

# 防火牆流程管理工具AlgoSec 清查系統2.0

清查系統 2.0 整合 AlgoSec 防火牆規則和客戶端的規則申請人，協助客戶可以有效率的清查檢核所有防火牆規則的使用狀態並進一步有效的管理防火牆規則。

## ■ 功能架構



## 1.系統管理—系統帳號管理

- 使用者資料匯入：匯入一般使用者的資料 ( 資料檔匯入 /AD 整合 )，整合客戶端 SSO 驗證密碼登入本系統
- 自建帳號：除了 admin 帳號是系統管理角色，可以手動新增其他系統管理帳號
- 使用者帳號查詢 / 修改：查詢已經匯入本系統的使用者帳號資訊並且可以啟用 / 停用某個帳號登入本系統
- 修改個人資料密碼：修改系統管理角色帳號的密碼 /email/ 姓名資訊
- 修改設定檔：設定 algoSec host/api 使用帳密 /smtp 設定 /AD ...等其他需要整合的 server 相關設定參數

### 1-1 系統帳號管理 > 使用者資料匯入

系統帳號管理	Home / 系統使用者資料查詢					
防火牆群組設定	條件: <input type="text"/> <input checked="" type="radio"/> 全部 <input type="radio"/> 啟用 <input type="radio"/> 無權限 <input type="text"/> 每頁顯示 15 條 <input type="button" value="查詢"/>					
啟動檢討報表	<input type="button" value="新增系統帳號"/> <input type="button" value="同步AD帳號"/> <input type="button" value="修改個人資料密碼"/> <input type="button" value="修改設定檔"/>					
規則保管人設定	共497條記錄，每頁顯示15條，當前第1/34頁 [首頁] [上一頁] [下一頁] [尾頁]					
保管人註解查詢	群組名稱	單位	使用者ID	使用者姓名	email	是否為保管人 權限編輯
檢討報表查詢	系統管理		admin	DaphneHsieh1	xhsieh@gmail.com	
	AD使用者	資訊安全產品處	1110001	蘇逸群	nomail	Y <input type="button" value="啟用"/>
	AD使用者	資訊安全產品處	1110002	吳嘉亦	nomail	Y <input type="button" value="啟用"/>
	AD使用者	資訊安全產品處	1110003	王名源	nomail	Y <input type="button" value="啟用"/>
	AD使用者	資訊安全產品處	1110004	方嘉玲	nomail	Y <input type="button" value="啟用"/>
	AD使用者	資訊安全產品處	1110005	藍雅清	nomail	Y <input type="button" value="啟用"/>
	AD使用者	資訊安全產品處	1110006	鮑煥惠	nomail	Y <input type="button" value="啟用"/>
	AD使用者	資訊安全產品處	1110007	鄭煥妃	nomail	Y <input type="button" value="啟用"/>
	AD使用者	資訊安全產品處	1110008	王仁杰	nomail	Y <input type="button" value="啟用"/>

## 1-2 系統帳號管理 > 自建帳號

系統帳號管理	Home / 新增系統帳號(*必填)
防火牆群組設定	*登入帳號 <input type="text"/> *姓名 <input type="text"/> 角色 <input type="radio"/> 系統管理 <input checked="" type="radio"/> AD使用者
啟動檢討報表	單位 <input type="text"/> *email <input type="text"/>
規則保管人設定	<input type="button" value="新增"/> <input type="button" value="回上一頁"/>
保管人註解查詢	
檢討報表查詢	

  

系統帳號管理	Home / 新增系統帳號(*必填)
防火牆群組設定	*登入帳號 <input type="text"/> *姓名 <input type="text"/> 角色 <input checked="" type="radio"/> 系統管理 <input type="radio"/> AD使用者
啟動檢討報表	*密碼 <input type="text"/> (長度至少6位數)
規則保管人設定	單位 <input type="text"/> *email <input type="text"/>
保管人註解查詢	<input type="button" value="新增"/> <input type="button" value="回上一頁"/>
檢討報表查詢	

## 1-3 系統帳號管理 > 修改個人資料密碼

系統帳號管理	Home / 修改個人資料密碼(*必填)
防火牆群組設定	種類 內容
啟動檢討報表	管理帳號 admin
規則保管人設定	請輸入舊密碼 <input type="text"/>
保管人註解查詢	請輸入新密碼 <input type="text"/> (長度至少6位數)
檢討報表查詢	請再輸入新密碼 <input type="text"/> (長度至少6位數)
	<input type="button" value="確定修改密碼"/>

  

管理帳號	admin
姓名	DaphneHsieh1
email	xhsieh@gmail.com
單位	<input type="text"/>
	<input type="button" value="確定修改資料"/> <input type="button" value="回上一頁"/>

## 1-4 系統帳號管理 > 修改設定檔

系統帳號管理	Home / 修改環境變數
防火牆群組設定	AD HOST <input type="text"/> 192.168.59.51 AD PORT <input type="text"/> 389 <input type="button" value="測試AD"/> AD DOMAIN <input type="text"/> issad.com
啟動檢討報表	AD帳號 <input type="text"/> CN=Administrator,CN=Users,DC=issad,DC=com AD密碼 <input type="text"/> .....
規則保管人設定	AD搜尋節點 <input type="text"/> DC=issad,DC=com
保管人註解查詢	SMTP Server <input type="text"/> 192.168.59.135 <input type="button" value="測試SMTP"/> 寄信者 <input type="text"/> algosec@jic.org.tw
檢討報表查詢	

  

Algosec host1	<input type="text"/> 192.168.59.134 <input type="button" value="測試"/>	Algosec帳號1	<input type="text"/> algosec	Algosec密碼1	<input type="text"/> .....
Algosec host2	<input type="text"/> 192.168.59.134 <input type="button" value="測試"/>	Algosec帳號2	<input type="text"/> algosec	Algosec密碼2	<input type="text"/> .....
			<input type="button" value="確定修改資料"/> <input type="button" value="回上一頁"/>		

## 2.系統管理—防火牆群組設定

- ➔ 更新設備：同步 algosec server 更新最新的防火牆設備資訊
- ➔ 新增 / 修改群組：新增群組目的是後續要執行檢討報表作業使用，一個群組不限設定幾台防火牆，端看客戶當下需求。

### 2-1 防火牆群組設定 > 新增防火牆群組

Home / 新增防火牆群組

Group Name:

序號	群組名稱	群組內容	編輯
1	IISI	CP_FW,192_168_59_137,10_20_106_1_Balfur_Balfur_root	<a href="#">編輯群組</a>

## 3.系統管理—啟動檢討報表

- ➔ 新增檢討作業：新增一個檢討作業，選擇特定群組進行 algosec 資料下載 / 整合處理。
- ➔ 每一項檢討作業有三種狀態需要更新，(a) 保管人註記開關：是否允許保管人編輯，預設是 Y，也可以手動先暫時關閉。(b) 結案：當本檢討作業完畢產出報告後，click[ 結案 ]，結案後的資料就無法在網頁查詢。(c) 刪除：如果檢討作業已經新增了，但是不需要此檢討作業，可以選擇刪除功能。

### 3-1 防火牆群組設定 > 新增防火牆群組

Home / 檢討報表作業

序號 資料時間 啟動時間 異動人 保管人是否可註記 是否結案 修改

1(IISI)	2022-06-20	2022-06-20 15:13:34	admin	<input checked="" type="checkbox"/> 可以 <input type="checkbox"/> 禁止	N	<a href="#">結案</a> <a href="#">刪除</a> <a href="#">通知保管人</a>
---------	------------	---------------------	-------	--	---	---

本次作業資料下載完成後，可以發通知保管人

Home / 保管人通知清單

Guardian ID	Guardian Name	Guardian Email
1110003(王名鴻)	/nomail	
1110009(曾國雄)	/nomail	
raynor(馬榮強)	/raynor@issad.com	

信件範本:

[確定發送信件](#) [回上一頁](#)



## 4.規則保管人設定

- 系統管理：可以個別修改設定某條規則的保管人，例如換保管人 / 刪除 / 新增保管人
- 使用者：可以一次勾選多筆規則設定自己為保管人，一條規則可以多個人設定保管

### 4-1規則保管人設定 > 系統管理員角色

系統帳號管理  
防火牆群組設定  
啟動檢討報表  
規則保管人設定  
保管人註解查詢  
檢討報表查詢

Home / 規則保管人設定

device: ALL [查詢]

保管人: [選擇] 每頁顯示 15 條 [全部] [有保管人] [無保管人]

共44條記錄，每頁顯示15條，當前第1/3頁 [首頁] [上一頁] [下一頁] [尾頁]

devicename	ruleid	來源	目的	服務	備註	保管人
10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Hello routing	1110003(王名源) 1110009(曾國雄) raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test change	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	4	ip-1.1.0.1	all	obj-all	Guy_L2	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	27	ip-172.18.18.19	ip-10.10.10.11	ANY	FireFlow #14	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	6	ip-1.1.0.1	ip-10.110.251.17	obj-all	Guy_L2	raynor(馬樂強) <a href="#">設定</a>

針對特定規則設定 / 修改保管人

### 4-1規則保管人設定 > 系統管理員角色

系統帳號管理  
防火牆群組設定  
啟動檢討報表  
規則保管人設定  
保管人註解查詢  
檢討報表查詢

Home / 規則保管人設定

device: ALL [查詢]

保管人: [選擇] 每頁顯示 15 條 [全部] [有保管人] [無保管人]

共44條記錄，每頁顯示15條，當前第1/3頁 [首頁] [上一頁] [下一頁] [尾頁]

devicename	ruleid	來源	目的	服務	備註	保管人
10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Hello routing	1110003(王名源) 1110009(曾國雄) raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test change	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	4	ip-1.1.0.1	all	obj-all	Guy_L2	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	27	ip-172.18.18.19	ip-10.10.10.11	ANY	FireFlow #14	raynor(馬樂強) <a href="#">設定</a>
10_20_106_1_Balfur_Balfur_root	6	ip-1.1.0.1	ip-10.110.251.17	obj-all	Guy_L2	raynor(馬樂強) <a href="#">設定</a>

既有的保管人可以做刪除 / 換人

可以新增保管人

### 4-2規則保管人設定 > 保管人角色

規則保管人設定

Home / 規則保管人設定

device: ALL [查詢]

保管人: [選擇] 每頁顯示 15 條 [全部] [有保管人] [無保管人]

共44條記錄，每頁顯示15條，當前第1/3頁 [首頁] [上一頁] [下一頁] [尾頁]

devicename	ruleid	來源	目的	服務	備註	保管人
10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Hello routing	1110003(王名源) 1110009(曾國雄) raynor(馬樂強)
10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬樂強)
10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test change	raynor(馬樂強)
10_20_106_1_Balfur_Balfur_root	4	ip-1.1.0.1	all	obj-all	Guy_L2	raynor(馬樂強)
10_20_106_1_Balfur_Balfur_root	27	ip-172.18.18.19	ip-10.10.10.11	ANY	FireFlow #14	raynor(馬樂強)
10_20_106_1_Balfur_Balfur_root	6	ip-1.1.0.1	ip-10.110.251.17	obj-all	Guy_L2	raynor(馬樂強)
10_20_106_1_Balfur_Balfur_root	7	ip-10.10.10.16	ip-172.18.18.16	KERBEROS	FireFlow #51 FireFlow #53 t5	raynor(馬樂強)
10_20_106_1_Balfur_Balfur_root	8	ip-172.18.18.18	ip-10.10.10.10	tcp-455	FireFlow #65	raynor(馬樂強)

保管人進入系統後可以一次多選屬於自己保管的規則

## 4-2規則保管人設定 > 保管人角色

- 系統管理：可以個別修改設定某條規則的保管人，例如換保管人 / 刪除 / 新增保管人
- 使用者：可以一次勾選多筆規則設定自己為保管人，一條規則可以多個人設定保管

規則保管人設定

Home / 規則保管人設定

device: ALL [選擇]

每頁顯示 15 條

設定保管規則 共44條記錄，每頁顯示15條，當前第1/3頁 [首頁] [上一頁] [下一頁] [尾頁]

<input type="checkbox"/> 全選	devicename	ruleid	來源	目的	服務	備註	保管人
<input checked="" type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Helio routing	1110003(王名源) 1110009(曾嘉維) raynor(馬業強)
<input checked="" type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬業強)
<input checked="" type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test change	raynor(馬業強)
<input type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	4	ip-1.1.0.1	all	obj-all	Guy_L2	raynor(馬業強)

勾選設定完成後，就不能重複選擇

規則保管人設定

Home / 規則保管人設定

device: ALL [選擇]

每頁顯示 15 條

設定保管規則 共44條記錄，每頁顯示15條，當前第1/3頁 [首頁] [上一頁] [下一頁] [尾頁]

<input type="checkbox"/> 全選	devicename	ruleid	來源	目的	服務	備註	保管人
<input type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Helio routing	1110003(王名源) 1110009(曾嘉維) raynor(馬業強) mana(謝銘漢)
<input type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬業強) mana(謝銘漢)
<input type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test change	raynor(馬業強) mana(謝銘漢)
<input type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	4	ip-1.1.0.1	all	obj-all	Guy_L2	raynor(馬業強)
<input type="checkbox"/>	10_20_106_1_Balfur_Balfur_root	27	ip-172.18.18.19	ip-10.10.10.11	ANY	FireFlow #14	raynor(馬業強)

## 5.使用者-檢討報表規則編輯

- 使用者只能編輯自己負責的規則，針對每一筆規則做規則註記 & 物件 (source/destination) 註記

規則保管人設定

Home / 檢討報表規則編輯

device: ALL [選擇]

每頁顯示 15 條

共4條記錄，每頁顯示15條，當前第1/1頁 [首頁] [上一頁] [下一頁] [尾頁]

編輯	devicename	ruleid	來源	目的	服務	備註	保管人
設定	10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Helio routing	1110003(王名源) 1110009(曾嘉維) raynor(馬業強) mana(謝銘漢)
設定	10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬業強) mana(謝銘漢)
設定	10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test change	raynor(馬業強) mana(謝銘漢)
設定	10_20_106_1_Balfur_Balfur_root	13	ip-172.18.18.11	ip-10.10.10.10	tcp-655	FireFlow #77	raynor(馬業強) mana(謝銘漢)

## 5-1使用者-檢討報表規則編輯

- 系統管理：可以個別修改設定某條規則的保管人，例如換保管人 / 刪除 / 新增保管人
- 使用者：可以一次勾選多筆規則設定自己為保管人，一條規則可以多個人設定保管

規則保管人設定

檢討報表規則編輯

檢討報表查詢

Home / 規則註記設定

保管人: mana(謝銘漢)

device

10\_20\_106\_1\_Balfur\_Balfur\_root

ruleid

2

source

ip-1.1.0.1

rule註記

destination

ip-10.10.10.16

service

ANY

comment

v2018.1.5.5

物件

ip-10.10.10.16

ip-1.1.0.1

註解

規則保管人設定

檢討報表規則編輯

檢討報表查詢

Home / 檢討報表規則編輯

device: -----ALL-----

每頁顯示 15 筆

共4條記錄，每頁顯示15條，當前第1/1頁 [首頁] [上一頁] [下一頁] [尾頁]

編輯	device	ruleid	物件	備註	保管人		
設定	10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Hello routing	1110003(王名源) 1110009(曾國雄) raynor(馬業強) mana(謝銘漢)
設定	10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬業強) mana(謝銘漢)
設定	10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test change	raynor(馬業強) mana(謝銘漢)
設定	10_20_106_1_Balfur_Balfur_root	13	ip-172.18.18.11	ip-10.10.10.10	tcp-655	FireFlow #77	raynor(馬業強) mana(謝銘漢)

註記填寫完成後，會呈現黃色提示

## 6.系統管理—防火牆物件列表

- 系統管理員可以查詢哪些規則是否已經註記

系統帳號管理

防火牆群組設定

啟動檢討報表

規則保管人設定

保管人註解查詢

檢討報表查詢

Home / 保管人註解查詢

device: -----ALL-----

保管人:

每頁顯示 15 筆

共46條記錄，每頁顯示15條，當前第1/4頁 [首頁] [上一頁] [下一頁] [尾頁]

保管人	device	Ruleid	物件	註解
1110003(王名源)	10_20_106_1_Balfur_Balfur_root	1		
1110009(曾國雄)	10_20_106_1_Balfur_Balfur_root	1		
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	1		使用用途
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	2		使用用途
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	3		使用用途
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	4		
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	5		使用用途
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	6		
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	7		
raynor(馬業強)	10_20_106_1_Balfur_Balfur_root	8		



## 7.檢討報表查詢

- 網頁查詢本次檢討的防火牆設備資料：針對特定欄位條件查詢本次檢討作業的規則資料
- 下載 excel 報表：區分為原始物件報表 & 解開物件詳細資料報表

系統帳號管理  
防火牆群組設定  
啟動檢討報表  
規則保管人設定  
保管人註解查詢  
檢討報表查詢

Home / AlgoSec 檢討報表查詢

設備: ☒ ALL ☐ IISI  
CP\_FW: ☒ 192\_168\_59\_137 ☒ 10\_20\_106\_1\_Balfur\_Balfur\_root

條件:  顯示欄位: ☐ ALL ☒ 來源 ☒ 目的 ☐ 服務 ☐ 動作 ☐ 風險 ☐ 保管人 ☐ 備註 ☐ 最後使用時間 ☐ 最後異動者

每頁顯示:  筆

共44條記錄, 每頁顯示15條, 當前第1/3頁 [首頁] [上一頁] [下一頁] [尾頁]

ruleid	devicename	ruleid	來源	目的	服務
1	10_20_106_1_Balfur_Balfur_root	1(無流量)	all	all	ANY
2	10_20_106_1_Balfur_Balfur_root	2(無流量)	ip-1.1.0.1	ip-10.10.10.16	ANY
3	10_20_106_1_Balfur_Balfur_root	5(無流量)	ip-10.20.3.6	ip-10.20.3.6	HTTP
4	10_20_106_1_Balfur_Balfur_root	4(無流量)	ip-1.1.0.1	all	obj-all
5	10_20_106_1_Balfur_Balfur_root	27(無流量)	ip-172.18.18.19	ip-10.10.10.11	ANY
6	10_20_106_1_Balfur_Balfur_root	6(無流量)	ip-1.1.0.1	ip-10.110.251.17	obj-all
7	10_20_106_1_Balfur_Balfur_root	7(無流量)	ip-10.10.10.16	ip-172.18.18.16	KERBEROS
8	10_20_106_1_Balfur_Balfur_root	8(無流量)	ip-172.18.18.18	ip-10.10.10.10	tcp-455

### 7-1 檢討報表查詢 > 查詢某一條規則source內容

Home / Source物件資料查詢

物件保管人: 1110003(王名源)

ruleid	規則註記	nodata
1		

物件名稱	物件內容	註解	次數
all	0.0.0.0-255.255.255.255		

物件保管人: 1110009(曾國權)

ruleid	規則註記	nodata
1		

物件名稱	物件內容	註解	次數
all	0.0.0.0-255.255.255.255		

物件保管人: raynor(馬業強)

ruleid	規則註記	使用用途
1		

物件名稱	物件內容	註解	次數
all	0.0.0.0-255.255.255.255	使用用途	

### 7-1 檢討報表查詢 > 特定欄位查詢資料/下載本次檢討報表excel file

系統帳號管理  
防火牆群組設定  
啟動檢討報表  
規則保管人設定  
保管人註解查詢  
檢討報表查詢

Home / AlgoSec 檢討報表查詢

設備: ☒ ALL ☐ IISI  
CP\_FW: ☒ 192\_168\_59\_137 ☒ 10\_20\_106\_1\_Balfur\_Balfur\_root

條件:  顯示欄位: ☐ ALL ☒ 來源 ☒ 目的 ☒ 服務 ☐ 動作 ☐ 風險 ☐ 保管人 ☐ 備註 ☐ 最後使用時間 ☐ 最後異動者

每頁顯示:  筆

共44條記錄, 當前第1/3頁 [首頁] [上一頁] [下一頁] [尾頁]

ruleid	devicename	ruleid	來源	目的	服務
1	fur_Balfur_root	1(無流量)	all	all	ANY
2	fur_Balfur_root	2(無流量)	ip-1.1.0.1	ip-10.10.10.16	ANY
3	10_20_106_1_Balfur_Balfur_root	5(無流量)	ip-10.20.3.6	ip-10.20.3.6	HTTP

download the result--> detail\_20220629\_225643.xls