

MailSherlock 商業規格

1 系統管理

- 1.1 公司資訊：可設定公司名稱、系統標題名稱，並且可替換系統預設的商標與背景圖示為公司自訂的圖示。
- 1.2 存取控制：設定管理介面的 IP 位址與通訊埠。可限制接受或拒絕連線來源位址，增加管理介面的安全性。
- 1.3 認證設定：啟動/關閉密碼保護設定及 session 認證設定。
- 1.4 操作記錄設定：啟動/關閉記錄網頁伺服器的操作記錄功能，並可設定只記錄特定的管理人員與模組。
- 1.5 操作記錄查詢：可查詢所有操作系統管理介面的歷史紀錄。
- 1.6 系統更新：可執行更新授權、檢查更新、安裝更新的功能，並可設定排程定期安裝更新。此外，會列出系統的保固日期、產品版本、授權人數、最後更新時間以及系統各模組 RPM 的版本資訊。
- 1.7 系統設定檔同步：當同時建置多台應用系統時，可指定一台作為 ConfigMaster，統一在 ConfigMaster 作設定即可同步至其它的系統主機，簡化管理的工作。**[附註] 採 SLB 架構才有此設計項目**
- 1.8 組態設定：提供 SWAP 目錄、語系、資料庫儲存方式、信件原始檔壓縮、時區等重要參數設定。

2 網路組態

- 2.1 網路介面設定：表列所有網路介面卡與其設定值。管理者可以修改網卡的 IP、子網路遮罩(netmask)與預設閘道(gateway)設定。
- 2.2 路由與閘道器：主要設定系統預設閘道器(default gateway)；靜態路由(static routing)，管理者可視需求做設定。
- 2.3 DNS 組態：可設定慣用 DNS 伺服器、其他 DNS 伺服器以及名稱解析查詢順序。
- 2.4 主機表：主機表是簡易的 DNS 資料(IP 對應主機名稱)，可用來加速常用 DNS 資料查詢。
- 2.5 掃描控制：設定系統對 SMTP 協定過濾的套用範圍。可設定排除特定網段或 IP 不做掃描。

3 郵件服務管理

- 3.1 郵件路由設定：提供 Mail Routing 的功能，可依網路環境設定郵件之目的地伺服器。
- 3.2 本地端郵件網域：設定郵件伺服器的收件網域，只要是包含在此設定中的郵件網域，都會做收信處理。

- 3.3 郵件轉寄權限設定：Relay 控制設定，利用連線來源 IP 位址限制及送信地址檢查來避免被利用發送廣告信。
- 3.4 MTA 雙佇列機制：系統採用 MTA 雙處理佇列技術，MTA 模組具有兩組獨立的工作流程，分別處理接收和投遞信件的工作，提高信件傳輸速度
- 3.5 系統佇列查詢：可列出系統信件佇列中的信件，被郵件稽核延遲寄送的信件會存放於此佇列中，可對佇列中的信件進行立即傳送或是刪除之處理。
- 3.6 信件佇列查詢：可列出信件佇列中的信件。可強制立即送出信件佇列中的信件。
- 3.7 信件佇列設定：信件佇列的重送時間，保存期限，與發送失敗的通知名單。
- 3.8 **DKIM/DomainKeys 設定**：可啟用DKIM/DomainKeys簽章與設定DKIM/DomainKeys簽章所需資訊。
- 3.9 進階參數設定：郵件伺服器相關參數設定
 - A. 進階參數設定
 - A.1 同時間最大處理信件數
 - A.2 每個連線可傳送的信件數量上限
 - A.3 每封郵件收件者數目上限
 - A.4 Inbound 郵件大小的最大限制
 - A.5 Outbound 郵件大小的最大限制
 - A.6 等待用戶端回應的時間上限
 - A.7 是否接受匿名寄件者
 - A.8 SMTP 認證 (支援 AD/LDAP/POP3/SMTP 認證主機)；進階核對帳號與寄件者
 - A.9 檢查本地端 Mailbox(寄件者與收件者)
 - B. 郵件格式設定
 - B.1 將員工經 密件副本 至它人信箱的信件加上主旨標籤
 - B.2 將員工經 直接轉寄 至它人信箱的信件加上主旨標籤
 - B.3 啟用 wimail.dat 信件格式自動解碼功能**
 - B.4 啟用本地端寄件者顯示名稱格式化功能
 - B.5 啟用本地端寄件者 Email 轉址功能
 - C. DoS 防治設定
 - C.1 DoS/DHA 攻擊封鎖時間
 - C.2 每個來源 IP 位址同時間最大連線數

C.3 每個來源 IP 位址一分鐘內最大連線數

- 3.10 **簽名檔設定**：可設定企業簽名檔，宣告企業郵件的使用聲明。簽名檔支援HTML可附加圖片的格式，語系支援繁中/簡中/英文等多國語系，系統會自動判讀信件內容語系選用對應的語系簽名檔。
- 3.11 SMTP 服務偵測來源：如果有服務偵測設備(例如：負載平衡器)在偵測系統的SMTP服務 (Port 25)，請在此處設定服務偵測設備的『來源 IP 位址』，以便 [統計報表 > 連線數統計] 能夠正確分類統計。
- 3.12 組態設定：提供分頁顯示每頁的資料筆數設定。

4 人員管理

- 4.1 LDAP 同步設定：人員名單可直接從 AD/LDAP 主機定期同步，並隨 AD/LDAP 主機中的人員異動而異動。
- 4.2 UNIX 帳號同步：人員名單可直接從 UNIX Mail Server 定期同步，並隨 UNIX Mail Server中的人員異動而異動。
- 4.3 **資料庫帳號同步**：人員名單可直接從遠端MySQL資料庫定期同步，並隨資料庫中的人員異動而異動。
- 4.4 部門管理：查詢目前部門資料，可新增或移除部門名單，提供 CSV 檔案匯出與匯入功能。
- 4.5 部門階層管理：部門階層以樹狀圖呈現，方便管理者修改部門設定與添加管理員、員工。
- 4.6 員工名單管理：查詢目前員工資料，可新增或移除員工，並提供 CSV 檔案匯出與匯入功能。
- 4.7 SpamCheck 隔離通知名單：被 SpamCheck 機制所隔離的信件，會定期發送
- 4.8 SpamCheck 隔離通知信，可批次設定人員是否要收到通知信。
- 4.9 End-user 設定值管理：可批次修改員工的系統個人化介面的設定，包含SpamCheck 選項以及自訂貼標籤、隔離與刪除的門檻值分數。
- 4.10 系統群組管理：可設定不同的系統群組，根據各個群組的權限設定每個登入系統管理介面的使用者權限。
- 4.11 系統帳號管理：設定登入系統管理介面的使用者帳號與密碼，以及管理權限分組。
- 4.12 系統認證設定：設定管理者登入的認證設定以及個人化介面的認證設定，支援本機認證，以及外部的 AD、LDAP、POP3 以及 SMTP 認證主機。
- 4.13 組態設定：可設定分頁顯示每頁的資料筆數、公司名稱、信件查詢的顯示類別、部門下拉選單、匯入 / 匯出 CSV 檔案語系、部門管理的顯示欄位、部門階層管理的顯示欄位、員工名單管理的顯示欄位以及員工名單管理中檢視員工信件的時間範圍。

5 郵件稽核

- 5.1 規則類別(Policy Group)：主要是以套用的對象做分類，例如全公司、研發部或是主管級，其次是以套用的稽核人員做為分類，例如：全公司有二組稽核人員，分別稽核不同的信件內容。
- 5.2 規則管理；管理系統中所有的規格，可以搜尋/編輯/啟用/停用/排序/刪除規則。**內建13條個資相關規則，可過濾信件本文與附件內容是否有出現身份證字號、生日、電話、手機號碼、信用卡卡號等資料。支援正規表示式(regular expression)可彈性設定樣式比對。**
- 5.3 稽核區；集中查詢命中稽核規則的信件，可以依稽核信件類別/規則，以及其他信件查詢常用條件，進行稽核郵件審核與調閱。
- 5.4 稽核通知：郵件稽核通知相關設定，如寄件者 Email/通知信提示訊息...等設定，以及指定重新寄送稽核通知信。
- 5.5 組態設定：設定事前/事後稽核模式，稽核區顯示的欄位與排序方式，附件檔遞迴解壓縮啟用與否以及解壓縮層數。

6 信件查詢

- 6.1 信件查詢：可查閱所有經過系統處理的郵件資訊。提供關聯式條件查詢，如：寄件者、收件者、主旨、內容、開始/結束日期、附加檔案檔名、信件大小及邏輯關係(AND/OR)等。
- 6.2 常用查詢條件：將常用的信件查詢條件彙整成列表，可供新增、編輯、刪除查詢條件。
- 6.3 隔離區管理：查詢出隔離區裡面的信件並做適當的處置，處置的方式包括刪除、轉寄、繼續寄信、繼續寄信並轉寄。隔離區會有三種信件，一種是因過濾條件而隔離的信件，一種是被判定為垃圾信而隔離的信件，一種是帶有病毒的信件。
- 6.4 收信記錄查詢：查詢所有系統處理的信件的記錄(log)，包含日期寄件者、收件者與信件處理狀態等訊息。收信記錄查詢表單提供多個常用的查詢條件，使用者可以依需求組合查詢條件做關聯式查詢。
- 6.5 Sendmail 記錄查詢：系統本身透過 Sendmail 來送信至下一端點，此功能可查詢 Sendmail 送信的記錄。
- 6.6 信件還原：信件還原功能，可以把管理者選定的信件，還原給原收件者或是指定的收件者。
- 6.7 信件還原記錄：可查看信件還原的所有記錄，了解信件還原的狀況。
- 6.8 備份信件管理：將備份信件還原後的存放管理區，可使用信件查詢的功能查看備份信件。
- 6.9 垃圾信提報管理：將管理者所提報的過的垃圾信記錄彙整成列表，並且提供設定提報垃圾信的寄送時間以及提報管理者 Email 位址。

6.10 組態設定：設定分頁顯示每頁的資料筆數，與顯示欄位設定。

7 統計報表

- 7.1 伺服器信件總覽：統計信件進出的信件大小和信件數量，提供日報表、週報表、月報表、年報表、資料庫統計及自定範圍等六種報表期間設定。
- 7.2 正常信件統計：提供日報表、週報表、月報表、年報表、資料庫統計及自定範圍等六種報表期間設定。
- 7.3 垃圾信件統計：提供日報表、週報表、月報表、年報表、資料庫統計及自定範圍等六種報表期間設定。幫助管理員了解在某一期間內的每個部門的垃圾郵件收發數量、比例以及垃圾信評比分數等。可將垃圾信的統計資料匯出成 CSV 檔。
- 7.4 病毒信件統計：提供日報表、週報表、月報表、年報表、資料庫統計及自訂範圍等六種報表期間設定。可依病毒名稱、病毒來源以及寄件者做病毒信件量排行。可將病毒的統計資料會出成 CSV 檔。
- 7.5 正常信件排行榜：可依寄件數、寄件量、信件大小等條件列出排行榜並提供友善列印功能。提供「匯出 CSV 檔」功能，將排行榜匯出成 CSV 檔。
- 7.6 垃圾信件排行榜：垃圾信件可依指定的部門、時間區段，針對垃圾信件來源 IP 位址、垃圾信件來源網域、寄件者、收件者等條件列出排行。
- 7.7 病毒信件排行榜：病毒信件可依寄件數、寄件量、信件大小，病毒名稱等條件列出排行榜並提供友善列印功能。提供「匯出 CSV 檔」功能，將排行榜匯出成 CSV 檔。
- 7.8 連線數統計：表示收信記錄的分類統計，方便管理者了解信件的處理狀況。信件狀態分類包含：Anti-Spam、連線逾時、郵件伺服器限制條件、郵件過濾、SMTP 命令錯誤、伺服器狀態及攻擊行為等。
- 7.9 放行信件統計：依據系統 User 所放行的信件，依照寄件者、收件者、來源IP 位址以及來源網域作為統計對象，並列出其放行信件數為何。
- 7.10 SpamCheck 分數統計：可統計經由 SpamCheck 引擎評分的垃圾信件，各分數的信件量統計。
- 7.11 DoS 連線次數統計：統計連線攻擊來線 IP。
- 7.12 報表寄送排程：可新增報表寄送排程與列出管理者所設定的所有報表排程設定，並且可以進行批次刪除/啟用的設定。
- 7.13 組態設定：設定伺服器信件統計預設值，正常信、病毒信統計預設值，正常信、病毒信排行榜預設值，DoS 連線次數統計預設值。

8 資料庫管理

- 8.1 資料庫設定：設定連線資料庫的帳號密碼。
- 8.2 MySQL 帳號管理：可設定系統 MySQL root 密碼。

- 8.3 資料庫總覽：可統一檢閱信件總數、附件檔案總數及資料庫總容量。
- 8.4 資料庫檢測：可即時檢測目前資料庫的檔案是否有毀損，分詳細檢測與快速檢測。
- 8.5 備份檔案管理：立即備份信件資料，可選擇備份信件種類、自訂信件時間、和分卷壓縮。
- 8.6 郵件備份排程：排程定期備份。可設定日期範圍備份該日期區間的信件資料。備份裝置支援本機硬碟與磁帶。支援分卷壓縮功能可將備份檔分成合適的檔案大小以便儲存於磁帶或燒製光碟。
- 8.7 郵件備份回存：對應備份功能，可將備份檔回存至主資料庫或是獨立的資料庫。
- 8.8 郵件保存期限：以「年」、「月」、「週」、「日」為單位設定信件紀錄保存期限。
- 8.9 **Near-lineDB 設定**：Near-line DB 是將主機之外的資料庫主機，用以儲存主機中的過期信件資料。程式會將本機上過期的資料移到 Near-line DB 上。
- 8.10 備援資料庫管理：可設定備援資料程式的排程、備援資料庫的連線帳戶、備援資料庫的郵件保存期限以及備援資料庫的總容量等，並且可做備份信件查詢。
- 8.11 遠端備份設定：可選用遠端FTP, NFS, USB 或網路芳鄰方式備份。
- 8.12 資料庫管理警訊：查看所有信件備份、信件回復及信件刪除動作的記錄，管理者可以檢閱所有動作的執行過程與結果。
- 8.13 組態設定：設定資料庫管理相關的組態參數。

9 系統管理

- 9.1 硬體資訊：顯示中央處理器資訊與記憶體使用量資訊。
- 9.2 磁碟使用狀況：可顯示磁碟大小 (MB)、剩餘空間 (MB)、已使用空間 (MB)、使用比例圖及使用比例等資訊。
- 9.3 處理程序管理：可設定系統各子系統(如sendmail、mysql、mailfilter、supervise_queue、maillog、POP3、web、FTP)之狀態(停止或啟動)。
- 9.4 遠端備份設定：可選用遠端FTP, NFS, USB 或網路芳鄰方式備份。
- 9.5 系統設定檔備份：可備份/回復系統相關設定檔、網路設定檔、密碼檔。可使用在系統重建時，方便回復系械相關設定檔。
- 9.6 系統時間：設定日期時間，並提供網路校時功能以及將系統本身作為時間伺服器，讓 Client 連接我們進行時間同步。
- 9.7 開機與關機：提供介面方便管理者重新啟動系統 (restart) 與關閉系統 (shutdown)。
- 9.8 密碼管理：可管理相關系統帳號，並提供更改密碼功能。
- 9.9 組態設定：設定分頁顯示每頁的資料筆數與系統設定檔備份路徑。

10 訊息通報

- 10.1 通報名單：管理通報名單、訊息通報的項目及通報方式。
- 10.2 訊息設定：列出目前系統有提供的訊息，包括：磁碟容量、處理程序以及信件佇列信件數超過特定數目警示訊息通報。
- 10.3 SMTP 伺服器設定：採用Email 的方式發送系統通報訊息。
- 10.4 組態設定：設定分頁顯示每頁的資料筆數。

11 設定精靈

設定精靈會一步一步說明與引導管理者進行系統設定。

12 Anti-Virus (選購：Sophos)

- 12.1 防毒引擎資訊：提供防毒引擎狀態、病毒碼更新狀態及病毒碼列表等病毒資訊。
- 12.2 病毒碼更新設定：管理員可設定以排程的方式定時更新病毒碼也可以手動的方式更新病毒碼。
- 12.3 防毒設定：防毒設定直接影響有夾檔的信件收發，因為系統會針對中毒或無法掃描的信件進一步做隔離、修復、刪除或放行的動作。管理者在設定時必須考慮到郵件的安全性和公司政策。
- 12.4 暫時性黑名單：主要是針對發送病毒來源 IP 做連線的限制，這樣能有效的避免在短時間內收到大量的病毒信件，減緩病毒信件攻擊力道。

13 Anti-Spam (選購：SpamCheck)

- 13.1 垃圾信防堵機制：提供多樣化的垃圾信防堵機制設定。
 - 13.1.1 Real-time Blackhole Lists (RBL) 檢查
 - 13.1.2 IP 位址 DNS 反查
 - 13.1.3 檢查 EHLO/HELO 所傳送的主機名稱是否有 DNS 記錄
 - 13.1.4 檢查信件虛假路由
 - 13.1.5 檢查假冒本地端寄件者 (FakeSender)
 - 13.1.5.1 外部來源假冒本地端寄件者：AntiSpam機制拒收
 - 13.1.5.2 內部來源假冒本地端寄件者(冒名發黑函)：可啟用「限制 SMTP 認證帳號與寄件者 Email 必須相符」
 - 13.1.6 灰名單檢查機制開關，或指定開啟時間
 - 13.1.7 檢查寄件者的 Email address 是否真的存在
- 13.2 RBL 管理：管理 RBL 清單，可新增、停用或刪除 RBL 清單，也可以查詢輸入的 IP 位址是否被列於 RBL 黑名單中。

- 13.3 白名單：可依電子郵件地址、IP 位址、郵件網域設定白名單。白名單是用來跳脫 Anti-Spam 的檢查機制，並可設定開啟自動白名單功能。
- 13.4 黑名單：根據設定條件拒收特定來源的郵件，可設定的三種擋信黑名單包括電子郵件地址名單、IP 位址名單、郵件網域名單。
- 13.5 DoS/DHA 暫時性黑名單：暫時性黑名單的有效期限允許管理員自行訂定，期限一到自動清除名單，並允許管理員自行手動新增或刪除名單。
- 13.6 SpamCheck 組態設定：SpamCheck 引擎功能開關，自動學習機制開關，忽略的郵件大小設定，垃圾信標記、隔離、刪除分數設定，標記名稱設定。
- 13.7 SpamCheck 規則更新：設定 SpamCheck 引擎規則，自動更新的排程。
- 13.8 SpamCheck 隔離通知：被 SpamCheck 引擎判斷為垃圾信，且開啟隔離時，是否要發送隔離通知的開關選項，並可自訂隔離通知信的發送者、標題，內容，指定發送的頻率，或自訂時間範圍發送，放行信件內容可指定有放行、放行並加入白名單、放行並加入黑名單等動作，並提供隔離通知信發送測試信介面與隔離通知信重新發送介面。
- 13.9 SpamCheck 放行記錄：可查詢相關人員放行信件的歷史資訊。
- 13.10 SpamCheck 規則管理：設定 SpamCheck 引擎規則的分數高低。
- 13.11 SpamCheck 關鍵字設定：SpamCheck 引擎使用的規則，可依使用自訂的關鍵字設定分數高低。
- 13.12 組態設定：設定分頁顯示每頁的資料筆數及 SpamCheck 隔離通知的發送時間範圍。

14 個人化介面功能(選購：SpamCheck)

- 13.1 信件查詢：可供查詢個人信件，包括不分類、正常信、垃圾信(未檢閱)、垃圾信(已檢閱)、過濾信和病毒信。
- 13.2 統計報表：依個人所收到的信件，將其繪成圖表，包括日報表/週報表/月報表/年報表。
- 13.3 黑名單：可管理(新增、刪除、匯出、匯入和搜尋)個人的黑名單，包含Email、IP 位址、網域。
- 13.4 白名單：可管理(新增、刪除、匯出、匯入和搜尋)個人的白名單，包含Email、IP 位址、網域。
- 13.5 設定項目：可設定個人化參數，包含郵件過濾設定、分數門檻值、修改密碼、設定語系、信件查詢預設排序欄位與信件查詢顯示欄位。