 文／編輯部

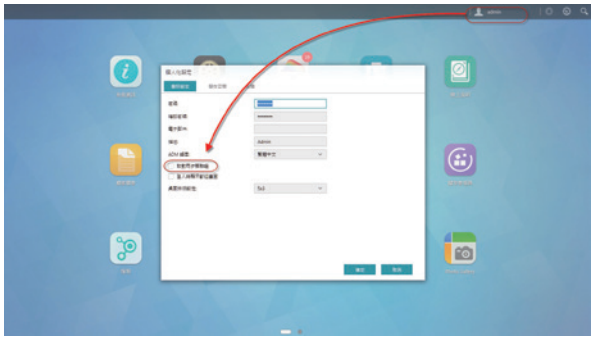
以ASUSTOR NAS為例

保障資料安全的防「駭」對策

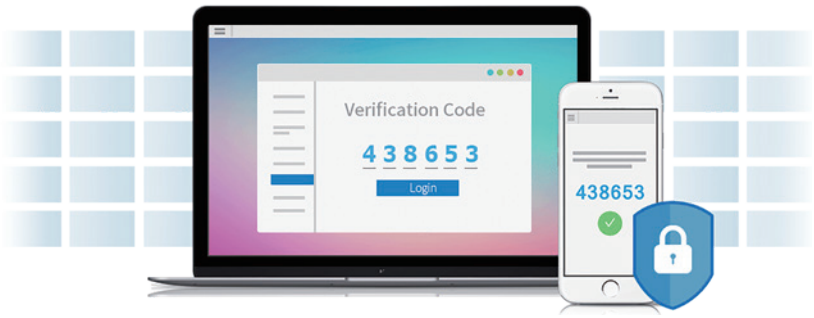
對於每日與網路為伍的科技人而言，最擔心的莫過於電腦中毒資料全毀，因此如何為自身的資料安全做好防護措施，成為個人及企業的必修課題。當然，你可以選擇防毒軟體來阻擋惡意軟體的侵襲，也能強化帳戶及資料存取的安全性，或是掌握3-2-1備份原則，將自己的重要資料「備份」起來。就讓我們一起來看看，華芸NAS所提供的防駭對策。

二步驟驗證

駭客最常使用的方式就是破解或盜用登入密碼，登入系統後植入惡意程式，因此密碼失竊事件層出不窮，且遠比想像中更容易發生。二步驟驗證可謂是防駭的第一道鎖，用來保障帳號登入的安全性。這個機制讓用戶必需事先指定自己隨身的手機號碼，作為每次登入時接收驗証碼的裝置，用戶在登入時同時需輸入指定手機上的驗証碼，驗明身份後才能登入NAS。因此可確保登入者即為手機持有人，保障帳號使用者身份的真實性。



由ADM的使用者帳號中可以啟動二步驟驗証功能。

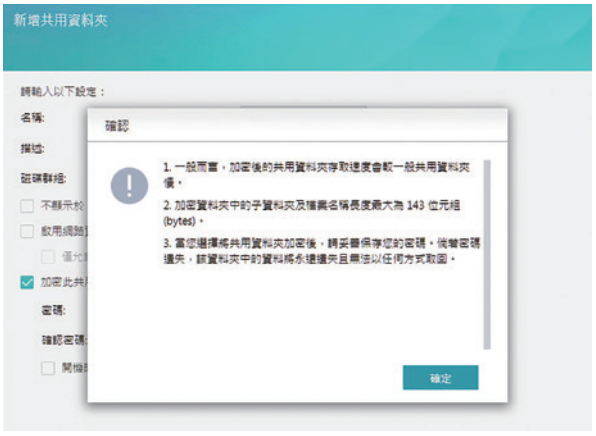


同時使用密碼和個人手機以確保帳號隱私及資料安全。

AES-256bit資料加密

保護資料的第二道鎖是將資料進行加密。ADM內建軍規級的AES 256-bit加密方案，將共用資料夾加密後，所有儲存在此共用資料夾的檔案都會自動被加密且無法輕易破解，即使NAS或硬碟被盜或遺失，都能有效保護資料不外洩。而ADM採用共用資料夾加密（Folder-based）而非磁碟空間加密（Volume-based），因此用戶可以將一般性資料與機密性資料分開，更有彈性的將高機密性資料夾進行加密，而不影響到系統整體的傳輸效能。

1 >> 存取控制新增共用資料夾時，將加密共用資料夾選項打勾即可。

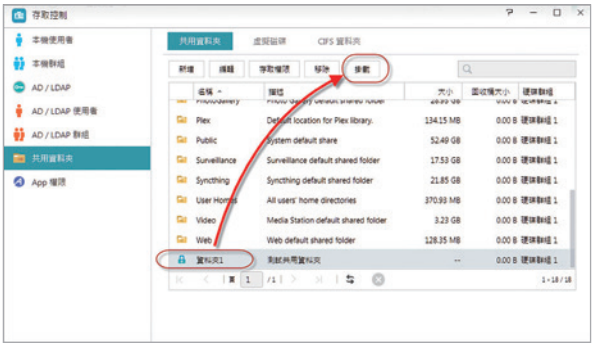


2 >> 設定精靈依步驟完成，資訊提示妥善保存密碼。

3 >> 設定密碼。

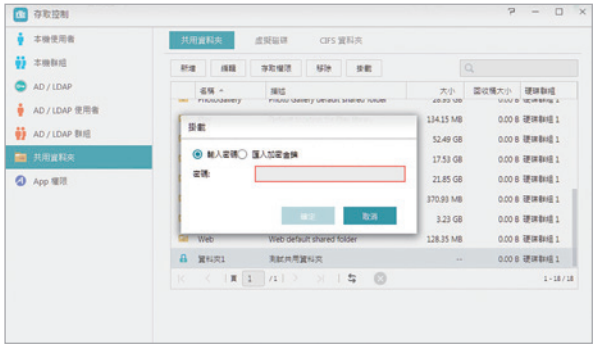
4 >> 設定存取權限。

5 >> 檢視設定後按完成。

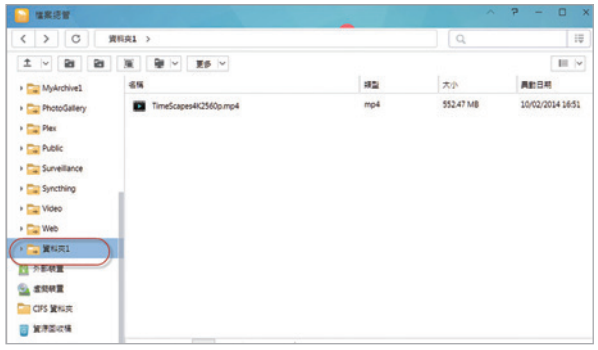


6 >> 選擇掛載加密資料夾。

管理者可設定存取此共用資料夾的使用者或群組權限，只要管理者輸入前步驟中所建立的密碼，就能將其掛載或取消掛載，掛載後則可於網路芳鄰或是ADM檔案總管中查看此資料夾。



7 >> 掛載加密資料夾需要輸入步驟三的密碼。

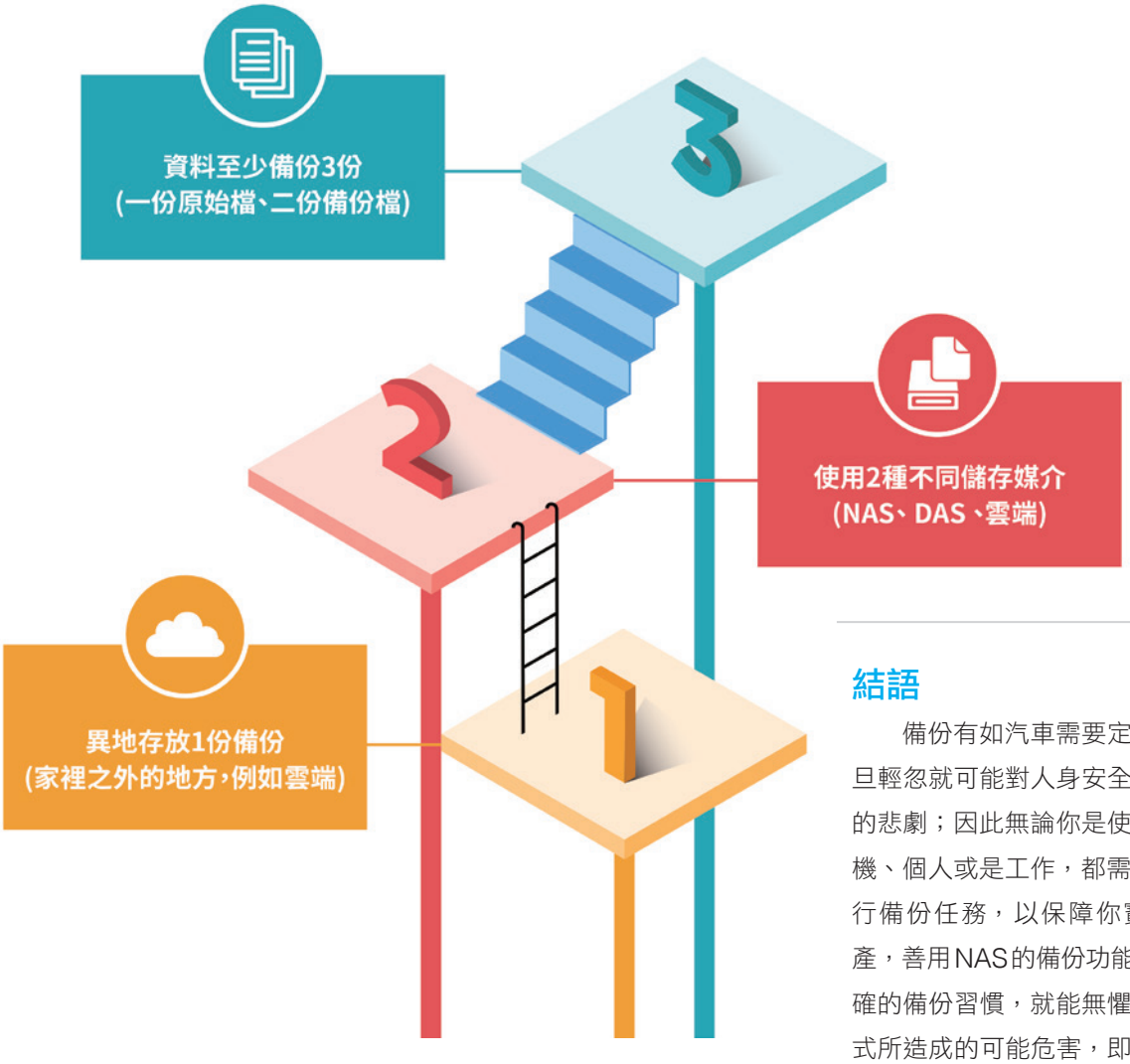


8 >> 掛載後可於檔案總管內檢視此資料夾，取消掛載則會隱藏此資料夾。

備份3-2-1

備份已是老生常談的議題了，所謂有備無患，預防重於治療，皆是保險的概念。那麼到底要做幾份備份才能保障資料安全呢？根據美國電腦緊急應變小組在2012年提出的備份原則，也是目前最能被接受的備份實作規則是3-2-1原則。何謂3-2-1原則呢？即是相同資料至少存三份，使用二種不同的儲存媒介來進行備份，而其中一份備份必需存放於異地。如此一來，無論那一份資料毀損，至少都會有一份備份被保留下來。

如何使用NAS來達成3-2-1備份原則呢？以ASUSTOR NAS為例，Backup Plan及Time Machine即是電腦與NAS間的備份工具；而NAS與NAS間也能設定為Rsync異地備份，或利用MyArchive方式將NAS資料備份為可卸載的MyArchive硬碟，以及充份用NAS的硬體介面再連結外接儲存裝置等，皆應用了二種儲存媒介及產生三份備份資料；透過NAS的App Central還能安裝第三方公有雲端App進行資料同步，無論是儲存媒介的使用或是異地儲存，都可在ASUSTOR NAS上實現。



結語

備份有如汽車需要定期保養般，一旦輕忽就可能對人身安全造成無法挽回的悲劇；因此無論你是使用電腦或是手機、個人或是工作，都需要定時定期執行備份任務，以保障你寶貴的數位資產，善用NAS的備份功能，並且養成正確的備份習慣，就能無懼駭客及惡意程式所造成的可能危害，即使在面臨硬碟毀損或資料遺失之時，也能輕鬆將資料回復，為個人或是公司降低損害。