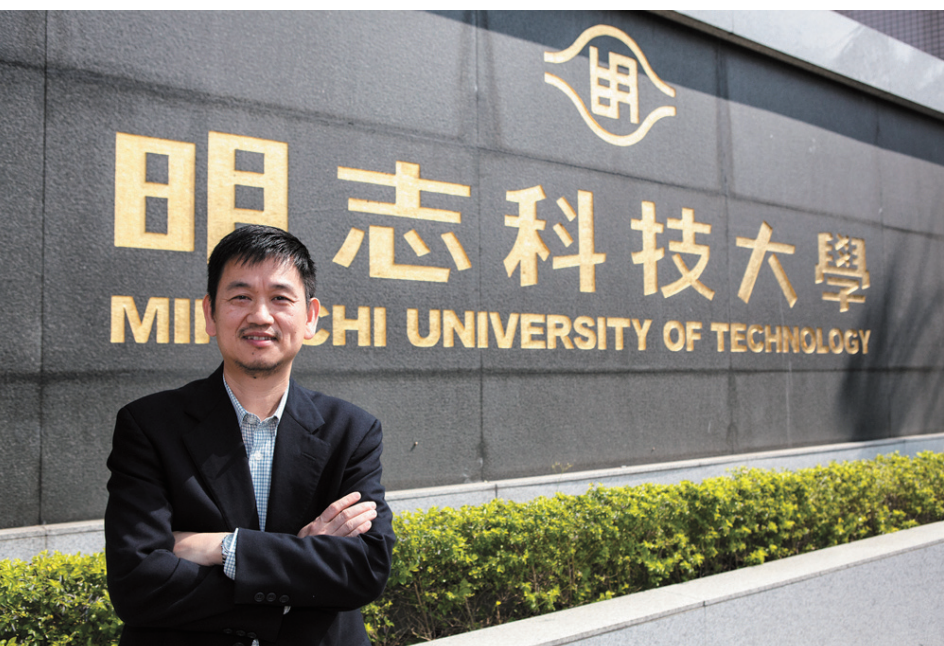


IBM Security Systems X 德瑞數位 單一簽入、自動管理、強化資安

助明志科技大學實現智慧化校園



校園 E 化與智慧化是明志科技大學持續追求的目標，而當教務、學務系統的應用發展日漸成熟，使用者帳號與權限管理也越來越複雜，不僅影響行政效率與 IT 服務品質，更有可能引發資安疑慮。其實，這樣的困擾，普遍存在於各大專院校與政府機構的 IT 環境中。

多元應用系統，增添管理難度

對於使用者而言，每天使用的應用系統數量最多可達十數種，每一個系統都必須單獨登入，且其授權模式、帳號原則、密碼規則都有差異，經常面臨忘記密碼、甚至將密碼寫在顯眼處以至於失去保護原意。對行政單位來說，頻繁在不同應用程式間登入、登出也會浪費工作時間、影響行政效率。

對 IT 管理者來說，分散的應用程式與帳號權限管理，更是一項吃力不討好的艱鉅任務。明志科技大學圖書資訊處圖資長黃植振博士便指出，尚未導入單一簽入系統之前，IT 團隊面臨多重挑戰：

- 一、多重應用程式、帳號與後端資料庫的維護作業，造成 IT 人員沉重負擔
- 二、跨系統與應用程式無法做到即時性管理
- 三、使用者權限沒有政策化管理，造成管理爭議
- 四、使用者身分更動無法立即反應於帳號權限，引發資安疑慮與機密資料風險
- 五、學期初、末，新舊生與畢業生的大量帳號新增與變動造成工作負擔
- 六、資訊散落各系統中，無法有效整合提供給使用者

位於新北市泰山區的明志科技大學，以與時俱進的紮實教學課程、豐富產學合作經驗及獨特「三明治」實習制度，培育許多兼具學術與實務經驗的優良學子。然而獨特的校務與學務體制，也增加了 IT 使用者身分管理的複雜性與資安挑戰。為提升行政效率與資訊服務品質，明志科技大學決定採用 IBM 的解決方案，並委由德瑞數位協助建置導入，打造全校通用的單一簽入系統 (single sign-on)，導入完成後的卓越管理效益與便捷效率，更被校方譽為其 IT 管理的一項重要里程碑。

產學合作制度，帶來獨特挑戰

在這些挑戰之上，明志科大廣受各界好評的「三明治」工讀實習制度，也讓帳號密碼管理更形複雜。在一年的工讀實習期間，學生會進入台塑集團、宏達電、華碩等企業實習，甚至遠赴國外。

身為台塑集團的成員，明志科大還必須與集團 IT 系統串聯整合，因為每一位教職員都會設立企業集團 ERP 系統權限，且可能在集團中身兼不同角色，有時集團子公司如長庚生技也會派人駐點於學校、使用學校的系統。這些跨組織、跨系統的管理都是明志科大 IT 團隊要面臨的獨特問題。

權限變更時間差，引發資安疑慮

除此之外，明志科大導入單一簽入系統之前，個資法雖尚未立法完成，但 IT 團隊已經預見可能帶來的挑戰與衝擊。既有系統從人事變動發布到帳號密碼權限變有一段時間差，最極端的情況是：員工被解職後，利用這段時間差做出影響個資安全或系統安全的行為。

為了一次解決以上所有難題，明志科大決定引進 IBM 單一簽入管理系統，並委由具有豐富經驗的德瑞數位協助導入單一簽入系統、建立使用者入口網站。黃處長指出，當初評比市面上相關廠商與解決方案，認為 IBM 具有領導品牌的高可靠性、優異產品整合度與可驗證的成功案例，而德瑞則在校園 E 化與目錄服務系統整合技術有專業資歷與實績，使得 IBM 與德瑞在縝密比較後雀屏中選、獲得明志科大青睞。

在與 IBM、德瑞數位深入討論後，明志科大 IT 團隊為這項專案設定了三大目標：

- 一、簡化帳號與權限管理，確保資料一致性，減少作業錯誤。
- 二、單一帳號密碼就能取用其權限允許的所有資源，並符合資訊安全稽核要求。
- 三、個人化入口網站提供詳盡應用與工作項目清單，訊息在校務單位、學生組織之間可即時傳遞，提升互動，並確保重大政策有效傳達。

四大解決方案，一次解決所有挑戰

為此，IBM 與德瑞數位為明志科技大學規劃建置四大功能 -

- 一、整合性的身分認證管理平台：建立教職員與學生身分資料總目錄，儲存於目錄伺服器 (LDAP Server) 中，作為集中認證與共通授權的基礎。透過 LDAP 權限控管機制與 web-based 管理介面，管理者在單一介面即可完成所有政策制定與權限管理需求。
- 二、統一化帳號服務系統：整合教職員人事資料庫 (Oracle 系統)、學生學籍資料庫 (MSSQL)、AD、OPEN LDAP 帳號，提供自動化處理大量帳號密碼變更的功能，減輕管理負擔，所有變更可即時生效，確保資安無虞。

三、單一簽入 (single sign-on) 的個人化校園入口網站：在單一入口網站登入一次，就可依使用者權限呈現所有應用程式與相關訊息，並使用被授權的網路資源。此外並提供人性化、高彈性的應用程式開發介面，以利新舊系統整合與未來開發所需。

四、發展協同運作平台，提供業務支援介面、知識入口網站、行事曆、知識社群討論區、問卷系統、公告、個人網路書籤、文件檔案分享等服務，提升行政效率與 IT 服務品質。

IBM TIM 身分管理自動化，十分鐘搞定品質與效率

德瑞數位運用 IBM Tivoli Identity Manager (TIM) 來打造高度自動化、零時間差的同步帳號管理能力。TIM 將明志科大現有的 Oracle、MS SQL 資料庫自動同步至 IBM LDAP 資料庫，管理者亦可將不同資料源的帳號透過 web-based 管理介面新增至同步機制中。

TIM 提供卓越的角色管理與人員組織群組管理功能，每一個角色所使用到的相關應用如電子郵件、學務系統、校務系統等等，都經由高度可視化的方式進行管理，由人事單位就能輕易進行調整，因此一項異動生效後僅需數分鐘就能完成權限調整，效率遠遠高於過去層層轉介、動輒數天的情形。

學生在學年升級、工讀實習之間產生的各種異動，也由 TIM 來進行其組織設計，完美符合其不同年級、不同系別規劃，滿足變動資料管理的需求。全自動化的管理，免除過去每學期大量人工轉檔的龐雜工作，只要在教務處系統中輸入變動需求，後續的權限更動與批次轉檔都可即時生效，大幅減少人工作業負擔、提升管理效率。

例如一位學生如果辦理休學，過去需要數天至一周才能完全將其應用權限修改完，現在僅需十分鐘就能取消其相關權限，效率顯著提升。而學生畢業後，也能立即將其組織角色進行調整，畢業生一登入校園入口網站，呈現的資訊就從社團活動或選課服務即時轉換成校友聯繫、就業資訊等等，為使用者與管理者帶來雙贏。

黃處長表示，這項專案導入後，不僅完美解決跨組織、跨系統、跨應用的複雜帳號管理問題，確實達成預設的三大目標，使用效益也十分顯著。IBM 的絕佳整合性與擴充彈性不僅能完美整合原有系統，亦可滿足學校提出的各項客製化個別要求。每一位使用者都能明確感受到單一簽入的便捷效益，而 IT 團隊的管理負擔也大大減輕，使得這項專案被校長譽為 IT 管理的一項重大里程碑！

註：IBM Tivoli Identity Manager 目前屬於 IBM Security Systems 產品線