



WinMatrix IT 資源管理系統 3.8.31.x 版 本機權限群組管理模組功能規格表

本機群組管理模組 (此為選購功能)										
本機群組 管理	功能效益									
	- 清查電腦本機權限群組*1 與群組中的帳號現況，了解是否有非預期的帳號擁有特殊權限(EX：Power Users)，確實落實管理與檢核程序，以降低資訊安全的風險。 - 建立標準程序化與系統化的本機群組帳號使用申請機制，減少日常維護的負擔，並由系統留下軌跡紀錄備查，以吻合 ISO 的作業精神。									
	<table border="1"> <thead> <tr> <th>編號</th><th>功能項目</th></tr> </thead> <tbody> <tr> <td>1-1</td><td> 本機群組的收集與清查： (1) 自動蒐集電腦中本機權限群組內的帳號與群組清單，呈現欄位包含：組織名稱、電腦名稱、IP 位址、機台使用人、隸屬（本機或網域）、類型、帳號/群組名稱、所屬本機群組、是否已停用、是否申請使用中、帳密回收、最後修改日期、描述等。 (2) 可排除特定帳號或群組，不須顯示於管理報表中。（例如：Guest） (3) 可從管理介面中將選取的網域帳號移出*2 本機群組（該電腦必須在線上）。 (4) 管理介面中有需要與 Windows Active Directory(AD)做查詢時，本系統支援 LDAP 與 LDAPS 通訊協定。（由 IT 系統管理員於本模組的設定中預先設定） (5) 可設定哪一些本機的權限群組，是可以被申請加入新的帳號成員。 (6) 本機群組的帳號成員發生變化時，系統將回報事件予以紀錄。可盡早發現是否有異常的行為發生。 </td></tr> <tr> <td>1-2</td><td> 本機群組帳號的使用申請機制(需要安裝 WinMatrix Web 套件)： (1) 可透過網頁選擇特定電腦（多選）申請將網域帳號加入本機群組中。 (2) 申請結果將透過網頁與 Email，告知申請人與使用人，無須其他人工介入。 (3) 可限定帳號加入本機群組的使用期間（有效期），當使用期間屆滿，電腦將顯示提示訊息後自動登出，並回收本機群組帳號（該網域帳號會從本機群組中被移出）。 (4) 使用期間屆滿前，原申請者可透過網頁延長本機群組帳號的使用期間。 (5) 支援一次申請多個本機群組權限。 </td></tr> <tr> <td>1-3</td><td> 本機群組使用紀錄覆核： (1) 可依照日期（每日）覆核本機群組的申請使用紀錄（包含欄位：電腦、IP 位址、申請時間、申請人、申請帳號、申請原因），並於紀錄中標註意見與已覆核的旗標。 (2) 可自動 Email 寄送本機群組的申請使用紀錄與主管（覆核人員），郵件中提供覆核連結，便於主管（覆核人員）進行覆核作業。 </td></tr> <tr> <td>1-4</td><td> 報表與查詢： (1) 使用 WinMatrix Console 中的通知樣版設定，自動寄送本機群組申請使用記錄，與本機群組的異動紀錄。 (2) 本機群組申請使用的紀錄查詢。 (3) 本機群組管理模組的操作記錄查詢。 </td></tr> </tbody> </table>	編號	功能項目	1-1	本機群組的收集與清查： (1) 自動蒐集電腦中本機權限群組內的帳號與群組清單，呈現欄位包含：組織名稱、電腦名稱、IP 位址、機台使用人、隸屬（本機或網域）、類型、帳號/群組名稱、所屬本機群組、是否已停用、是否申請使用中、帳密回收、最後修改日期、描述等。 (2) 可排除特定帳號或群組，不須顯示於管理報表中。（例如：Guest） (3) 可從管理介面中將選取的網域帳號移出*2 本機群組（該電腦必須在線上）。 (4) 管理介面中有需要與 Windows Active Directory(AD)做查詢時，本系統支援 LDAP 與 LDAPS 通訊協定。（由 IT 系統管理員於本模組的設定中預先設定） (5) 可設定哪一些本機的權限群組，是可以被申請加入新的帳號成員。 (6) 本機群組的帳號成員發生變化時，系統將回報事件予以紀錄。可盡早發現是否有異常的行為發生。	1-2	本機群組帳號的使用申請機制(需要安裝 WinMatrix Web 套件)： (1) 可透過網頁選擇特定電腦（多選）申請將網域帳號加入本機群組中。 (2) 申請結果將透過網頁與 Email，告知申請人與使用人，無須其他人工介入。 (3) 可限定帳號加入本機群組的使用期間（有效期），當使用期間屆滿，電腦將顯示提示訊息後自動登出，並回收本機群組帳號（該網域帳號會從本機群組中被移出）。 (4) 使用期間屆滿前，原申請者可透過網頁延長本機群組帳號的使用期間。 (5) 支援一次申請多個本機群組權限。	1-3	本機群組使用紀錄覆核： (1) 可依照日期（每日）覆核本機群組的申請使用紀錄（包含欄位：電腦、IP 位址、申請時間、申請人、申請帳號、申請原因），並於紀錄中標註意見與已覆核的旗標。 (2) 可自動 Email 寄送本機群組的申請使用紀錄與主管（覆核人員），郵件中提供覆核連結，便於主管（覆核人員）進行覆核作業。	1-4
編號	功能項目									
1-1	本機群組的收集與清查： (1) 自動蒐集電腦中本機權限群組內的帳號與群組清單，呈現欄位包含：組織名稱、電腦名稱、IP 位址、機台使用人、隸屬（本機或網域）、類型、帳號/群組名稱、所屬本機群組、是否已停用、是否申請使用中、帳密回收、最後修改日期、描述等。 (2) 可排除特定帳號或群組，不須顯示於管理報表中。（例如：Guest） (3) 可從管理介面中將選取的網域帳號移出*2 本機群組（該電腦必須在線上）。 (4) 管理介面中有需要與 Windows Active Directory(AD)做查詢時，本系統支援 LDAP 與 LDAPS 通訊協定。（由 IT 系統管理員於本模組的設定中預先設定） (5) 可設定哪一些本機的權限群組，是可以被申請加入新的帳號成員。 (6) 本機群組的帳號成員發生變化時，系統將回報事件予以紀錄。可盡早發現是否有異常的行為發生。									
1-2	本機群組帳號的使用申請機制(需要安裝 WinMatrix Web 套件)： (1) 可透過網頁選擇特定電腦（多選）申請將網域帳號加入本機群組中。 (2) 申請結果將透過網頁與 Email，告知申請人與使用人，無須其他人工介入。 (3) 可限定帳號加入本機群組的使用期間（有效期），當使用期間屆滿，電腦將顯示提示訊息後自動登出，並回收本機群組帳號（該網域帳號會從本機群組中被移出）。 (4) 使用期間屆滿前，原申請者可透過網頁延長本機群組帳號的使用期間。 (5) 支援一次申請多個本機群組權限。									
1-3	本機群組使用紀錄覆核： (1) 可依照日期（每日）覆核本機群組的申請使用紀錄（包含欄位：電腦、IP 位址、申請時間、申請人、申請帳號、申請原因），並於紀錄中標註意見與已覆核的旗標。 (2) 可自動 Email 寄送本機群組的申請使用紀錄與主管（覆核人員），郵件中提供覆核連結，便於主管（覆核人員）進行覆核作業。									
1-4	報表與查詢： (1) 使用 WinMatrix Console 中的通知樣版設定，自動寄送本機群組申請使用記錄，與本機群組的異動紀錄。 (2) 本機群組申請使用的紀錄查詢。 (3) 本機群組管理模組的操作記錄查詢。									

		(4) 覆核紀錄查詢。
1-5		角色指派：透過網頁可設定各單位的 (1) 主管角色：負責覆核特定單位本機群組申請使用紀錄，並可指派單位中可申請本機群組的人員。 (2) 本機群組申請者角色：擁有對特定單位的電腦做本機群組申請使用的權限。
1-6		提供分權分責委任覆核的管理作業： 例一：分公司主管可以指派分公司的某一位或多位電腦維護同仁，才可以申請本機權限。而被授權的電腦維護同仁透過 Web 介面進行帳號加入分公司特定電腦、特定權限群組的申請作業，即可獲得該帳號取得對應的權限，以便協助同仁進行電腦的維護工作。電腦維護同仁的作業內容，分公司主管於隔日可進行覆核作業。 例二：各單位同仁有電腦維護的需求時，填寫公司內部既有資訊服務申請單，經主管同意後，送往資訊單位。資訊單位接獲紙本單據後，於本系統中依照需求，將特定帳號加入特定電腦的某個權限群組中，以令該帳號能順利取得對應權限，進行相關的作業。資訊部門主管或此作業的管理人員，隔日即可覆核前一日的所有權限申請的項目。

系統畫面

電腦本機群組成員清單：清楚呈現所有電腦中，所有本機群組中的帳號清單。

Web 125.45 (IE 11.0) 繁體中文 简体中文 English

本機群組管理 > 本機群組清單

查詢條件: 電腦名稱: 包含: 模型/顯示群組: 顯示排除: 查詢

刪除 設定/刪除 更新資料 新增帳號/加入群組

完成帳號列表和進行分組

選擇名稱	電腦名稱	IP 位址	機台使用者	群組	模型	帳號/群組名稱	所屬本機群組	已啟用	申請使用卡	帳號日期	最後修改日期	備註
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	WDIA00slipd.comat		是	否	否	2020/03/17 11:06:31	系統針對 Windows Defender 應用
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	a b c	Usern	否	否	否	2020/03/17 11:06:31	
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	a-b	Usern	否	否	否	2020/03/17 11:06:31	
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	內置机号	Usern	否	否	否	2020/03/17 11:06:31	
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	ミサイル	Usern	否	否	否	2020/03/17 11:06:31	
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	12345678	Usern	否	否	否	2020/03/17 11:06:31	
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	TEST	Usern	否	否	否	2020/03/17 11:06:31	
☐	TEST	WIN-10-SUPPORT	192.168.81.60	本機	帳號	DetonAccount	System Managed Account Group	是	否	否	2020/03/17 11:06:31	由系統管理的使用者帳戶。
☐	TEST	WIN-10-SUPPORT	192.168.81.60	網域	帳號	sl07018	Remote Desktop Users	是	否	否	2020/03/17 11:06:31	

透過網頁申請使用本機群組使用帳號：分權分責機制，無須 IT 同仁介入即可完成申請，並留下紀錄備查。

Web 125.45 (IE 11.0) 繁體中文 简体中文 English

本機群組管理 > 申請網域帳號加入本機群組

申請網域帳號

申請類別	一般申請	電腦名稱	選擇 移除
申請期間	☐ 永久有效 ☒ 2020/03/17 12:03:07 起 使用 8 小時 ☐ 2020/03/17 12:03:07 起 至截止日期 23 : 59	申請本機群組	☐ Power Users ☐ Users ☐ Network Configuration Operators ☐ Remote Desktop Users
申請帳號	simopro.com \ admin 檢查帳號	使用人	testadmin1 選擇
申請原因	軟體安裝	填報人	admin (testadmin1)
填報時間	2020/03/17 12:03:07	備註	↑ ↓
建立人	admin (testadmin1)	建立日期	2020/03/17 12:03:07
修改者	admin (testadmin1)	修改日期	2020/03/17 12:03:07

申請

清除重填

主管每日覆核本機群組使用紀錄：透過電子郵件通知與網頁覆核機制，達到紀錄清單產出與通知自動化，覆核作業無紙化的目標。

本機群組管理

本機群組清單

排除顯示群組成員設定

申請及使用紀錄

角色指派紀錄

操作紀錄

設定

指派角色

管理設定

本機作業

申請網域帳號加入本機群組

申請延長使用

覆核紀錄

覆核作業

日期

2019/12/30

備註

組織

simopro.com\TEST\

本機群組使用紀錄

0筆

覆核時間

角色指派紀錄(本機群組)

8筆

覆核人員

覆核

回上一層

角色指派紀錄(本機群組) : 8筆

回頂端

列印匯出欄位設定

拖曳標題列至此進行分組

組織名稱	角色類型	操作類型	指派者	被指派者	建立日期	建立者
TEST	單位主管	移除	rd107017 (陳威佐)	陳威佐	2019/12/30 10:14:27	rd107017 (陳威佐)
TEST	單位主管	新增	rd107017 (陳威佐)	陳威佐	2019/12/30 10:14:25	rd107017 (陳威佐)
TEST	單位主管	移除	rd107017 (陳威佐)	陳威佐	2019/12/30 10:12:59	rd107017 (陳威佐)
TEST	單位主管	新增	rd107017 (陳威佐)	陳威佐	2019/12/30 10:12:57	rd107017 (陳威佐)
TEST	單位主管	移除	rd107017 (陳威佐)	陳威佐	2019/12/30 10:11:22	rd107017 (陳威佐)
TEST	單位主管	新增	rd107017 (陳威佐)	陳威佐	2019/12/30 10:11:19	rd107017 (陳威佐)
TEST	單位主管	移除	rd107017 (陳威佐)	陳威佐	2019/12/30 10:07:28	rd107017 (陳威佐)
TEST	單位主管	新增	rd107017 (陳威佐)	陳威佐	2019/12/30 10:07:25	rd107017 (陳威佐)

文件編修日期：2023 年 5 月 23 日。

- *1：電腦本機權限群組（本文中簡稱本機群組或群組）是指 Windows 中管理帳號權限的群組，而本模組的功能係針對「Administrators 以外」的所有權限群組進行清查與管理。
- *2：「網域帳號移出群組」的意思是指，從 Web 管理介面中的「本機群組清單」的清查畫面中，管理人員可以挑選特定的一筆或多筆資料，進行移出群組的操作，當系統執行成功後，這些網域帳號將從本機群組成員中被移除。然而網域帳號仍然存在 AD 主機中，本系統並不具備編修維護 AD 主機的功能。如果執行「網域帳號移出群組」時，目標電腦並不存在（不在線上），系統將提示錯誤訊息。
- * 「本機群組管理模組」為 WinMatrix 選購的功能模組，若您有此需求，可洽 support@simopro.com 以獲得更多資訊與訂購的協助。（使用本模組，客戶需要已經購買 WinMatrix Server 與標準功能模組的軟體使用授權）