NTS 版本 5.2.1 軟體更新內容說明

適用型號

NTS 1134F / NTS 1136F / NTS 1154FR / NTS 3356FR / NTS 3372FR / NTS5572FT

適用版本

5.2.0.4

注意事項

1.軟體更新之後, 系統會自動重新開機約 3 ~ 5 分鐘

2.如果 5.2.0.x（非 5.2.0.4）版本，不會更新成功，但是設備會重開機一次

更新事項

==========

##首頁

-新增 登入和首頁,增加有新韌體版本可以更新提示

##系統設定 > 備份和升級

-新增 USB 還原功能

##系統設定 > 訊息通知

-修正 訊息通知信，紀錄都不會含昨天最後一次寄送之後的紀錄

##系統設定 > 統計報表

-修正 系統設定 > 統計報表 > 報表查詢區間 - 修改查詢範圍最大值修正最大日期為 99 天

-修正 報表>系統回報與安全係數的事件,拿掉 "NO_"

##系統設定 > AP 管理

-修正 系統設定 > AP 管理派送多台 NWA1100-NH 時，只有第一台會派送成功。

##網路介面及路由 > 網路介面

-修正 DMZ 設定 T-Briding，無法新增 subnet

-修正 線路偵測方式

-修正 DMZ Transparent Bridging 設定問題

-修正 LAN 介面儲存， 發生的系統錯誤

##管制條例

-修正 管制條例 即時流量資料出不來問題

-修正 IPv6 條例,編輯時無法選擇使用的外部網路

-修正 內對外 IPv6 NAT 或 Routing 不通

-修正 管制條例，當選擇應用程式管制又切換動作為拒絕後，封包不會被 Drop 掉，且會跑應用程式管制

-修正 IPv6 條例管制 指定線路不通時, 往下一筆條例比對

-修正 IPv6 線路負載, 判斷該介面斷線

-修正 設備開機,流量配額的設定值載入錯誤

-修正 在解析度大於 1600*900 ，顯示不正常

##管理目標 > 位址表

-修正 部份 ARP Table 無法清掉

##管理目標 > 服務表
-新增 服務群組 ICMP 封包
##管理目標 > 應用程式管理
-修正 開啟 BT 阻擋，會影響 Google 服務無法正常使用
-新增 應用程式管理，支援 OneDrive（2015 版 17.3.6390.0509 , 2016 版 17.3.6743.1212）
-修正 應用程式 BT，誤擋 DHCP
##管理目標 > URL 管理
-修正 URL 白名單 Domain 白名單設定相同網域時,誤擋狀況
-調整 管理目標 > URL 管理、位址表 的 Domain 是否真實存在檢查拿掉
##管理目標 > 上網認證
-修正 管理目標 > 上網認證 [頁面設定] 按儲存後出現 "CMD Error"
-修正 使用者群組>POP3 伺服器設定設定多台,其一 SERVER 無回應登入過久的問題
-新增 管理目標 > 上網認證 > 頁面設定 增加 上網認證登入頁面背景及文字的顏色自訂項目
##管理目標 > 電子白板
-修正 使用電子白板時,若電腦打開的網址有帶斜線的目錄位置,導向錯誤的問題
##管理目標 > RADIUS
-新增 管理目標 > RADIUS
-修正 管理目標 > RADIUS > 客戶端 客戶端位址 設為網段，登入 AP 後，無法自動認證上網認證，會出現輸入帳密畫面
##網路服務 > DHCP 服務
-修正 DMZ 介面沒有綁定 IP，啟用 DMZ DHCP，導致服務錯誤
##網路服務 > DNS 伺服器
-新增 DNS SRV 紀錄需求
-新增 IPv6 反解設定
-新增 AAAA 記錄 負載平衡功能
##網路服務 > FTP 服務
-修正 Loading 過重，Lose 掉的狀況
##網路服務 > 病毒引擎
-修正 網路服務 > 病毒引擎 > ClamAV 引擎 無法更新病毒碼
-修正 卡巴斯基 無法啟動問題
-修正 網路服務 > 病毒引擎 > Kaspersky 引擎清除紀錄 無效
##網路服務 > 高可用性
-修正 HA 運作時的相關錯誤問題
##進階防護 > 異常 IP 分析
-修正 進階防護 > 異常 IP 分析 偵測不到
##進階防護 > 交換器管理

-修正 編輯綁定清單 的操作日誌錯誤

-修正 網路狀態圖 > 點兩下 > Port 資訊 表格的排序有問題
-修正 網路狀態圖 > 點兩下 > Port 資訊 排序資料時，更新時間會錯誤
-修正 DHCP Snooping 啟用的 vlan 其範圍若是連續數字(eg: 1-5)，會解析錯誤
-新增 進階防護 > 交換器管理 > IP Source Guard 綁定清單，綁定 port 可以設置 Any
-修正 刪除綁定清單時，在某些情況下會誤關掉 IP Source Guard
##進階防護 > 內網防護
-調整 IP 衝突偵測方式
-調整 [進階防護 > 內網防護 > 防護介面 > 偵測介面] 介面需為 NAT 模式
-新增 自動封鎖，可設定封鎖 Dump Switch port
-修正 [進階防護 > 內網防護 > Mac 衝突紀錄] 顯示 169.254.0.0/16
##郵件管理 > 郵件過濾與記錄
-調整 AD 有效帳號同步
-修正 郵件問題
-新增 郵件內文 URL 過濾功能
-新增 垃圾郵件過濾，垃圾郵件過濾引擎 Rspamd
**設定 垃圾郵件過濾引擎 Rspamd 取代 SpamAssassin 後 ，此動作不可逆且 SpamAssassin 的學習資料庫將被清除
-新增 郵件 POP3 中毒信件的動作 => 修改附檔名跟主旨
-修正 DMZ-Bridge 模式下開啟郵件記錄會不通問題
##郵件管理 > 郵件記錄查詢
-修正 刪除的信件按下載，會有錯誤訊息
##SSL VPN > SSL VPN 設定
-修正 本機帳號設定到期日已到期，但 sslvpn 還能連線
-修正 SSLVPN 登入 密碼支援特殊字元 "
-新增 SSL VPN > SSL VPN 設定 > 連線軟體下載自訂頁面設定
##VPN > IPSec Tunnel
-新增 IPSEC 建立時可以多網段
-修正 IPSEC 連線錯誤
##VPN > L2TP
-新增 L2TP 功能
##其他
-修正 在 DMZ bridging 模式下，可以用其他 WAN1 IP 連到管理介面