

# 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 / 素統個	用者資料查約					
防火牆群組設定	<b>曾</b> 條件	●全部○数	用〇無欄限 ▲每頁顯示[1	15 筆 重測			
啟動檢討報表	新爆系流報號	司步AD唱號	個人資料密碼				
規則保管人設定	共497條記錄 : #	写面顯示15條,當前第1/34	] [頁一不] [頁一上] [页首] 頁	5 <b>0</b> ]			
保管人註解查詢	料組名稱	#111	使用者ID	使用有姓名 DaphneHsieh1	email xhsieh@gmail.com	是百有味言人	相同致語解釋時
檢討報表查詢	AD使用者	資訊安全產品處	1110001	緊逸群	nomail	Y	展開
	AD使用者	資訊安全產品處	1110002	吳喬亦	nomail	Y	開閉
	AD使用者	資訊安全產品處	1110003	王名源	nomail	Y	SIM
	AD使用者	資訊安全產品處	1110004	方嘉玲	nomail	Ŷ	展開
	AD使用者	資訊安全產品處	1110005	藍薯油	nomail	Y	開開
	AD使用者	資訊安全產品處	1110006	鲍妍惠	nomail	Y	開間
	AD使用者	資訊安全產品處	1110007	鄭煤妃	nomail	Y	30.62
	AD使用者	資訊安全產品處	1110008	王仁杰	nomail	Y.	30.55



#### 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	項)					
防火牆群組設定	*登入帳號	*姓名	<b>A</b>	é	○系統管理●AD使用者		
啟動檢討報表	單位	*email					
規則保管人設定				新雄	回上-頁		
保管人註解查詢				_			
檢討報表查詢							
系統帳號管理	Home / 新增新瓶帳號(*心	填)					
防火牆群組設定	*登入顿残	*姓名	<b>A</b>	色	●系統管理○AD使用者	(高度至少6位數)	
啟動檢討報表	7單位	*email					
規則保管人設定			 	_			
保管人註解查詢				新增	西上一首		
检討超主委的							

### 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(*公場)	
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	讀輸入舊密碼	
保管人許解查詢	請輸入新密碼	(長度至少6位數)
檢討報表查詢	調再輸入新密碼	(長度至少6位数)
		海定修改四南
	審理帳號	admin
	姓名	DaphneHsieh1
	email	xhsieh@gmail.com
	單位	
		· · · · · · · · · · · · · · · · · · ·

## 1-4系統帳號管理>修改設定檔

系統帳號管理	Home / 修改環境	121 R						
防火牆群組設定	AD HOST	192.168.59.51	AD PORT 389	SHAD	AD DOMAIN	issad.com		
啟動檢討報表	AD根號	CN=Administrator, CN=Users,	DC=issad,DC=com		AD密碼			
規則保管人設定	AD搜粤訪點	DC=issad,DC=com						
保管人註解查詢	SMTP Server	192.168.59.135	则試SMTP		寄信者	algosec@jcic.org.tw		
檢討報表查詢	Algosec host1	192.168.59.134	2	Algosec帳號1	algosec	Algosec密碼1	[	
	Algosec host2	192.168.59.134		Algosec根號2	algosec	Algosec宏碼2	•••••	
				建定修改算	a al-a			

## 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

系統帳號管理	Home / 防火器	員詳組設定				
防火牆群組設定	▲每頁顕示 15	筆所增計組	更新設備			
啟動檢討報表	共1條記錄·每]	貢顒示15條・當前第1	1/1頁 (首頁] (上一頁) [下一頁] [尾頁]			
規則保管人設定	序號	群組名稱	群組內容		編	R.
保管人註解查詢	1	IISI	CP_FW,192_168_59_137,10_20_106_1_Balfur_Balfur_root			制輕料組
檢討報表查詢						
系統帳號管理	Home / 新增	防大續群組				
防火牆群組設定	Group Name					
啟動檢討報表	C Select All	brand de	evicename		brand	devicename
規則保管人設定	0	Amazon AWS 80	01024405411_us_east_2_DevOps_DevOps_SG_DevOps_ACL		Amazon AWS	801024405411_ca_c
保管人註解查詢	0	Amazon AWS 80	01024405411_us_east_2_HR_Department_HR_SG_HR_ACL		Amazon AWS	801024405411_us_e
	0	Amazon AWS 80	01024405411_ca_central_1_Marketing_department_Marketing_SG_Marketing_ACL		Amazon AWS	801024405411_ca_c
檢討報夜直詞	a	Amazon AWS Se	eqouia_DB_Server		Amazon AWS	Sequoia_Amazon
	0	Amazon AWS Se	equoia_Backend		Amazon AWS	Sequoia_AWS_Dem
		Amazon AWS Se	equola_PREPROD_Backend	0	Amazon AWS	Sequoia_AWS_Dem
	0	Amazon AWS Se	equola_PREPROD_DB	0	Amazon AWS	Sequoia_PREPROD_
	0	Amazon AWS Se	equoia AWS Demo i 285684b7		Amazon AWS	Seguoia Web Front

## 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

系統帳號管理	Home / 機討報表	反作業					
防火牆群組設定	▲每頁顯示 15 前	新增檢討作應					
啟動檢討報表	共1條記錄,每頁副	東示15條·黨前第1/1頁[首頁][上	一頁] [下一頁] [尾頁]				
規則保管人設定	序號	資料時間	較動時間	異動人	保管人是否可註記	是否結素	修改
保管人註解查詢	1(((S))	2022-06- 20	2022-06-20 15:13:34	admin	●可以 ○需止	N	(結果) 副除 通知保留人
检討朝表香諭							
INEL TRACE PU	J		本	次作業資	料下載完成後,	, 可以發通	知保管人
~ 竹枝 财政 11	Home / 保智人语	知濟單	本	次作業資	料下載完成後,	, 可以發通	知保管人
永統帳號管理 防火牆群組設定	Home / 保管入语 1110003(王名源)/	知清單 /nomail	本 1110009(首函维)/nomail	次作業資	料下載完成後,	, 可以發通	知保管人
系統帳號管理 防火牆群組設定 501-101-121-1	Home / 保管人语 1110003(王名湾)/	迎清單 /nomail	本 1110009(普函總)/nomail	次作業資	料下載完成後,	, 可以發通	知保管人
系統帳號管理 防火牆群組設定 啟動檢討報表	Home / 保筆人语 1110003(王名湾)/ 信件範本:	知清單 /nomail 檢討作業開始,調合也保備人名	本 1110009(曾國維)/nomail 8人系統確認負責的防火運視則!	次作業資	料下載完成後, ynor(嗎樂強)(raynor@issad.com	, 可以發通	知保管人
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	Home / 保護人语 1110003(王名淸)/ 信件載本:	知清單 /nomail 檢討作業開始,講各位保養人登	本 1110009(曾丽维)/nomail 8人系統確認負責的防火運規則	次作業資	料下載完成後, ynor(馬樂強)/raynor@issad.com	, 可以發通	知保管人
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 屎管人註解查詢	Home / 保留入语 1110003(王名湾)/ 信件載本:	知清單 /nomail 檢討作業開始,調合位保管人型	本 1110009(曾丽维)/nomail 2人系統確認負責的防火續規則!	文作業資	料下載完成後, ynor(馬樂選)/raynor@issad.com	, 可以發通	知保管人

道家 資拓宏宇國際股份有限公司 International Integrated Systems, Inc.

always innovative always IISI

## 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	Home / 規則保管人設定											
防火牆群組設定	●deviceALL	-				針對特定規則設定	2/修改保管/					
啟動檢討報表												
規則保管人設定	共44條記錄,每頁顯示15條,當前第1/3頁 (首 devicename	頁] [上一 ruleid	頁] [下一頁] [尾頁] 來源	目的	服務	備註	保管人					
呆管人註解查詢	10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Hello routing	1110003(王名源)					
檢討報表查詢							1110009(曾國維) raynor(馬樂強) 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(馬養強) 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) 設定					
	10_20_106_1_Balfur_Balfur_root	4	ip-1.1.0.1	all	obj-all	Guy_L2	raynor(馬樂強) 設定					
	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) 設定					
	10_20_106_1_Balfur_Balfur_root	6	ip-1.1.0.1	ip-10.110.251.17	obj-all	Guy_L2	raynor(馬崗強) 設定					

#### 4-1規則保管人設定 > 系統管理員角色

Home / 保管入實料認	ΤĒ.				
devicename	10_20_106_1_Balfur_Balf	ur_root	ruleid	t	
source	all		destination	all	
service	ANY		comment	Hella routing	
保管人新增	1110003(王名源)		RE10(K		
	1110009(曾國維)		🔜 — 既有的	保管人可以做删除 / 排	<b>渔人</b>
	raynor(馬樂道)	請點道 > 加人	WIDE		
Home / 保管入資料證	定				
devicename	10_20_106_1_Balfur_Ba	Ifur_root	ruleid	i l	
source	all		destination	all	
service	ANY		comment	Hello routing	
	1110003(T.C.)				
保管人新增	1110003(主名源)	請點選 ¥ 換人	删除		
	1110009(曾國維)		删除		
可以新增保管	會人 raynor(馬業強)	請點選 > 第人	Rife.		
	請點選 > 1	所爆烧管人			
	Home / 保管入資料認 devicename service 保管入 新憲 devicename source service 保管入 新憲 可以新增保管	Home / 原音人資料設定 devicename 10_20_106_1_Balfur_Balf source all service ANY 保管人 新聞 1110003(王名湾) 1110009(留圖編) raynor(馬爾強) Home / 保管人資料設定 devicename 10_20_106_1_Balfur_Balfu	Home / 探管人質料認定     devicename   10_20_106_1_Balfur_Balfur_root     source   all     service   ANY     瘤瘤人 調査   1110009(冒屈曲)     1110009(冒屈曲)   ····································	Home / 探發人質和認定     devicename   10_20_106_1_Balfur_root   ruleid     service   ANY   comment     服養人医療   1110003(王名源)  請贴書 》 ●人 回答     I110009(冒屈曲)  請貼書 》 ●人 回答   DE Comment     Remc / 保養人資料設定   10_20_106_1_Balfur_Balfur_root   ruleid     devicename   10_20_106_1_Balfur_Balfur_root   ruleid     source   ail   destination     service   ANY   comment     T110003(王名源)  請點書 》 送人 副將     1110009(盲面曲)  請點書 》 送人 副將     1110009(盲面曲)  請點書 》 送人 副將     1110009(盲面曲)  請點書 》 送人 副將    請點書 》 送人 副將	Home / 原發人質科認定     devicename   10_20_106_1_Balfur_root   ruleid   1     service   ANY   comment   Hello routing     服業人 原源   1110003(在名示)

回上一日

道家 資拓宏宇國際股份有限公司 International Integrated Systems, Inc.

#### 4-2規則保管人設定 > 保管人角色

規則保管人設定	Home /	明剛保管人設定													
檢討報表規則編輯	device	₩device													
檢討報表查詢	▲ 电贝朗7														
	設定保備接用]共44條記錄,每頁觀示15條,富前第1/3頁[當頁][上一頁][下一頁][尾頁]														
	日全選	devicename	ruleid	來源	目的	服務	側註	保管人							
	a	10_20_106_1_Balfur_Balfur_root	į	all	all	ANY	Hello routing	1110003(王名源) 1110009(曾國維) raynor(馬莱強)							
		10_20_106_1_Balfur_Balfur_root	2	ip-1.1.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬業強)							
	0	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)							
		10_20_106_1_Balfur_Balfur_root	4	ip-1.1.0.1	all	obj-all	Guy_L2	raynor(萬業強)							
		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)							
	0	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(馬懶強)							
	Ø	10_20_106_1_Balfur_Balfur_root	8	ip-172.18.18.18	ip-10.10.10.10	tcp-455	FireFlow #65	raynor(馬蘭強)							



#### 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



## 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	e / 他討蝦表現則編輯												
討報表規則編輯	dev	rice ALL	-	▼IISI 重調										
檢討報表查詢	<b>二</b> 年月	▲每貝酮示 <u>15</u> 廉												
	共4條	記録,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	來轟	目的	服務	御註	保管人						
	設定	10_20_106_1_Balfur_Balfur_root	1	all	ali	ANY	Hello routing	1110003(王名將 1110009(普圖納 raynor(馬黃強) mana(謝銘淇)						
	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(馬美強) mana(謝銘淇)						
	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(馬樂强) mana(謝銘淇)						
	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(馬樂強) mana(謝銘淇)						



#### 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	Home	/ 規則註記證定						
約封銀売規則編輯	保營人;	mana(謝銘漢)						
	device	name 10_20_106_1_Balfur_B	Balfur_root		ruleid	2		
<b>极</b> 訂報表查詢	source	ip-1.1.0.1			rule註記			
	destin	ation ip-10.10.10.16						
	servic	e ANY						4
	comm	v2018.1.5.5						
	物件			LEAN				
	ip-10.	10.10.16						
	ip-1.1	.0.1						
相則保等人設定	Home	2/ 檢討報表規則編輯						
AND AN IN A CARAC	#den	dice All and		-				
檢討報表規則編輯	 ● 新育	間示 15 筆						
檢討報表查詢	-	amos [12]+						
	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	註記填寫完	成後,會呈現黃	色提示	備註	保管人
Г	設定	10_20_106_1_Balfur_Balfur_root	1	all	all	ANY	Hello routing	1110003(王名源 1110009(曾國維 raynor(馬榮強) mana(開終事)
	設定	10_20_106_1_Balfur_Balfur_root	2	jp-1.4.0.1	ip-10.10.10.16	ANY	v2018.1.5.5	raynor(馬養殘) mana(謝銘淇)
	股	10_20_106_1_Balfur_Balfur_root	5	ip-10.20.3.6	ip-10.20.3.6	HTTP	FF #2209 FF #3885 test	raynor(馬簧強)
L	Æ						change	mana(謝懿淇)
	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(馬藥強) mana(謝銘淇)

## 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	Home / 保管人註解言	120				
防火牆群組設定	device ALL	· · · · · · · · · · · · · · · · · · ·	●全部 ○ 有註解 ○)	無註解 宣吻		
啟動檢討報表						
規則保管人設定	共46條記錄,每頁顯示 保管人	15條,當前第1/4頁[首頁][上一頁][下一頁] devicename	尾頁] Ruleid	物件	註解	
保管人註解查詢	1110003(王名源)	10_20_106_1_Balfur_Balfur_root	1			
檢討報表查詢	1110009(管题维)	10_20_106_1_Balfur_Balfur_root	4			
	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(馬樂強)	10_20_106_1_Balfur_Balfur_root	3		使用用途	
	raynor(馬樂強)	10_20_106_1_Balfur_Balfur_root	4			
	raynor(馬鰲強)	10_20_106_1_Balfur_Balfur_root	5		使用用途	1
	raynor(馬鰲強)	10_20_106_1_Balfur_Balfur_root	6			
	raynor(馬養強)	10_20_106_1_Balfur_Balfur_root	7			
	raynor(馬樂姓)	10_20_106_1_Balfur_Balfur_root	8			1

## 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	田ome / Algosec 他封卵表面的 日の / Algosec 他封卵表面的 日の / Algosec 他封卵表面的 田の / Algosec 他封卵素面的 田の / Algosec 他封 田の / Algosec  田の / Algosec 他封 田の / Algosec  田の / Algosec 田の / Algosec  田の / Algo								
防火牆群組設定									
啟動檢討報表									
規則保管人設定									
呆管人註解查詢	共44條記錄	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]							
檢討報表查詢	rulenum	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

fome / Sou	urce物件資料查詢				
物件保管人: 1	1110003(王名源)				
ruleid	1	規則註記	nodata		
物件名稱		物件内容	註解	次數	
all 0.0.0.0-255.255.255.255					
物件保管人:1	1110009(曾國維)				
ruleid	1	規則註記	nodata		
物件名稱		物件内容	註解	次數	
all		0.0.0.0-255.255.255.255			
物件保管人:	raynor(馬寨強)				
ruleid	1	規則註記	使用用途		
物件名稱		物件内容	註解	求數	
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	Home / Alg	osec 检討報表查	iii						
防火牆群組設定	全級情 図ALL IISI GCP.FW 図192_166_59_137 図10_20_106_1_Balfur_Balfur_root 養体作   展示欄位:□ALL図 來源 図目的 図 服務 □ 動作 □ 星版 □ 保管人 □ 備註 □ 最後使用時間 □ 最後異動者								
啟動檢討報表									
規則保管人設定	「 画詞 アロ 一 来 日	eid Ø	無約件權調下數	▲每頁顯示 15 華					
保管人註解查詢									
榆封蝦夷香鉤	rulenun 備	注		ruleid	來源	目的	服務		
WHO THINK THO	1 風	三人	fur_Baifur_root	1(無流量)	all	all	ANY		
	2 最	後使用時間 後異動者	fur_Balfur_root	2(無流量)	ip-1.1.0.1	ip-10.10.10.16	ANY		
	and the second s								



