clientron 公信電子股份有限公司

在現今VDI, DaaS, Cloud 數位工作環境下，使用IGEL Linux endpoint OS　於終端電腦設備，搭配IT 管理者充分使用IGEL UMS 通用管理介面，經由 適當的設定與遠端部屬，能大幅提高端點電腦設備的安全性。

IT管理人員透過操作IGEL UMS (Universal Management Suite) 管理系統
，藉由以下設定方式可提高端點設備的安全性。

1. Leverage Attack Surface

IT管理者可藉由UMS的profile設定功能，針對不同單位的使用者給予其所 需要的功能，降低使用者誤操作的風險。

2. Disable unneeded potential leaks

IT管理者可針對可能造成資料外流或資料庫被入侵的外接設備做控管。

3. Securing the endpoints security level

使用者透過IGEL OS 再登入公司VDI 網域之前可加一組帳密，通過後，需 再輸入另一組帳密才會真的連進VDI，提供雙重防護。

4. Avoid bad devices

禁止使用沒有被授權的外接設備，例如藍芽，webcam, USB等裝置。 禁止使用任何可hot-plug 的設備。

5. Block unneeded access

關閉SSH連線，預防有心人透過tunnel連線登入代理伺服器。
在VDI 連線下，啟動螢幕保護程式，當使用者暫時離開座位時，可避免被 有心人登入。可禁止使用者使用控制台快捷切換程式進入terminal.

6. Hid unnecessary tools

IT 管理者可在UMS設定關閉或隱藏使用者用不到的設定或功能，降低被攻 擊的風險。

IGEL OS 採用以下方式，確保自身 OS 的安全性:

安全性整合	達到的功能
模組塊分區	每一個端點設備允許預先設定特殊功能的開啟或關閉(例如Citrix Workspace，瀏覽器，ThinPrint等)。特殊資料區以加密方式做進 一步的保護。
自動登出	當session 設定為自動登出且使用者在 session 模式下執行登出， 則端點設備會執行登出指令並做自動登出動作。 結合 Kerberos 技 術，設備在登出後於下次登入時，需重新輸入使用者帳號與密碼 以進行登錄。
預先安裝的安全機制	完整的Kerberos 授權是建構在使用者帳號密碼與雙因子智能卡認 證機制的三方結合。 ● 精簡型電腦 ● Active Directory架構 ● Kerberos 的服務 (例如 Citrix XenApp or XenDesktop)規則與授權可以跨AP 層來做管理服務 。
VNC 安全模式	● 基於各個公司的標準可執行以下的控制: ● Log the shadowing (可記錄端點電腦曾經被執行過的桌面對應) ● Distribute different shadowing permissions (可分配桌面對應的權限) ● Define shadowing groups and security levels (可區分桌面對應群組與設定安全等級) ● Ban VNC sessions between client to client (可禁止端點對端點的桌面對應) ● Allow only the IGEL shadowing or a 3rd party VNC client at the UMS console ● (只允許IGEL預設或掛載於UMS console 上的第三方VNC 程式) ● Ban external/unknown 3rd party VNC clients in the whole network (禁止其他不被認可的第三方VNC連線) ● Encrypted with TLSv1.2 (TLSv1.2 加密)
USB的管理	提供不被入侵的安全保護機制。USB 的設備，包括隨身碟、無線網卡或是印表機， 都有可能成為被竊取資料與散播病毒的媒 介。在USB 設定下，你可以制定規則去阻擋讀取未經授權的USB 設備。 可以使用USB的類別，供應商名稱，產品的ID或設備的UUID來做USB的管控。