I.X Trio 管理系統

使用手冊

版本 1.09

目錄

申請 Trio 企業網域

管理企業內的 Trio 服務

申請 Trio 企業網域

1. 申請 Trio 建立企業網域

加入您是在線上申請試用的用戶，您可跳過本章節，直接前往 管理企業內的 Trio 服務。假如您的企業尚未在 I.X Trio 上申請建立企業網域，請先到
https://service.ix-security.com/console/#/signup

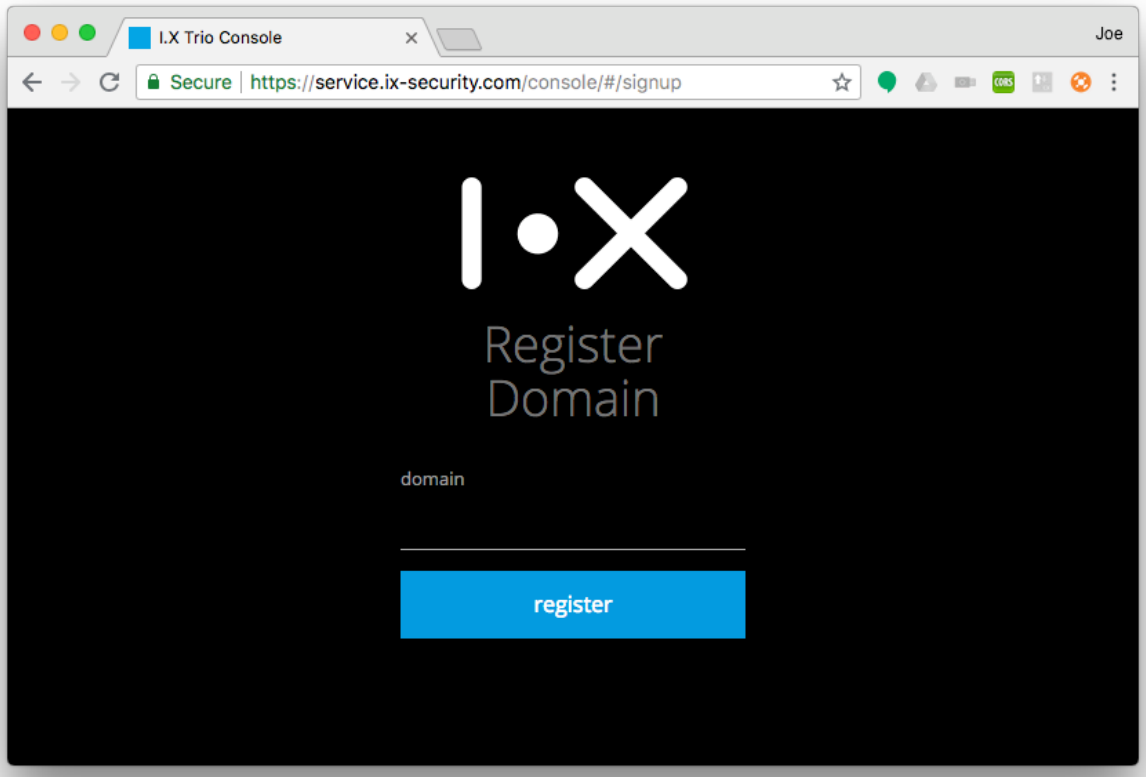


FIG. 1-1 TRIO 企業網域申請畫面 1

輸入 domain 名稱，如: yourdomain.com，並按下 “register” 鍵，該 domain 必須為公司所擁有的 domain。

若規則檢查通過，畫面將引導您寄送啟用信，到 r2admin@yourdomain.com 。

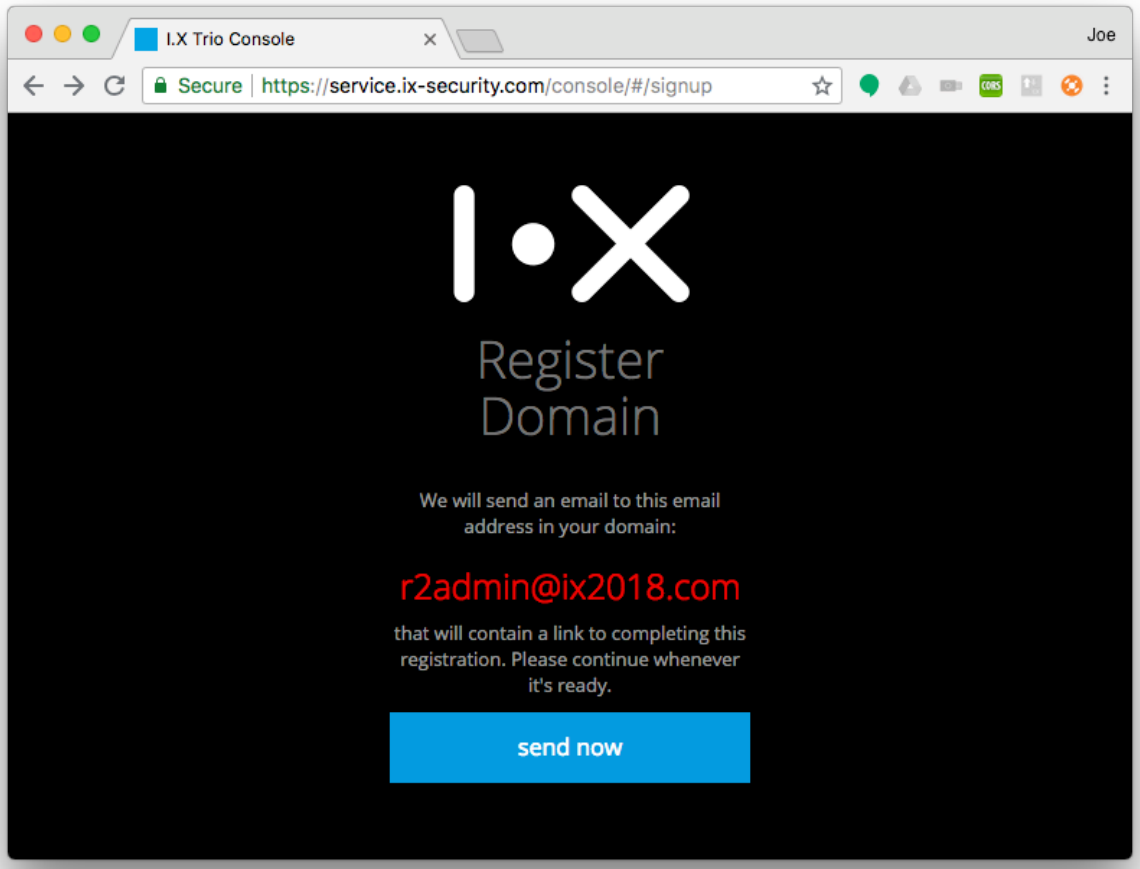


FIG. 1-2 TRIO 企業網域申請畫面 2

2. 建立 Trio 管理員郵件帳號

請公司的帳號管理員新建 r2admin@yourdomain.com 後，按下 “send now”，I.X 服務將送 domain 啟用認證信到該郵件信箱。

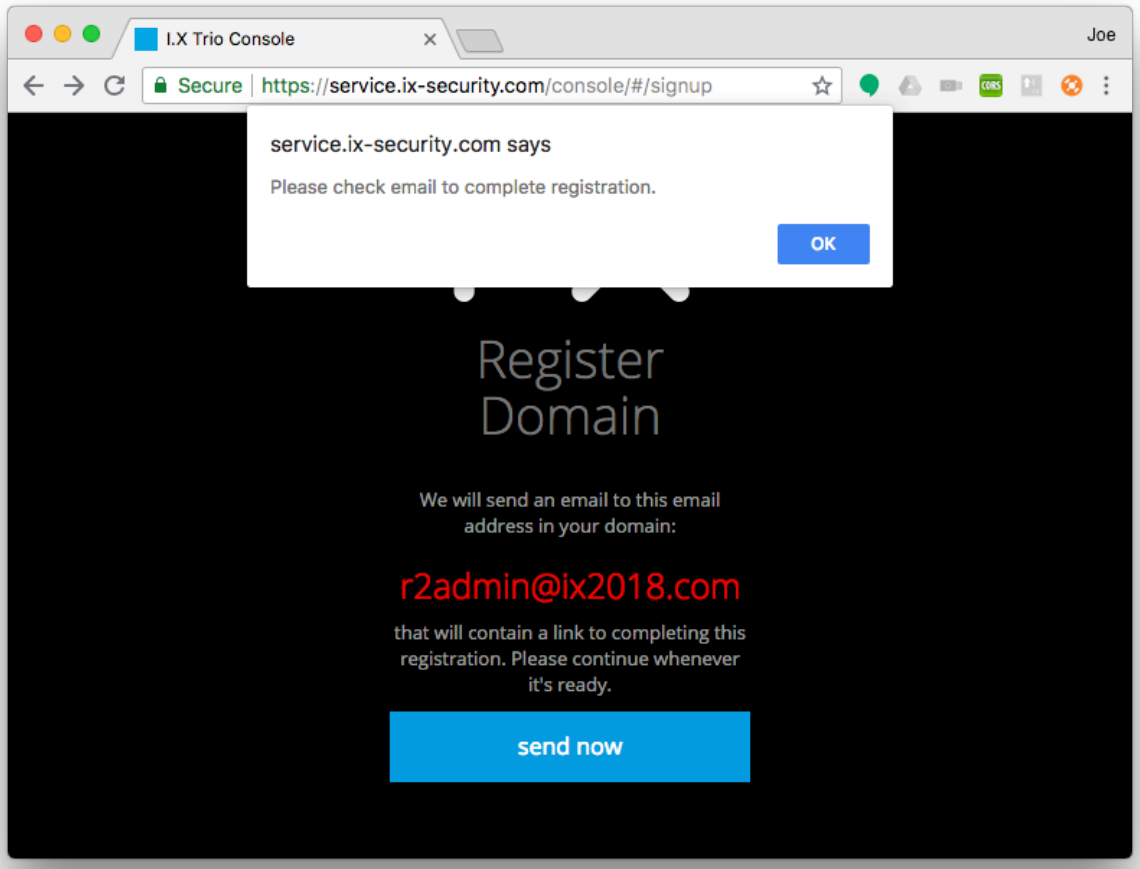


FIG. 2-1 TRIO 企業網域申請畫面 3

3. 確認是否收到啟用信

Domain 啟用信的內容範例如下

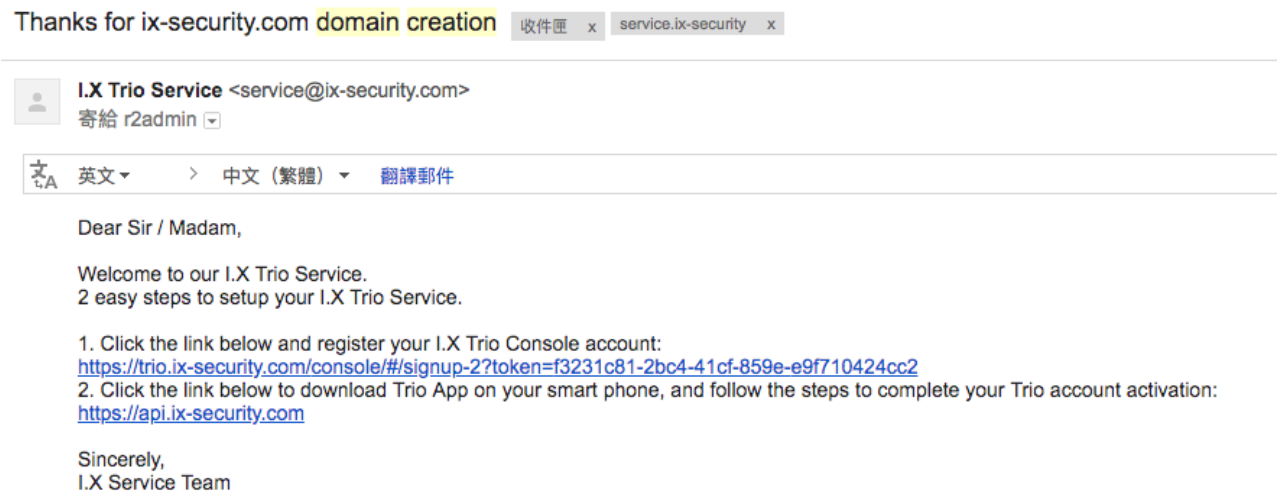


FIG. 3-1 TRIO 企業網域啟用信範例畫面

假如沒收到，請先檢查郵件帳號是否設定無誤，或確認是否被誤認為垃圾郵件。

4. 下載 I.X Trio App

收到信後，先透過以下連結下載 I.X Trio App
https://www.ix-security.com/download/trio/app.html

並且，依照 App 的指示，完成帳號註冊程序

5. 設定管理人員的 Trio 帳號

Trio 帳號註冊完成後，再次開啟 domain 啟用信，並點擊 Domain 啟用信內的連結
https://trio.ix-security.com/console/#/signup-2?token=f3231c81-2bc4-41cf-859e-e9f710424cc2

網頁會導引您建立企業網域管理員資訊

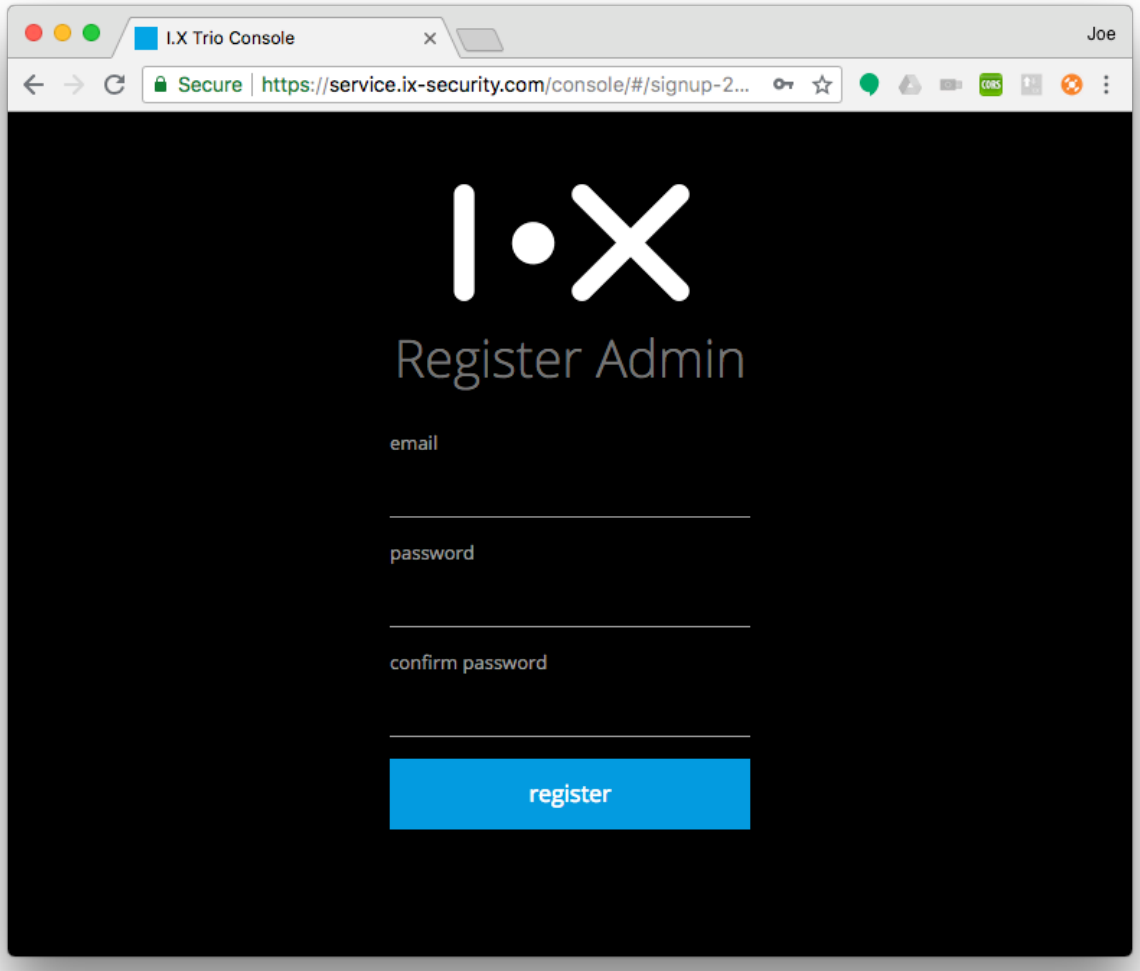


FIG. 5-1 企業網域管理員帳號綁定畫面

依頁面提示，設定完您企業網域的第一位管理員後，按 “register”。待設定完成後，網頁將跳出設定完成通知，並跳轉至管理員登入頁面。

完成！開始管理網域內的 Trio 服務

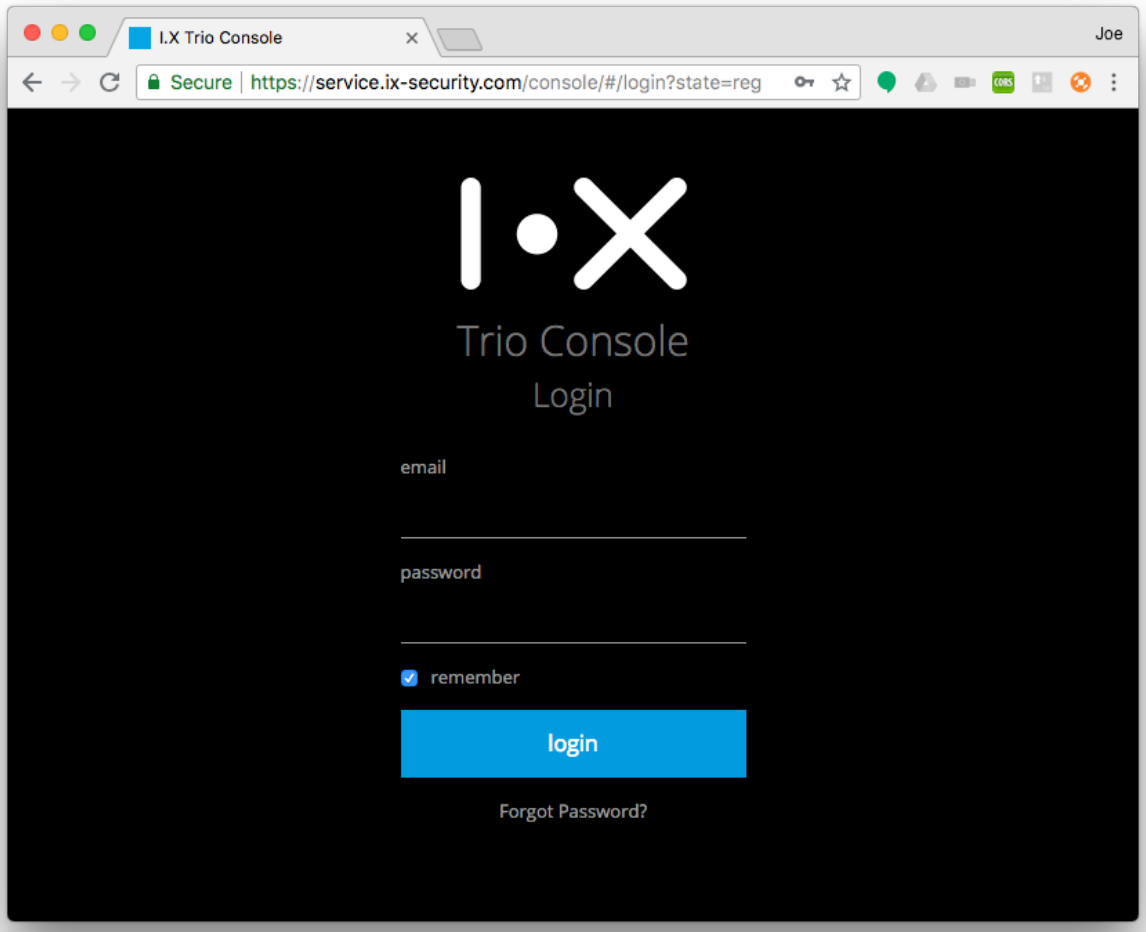


FIG. 6-1 TRIO 管理平台登入畫面

管理企業內的 Trio 服務

1. 登入管理系統

僅具備管理員身份者，可登入管理系統。登入管理系統前，請先確認：

- 手機可連線上 Internet 網路
- 手機藍牙連線已開啟
- 卡片已開啟，且在手機藍牙可連線的範圍

輸入管理員的電子郵件和密碼，該密碼為設定管理員時設定的密碼。

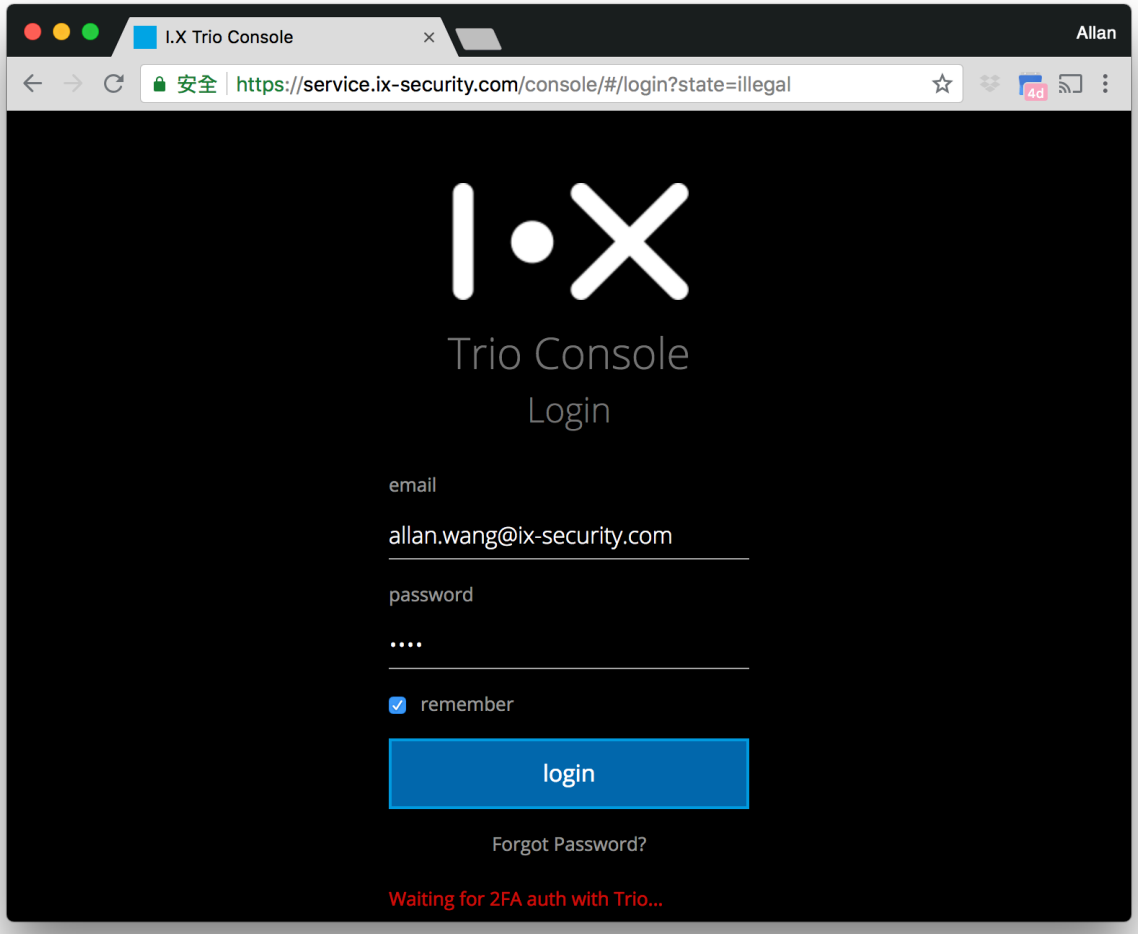


FIG. 1-1 TRIO 管理平台登入畫面

登入時，若帳號密碼輸入正確，系統會發送 2FA 請求至該帳號綁定的手機。

倘若您為試用客戶，且為該網域的 Trio 管理員，可以到您電子郵件信箱找到標題為 “I.X Trio Console Activated” 的郵件，信件內容有您預設的密碼。或者，您也可直接點擊下方的 “忘記密碼?” 的連結，並輸入您的帳號，以重置您管理平台的密碼。

2. 開啟卡片，手機同意 2FA 登入

手機收到 2FA 認證通知後，點擊認證通知。確認為本人授權的登入行為時，點選同意。

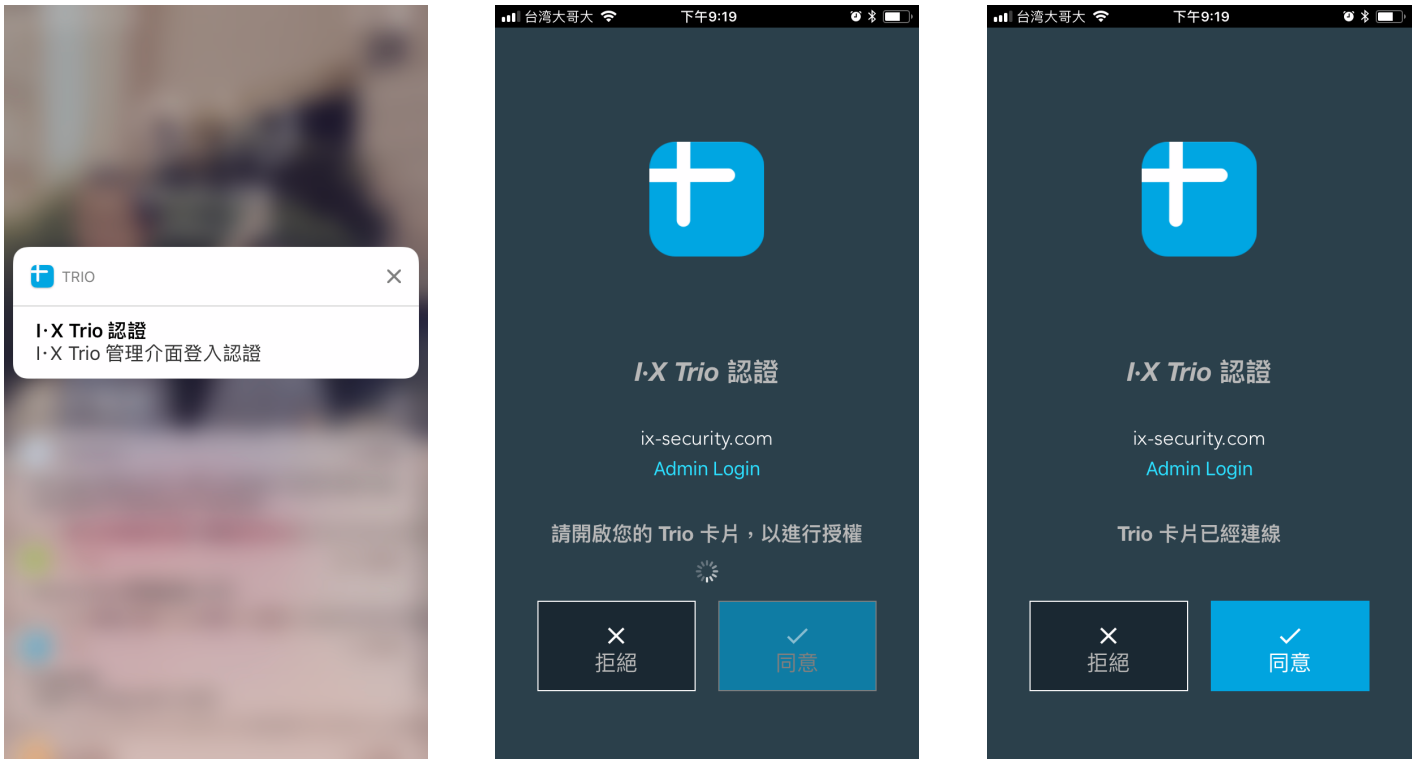


FIG. 2-1 手機 2FA 認證通知畫面

3. 管理介面介紹

左列為功能列，右邊為內容頁。

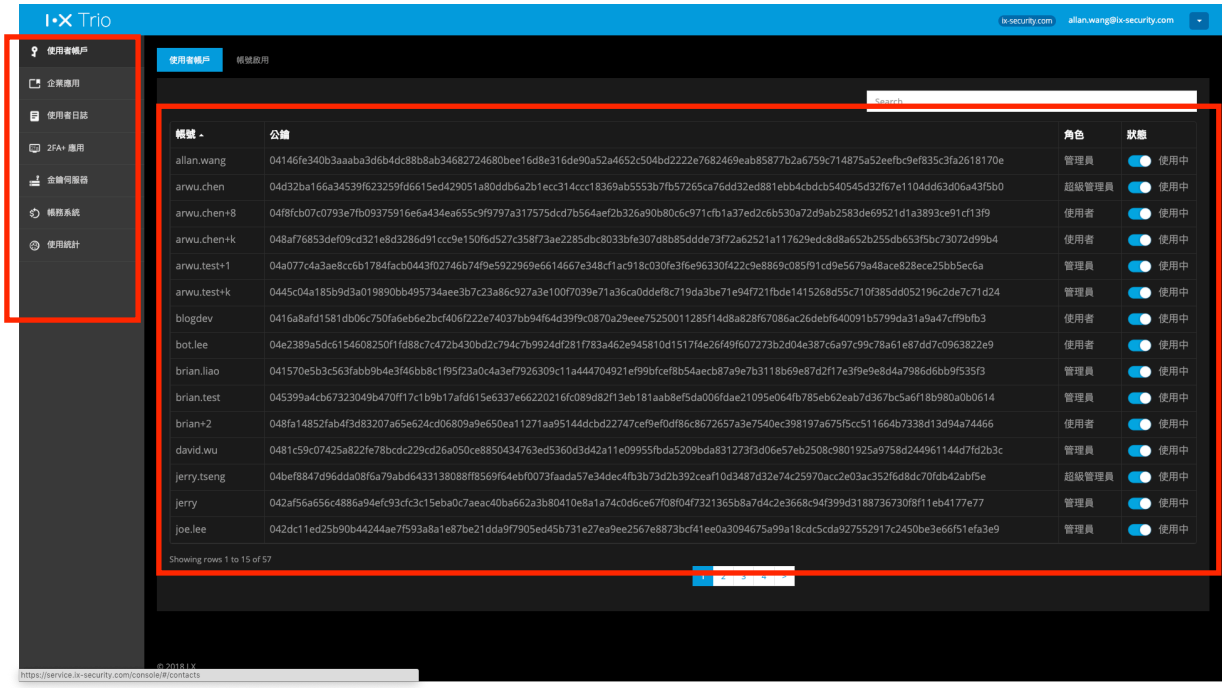


FIG. 3-1 管理界面網頁畫面

3.1. 使用者帳戶

可管理網域內，所有使用者的金鑰狀態，及使用者權限。

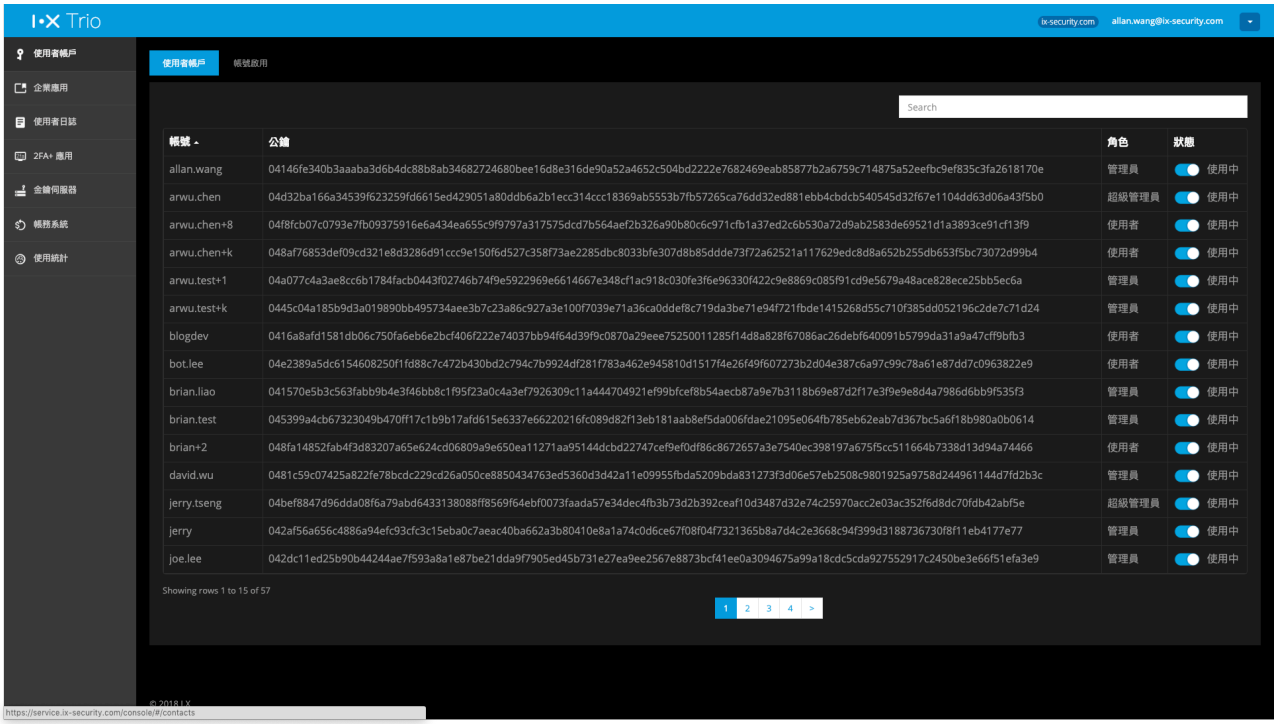


FIG. 3.1-1 管理企業網域內的 TRIO 使用者

3.1.1.狀態

只有在使用者帳號狀態仍在 Active 時，系統會允許使用 Trio 金鑰解密受保護的對話及文件。管理員可視實際需求暫停特定使用者的 Trio 權限。

3.1.2.編輯 - 編輯權限

系統管理員可透過權限設定，為特定使用者提供適當的使用權限。

包含：

FIG. 3.1.2-1 設定使用權限

- filing - 該使用者能否匯出群組對話內容
- forward - 該使用者能否轉發文件至其他對話群組
- invite - 該使用者能否邀請外部聯絡人加入對話群組
- office - 該使用者能否於手機 Trio App，開啟 office 檔案
- VDP - 該使用者能否使用 Trio 安全編輯功能
  僅限有加購 Trio 安全編輯服務的用戶使用

3.1.3.編輯 - 指派角色

可指定特定人員為管理員 (Console Admin) 或監管人員 (Supervisor)。

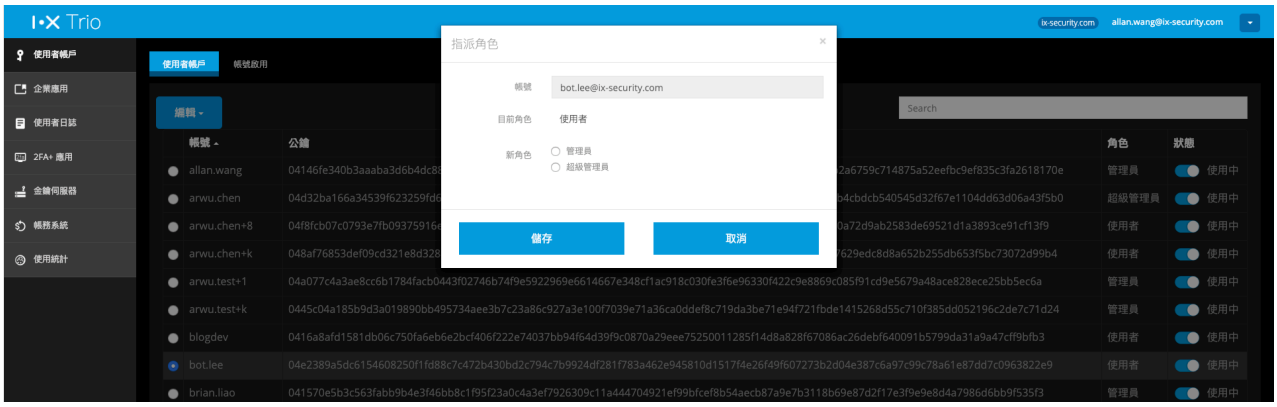


FIG. 3.1.3-1 升級使用者的管理權限

- 系統管理員

系統管理員，為主要管理平台的人。具有權限可管理網域內使用者的金鑰狀態、使用權限、管理對接的服務等。

系統管理員可提升其他使用者成為系統管理員。一旦提升後，該使用者即有權限登入管理平台。

- 監管人員

監管人員，一般為企業負責人。具有權限可取得網域內使用群組的加密內容及檔案的金鑰，因此，具有權限可查看該網域內所有的加密內容。

在系統還沒有 Supervisor 的情況下，系統管理員 (Console Admin) 可提升一位使用者成為 Supervisor；一旦系統具有 Supervisor 後，當要提升其他使用者成為 Supervisor 時，需要至少一位 Supervisor 同意。

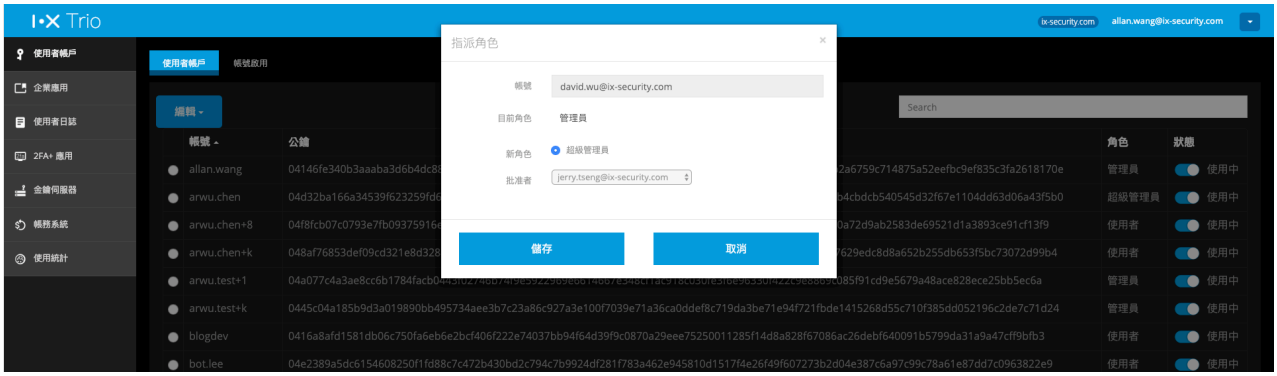


FIG. 3.1.3-2 將使用者升級為監管人員

3.1.4.編輯 - 帳號啟用設定

若您企業的 G Suite 導入 Trio 服務，或您希望將企業網路郵件設定使用 Trio 做身份認證，網域內的所有使用者將必須註冊 Trio 才能存取公司網域的電子郵件，即使是尚未註冊成為 Trio 用戶的員工也是如此。此情況下，必須先協助新員工完成註冊，該員工才能存取網路郵件服務。此時，管理員可透過 **編輯 > 帳號啟用設定**，為該員工設定 **24 小時內**改帳號註冊時，可暫時一併抄送註冊認證信到其他電子郵件信箱，以便在新員工註冊時，為其 Trio 帳號開通。若舊員工因更換手機，重新安裝 Trio 服務，而暫時無法存取郵件完成註冊時，也可以用相同的方式完成註冊。

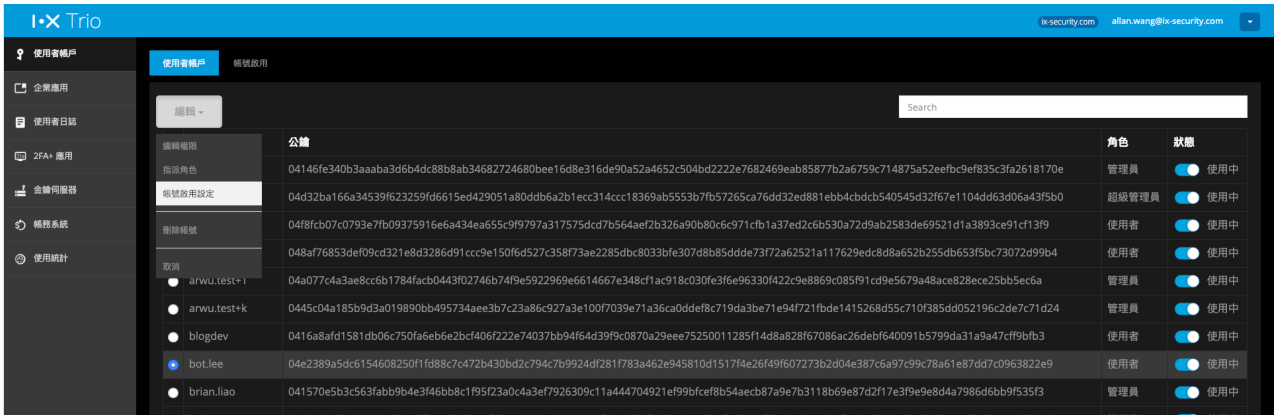


FIG. 3.1.4-1 為帳號開啟帳號啟用設定

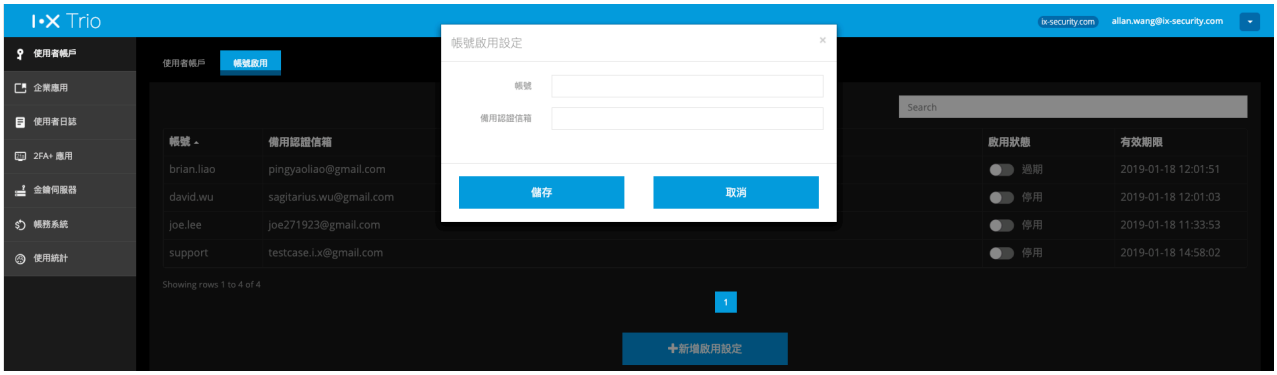


FIG. 3.1.4-2 帳號啟用設定界面

需要注意的是，基於安全性考量，一旦該員工完成註冊，或若此某帳號設定帳號啟用功能超過 24 小時未完成註冊，此臨時設定均會失效或過期。管理員可透過設定，為已過期的帳號啟用設定重新開放。此外，管理員也可透過界面，編輯啟用的內容，或管理已經建立好的相關設定。

3.2. Cloud Gateway

I.X Cloud Gateway，可即時檢驗所有流經的封包合法性，僅允許具備權限的使用者存取指定的網址，相當於企業服務的雲端守門員。

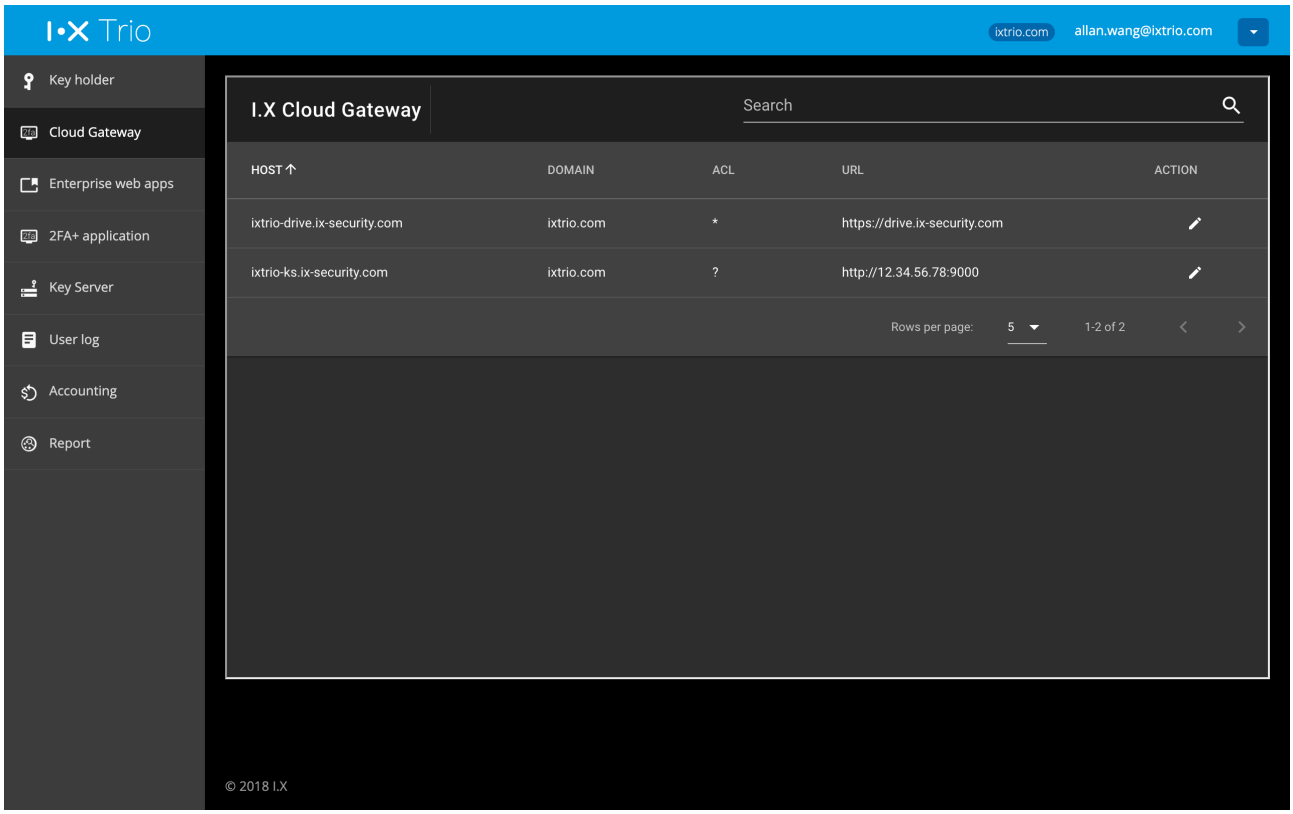


FIG. 3.2-1 I.X CLOUD GATEWAY 畫面

I.X Cloud Gateway 的設定參數說明如下：

欄位名稱	欄位說明
代表路徑 HOST	此欄由 I.X 填寫，不開放修改 (如有需求，請洽 I.X) 企業管理人員取得特定企業應用的代表路徑後，需要將之配置到企業應用的【網址】欄位
企業網域名 DOMAIN	此欄由 I.X 填寫，為企業網域名，不開放修改
ACL	此欄可由企業管理人員依需求設定存取權限。設定參數格式如下： • ? - Cloud Gateway 不檢驗簽章 • * - Cloud Gateway 僅允許帶有 Trio 服務簽章的網路請求，存取指定的代表路徑 • [“user1@DOMAIN”, “user2@DOMAIN”, “user3@DOMAIN”, …] - Cloud Gateway 僅允許名單內的使用者存取指定的代表路徑，該名單的使用和必須為企業內部人員帳號。
URL	此欄由企業管理人員填寫實際的企業應用服務網址

3.3.企業應用

Trio 內建安全瀏覽器，可加強保護您使用網頁型的企業應用服務的資料安全，例如：Web mail、ERP等企業應用服務。安全瀏覽器在使用者的瀏覽過程，都可帶上使用者簽章，讓伺服器得以判別流量的存取者。安全瀏覽器也能為您控管或紀錄使用者存取及下載行為，還可管制使用者複製內文與螢幕截圖的行為。

若您希望將過去企業內部網路才能存取的網頁服務，透過安全的方式開放給外勤人員也可在公司外部使用，可搭配 I.X Reverse Proxy 的服務，確保只有您企業內部員工可透過 Trio 安全瀏覽器，存取該網頁服務。相關細節，請洽詢 I.X 服務人員。

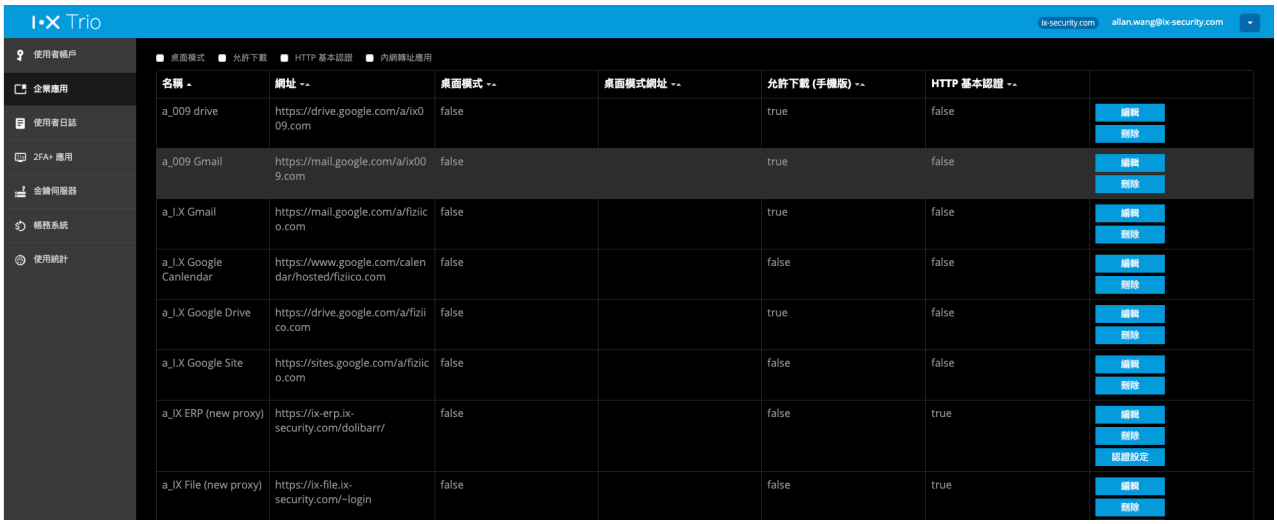


FIG. 3.2-1 企業應用設定頁面

點擊 Add New，新增企業應用服務

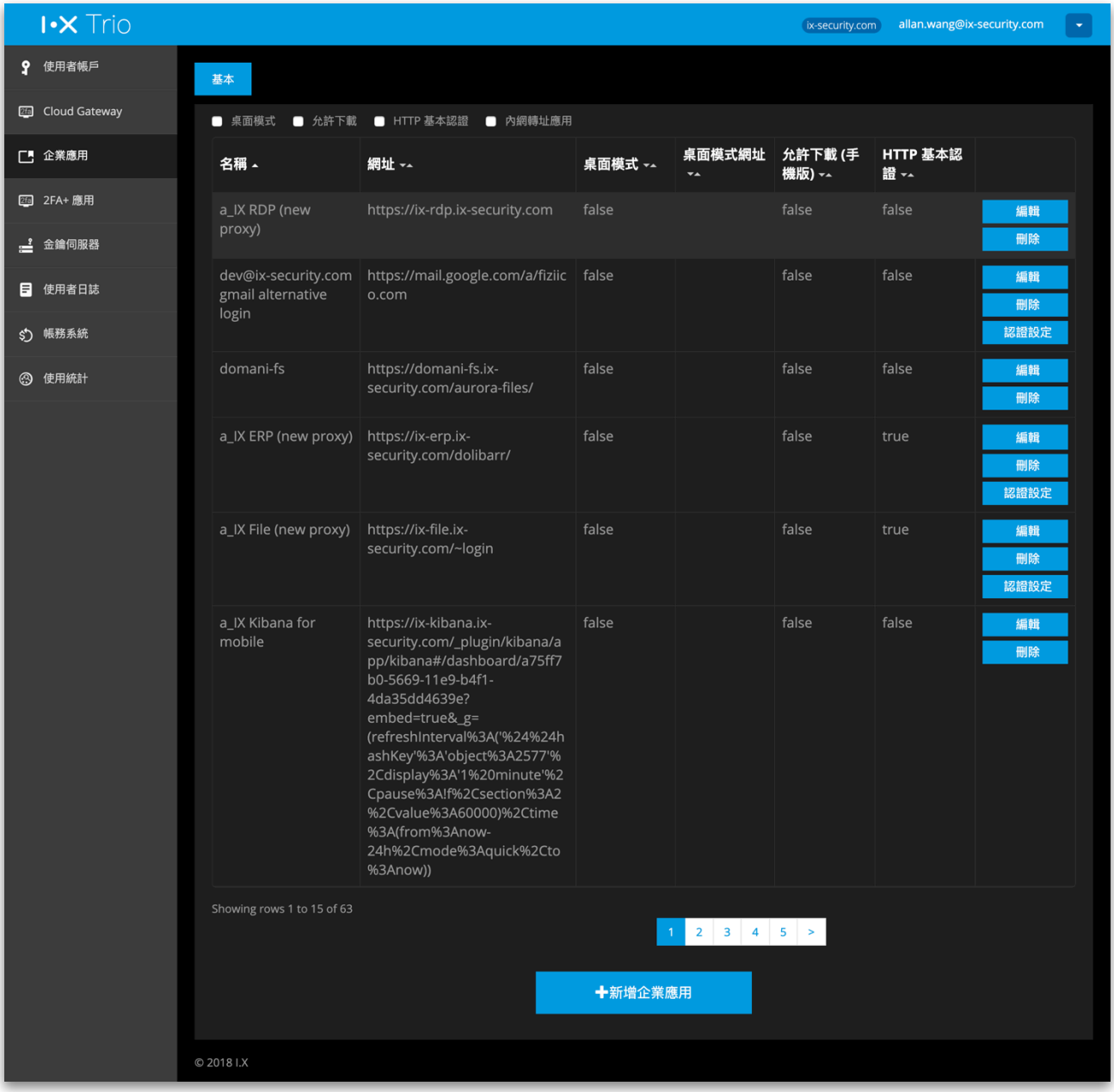


FIG. 3.2-2 新增企業應用服務

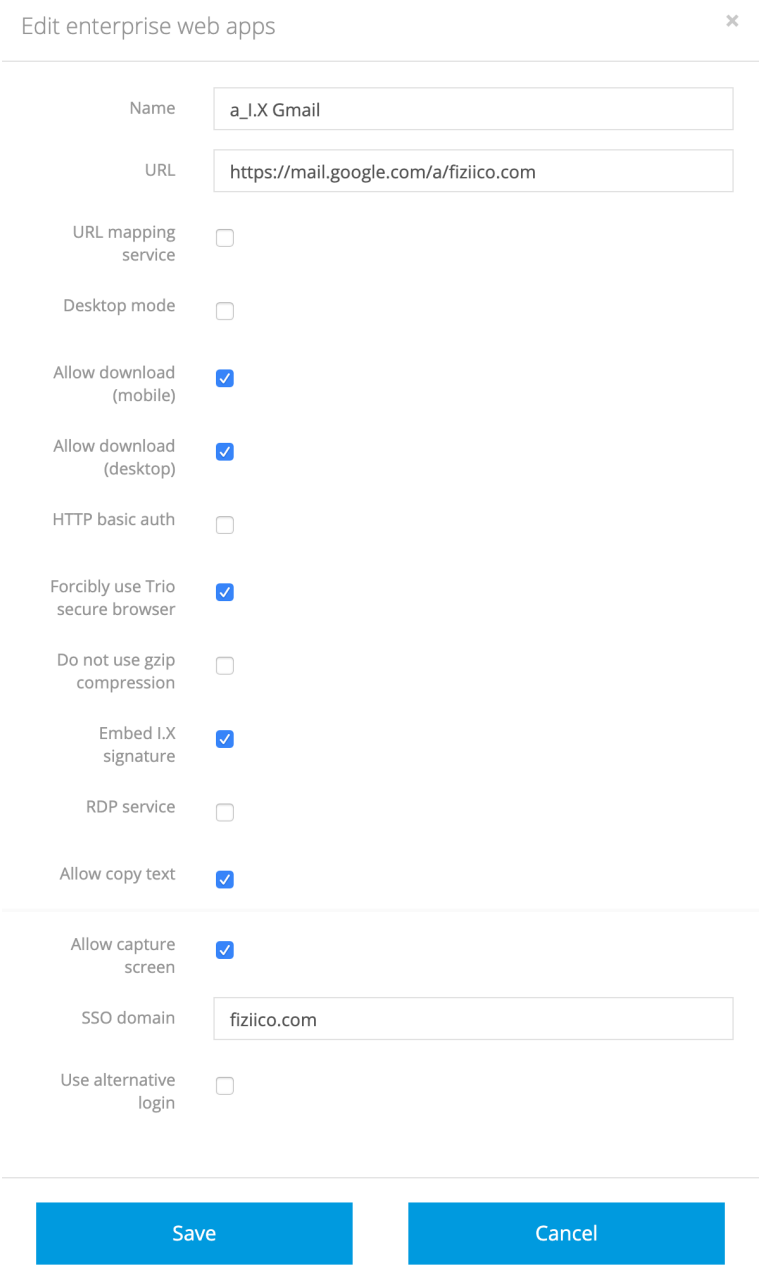
企業應用欄位參數說明

FIG. 3.2-3 企業應用設定

欄位名稱	功能說明	適用情形
名稱 Name	企業應用名稱	必填項目，方便使用者區別不同的企業應用
網址 URL	企業應用服務網址。支援 HTTP/HTTPS	必填項目，用以指定該企業應用服務網址

欄位名稱	功能說明	適用情形
內網轉址應用 URL mapping service	用以關聯某內部網址與可協助連線的外部端口	當企業應用或其內容中的網址需要重新定向到企業內部的另一網址時，使用
桌面模式 Desktop mode	手機模擬電腦版瀏覽器，使用企業應用服務。 **true**: 模擬電腦版瀏覽器 **false**: 維持手機瀏覽器界面	僅適用於手機需要使用電腦版界面時使用
允許下載 (手機版) Allow download (mobile)	是否允許下載*該企業應用服務內的連結檔案。 **true**: 允許下載 **false**: 不允許下載 * 下載僅限手機版，下載到安全檔案區	僅適用於手機需要允許下載檔案到手機安全檔案區
允許下載 (桌面版) Allow download (desktop)	Trio 電腦版是否允許下載*檔案。 **true**: 允許下載 **false**: 不允許下載 * 下載時會對下載畫面截圖，並同步發送下載紀錄到日誌伺服器	僅適用於 Trio 電腦版需要允許下載檔案時使用。
HTTP 基本認證 HTTP basic auth	連線此企業應用時，是否要透過 Trio 完成 HTTP 認證。 **true**: 透過 Trio 做 HTTP 認證。應搭配 Auth Setting 使用 **false**: 不需要透過 Trio 做 HTTP 認證	當企業應用網頁服務支援 HTTP basic auth，且希望統一由 Trio 管理界面設定 HTTP 登入資訊時使用
強制使用安全瀏覽器 Forcibly use Trio secure browser	強制以安全瀏覽器開啟透過安全瀏覽器瀏覽網頁時，點擊的所有網頁連結	當希望企業應用內所有連結都強制限制僅在安全瀏覽器使用時設定
不使用 gzip 壓縮 Do not use gzip compression	瀏覽此企業應用時，是否不允許使用 gzip 壓縮 **true**: 不使用 gzip **false**: 允許使用 gzip	當該企業應用可能會查詢資料庫，且可能回傳大量資料時使用
嵌入 I.X 簽章	使用此企業應用時，安全瀏覽器是否要挾帶使用者的金鑰簽章 **true**: 挾帶使用者簽章 **false**: 不帶使用者簽章	因部分網頁服務會阻擋無法識別的 User Agent 內容，此情況下，可移除 I.X 簽章
遠端桌面服務	此企業應用是否為遠端桌面服務 **true**: 為遠端桌面服務 **false**: 非遠端桌面服務	當該企業應用是遠端桌面服務時，此選項必須打勾
允許拷貝文字	允許拷貝文字時，當使用者拷貝文字，系統將紀錄拷貝的完整內容 **true**: 允許拷貝文字 **false**: 不允許拷貝文字	
允許螢幕截圖	允許使用者擷取此企業應用的使用畫面。 **true**: 允許擷取畫面 **false**: 不允許擷取畫面	使用者擷取畫面時，會留存紀錄；但若擷取畫面的同時
SSO 網域 SSO domain	指定此企業應用的 SAML 網域	若設定 SAML Login 時，此為必填項目

欄位名稱	功能說明	適用情形
使用代登入功能 Use alternative login	為 G Suite 群組帳號設定代登入帳號，僅在 SSO 網域有設定時可設定	適用於需要為 G Suite 群組帳號代登入時使用
代登入信箱 Login email	群組帳號信箱，而可為該帳號代登入的帳號，則在 Auth Setting 中指定	群組帳號不能為 Trio 帳號



若選擇需要認證，Trio 允許將使用者帳號密碼建立在 Console 上，讓使用者僅需登入 Trio，即可使用需要認證的企業應用服務。此時，需要搭配設定 Auth Setting。若 Auth Setting 有設定使用者的登入帳號、密碼，Trio App 會自動使用該帳號、密碼嘗試登入；若未設定，則 Trio App 會提供界面輸入登入帳號、密碼。

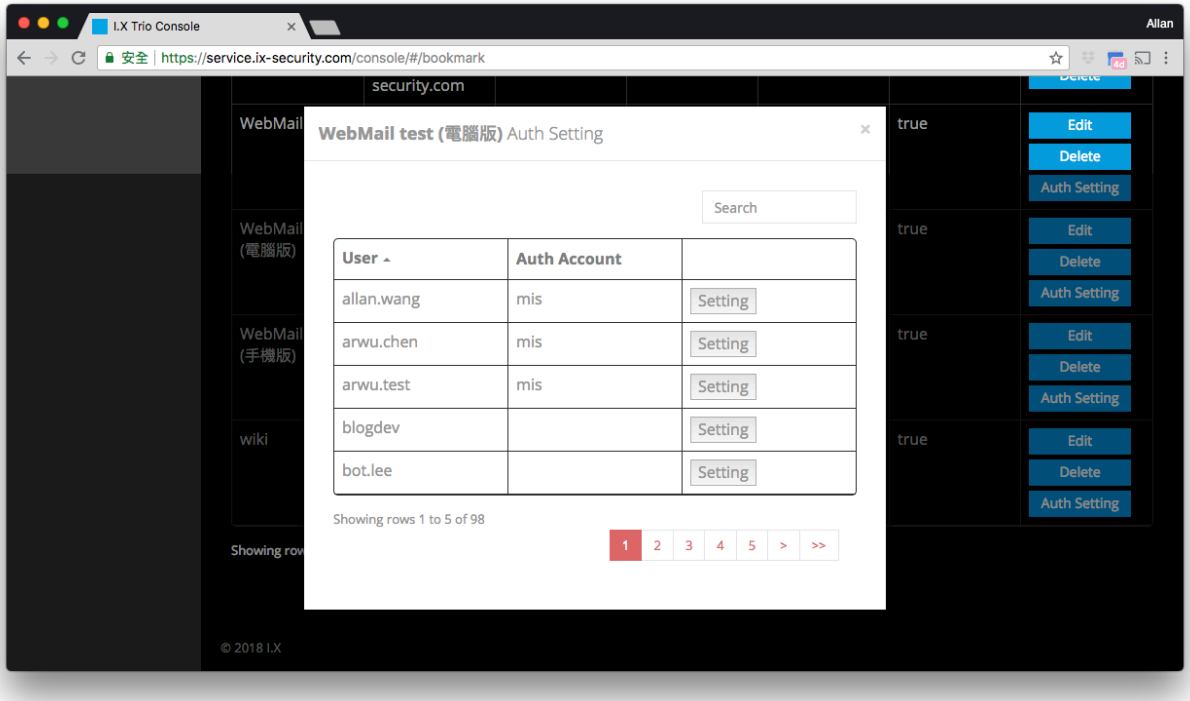


FIG. 3.2-3 編輯 AUTH SETTING 的畫面

3.3.1. I.X Cloud Gateway

以往企業員工在公司外要存取內網的網頁應用服務時，如 ERP 等內部網站，必須先撥入 VPN，才能存取該網頁應用服務；然而，一旦撥入 VPN，相當於進入企業內網環境，若未經妥善管理，反而容易成為資安漏洞。I.X 提供的安全瀏覽器搭配 I.X Cloud Gateway 的方案，讓您可在不開放 VPN 的情況下，即可允許企業員工，自公司外存取內網的網頁應用服務。
圖 3.2.1-1 為使用 I.X Cloud Gateway 時的網路連線示意圖。透過 I.X Cloud Gateway，可以協助您確保來自企業外部的連線請求者，為您核可的員工使用 I.X Trio 安全瀏覽器發起的連線請求。

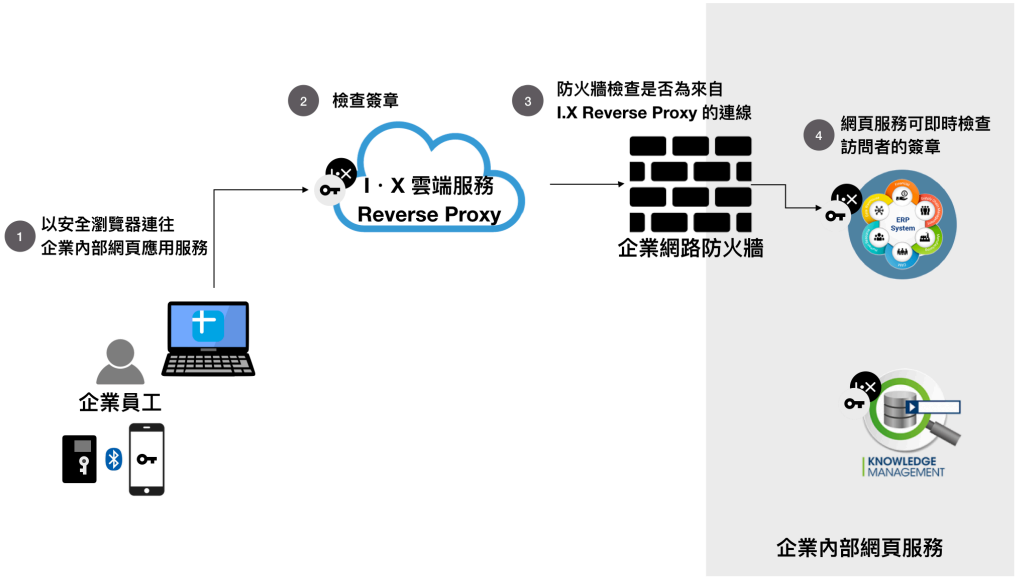


FIG. 3.2.1-1 使用 I.X CLOUD GATEWAY 網路連線示意圖

3.3.2. 如何為網頁應用服務設定 I.X Cloud Gateway

相關需求

為確保連線的安全性，要透過 I.X Cloud Gateway 服務接入的網頁應用伺服器，必須支援

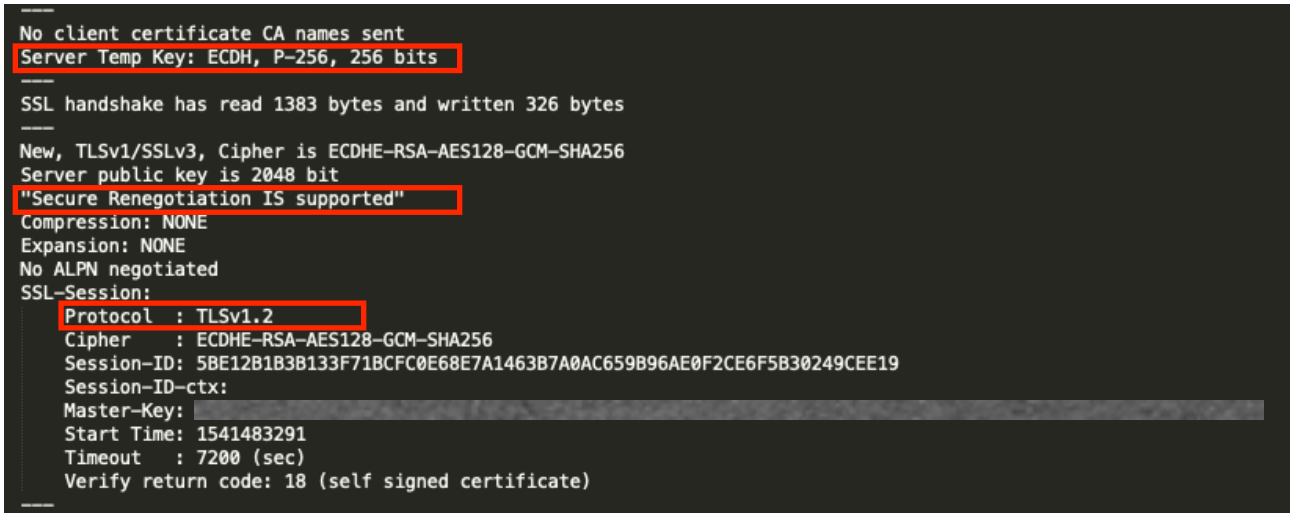
- TLS v1.2
- Secure Renegotiation
- Server Temp Key 支援 ECDH, P-256, 256 bits

檢查網頁應用伺服器支援的安全連線

您可使用 openSSL client 以下列指令測試您的網頁伺服器

```
openssl s_client -connect <host:port>
```

執行完畢後，應可看到結果如下：



設定企業網路防火牆

企業網路防火牆必須允許來自 I.X Cloud Gateway IP 地址，向特定端口發送網頁連線請求，當防火牆收到請求後，再將請求轉送到指定的網頁伺服器內部 IP 地址。

設定 I.X Reverse Proxy

請 I.X 管理人員協助，並提供 I.X Cloud Gateway 應向哪個 IP 及 端口發送網頁連線請求，I.X 管理人員會為您的特定企業應用設定 I.X Reverse Proxy 服務，並於設定完成後，告知您專屬於此企業應用服務對應的 I.X Reverse Proxy 服務網址，以便您接續於 Trio 管理平台之企業應用服務設定相應的服務項目。

(可選) 網頁伺服器動態檢查請求者身份

為了確保安全，I.X Trio 安全瀏覽器在訪問企業應用服務時，都會在請求中帶上使用者的身份簽章。若您有極高的安全需求，您可在網頁伺服器收到網頁訪問請求時，驗證該請求是否來自您企業內部的 Trio 使用者透過 Trio 安全瀏覽器發送出來的，並做相應的權限控制。

3.3.3. 為轉址到內網的連結設定內網轉址應用

若您的企業應用服務網頁內，有部分連結導向其他內網伺服器或其他僅內部網路可存取的網頁服務，您必須設定內網轉址應用。例如 ERP 內的某張表單附件，指向內網另一不直接對外開放的檔案伺服器的文件。此時，需要為檔案伺服器建立一內網轉址應用設定，以告知安全瀏覽器該內網網址所對應的防火牆公網網址為何，並且，防火牆需搭配設定將特定連接埠的請求，導向該檔案伺服器。

	URL provided Web item (由 I.X 提供)	Firewall Public IP	Intranet IP
ERP	https://server1.ix-security.com	https://1.2.3.4:8000	https://10.1.1.10
檔案伺服器	https://server2.ix-security.com	https://1.2.3.4:9000	https://10.1.1.20

TABLE 3.2.3-1 設定範例之 IP 表

企業應用設定範例

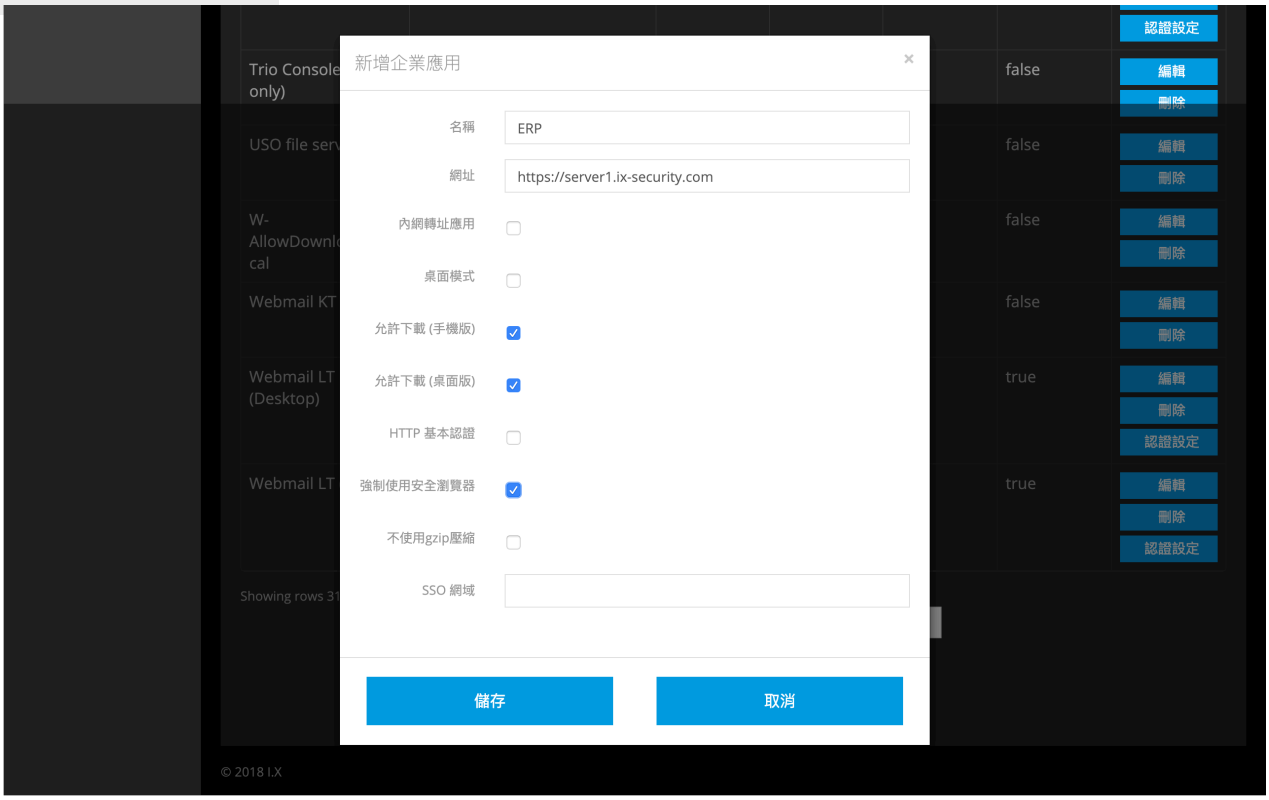


FIG.3.2.3-1 範例 ERP 之企業應用設定

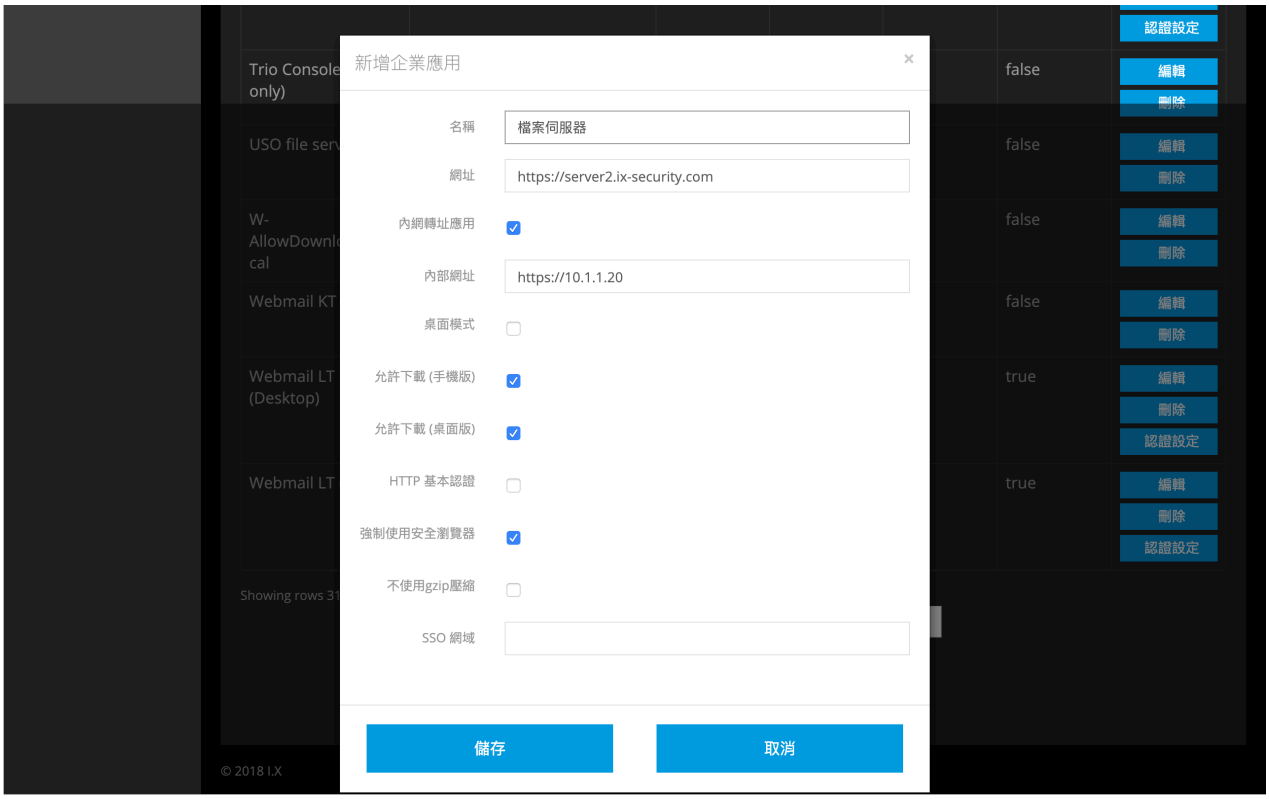


FIG.3.2.3-2 範例中，不直接對外開放之檔案伺服器內部轉址設定

3.3.4.SSO 相關設定

若您設定的企業應用服務支援 SAML，您可設定使用 Trio 作為您的身份認證服務提供商 (IdP, Identity Provider)，為您驗證登入服務的使用者身份。例如，若您希望由 Trio 為您的 Google G Suite 服務認證身份，您可以下範例說明。

範例情境

以下範例為某企業為 G Suite 用戶，希望導入 I.X Trio SSO 解決方案，解決以下問題：

- 以 Trio 的簽章機制認證身份，加強 G Suite 身份認證的安全性
- 強制企業員工僅能使用安全瀏覽器，存取 Gmail 及 Google Drive
- 允許員工可下載 Gmail 附件及 Google Drive 文件，但需要留存下載紀錄
- 企業客服部門使用群組帳號 support@company.com 統一作為與客戶的聯絡窗口，因此，所有客服人員都需要可登入客服部門的群組帳號

以下設定範例，僅針對管理平台企業應用設定 G-mail 及 Google Drive 相關設定說明。G Suite 導入 Trio 身份認證的設定方式，請參考 “G Suite存取權限管理設定指南”。

新增 Gmail企業應用

於 **企業應用** 頁面分別新增 Gmail 如下：

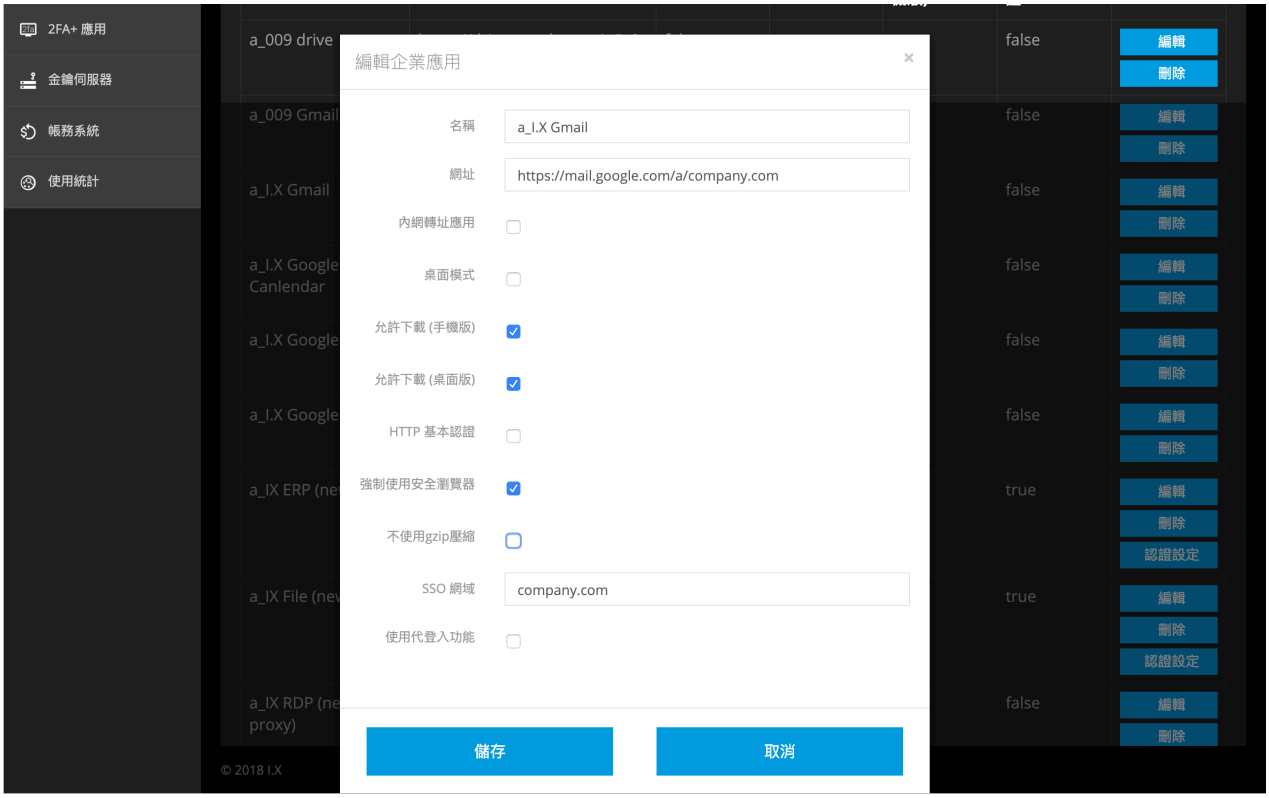


FIG. 3.2.4-1 COMPANY.COM 新增 GMAIL 企業應用設定範例

欄位名稱	設定值	說明
名稱	a_I.X Gmail	依易於辨識的名稱設定即可

網址	https://mail.google.com/a/company.com	依公司 gmail 的服務網址填寫
允許下載 (手機版)	勾選	若勾選，手機 Trio App 可將此企業應用 (Gmail) 的圖檔 (JPG, PNG) 及 Office 文件檔 (doc(x), xls(x), ppt(x)) 以加密的形式存於儲存於手機的儲存空間 若未勾選，則安全瀏覽器不允許下載此企業應用 (Gmail) 附件
允許下載 (桌面版)	勾選	若勾選，Trio 電腦版可將此企業應用 (Gmail) 的所有附件，以未加密的方式儲存在電腦上，並於儲存時，留存下載紀錄 若未勾選，則安全瀏覽器不允許下載此企業應用 (Gmail) 附件
強制使用安全瀏覽器	勾選	由於，Gmail 企業應用是採 SAML Login，因此，SSO 網域需要填上要登入的網域名稱
SSO 網域	company.com	依公司網域填寫

TABLE 3.2.4-1 COMPANY.COM 新增 GMAIL 企業應用的設定說明

新增 Google Drive 之企業應用

於 **企業應用** 頁面分別新增 Gmail 如下：

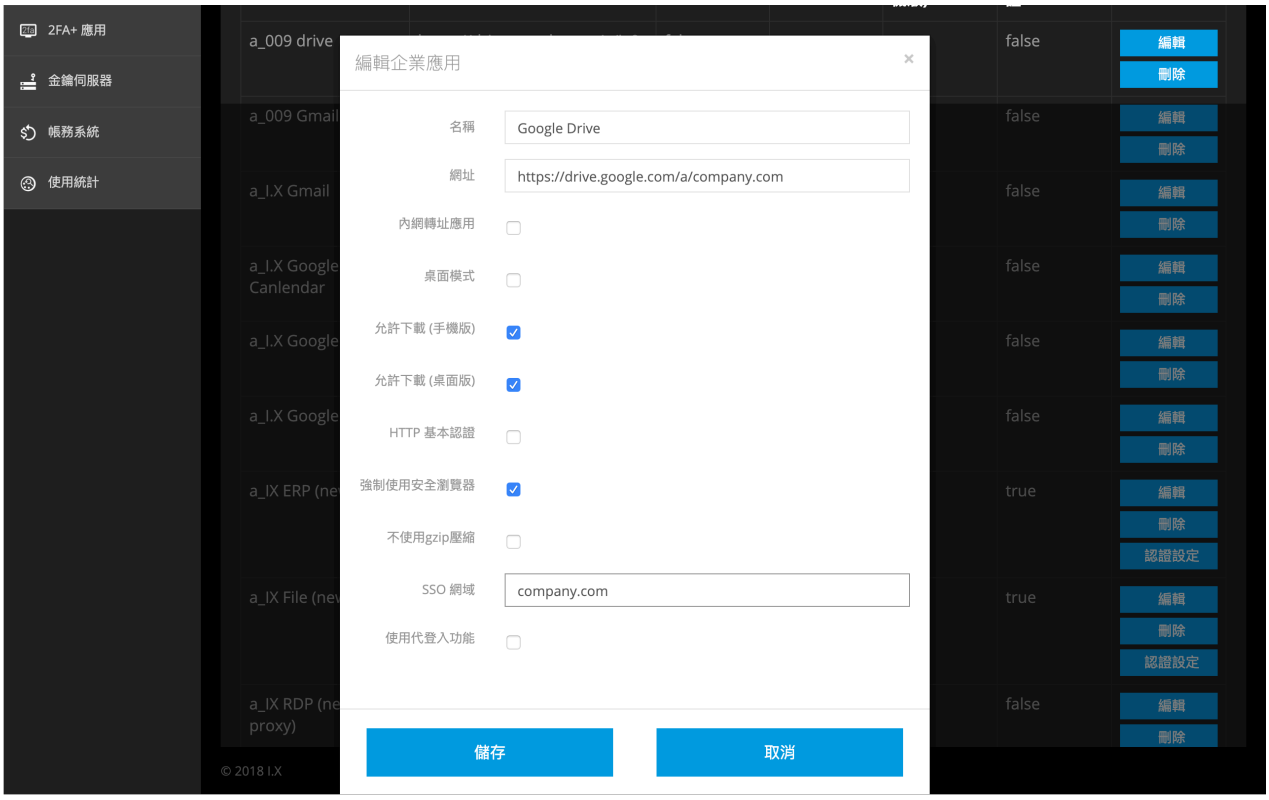


FIG. 3.2.4-2 COMPANY.COM 新增 GOOGLE DRIVE 企業應用設定範例

欄位名稱	設定值	說明
名稱	Google Drive	依易於辨識的名稱設定即可
網址	https://drive.google.com/a/company.com	依公司 Google Drive 的服務網址填寫
允許下載 (手機版)	勾選	若勾選，手機 Trio App 可將此企業應用 (Google Drive) 的圖檔 (JPG, PNG) 及Office 文件檔 (doc(x), xls(x), ppt(x)) 以加密的形式存於儲存於手機的儲存空間 若未勾選，則安全瀏覽器不允許下載此企業應用 (Google Drive) 檔案
允許下載 (桌面版)	勾選	若勾選，Trio 電腦版可將此企業應用 (Google Drive) 的所有檔案，以未加密的方式儲存在電腦上，並於儲存時，留存下載紀錄 若未勾選，則安全瀏覽器不允許下載此企業應用 (Google Drive) 檔案
SSO 網域	company.com	依公司網域填寫

TABLE 3.2.4-2 COMPANY.COM 新增 GOOGLE DRIVE 企業應用的設定說明

為客服部門群組帳號設定代登入方式

Trio 支援為相同網域之群組帳號指定可代為登入的功能，該群組帳號必須非 Trio 帳號，以範例為例，亦即不能存在 support@company.com 的 Trio 帳號。本設定範例為說明如何指定哪些人員可用自己帳號，登入使用 support@company.com 的 Gmail 信箱。

為 Support 的 Gmail 信箱建立一獨立的企業應用：

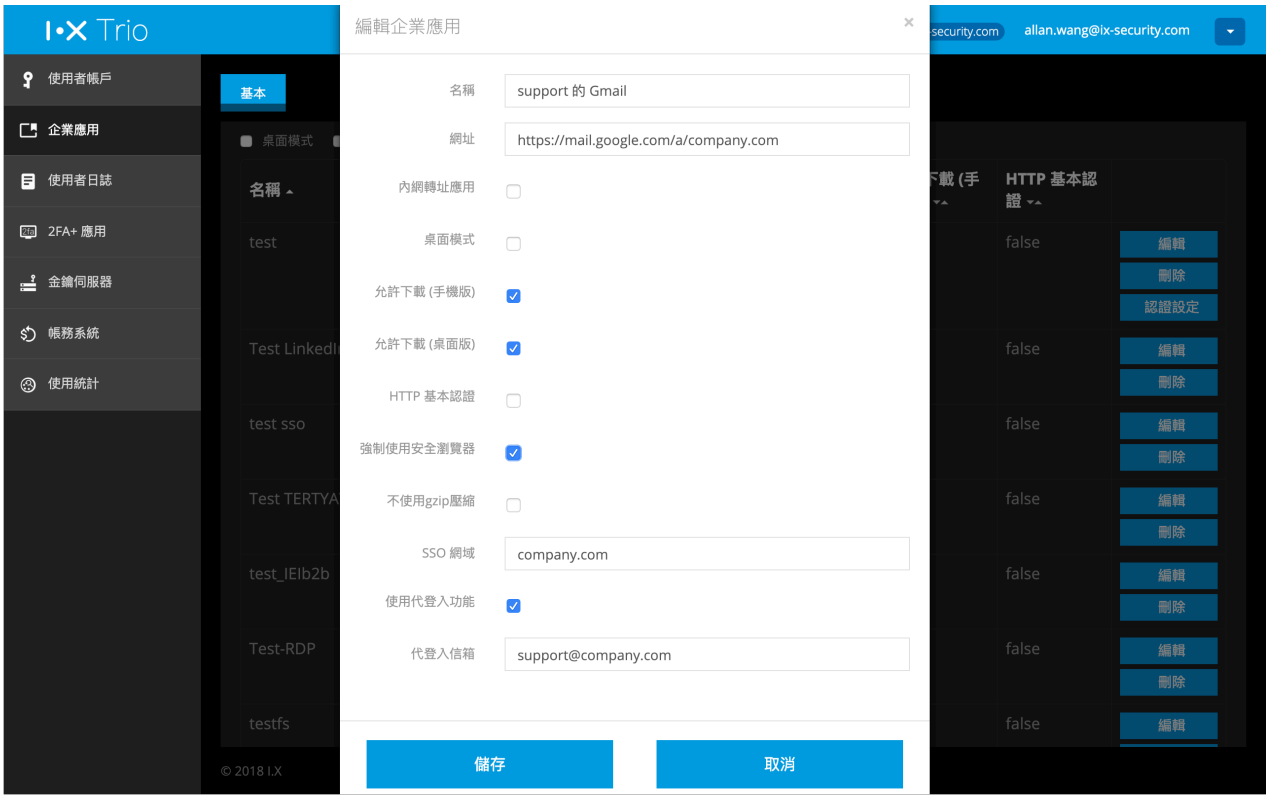


FIG. 3.2.4-3 為客服部門群組帳號設定代登入方式

欄位名稱	設定值	說明
名稱	support 的 Gmail	依易於辨識的名稱設定即可
網址	https://mail.google.com/a/company.com	(同 TABLE 3.2.4-1)
允許下載 (手機版)	勾選	(同 TABLE 3.2.4-1)
允許下載 (桌面版)	勾選	(同 TABLE 3.2.4-1)
強制使用安全瀏覽器	勾選	(同 TABLE 3.2.4-1)
SSO 網域	company.com	(同 TABLE 3.2.4-1)
使用代登入功能	勾選	勾選以使用代登入功能
代登入信箱	support@company.com	填寫需要代登入的群組帳號。 注意！此群組帳號不能為 Trio 的使用者帳號

TABLE 3.2.4-3 客服部門群組帳號專用之企業應用設定範例

代登入帳號設定完後，於外部的 “認證設定” 指定可代登入的使用者

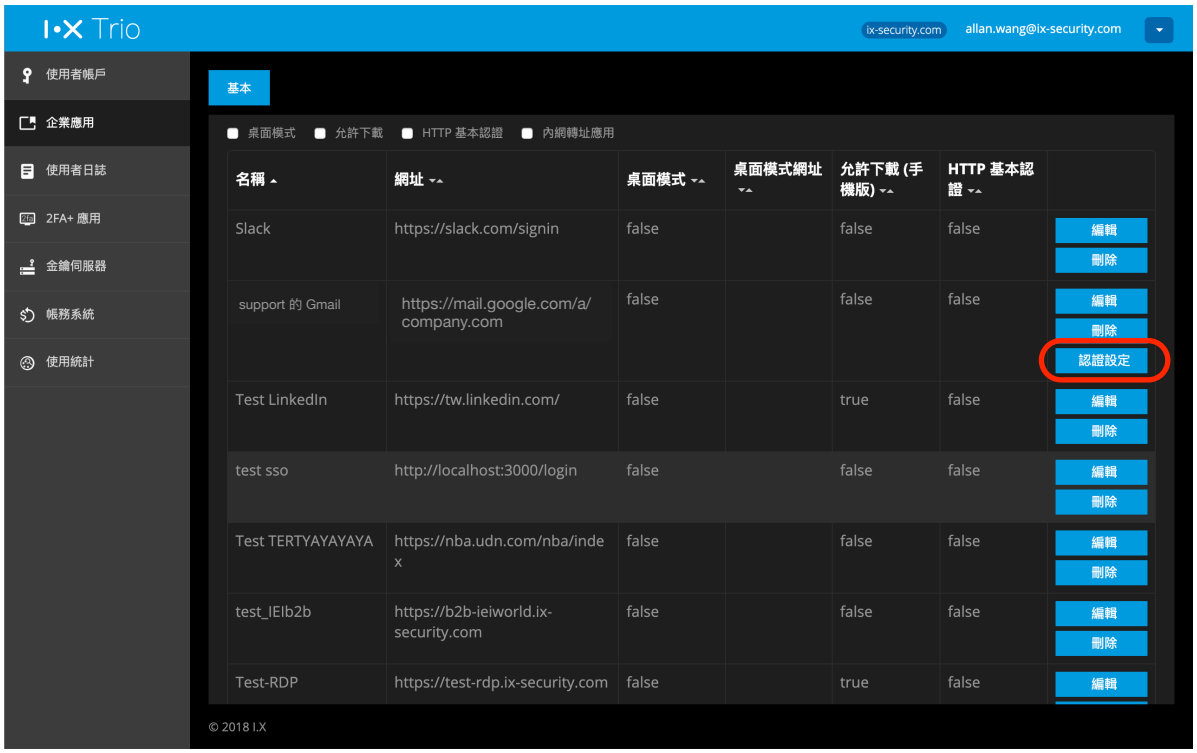


FIG. 3.2.4-4 到 “認證設定” 指定可代登入的使用者

點選要指定可代登入的 Trio 使用者，該使用者即可以自己的帳號，透過 “support 的 Gmail” 登入 support@company.com 的 Gmail 信箱。需要注意的是，進入代登入帳號信箱前，安全瀏覽器必須先登出自己的信箱。

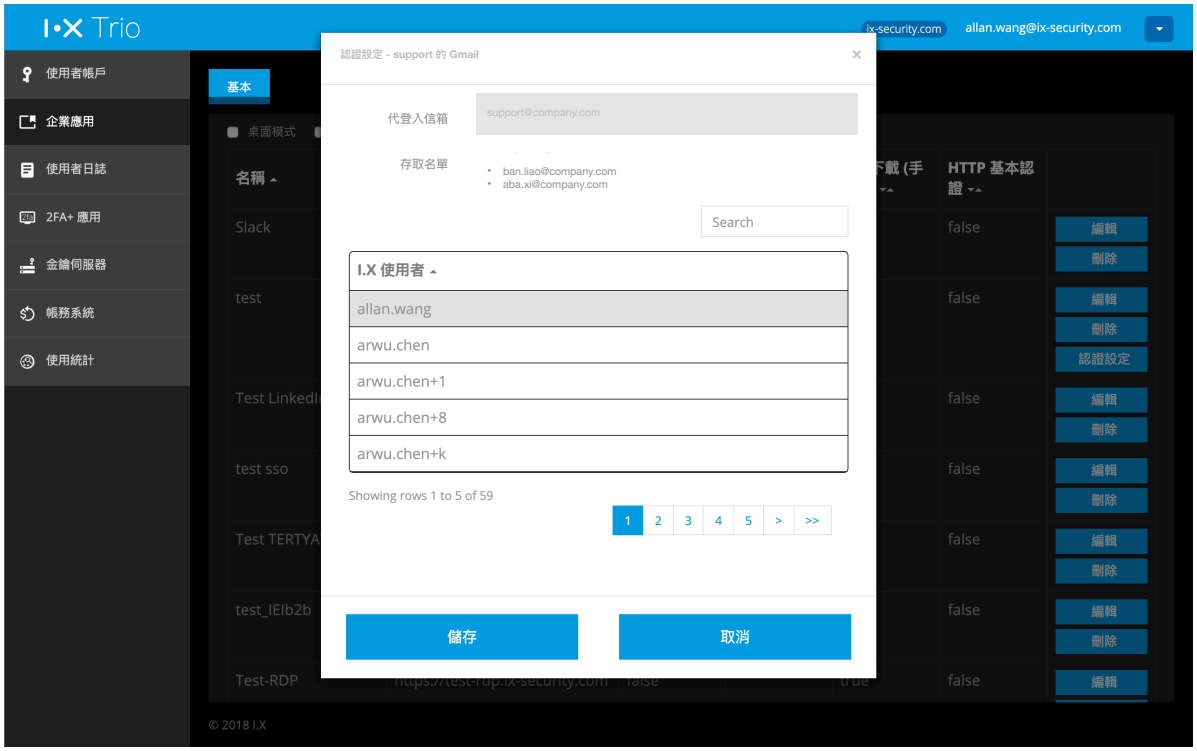


FIG. 3.2.4-5 指定可代登入的使用者

3.4.使用者日誌

您可以透過使用者日誌功能，查看企業內 Trio 使用者的使用行為，此頁面預設可查詢近 7 天的日誌，包含系統登入 (2FA+)、通話紀錄、檔案分享、匯出、群組警告 (在對話或檔案預覽時截圖)，及企業應用中的截圖行為。

3.4.1. 系統登入 (2FA+)

所有透過 Trio 2FA 登入的紀錄，包含登入管理平台、Trio Desktop、以 2FA+ 整合 Trio 2FA 的紀錄。

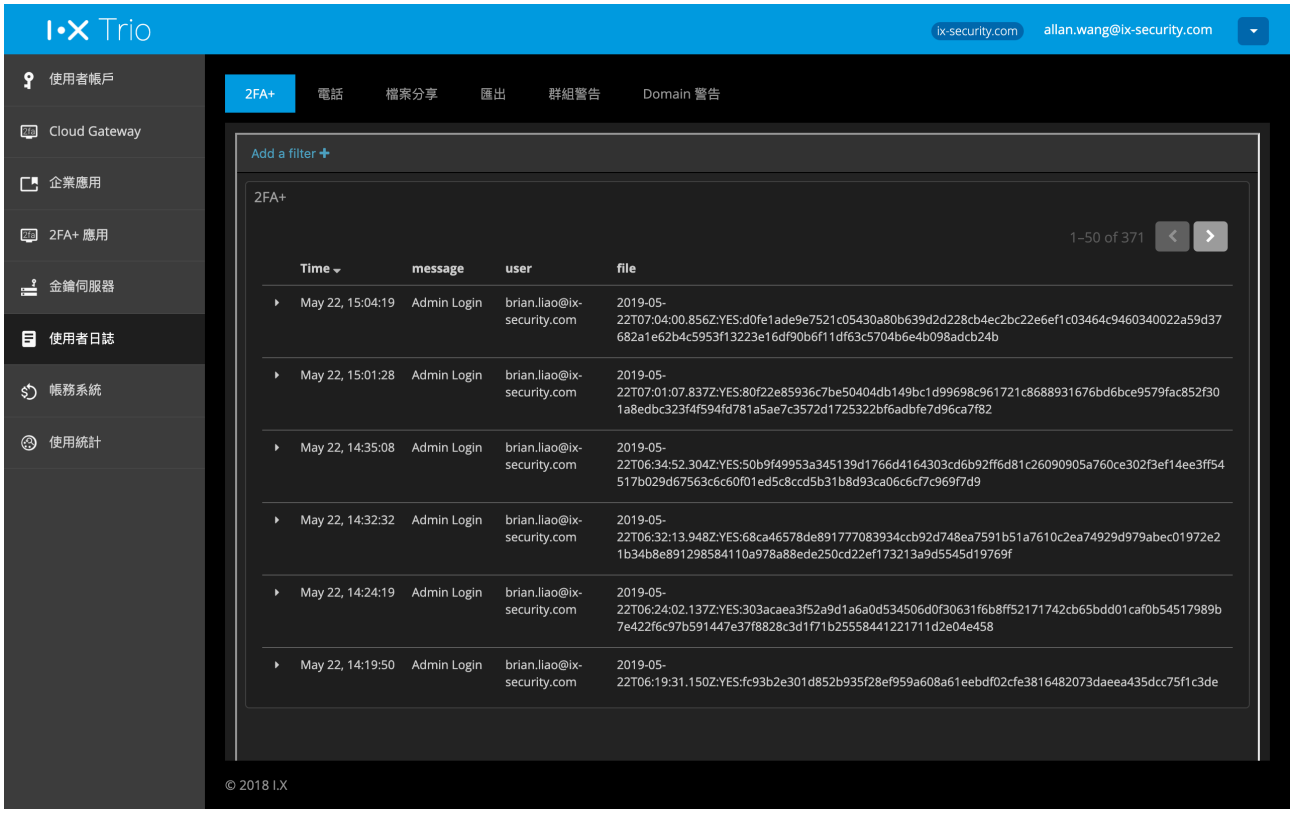


FIG. 3.3-1 使用者系統登入 (2FA+) 紀錄

欄位說明：

欄位名稱	欄位說明
Time	使用者登入系統時，回應 2FA 通知的時間
message	登入的系統
user	此次登入的使用者帳號
file	此次回應 2FA 時，使用者簽回的簽章內容

3.4.2.通話紀錄

在【電話】分頁中，您可看到企業員工透過 Trio 撥打及接聽電話的紀錄。

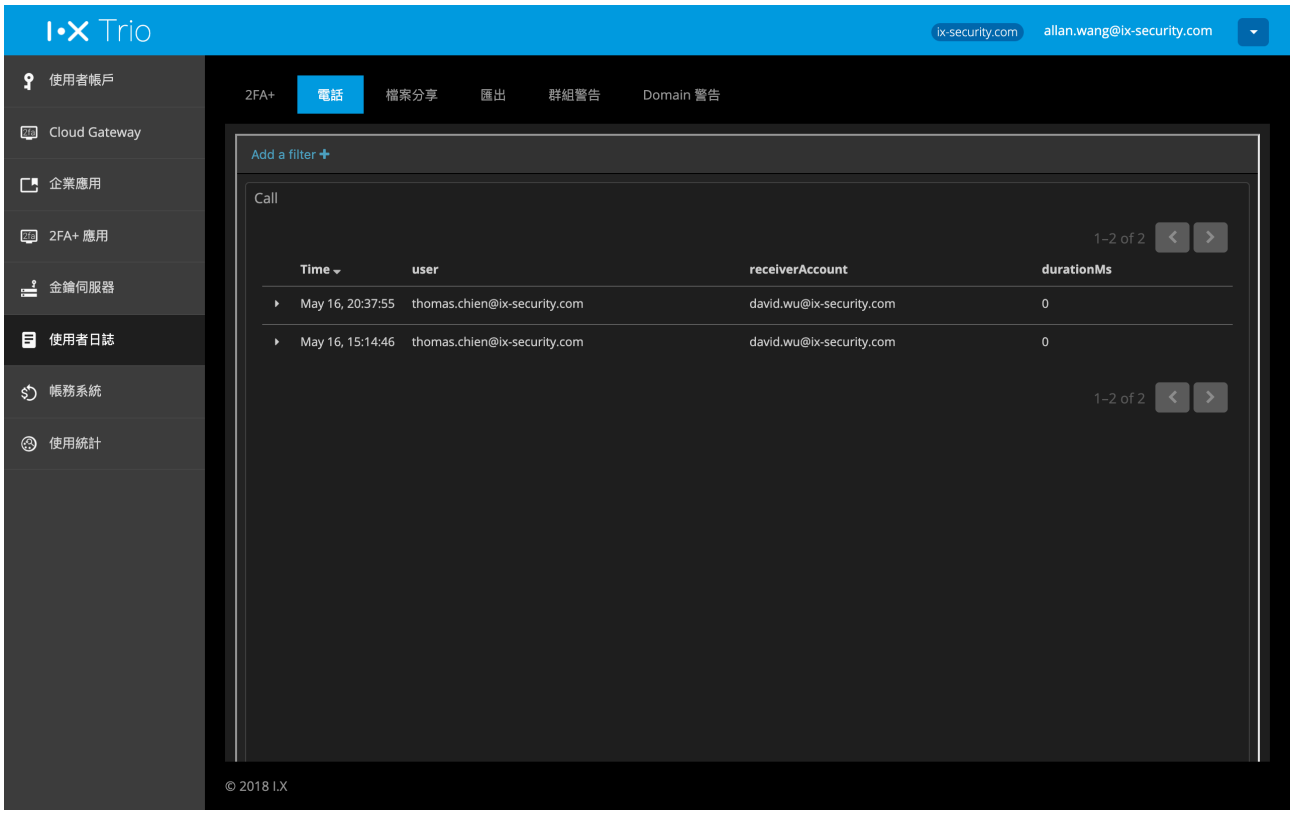


FIG. 3.4.2-1 使用者通話紀錄

欄位說明：

欄位名稱	欄位說明
Time	撥打電話的時間
user	撥打電話的使用者帳號
file	接聽電話的使用者帳號
message	通話時間長度 (ms) 或斷線問題原因

3.4.3. 檔案分享

在【檔案分享】頁面，您可查看企業內部使用者透過 Trio IM，分享檔案的狀況，以及接收者閱讀檔案的狀況。

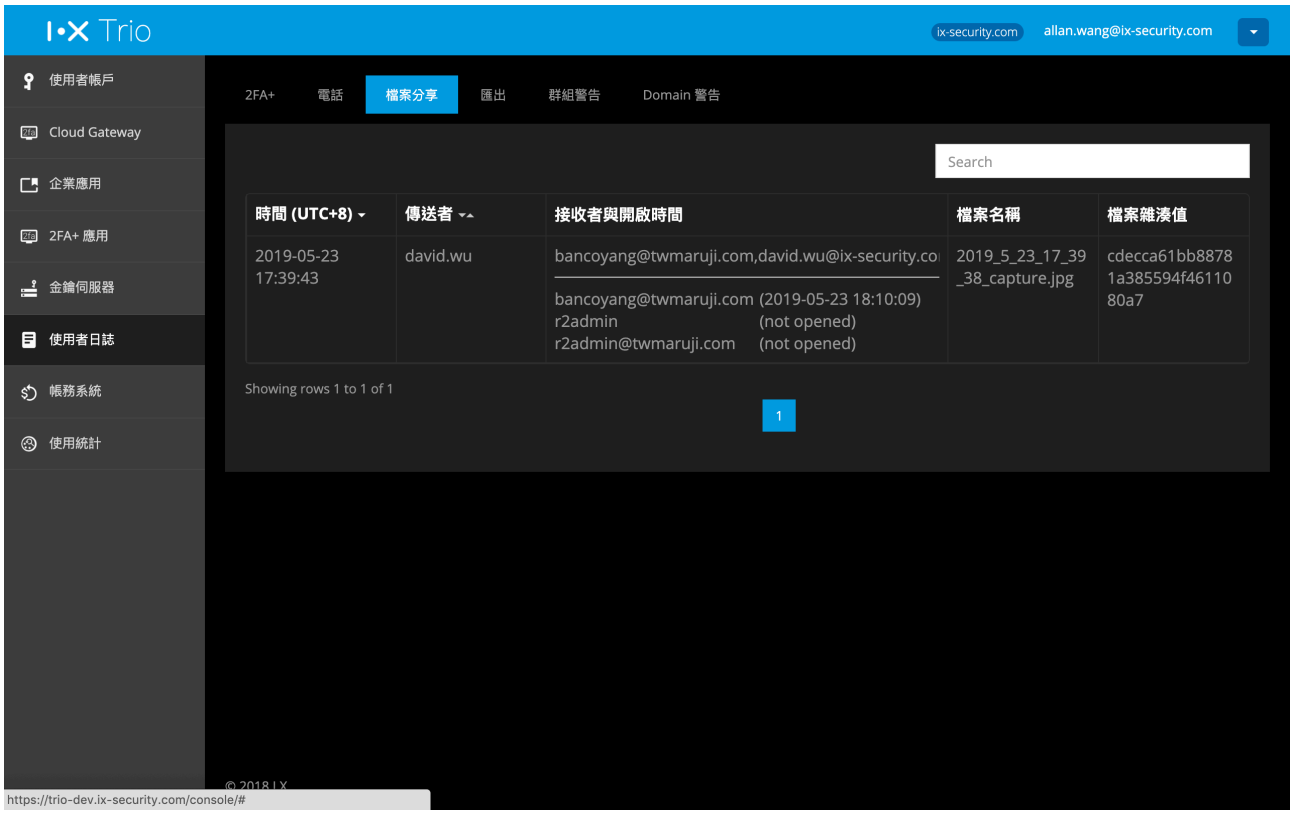


FIG. 3.4.3-1 使用者在 TRIO IM 中，分享檔案的紀錄與狀態

欄位說明：

欄位名稱	欄位說明
時間	使用者傳送檔案的時間
傳送者	檔案傳送者的使用者帳號
接收者與開啟時間	分隔線以上為傳送的群組名稱 分隔線以下為群組內所有使用者 括弧內為各個接收者開啟檔案的狀態或時間
檔案名稱	檔案名稱
檔案雜湊值	檔案的雜湊值，可用以分辨相同的檔案

3.4.4. 匯出

在【匯出】分頁中，可查看使用者匯出群組對話的紀錄。

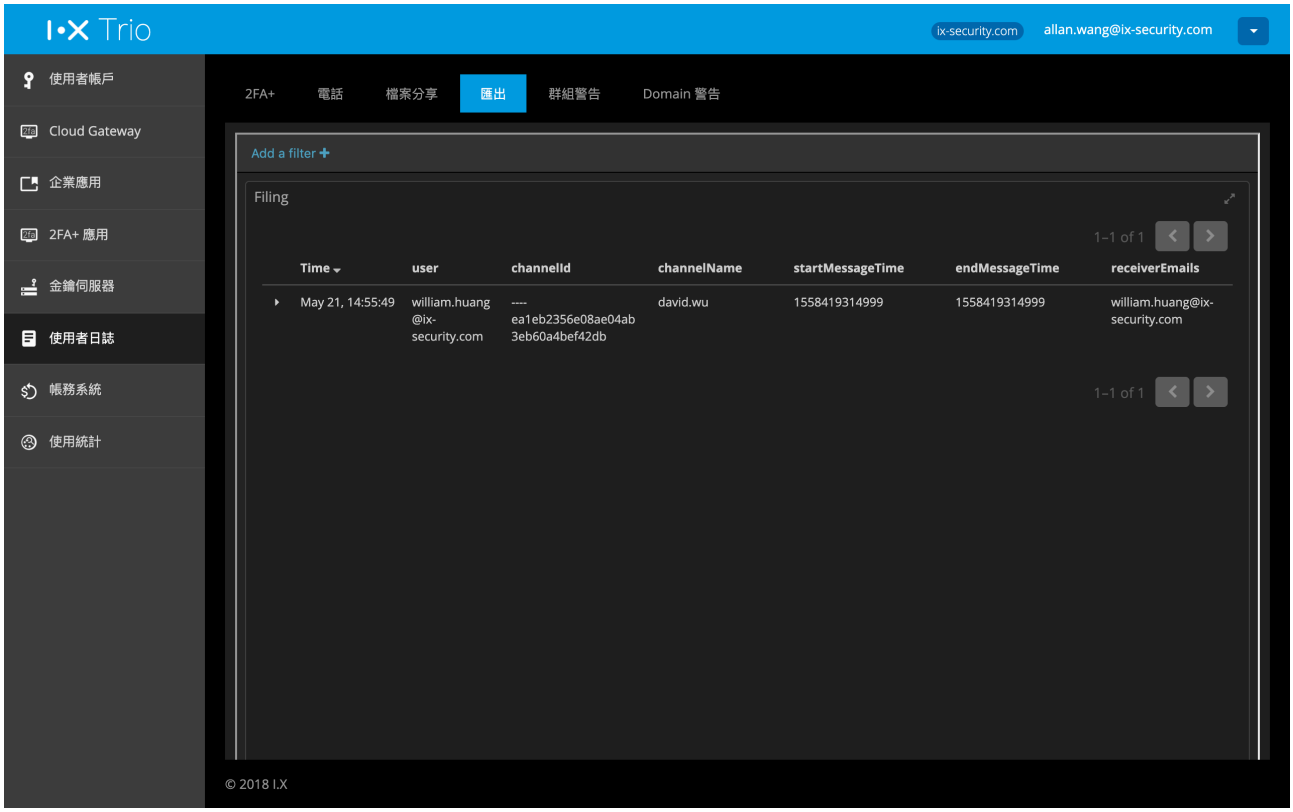


FIG. 3.4.4-1 使用者匯出群組對話紀錄

欄位說明：

欄位名稱	欄位說明
Time	匯出群組對話的時間
user	執行匯出群組對話的使用者
channelId	匯出對話的群組 ID (方便在系統上查詢)
channelName	匯出對話的群組名稱
startMessageTime	匯出對話串的起始時間
endMessageTime	匯出對話串的結束時間
receiverEmails	匯出時的接收者 email 列表

3.4.5. 群組警告

當 iPhone 使用者在群組對話界面中截圖，會發送群組警告，並顯示在【群組警告】分頁中。

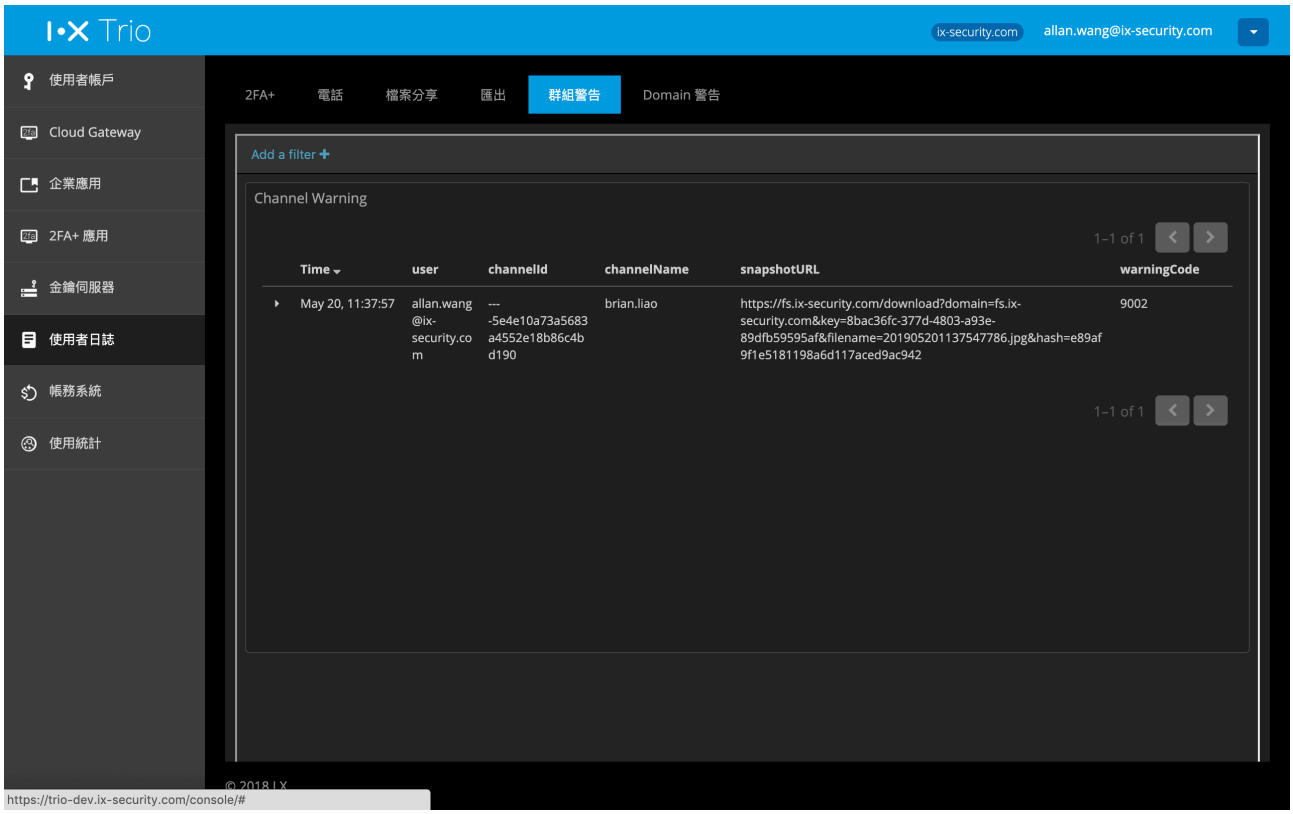


FIG. 3.4.5-1 IPHONE 使用者擷取對話畫面的紀錄

欄位說明：

欄位名稱	欄位說明
Time	使用者截圖時間
user	截圖的使用者帳號
channelId	截圖的群組對話 ID
channelName	截圖的群組對話名稱
snapshotURL	截圖內容備份

3.4.6. Domain 警告

當 iPhone 使用者在企業應用中截圖，會發送 Domain 警告，並顯示在【Domain 警告】分頁中。

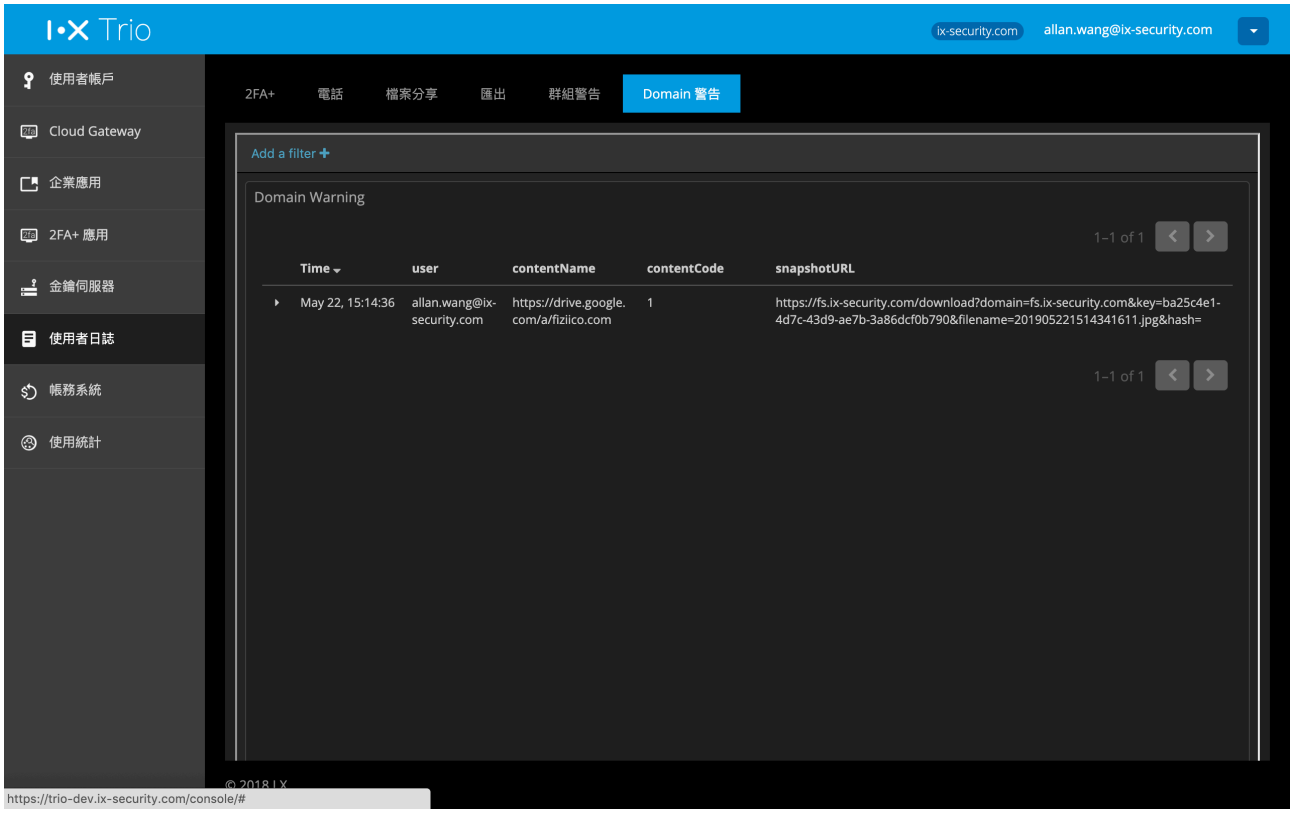


FIG. 3.4.6-1 IPHONE 使用者在企業應用中的截圖紀錄

欄位說明：

欄位名稱	欄位說明
Time	使用者截圖時間
user	截圖的使用者帳號
contentName	企業應用名稱
snapshotURL	截圖內容備份

3.5. 2FA+應用

若您企業內其他系統的身份認證機制也希望導入 2FA，借助 Trio 為您把關，您可於應用服務內新建一服務。

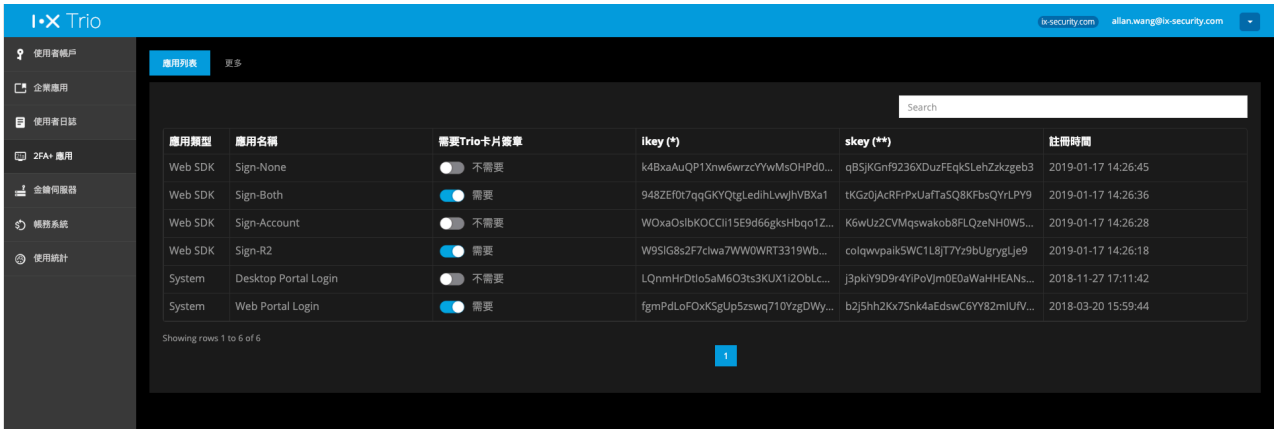


FIG. 3.4-1 應用服務設定頁面

在 More 的頁面中，選擇 Web SDK，點擊 ＋New App，設定登入時，是否必須使用卡片金鑰做簽章。建立完成後，系統會提供一組 ikey、skey，讓應用服務呼叫 Web SDK 時使用。

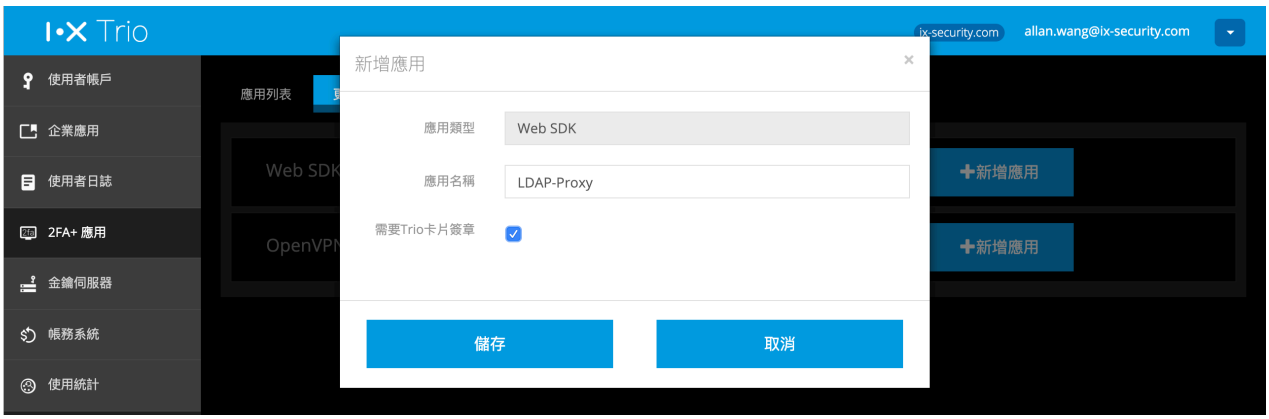


FIG. 3.4-2 新增應用服務設定頁面

您可參照附錄設定範例，了解相關使用方式。

3.6. 金鑰伺服器

除了 Trio 卡片外，您還可添購金鑰伺服器。當您的企業配置有金鑰伺服器時，您網域內的使用者日常使用 Trio 服務將不需要隨時帶著 Trio 卡片，直到登入較重要的系統，再開啟自己的 Trio 卡片登入系統即可。如需更多資訊，請洽詢 I.X 或 I.X 經銷商。

3.7. 帳務系統

若您為預付費的企業用戶，當員工帳號於接下來三個月內即將到期，系統會寄送通知信件提醒您，或者，您可於帳務系統界面中，看到即將到期的帳號列表。
您可透過此頁面為即將過期的使用者儲值。每次儲值，將預儲一年份。若因故需要刪除帳號時，該帳號剩餘點數將返還至企業帳戶。

3.8. 使用統計

當您開始使用 Trio 服務後，I.X 管理員會視您使用 I.X 服務的類型，為您建立與您服務相關的統計報表，以便您能快速了解企業內部使用 Trio 服務的狀況，例如每天上線人數、存取各系統的頻繁度、各系統的登入狀況、從檔案伺服器下載檔案的頻繁度等。

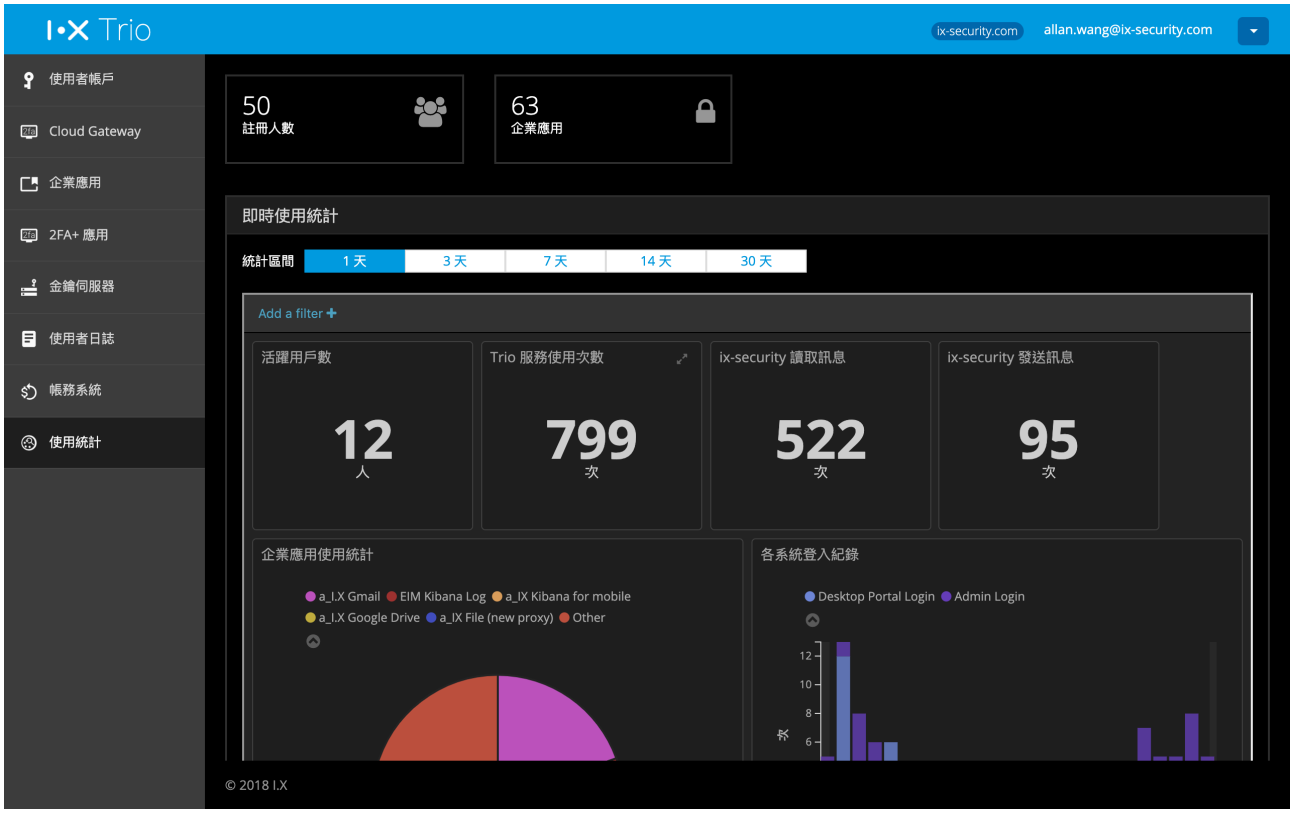


FIG. 3.7-1 TRIO 服務使用統計

部分統計內容需要搭配伺服器端的設計配合。因此，若您有統計報表相關需求，可向經銷商或 I.X 服務人員諮詢。

附錄一、Fortigate SSLVPN 整合範例

情境概述

某企業要導入 Fortigate VPN，並希望企業員工使用者登入 VPN 時，不使用 OTP token，改使用I.X 無線金鑰卡驗證員工身份。

通訊流程圖

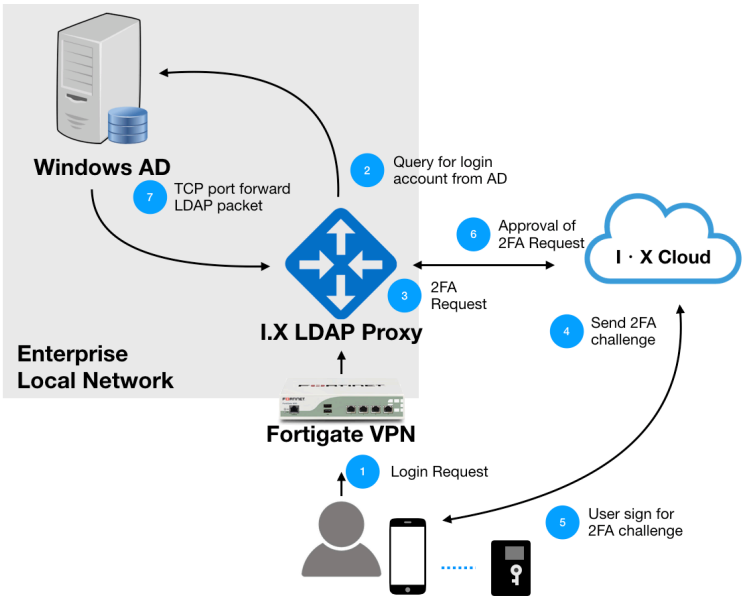


FIG. 3.4.1-1 整合網路架構與流程圖

原本 VPN 直接透過 LDAP protocol 向 AD 進行使用者查詢與認證，導入 I.X 服務後，VPN 改向 I.X LDAP Proxy 進行使用者查詢與認證，此時，I.X LDAP Proxy 會進行以下兩步驟認證：

1. 向 AD 進行使用者查詢與認證
2. 透過 I.X 身份認證服務，向使用者配對的手機發送認證通知，驗證登入者身份

當使用者確認登入認證時，將透過卡片簽回一電子簽章，I.X LDAP Proxy 驗證確認後，始得放行。

整合範例設定說明

Trio Console 管理平台

於 Application 新建一 Web SDK 類型的應用，步驟如下：
點擊 More

FIG. 3.4.1-2 新增 APPLICATION 步驟 1

於 **Web SDK** 處點擊 **+ New App**，為您的服務命名，勾選 “Required R2 Card”，以設定要使用卡片認證。

FIG. 3.4.1-3 新增 APPLICATION 步驟 2

儲存後，在 **Protected App** 頁面中，可找到系統為您服務所產生的金鑰對，將此 ikey 及skey 設定到 I.X LDAP Proxy 中，作為與 I.X 身份認證溝通時的加解密使用。

Fortigate VPN

將原本設定指向 AD 欄位的 IP，改指向 I.X LDAP Proxy 的 IP，並確認 VPN 上設定的 LDAP BindType、BaseDN、AdminDN，及 AdminDN 的密碼，這些設定將需要設定到 I.X LDAP Proxy 上。

將 Fortigate VPN 認證超時的設定值，延長至適當的時間。Fortinet appliance 預設遠端認證超時時間為 5 秒，該超時設定值可透過 Fortinet 的指令界面調整。此處，建議可調整至 300 秒。

- 連上 Fortinet appliance 指令行界面 (CLI)
- 執行以下指令
  # config system global
  # set remoteauthtimeout 300
  # end

I.X LDAP Proxy

安裝 I.X LDAP Proxy 服務，相關需求如下

硬體需求

- 伺服器等級設備
- 雙核心 CPU 2GB
- 8GB 記憶體

OS

- Debian 9 / Ubuntu 18.04 LTS (VM)

軟體

- 安裝 curl 套件
- 對外開放 *.docker.com:443

防火牆相關設定

以 I.X LDAP Proxy 導入 2FA 認證時，除了需要在 I.X LDAP Proxy 上，開放 I.X 服務所需要的端口服務外，若認證用的手機也會接入公司 WiFi 網路，也有需要開放的相應端口，以接收認證通知。

I.X LDAP Proxy 上的防火牆設定

- In-bond 開放 TCP 22, 1389
- In-bond IP 允許 Fortigate VPN IP
- Out-bond 開放 TCP 389, 443
- Out-bond IP 允許連線至 AD 及 https://api.ix-security.com

公司防火牆設定

iPhone 連線所需要的端口與連線

- 開放 TCP 443, 2195, 2196, 5223
- Apple 服務器為整個 17.0.0.0/8 位址區塊，該區塊為 Apple 專用
- I.X 服務 https://*.ix-security.com

Android phone 連線所需要的端口與連線

- 開放 TCP/UDP 443, 5228, 5229, 5230
- Google 服務器 IP 列表 https://ipinfo.io/AS15169
- I.X 服務 https://*.ix-security.com