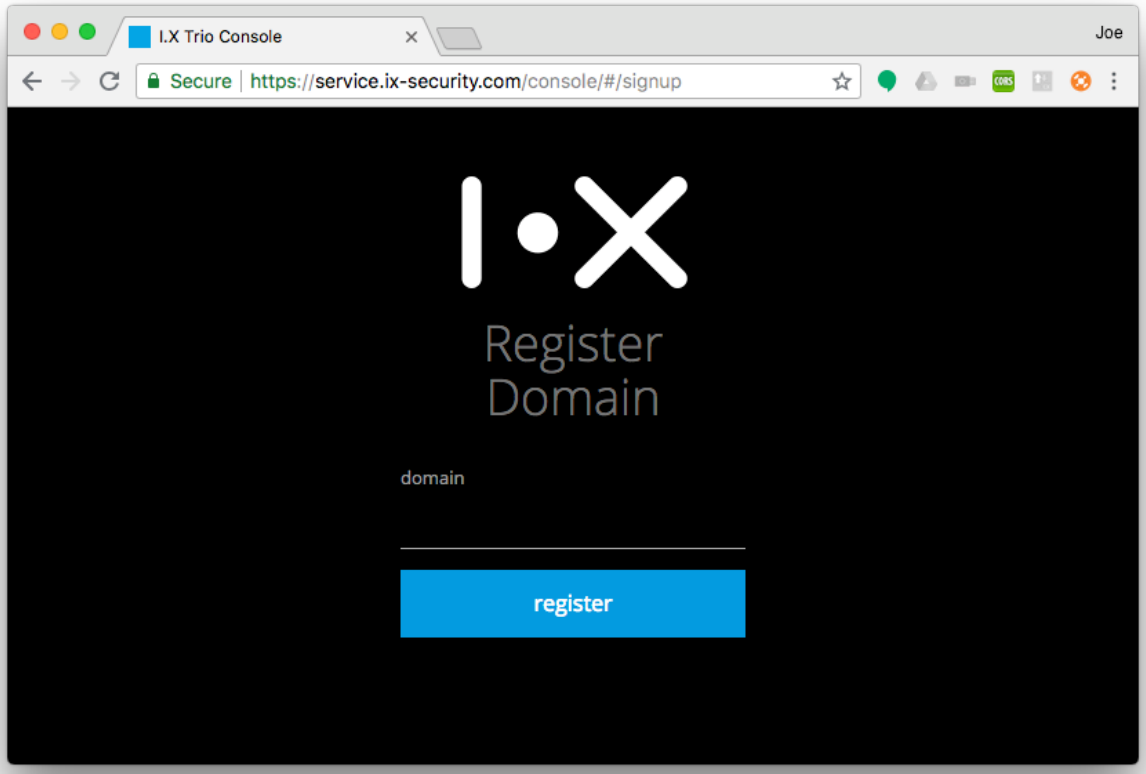


FIG. 1-1 TRIO DOMAIN REGISTRATION SCREEN 1

Input your domain name, e.g.: yourdomain.com, press "register" button. Make sure you own this domain with r2admin@yourdomain.com email account / alias.

Once the domain name is verified, it will show a screen as follows:

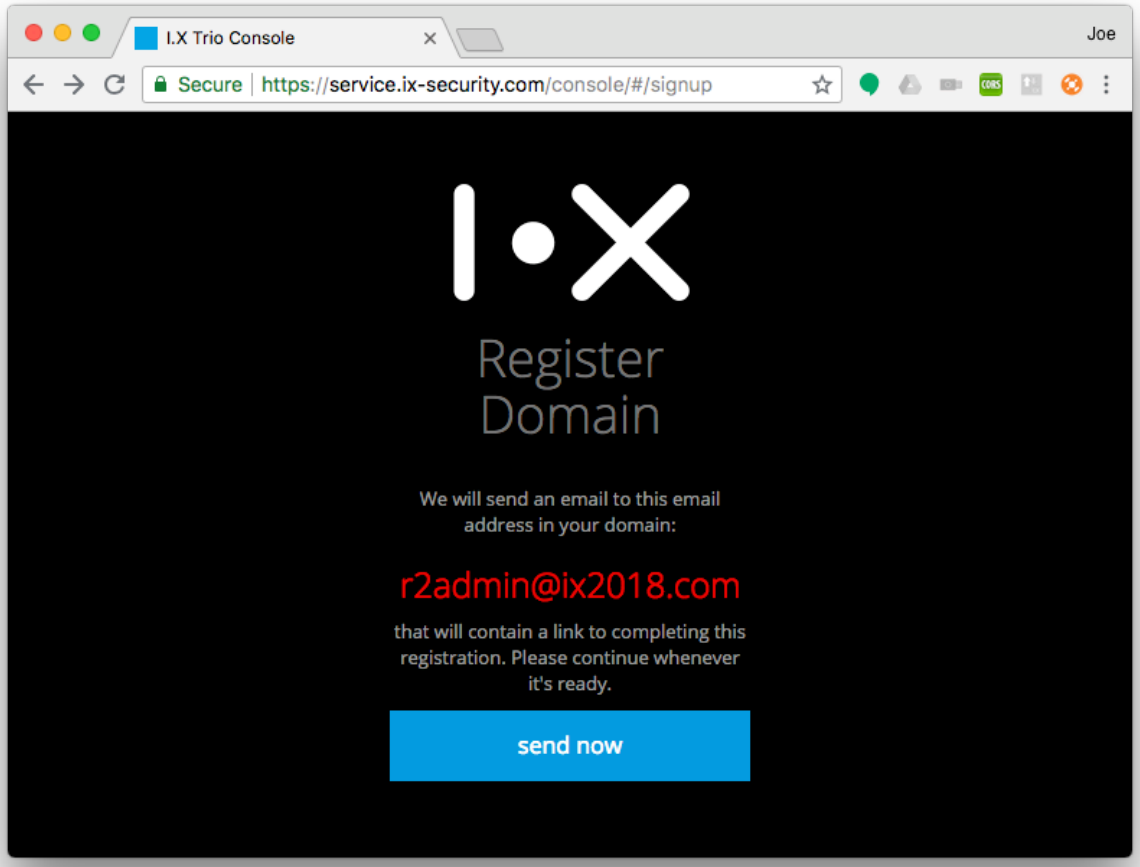


FIG. 1-2 TRIO DOMAIN REGISTRATION SCREEN 2

2. Create Trio administrator's email account

Please remember to create an email account of email alias of r2admin@yourdomain.com, click "send now" will send a domain activation email to r2admin@yourdomain.com.

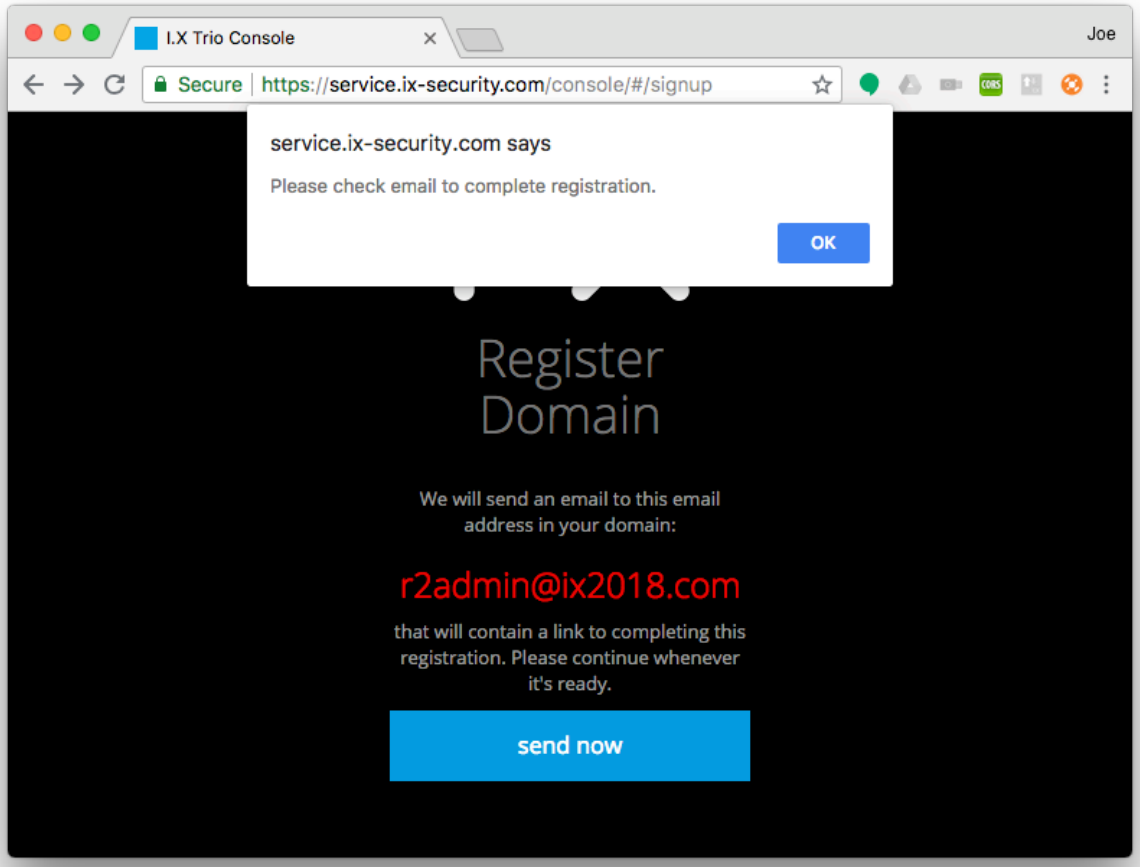


FIG. 2-1 TRIO DOMAIN REGISTRATION SCREEN 3

3. Confirm in activation email

The following is an example of domain activation email:

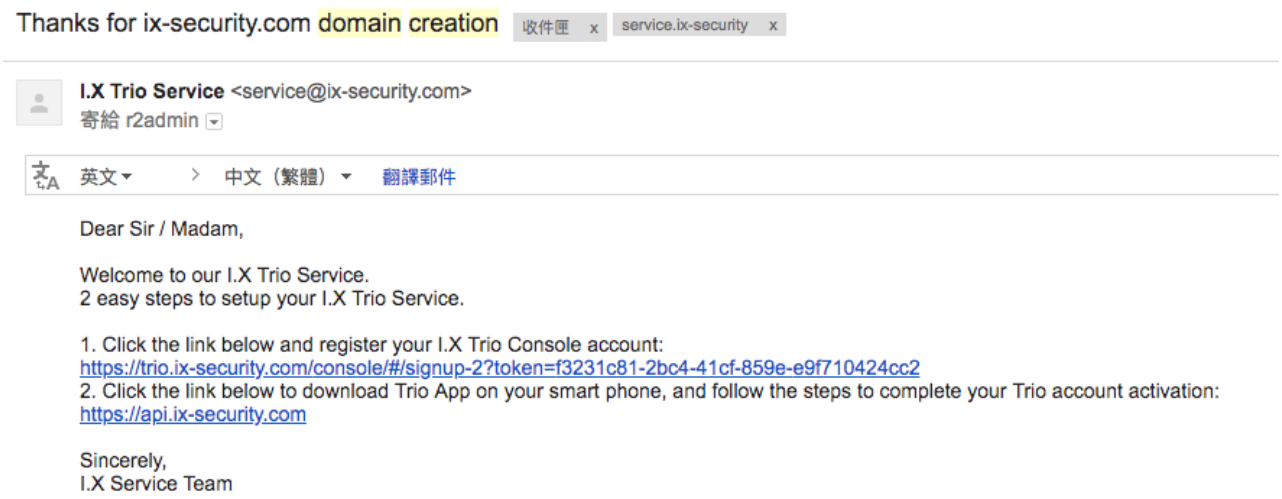


FIG. 3-1 TRIO DOMAIN ACTIVATION EMAIL

If you don’t receive it, please examine if the email account / alias is setup correctly, or examine if it’s filtered as a spam email.

4. Install I.X Trio App

Please visit the following URL to download I.X Trio App

https://www.ix-security.com/download/trio/app.html

Follow the application setup process, to finish Trio account registration process. Here you could use your own email to setup the Trio App.

5. Register administrator's email account in Trio Console

Once you finish Trio account registration on Trio App, please check the domain activation email, and click the link to register your account as Trio administrator of your domain.

https://trio.ix-security.com/console/#/signup-2?token=f3231c81-2bc4-41cf-859e-e9f710424cc2

The web page will guide you to setup email / password for Trio domain administrator.

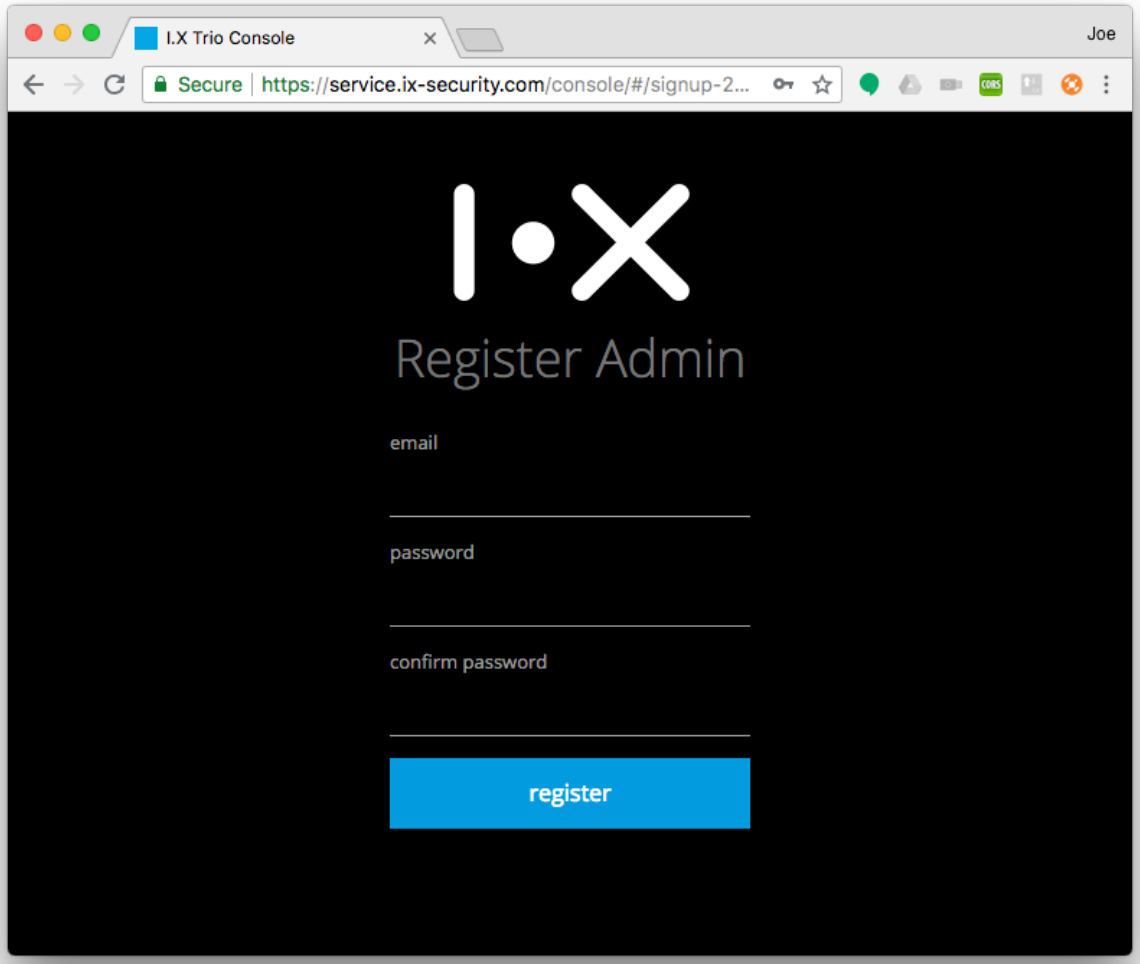


FIG. 5-1 DOMAIN ADMINISTRATOR ACCOUNT SETUP SCREEN

Follow the web page, fill the necessary information and press “register” button. If all data are filled correctly, it will pop up setup complete and redirect to Trio Console login screen.

Start managing Trio service for your domain!

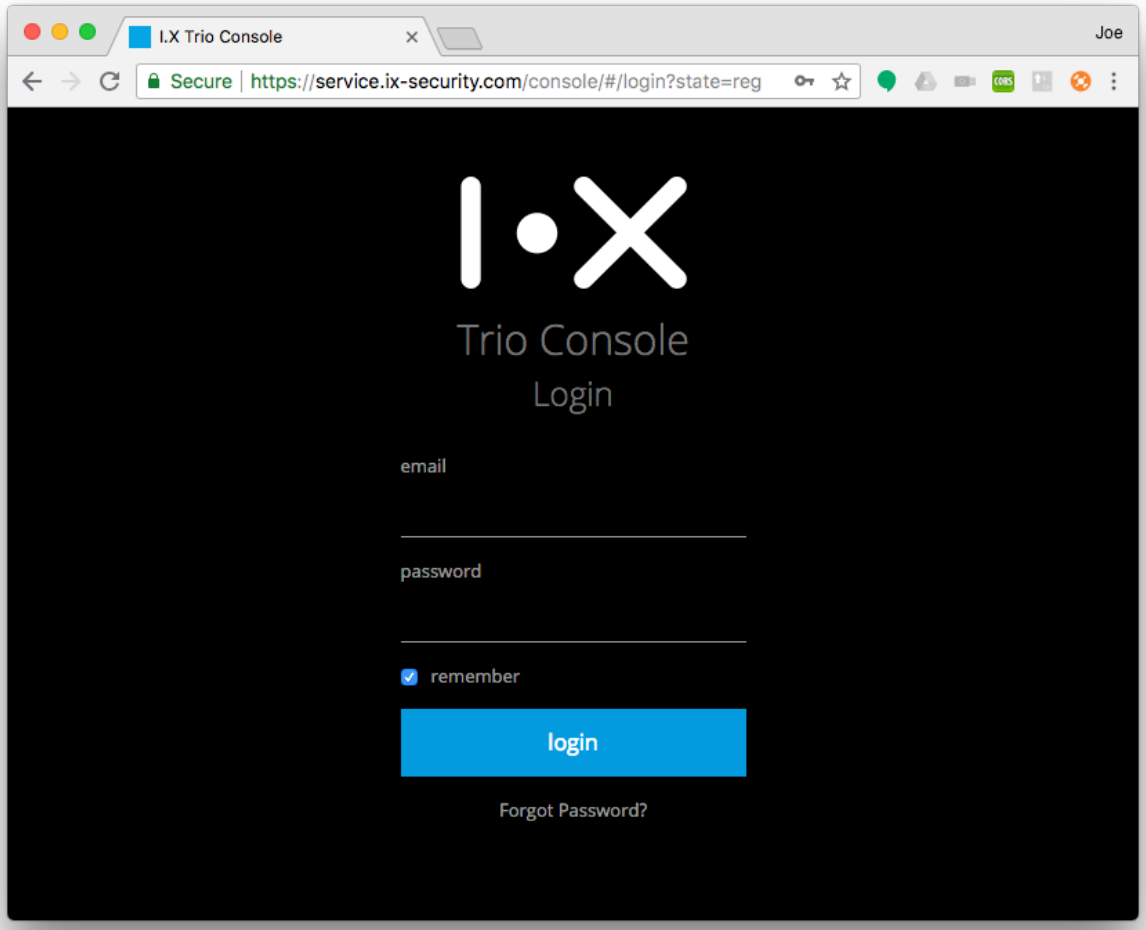


FIG. 6-1 TRIO ADMINISTRATION CONSOLE LOGIN SCREEN

Manage Trio Service for Your Company

1. Login Trio Console

Only Trio administrator can login Trio console. Before login, please make sure:

- your smartphone can connect to Internet
- smartphone Bluetooth setting is ON
- Trio Key is power-on, and in the range the your smartphone can discover and connect.

Input your email and password (please note this password is setup when you register administrator email account for Trio Console).

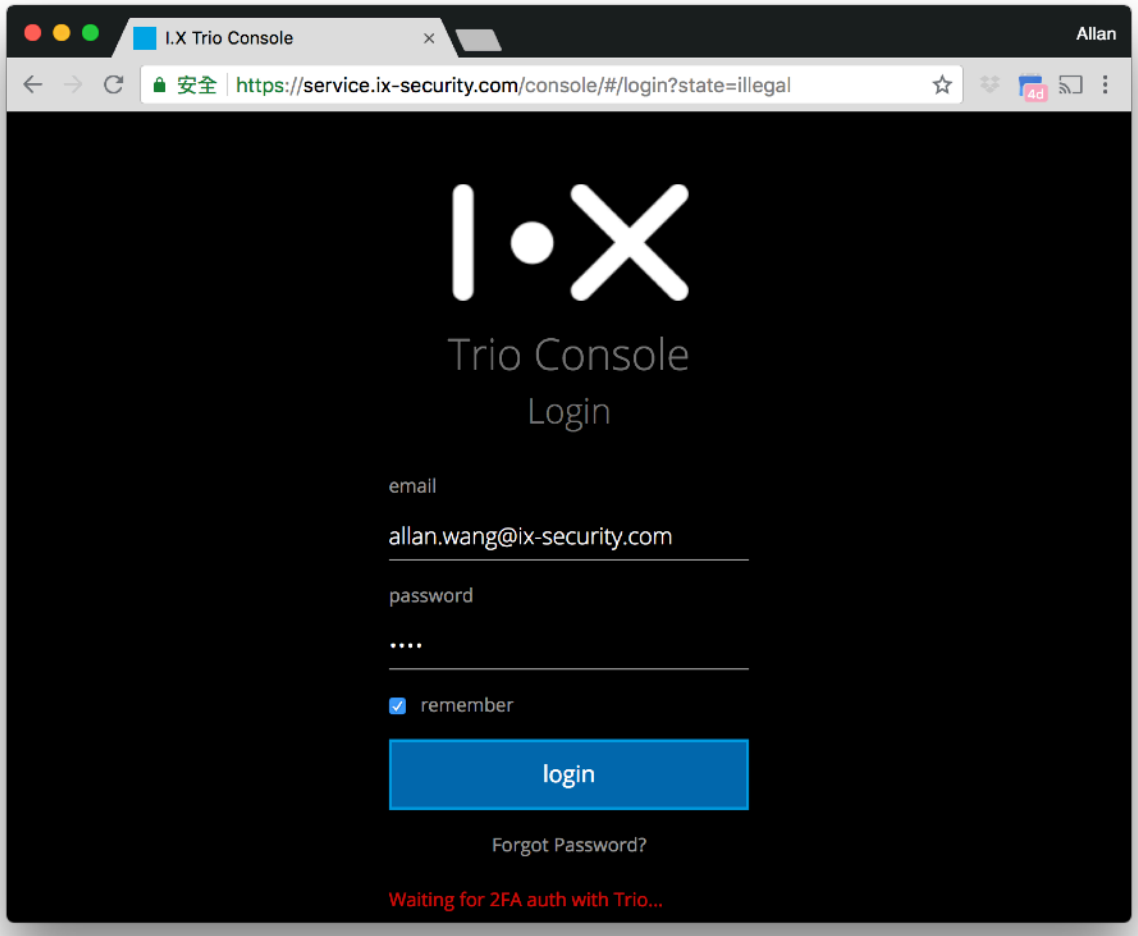


FIG. 1-1 TRIO CONSOLE LOGIN SCREEN

During login, if account / password is input correctly, the system will send a two-factor authentication (2FA) push notification to your smartphone.

2. Power on Trio Key, approve in 2FA notification

After your smartphone receive 2FA notification, click it to open this authentication page. Confirm the login action by pressing “Approve” button.

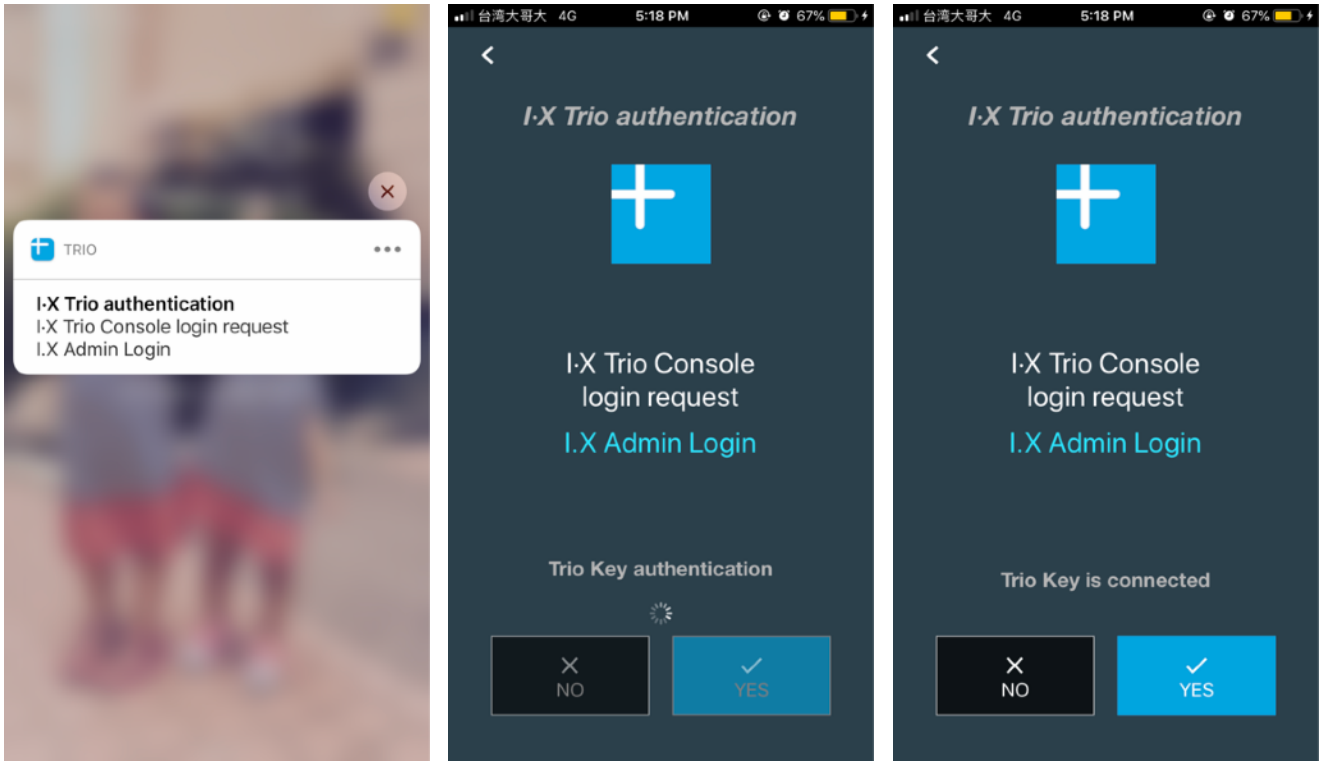


FIG. 2-1 2FA NOTIFICATION SCREEN ON SMARTPHONE

3. Trio Console Functionality

The left panel is function category, and the right panel is detail function of the selected category:

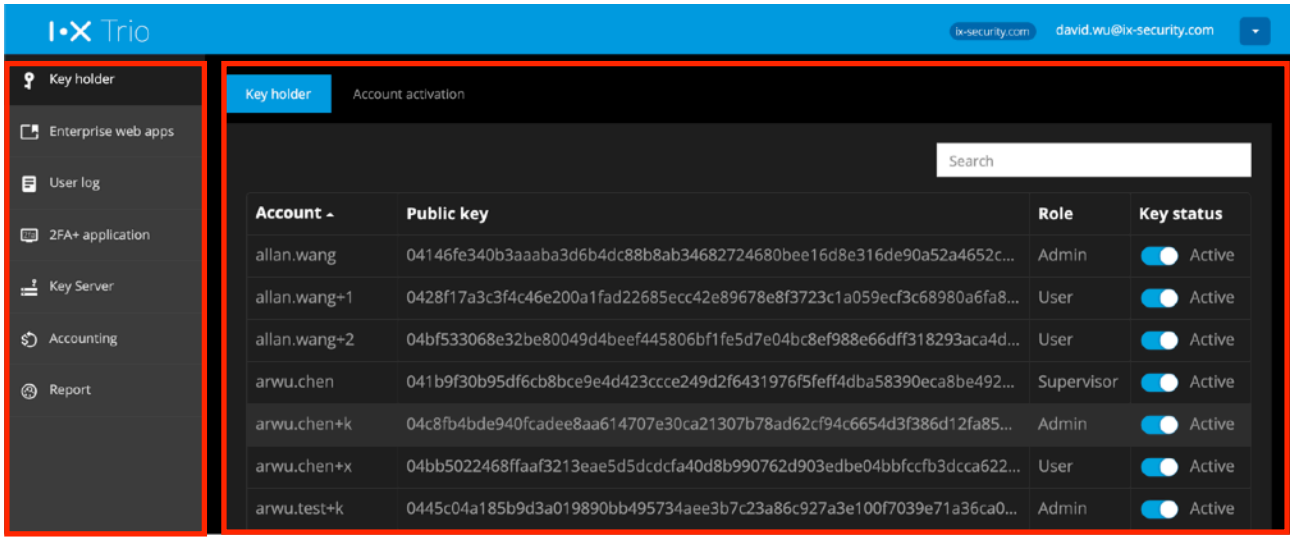


FIG. 3-1 TRIO CONSOLE FUNCTION LAYOUT

3.1. Key holder

Here you can manage every user's key status and access right

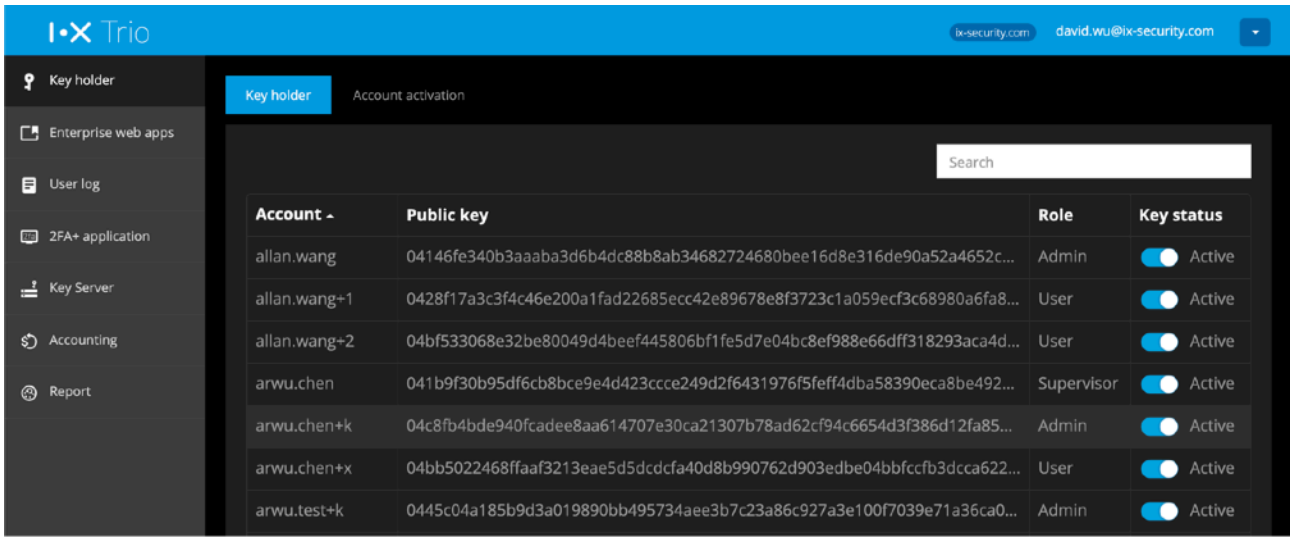


FIG. 3.1-1 MANAGE TRIO USER IN YOUR DOMAIN

3.1.1.Key status

Only when the user account is still active, then this user will be allowed to use Trio service and decrypt Trio protected conversation and documents. Administrator can disable any Trio user account when necessary.

3.1.2.Edit - Edit permission

Administrator can edit permission for any user account, including:

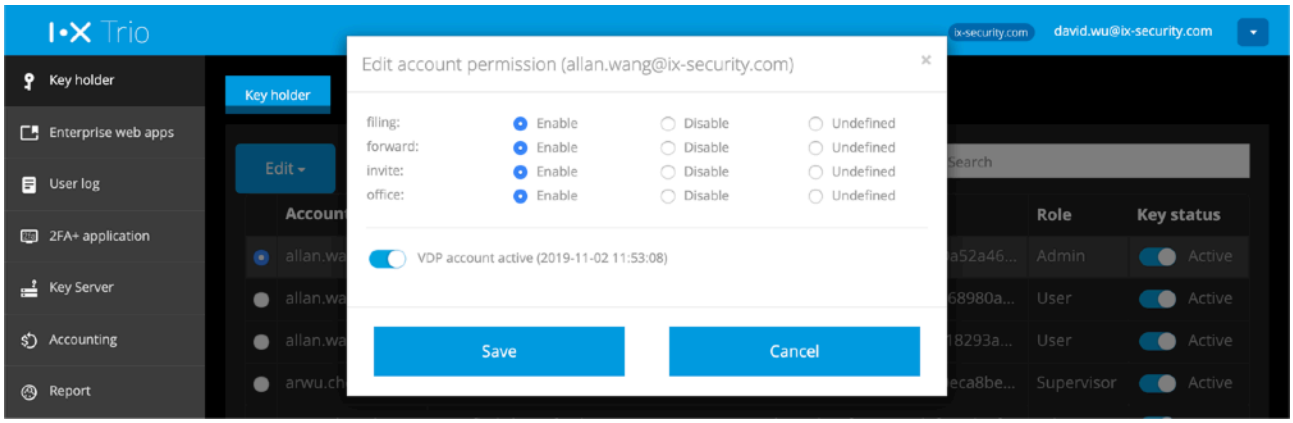


FIG. 3.1.2-1 SETUP USER'S PERMISSION

- filing - enable to allow user to export IM conversation content
- forward - enable to forward document to other IM channels
- invite - enable to invite external Trio contacts to IM channel
- office - enable to allow user open office file format on user's smartphone
- VDP - enable to activate user to use Trio secure editing solution (TrustView VDP, please note that Trio secure editing service should be subscribed for this domain)

3.1.3.Edit - Assign role

You could assign specific user to Console admin or Supervisor.

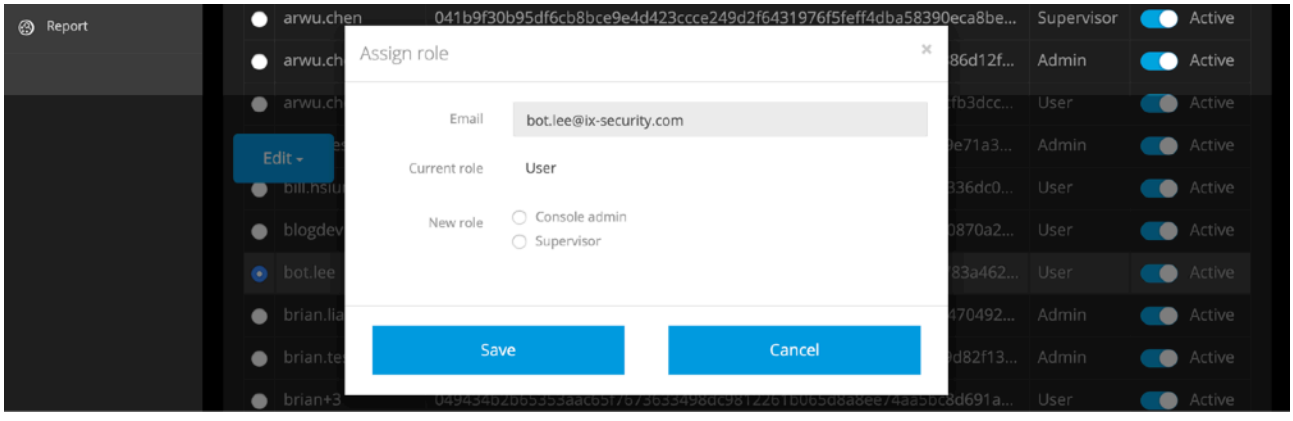


FIG. 3.1.3-1 UPGRADE USER TO ADMINISTRATOR

- Administrator

Trio administrator is the main user to Trio Console, can manage user's key status, access right, web applications for secure browser, and 2FA applications.

Administrator can promote other users to be administrator. Once a user is promoted, he can login Trio Console.

- Supervisor

Supervisor is generally the role of CEO or CIO. Supervisor has special access right to decrypt any IM channel content.

When there is no supervisor been setup, administrator can promote one user to be supervisor. Once this domain has supervisors, any more supervisor promotion would require one of the supervisors to approve.

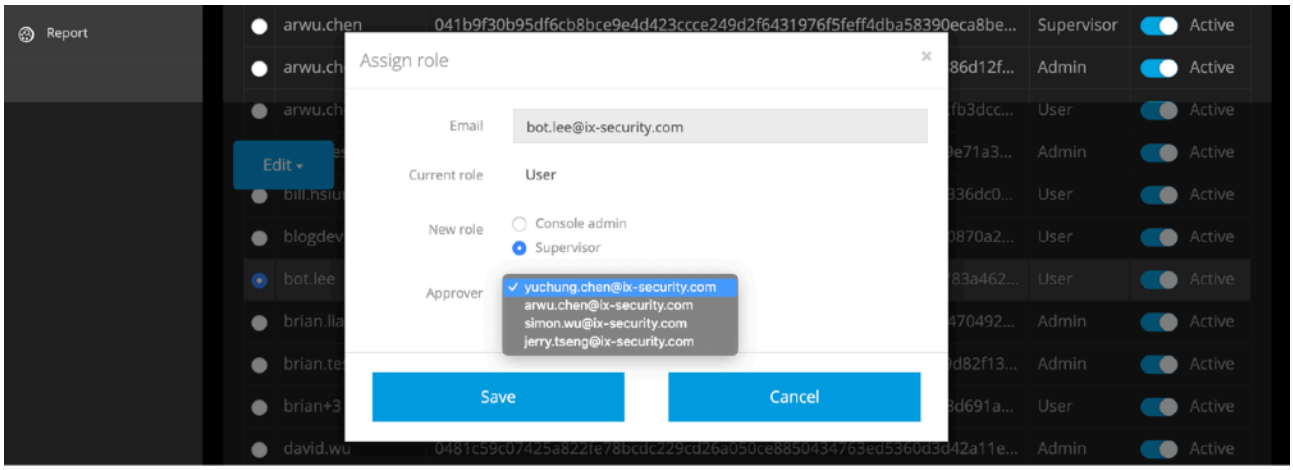


FIG. 3.1.3-2 UPGRADE USER TO SUPERVISOR

3.1.4.Edit - Account activation

If your company use G Suite or other cloud email service and would like to use Trio SAML gateway to protect, users might not be able to access email account before Trio account registration. In this condition, administrator can use this function to setup alternative email for users, such that the user can finish Trio account registration. Once the alternative email for the specified Trio account is setup, when the user register Trio service, the account activation email will be sent to alternative email as well. Note that such alternative email is only valid for 24 hours. For new employee to Trio service, you may switch to Account activation tab, and press “Create new activation” to setup alternative email for the user.

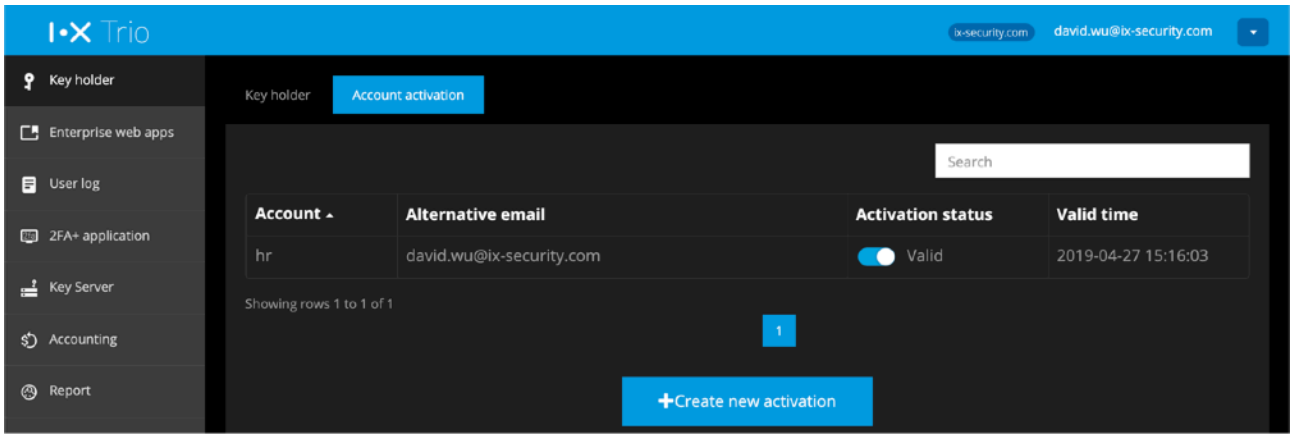


FIG. 3.1.4-1 MANAGE NEW USERS IN ACCOUNT ACTIVATION TAB

After pressing “Create new activation”, you will see dialog as follows:

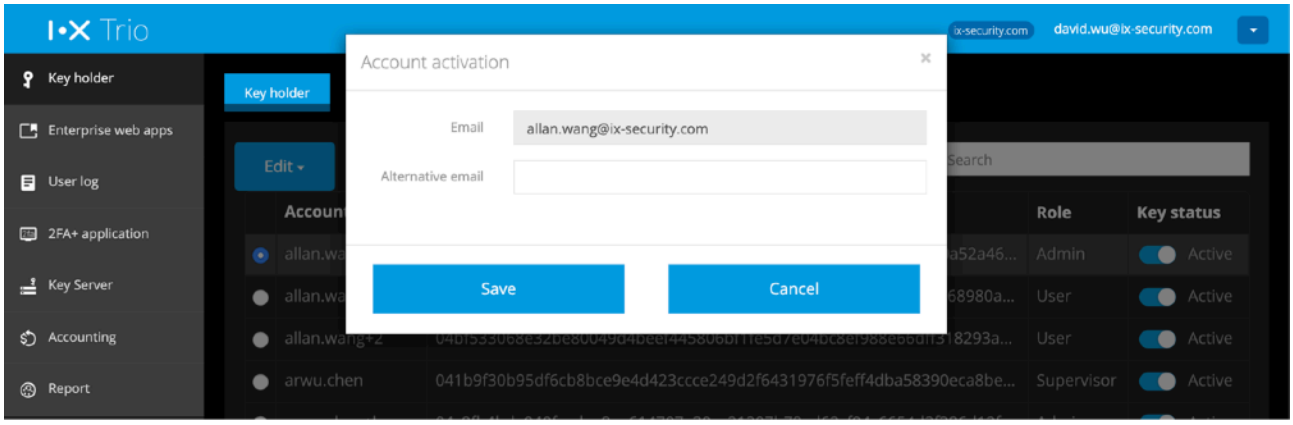


FIG. 3.1.4-2 ACCOUNT ACTIVATION SETUP DIALOG

For users who need to replace smartphone or re-install Trio App such that the email cannot be accessed, can follow this way to activate Trio account.

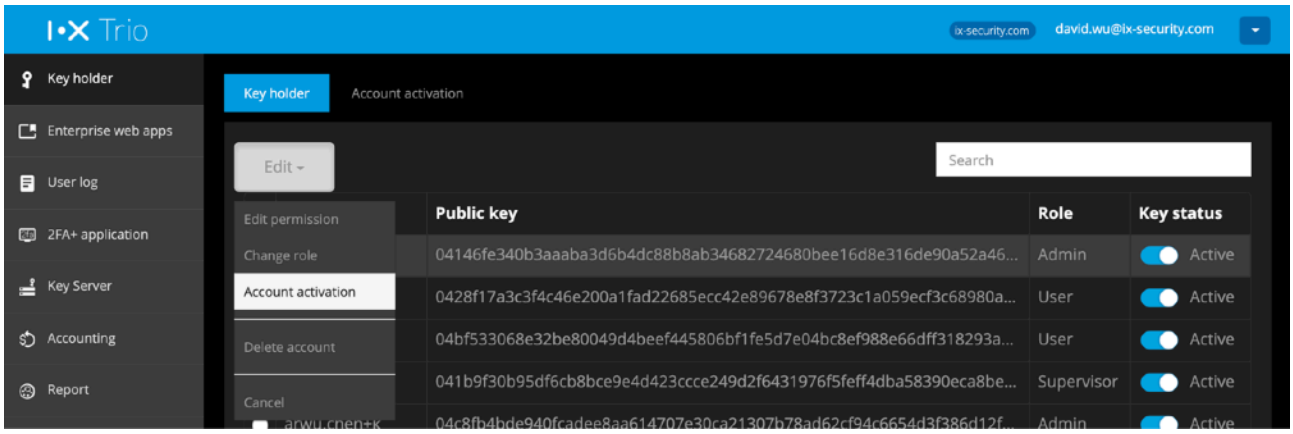


FIG. 3.1.4-3 SETUP ACCOUNT ACTIVATION FOR SPECIFIC ACCOUNT

Please notice that when the employee finish account registration, or user doesn’t activate the account within 24 hours, such alternative email setting will be disabled. Administrator can edit such setting per account, to modify email setting or activate.

3.2. Cloud Gateway

I.X Cloud Gateway can verify all packets’ access control in real time, only allow authorized users to access each enterprise web app. Packets without valid digital signature will be blocked, such that the systems can prevent hacker’s attack.

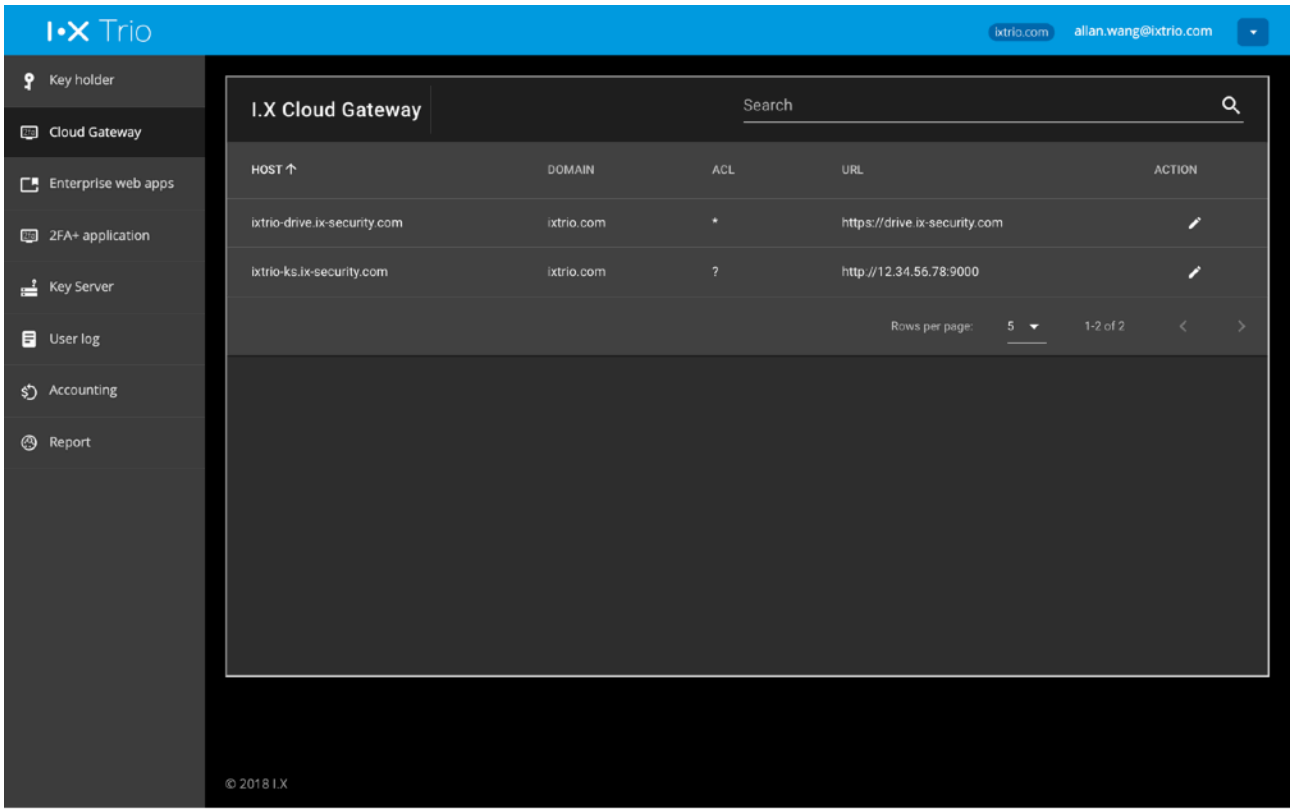


FIG. 3.2-1 I.X CLOUD GATEWAY 畫面

Click edit icon, you will see a dialog to configure in I.X Cloud Gateway, parameters are listed as follows:

Parameter	Description
HOST	Assigned by I.X, it's the URL mapped by I.X Cloud Gateway, cannot edit (please contact I.X support if customization is needed) Once IT admin get the URL of corresponding enterprise web app, then it should be configured in URL parameter of the enterprise web app
DOMAIN	Assigned by I.X, it's Trio domain name, cannot edit
URL	Assigned by IT admin, it's public IP address or URL of this enterprise web app,
ACL	Assigned by IT admin, it's access control configuration, parameters as follows: • ? - Cloud Gateway won't verify digital signature • * - Cloud Gateway allow request with any Trio digital signature to access this host • @ - Cloud Gateway allow request with Trio digital signature from this domain to access this host • ["user1@DOMAIN", "user2@DOMAIN", "user3@DOMAIN", …] - Cloud Gateway only allow the white list users to access this host, please use email list to define this white list.

3.3. Enterprise web apps

Trio has built-in secure browser, to access your enterprise web app securely, e.g., webmail, ERP system. The secure browser can prevent data downloaded, content copied to clipboard, and screen capture on user device.

For more intranet services, you could configure them here to let mobile workers access them securely. The setup need to adapt to settings in I.X Cloud Gateway, such that you can control access right and prevent unauthorized user to access your intranet services. For more details, please check 3.2.1.

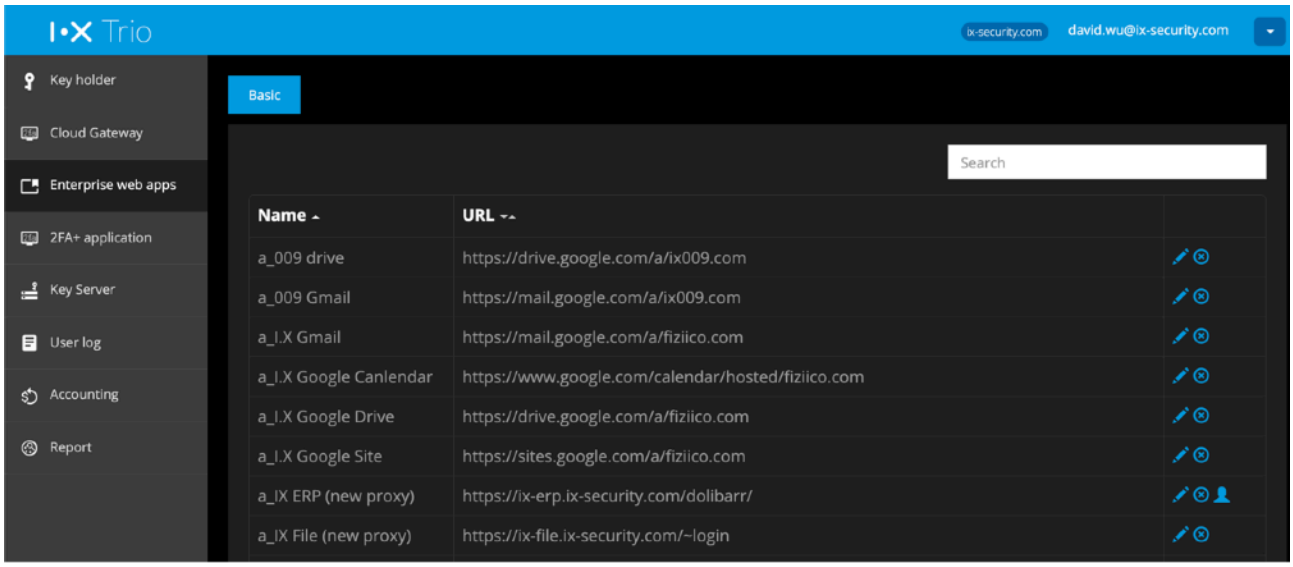


FIG. 3.2-1 ENTERPRISE WEB APP SETTINGS

Click “Add new” to create a new entry of enterprise web app

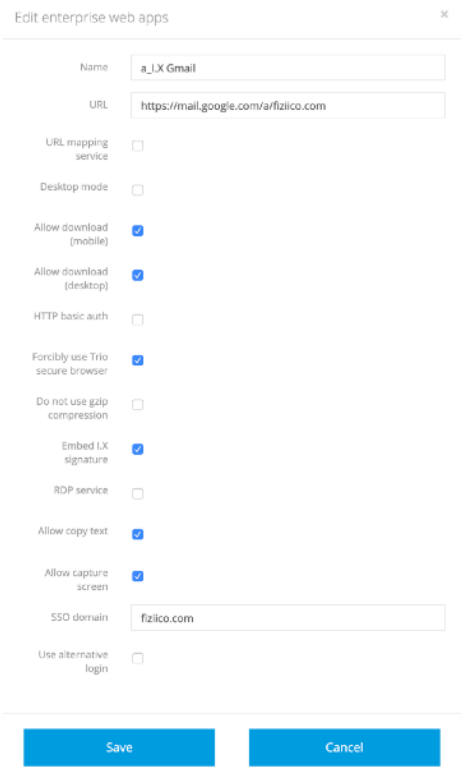


FIG. 3.2-2 ADD A NEW ENTERPRISE WEB APP DIALOG

Description of each parameter in enterprise web app setting

Parameter	Description	Note
Name	Web app name	Mandatory, used to discriminate different web apps
URL	Cloud service URL, or URL mapped by I.X Cloud Gateway, support both HTTP/HTTPS	Mandatory, used to specify the URL of enterprise web app
URL mapping service	Map to internal URL, sometimes the intranet web will redirect to an internal URL, configure this can make remote access possible.	Used when enterprise web app need to redirect to another internal URL
Desktop mode	On smartphone, use desktop browser UA to access this web app	Used only when enterprise web app has specific function available in desktop browser
Allow download (mobile)	Allow user to download file in web application of Trio Mobile. The downloaded file will be stored in secure storage of Trio Mobile.	Designed for Trio Mobile only
Allow download (desktop)	Allow user to download file in web application of Trio Desktop. Downloaded file will be decrypted, Trio Desktop will capture screen and log the download action while download.	Designed for Trio Desktop only
HTTP basic auth	Use HTTP basic auth to connect to this web app. Turn on this setting need to setup username / password per user in Auth Setting.	When enterprise web app support HTTP basic auth and admin can use this setting to manage user authorization
Forcibly use Trio secure browser	Use secure browser to open any link in this web app	Used only when enterprise want to force any URL link browsing in secure browser
Do not use gzip compression	Dis-allow gzip compression when open this web app	Used when this enterprise web app query database and return a lot of data.
Embed I.X signature	Embed I.X digital signature in every secure browser access	Suggest to turn on to prevent unauthorized access, unless this web app has compatibility issue
RDP service	Set this web app as a RDP service	Need to setup RDP gateway in advance
Allow copy text	Allow copy text to system clipboard in this web app	Suggest to turn off to prevent data leak
SSO domain	Specify SAML domain for this web app	Mandatory if this web app is configured by SAML login
Use alternative login	Specify alternative login account for G Suite anonymous account, SSO domain should be setup to specify this parameter	Used only when some users need to login G Suite anonymous account
Login email	Anonymous email account. Alternative login account should be configured in Auth Setting.	Anonymous account cannot be any of Trio account

To use HTTP Basic Auth, Trio can setup username / password for this web app in Console, such that user can access this web app without additional authentication once user login Trio App. In Auth Setting dialog, if username / password is configured for a Trio user, Trio App will use this username / password to login automatically. If it's empty, user will be prompted for username / password when user open this web app.

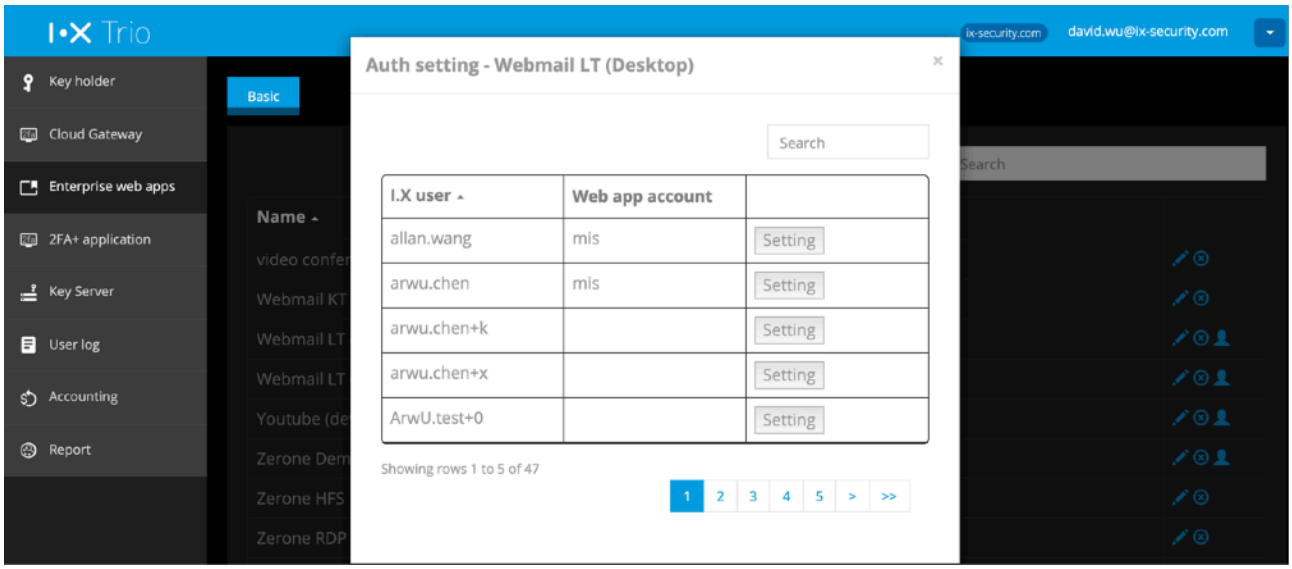


FIG. 3.2-3 EDIT AUTH SETTING DIALOG

3.3.1. I.X Cloud Gateway

In the past, whenever employees need to access intranet system (e.g., ERP), they need to login VPN, then intranet system can be used. However, login VPN is equivalent to enter intranet. Many cybersecurity issues start here. I.X secure browser can cooperate with I.X Cloud Gateway to provide secure access to your intranet system, without open VPN connection.

I.X Cloud Gateway will examine digital signature embedded in browser, without valid digital signature, connection request will be blocked. Enterprise system in intranet can verify this digital signature, to remove the security dependency of I.X Cloud Gateway.

3.3.2. Create an enterprise web application in I.X Cloud Gateway

System requirement of web server

To ensure connection security, the enterprise web server should support

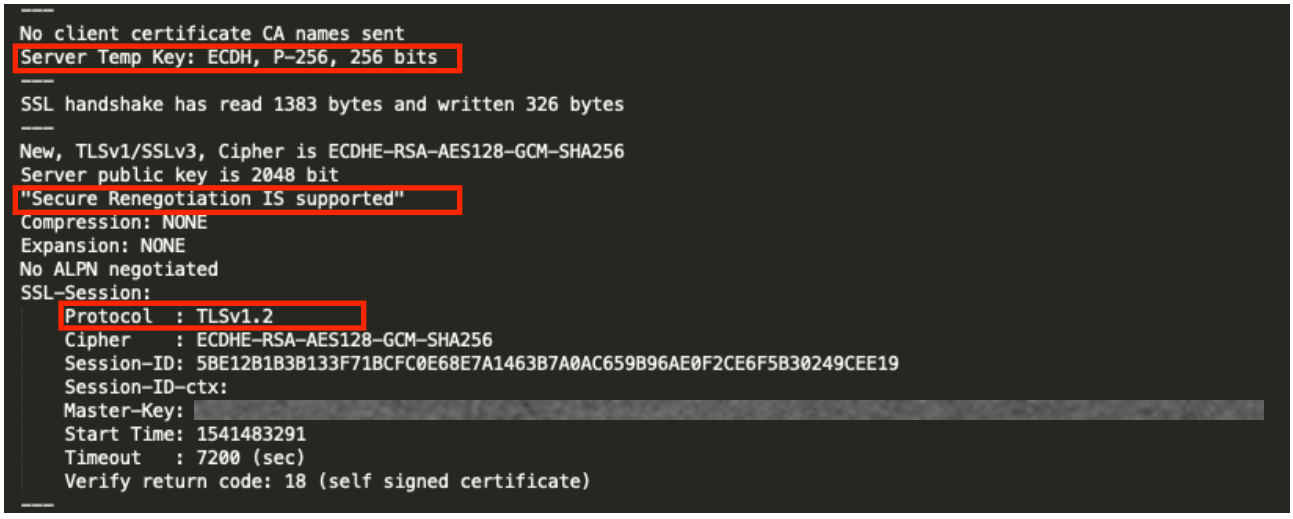
- TLS v1.2
- Secure Renegotiation
- Server Temp Key support ECDH, P-256, 256 bits

Verify SSL connection of your web server

Please use the following command line to test your web server

openssl s_client -connect <host:port>

After execution, compatible server's response should be shown as follows (check red frames):



Adjust setting in enterprise firewall

Your enterprise firewall should allow IP address of I.X Cloud Gateway to trigger http connection request to the IP address and port number of your enterprise web app. I.X Cloud Gateway's IP address are:

IP1	IP2	IP3	IP4
52.194.216.229	18.179.102.92	52.194.41.21	13.115.61.39

Setup entry in I.X Cloud Gateway

- Prepare public IP address and port number for the enterprise web app.
- Ask for I.X tech support to create an entry for this enterprise web app in I.X Cloud Gateway.
- I.X Cloud Gateway manager will provide a URL for you to configure this enterprise web app in Trio Console.

(Optional) Verify user's digital signature in your web server

To ensure web access security, I.X Trio secure browser will embed user's digital signature in every http request, and I.X Cloud Gateway will verify digital signature. If you have higher security requirement, you can verify digital signature of incoming http request on your web server, to verify user's identity and exercise zero-trust access control.

3.3.3. Internal URL mapping service

If your enterprise web app contains some links to other intranet server which cannot open to internet, you need to setup internal URL for this enterprise web app. For example, one attachment of a ERP form is linked to another intranet file server. In this case, you can create another enterprise web app point for the intranet file server, specify its corresponding public IP address and port number and internal URL. Make sure you map the public IP address and port number to this file server in firewall as well.

	URL provided Web item	Firewall Public IP	Intranet IP
ERP	https://server1.ix-security.com	https://1.2.3.4:8000	https://10.1.1.10
File server	https://server2.ix-security.com	https://1.2.3.4:9000	https://10.1.1.20

TABLE 3.2.3-1 SETUP EXAMPLE - IP MAPPING TABLE OF TWO WEB APPS

企業應用設定範例

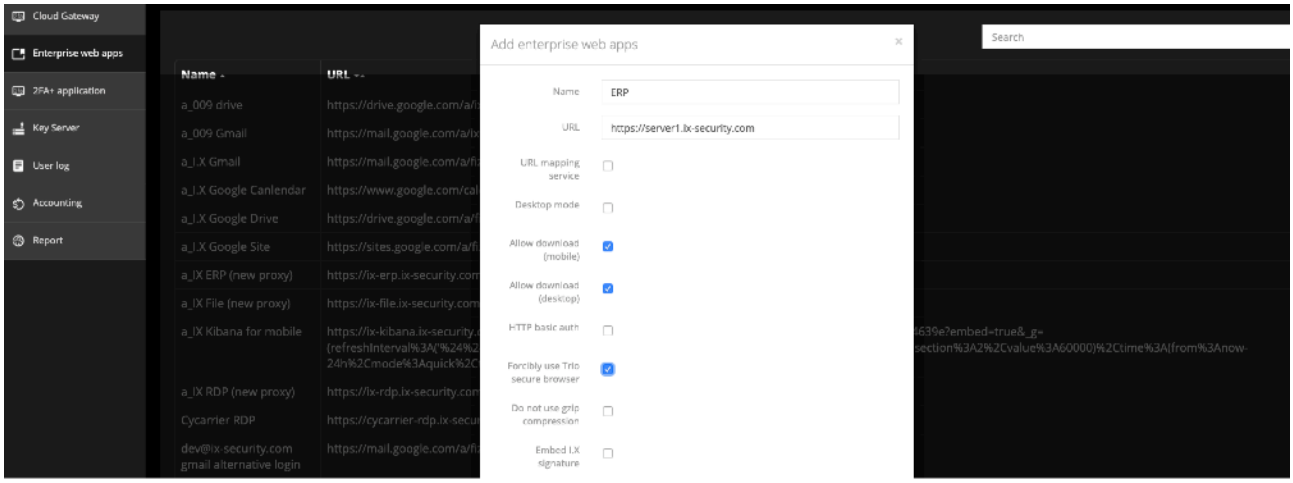


FIG.3.2.3-1 ENTERPRISE WEB APP SETTING FOR ERP

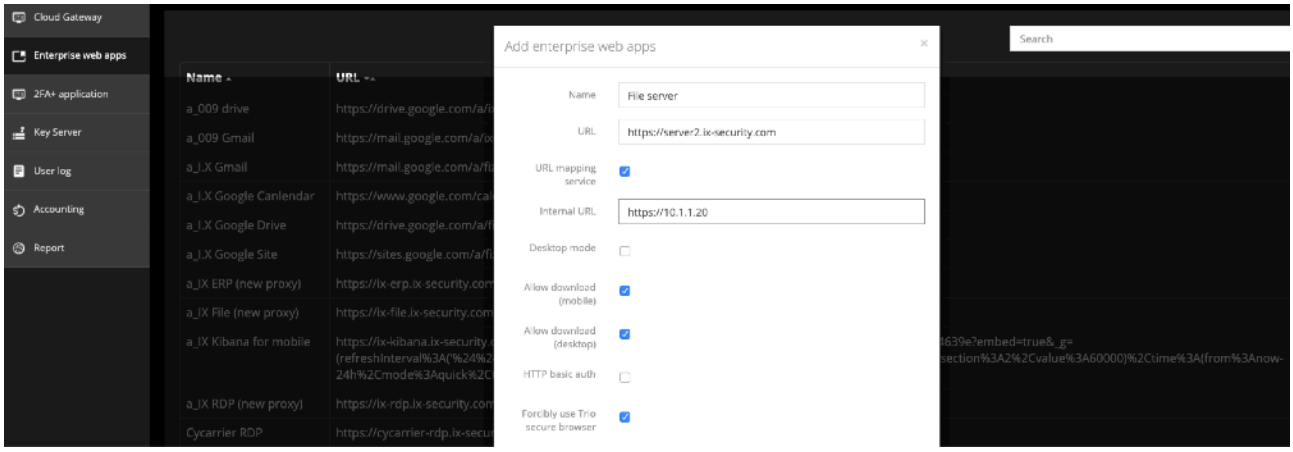


FIG.3.2.3-2 ENTERPRISE WEB APP SETTING FOR FILE SERVER, WITH INTERNAL URL MAPPING

3.3.4.SSO related setting

If your enterprise web app support SAML, you can use Trio to be your identity provider (IdP), to do user authentication during login. For example, if you want to use Trio to authenticate G Suite service, the following is an example:

Scenarios

One enterprise uses G Suite service, they want to use I.X Trio SSO solution, to address the following scenarios:

- Authenticate G Suite user with Trio digital signature mechanism.
- Force employee to use secure browser when accessing Gmail and Google Drive
- Allow user to download Gmail attachment and Google Drive file with download record
- Customer service team uses group account support@company.com to interact with customers, need a solution to login this group account with Trio authentication.

The following example focus on Trio Console setup related to Gmail and Google Drive. To understand more how to setup Trio authentication in G Suite, please reference “G Suite SAML setup guide for I.X Trio”.

Add enterprise web app for Gmail

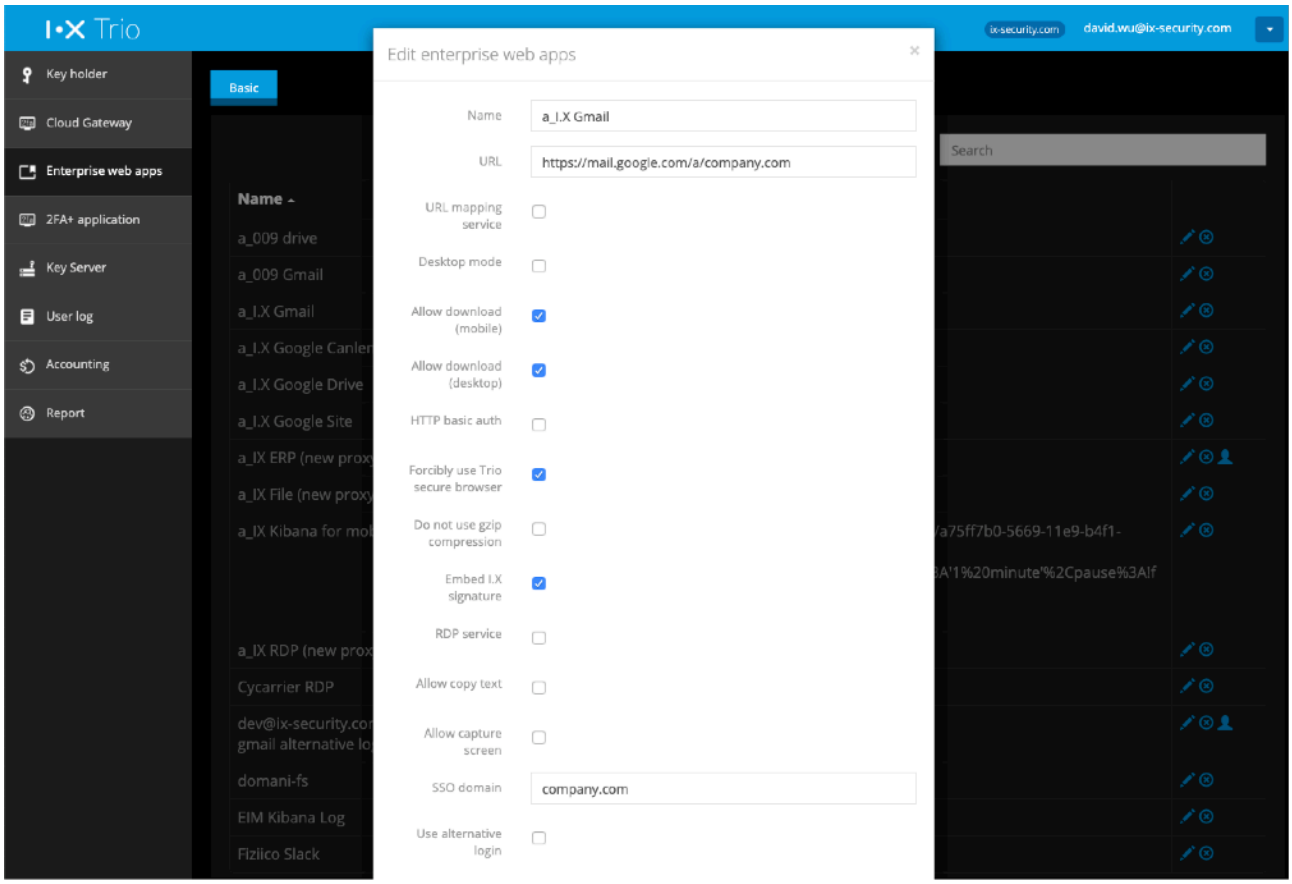


FIG. 3.3.4-1 ADD GMAIL WEB APP FOR COMPANY.COM

In enterprise web app, add an entry of Gmail as following setting:

Parameter	Value	Description
Name	a_I.X Gmail	Choose a name which is easy to differentiate
URL	https://mail.google.com/a/company.com	Fill the Gmail URL of company.com
Allow download (mobile)	Checked	If checked, Trio mobile will allow Gmail attachments (images or office documents) download to Trio secure folder. If unchecked, Trio mobile won’t allow Gmail attachments download in secure browser

Allow download (desktop)	Checked	If checked, Trio Desktop will allow any Gmail attachment download, and store in computer with plaintext, and leave a download record. If unchecked, Trio Desktop secure browser will block any download action.
Forcibly use Trio secure browser	Checked	Force using secure browser when user click link inside Gmail
SSO domain	company.com	Fill your domain here

TABLE 3.3.4-1 SETUP PARAMETERS FOR GMAIL WEB APP OF COMPANY.COM

Add enterprise web app for Google Drive

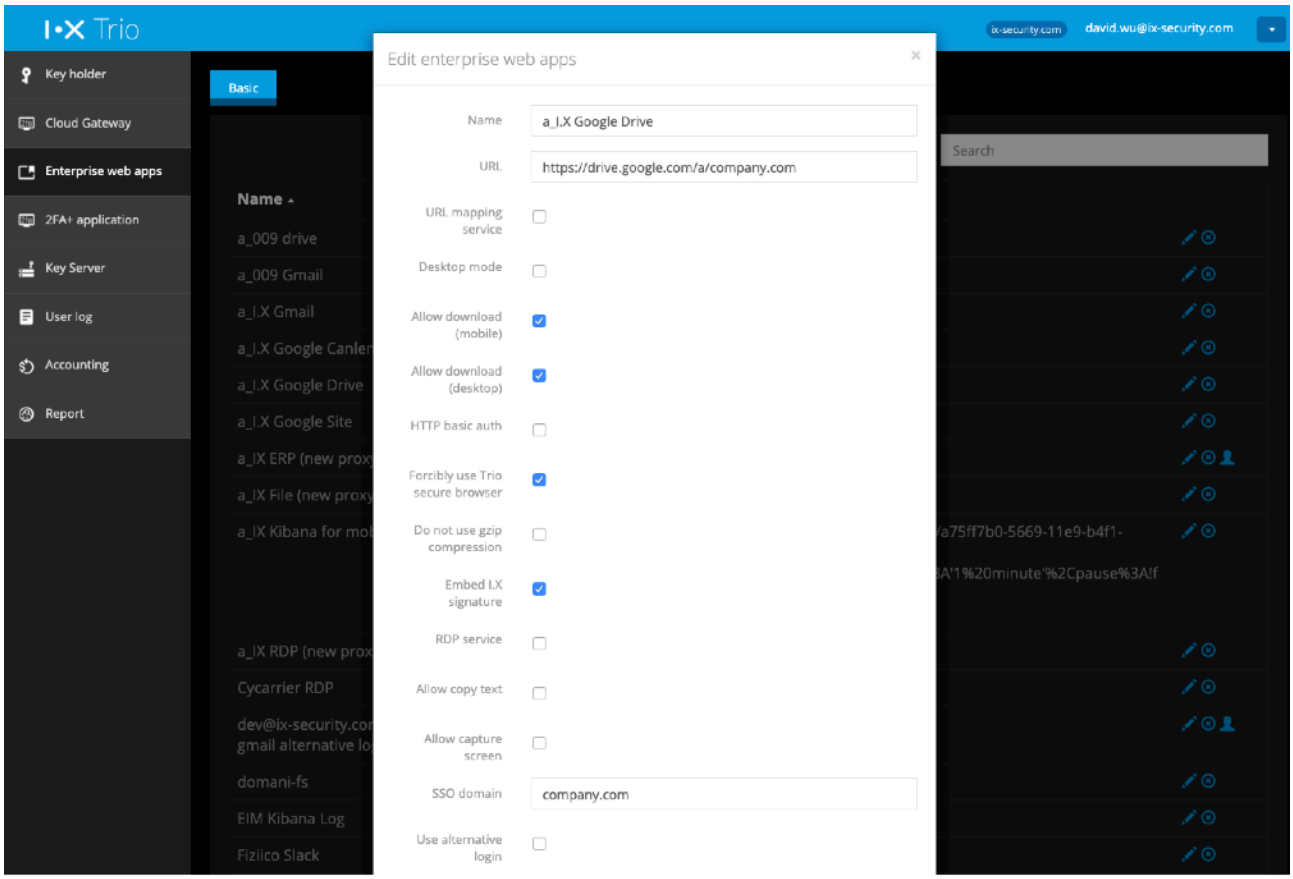


FIG. 3.3.4-2 ADD GOOGLE DRIVE WEB APP FOR COMPANY.COM

In enterprise web app, add an entry of Google Drive as following setting:

Parameter	Value	Description
Name	a._I.X Google Drive	Choose a name which is easy to differentiate
URL	https://drive.google.com/a/company.com	Fill the Google Drive URL of company.com

Allow download (mobile)	Checked	If checked, Trio mobile will allow Google Drive files (images or office documents) download to Trio secure folder. If unchecked, Trio mobile won't allow Google Drive files download in secure browser
Allow download (desktop)	Checked	If checked, Trio Desktop will allow any Google Drive file download, and store in computer with plaintext, and leave a download record. If unchecked, Trio Desktop secure browser will block any download action.
SSO domain	company.com	Fill your domain here

TABLE 3.3.4-2 SETUP PARAMETERS FOR GOOGLE DRIVE WEB APP OF COMPANY.COM

Setup alternative login for group account

Trio support alternative login for group account of the same domain, such group account must be non-Trio account. In the following example, service@company.com is the group account, then it cannot be registered to Trio service. This example will show how to create an enterprise web app and manage the list of Trio users to do alternative login and use service@company.com.

First, create an enterprise web app for service@company.com:

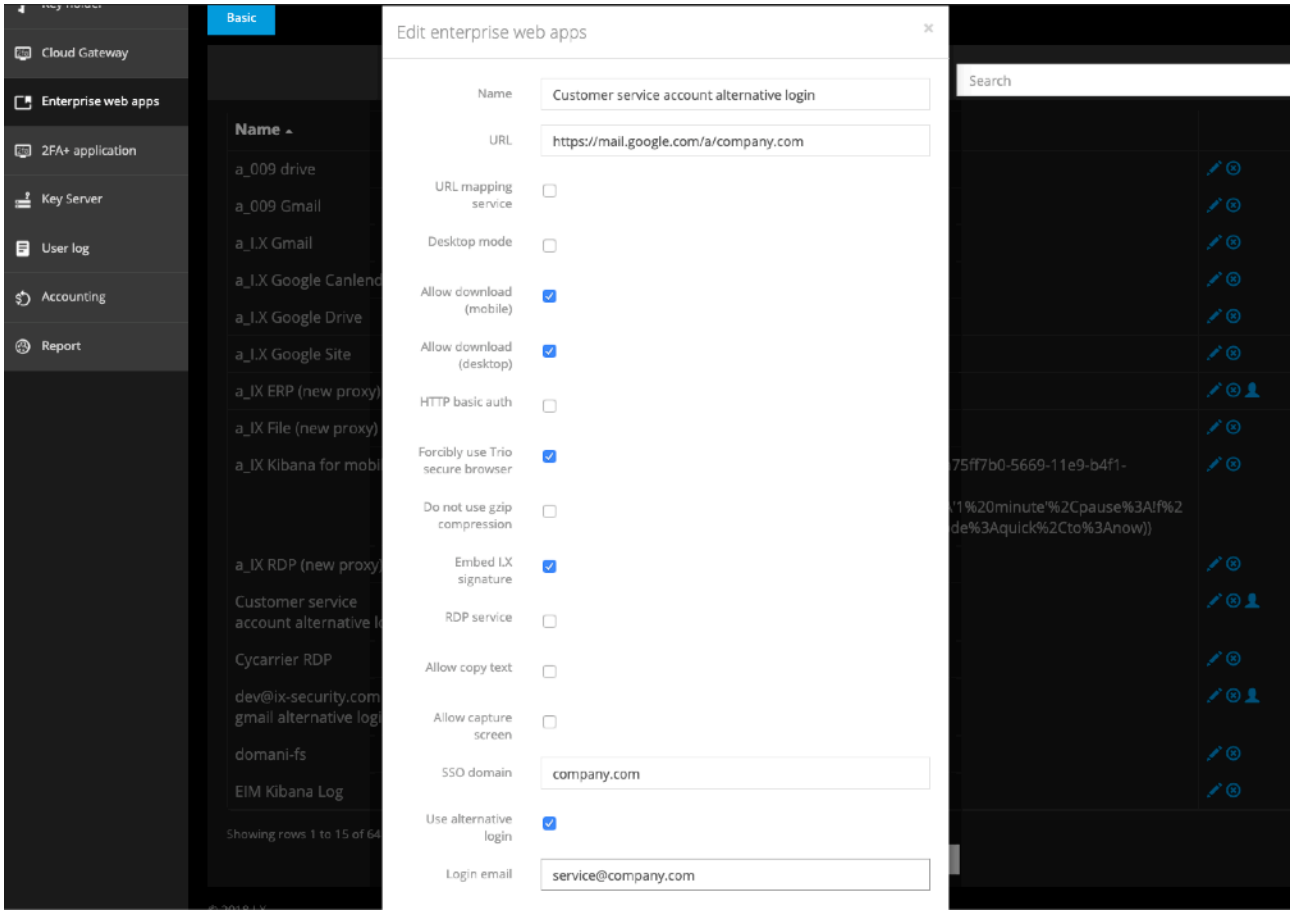


FIG. 3.3.4-3 SETUP ALTERNATIVE LOGIN FOR GROUP ACCOUNT

Parameter	Value	Description
Name	Customer service account alternative login	Choose a name which is easy to differentiate
URL	https://mail.google.com/a/company.com	(same as TABLE 3.3.4-1)
Allow download (mobile)	Checked	(same as TABLE 3.3.4-1)
Allow download (desktop)	Checked	(same as TABLE 3.3.4-1)
Forcibly use Trio secure browser	Checked	(same as TABLE 3.2.4-1)
SSO domain	company.com	(same as TABLE 3.2.4-1)
Use alternative login	Checked	Checked to activate alternative login

Use alternative login	Checked	Checked to activate alternative login
Login email	service@company.com	Fill the group account name which require alternative login. Attention: this account cannot be registered as Trio account

TABLE 3.3.4-3 SETUP PARAMETERS FOR GROUP ACCOUNT ALTERNATIVE LOGIN

After setup the enterprise web app, click auth setting icon (red circle of the following figure) to manage user list to do alternative login

FIG. 3.3.4-4 AUTH SETTING OF ALTERNATIVE LOGIN

It will open a dialog, which will allow you to select Trio user list who can do alternative login for support@company.com. Please note, any user who want to login as support@company.com, need to logout his account in secure browser.

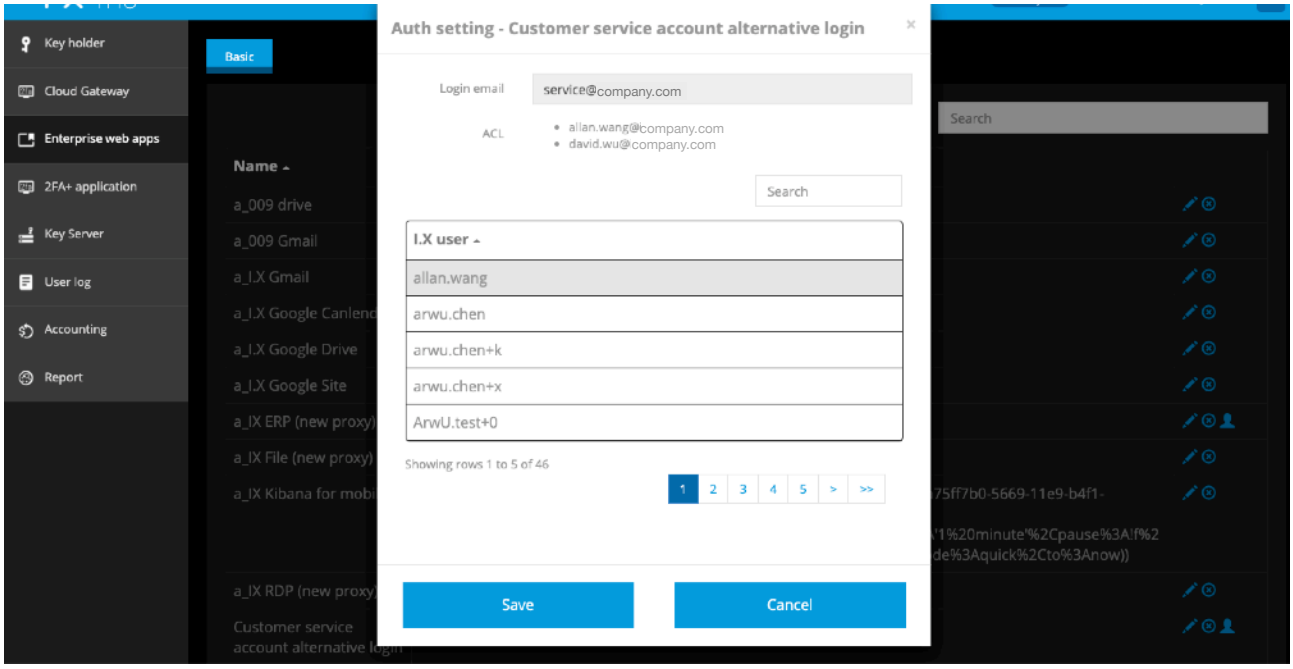


FIG. 3.3.4-5 SELECT TRIO USERS TO DO ALTERNATIVE LOGIN

3.4. User log

You can use user log function, to monitor users' behavior of your domain. This page will browse 7-day Trio system log, including logs for 2FA+, call, file sharing, export, group warning (screen capture in Trio IM), and domain warning (screen capture in secure browser).

3.4.1. 2FA+ (system logon)

Any system which uses Trio 2FA to authenticate user, including Trio Console, Trio Desktop, and other 2FA+ applications will have logs here.

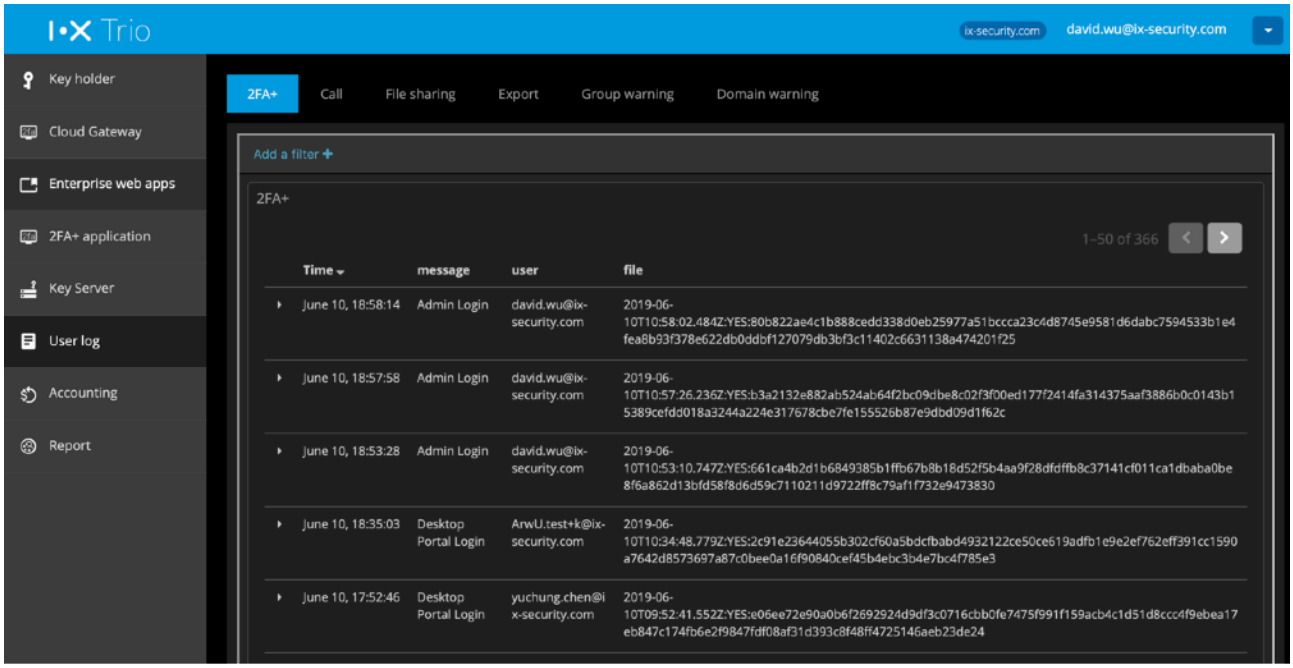


FIG. 3.4-1 2FA+ LOGIN LOG

Data field description listed as follows:

Name	Description
Time	2FA response time when user login system
message	2FA application name
user	User account
file	User's digital signature of this 2FA response

3.4.2. Call

In call tab, you can see all Trio VoIP call logs of your domain.

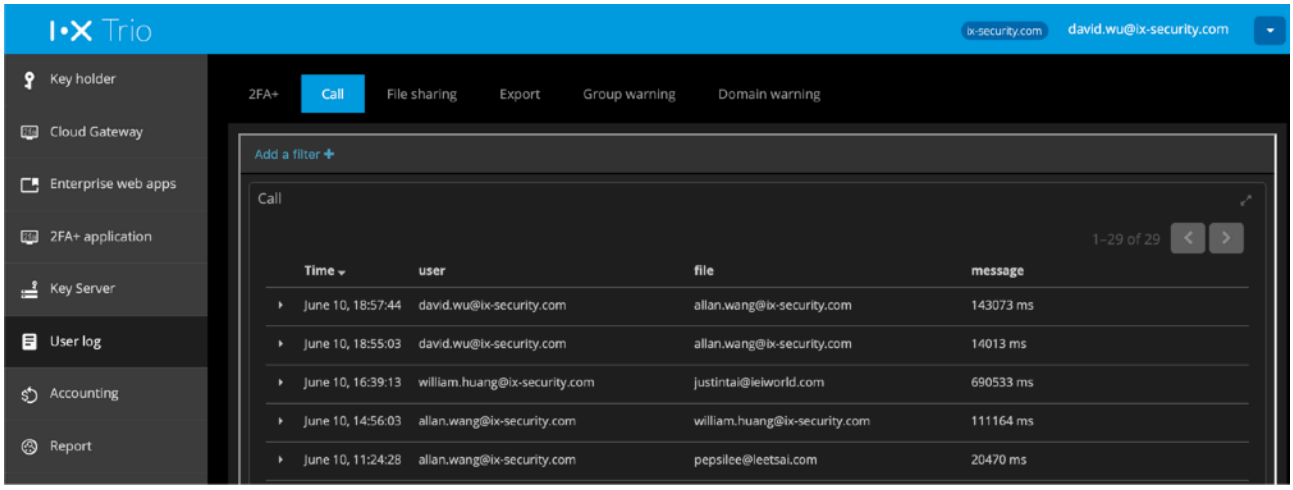


FIG. 3.4.2-1 CALL LOG

Data field description listed as follows:

Name	Description
Time	Time to make VoIP call
user	Caller's user account
file	Callee's user account
message	Call time (ms) or drop-call reason

3.4.3. File sharing

In file sharing tab, you can browse the logs of any sender who share image or document over Trio IM, and which receivers open this file.

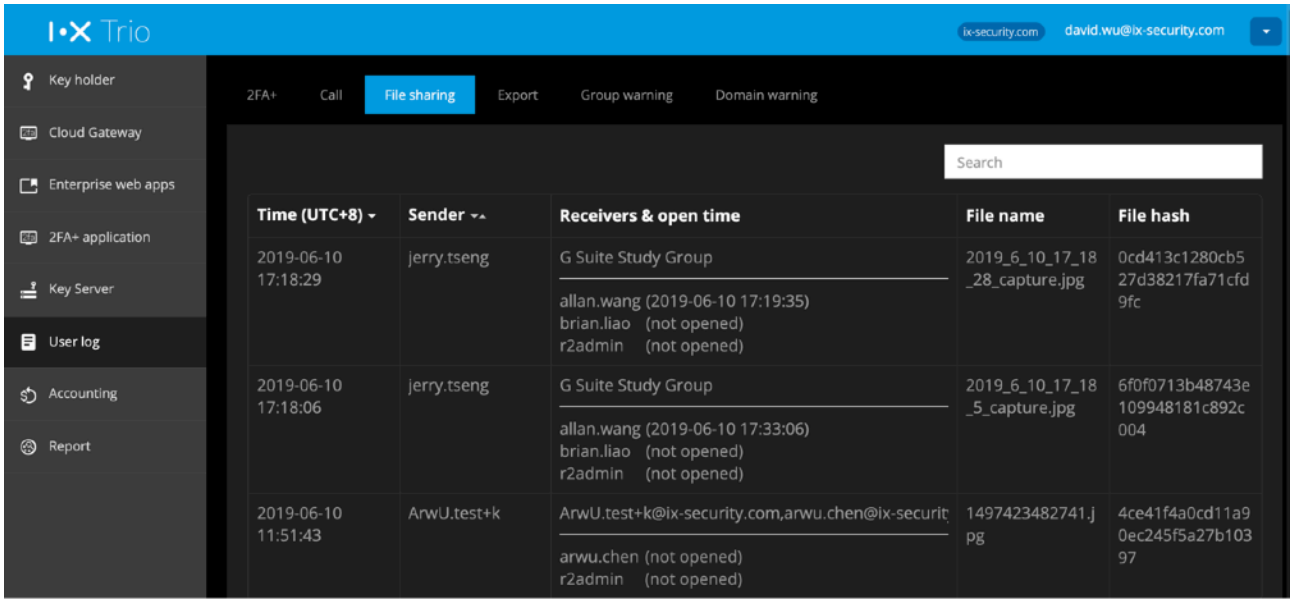


FIG. 3.4.3-1 FILE SHARING LOG IN TRIO IM

Data field description listed as follows:

Name	Description
Time	The time sender sends the file
Sender	Sender's user account
Receivers & open time	Group name (above the separator line) Member list and the corresponding file open status or open time
File name	File name
File hash	Hash value of this file, can be used to differentiate file

3.4.4. Export

In Export tab, you can browse export logs for all channels

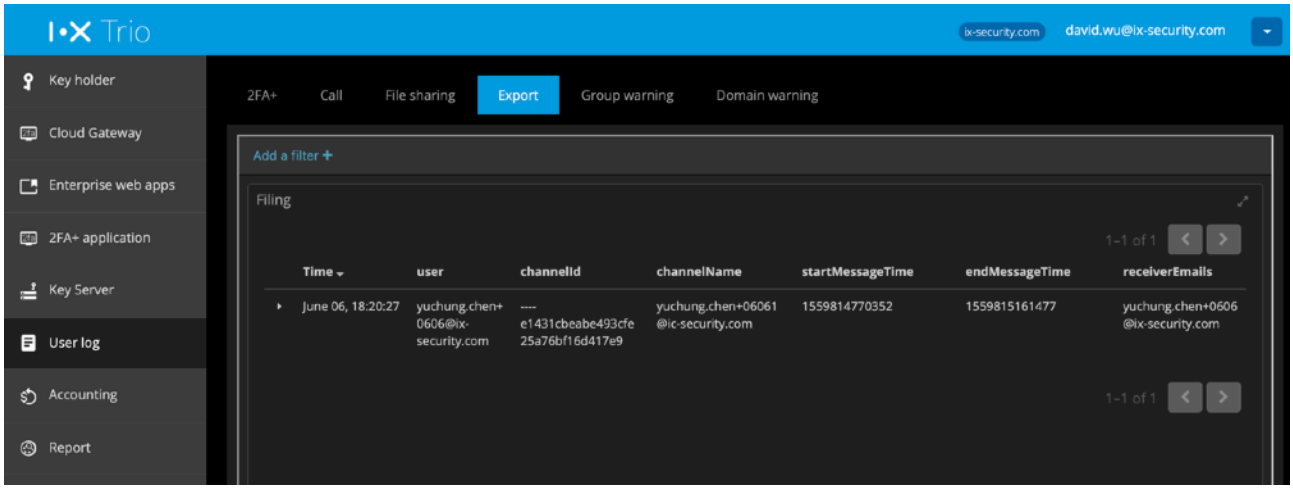


FIG. 3.4.4-1 EXPORT GROUP CHAT LOG

Data field description listed as follows:

Name	Description
Time	Time to export group chat
user	The user who trigger this task
channelId	Group chat ID
channelName	Group chat name
startMessageTime	The time of the first message to be exported
endMessageTime	The time of the last message to be exported
receiverEmails	Define who will receive the exported conversation in email

3.4.5. Group warning

When iPhone user capture screen in any group chat, group warning will be posted in group chat window, and left a group warning log in Trio Console.

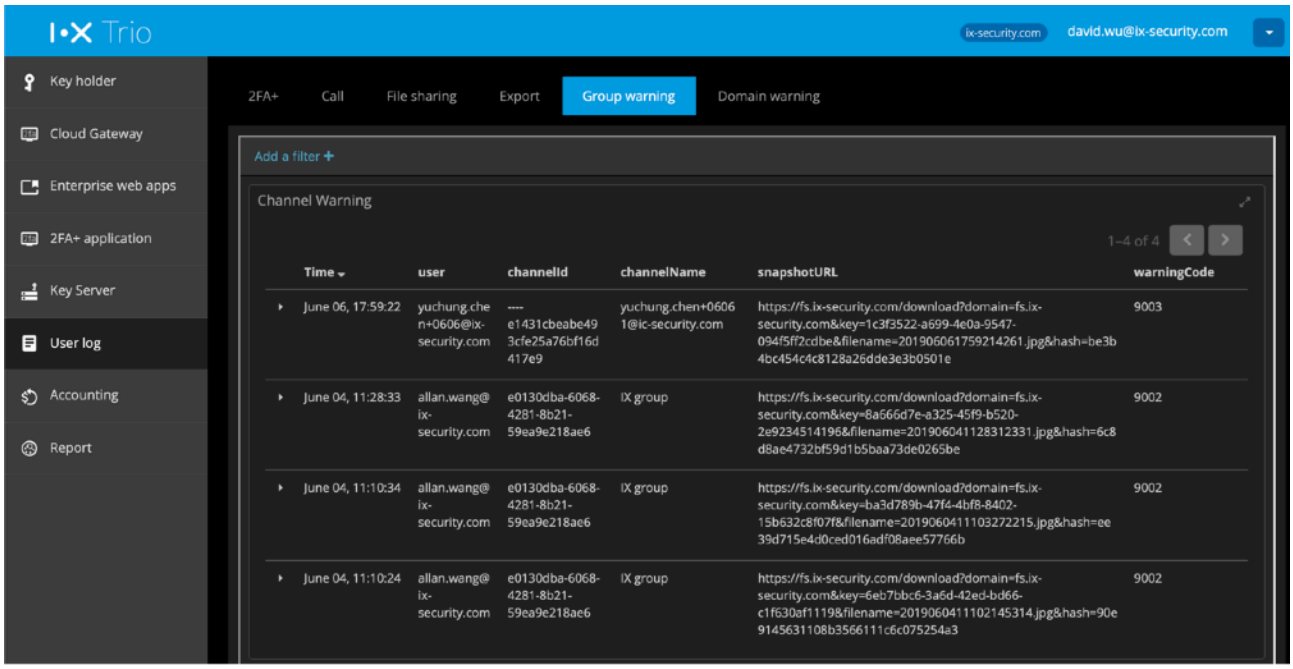


FIG. 3.4.5-1 TRIO IM SCREEN CAPTURE LOG (IPHONE USERS)

Data field description listed as follows:

Name	Description
Time	Screen capture time
user	The user who do screen capture
channelId	Group chat ID
channelName	Group chat name
snapshotURL	The URL to store screen capture image

3.4.6. Domain warning

When iPhone user do screen capture in enterprise web app, domain warning will be triggered and create a log in this category.

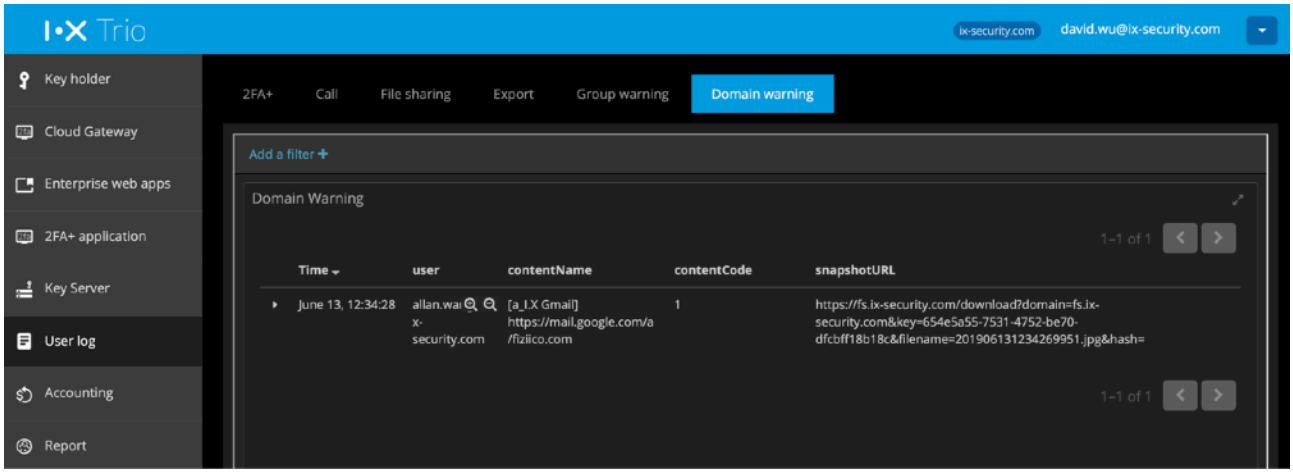


FIG. 3.4.6-1 TRIO SECURE BROWSER SCREEN CAPTURE LOG (IPHONE USER)

Data field description listed as follows:

Name	Description
Time	Screen capture time
user	The user who do screen capture
contentName	Enterprise web app name
snapshotURL	The URL to store screen capture image

3.5. 2FA+ application

If you have more system login want to be protected by Trio 2FA, you may create more 2FA+ application in Trio Console.

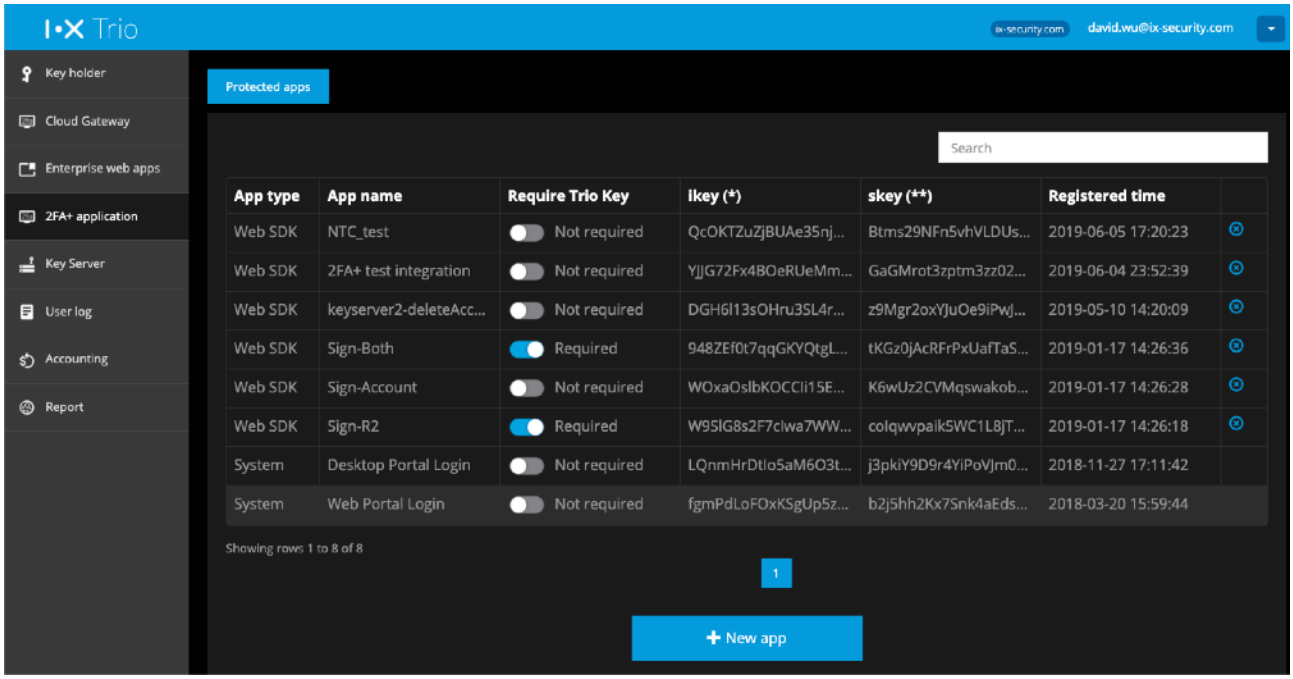


FIG. 3.5-1 2FA+ APPLICATION CONFIGURATION

Click “+ New app”, it will prompt a dialog as follows. You can setup application name, and the option to use hardware key to do digital signature. Once it’s setup, the system will generate a set of ikey and skey to let application use in Web SDK.

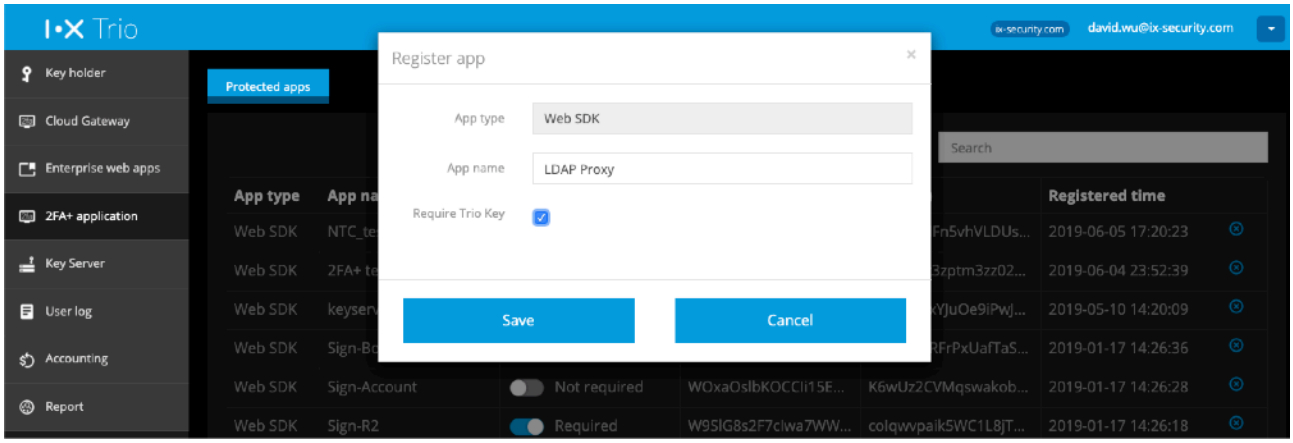


FIG. 3.5-2 ADD A NEW 2FA+ APPLICATION

In the appendix A, there is an example to setup 2FA+ application.

3.6. Key server

In addition to Trio Key, you can purchase key server to deploy system easily. Once you deploy key server for your domain, your Trio users doesn't require Trio Key to login, key server will play the role of virtual key. Only when you need to login system with higher security, for example, Trio Console must use Trio Key. For more information about key server, please contact I.X reseller or I.X online support.

3.7. Accounting

If you are a prepaid customer and purchase credit points, when any user account will expire in 3 months, will be listed here and the system will send notification email to you.

You can redeem credits for expiry users here. Every redeem action will extend 1 year of service, and deduct from your credit pool. Once you delete an account, the remaining credit will return to this pool.

3.8. Report

When you start using Trio service, I.X service administrator will build a report dashboard based on your subscribed service type, such that you can understand Trio service usage statistics and logs. For example, active users, enterprise web app or 2FA+ application access frequency, etc.

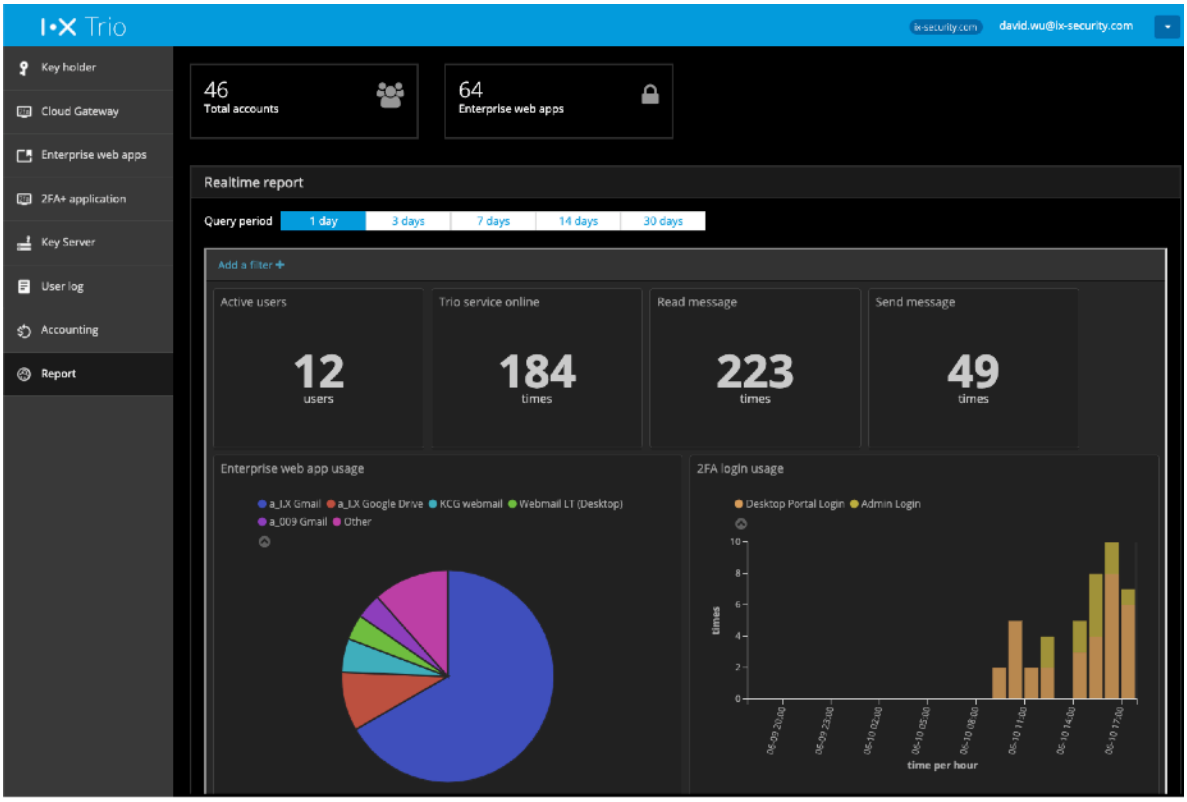


FIG. 3.7-1 TRIO SERVICE USAGE REPORT

The statistic report template is owned by I.X. If you have specific requirement, please contact I.X reseller or I.X online support.

Appendix A. Fortigate SSLVPN 2FA integration

Scenario

One customer would like to introduce Trio 2FA for Fortigate VPN login, without depending old OTP token.

Communication flow

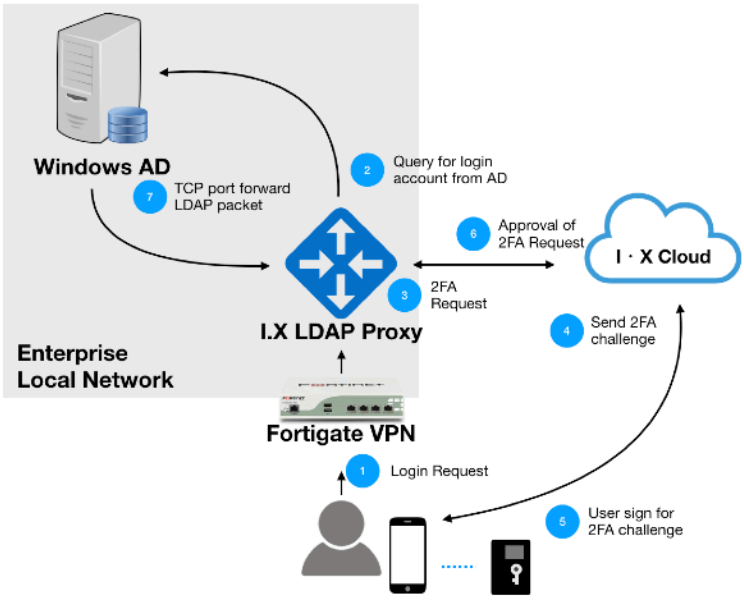


FIG. 3.4.1-1 NETWORK ILLUSTRATION AND COMMUNICATION FLOWCHART

Originally, the customer use LDAP protocol to query AD server and do user authentication in VPN connection. After using I.X Trio 2FA service, VPN connect to I.X LDAP Proxy to do user authentication. During this process, I.X LDAP proxy will:

1. Query user account from AD server

2. Through I.X 2FA Authentication service, it will push a 2FA notification to user's smartphone, and do user authentication.

After user press "Approve" on smartphone, Trio app will provide digital signature of user's key, I.X LDAP proxy will validate this digital signature and then pass to AD server to finish LDAP protocol.

How to setup

Step 1. Create an entry in Trio Console

Click “+ New App” button, it will prompt a dialog to let you create a new 2FA application, assign the name. Check “Required R2 Card” if you want to use hardware Trio Key to authenticate user.

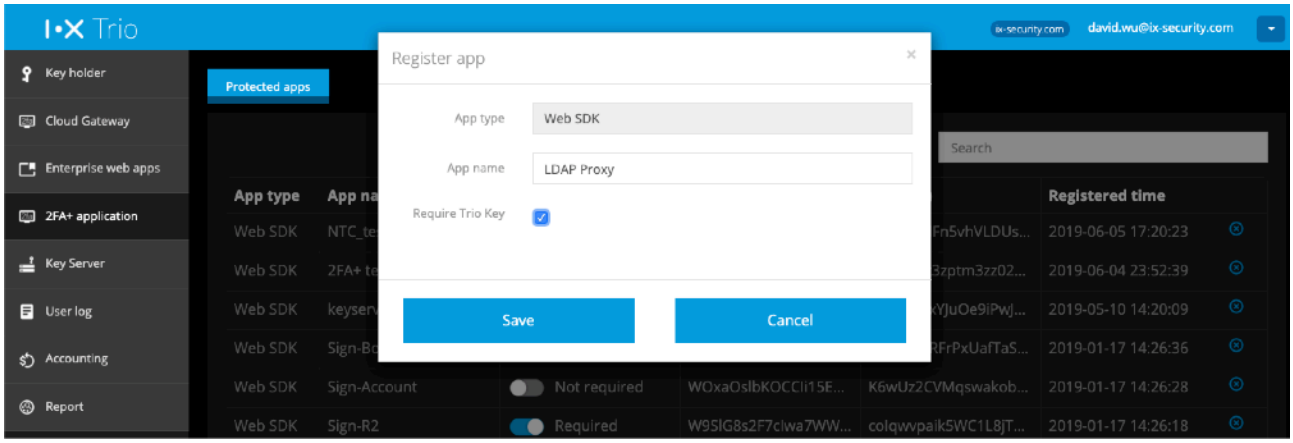


FIG. 3.4.1-2 CREATE A 2FA APPLICATION

In **Protected App**, you can find the corresponding key pair information of this 2FA application, the ikey and skey need to setup in I.X LDAP Proxy, such that I.X LDAP proxy can communicate with I.X Auth service.

Step 2. Configure Fortigate VPN

On Fortigate VPN console, change the IP address of AD server, to the IP address of I.X LDAP Proxy. Check the LDAP BindType, BaseDN, AdminDN, and AdminDN’s password of AD server, since these parameters will be used to configure I.X LDAP Proxy later.

Fortinet application default authentication timeout is 5 seconds, please extend this timeout value to appropriate value. The following example will extend the timeout to 300 seconds.

- Connect Fortinet appliance command line interface (CLI)
- Execute the following commands
  # config system global
  # set remoteauthtimeout 300
  # end

Step 3. Setup I.X LDAP Proxy

To install I.X LDAP Proxy, please prepare a linux server with the following requirement:

Hardware requirement

- Dual core CPU 2GHz
- 8GB RAM

OS

- Debian 9 / Ubuntu 18.04 LTS (VM)

Software

- Install curl package
- Allow *.docker.com:443

Firewall setup

To setup I.X LDAP Proxy, you need to open necessary port on that server. If user's smartphone will connect to office WiFi network, more ports should be open, such that 2FA notification can be received.

I.X LDAP Proxy firewall setup

- In-bond open TCP 22, 1389
- In-bond IP allow Fortigate VPN IP
- Out-bond open TCP 389, 443
- Out-bond IP allow connection to AD server and https://api.ix-security.com

Corporate firewall setup for smartphone
IP and port number for iPhone users

- Open TCP 443, 2195, 2196, 5223
- Apple push server is the complete 17.0.0.0/8 IP address block
- I.X cloud server: https://*.ix-security.com

IP and port number for Android users

- Open TCP/UDP 443, 5228, 5229, 5230
- Google FCM server IP address: https://ipinfo.io/AS15169
- I.X cloud server: https://*.ix-security.com