



Dominion KX II-101-V2

使用指南
3.5.0 版

Copyright © 2012 Raritan, Inc.

KX2101V2-v3.5.0-D-CHT

2012 年 9 月

255-62-3059-00

本文件包含受版權保護的專利資訊。保留一切權利。若未事先取得力登電腦股份有限公司的書面同意，不得將本文件的任何部分複印、重製或翻譯成另一種語言。

© 版權所有 2012 力登電腦股份有限公司。本文件中提及之所有協力廠商軟體與硬體的註冊商標或商標為各所有人所有。

FCC 資訊

本設備業經測試證明符合 FCC 規則第 15 章的 A 級數位裝置限制。這些限制的設計目的，旨在提供合理的保護，避免在商業環境安裝中產生有害干擾。本設備會產生、使用並放射無線電頻率能量，如不依照指示安裝使用，可能會干擾無線電通訊。在住宅區中操作本設備可能會導致有害干擾。

VCCI 資訊 (日本)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

本產品因意外、災害、誤用、不當使用、產品非經 Raritan 修改，或是 Raritan 責任控制範圍外或非因正常操作條件所引發之其他事件所造成的損害，Raritan 概不負責。

如果本產品隨附一條電源線，其必須專供本產品使用。



機架裝載安全注意事項

對於需要機架固定的 Raritan 產品，請遵循以下預防措施：

- 於密閉機架環境中的操作溫度可能高於室溫。請勿超過設備訂定的週遭環境溫度上限。請參閱〈規格〉。
- 請確保機架環境的空氣流通。
- 在機架中，請小心地安裝設備以避免機械負載不平均。
- 小心地將設備連接至供應電路以避免電路過載。
- 所有設備均應正確接地至分支斷路器，尤其是供電連線，例如電源插座（直接連線除外）。

目錄

簡介	1
KX II-101-V2 概覽	2
KX II-101-V2 說明	3
說明的新增內容.....	4
相關文件	4
產品圖片	5
產品功能.....	5
介面.....	5
網路組態	5
系統管理功能	6
管理功能	6
使用者功能.....	7
電源.....	7
視訊解析度.....	7
裝載.....	7
術語	7
套件內容.....	8
安裝與組態	9
概覽.....	9
預設登入資訊	9
快速入門.....	10
步驟 1：設定目標伺服器.....	10
步驟 2：設定網路防火牆設定.....	21
步驟 3：連接設備.....	22
步驟 4：設定 KX II-101-V2	26
使用目標伺服器	34
介面	34
KX II-101-V2 遠端主控台介面.....	34
多平台用戶端 (MPC).....	43
虛擬 KVM 用戶端 (VKC).....	43
概覽.....	43
連線到 KVM 目標伺服器	43
工具列按鈕與狀態列圖示.....	44
目標伺服器的電源控制.....	45

中斷 KVM 目標伺服器連線.....	46
連線內容	46
連線資訊	48
鍵盤選項	49
視訊內容	54
滑鼠選項	58
VKC 虛擬媒體	62
工具選項	62
檢視選項	66
說明選項	68

虛擬媒體 69

概覽.....	70
使用虛擬媒體的必要條件	72
Windows XP 環境的虛擬媒體	73
Linux 環境的虛擬媒體	74
Mac 環境的虛擬媒體	75
無法使用讀取/寫入的情況	76
使用虛擬媒體	76
連接虛擬媒體	77
本機磁碟機.....	77
裝載 CD-ROM/DVD-ROM/ISO 映像檔.....	78
中斷虛擬媒體的連線.....	79

使用者管理 80

使用者群組	80
使用者群組清單.....	81
使用者與群組之間的關聯性	81
新增使用者群組.....	81
修改現有的使用者群組.....	85
使用者	86
檢視 KX II-101-V2 使用者清單	86
按連接埠檢視使用者	87
與連接埠的使用者中斷連線	87
將使用者登出 KX II-101-V2 (強制登出).....	88
新增使用者.....	88
修改現有使用者.....	89
封鎖和解除封鎖使用者.....	89
驗證設定.....	90
執行 LDAP/LDAPS 遠端驗證	90
從 Active Directory 伺服器傳回使用者群組資訊.....	94
執行 RADIUS 遠端驗證.....	95
透過 RADIUS 傳回使用者群組資訊.....	97

RADIUS 通訊交換規格.....	97
使用者驗證程序.....	99
變更密碼.....	101
裝置管理	102
網路設定.....	102
網路基本設定.....	103
LAN 介面設定.....	106
裝置服務.....	107
啟用 Telnet.....	107
啟用 SSH.....	107
HTTP 與 HTTPS 連接埠設定.....	108
輸入探查連接埠.....	108
透過 URL 啟用直接連接埠存取.....	108
設定 SNMP 代理程式.....	109
鍵盤/滑鼠設定.....	111
序列連接埠設定.....	111
Admin 連接埠.....	112
Raritan 電源插座裝置控制.....	112
數據機.....	112
設定日期/時間設定.....	113
事件管理.....	114
設定事件管理 - 設定.....	114
設定事件管理 - 目的地.....	121
連接埠組態.....	122
管理 KVM 目標伺服器 (連接埠頁面).....	123
電源控制.....	125
類比 KVM 切換器.....	130
使用「Reset」(重設) 按鈕重設 KX II-101-V2.....	131
變更預設的 GUI 語言設定.....	132
管理 USB 連線	133
概覽.....	133
USB 連線設定.....	134
進階 USB 連線設定.....	135
安全性管理	137
安全性設定.....	137
登入限制.....	137
強固密碼.....	139
封鎖使用者.....	140

目錄

加密與共用	142
啟用 FIPS 140-2	145
設定 IP 存取控制	146
SSL 憑證	149
安全性標題	151

維護 153

稽核記錄	153
裝置資訊	154
Backup and Restore (備份與還原)	155
升級韌體	157
升級歷程記錄	158
出廠重設	158
將 KX II-101-V2 重新開機	159
停止 CC-SG 管理	160

診斷 162

網路介面頁面	162
Network Statistics (網路統計資料) 頁面	163
偵測 (Ping) 主機頁面	165
Trace Route to Host (追蹤主機路由) 頁面	165
裝置診斷	167

指令行介面 (CLI) 169

概覽	169
使用 CLI 存取 KX II-101-V2	170
KX II-101-V2 的 SSH 連線	170
Windows 電腦的 SSH 存取方法	170
UNIX/Linux 工作站的 SSH 存取方法	171
登入	171
瀏覽 CLI	171
CLI 提示	171
自動完成指令	172
CLI 語法 - 祕訣與快速鍵	172
所有指令行介面層級的常見指令	172
CLI 指令	173
診斷	174
組態	175
Listports 指令	177
Userlist 指令	177

CC-SG 管理	178
概覽.....	178
從 CC-SG 移除對 KX II-101-V2 的管理.....	179
在 Proxy 模式下使用 CC-SG.....	180
規格	181
實物規格.....	181
支援的作業系統 (用戶端).....	182
支援的瀏覽器.....	183
接頭.....	184
經過認證的數據機.....	184
支援的視訊解析度.....	184
支援的鍵盤語言.....	185
使用的 TCP 及 UDP 連接埠.....	186
Network Speed Settings.....	Error! Bookmark not defined.
9 針腳.....	189
更新 LDAP 架構	190
傳回使用者群組資訊.....	190
從 LDAP.....	190
從 Microsoft Active Directory.....	190
設定登錄允許對架構進行寫入作業.....	191
建立新屬性.....	191
新增類別的屬性.....	193
更新結構描述快取.....	194
編輯使用者成員的 rciusergroup 屬性.....	194
安裝機架	198
裝上 L 型托架水平裝載 KX II-101-V2.....	198
重要注意事項：	200
Java Runtime Environment (JRE).....	200
IPv6 支援注意事項.....	201
作業系統 IPv6 支援注意事項.....	201
鍵盤、視訊以及滑鼠注意事項.....	201
Sun Blade 視訊、鍵盤及滑鼠支援限制.....	201
從本機鍵盤存取 BIOS 的限制.....	202
HP UX RX 1600 鍵盤與滑鼠組態.....	203

目錄

Compaq Alpha 與 IBM P 伺服器滑鼠模式限制	203
Windows 2000 與 Windows 2003 Server 鍵盤限制	203
CC-SG	203
Proxy 模式與 MPC	203

常見問題集 **204**

一般常見問題集	204
IPv6 網路功能	205

索引 **207**

Ch 1

簡介

本章內容

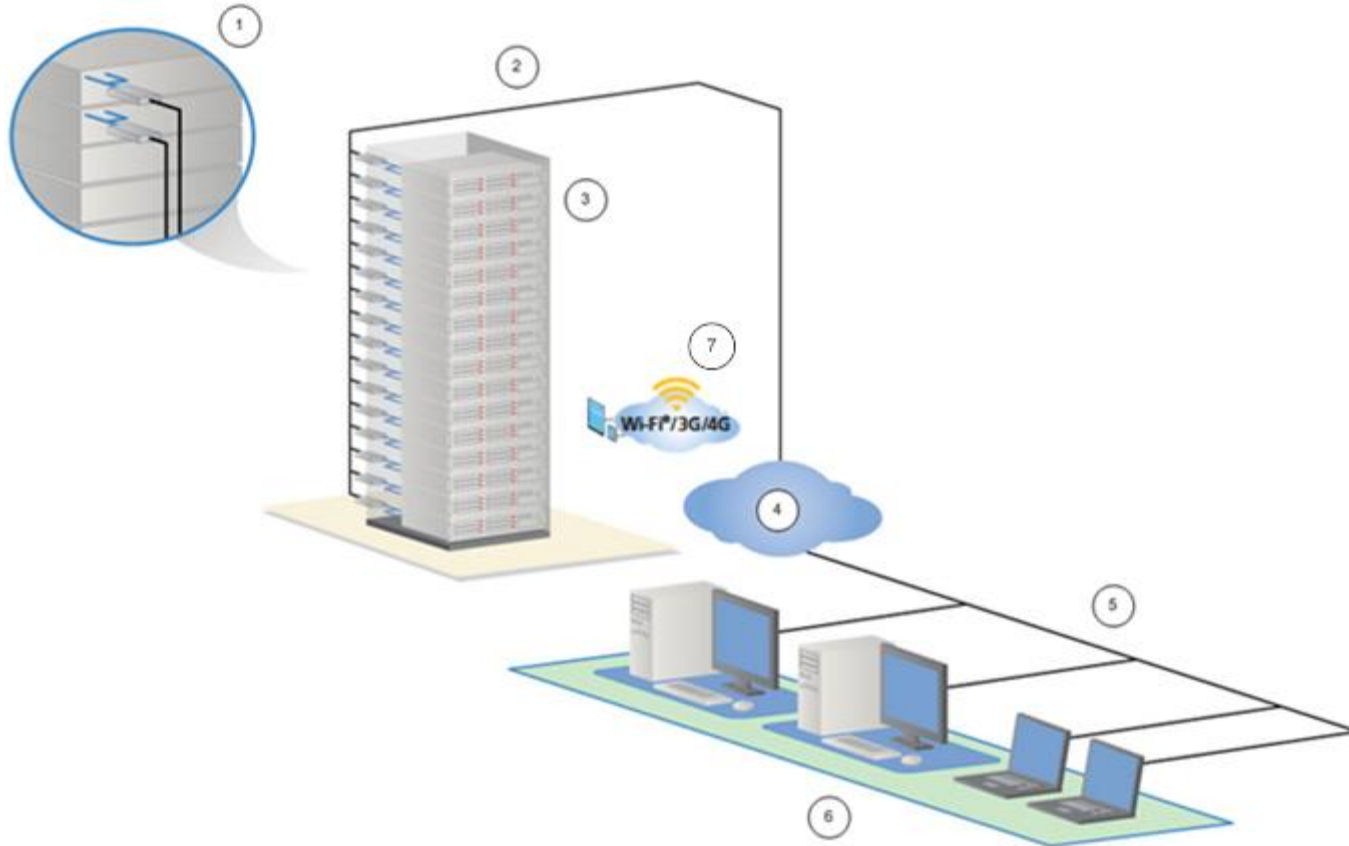
KX II-101-V2 概覽	2
KX II-101-V2 說明	3
產品圖片	5
產品功能	5
術語.....	7
套件內容	8

KX II-101-V2 概覽

感謝您購買 Dominion KX II-101-V2。KX II-101-V2 提供一個鍵盤、視訊以及滑鼠 (KVM) 連接埠，可供連接到目標伺服器，還有一個 IP 連接埠可供連接到 IP 網路。在 KX II-101-V2 裝置內部會將來自伺服器的 KVM 訊號轉換成 IP 格式，然後加以壓縮以供在 IP 網路上傳輸。

KX II-101-V2 硬體鎖的外型尺寸容易安裝在目標伺服器附近，而且每部個別的 KX II-101-V2 裝置都有自己的 IP 位址。每部裝置均是透過外部電源模組來提供電源。

KX II-101-V2 可以如同獨立的設備般運作，或可連同其他 Raritan 存取產品，運用 Raritan CommandCenter Secure Gateway (CC-SG) 5.4 (或更新版本) 管理裝置，整合為單一邏輯解決方案。



圖解	
1	KX II-101-V2
2	LAN
3	Windows®、Linux® 及 Sun™ 伺服器
4	TCP/IP
5	LAN
6	遠端 (網路) 存取
7	使用 CC-SG 透過 iPhone® 與 iPad® 行動裝置存取

KX II-101-V2 說明

KX II-101-V2 說明提供如何安裝、設置和設定 KX II-101-V2。其中還包括存取目標伺服器、使用虛擬媒體、管理使用者與安全性以及維護和診斷 KX II-101-V2 的資訊。

在開始使用 KX II-101-V2 裝置之前，如需目前版本注意事項的重要資訊，請參閱 KX II-101-V2 版本注意事項。

您可以從力登網站的**韌體與文件**頁面下載 PDF 版說明。建議您參閱力登網站以取得最新的使用指南。

若要使用線上說明，則必須在瀏覽器中啟用「主動式內容」。如果使用 Internet Explorer 7，您必須啟用 **Scriptlets**。請參閱瀏覽器說明，瞭解啟用這些功能的相關資訊。

說明的新增內容

下列已根據強化功能以及設備與/或使用者的變更而增添資訊。

- 支援 FIPS 140-2 加密功能
- 支援登入安全性標題
- 從 iPad® 與 iPhone® 行動裝置存取與受 CC-SG 管理的 KX II-101-V2 連線的伺服器
- SNMPv3 支援
- 能夠將您自己的 SSL 憑證上載到 KX II-101-V2
- 支援 1920x1080 & 寬螢幕視訊解析度
- 可設定 TCP/IP 連接埠編號 (隱形模式)
- 可在受 CC-SG 5.4 或更新版本管理時直接存取 KX II-101-V2
- Linux® 與 Mac® 支援虛擬媒體
- 支援日文、繁體中文及簡體中文使用者介面
- 支援 IPv4 與 IPv6 的雙重堆疊環境
- 與連接埠的使用者中斷連線
- 強制使用者登出
- 更新 KX II-101-V2 中的 SNMP 設陷與 SNMP 代理程式使用者介面

如需設備與本版說明適用之變更的詳細說明，請參閱「KX II-101-V2 版本注意事項」。

相關文件

KX II-101-V2 說明隨附的《KX II-101-V2 快速安裝指南》可以在**力登網站** (<http://www.raritan.com/support/firmware-and-documentation>)的**韌體與文件**頁面上找到。

如需用戶端應用程式與 KX II-101-V2 裝置搭配使用的安裝需求與指示，可以在《**KVM 與序列存取用戶端指南**》以及力登網站上找到。適用時，本說明還包含與 KX II-101-V2 裝置搭配使用的特定用戶端功能。

產品圖片



KX II-101-V2

產品功能

介面

- 整合式 PS/2 KVM 連線
- 可取得控制與虛擬媒體的 USB 連線
- 可供初始裝置組態與診斷使用的序列管理 (Admin) 連接埠，還可以搭配使用外部連接埠存取與 Raritan 電源插座裝置控制
- 監視器連線的本機連接埠
- 可支援 10/100-base-T 自動感應、全雙工的乙太網路 LAN 連接埠

網路組態

- DHCP 或 靜態 IP 裝置位址

系統管理功能

- 韌體可透過乙太網路升級
- 故障安全韌體升級功能
- 可以手動設定或利用網路時間通訊協定 (NTP/SNTP) 同步的時鐘
- 管理員可以停用有本機時間戳記的管理員活動記錄 SNMP V2 代理程式
- 支援 RADIUS 與 LDAP/LDAPS 驗證通訊協定

管理功能

- 網頁型管理
- LDAP、Active Directory®、RADIUS 或內部驗證與授權
- DHCP 或固定的 IP 定址
- 與 Raritan CommandCenter Secure Gateway (CC-SG) 管理應用裝置相整合
- 從 iPad® 與 iPhone® 行動裝置存取伺服器 (其連線到受 CC-SG 管理的 KX II-101-V2)
- 支援 FIPS 140-2
- 支援登入安全性標題
- SNMPv3 支援
- 能夠將您自己的 SSL 憑證上載到 KX II-101-V2
- 可設定 TCP/IP 連接埠編號 (隱形模式)
- 支援 IPv4 與 IPv6 的雙重堆疊環境
- 與連接埠的使用者中斷連線
- 強制使用者登出

使用者功能

- 透過一般瀏覽器以網頁存取
- 直覺式圖形化使用者介面 (GUI)
- 電腦共用模式，可讓多位遠端使用者連線到目標
- TCP 通訊
- 支援英文、日文、繁體中文及簡體中文使用者介面與說明
- 虛擬媒體存取
- Absolute Mouse Synchronization™ (滑鼠絕對同步)
- 隨插即用
- KVM 訊號完全以 256 位元加密，包括視訊及虛擬媒體

電源

- 透過外部 AC-DC 變壓器提供電源

視訊解析度

- 最高可達 1920x1080 (最高 60 Hz) 與寬螢幕視訊解析度

裝載

- 機架安裝托架

術語

專有名詞	說明
目標伺服器	要透過 KX II-101-V2 與其連接的 KVM 組態存取的伺服器。
遠端電腦	Windows®、Linux® 或 Apple Macintosh® 電腦，用以存取和控制連接到 KX II-101-V2 的目標伺服器。
管理 (Admin) 序列連接埠	使用管理 (Admin) 序列連接埠將 DB9 纜線公接頭連接到電腦的序列連接埠。然後使用標準的模擬軟體套件 (例如 HyperTerminal)，存取管理 (Admin) 序列連接埠，而管理序列連接埠是用於網路組態。
本機使用者 (Local User) 連接埠	其可讓使用者不需要拔除 KX II-101-V2，臨機使用目標伺服器原本的監視器。
虛擬媒體	可讓 KVM 目標伺服器從遠端存取用戶端電腦與網路檔案伺服器的媒體。

套件內容

每部 KX II-101-V2 裝置出貨時均附有：

- KX II-101-V2 - KVM over IP
- KVM 纜線
- 變壓器 - 附通用轉接頭的 AC/DC 5VDC
- 安裝托架組
- 印刷版快速安裝指南
- 印刷版應用程式版本注意事項 (適用的話)
- 印刷版技術注意事項 (適用的話)

本章內容

概覽.....	9
預設登入資訊.....	9
快速入門.....	10

概覽

本章說明如何安裝和設定 KX II-101-V2。安裝與設定步驟如下：

- **步驟 1：設定目標伺服器** (p. 10)
- **步驟 2：設定網路防火牆設定** (p. 21)
- **步驟 3：連接設備** (p. 22)
- **步驟 4：設定 KX II-101-V2** (p. 26)

為了確保能有最佳效能，請在安裝 KX II-101-V2 之前，設定您想要透過 >ProductName< 存取的目標伺服器。請注意，下列組態需求僅適用於目標伺服器，而您要用以從遠端存取 KX II-101-V2 的電腦則不適用。

預設登入資訊

預設	值
使用者名稱	預設使用者名稱是 admin 。此一使用者具有管理權限。
密碼	預設的密碼為 raritan 。 密碼須區分大小寫，且輸入的大小寫組合必須與建立時完全相同。例如，預設密碼 raritan 必須全以小寫字母輸入。 第一次啟動 KX II-101-V2 裝置時，系統會要求您變更預設密碼。
IP 位址	KX II-101-V2 裝置出貨時附有預設的 IP 位址 192.168.0.192。
重要： 基於備份與延續商業營運目的，強烈建議您建立管理員使用者名稱與密碼備份，並妥善收存此資訊。	

快速入門

使用 Microsoft® Internet Explorer® 6 版或 Windows 2000® 的 KX II-101-V2 使用者必須升級至 Service Pack 4 (SP4) 或以上的版本。

KX II-101-V2 出貨時附有預設的靜態 IP 位址。在沒有 DHCP 伺服器的網路上，您必須使用 KX II-101-V2 序列管理主控台或 KX II-101-V2 遠端主控台，設定新的靜態 IP 位址、網路遮罩以及閘道位址。

如需使用遠端主控台對 KX II-101-V2 指派 IP 位址的詳細資訊，請參閱 <指派 IP 位址> (請參閱 "指派 IP 位址" p. 27)。如需使用序列管理主控台設定 IP 位址的詳細資訊，請參閱 <設定 KX II-101-V2 使用終端機模擬程式 (選用)> (請參閱 "設定 KX II-101-V2 使用終端機模擬程式 (選用)" p. 31)。

步驟 1：設定目標伺服器

安裝 KX II-101-V2 之前，請先設定您想要透過 >ProductName< 存取的目標伺服器，以確保能有最佳效能。請注意，下列組態需求僅適用於目標伺服器，而您要用以從遠端存取 KX II-101-V2 的電腦則不適用。

設定伺服器視訊解析度

如要獲得最佳的頻寬效率與視訊效能，像是 Windows®、X-Windows®、Solaris™ 以及 KDE 等執行圖形化使用者介面的目標伺服器，應將桌面背景設為以單色、淺明的簡單圖形為主。避免使用相片或有複雜漸層的背景。

確認 KX II-101-V2 能支援伺服器的視訊解析度與螢幕更新頻率，同時訊號為非交錯式。KX II-101-V2 支援以下解析度：

解析度	
640x350 @70Hz	1024x768@85
640x350 @85Hz	1024x768 @ 75Hz
640x400 @56Hz	1024x768 @ 90Hz
640x400 @84Hz	1024x768 @ 100Hz
640x400 @85Hz	1152x864 @ 60Hz
640x480 @ 60Hz	1152x864 @ 70Hz
640x480 @ 66.6Hz	1152x864 @ 75Hz
640x480 @ 72Hz	1152x864 @ 85Hz
640x480 @ 75Hz	1152x870 @75.1Hz

解析度	
640x480 @ 85Hz	1152x900 @66Hz
720x400 @70Hz	1152x900 @76Hz
720x400 @84Hz	1280x720@60Hz
720x400 @85Hz	1280x960 @60Hz
800x600 @ 56Hz	1280x960 @85Hz
800x600 @ 60Hz	1280x1024 @ 60Hz
800x600 @ 70Hz	1280x1024 @ 75Hz
800x600 @ 72Hz	1280x1024 @ 85Hz
800x600 @ 75Hz	1360x768@60Hz
800x600 @ 85Hz	1366x768@60Hz
800x600 @ 90Hz	1368x768@60Hz
800x600 @ 100Hz	1400x1050@60Hz
832x624 @75.1Hz	1440x900@60Hz
1024x768 @ 60Hz	1600x1200 @ 60Hz
1024x768@70	1680x1050@60Hz
1024x768@72	1920x1080@60Hz

Sun 視訊解析度

Sun™ 系統有兩種解析度設定，分別為指令行解析度與 GUI 解析度。如需 KX II-101-V2 所支援解析度的詳細資訊，請參閱 [〈設定伺服器視訊解析度〉](#) (請參閱 "設定伺服器視訊解析度" p. 10)。

附註：如果所有支援的解析度均沒有作用，請確定使用的是多重同步監視器。有些監視器無法處理水平與垂直 (H&V) 同步訊號。

指令行解析度

▶ 若要檢查指令行解析度：

1. 以 root 的身分執行下列指令：`# eeprom output-device`

▶ 若要變更指令行解析度：

1. 執行下列指令：`# eeprom output-device=screen:r1024x768x75`，其中 `1024x768x75` 可以是 KX II-101-V2 支援的任一解析度。
2. 重新啟動電腦。

GUI 解析度/32 位元

▶ 若要檢查 32 位元卡的 GUI 解析度：

1. 執行下列指令：`# /usr/sbin/pgxconfig -prconf`

▶ 若要變更 32 位元卡的 GUI 解析度：

1. 執行下列指令：`# /usr/sbin/pgxconfig -res1024x768x75`，其中 `1024x768x75` 可以是 KX II-101-V2 支援的任一解析度。
2. 重新啟動電腦。

GUI 解析度/64 位元

▶ 若要檢查 64 位元卡的 GUI 解析度：

1. 執行下列指令：`# /usr/sbin/m64config -prconf`

▶ 若要變更 64 位元卡的解析度：

1. 執行下列指令：`# /usr/sbin/m64config -res1024x768x75` where `1024x768x75` 可以是 KX II-101-V2 支援的任一解析度。
2. 重新啟動電腦。

GUI 解析度/Solaris 8

▶ 若要檢查 Solaris™ 8 上 32 位元與 64 位元卡的 GUI 解析度：

1. 執行下列指令：`# /usr/sbin/fbconfig -prconf`

▶ 若要變更 Solaris 8 上 32 位元與 64 位元卡的 GUI 解析度：

1. 執行下列指令：`# /usr/sbin/fbconfig -res1024x768x75` where `1024x768x75` 可以是 KX II-101-V2 支援的任一解析度。
2. 重新啟動電腦。

滑鼠設定

KX II-101-V2 可在數種滑鼠模式下操作：Absolute Mouse Synchronization™ (絕對滑鼠同步)、智慧滑鼠模式及標準滑鼠模式。

附註：使用智慧滑鼠模式時，請勿使用動畫滑鼠。

Absolute Mouse Synchronization (滑鼠絕對同步) 模式的滑鼠參數可以保持不變。對於標準與智慧滑鼠模式，則必須設定特定的滑鼠參數值，其會在本節加以說明。

不同的目標作業系統會有不同的滑鼠組態。如需其他詳細資料，請參閱作業系統文件。

Windows XP、Windows 2003 及 Windows 2008 設定

▶ 若要設定執行 Microsoft® Windows XP® 作業系統、Windows 2003® 作業系統或 Windows 2008® 作業系統的 KVM 目標伺服器：

1. 設定滑鼠設定：
 - a. 選擇「開始」>「控制台」>「滑鼠」。
 - b. 按一下「指標設定」索引標籤。
 - c. 在「速度」群組中：
 - 將滑鼠移動速度設定在剛好中間速度的位置。
 - 停用「增強指標的準確性」選項。
 - 停用「指到」選項。
 - 按一下「確定」。

附註：在目標伺服器執行 Windows 2003 時，如果透過 KVM 存取該伺服器，而且執行下列任一種一次性動作，先前啟用的滑鼠同步化效果就會失去作用。您必須在用戶端從「滑鼠」功能表選取「同步化滑鼠」指令，才能再次啟用。以下是可能會導致這種情況發生的動作：

- 開啟文字編輯器。
 - 從 Windows 控制台存取「滑鼠」內容、「鍵盤」內容、以及「電話和數據機選項」。
-

2. 停用轉移特效：
 - a. 從「控制台」選取「顯示」選項。
 - b. 按一下「外觀」索引標籤。
 - c. 按一下「效果」。
 - d. 取消選取「在功能表及工具列提示上使用以下切換效果」選項。

- e. 按一下「確定」。
3. 關閉「控制台」。

附註：對於執行 Windows XP、Windows 2000 或 Windows 2008 的 KVM 目標伺服器，您可能希望建立一個使用者名稱，僅供透過 KX II-101-V2 從遠端連線時使用。這可讓您為 KX II-101-V2 連線保留目標伺服器的慢速滑鼠指標速度/加速設定。

Windows XP、2000 及 2008 登入畫面會還原為預先設定的滑鼠參數，而這些與最佳 KX II-101-V2 效能的建議參數不同。結果是這些畫面可能無法達到最佳的滑鼠同步效果。

附註：只有當您瞭解如何調整 Windows KVM 目標伺服器的登錄時才可繼續。您可以使用 Windows 登錄編輯程式來變更下列設定，讓登入畫面能有更好的 KX II-101-V2 滑鼠同步效果：`HKey_USERS\DEFAULT\Control Panel\Mouse: > MouseSpeed = 0; MouseThreshold 1=0; MouseThreshold 2=0`。

Windows 7 與 Windows Vista 設定

▶ 若要設定執行 Windows Vista® 作業系統的 KVM 目標伺服器：

1. 設定滑鼠設定：
 - a. 選擇「開始」>「設定」>「控制台」>「滑鼠」。
 - b. 從左瀏覽面板選取「進階系統設定」。隨即會開啟「系統內容」對話方塊。
 - c. 按一下「指標設定」索引標籤。
 - d. 在「速度」群組中：
 - 將滑鼠移動速度設定在剛好中間速度的位置。
 - 停用「增強指標的準確性」選項。
 - 按一下「確定」。
2. 停用動畫與淡化效果：
 - a. 從「控制台」選取「系統」選項。
 - b. 選取「效能資訊」，再選取「工具」>「進階工具」>「調整為」，以調整 Windows 的外觀與效能。
 - c. 按一下「進階」索引標籤。
 - d. 在「效能」群組中，按一下「設定」，便會開啟「效能選項」對話方塊。
 - e. 取消選取「自訂」選項下方的以下核取方塊：

- 動畫選項：
 - 視窗內部的動畫控制項和元素
 - 將視窗最大化或最小化時顯示視窗動畫
 - 淡化選項：
 - 將功能表淡出或滑動到檢視
 - 工具提示逐漸消失或滑動到檢視
 - 按下功能表項目後逐漸消失
3. 按一下「確定」並關閉「控制台」。

▶ 若要設定執行 **Windows 7®** 作業系統的 **KVM** 目標伺服器：

1. 設定滑鼠設定：
 - a. 選擇「Start」(開始) > 「Control Panel」(控制台) > 「Hardware and Sound」(硬體和音效) > 「Mouse」(滑鼠)。
 - b. 按一下「Pointer Options」(指標設定) 索引標籤。
 - c. 在「Motion」(速度) 群組中：
 - 將滑鼠移動速度設定在剛好中間速度的位置。
 - 停用「Enhanced pointer precision」(增強指標的準確性) 選項。
 - 按一下「OK」(確定)。
2. 停用動畫與淡化特效：
 - a. 選取「Control Panel」(控制台) > 「System and Security」(系統及安全性)。
 - b. 選取「System」(系統)，然後從左導覽面板中選取「Advanced system settings」(進階系統設定)。隨即會顯示「System Properties」(系統內容) 對話方塊。
 - c. 按一下「Advanced」(進階) 索引標籤。
 - d. 按一下「Performance」(效能) 群組的「Settings」(設定) 按鈕，以開啟「Performance Options」(效能選項) 對話方塊。
 - e. 取消選取「Custom」(自訂) 選項下的以下核取方塊：
 - 動畫選項：
 - 視窗內部的動畫控制項和元素
 - 將視窗最大化或最小化時顯示視窗動畫
 - 淡化選項：

- 將功能表淡出或滑動到檢視
 - 工具提示逐漸消失或滑動到檢視
 - 按下功能表項目後逐漸消失
3. 按一下「OK」(確定)，即可關閉「Control Panel」(控制台)。

Windows 2000 設定

▶ 若要設定執行 Microsoft® Windows 2000® 作業系統的 KVM 目標伺服器：

1. 設定滑鼠設定：
 - a. 選擇「Start」(開始) > 「Control Panel」(控制台) > 「Mouse」(滑鼠)。
 - b. 按一下「Motion」(速度) 索引標籤。
 - 將加速設定為「None」(無)。
 - 將滑鼠移動速度設定在剛好中間速度的位置。
 - 按一下「OK」(確定)。
2. 停用轉移特效：
 - a. 從「Control Panel」(控制台) 選取「Display」(顯示) 選項。
 - b. 按一下「Effects」(效果) 索引標籤。
 - 取消選取「Use the following transition effect for menus and tooltips」(在功能表及工具列提示上使用以下轉移特效) 選項。
3. 按一下「OK」(確定)，即可關閉「Control Panel」(控制台)。

附註：對於執行 Windows XP、Windows 2000 或 Windows 2008 的 KVM 目標伺服器，您可能希望建立一個使用者名稱，僅供透過 KX II-101-V2 從遠端連線時使用。這可讓您為 KX II-101-V2 連線保留目標伺服器的慢速滑鼠指標速度/加速設定。

Windows XP、2000 及 2008 登入畫面會還原為預先設定的滑鼠參數，而這些與最佳 KX II-101-V2 效能的建議參數不同。結果是這些畫面可能無法達到最佳的滑鼠同步效果。

附註：只有當您瞭解如何調整 Windows KVM 目標伺服器的登錄時才可繼續。您可以使用 Windows 登錄編輯程式來變更下列設定，讓登入畫面能有更好的 KX II-101-V2 滑鼠同步效果：`HKey_USERS\DEFAULT\Control Panel\Mouse: > MouseSpeed = 0; MouseThreshold 1=0; MouseThreshold 2=0`。

Linux 設定 (Red Hat 4 與 5 以及 Fedora 14)

附註：下列設定只有在用於「標準滑鼠」模式時效果最佳。

▶ 若要設定執行 Linux® (圖形化使用者介面) 的 KVM 目標伺服器：

1. 設定滑鼠設定：
 - a. 選擇「Main Menu」(主功能表) > 「Preferences」(喜好設定) > 「Mouse」(滑鼠)。隨即會出現「Mouse Preferences」(滑鼠喜好設定) 對話方塊。
 - b. 按一下「Motion」(速度) 索引標籤。
 - c. 在「Speed」(速度) 群組內，將「Acceleration」(加速) 滑桿設定在剛好中間的位置。
 - d. 在「Speed」(速度) 群組內，將「Sensitivity」(敏感度) 設定為低。
 - e. 在「Drag & Drop」(拖放) 群組內，將「Threshold」(臨界值) 設定為小。
 - f. 關閉「Mouse Preferences」(滑鼠喜好設定) 對話方塊。

附註：如果這些步驟均無作用，請依照 Linux 指令行指示中的描述，發出 `xset mouse 1 1` 指令。

2. 設定螢幕解析度：
 - a. 選擇「Main Menu」(主功能表) > 「System Settings」(系統設定) > 「Display」(顯示)。隨即會出現「Display Settings」(顯示設定) 對話方塊。
 - b. 從「Display」(顯示) 索引標籤選取 KX II-101-V2 支援的「Resolution」(解析度)。
 - c. 從「Advanced」(進階) 索引標籤確認 KX II-101-V2 可支援該「Refresh Rate」(螢幕更新頻率)。

附註：與目標伺服器連線之後，`<Ctrl> <Alt> <+>` 指令在許多 Linux 圖形化環境下會變更視訊解析度，讓您在 XF86Config 或 `/etc/X11/xorg.conf` (視 X 伺服器的發佈而定) 中捲動瀏覽所有仍為啟用狀態的可用解析度。

▶ 若要設定執行 Linux (指令行) 的 KVM 目標伺服器：

1. 將滑鼠加速度值設為 1，並將臨界值也同時設為 1。輸入此指令：`xset mouse 1 1`。如此應會設為於登入時執行。
2. 請確定每部執行 Linux 的目標伺服器所使用的解析度，皆是 KX II-101-V2 所支援的標準 VESA 解析度及螢幕更新頻率。
3. 另請設定每部 Linux 目標伺服器，使閃爍次數在 VESA 標準值的 +/- 40% 範圍內：

- a. 找到 Xfree86 組態檔 XF86Config。
- b. 使用文字編輯器，停用 KX II-101-V2 不支援的所有解析度。
- c. 停用虛擬桌面功能 (KX II-101-V2 並不支援)。
- d. 檢查遮沒時間 (在 VESA 標準的 +/- 40% 範圍內)。
- e. 重新啟動電腦。

附註：如果變更視訊解析度，您必須登出目標伺服器，然後再次登入，視訊設定才會生效。

Red Hat 與 Fedora KVM 目標伺服器的注意事項

若使用 USB CIM 在目標伺服器上執行 Red Hat®，而產生鍵盤及/或滑鼠方面的問題，您可以嘗試其他組態設定。

祕訣：即使是剛完成作業系統安裝，您也必須執行這些步驟。

▶ 若要使用 USB CIM 設定 Red Hat 伺服器：

1. 找出系統中的組態檔 (通常為 /etc/modules.conf)。
2. 使用您所選擇的編輯器，確定 modules.conf 檔案中的 alias usb-controller 一行如下所示：

```
alias usb-controller usb-uhci
```

附註：若在 /etc/modules.conf 檔案中有其他行使用 usb-uhci，則必須加以移除或將其標為註釋。

3. 儲存檔案。
4. 將系統重新開機，以使變更改生效。

Linux 設定 (適用於標準滑鼠模式)

附註：下列設定只有在用於「標準滑鼠」模式時效果最佳。

▶ 若要設定執行 Linux® (圖形化使用者介面) 的 KVM 目標伺服器：

1. 設定滑鼠設定：
 - a. Red Hat 5 使用者請選擇「Main Menu」(主要功能表) > 「Preferences」(喜好設定) > 「Mouse」(滑鼠)。Red Hat 4 使用者請選擇「System」(系統) > 「Preferences」(喜好設定) > 「Mouse」(滑鼠)。隨即會出現「Mouse Preferences」(滑鼠喜好設定) 對話方塊。
 - b. 按一下「Motion」(速度) 索引標籤。

- c. 在「Speed」(速度) 群組內，將「Acceleration」(加速) 滑桿設定在剛好中間的位置。
- d. 在「Speed」(速度) 群組內，將「Sensitivity」(敏感度) 設定為低。
- e. 在「Drag & Drop」(拖放) 群組內，將「Threshold」(臨界值) 設定為小。
- f. 關閉「Mouse Preferences」(滑鼠喜好設定) 對話方塊。

附註：如果這些步驟均無作用，請依照 *Linux* 指令行指示中的描述，發出 `xset mouse 1 1` 指令。

2. 設定螢幕解析度：

- a. 選擇「Main Menu」(主功能表) > 「System Settings」(系統設定) > 「Display」(顯示)。隨即會出現「Display Settings」(顯示設定) 對話方塊。
- b. 在「Settings」(設定) 索引標籤上，選取 KX II-101-V2 支援的「Resolution」(解析度)。
- c. 按一下「OK」(確定)。

附註：與目標伺服器連線之後，<Ctrl> <Alt> <+> 指令在許多 *Linux* 圖形化環境下會變更視訊解析度，讓您在 *XF86Config* 或 */etc/X11/xorg.conf* (視 X 伺服器的發佈而定) 中捲動瀏覽所有仍為啟用狀態的可用解析度。

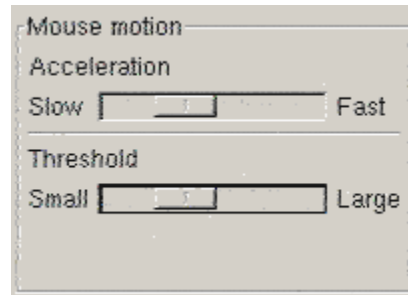
附註：如果變更視訊解析度，您必須登出目標伺服器，然後再次登入，視訊設定才會生效。

Sun Solaris 設定

Solaris™ 目標伺服器必須設定為 KX II-101-V2 支援的其中一種解析度。Sun™ 電腦最普遍支援的解析度包括：

解析度
1024x768@60Hz
1024x768@70Hz
1024x768@75Hz
1024x768@85Hz
1280x1024@60Hz

將滑鼠加速值與臨界值同時設為 1。執行 Solaris 作業系統的目標伺服器必須輸出 VGA 視訊 (水平同步與垂直同步訊號，而不是複合同步訊號)。請在圖形使用者介面進行此項設定，或使用指令行 `xset mouse a t`，此處的 `a` 為加速，而 `t` 為臨界值。



► 將 Sun 視訊卡輸出從複合式同步訊號變更為非預設的 VGA 輸出：

1. 發出 `Stop+A` 指令進入 `bootprom` 模式。
2. 發出 `#EEPROM output-device=screen:r1024x768x75` 指令變更輸出解析度。
3. 發出 `boot` 指令，將伺服器重新開機。

或者也可以聯絡 Raritan 業務代表，購買視訊輸出介面卡。若要搭配 KX II-101-V2 使用，採用複合同步輸出的 Sun 需要使用 APSSUN II Raritan Guardian 轉換器。若要搭配 KX II-101-V2 使用，採用分離同步輸出的 HD15 Sun 需要使用 APKMSUN Raritan Guardian 轉換器。

Apple Macintosh 設定

KX II-101-V2 拆封後即可和 Mac® 一起使用。不過，您必須使用「Absolute Mouse Synchronization」(滑鼠絕對同步)，以及在「KX II-101-V2 Port」(KX II-101-V2 連接埠) 頁面上，啟用「Absolute Mouse」(絕對滑鼠) 模式並為 Mac 伺服器調整滑鼠。

► 若要啟用此設定：

1. 選擇「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態)。隨即會開啟「Port Configuration」(連接埠組態) 頁面。
2. 對要編輯的連接埠，按一下「Port Name」(連接埠名稱)。
3. 在「USB Connection Settings」(USB 連線設定) 區段中，選取「Enable Absolute Mouse」(啟用絕對滑鼠) 與「Enable Absolute mouse scaling for MAC server」(啟用 Mac 伺服器的絕對滑鼠調整功能) 核取方塊。按一下「OK」(確定)。

請參閱 <連接埠組態> (請參閱 "連接埠組態" p. 122)。

IBM AIX 設定

1. 進入「Style Manager」(樣式管理員)。
2. 按一下「Mouse Settings」(滑鼠設定)，然後將「Mouse acceleration」(滑鼠加速) 設為 1.0，同時將「Threshold」(臨界值) 設為 3.0。

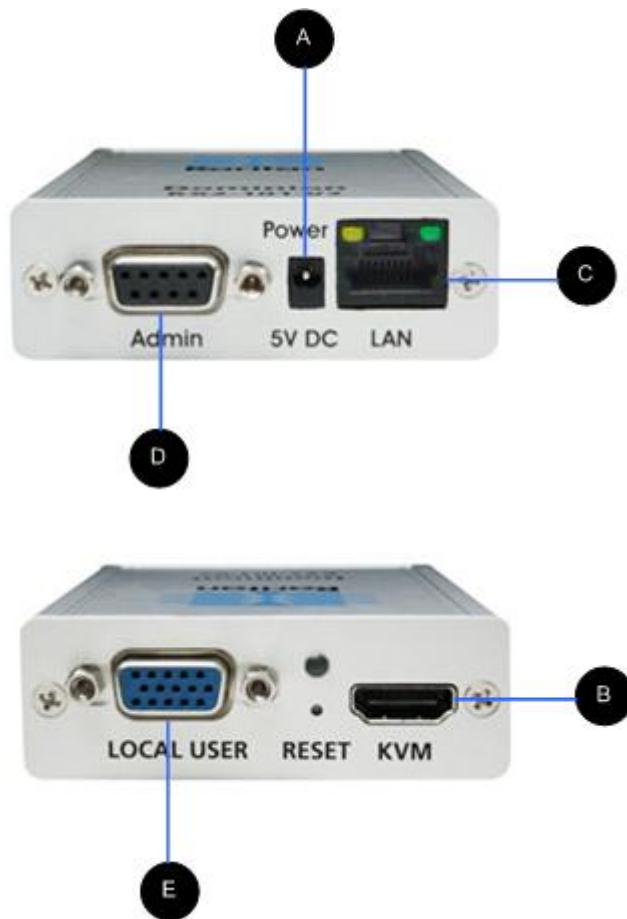
步驟 2：設定網路防火牆設定

若要透過網路防火牆存取 KX II-101-V2，您的防火牆必須允許 TCP 連接埠 5000 的通訊。或者，亦可設定 KX II-101-V2 使用您自行指定的另一個 TCP 連接埠。

若要運用 KX II-101-V2 的網頁瀏覽器存取功能，防火牆必須允許 TCP 連接埠 443 (HTTPS 通訊的標準 TCP 連接埠) 上的入埠通訊。若要利用 KX II-101-V2 將 HTTP 要求重新導向到 HTTPS 的功能 (因此使用者可以輸入常用的 `http://xxx.xxx.xxx.xxx` 而不必輸入 `https://xxx.xxx.xxx.xxx`)，此防火牆必須也允許 TCP 連接埠 80 (HTTP 通訊的標準 TCP 連接埠) 的入埠通訊。

步驟 3：連接設備

圖中說明 KX II-101-V2 的實體連線：圖示中的每個字母分別對應到此處所述設備連接程序的步驟。



圖解		
A	電源接頭	一個變壓器。
B	KVM 纜線搭配監視器、PS/2 及 USB 接頭 (附件)	將提供的 KVM 纜線連接到目標伺服器的鍵盤、視訊及滑鼠連接埠
C	乙太網路 LAN	提供 LAN 連線。

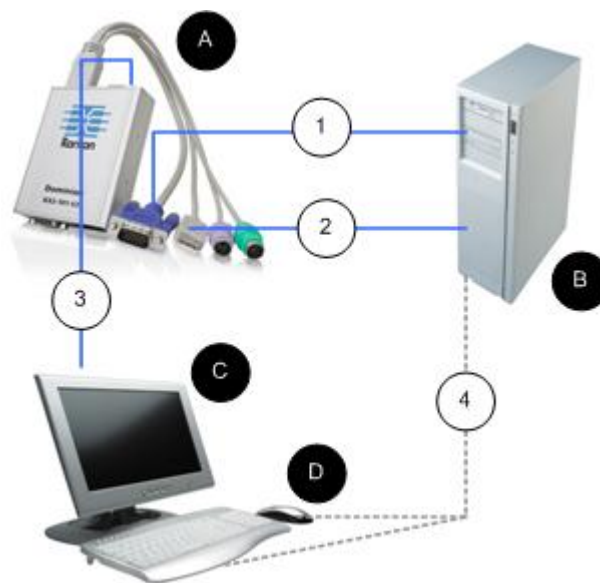
圖解		
D	管理 (Admin) 連接埠	用以執行下列其中一項動作： <ul style="list-style-type: none"> • 利用電腦上的終端機模擬程式來設定和管理裝置。 • 設定和管理電源插座裝置 (需要轉接頭，未隨附)。 • 連接外接式數據機以撥入裝置。
E	本機使用者 (Local User)	本機連接埠可連接至監視器。

A：電源

KX II-101-V2 是透過裝置隨附的電源變壓器 (100-240V AC 輸入與 5VDC 輸出) 提供電源。如需標準 AC 電源，請將隨附的 AC 電源變壓器插入電源插孔，然後將另一端插入附近的 AC 電源插座。

B：目標伺服器

使用 PS/2 或 USB 連接到目標伺服器。請先將目標伺服器的視訊設定為支援的解析度，然後再接連接纜線。如果使用虛擬媒體或絕對滑鼠模式，便必須使用 USB 連線。

USB 組態

▶ 若要設定 **KX II-101-V2** 以搭配 **USB** 目標伺服器使用：

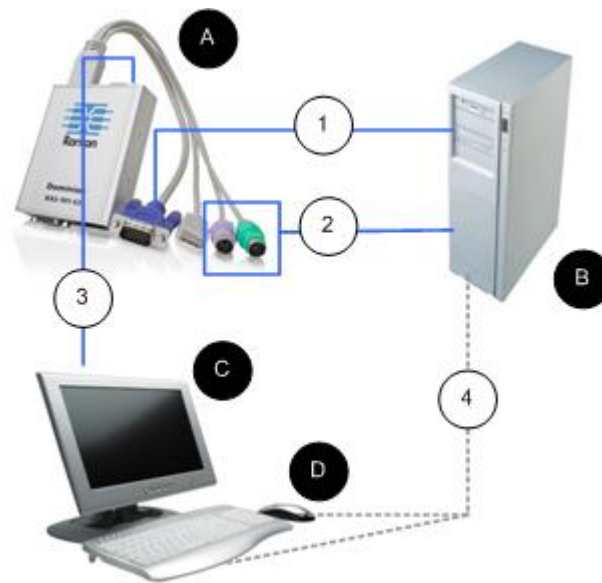
1. 使用所附視訊纜線，將 **KX II-101-V2** 連接到目標視訊連接埠。
2. 將 **KVM** 纜線的 **USB** 接頭連接到 **KX II-101-V2**，然後將 **USB** 接頭連接到目標伺服器上的 **USB** 連接埠。
3. 如果您需要使用本機視訊，請將監視器連接到 **KX II-101-V2** 的本機使用者 (**Local User**) 連接埠。**選用**
4. 將 **USB** 鍵盤與滑鼠直接連接到目標伺服器。**選用**

附註：如果使用虛擬媒體，便必須使用 **USB** 連線。

USB 連線圖解

A	KX II-101-V2
B	目標伺服器
C	本機監視器 (選用)
D	本機滑鼠與鍵盤 (選用)
1	從 KX II-101-V2 連至目標伺服器的視訊連線
2	從 KX II-101-V2 連至目標伺服器的 USB 連線
3	從 KX II-101-V2 本機使用者 (Local User) 連接埠連至監視器的選用監視器連線
4	從目標伺服器連至滑鼠與鍵盤的選用 USB 連線 (纜線非隨附)

PS/2 組態



▶ 若要設定 KX II-101-V2 以搭配 PS/2 目標伺服器使用：

1. 使用所附視訊纜線，將 KX II-101-V2 連接到目標視訊連接埠。
2. 將 KVM 纜線的 PS/2 接頭連接到目標伺服器上的 PS/2 連接埠。
3. 如果您需要使用本機視訊，請將監視器連接到 KX II-101-V2 的本機使用者 (Local User) 連接埠。**選用**
4. 如果有 PS/2 鍵盤與滑鼠，請使用 PS/2 對 USB 轉接頭 (非隨附)，直接連接到目標伺服器的 USB 連接埠。**選用**

附註：如果使用虛擬媒體，便必須使用 USB 連線。

PS/2 連線圖解	
A	KX II-101-V2
B	目標伺服器
C	本機監視器
D	本機滑鼠與鍵盤 (選用)
1	從 KX II-101-V2 連至目標伺服器的視訊連線

PS/2 連線圖解	
2	從 KX II-101-V2 連至目標伺服器的 KVM 纜線
3	KX II-101-V2 連至監視器的選用連線
4	從目標伺服器連至鍵盤與滑鼠的選用 PS/2 對 USB 轉接頭連線 (纜線非隨附)

C: 網路

將標準乙太網路纜線從標示為 LAN 的網路連接埠，連接到乙太網路交換器、集線器或路由器。乙太網路連線上出現的 LAN LED 可指出乙太網路活動。KX II-101-V2 正在使用時會閃爍黃光，代表正以 10 Mbps 傳輸 IP 流量。綠光則代表連線速度為 100 Mbps。

D: Admin 連接埠

管理連接埠可讓您使用像是 HyperTerminal 的終端機模擬程式，對 KX II-101-V2 執行設定工作。使用一條 DB9M 對 DB9F 的一對一序列纜線，從 KX II-101-V2 連接到電腦或膝上型電腦上的序列連接埠。序列連接埠的通訊組態應該設定如下：

- 115,200 傳輸速率
- 8 資料位元
- 1 停止位元
- 無同位檢查
- 無流量控制

E: 本機使用者 (Local User) 連接埠

本機使用者 (Local User) 連接埠可直接連接到監視器，做為目標伺服器視訊的通道。本機鍵盤與滑鼠必須直接連接到目標伺服器。

若為 USB 組態，只有本機視訊會透過本機使用者連接埠，連接到目標伺服器。鍵盤與滑鼠則是使用 USB 連接埠，直接連接到目標伺服器。

步驟 4: 設定 KX II-101-V2

附註：如果您要透過網頁瀏覽器設定 KX II-101-V2，便必須在 KX II-101-V2 與用戶端之間使用跳接纜線。

設定 KX II-101-V2 使用遠端主控台

KX II-101-V2 遠端主控台是一種網頁型應用程式，可讓您在使用前事先設定裝置，以及在完成設定後加以管理。在使用遠端主控台來設定 KX II-101-V2 之前，您必須將工作站與裝置連線到網路。

您也可以使用終端機模擬程式設定 `>ProductName<`。請參閱 **〈設定 KX II-101-V2 使用終端機模擬程式 (選用)>** (請參閱 "設定 KX II-101-V2 使用終端機模擬程式 (選用)" p. 31)。

設定新密碼

當您初次登入遠端主控台時，系統會提示您，要求設定新的密碼以取代預設密碼。然後您才可以設定 KX II-101-V2。

1. 登入與 KX II-101-V2 裝置有網路連線的工作站。
2. 啟動支援的網頁瀏覽器，例如 Internet Explorer® (IE) 或 Firefox®。
3. 在瀏覽器的網址欄位中，請輸入裝置的預設 IP 位址：192.168.0.192。
4. 按下 **Enter**。隨即會開啟「Login」(登入) 頁面。
5. 輸入使用者名稱 `admin` 與密碼 `raritan`。
6. 按一下「Login」(登入)。隨即會顯示「Change Password」(變更密碼) 頁面。
7. 在「Old Password」(舊密碼) 欄位中，輸入 `raritan`。
8. 在「New Password」(新密碼) 欄位與「Confirm New Password」(確認新密碼) 欄位中輸入新的密碼。密碼長度最多可有 64 個字元，其中可包含英文的英數字元與可列印的特殊字元。
9. 按一下「Apply」(套用)。您會收到已順利變更密碼的確認訊息。
10. 按一下「OK」(確定)。隨即會開啟「Port Access」(連接埠存取) 頁面。

指派 IP 位址

下列程序會說明如何使用「Network Settings」(網路設定) 頁面指派 IP 位址。如需有關此頁面全部欄位及作業的完整資訊，請參閱 **〈網路設定〉** (請參閱 "網路設定" p. 102)。

▶ 若要指派 IP 位址：

1. 選擇「Device Settings」(裝置設定) > 「Network」(網路)。隨即會開啟「Network Settings」(網路設定) 頁面。
2. 為 KX II-101-V2 裝置指定有意義的「Device Name」(裝置名稱)。最多可有 32 個英數字元，可包含有效的特殊字元，但不可包含空格。
3. 在 IPv4 區段中，輸入或選取適當的 IPv4 特定網路設定：

- a. 視需要輸入「IP Address」(IP 位址)。預設的 IP 位址為 192.168.0.192。
 - b. 輸入「Subnet Mask」(子網路遮罩)。預設的子網路遮罩為 255.255.255.0。
 - c. 如果「IP Auto Configuration」(IP 自動組態) 下拉式清單選取「None」(無)，請輸入「Default Gateway」(預設閘道)。
 - d. 如果「IP Auto Configuration」(IP 自動組態) 下拉式清單選取「DHCP」，請輸入「Preferred DHCP Host Name」(慣用 DHCP 主機名稱)。
 - e. 選取「IP Auto Configuration」(IP 自動組態)。有以下選項可用：
 - None (無，靜態 IP) - 此選項需要手動指定網路參數。
此為建議選項，因為 KX II-101-V2 是基礎結構裝置，因此其 IP 位址不應變更。
 - DHCP - 由網路電腦 (用戶端) 使用動態主機設定通訊協定，從 DHCP 伺服器取得唯一的 IP 位址與其他參數。
使用此選項，則由 DHCP 伺服器指定網路參數。如果使用 DHCP，請輸入「Preferred host name」(慣用主機名稱，僅限 DHCP)。最多 63 個字元。
4. 如果使用 IPv6，請在 IPv6 區段中輸入或選取適當的 IPv6 特定網路設定：
- a. 選取 IPv6 核取方塊以啟動該區段中的欄位。
 - b. 輸入「Global/Unique IP Address」(全域/唯一 IP 位址)。這是指派給 KX II-101-V2 的 IP 位址。
 - c. 輸入「Prefix Length」(首碼長度)。這是 IPv6 位址中使用的位元數目。
 - d. 輸入「Gateway IP Address」(閘道 IP 位址)。
 - e. Link-Local IP Address (連結本機 IP 位址)。這是自動指派給裝置的位址。用來進行芳鄰探索或是在沒有路由器存在時使用。**唯讀**
 - f. Zone ID (區域 ID)。這會以相關聯的位址來識別裝置。**唯讀**
 - g. 選取「IP Auto Configuration」(IP 自動組態設定)。有以下選項可用：
 - None (無) - 若不要自動 IP 組態，而偏好自行設定 IP 位址 (靜態 IP)，請使用此選項。此為預設及建議選項。

如果在「IP auto configuration」(IP 自動組態設定) 中選取「None」(無)，即會啟用下列網路基本設定欄位：「Global/Unique IP Address」(全域/唯一 IP 位址)、「Prefix Length」(首碼長度) 及「Gateway IP Address」(閘道 IP 位址)，讓您手動設定 IP 組態。

- Router Discovery (路由器探索) - 除了只適用於直接連接之子網路的「連結本機」IPv6 位址以外，若要自動指派「全域」或「唯一」的本機 IPv6 位址，請使用此選項。
5. 如果選取「DHCP」，同時已啟用「Obtain DNS Server Address」(取得 DNS 伺服器位址)，請選取「Obtain DNS Server Address Automatically」(自動取得 DNS 伺服器位址)。選取「Obtain DNS Server Address Automatically」(自動取得 DNS 伺服器位址) 後，就會使用由 DHCP 伺服器提供的 DNS 資訊。
 6. 如果選取「Use the Following DNS Server Addresses」(使用下列的 DNS 伺服器位址)，不論是否選取「DHCP」，都會使用在此區段中輸入的位址來連線到 DNS 伺服器。

如果選取「Use the Following DNS Server Addresses」(使用下列的 DNS 伺服器位址) 選項，請輸入下列資訊。若因為連線中斷而使主要 DNS 伺服器連線中斷，就會使用以下的主要與次要 DNS 位址。

- a. Primary DNS Server IP Address (主要 DNS 伺服器 IP 位址)
 - b. Secondary DNS Server IP Address (次要 DNS 伺服器 IP 位址)
7. 完成後，請按一下「OK」(確定)。

如需在「Network Settings」(網路設定) 頁面中設定此區段的詳細資訊，請參閱 **<LAN 介面設定>** (請參閱 "LAN 介面設定" p. 106)。

附註：在某些環境中，「LAN Interface Speed & Duplex」(LAN 介面速度與雙工) 設定的「Autodetect」(自動偵測，自動交涉程式)，並不會正確設定網路參數，因而引發網路問題。在執行實例中，將 KX II-101-V2 的「LAN Interface Speed & Duplex」(LAN 介面速度與雙工) 欄位設為「100 Mbps/Full Duplex」(100 Mbps/全雙工) 或適合您網路的其他選項，即可解決此問題。如需詳細資訊，請參閱「Network Settings」(網路設定) (請參閱 "網路設定" p. 102) 頁面。

命名目標伺服器

1. 將 KX II-101-V2 接上目標伺服器。
2. 選擇「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態)。隨即會開啟「Port Configuration」(連接埠組態) 頁面。
3. 按一下目標伺服器的「Port Name」(連接埠名稱)。隨即會開啟「Port」(連接埠) 頁面。
4. 輸入一個名稱，最多可有 32 個英數字元及特殊字元。

5. 按一下「OK」(確定)。

The screenshot shows a configuration window with a blue header 'Port 1'. Below it, the 'Type' is set to 'KVM' and the 'Name' is 'Dominion_KX2_101_Port1'. The 'Power Association' section has a 'Power Strip Name' dropdown set to 'None' and four 'Outlet Name' dropdowns, all currently showing '---'. Below these are two expandable sections: '▶ USB Connection Settings' and '▶ Advanced USB Connection Settings'.

遠端驗證

CC-SG 使用者注意事項

當 KX II-101-V2 是由 CommandCenter Secure Gateway 控制時，CC-SG 會驗證使用者與群組。

如需 CC-SG 驗證的詳細資訊，請參閱可從 Raritan 網站 (www.raritan.com) 的「Support」(技術支援) 網頁下載的《CommandCenter Secure Gateway 使用者指南》、《管理員指南》或《部署指南》。

支援的通訊協定

為了簡化使用者名稱與密碼管理，KX II-101-V2 提供將驗證要求轉寄到外部驗證伺服器的功能。支援的外部驗證通訊協定有兩種：LDAP/LDAPS 與 RADIUS。

Microsoft Active Directory 注意事項

Microsoft® Active Directory® 原本使用 LDAP/LDAPS 通訊協定，並可當作 KX II-101-V2 的 LDAP 伺服器與驗證來源使用。如果有 IAS (Internet Authorization Server, 網際網路授權伺服器) 元件，Microsoft Active Directory 伺服器亦可當作 RADIUS 驗證來源使用。

建立使用者群組與使用者

進行初始組態時，您必須定義使用者群組與使用者，如此使用者才能存取 KX II-101-V2。

KX II-101-V2 使用系統所提供的預設使用者群組，且允許您建立群組，以及指定適當的權限以符合您的需求。

您必須有使用者名稱與密碼，才能存取 KX II-101-V2。此項資訊是用來驗證嘗試存取 KX II-101-V2 的使用者。如需新增與編輯使用者群組與使用者的詳細資訊，請參閱〈使用者管理〉（請參閱 "使用者管理" p. 80）。

設定 KX II-101-V2 使用終端機模擬程式 (選用)

您可以使用像是 HyperTerminal 的終端機模擬程式，使用管理序列主控台設定 KX II-101-V2 的下列組態參數：

- IP 位址
- 子網路遮罩位址
- 閘道位址
- IP 自動組態設定
- LAN 速度
- LAN 介面模式

若要使用終端機模擬程式搭配 KX II-101-V2，您必須先以隨附的 RS-232 序列纜線，從 KX II-101-V2 的管理連接埠連接到電腦上的 COM 連接埠。

基於示範目的，本節中說明的終端機模擬程式為 HyperTerminal。您可以使用任何終端機模擬程式。

▶ 若要使用終端機模擬程式設定 KX II-101-V2：

1. 將 KX II-101-V2 連接到本機電腦。
2. 連接 KX II-101-V2 上的管理連接埠與電腦上的 COM1 連接埠。
3. 啟動您想要用以設定 KX II-101-V2 的終端機模擬程式。
4. 在終端機模擬程式中設定下列連接埠組態：
 - 每秒傳輸位元 - 115200
 - 資料位元 - 8
 - 同位檢查 - 無
 - 停止位元 - 1
 - 流量控制 - 無
5. 連接 KX II-101-V2。隨即會開啟「Login」(登入) 頁面。

6. 輸入管理員使用者名稱，然後按下 **Enter**。系統會提示您，要求輸入密碼。
7. 輸入預設管理員名稱 *admin*，然後按下 **Enter**。系統會提示您，要求輸入密碼。
8. 在「Admin Port >」(管理連接埠) 提示，輸入 *config*，然後按下 **Enter**。
9. 在「Config >」(設定) 提示，輸入 *network*，然後按下 **Enter**。
10. 若要設定新的網路設定，請在「Network」(網路) 提示，輸入 *interface*，後面加上下列其中一個指令與適當的引數 (選項)，然後按下 **Enter**。

指令	引數	選項
ipauto	none dhcp	<p>none - 可讓您手動指定裝置的 IP 位址。您必須在此選項後面加上 ip 指令與 IP 位址，如下列範例所示：</p> <pre>interface ipauto none ip 192.168.50.12</pre> <p>dhcp - 於啟動時自動將 IP 位址指派給裝置。</p> <pre>interface ipauto dhcp</pre>
ip	IP 位址	<p>要指派給裝置的 IP 位址。若是第一次手動設定 IP 位址，此指令必須跟 ipauto 指令與 none 選項一起使用。如需詳細資訊，請參閱 ipauto。只要手動指派 IP 位址一次後，您便可以單獨使用 ip 指令來變更 IP 位址。</p>
mask	子網路遮罩	<p>指令欄應是 "interface"</p> <pre>interface ip ...</pre> <pre>interface mask 子網路遮罩 IP 位址</pre> <pre>interface gw 閘道 IP 位址</pre> <pre>interface mode </pre>
gw	IP 位址	閘道的 IP 位址
mode	mode	乙太網路模式：您有下列選

指令	引數	選項
		擇： <ul style="list-style-type: none"> ▪ auto - 根據網路，自動設定速度與介面模式。 ▪ 10hdx - 10 MB/s，半雙工。 ▪ 10fdx - 10 MB/s，全雙工 ▪ 100hdx - 100 MB/s，半雙工 ▪ 100fdx - 100 MB/s，全雙工

當您順利變更設定時，會看見下列確認訊息：

```
Admin Port > config
```

```
Admin Port > Config > network
```

```
Admin Port > Config > Network > interface ipauto none
ip 192.168.50.126
```

```
Network interface configuration successful. (網路介面
組態設定成功。)
```

完成設定 **KX II-101-V2** 後，請在指令提示輸入 *logout*，然後按下 **Enter**。您會隨即登出指令行介面。

本章內容

介面.....	34
虛擬 KVM 用戶端 (VKC).....	43

 介面

KX II-101-V2 遠端主控台介面

「KX II-101-V2 遠端主控台」是瀏覽器圖形化使用者介面，可讓您登入 KVM 目標伺服器以及與 KX II-101-V2 連接的序列目標，還可以從遠端管理 KX II-101-V2。

「KX II-101-V2 遠端主控台」可對已連線的 KVM 目標伺服器提供數位連線。每當您使用「KX II-101-V2 遠端主控台」登入 KVM 目標伺服器時，隨即會開啟「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗。

附註：如果使用 Internet Explorer® 7，您在嘗試連線至目標伺服器時，可能會遇到權限問題。為了避免發生此問題，請執行下列動作：

1. 在 Internet Explorer 中，按一下「Tools」(工具) > 「Internet Options」(網際網路選項)，以開啟「Internet Options」(網際網路選項) 對話方塊。
2. 在「Temporary Internet files」(網際網路暫存檔) 區段中，按一下「Settings」(設定)。隨即會開啟「Settings」(設定) 對話方塊。
3. 在「Check for newer versions of stored pages」(檢查儲存的畫面是否有較新的版本)區段中，選取「Automatically」(自動)。
4. 按一下「OK」(確定)，即可套用設定。

啟用直接連接埠存取

直接連接埠存取可讓您存取 KX II-101-V2 遠端主控台，而無須逐步進行往常的登入頁面。啟用直接連接埠存取，您便可以定義 URL，直接瀏覽到「Port Access」(連接埠存取) 頁面。

▶ **若要啟用直接連接埠存取：**

1. 啟動 KX II-101-V2 遠端主控台。
2. 選擇「Device Settings」(裝置設定) > 「Device Services」(裝置服務)。隨即會開啟「Device Services」(裝置服務) 頁面。

3. 選取「Enable Direct Port Access via URL」(透過 URL 啟用直接連接埠存取) 核取方塊。
4. 按一下「Save」(儲存)。

▶ **若要定義直接連接埠存取 URL：**

- 定義具有 IP 位址、使用者名稱、密碼的 URL，亦可視需要定義 KX II-101-V2 的連接埠編號。

直接連接埠存取 URL 的格式如下：

```
https://IP
address/dpa.asp?username=username&password=password
```

祕訣：定義直接連接埠存取 URL 之後，在網頁瀏覽器中將此 URL 儲存為書籤，如此可更方便您重複使用。

KX II-101-V2 主控台瀏覽方式

KX II-101-V2 主控台介面提供許多方法，供您進行瀏覽和選取項目。

▶ **若要選取選項 (使用下列任一方法)：**

- 按一下索引標籤。隨即會出現列有可用選項的頁面。
- 將游標移到索引標籤上，然後從功能表選取適當的選項。
- 直接從顯示的功能表階層按一下選項 (「breadcrumbs」或稱「導覽路徑標示」)。

▶ **若要捲動瀏覽超出螢幕的頁面：**

- 使用鍵盤上的 Page Up 及 Page Down 鍵。
- 使用右側的捲軸。

左面板

KX II-101-V2 介面的左面板包含下列資訊。請注意，有些是條件式資訊 - 表示當您身為特定使用者、使用特定功能等時才會顯示。條件式資訊收錄於此。

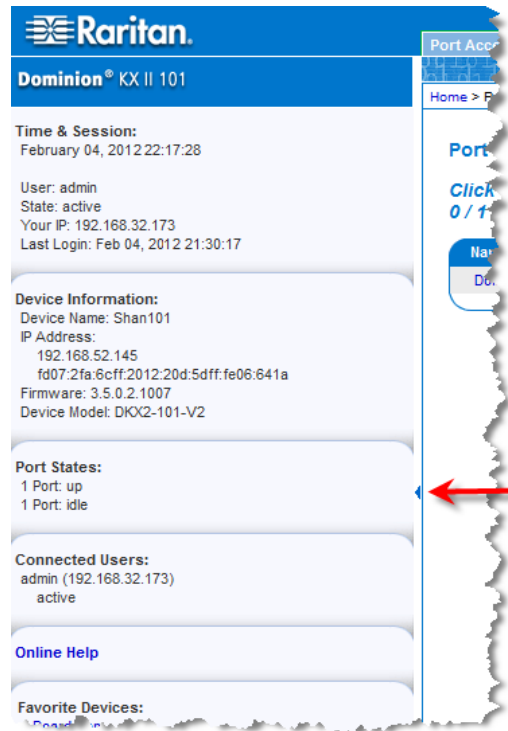
資訊	說明	顯示時機
Time & Session (時間與階段作業)	目前的日期與時間。	一律顯示
使用者	目前使用者的使用者名稱	一律顯示

資訊	說明	顯示時機
State (狀態)	目前的應用程式狀態，其為閒置或作用中。若處於閒置，應用程式便會追蹤和顯示階段作業閒置的時間長度。	一律顯示
Your IP (您的 IP)	用來存取 KX II-101-V2 的 IP 位址。	一律顯示
Last Login (上次登入)	目前使用者上次登入的日期與時間	一律顯示
Under CC-SG Management (受 CC-SG 管理)	管理 KX II-101-V2 的 CC-SG 裝置 IP 位址。	KX II-101-V2 受 CC-SG 管理時
裝置資訊	您所使用 KX II-101-V2 裝置的專屬資訊。	一律顯示
Device Name (裝置名稱)	指派給裝置的名稱。	一律顯示
IP Address (IP 位址)	KX II-101-V2 的 IP 位址。	一律顯示 IPv4，而 IPv6 若設定才予以顯示
Firmware (韌體)	目前的韌體版本。	一律顯示
Device Model (裝置機型)	KX II-101-V2 裝置的機型	一律顯示
Port States (連接埠狀態)	KX II-101-V2 使用的連接埠狀態。	一律顯示
Connect Users (連線使用者)	透過使用者名稱與 IP 位址來識別的使用者，其目前已和 KX II-101-V2 連線。	一律顯示
Online Help (線上說明)	可連至線上說明的連結。	一律顯示
Favorite Devices (愛用裝置)	請參閱 <管理我的最愛>。	一律顯示
FIPS 模式	FIPS 模式：EnabledSSL 憑證：FIPS 模式相容	FIPS 啟用時

您可以收攏左面板來增加顯示的頁面區域。

▶ 若要收攏左面板：

- 按一下面板左側中間的藍色向左箭頭。收攏面板之後，再按一次藍色箭頭，就會展開面板。



連接埠存取頁面

成功登入「KX II-101-V2 遠端主控台」之後，隨即會出現「Port Access」（連接埠存取）頁面。此頁面會列出 KX II-101-V2 連接埠、已連接的 KVM 目標伺服器與其可用性。「Port Access」（連接埠存取）頁面可讓您存取已連接到 KX II-101-V2 的 KVM 目標伺服器。KVM 目標伺服器就是您想要透過 KX II-101-V2 裝置控制的伺服器。這些伺服器都要連接到裝置背面的 KX II-101-V2 連接埠。

▶ 若要使用「Port Access」（連接埠存取）頁面：

1. 從 KX II-101-V2 遠端主控台按一下「Port Access」（連接埠存取）索引標籤。隨即會開啟「Port Access」（連接埠存取）頁面。顯示的資訊如下：

- **Port Name** (連接埠名稱) - KX II-101-V2 連接埠的名稱。此名稱最初是設定為 **Dominion_KX2_101_Port1**，但您可將其變更為較具敘述性的名稱。按一下「**Port Name**」(連接埠名稱) 連結，隨即會開啟「**Port Action**」(連接埠動作) 功能表。
 - **Availability** (可用性) - 「**Availability**」(可用性) 可以是「**Idle**」(閒置)、「**Connected**」(已連線) 或「**Busy**」(忙碌)。
2. 按一下要存取之目標伺服器的連接埠名稱。隨即會出現「**連接埠動作**」功能表。如需可用功能表選項的詳細資訊，請參閱 <[連接埠動作功能表](#)> (請參閱 "[連接埠動作功能表](#)" p. 38)。
 3. 從「**連接埠動作**」功能表選擇所需的**功能表指令**。

連接埠動作功能表

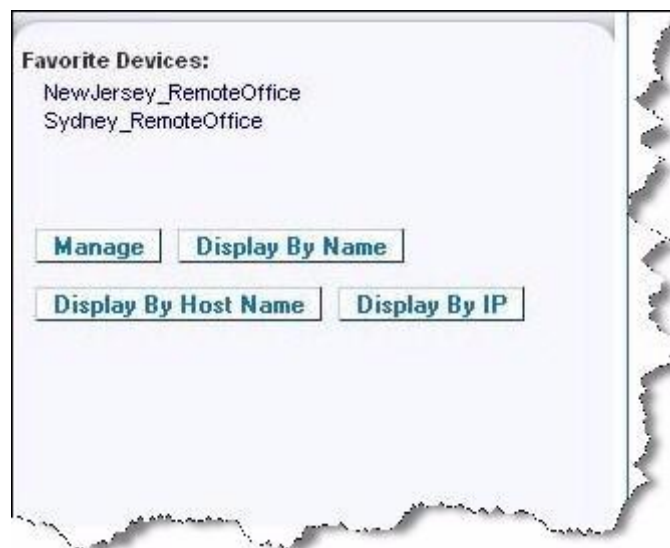
當您按一下「**連接埠存取**」清單中的「**連接埠名稱**」時，隨即會出現「**連接埠動作**」功能表。請選擇該連接埠所需的**功能表選項**，開始執行。請注意，根據連接埠的狀態與可用性，「**連接埠動作**」功能表中只會列出目前可用的選項。

- **Connect** (連線) - 建立新的目標伺服器連線。若為「**KX II-101-V2 遠端主控台**」，隨即會出現新的「**Virtual KVM Client**」(虛擬 KVM 用戶端，**VKC**) (請參閱 "[虛擬 KVM 用戶端 \(VKC\)](#)" p. 43) 頁面。
- **Disconnect** (中斷連線) - 中斷此連接埠的連線，並關閉此目標伺服器的「**Virtual KVM Client**」(虛擬 KVM 用戶端)頁面。唯有當連接埠狀態為開啟且已連線或是開啟且忙碌時，才會提供此功能表項目。
- **Power On** (開啟電源) - 利用相關聯的插座開啟目標伺服器的電源。唯有當目標有一或多個電源關聯時，以及當使用者有權操作此項服務時，才會看見此選項。
- **Power Off** (關閉電源) - 利用相關聯的插座關閉目標伺服器的電源。唯有當目標有一或多個電源關聯時、當目標的電源已開啟時 (連接埠狀態為開啟)，以及當使用者有權操作此項服務時，才會看見此選項。
- **Power Cycle** (重新開啟電源) - 利用相關聯的插座重新開啟目標伺服器的電源。唯有當目標有一或多個電源關聯時，以及當使用者有權操作此項服務時，才會看見此選項。

管理我的最愛

「愛用裝置」功能可讓您整理及快速存取常用裝置。「愛用裝置」區段位於「連接埠存取」頁面左下方 (提要欄位)，其可提供下列功能：

- 建立和管理愛用裝置清單
 - 快速存取常用的裝置
 - 依「裝置名稱」、「IP 位址」或「DNS 主機名稱」列出愛用裝置
 - 在子網路探查 KX II-101-V2 裝置 (登入之前與之後)
 - 從連線的 Dominion 裝置擷取探查到的 KX II-101-V2 裝置 (登入之後)
- ▶ **若要存取愛用的 KX II-101-V2 裝置：**
- 按一下裝置名稱 (列在「Favorite Devices」(愛用裝置) 下)。隨即會為該裝置開啟新的瀏覽器視窗。
- ▶ **若要依名稱顯示愛用裝置：**
- 按一下「Display by Name」(依名稱顯示)。
- ▶ **若要依 IP 位址顯示愛用裝置：**
- 按一下「Display by IP」(依 IP 顯示)。
- ▶ **若要依主機名稱顯示愛用裝置：**
- 按一下「Display by Host Name」(依主機名稱顯示)。



管理愛用裝置頁面

▶ 若要開啟「管理愛用裝置」頁面：

- 按一下左面板的「管理」。隨即會出現「管理愛用裝置」頁面，而且上面包含下列選項：

使用：	執行：
愛用裝置清單	管理愛用裝置清單。
探查裝置 – 本機子網路	在用戶端電腦的本機子網路上探查力登裝置。
探查裝置 – KX II-101-V2 子網路	探查 KX II-101-V2 裝置子網路上的力登裝置。
新增裝置到愛用裝置	在「愛用裝置」清單中新增、編輯及刪除裝置。

愛用裝置清單頁面

您可以從「愛用裝置清單」頁面，新增、編輯及刪除愛用裝置清單中的裝置。

▶ 若要開啟「愛用裝置清單」頁面：

- 選擇「管理」>「愛用裝置清單」。隨即會開啟「愛用裝置清單」頁面。

探查本機子網路上的 Raritan 裝置

此選項可以在執行 KX II-101-V2 遠端主控台的本機子網路上探查裝置。您可以直接從此頁面存取這些裝置，或是將它們加入愛用裝置清單。請參閱 <愛用裝置清單頁面> (請參閱 "愛用裝置清單頁面" p. 40)。

▶ 若要探查本機子網路上的裝置：

1. 選擇「管理」>「探查裝置 – 本機子網路」。隨即會出現「探查裝置 – 本機子網路」頁面。
2. 選擇適當的探查連接埠：
 - 若要使用預設的探查連接埠，請選取「使用預設連接埠 5000」核取方塊。
 - 若要使用其他探查連接埠：
 - a. 取消選取「使用預設連接埠 5000」核取方塊。

- b. 在「執行探查的連接埠」欄位輸入連接埠編號。
 - c. 按一下「儲存」。
3. 按一下「重新整理」。隨即會重新整理本機子網路的裝置清單。

▶ **若要將裝置加入「愛用裝置清單」：**

1. 選取裝置名稱/IP 位址旁邊的核取方塊。
2. 按一下「新增」。

▶ **若要存取探查到的裝置：**

按一下該裝置的名稱或 IP 位址。隨即會為該裝置開啟新的瀏覽器視窗。

探查 KX II-101-V2 子網路的 Raritan 裝置

此選項可以在裝置子網路 (KX II-101-V2 裝置 IP 位址自己的子網路) 上探查裝置。您可以直接從「子網路」頁面存取這些裝置，或是將它們加入愛用裝置清單。請參閱 [〈愛用裝置清單頁面〉](#) (請參閱 "[愛用裝置清單頁面](#)" p. 40)。

此功能可讓多部 KX II-101-V2 裝置自動交互操作和擴充。KX II-101-V2 遠端主控台可自動探查 KX II-101-V2 裝置子網路中的 KX II-101-V2 裝置及任何其他力登裝置。

▶ **若要探查裝置子網路上的裝置：**

1. 選擇「管理」>「探查裝置 - KX II-101-V2 子網路」。隨即會出現「探查裝置 - KX II-101-V2 子網路」頁面。
2. 按一下「重新整理」。隨即會重新整理本機子網路的裝置清單。

▶ **若要將裝置加入「愛用裝置清單」：**

1. 選取裝置名稱/IP 位址旁邊的核取方塊。
2. 按一下「新增」。

▶ **若要存取探查到的裝置：**

- 按一下該裝置的名稱或 IP 位址。隨即會為該裝置開啟新的瀏覽器視窗。

新增、編輯和刪除我的最愛

▶ **若要將裝置加入「愛用裝置清單」：**

1. 選取「管理」>「新增裝置到愛用裝置」。隨即會出現「新增愛用裝置」頁面。
2. 輸入有意義的說明。

3. 輸入該裝置的「IP 位址/主機名稱」。
4. 變更探查連接埠 (如有需要)。
5. 選取「產品類型」。
6. 按一下「確定」。便會將該裝置加入愛用裝置清單。

▶ **若要編輯某部愛用裝置：**

1. 從「愛用裝置清單」頁面，選取適當 KX II-101-V2 裝置旁邊的核取方塊。
2. 按一下「編輯」。隨即會出現「編輯」頁面。
3. 視需要更新欄位：
 - 說明
 - IP 位址/主機名稱 - 輸入 KX II-101-V2 裝置的 IP 位址
 - 連接埠 (視需要)
 - 產品類型
4. 按一下「確定」。

▶ **若要刪除某部愛用裝置：**

重要：移除愛用裝置時務必謹慎小心。系統並不會顯示提示要求您確認刪除作業。

1. 選取適當 KX II-101-V2 裝置旁邊的核取方塊。
2. 按一下「刪除」。隨即會從愛用裝置清單中移除該愛用裝置。

登出

▶ **若要結束 KX II-101-V2：**

- 按一下頁面右上角的「Logout」(登出)。

*附註：*登出也會關閉所有開啟的「虛擬 KVM 用戶端」與序列用戶端階段作業。

多平台用戶端 (MPC)

Raritan 多平台用戶端 (MPC) 是適用於 Raritan 產品系列的圖形化使用者介面，可讓您從遠端存取與 Raritan KVM-over-IP 裝置連接的目標伺服器。如需使用 MPC 的詳細資訊，請參閱 Raritan 網站上與《使用者指南》位於同一網頁的《KVM 與序列存取用戶端指南》。該處也提供啟動 MPC 的指示。

請注意，多種不同的 Raritan 產品均使用此用戶端。因此，此段說明可能會參照其他產品。

虛擬 KVM 用戶端 (VKC)

請注意，多種不同的 Raritan 產品均使用此用戶端。因此，此段說明可能會參照其他產品。

概覽

每當您使用遠端主控台存取目標伺服器時，隨即會開啟「Virtual KVM Client」(虛擬 KVM 用戶端, VKC) 視窗。您所連接的目標伺服器都會有各自的虛擬 KVM 用戶端。您可以透過 Windows® 工作列存取此視窗。

「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗可以縮到最小、放到最大，還可以在電腦桌面上四處移動。

附註：重新整理 HTML 瀏覽器會關閉「虛擬 KVM 用戶端」的連線，執行作業時請務必謹慎。

附註：如果使用 Firefox 3.0.3，啟動應用程式時可能會發生問題。如果發生這種情況，請清除瀏覽器快取，然後再次啟動應用程式。

連線到 KVM 目標伺服器

▶ 若要連線到 KVM 目標伺服器：

1. 從「KX II-101-V2 遠端主控台」按一下「Port Access」(連接埠存取) 索引標籤。隨即會開啟「Port Access」(連接埠存取) 頁面。
2. 按一下要存取之目標的「Port Name」(連接埠名稱)。隨即會出現「Port Action」(連接埠動作) 功能表。
3. 按一下「Connect」(連線)。隨即會為連接至該連接埠的目標伺服器開啟「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗。

工具列按鈕與狀態列圖示

按鈕	按鈕名稱	說明
	連線內容	開啟「修改連線內容」對話方塊，您可在此處手動調整頻寬選項（例如連線速度、色彩深度、平滑化等）。
	視訊設定	開啟「Video Settings」(視訊設定) 對話方塊，可讓您手動調整視訊轉換參數。
	Color Calibration (色彩校準)	調整色彩設定，以減少過度的色彩雜訊。 作用和選擇「Video」(視訊) > 「Color Calibrate」(色彩校準) 一樣。 <hr/> <i>附註：不適用於 KX II-101-V2。</i>
	Target Screenshot (目標螢幕擷取畫面)	按一下即可擷取目標伺服器的螢幕擷取畫面，然後另存為選擇的檔案。
	音訊	您可以在開啟的對話方塊從已和用戶端電腦連接的音訊裝置清單中加以選擇。 在音訊裝置與目標連線之後，加以選取則會中斷該裝置的連線。 <hr/> <i>附註：此功能可與 KX II 2.4.0 (及更新的版本) 一起使用。</i> <i>附註：LX 裝置不支援此功能。KX II-101-V2 不支援此功能。</i>
	同步化滑鼠	雙滑鼠模式會讓滑鼠指標強制與目標伺服器的滑鼠指標重新對齊。 <hr/> <i>附註：如果選取絕對滑鼠模式，則無法使用。</i>
	重新整理畫面	強制重新整理視訊螢幕。
	自動偵測視訊設定	強制重新整理視訊設定 (解析度、螢幕更新頻率)。
	Smart Card (智慧卡)	您可以在開啟的對話方塊從已和用戶端電腦連接的智慧卡讀卡機清單中加以選擇。 <hr/> <i>附註：只有 KSX II 2.3.0 (及更新版本) 及 KX II 2.1.10 (及更新版本) 才提供此功能。</i>

按鈕	按鈕名稱	說明
		附註：LX 裝置不支援此功能。KX II-101-V2 不支援此功能。
	Send Ctrl+Alt+Del (傳送 Ctrl+Alt+Del)	將 CTRL+ALT+DEL 快速鍵組合傳送至目標伺服器。
	Single Cursor Mode (單游標模式)	啟動單游標模式，在此模式中，本機電腦滑鼠指標將不再顯示於螢幕上。 按 CTRL+ALT+O 可結束此模式。
	全螢幕模式	將螢幕最大化，以檢視目標伺服器桌面。
	Scaling (縮放比例)	放大或縮小目標視訊大小，讓您不需使用捲軸即可檢視目標伺服器視窗的所有內容。

目標伺服器的電源控制

附註：唯有已建立電源關聯時才能使用這些功能。

▶ 若要重新開啟 KVM 目標伺服器的電源：

1. 從 KX II-101-V2 遠端主控台按一下「Port Access」(連接埠存取) 索引標籤。隨即會開啟「Port Access」(連接埠存取) 頁面。
2. 按一下適當目標伺服器的「Port Name」(連接埠名稱)。隨即會出現「Port Action」(連接埠動作) 功能表。
3. 選擇「Power Cycle」(重新開啟電源)。隨即會顯示確認訊息。

▶ 若要開啟目標伺服器的電源：

1. 從 KX II-101-V2 遠端主控台按一下「Port Access」(連接埠存取) 索引標籤。隨即會開啟「Port Access」(連接埠存取) 頁面。
2. 按一下適當目標伺服器的連接埠名稱。隨即會出現「Port Action」(連接埠動作) 功能表。
3. 選擇「Power On」(開啟電源)。隨即會顯示確認訊息。

▶ 若要關閉目標伺服器的電源：

1. 從「KX II-101-V2 遠端主控台」按一下「Port Access」(連接埠存取) 索引標籤。隨即會開啟「Port Access」(連接埠存取) 頁面。

2. 按一下適當目標伺服器的連接埠名稱。隨即會出現「Port Action」(連接埠動作) 功能表。
3. 選擇「Power Off」(關閉電源)。隨即會顯示確認訊息。

中斷 KVM 目標伺服器連線

▶ 若要中斷目標伺服器連線：

- 按一下要中斷連線之目標伺服器的連接埠名稱。在「連接埠動作」功能表出現時，按一下「中斷連線」。


祕訣：您也可以從「Virtual KVM」(虛擬 KVM) 功能表選取「Connection」(連線) > 「Exit」(結束)，關閉「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗。

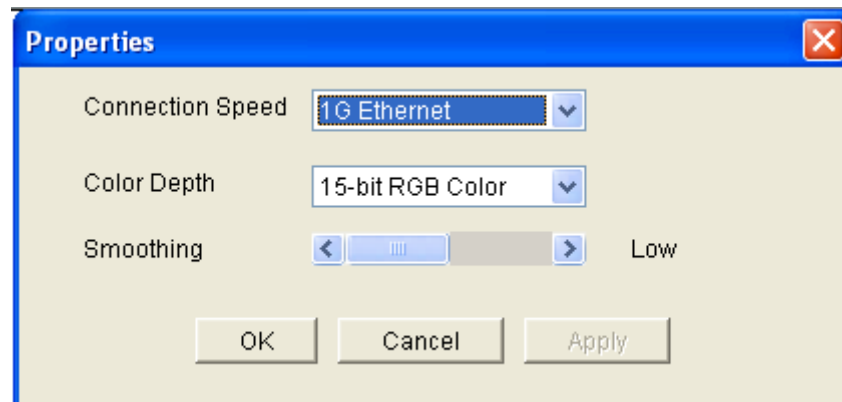
連線內容

動態視訊壓縮演算法可在不同的頻寬限制下維護 KVM 主控台的可用性。裝置不僅可為 LAN 用途最佳化 KVM 輸出，WAN 用途亦可蒙受此益處。這些裝置還可以控制色彩深度與限制視訊輸出，在視訊品質與系統對所有頻寬的回應之間取得最佳平衡。

您可最佳化「Properties」(內容) 對話方塊中的參數，以符合不同作業環境的需求。連線內容是在設定和儲存後，跨後續連線儲存到第二代裝置。

▶ 若要設定連線內容：

1. 選擇「Connection」(連線) > 「Properties」(內容) 或按一下工具列中的「Connection Properties」(連線內容) 按鈕 。隨即會開啟「Properties」(內容) 對話方塊。



附註：KX II-101 不支援 1G 乙太網路。

2. 從下拉式清單中選擇「**Connection Speed**」(連線速度)。裝置會自動偵測可用的頻寬，但不限制頻寬使用。不過，您也可以根據頻寬限制調整此用法。
 - Auto (自動)
 - 1G Ethernet (1 G 乙太網路)
 - 100 Mb Ethernet (10 Mb 乙太網路)
 - 10 Mb Ethernet (10 Mb 乙太網路)
 - 1.5 Mb (MAX DSL/T1) (極速 DSL/T1)
 - 1 Mb (Fast DSL/T1) (高速 DSL/T1)
 - 512 Kb (Medium DSL/T1) (中速 DSL/T1)
 - 384 Kb (Slow DSL/T1) (低速 DSL/T1)
 - 256 Kb (Cable) (纜線)
 - 128 Kb (Dual ISDN) (雙 ISDN)
 - 56 KB (ISP Modem) (ISP 數據機)
 - 33 KB (Fast Modem) (高速數據機)
 - 24 KB (Slow Modem) (低速數據機)

請注意，上述設定為特定情況下的最佳值，與實際速度或有出入。無論目前的網路速度與加密設定為何，用戶端與伺服器一律會嘗試以最快速度透過網路傳送視訊。但在設定符合實際操作環境時，系統的回應速度最佳。

3. 從下拉式清單中選擇「**Color Depth**」(色彩深度)。裝置可動態調整傳送給遠端使用者的色彩深度，以充分利用頻寬達到最大的使用。
 - 15 位元 RGB 色彩
 - 8 位元 RGB 色彩
 - 4 位元色彩
 - 4 位元灰階
 - 3 位元灰階
 - 2 位元灰階
 - 黑白

重要：大部分的管理工作 (伺服器監控、重新設定等等) 並不需要多數新式視訊顯示卡所提供的 24 位元或 32 位元的全彩色譜。嘗試以如此高的色彩深度進行傳輸，會浪費網路頻寬。

4. 使用滑桿選取所需的平滑度等級 (僅限 15 位元色彩模式)。平滑度等級可決定含少量雜色的螢幕區域融為平滑單色的力度。平滑度功能可降低螢幕所顯示的視訊雜訊，而提升目標視訊的外觀。
5. 按一下「OK」(確定) 即可設定內容。

連線資訊

▶ 若要取得虛擬 KVM 用戶端連線的相關資訊：

- 選擇「Connection」(連線) > 「Info...」(資訊)。隨即會開啟「Connection Info」(連線資訊) 視窗：

視窗上會顯示目前連線的下列資訊：

- Device Name (裝置名稱) - 裝置的名稱。
- IP Address (IP 位址) - 裝置的 IP 位址。
- Port (連接埠) - 用以存取目標裝置的 KVM 通訊 TCP/IP 連接埠。
- Data In/Second (每秒傳入資料) - 傳入資料的速率。
- Data Out/Second (每秒傳出資料) - 傳出資料的速率。
- Connect Time (連線時間) - 連線持續時間。
- FPS - 視訊每秒傳輸的畫面數。
- Horizontal Resolution (水平解析度) - 畫面的水平解析度。
- Vertical Resolution (垂直解析度) - 螢幕的垂直解析度。
- Refresh Rate (螢幕更新頻率) - 重新整理螢幕畫面的頻率。
- Protocol Version (通訊協定版本) - RFB 通訊協定版本。

▶ 若要複製此項資訊：

- 按一下「Copy to Clipboard」(複製剪貼簿)。即會將資訊貼至您所選擇的程式中。

鍵盤選項

鍵盤巨集

鍵盤巨集可確保所要傳送至目標伺服器的按鍵組合，必會傳送至該目標伺服器，而且只能由該目標伺服器進行轉譯。否則，其可能會由正在執行虛擬 KVM 用戶端的電腦 (即用戶端電腦) 所轉譯。

巨集儲存在用戶端電腦且為該台電腦專用。因此，使用其他電腦即看不到您的巨集。此外，若他人使用您的電腦並以其他名稱登入，則該使用者會看到您的巨集，因為巨集是全電腦通用的。

在虛擬 KVM 用戶端中建立的鍵盤巨集可在多平台用戶端 (MPC) 中使用，反之亦然。不過，在作用中 KVM 用戶端 (AKC) 中建立的鍵盤巨集無法在 VKC 或 MPC 中使用，反之亦然。

附註：KX II-101 不支援 AKC。

匯入/匯出鍵盤巨集

從作用中 KVM 用戶端 (AKC) 匯出的巨集無法匯入多平台用戶端 (MPC) 或虛擬 KVM 用戶端 (VKC)。從 MPC 或 VKC 匯出的巨集無法匯入 AKC。

附註：KX II-101 不支援 AKC。

▶ 若要匯入巨集：

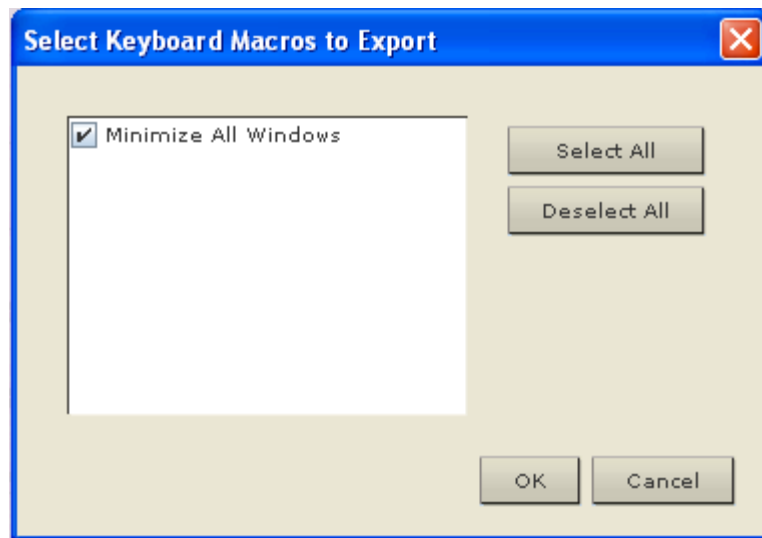
1. 選擇「Keyboard」(鍵盤) > 「Import Keyboard Macros」(匯入鍵盤巨集) 以開啟「Import Macros」(匯入巨集) 對話方塊。瀏覽到巨集檔案所在的資料夾位置。
2. 按一下巨集檔案，然後按一下「Open」(開啟) 以匯入巨集。
 - a. 如果在檔案中找到太多巨集，便會顯示一則錯誤訊息，並在您選取「OK」(確定) 之後終止匯入。
 - b. 如果匯入失敗，便會出現錯誤對話方塊，以及顯示有關匯入失敗原因的訊息。請選取「OK」(確定) 繼續匯入其他可以匯入的巨集。
3. 勾選巨集的對應核取方塊或使用「Select All」(全選) 或「Deselect All」(取消全選) 選項，選取要匯入的巨集。
4. 按一下「OK」(確定)，便可開始匯入。
 - a. 如果找到重複的巨集，隨即會出現「Import Macros」(匯入巨集) 對話方塊。請執行下列其中一項動作：

- 按一下「Yes」(是)，以匯入的版本取代現有的巨集。
 - 按一下「Yes to All」(全部皆是)，以取代目前選取的巨集和找到的任何其他重複巨集。
 - 按一下「No」(否)，以保留原來的巨集，並繼續匯入下一個巨集。
 - 按一下「No to All」(全部皆否)，以保留原來的巨集，並繼續匯入下一個巨集。找到的任何其他重複巨集也會被略過。
 - 按一下「Cancel」(取消)，便可停止匯入。
 - 或者，按一下「Rename」(重新命名) 以重新命名巨集，然後予以匯入。如果選取「Rename」(重新命名)，隨即會出現「Rename Macro」(重新命名巨集) 對話方塊。在欄位中輸入巨集的新名稱，然後按一下「OK」(確定)。隨即會關閉對話方塊，並繼續進程序。如果輸入的名稱和其他巨集重複，便會出現警示，並要求您為巨集輸入其他名稱。
- b. 如果在進行匯入程序時，超過允許匯入的巨集數目上限，便會出現一個對話方塊。按一下「OK」(確定) 嘗試繼續匯入巨集，或按一下「Cancel」(取消) 以停止匯入程序。

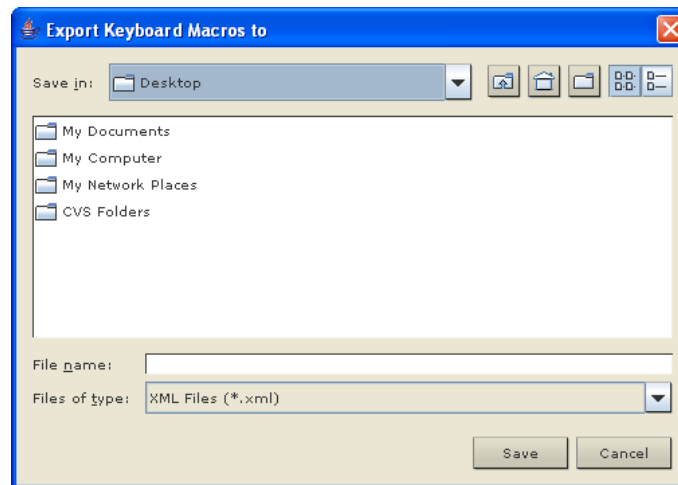
然後便會完成匯入巨集。如果匯入的巨集所含的快速鍵已經存在，便會捨棄所匯入巨集的快速鍵。

► **若要匯出巨集：**

1. 選擇「Tools」(工具) > 「Export Macros」(匯出巨集)，便可開啟「Select Keyboard Macros to Export」(選取要匯出的鍵盤巨集) 對話方塊。



2. 勾選和巨集對應的核取方塊或是使用「Select All」(全選) 或「Deselect All」(取消全選) 選項，來選取要匯出的巨集。
3. 按一下「OK」(確定)。隨即會顯示「鍵盤巨集匯出目標」對話方塊。尋找和選取巨集檔案。根據預設，巨集存在於桌面。
4. 選取可供儲存巨集檔案的資料夾，輸入該檔案的名稱，然後按一下「Save」(儲存)。如果該巨集已經存在，您便會收到警示訊息。選取「Yes」(是) 以覆寫現有巨集，或是選取「No」(否) 以關閉該警示而不覆寫巨集。



建置鍵盤巨集

▶ 若要建置巨集：

1. 按一下「Keyboard」(鍵盤) > 「Keyboard Macros」(鍵盤巨集)。隨即會出現「Keyboard Macros」(鍵盤巨集) 對話方塊。
2. 按一下「Add」(新增)，隨即會出現「Add Keyboard Macro」(新增鍵盤巨集) 對話方塊。
3. 在「Keyboard Macro Name」(鍵盤巨集名稱) 欄位中輸入巨集的名稱。這個名稱會在建立之後，顯示在「Keyboard」(鍵盤) 功能表中。
4. 從「Hot-Key Combination」(快速鍵組合) 欄位的下拉式清單中選取鍵盤組合。如此可讓您以預先定義的按鍵執行巨集。<選用>
5. 在「Keys to Press」(按鍵) 下拉式清單中，選取您要用來模擬按鍵以執行指令的每個按鍵。請依照按下的順序來選取按鍵。並在每次完成選擇之後，選取「Add Key」(新增按鍵)。每個選取的按鍵都會顯示在「Macro Sequence」(巨集組合) 欄位中，並會在每個選擇後面自動加上「Release Key」(發送按鍵) 指令。

例如，選取左邊的 **Ctrl + Esc** 來建立會關閉視窗的巨集。這在「Macro Sequence」(巨集組合) 方塊中會如下所示：

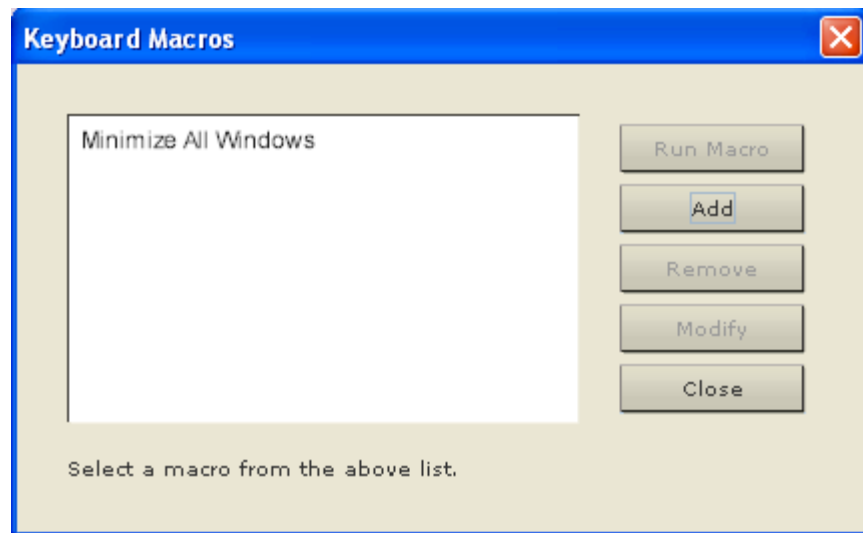
按下左邊的 Alt

按 F4

放開 F4

放開左邊的 Alt

6. 檢閱「Macro Sequence」(巨集組合) 欄位，確定已正確定義巨集組合。
 - a. 若要移除組合中的某個步驟，請選取該步驟，然後按一下「Remove」(移除)。
 - b. 若要變更組合中的步驟順序，請按一下步驟，然後按一下向上或向下箭頭按鈕，視需要重新排序。
7. 按一下「OK」(確定) 即可儲存巨集。按一下「Clear」(清除)，以清除所有欄位並從頭開始作業。按一下「OK」(確定) 時，隨即會出現「Keyboard Macros」(鍵盤巨集) 對話方塊，並列出新的鍵盤巨集。
8. 按一下「Close」(關閉) 以關閉在「Keyboard Macros」(鍵盤巨集) 對話方塊。該巨集隨即會出現在應用程式的「Keyboard」(鍵盤) 功能表上。選取功能表上的新巨集，或使用您指派給該巨集的按鍵來執行。



► 若要使用「將文字傳送至目標」的巨集功能：

1. 按一下「鍵盤」>「將文字傳送至目標」。隨即會出現「將文字傳送至目標」對話方塊。
2. 輸入您想要傳送至目標的文字。

附註：「將文字傳送至目標」功能不支援非英文字元。

3. 如果目標使用美式/國際通用鍵盤配置，請選取「目標系統設為美式/國際通用鍵盤配置」核取方塊。
4. 按一下「OK」(確定)。

執行鍵盤巨集

鍵盤巨集建立之後，您便可以使用指派給該巨集的鍵盤巨集，或是從「Keyboard」(鍵盤) 功能表選擇巨集來執行。

從功能表列執行巨集

建立巨集時，隨即會出現在「Keyboard」(鍵盤) 功能表下。若要執行鍵盤巨集，請在「Keyboard」(鍵盤) 功能表中按一下該巨集。

使用鍵盤組合執行巨集

若在建置巨集時已為其指派鍵盤組合，則只需按下指派的按鍵即可執行該巨集。例如，同時按下 CTRL+ALT+0 等鍵，即可將 Windows 目標伺服器上所有的視窗最小化。

修改和移除鍵盤巨集

▶ 若要修改巨集：

1. 選擇「Keyboard」(鍵盤) > 「Keyboard Macros」(鍵盤巨集)。隨即會出現「Keyboard Macros」(鍵盤巨集) 對話方塊。
2. 從列出的項目中選擇巨集。
3. 按一下「Modify」(修改)。隨即會開啟「Add/Edit Macro」(新增/編輯巨集) 對話方塊。
4. 請進行變更。
5. 按一下「OK」(確定)。

▶ 若要移除巨集：

1. 選擇「Keyboard」(鍵盤) > 「Keyboard Macros」(鍵盤巨集)。隨即會出現「Keyboard Macros」(鍵盤巨集) 對話方塊。
2. 從列出的項目中選擇巨集。
3. 按一下「Remove」(移除)。隨即會刪除該巨集。

與刀峰機架切換按鍵組合相同的快速鍵組合不會傳送到儲放在那些機架內的刀峰電腦。

視訊內容


重新整理畫面

「Refresh Screen」(重新整理畫面) 選項會強制重新整理視訊畫面。有數種方法可自動重新整理視訊設定：

- 「Refresh Screen」(重新整理畫面) 選項會強制重新整理視訊畫面。
- 「Auto-sense Video Settings」(自動感應視訊設定) 指令會自動偵測目標伺服器的視訊設定。

此外，您也可以使用「Video Settings」(視訊設定) 指令手動調整設定。


▶ **若要重新整理視訊設定，請執行下列其中一項動作：**

- 選擇「Video」(視訊) > 「Refresh Screen」(重新整理畫面) 或按一下工具列中的「Refresh Screen」(重新整理畫面) 按鈕 。

自動感應視訊設定

「Auto-sense Video Settings」(自動感應視訊設定) 指令會強制重新感應視訊設定 (解析度、螢幕更新頻率) 並重繪視訊畫面。

▶ **若要自動偵測視訊設定，請執行下列動作：**

- 選擇「Video」(視訊) > 「Auto-Sense Video Settings」(自動感應視訊設定) 或按一下工具列中的「Auto-Sense Video Settings」(自動感應視訊設定) 按鈕 。隨即會顯示訊息，表示正在進行自動調整。

調整視訊設定

使用「Video Settings」(視訊設定) 指令可手動調整視訊設定。

▶ **若要變更視訊設定：**

1. 選擇「Video」(視訊) > 「Video Settings」(視訊設定) 或按一下工具列中的「Video Settings」(視訊設定) 按鈕 ，即可開啟「Video Settings」(視訊設定) 對話方塊。
2. 視需要調整下列設定。您可在調整設定時立即看到效果：
 - a. 過濾雜訊

裝置可濾除顯示卡視訊輸出的電子干擾。此功能可最佳化圖片品質並減少頻寬用量。與周邊像素相較之下有大量的色彩變化存在時，較高的設定值才會傳送不同的像素。但設定過高的臨界值可能會意外濾除所需的畫面變更。

較低的設定值會傳送大部分的像素變更。此臨界值設定過低會導致較高的頻寬用量。

b. PLL 設定：

Clock (時脈) - 控制視訊像素透過視訊螢幕顯示的速度。變更時脈設定，將使得視訊影像水平拉長或縮短。建議使用奇數作為設定值。大多數情況都不必變更此設定，因為通常自動偵測即相當精準。

Phase (相位) - 相位值範圍介於 0 到 31 之間，並且會換行。請採用可讓使用中目標伺服器產生最佳視訊影像的相位值。

c. **Brightness (亮度)**: 使用此設定可調整目標伺服器顯示畫面的亮度。

d. **Brightness Red (紅色亮度)** - 控制紅色訊號的目標伺服器顯示畫面亮度。

e. **Brightness Green (綠色亮度)** - 控制綠色訊號的亮度。

f. **Brightness Blue (藍色亮度)** - 控制藍色訊號的亮度。

g. **Contrast Red (紅色對比)** - 控制紅色訊號對比。

h. **Contrast Green (綠色對比)** - 控制綠色訊號。

i. **Contrast Blue (藍色對比)** - 控制藍色訊號。

視訊影像若極為模糊或失焦，請調整時脈及相位的設定，直到使用中的目標伺服器出現較佳的影像為止。

警告：變更「Clock」(時脈) 與「Phase」(相位) 設定時請務必謹慎小心。此作業可能會導致視訊遺失或失真，而您可能無法回復之前的狀態。進行任何變更前，請先聯絡 **Raritan** 技術支援。

j. **Horizontal Offset (水平位移)** - 控制目標伺服器顯示畫面在監視器上的水平定位。

k. **Vertical Offset (垂直位移)** - 控制目標伺服器顯示畫面在監視器上的垂直定位。

3. 選取「Automatic Color Calibration」(自動色彩校準)，即可啟用此功能。

4. 選取視訊感應模式：

- 最佳可用視訊模式

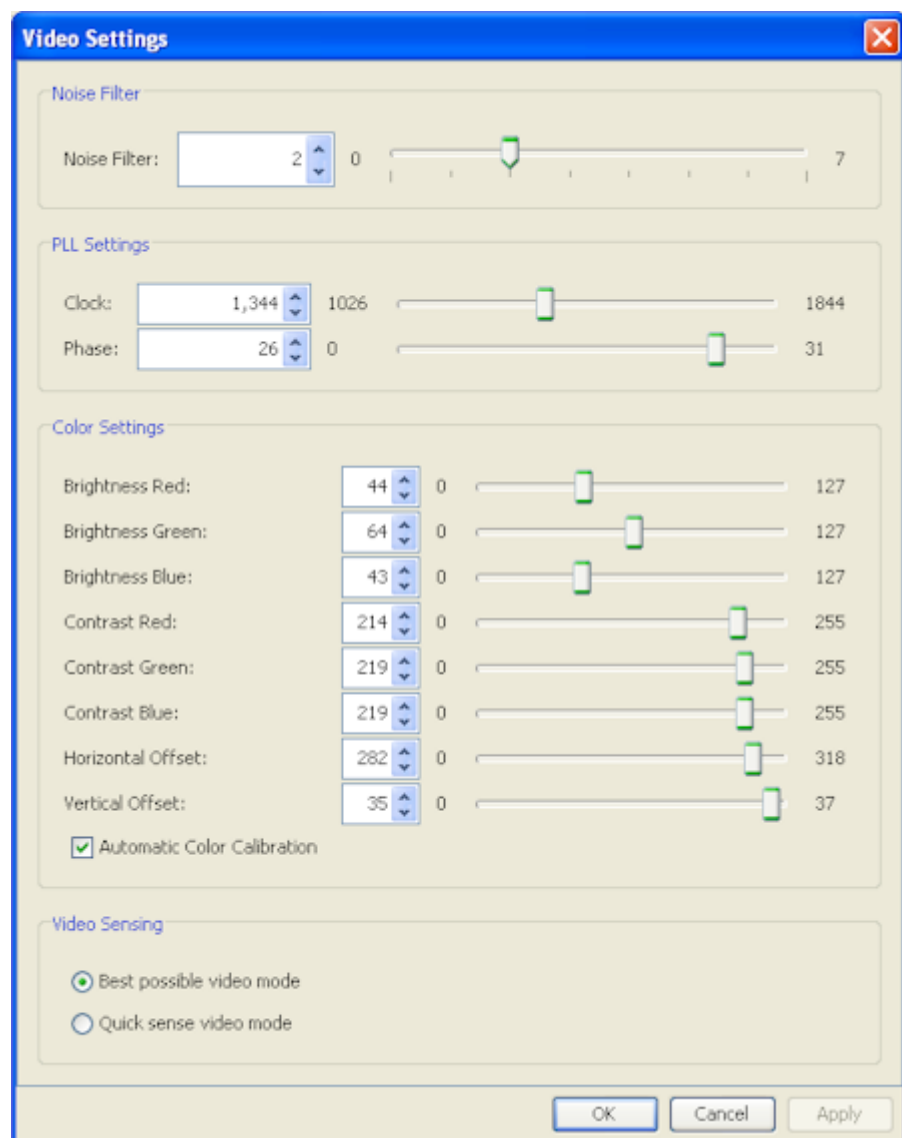
裝置在切換目標或目標解析度時，會執行完整的「自動感應」程序。選取此選項可校準視訊，以取得最佳影像品質。

- 快速偵測視訊模式

選取此選項，會使得裝置使用快速的視訊「自動感應」模式，以較快的速度顯示目標視訊。若要在重新開機後立即輸入目標伺服器的 BIOS 組態，此選項特別有幫助。

5. 按一下「OK」(確定)，即可套用設定，然後關閉對話方塊。按一下「Apply」(套用)，可套用設定但不會關閉對話方塊。


附註：某些 Sun 背景畫面 (如有深色邊框的畫面) 在特定 Sun 伺服器上，可能不會顯示在正中央的位置。請使用其他背景，或在螢幕左上角放置淺色圖示。

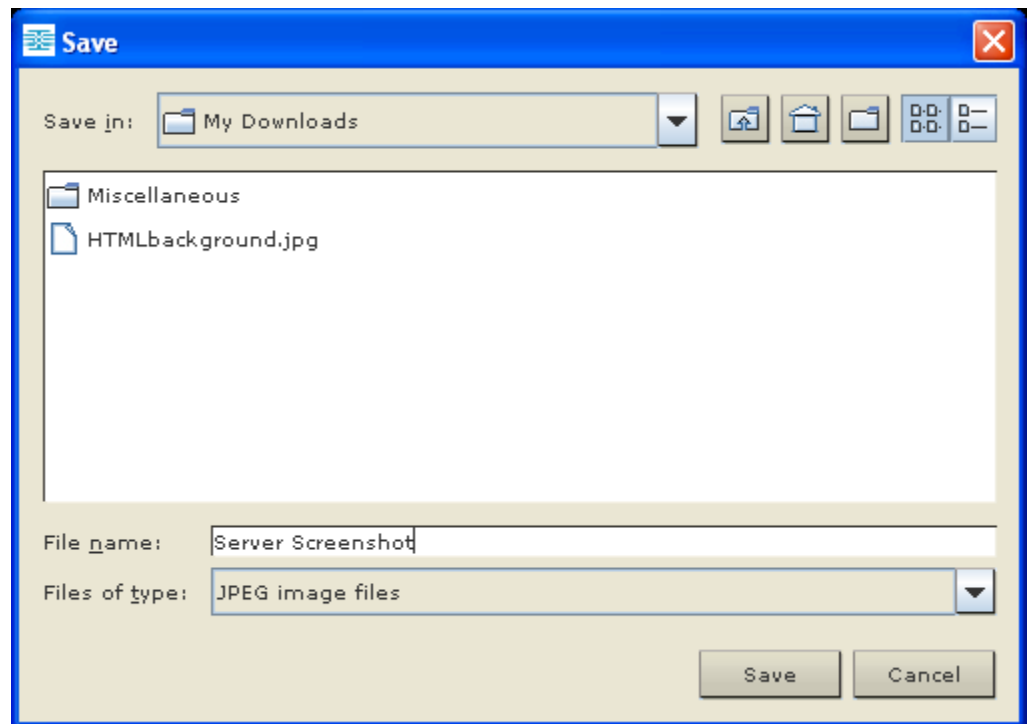


使用目標的螢幕擷取畫面

您可以從使用「Screenshot from Target」(目標的螢幕擷取畫面) 伺服器指令，擷取目標伺服器的螢幕擷取畫面。視需要將此螢幕擷取畫面儲存到您選擇的檔案位置，另存為點陣圖、JPEG 或 PNG 檔案。

▶ 若要擷取目標伺服器的螢幕擷取畫面：

1. 選取「Video」(視訊) > 「Screenshot from Target」(目標的螢幕擷取畫面) 或按一下工具列中的「Screenshot from Target」(目標的螢幕擷取畫面) 按鈕 。
2. 在「Save」(儲存) 對話方塊中，選擇要儲存檔案的位置，命名該檔案，然後從「Files of type」(檔案類型) 下拉式清單選取一種檔案格式。
3. 按一下「Save」(儲存) 以儲存螢幕擷取畫面。



變更最大螢幕更新頻率

如果目標上使用的視訊卡使用自訂軟體，而您是透過 MPC 或 VKC 存取目標，則必須變更監視器的最大螢幕更新頻率，螢幕更新頻率才會在目標上生效。

▶ **若要調整監視器螢幕更新頻率：**

1. 在 Windows® 中，選取「Display Properties」(顯示內容) > 「Settings」(設定值) > 「Advanced」(進階)，以開啟「Plug and Play」(隨插即用) 對話方塊。
2. 按一下「Monitor」(監視器) 索引標籤。
3. 設定「Screen refresh rate」(螢幕更新頻率)。
4. 按一下「OK」(確定)，再按一下「OK」(確定)，即可套用設定。

滑鼠選項

控制目標伺服器時，遠端主控台會顯示兩個滑鼠游標：一個屬於用戶端軟體工作站，另一個屬於目標伺服器。

您可以在單滑鼠模式或雙滑鼠模式下操作。處於雙滑鼠模式且已提供正確設定的選項時，兩個滑鼠游標即會對齊。

當有兩個滑鼠游標時，裝置會提供數種滑鼠模式：

- Absolute (絕對，滑鼠同步)
- Intelligent (智慧，滑鼠模式)
- Standard (標準，滑鼠模式)


滑鼠指標同步

從遠端檢視使用滑鼠的目標伺服器時，便會顯示兩個滑鼠游標：一個屬於遠端用戶端工作站，另一個則屬於目標伺服器。當滑鼠指標位於「虛擬 KVM 用戶端」目標伺服器的視窗內時，滑鼠的位移與按鍵動作會直接傳送到所連線的目標伺服器。移動時，因為滑鼠加速設定之故，用戶端滑鼠指標會略先於目標滑鼠指標。

若 LAN 連線的速度夠快，您可以停用虛擬 KVM 用戶端的滑鼠指標，只檢視目標伺服器的指標。您可切換使用這兩種模式（單滑鼠與雙滑鼠）。

滑鼠同步化祕訣

設定滑鼠同步時，請務必依照下列步驟進行：

1. 確認選取的視訊解析度與螢幕更新頻率在裝置可支援的範圍內。
「Virtual KVM Client Connection Info」(虛擬 KVM 用戶端連線資訊) 對話方塊會顯示裝置所見的實際值。
2. 若為 KX II 與 LX 裝置，請確認纜線長度並未超過所選取視訊解析度的特定限制。
3. 確認已在進行安裝程序時，正確設定滑鼠與視訊。
4. 按一下虛擬 KVM 用戶端的自動感應按鈕，即可強制進行自動感應。
5. 如果還是無法改善滑鼠同步的情況 (對於 Linux、UNIX 以及 Solaris KVM 目標伺服器)，請：
 - a. 開啟終端機視窗。
 - b. 輸入下列指令：`xset mouse 1 1`
 - c. 關閉終端機視窗。
6. 按一下「Virtual KVM Client mouse synchronization」(虛擬 KVM 用戶端的滑鼠同步) 按鈕 。


智慧滑鼠模式的其他注意事項

- 請確定螢幕的左上方沒有任何圖示或應用程式，因為會在該處進行同步化常式。
- 請勿使用動畫滑鼠。
- 停用 KVM 目標伺服器上的 Active Desktop。

同步化滑鼠

在雙滑鼠模式中，「Synchronize Mouse」(同步化滑鼠) 指令會強制重新對齊目標伺服器與「虛擬 KVM 用戶端」的滑鼠指標。

▶ 若要同步化滑鼠，請執行下列其中一項動作：

- 選擇「Mouse」(滑鼠) > 「Synchronize Mouse」(同步化滑鼠)；或按一下工具列中的「Synchronize Mouse」(同步化滑鼠) 按鈕 。

附註：此選項僅適用於「智慧」與「標準」滑鼠模式。

標準滑鼠模式

標準滑鼠模式使用相對滑鼠位置的標準滑鼠同步演算法。標準滑鼠模式必須停用滑鼠加速且正確設定其他滑鼠參數，才能讓用戶端與伺服器的滑鼠保持同步。

▶ 若要進入標準滑鼠模式：

- 選擇「Mouse」(滑鼠) > 「Standard」(標準)。

智慧滑鼠模式

在智慧滑鼠模式中，裝置可偵測目標滑鼠設定並據以同步化滑鼠游標，因而允許使用目標伺服器的滑鼠加速設定。智慧滑鼠模式是非 VM 目標的預設值。

進行同步化時，滑鼠游標會在螢幕左上角「跳動」並計算加速。必須符合特定的條件，此模式才能正常運作。

▶ 若要進入智慧滑鼠模式：

- 選擇「Mouse」(滑鼠) > 「Intelligent」(智慧)。

智慧滑鼠同步條件

您可以使用「Mouse」(滑鼠) 功能表提供的「Intelligent Mouse Synchronization」(智慧滑鼠同步) 指令，在滑鼠不在使用中時自動重新同步化滑鼠游標。不過，要讓此功能正常運作，必須符合下列條件：

- 應停用目標上的 **Active Desktop**。
- 目標頁面的左上角不應出現任何視窗。
- 目標頁面的左上角不應有動畫背景。
- 應使用一般而非動畫的目標滑鼠游標。
- 目標滑鼠的速度不應設為過快或過慢的值。
- 應停用像是「增強指標的準確性」或「將滑鼠迅速移至對話方塊中的預設按鈕」的進階滑鼠內容。
- 在「Video Settings」(視訊設定) 視窗中選擇「Best Possible Video Mode」(最佳可用視訊模式)。
- 目標視訊的邊緣必須清楚可見 (也就是說，當您捲動至目標視訊影像的邊緣時，目標桌面與遠端 KVM 主控台視窗之間應有可見的黑色邊框)。
- 使用智慧滑鼠同步功能時，桌面的左上角若有檔案圖示或資料夾圖示，可能會造成此功能無法正確運作。請務必避免在使用此功能時發生任何問題，Raritan 建議您不要在桌面的左上角放置檔案圖示或資料夾圖示。

自動感應目標視訊後，請按一下工具列上的「Synchronize Mouse」(同步化滑鼠) 按鈕，以手動初始化滑鼠同步。如果滑鼠游標在目標的解析度變更後開始出現彼此不同步的現象，也應該執行此動作。

如果智慧滑鼠同步失敗，此模式會回復到標準滑鼠同步行為。

請注意，不同的目標作業系統會有不同的滑鼠組態。如需進一步詳細資料，請參閱作業系統指導原則。另請注意，智慧滑鼠同步模式無法在 UNIX 目標中運作。

絕對滑鼠模式

此模式使用絕對座標讓用戶端與目標游標保持同步，即使目標滑鼠設定為其他加速或速度亦然。具有 USB 連接埠的伺服器都支援此模式，並且是 VM 及雙 VM 目標的預設模式。

▶ 若要進入絕對滑鼠模式：

- 選擇「Mouse」(滑鼠) > 「Absolute」(絕對)。

附註：使用絕對滑鼠設定時必須具備 USB 目標系統，建議對 KX II-101 使用此滑鼠設定。

附註：對於 KX II 裝置，滑鼠絕對同步只能搭配具虛擬媒體功能的 USB CIM (D2CIM-VUSB 與 D2CIM-DVUSB) 使用。

VKC 虛擬媒體

如需設定和使用虛擬媒體的完整資訊，請參閱 <虛擬媒體> (請參閱 "虛擬媒體" p. 69)一章。

工具選項

一般設定

▶ 若要設定工具選項：

1. 按一下「Tools」(工具) > 「Options」(選項)。隨即會出現「Options」(選項) 對話方塊。
2. 只有在技術支援部門的指導下，才能選取「Enable Logging」(啟用記錄) 核取方塊。此選項會在主目錄中建立記錄檔。
3. 請視需要從下拉式清單中選擇「Keyboard Type」(鍵盤類型)。此選項包括：
 - 美式鍵盤/國際通用
 - 法文鍵盤 (法國)
 - 德文鍵盤 (德國)
 - 日文
 - 英國
 - 韓文鍵盤 (南韓)
 - French (Belgium) (法文鍵盤 (比利時))
 - Norwegian (Norway) (挪威文鍵盤 (挪威))

- Portuguese (Portugal) (葡萄牙文 (葡萄牙))
- Danish (Denmark) (丹麥文鍵盤 (丹麥))
- Swedish (Sweden) (瑞典文鍵盤 (瑞典))
- German (Switzerland) (德文鍵盤 (瑞士))
- Hungarian (Hungary) (匈牙利文鍵盤 (匈牙利))
- Spanish (Spain) (西班牙文鍵盤 (西班牙))
- Italian (Italy) (義大利文鍵盤 (義大利))
- Slovenian (斯洛維尼亞文鍵盤)
- 轉譯：法文 - 美式
- 轉譯：法文 - 美式/國際通用

在 AKC 中，鍵盤預設為本機用戶端的鍵盤類型，因而此選項不適用。此外，KX II-101 與 KX II-101-V2 不支援單游標模式，因此「單游標模式」功能不適用於那些裝置。

4. 設定快速鍵：

- **Exit Full Screen Mode - Hotkey** (退出全螢幕模式 - 快速鍵)。當您進入「全螢幕」模式時，目標伺服器的顯示畫面會變成全螢幕，並取得與目標伺服器相同的解析度。此即為結束此模式所使用的快速鍵。
- **Exit Single Cursor Mode - Hotkey** (結束單游標模式 - 快速鍵)。當您進入單游標模式時，只會看見目標伺服器滑鼠游標。此即為用以結束單游標模式並恢復用戶端滑鼠游標的快速鍵。
- **Disconnect from Target - Hotkey** (與目標中斷連線 - 快速鍵)。啟用此快速鍵可讓使用者快速與目標中斷連線。

對於快速鍵組合，應用程式不允許您將同一組的快速鍵組合指派給多項功能。例如，如果已將 Q 套用到「Disconnect from Target」(與目標中斷連線) 功能，其便無法用於「Exit Full Screen Mode」(退出全螢幕模式) 功能。再者，如果快速鍵是因為升級而新增至應用程式，但該快速鍵的預設值已在使用中，便會改為將下一個可用的值套用於該功能。

5. 按一下「OK」(確定)。

鍵盤限制

土耳其文鍵盤

如果使用土耳其文鍵盤，您必須透過作用中 KVM 用戶端 (AKC) 來與目標伺服器連線。其他 Raritan 用戶端並不支援。

斯洛維尼亞文鍵盤

由於 JRE 限制使得斯洛維尼亞文鍵盤上的 < 鍵沒有作用。

Linux 上的語言組態

因為對於使用「System Preferences」(系統喜好設定) 來設定的外國語言鍵盤，Linux 上的 Sun JRE 無法產生正確的「Key Events」(按鍵事件)，因此 Raritan 建議您使用下表中說明的方法來設定外文鍵盤。

語言	設定方法
美式/國際通用鍵盤	預設
法文	Keyboard Indicator (鍵盤指示符)
德文	System Settings (Control Center) (系統設定 (控制中心))
日文	System Settings (Control Center) (系統設定 (控制中心))
英式鍵盤	System Settings (Control Center) (系統設定 (控制中心))
韓文	System Settings (Control Center) (系統設定 (控制中心))
比利時文鍵盤	Keyboard Indicator (鍵盤指示符)
挪威文	Keyboard Indicator (鍵盤指示符)
丹麥文	Keyboard Indicator (鍵盤指示符)
瑞典文	Keyboard Indicator (鍵盤指示符)
匈牙利文	System Settings (Control Center) (系統設定 (控制中心))
西班牙文	System Settings (Control Center) (系統設定 (控制中心))
義大利文	System Settings (Control Center) (系統設定 (控制中心))
斯洛維尼亞文	System Settings (Control Center) (系統設定 (控制中心))

語言	設定方法
	心))
葡萄牙文	System Settings (Control Center) (系統設定 (控制中心))

附註：使用 **Gnome** 做為桌面環境的 **Linux** 系統便應該使用「**Keyboard Indicator**」(鍵盤指示符)。

用戶端啟動設定

設定用戶端啟動設定，可讓您定義 **KVM** 階段作業的畫面設定。

附註：**LX** 裝置在 **MPC** 支援此功能。**LX** 在 **VKC** 與 **AKC** 不支援用戶端啟動設定。

▶ 若要設定用戶端啟動設定：

- 按一下「工具」>「選項」。隨即會出現「選項」對話方塊。
- 按一下「用戶端啟動設定」索引標籤。
 - 若要設定目標視窗設定：
 - 選取「標準 - 調整為目標解析度的大小」，以使用目標目前的解析度來開啟視窗。如果目標解析度大於用戶端解析度，目標視窗會儘可能容納畫面區域，並視需要加上捲軸。
 - 選取「全螢幕」即可以全螢幕模式開啟目標視窗。
 - 若要設定目標檢視器啟動的監視器：
 - 如果您想讓目標檢視器使用和用戶端所使用應用程式相同的畫面來啟動 (例如網頁瀏覽器或 **Applet**)，請選取「監視器用戶端啟動來源」。
 - 使用「從偵測到的監視器中選取」以從應用程式目前偵測到的監視器清單中選擇。如果無法再偵測到先前選取的監視器，即會顯示「未偵測到目前選取的監視器」。
 - 若要設定其他啟動設定：
 - 選取「啟用單游標模式」，可啟用單滑鼠模式做為存取伺服器時的預設滑鼠模式。
 - 選取「啟用調整視訊大小」，可在存取目標伺服器時自動調整顯示畫面的大小。
 - 選取「釘選功能表工具列」，在目標處於全螢幕模式時，仍可以看見工具列。根據預設，當目標處於全螢幕模式時，只有讓滑鼠暫留在螢幕畫面上方時，才可以看見功能表。

3. 按一下「確定」。

以 VKC 與 AKC 設定掃描設定

KX II 與 LX 提供可以搜尋所選取目標的連接埠掃描功能，並以投影片形式顯示，最多可讓您一次監視 32 個目標。您可以視需要連線到目標，或是將焦點放在特定目標。掃描功能可以找出標準目標、刀峰伺服器、層級 Dominion 裝置及 KVM 切換器連接埠等。請從虛擬 KVM 用戶端 (VKC) 或是作用中 KVM 用戶端 (AKC) 來設定掃描設定。如需詳細資訊，請參閱 <以 VKC 與 AKC 設定掃描設定>。請參閱 <掃描連接埠>。您可以使用「掃描設定」索引標籤，自訂掃描間隔與預設顯示選項。

▶ 若要設定掃描設定：

1. 按一下「工具」>「選項」。隨即會出現「選項」對話方塊。
2. 選取「掃描設定」索引標籤。
3. 在「顯示間隔 (10-255 秒)：」欄位中，指定要讓焦點停留在目標使其顯示在「連接埠掃描」視窗中央的秒數。
4. 在「Interval Between Ports (10 - 255 sec):」(連接埠間隔 (10-255 秒)) 欄位中，指定裝置應在連接埠間暫停的間隔。
5. 在「顯示」區段為「連接埠掃描」視窗的縮圖大小與分割方向變更預設的顯示選項。
6. 按一下「確定」。

檢視選項

檢視工具列

使用「虛擬 KVM 用戶端」時，可顯示也可不顯示工具列。

▶ 若要切換工具列顯示 (開啟和關閉)：

- 選擇「View」(檢視) > 「View Toolbar」(檢視工具列)。

檢視狀態列

根據預設，狀態列是顯示在目標視窗的底部。

▶ 若要隱藏狀態列：

- 按一下「View」(檢視) > 「Status Bar」(狀態列)，予以取消選取。

▶ 若要還原狀態列：

- 按一下「View」(檢視) > 「Status Bar」(狀態列)，即可加以選取。

縮放比例

您可以調整目標視窗大小，以檢視目標伺服器視窗的所有內容。這項功能可放大或縮小目標視訊的大小，使符合虛擬 KVM 用戶端視窗大小並維持外觀比例，讓您不使用捲軸亦可檢視整個目標伺服器桌面。

▶ 若要切換縮放比例 (開啟和關閉)：

- 選擇「View」(檢視) > 「Scaling」(縮放比例)。

全螢幕模式

當您進入「全螢幕」模式時，會以全螢幕顯示目標的畫面，並取得與目標伺服器相同的解析度。結束此模式所使用的快速鍵是在「Options」(選項) 對話方塊中指定，請參閱 <工具選項> (請參閱 "工具選項" p. 62)。

處於全螢幕模式時，將滑鼠移至畫面上方便會顯示全螢幕模式功能表列。如果您想在處於全螢幕模式時，仍可以看見功能表工具列，請從「Tool Options」(工具選項) 對話方塊啟用「Pin Menu Toolbar」(釘選功能表工具列) 選項。請參閱 <工具選項> (請參閱 "工具選項" p. 62)。

▶ 若要進入全螢幕模式：

- 選擇「View」(檢視) > 「Full Screen」(全螢幕)。

▶ 若要結束全螢幕模式：

- 按下在「Tools」(工具) 的「Options」(選項) 對話方塊中設定的快速鍵。預設值為 **Ctrl+Alt+M**。

若您想要一直以全螢幕模式存取目標，可讓全螢幕模式成為預設。

▶ 若要將全螢幕模式設定為預設模式：

1. 按一下「Tools」(工具) > 「Options」(選項)，以開啟「Options」(選項) 對話方塊。

2. 選取「Enable Launch in Full Screen Mode」(啟用以全螢幕模式啟動)，然後按一下「OK」(確定)。

說明選項

關於 Raritan 虛擬 KVM 用戶端

此功能表指令提供「虛擬 KVM 用戶端」的版本資訊，以備您要求「Raritan 技術支援部門」提供協助時之所需。

▶ **若要取得版本資訊：**

1. 請選取「Help」(說明) > 「About Raritan Virtual KVM Client」(關於 Raritan 虛擬 KVM 用戶端)。
2. 使用「Copy to Clipboard」(複製到剪貼簿) 將對話方塊中所含的資訊複製到剪貼簿檔案，之後可以在需要處理技術支援方面的問題時存取。

Ch 4

虛擬媒體

本章內容

概覽.....	70
使用虛擬媒體	76
連接虛擬媒體	77
中斷虛擬媒體的連線	79

概覽

虛擬媒體是藉由讓 KVM 目標伺服器從遠端存取用戶端電腦及網路檔案伺服器的媒體，來擴充 KVM 功能。透過此功能，用戶端電腦及網路檔案伺服器上所裝載的媒體，基本上就如同實際裝載在目標伺服器。然後目標伺服器便可讀取和寫入有如實際連接到目標伺服器的媒體。虛擬媒體包括內建和以 USB 裝載的 CD 及 DVD 光碟機、USB 大型存放裝置、電腦硬碟、軟碟機以及 ISO 映像檔 (磁碟映像檔)。

虛擬媒體提供從遠端執行其他工作的功能，例如：

- 傳輸檔案
- 執行診斷
- 安裝或修補應用程式
- 完整的作業系統安裝 (如果電腦 BIOS 支援的話)
- 有了這項擴充的 KVM 控制功能便無須再奔波往返資料中心，省下時間與金錢。

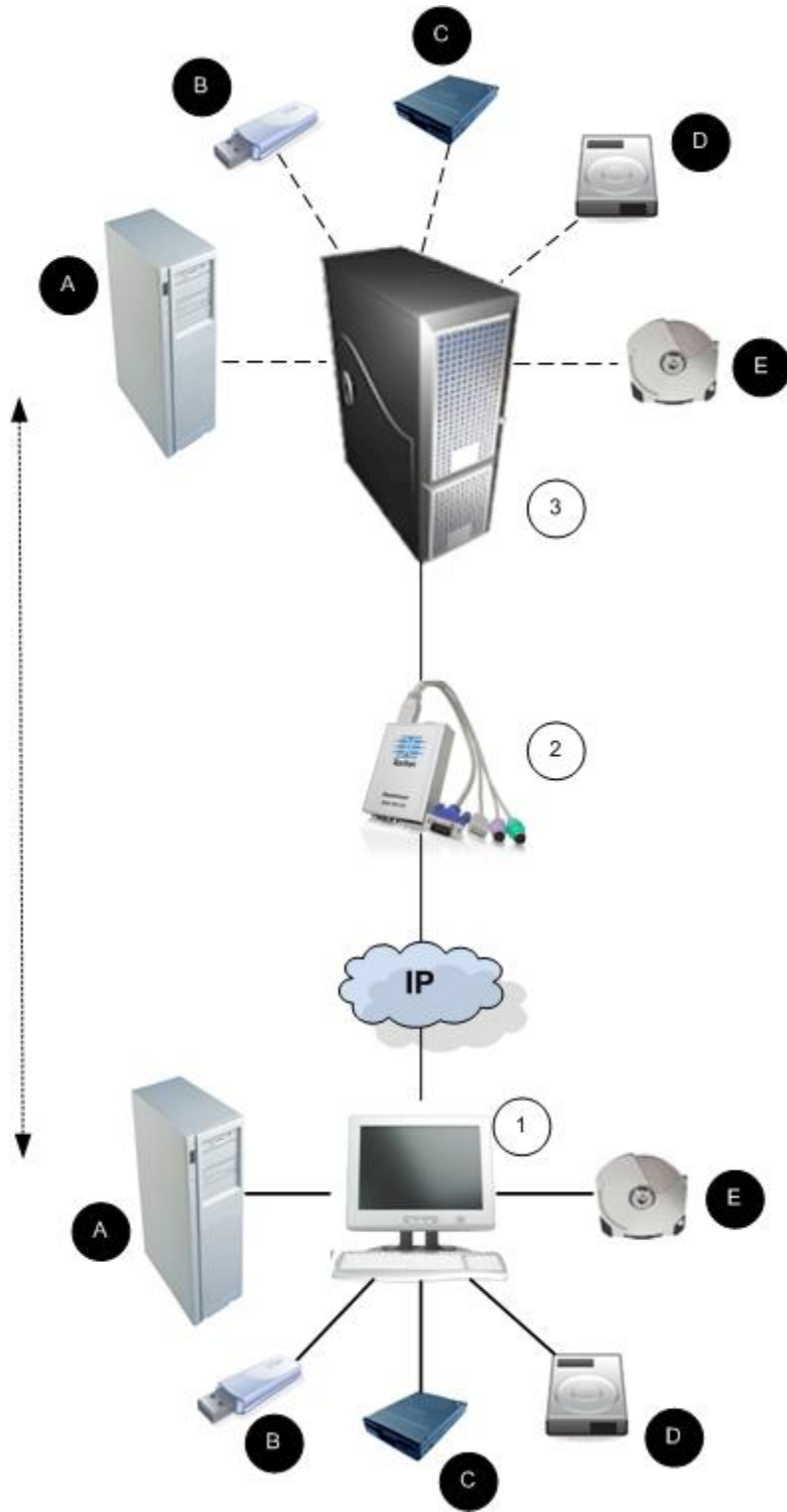
Windows®、Mac® 及 Linux™ 用戶端支援下列虛擬媒體類型：

- 內部及 USB 裝載的 CD 與 DVD 光碟機
- USB 大量儲存裝置
- 電腦硬碟
- ISO 映像檔 (磁碟映像檔)
- 數位音訊裝置*

附註：ISO9660 是力登支援的標準。不過，亦可使用其他 ISO 標準。

支援下列用戶端作業系統：

- Windows
- Mac OS X 10.5、10.6 及 10.7
- Red Hat Desktop 4.0 及 5.0
- Open SUSE 10、11
- Fedora 13 及 14



附註：如果使用虛擬媒體，便必須使用 USB 連線。

使用虛擬媒體的必要條件

使用虛擬媒體功能，您最多可裝載兩部不同類型的磁碟機，前提是該目標目前所套用的 USB 設定檔可以支援。這些磁碟機可在 KVM 階段作業期間提供存取。

例如，您可以裝載特定的 CD-ROM 並加以使用，然後在作業完成後中斷其連線。但 CD-ROM 虛擬媒體「通道」仍會保持開啟，以供您虛擬裝載其他 CD-ROM。在 KVM 階段作業結束前，而且只要 USB 設定檔可支援，這些虛擬媒體「通道」皆會保持為開啟狀態。

若要使用虛擬媒體，請將媒體連線/連接至要從目標伺服器存取的用戶端或網路檔案伺服器。這不一定是第一個步驟，但在嘗試存取此媒體之前請務必完成此步驟。

若要使用虛擬媒體，必須符合下列條件：**a**

Dominion 裝置

- 對於需要存取虛擬媒體的使用者，必須設定裝置權限允許存取相關的連接埠，並針對那些連接埠設定虛擬媒體存取權 (VM 存取連接埠權限)。連接埠權限會設定為群組層級。
- 裝置與目標伺服器之間必須要有 USB 連線存在。
- 如果您想要使用「PC-Share」(電腦共用)，就必須在「Security Settings」(安全性設定) 頁面中啟用「Security Settings」(安全性設定)。選用
- 您必須為正要連線的 KVM 目標伺服器選擇正確的 USB 設定檔。

用戶端 PC

- 使用者必須具備用戶端電腦的管理權限，才能使用特定虛擬媒體選項 (例如，完整磁碟機的重新導向)。

附註：如果使用 Microsoft Vista 或 Windows 7，請停用「使用者帳戶控制」或在啟動時 Internet Explorer，選擇「以系統管理員身分執行」。若要這樣做，請按一下「Start」(開始) 功能表，找到 IE，按一下滑鼠右鍵，然後選取「Run as Administrator」(以系統管理員身分執行)。

目標伺服器

- KVM 目標伺服器必須支援透過 USB 連接的磁碟機。
- 執行 Windows 2000 的 KVM 目標伺服器必須已安裝所有最新的修補程式。
- USB 2.0 連接埠不僅速度快，在此也是較好的選擇。

Windows XP 環境的虛擬媒體

如果在 Windows® XP 環境中執行虛擬 KVM 用戶端，使用者必須要有系統管理員權限，才能存取 CD-ROM 連線、ISO 及 ISO 映像檔以外的任何虛擬媒體類型。

Linux 環境的虛擬媒體

下列是有關使用虛擬媒體的 Linux® 使用者重要資訊。

超級使用者權限需求

如果您將 Linux 用戶端的 CD ROM 裝載於目標伺服器，然後卸載該 CD ROM，便會關閉虛擬媒體連線。裝載軟碟機後，將軟碟機移除時，也會關閉連線。您必須身為超級使用者，才能避免發生這些問題。

權限

使用者必須要有適當的存取權限，才能將磁碟機/CD-ROM 連線到目標。這可以利用下列指令來檢查：

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0
brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

在上述範例中，必須將權限變更為允許讀取存取權。

在利用其檔案公用程式支援 ACL 的系統上，ls 指令的行為會有下列變更：

- 對於有預設 ACL 的檔案或是包含三個以上必要 ACL 項目的存取 ACL，透過 ls -l 以 long 形式產生的 ls(1) 公用程式會在權限字串後面顯示一個加號 (+)。

此處為 /dev/sr0 提供的範例即指出這種情況，請使用 getfacl -a /dev/sr0 來查看是否已將存取權做為 ACL 的一部分提供給使用者。在此種情況下，使用者因而能將 CD-ROM 連線到目標，即使 ls -l 指令的輸出所指出的情況相反。

```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl: Removing leading '/' from absolute path names
# file: dev/sr0
# owner: root
# group: cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

可對卸除式裝置進行類似的權限檢查顯示如下：

```

guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
> getfacl -a /dev/sdb1
getfacl: Removing leading '/' from absolute path names
# file: dev/sdb1
# owner: root
# group: disk
user::rw-
group::rw-
other::---

```

下列要求將卸除式裝置的唯讀權限授與使用者：

```

root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

```

然後才能將該磁碟機連線到目標。

Mac 環境的虛擬媒體

下列是有關使用虛擬媒體的 Mac® 使用者重要資訊。

作用中的系統磁碟分割

- 您無法使用虛擬媒體來裝載 Mac 用戶端作用中的系統磁碟分割。

磁碟分割

- 現有的作業系統存有下列磁碟分割限制：
 - Windows 與 Mac 目標無法讀取 Linux 格式的磁碟分割
 - Windows® 與 Linux® 無法讀取 Mac 格式的磁碟分割
 - Linux 只支援 Windows FAT 磁碟分割
 - Mac 支援 Windows FAT 與 NTFS

- Mac 使用者必須卸載任何已裝載的裝置，才能連線到目標伺服器。使用 `>diskutil umount /dev/disk1s1` 來卸載該裝置，然後再使用 `diskutil mount /dev/disk1s1` 重新予以裝載。

無法使用讀取/寫入的情況

在下列情況下無法讀取/寫入虛擬媒體：

- 用於 Linux® 與 Mac® 用戶端時
- 用於所有硬碟時
- 磁碟機防寫時
- 使用者不具讀取/寫入權限時：
 - 連接埠權限的「Access」(存取) 設為「None」(無) 或「View」(檢視)
 - 連接埠權限的「VM Access」(VM 存取) 設為「Read-Only」(唯讀) 或「Deny」(拒絕)

使用虛擬媒體

在您開始使用虛擬媒體之前，請參閱 [〈使用虛擬媒體的必要條件〉](#) (請參閱 "使用虛擬媒體的必要條件" p. 72)。

▶ **若要使用虛擬媒體：**

1. 如果您計劃存取檔案伺服器 ISO 映像檔，請透過「遠端主控台」的「File Server Setup」(檔案伺服器設定) 頁面，識別這些檔案伺服器與映像檔。

附註：ISO9660 是 Raritan 支援的標準格式。不過，亦可能使用其他 CD-ROM Extension。

2. 以適當的目標伺服器開啟 KVM 階段作業。
 - a. 請從遠端主控台開啟「Port Access」(連接埠存取) 頁面。
 - b. 從「Port Access」(連接埠存取) 頁面連線到目標伺服器：
 - 按一下適當伺服器的「Port Name」(連接埠名稱)。
 - 從「Port Action」(連接埠動作) 功能表選擇「Connect」(連接) 指令。隨即會在「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗中開啟目標伺服器。
3. 連接虛擬媒體。

針對	選取此 VM 選項：
本機磁碟機	Connect Drive (連接磁碟機)

針對	選取此 VM 選項：
本機 CD/DVD 光碟機	連接 CD-ROM/ISO 映像檔
ISO 映像檔	連接 CD-ROM/ISO
檔案伺服器 ISO 映像檔	連接 CD-ROM/ISO

工作完成後，請中斷虛擬媒體的連線。請參閱 <中斷虛擬媒體的連線> (請參閱 "中斷虛擬媒體的連線" p. 79)。

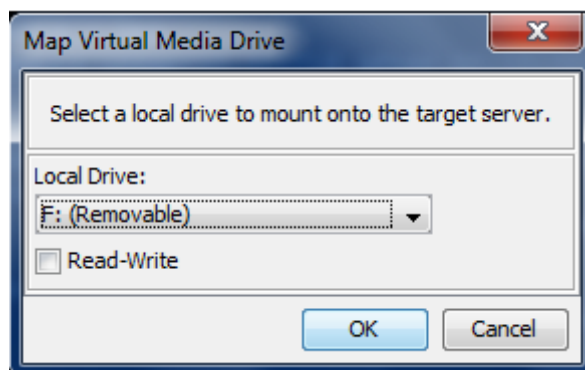
連接虛擬媒體

本機磁碟機

此選項可裝載整部磁碟機，表示整部磁碟機會虛擬裝載於目標伺服器上。此選項只適用於硬碟與外接式磁碟機。其中不包括網路磁碟機、CD-ROM 或 DVD-ROM 光碟機。這是唯一可進行讀取/寫入的選項。

▶ 存取用戶端電腦上的磁碟機：

- 請從「Virtual KVM Client」(虛擬 KVM 用戶端) 選擇「Virtual Media」(虛擬媒體) > 「Connect Drive」(連接磁碟機)。隨即會開啟「Map Virtual Media Drive」(對應虛擬媒體磁碟機) 對話方塊。()



- 選擇「Local Drive」(本機磁碟機) 下拉式清單中的磁碟機。
- 如需「讀取」與「寫入」功能，請選取「Read-Write」(讀寫) 核取方塊。若不是卸除式磁碟機，則會停用此選項。如需詳細資訊，請參閱 <無法使用讀取/寫入的情況> (請參閱 "無法使用讀取/寫入的情況" p. 76)。選取此選項後，即可讀取或寫入連接的 USB 磁碟。

警告：啟用「讀取/寫入」存取權具有其危險性。若同時有多個實體存取同一部磁碟機，可能會導致發生資料損毀。如果不需要「寫入」存取權，請勿選取此選項。

4. 按一下「OK」(確定)。便會在目標伺服器上虛擬裝載媒體。存取此媒體時，可以直接將其視為任何其他磁碟機。

裝載 CD-ROM/DVD-ROM/ISO 映像檔

此選項可裝載 CD-ROM、DVD-ROM 與 ISO 映像檔。

附註：ISO9660 是 Raritan 支援的標準格式。不過，亦可能使用其他 CD-ROM Extension。

▶ 若要存取 CD-ROM、DVD-ROM 或 ISO 映像檔：

1. 請從「Virtual KVM Client」(虛擬 KVM 用戶端) 選取「Virtual Media」(虛擬媒體) > 「Connect CD-ROM/ISO Image」(連接 CD-ROM/ISO 映像檔)。隨即會開啟「Map Virtual Media CD/ISO Image」(對應虛擬媒體 CD/ISO 映像檔) 對話方塊：
 2. 針對內建與外接 CD-ROM 或 DVD-ROM 光碟機：
 - a. 選擇「Local CD/DVD Drive」(本機 CD/DVD 光碟機) 選項。
 - b. 從「Local CD/DVD Drive」(本機 CD/DVD 光碟機) 下拉式清單中選擇磁碟機。所有可用的內建與外接 CD/DVD 磁碟機名稱，均會填入下拉式清單中。
 - c. 按一下「Connect」(連線)。
 3. 針對 ISO 映像檔：
 - a. 選擇「ISO Image」(ISO 映像檔) 選項。若要存取 CD、DVD 或硬碟的磁碟映像檔，請使用此選項。ISO 格式是唯一受支援的格式。
 - b. 按一下「Browse」(瀏覽)。
 - c. 瀏覽到所要使用之磁碟映像檔的所在路徑，然後按一下「Open」(開啟)。此路徑會填入「Image Path」(映像檔路徑) 欄位中。
 - d. 按一下「Connect」(連線)。
 4. 針對檔案伺服器的遠端 ISO 映像檔：
 - a. 選擇「Remote Server ISO Image」(遠端伺服器 ISO 映像檔) 選項。
 - b. 從下拉式清單中選擇「Hostname」(主機名稱) 與「Image」(映像檔)。您已使用「File Server Setup」(檔案伺服器設定) 頁面設定可用的檔案伺服器與映像檔路徑。而只有使用「File Server Setup」(檔案伺服器設定) 頁面所設定的項目，才會出現在下拉式清單中。
 - c. File Server Username (檔案伺服器使用者名稱) - 存取檔案伺服器所需的使用者名稱。此名稱可以包括網域名稱，例如 mydomain/username。

- d. File Server Password (檔案伺服器密碼) - 存取檔案伺服器所需的密碼 (輸入此欄位時會以遮罩處理)。
- e. 按一下「Connect」(連線)。

便會在目標伺服器上虛擬裝載媒體。存取此媒體時，可以直接將其視為任何其他磁碟機。

附註：如果在使用 Linux® 目標上的檔案，請在使用虛擬媒體複製檔案之後，使用 Linux 同步指令，如此才能檢視複製的檔案。除非完成同步，否則檔案不會出現。

附註：如果使用 Windows 7® 作業系統®，當您裝載本機 CD/DVD 磁碟機或是本機或遠端 ISO 映像檔時，在 Windows 的「我的電腦」資料夾中，預設不會顯示卸除式磁碟。若要在此資料夾中檢視本機 CD/DVD 磁碟機或是本機或遠端 ISO 映像檔，請選取「工具」>「資料夾選項」>「檢視」，然後取消選取「隱藏 [電腦] 資料夾中空的磁碟機」。

附註：因為受到協力廠商軟體的技術限制，所以您無法透過使用 IPv6 位址的虛擬媒體來存取遠端 ISO 映像檔。

中斷虛擬媒體的連線

▶ 若要中斷虛擬媒體磁碟機的連線：

- 若為本機磁碟機，請選擇「Virtual Media」(虛擬媒體) > 「Disconnect Drive」(中斷磁碟機連線)。
- 若為 CD-ROM、DVD-ROM 與 ISO 映像檔，請選取「Virtual Media」(虛擬媒體) > 「Disconnect CD-ROM/ISO Image」(中斷 CD-ROM/ISO 映像檔連線)。

附註：除了使用「Disconnect」(中斷連線) 指令外，直接結束 KVM 連線亦會關閉虛擬媒體的連線。

本章內容

使用者群組.....	80
使用者.....	86
驗證設定.....	90
變更密碼.....	101

使用者群組

每台 KX II-101-V2 裝置出貨時皆附有三個無法刪除的預設使用者群組：

使用者	說明
Admin (管理)	此群組成員的使用者有完整的管理權限。出廠預設的使用者即是此群組的成員，而且擁有一組完整的系統權限。此外，「Admin」(管理) 使用者必須身為「Admin」(管理) 群組的成員。
Unknown (不明)	此預設群組係供使用 LDAP/LDAPS 或 RADIUS 經外部驗證的使用者，或是供系統無法識別的使用者所用。如果外部 LDAP/LDAPS 或 RADIUS 伺服器無法識別出有效的使用者群組，即會使用「Unknown」(不明) 群組。此外，任何新建立的使用者都會放入此一群組，等待您指派給其他群組。
Individual Group (個別群組)	個別群組其實就是一個「群組」。也就是說，特定使用者自成一個群組，不屬於其他實際群組。在「Group Name」(群組名稱) 中會以“@”來識別個別群組。個別群組可讓使用者帳戶擁有跟群組一樣的權限。

在 KX II-101-V2 中最多可以建立 254 個使用者群組。

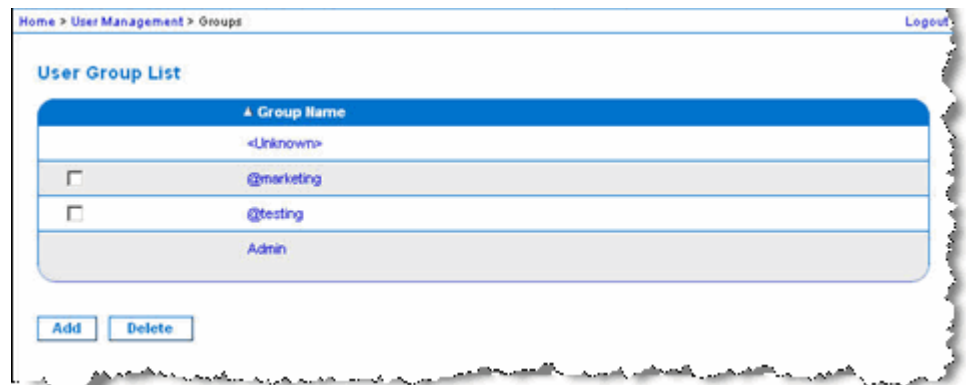
使用者群組清單

本機與遠端驗證皆會利用使用者群組 (透過 RADIUS 或 LDAP/LDAPS)。因為當您新增使用者時，必須將該使用者指定給現有的使用者群組，所以最好先定義使用者群組，然後再建立個別的使用者。

「使用者群組清單」頁面會顯示所有使用者群組的清單，按一下「群組名稱」欄標題即會以遞增或遞減的順序來排序清單。您也可以在此「使用者群組清單」頁面新增、修改或刪除使用者群組。

▶ 若要列出使用者群組：

- 選擇「使用者管理」>「使用者群組清單」。隨即會開啟「使用者群組清單」頁面。



使用者與群組之間的關聯性

使用者隸屬於群組，而群組則擁有權限。分組歸類各式 KX II-101-V2 使用者，可讓您一次管理一個群組中所有使用者的權限，而非逐一管理各使用者權限，進而節省時間。

您也可以選擇不讓特定使用者與群組建立關聯。在此種狀況下，您可將使用者分類為「個別」群組。

驗證成功時，裝置會使用群組資訊判斷使用者的權限，例如該使用者可以存取的伺服器連接埠、是否允許將裝置重新開機，以及其他功能。

新增使用者群組

▶ 若要新增使用者群組：

- 選取「使用者管理」>「新增使用者群組」，或是在「使用者群組清單」頁面上，按一下「新增」。
- 請在「Group Name」(群組名稱) 欄位中輸入新使用者群組的敘述性名稱 (最多 64 個字元)。

3. 在要指派給此群組下所有使用者的權限旁邊，選取核取方塊。請參閱 < [設定權限](#) > (請參閱 " [設定權限](#) " p. 84)。

設定連接埠權限

您可以為伺服器連接埠指定群組的存取類型，以及存取虛擬媒體與電源控制的連接埠類型。請注意，所有權限的預設設定皆為「Deny」(拒絕)。

連接埠存取權

選項	說明
Deny (拒絕)	完全拒絕存取
View (檢視)	檢視所連接目標伺服器的視訊 (但不與之互動)
Control (控制)	控制所連接的目標伺服器。如果同時授與 VM 與電源控制存取權，則必須將「Control」(控制) 權限指派給該群組。

VM 存取權

選項	說明
拒絕	完全拒絕連接埠的虛擬媒體權限。
唯讀	虛擬媒體存取僅限讀取存取權。
讀寫	可完整存取虛擬媒體 (讀取、寫入)

電源控制存取權

選項	說明
Deny (拒絕)	拒絕對目標伺服器進行電源控制
Access (存取)	可在目標伺服器上進行電源的完整權限

分組的 IP ACL (存取控制清單)

重要：使用分組的 IP 存取控制時，請務必謹慎小心。IP 位址如果落在拒絕存取的範圍內，即可能被阻擋在 KX II-101-V2 之外。

此功能限定只有在所選取特定 IP 位址範圍內的使用者，才能存取 KX II-101-V2 裝置。本功能僅適用於隸屬特定群組的使用者（會先行處理並具有優先權），不像「IP 存取控制清單」功能適用於所有對裝置的存取嘗試。

重要:KX II-101-V2 本機連接埠使用的 IP 位址為 127.0.0.1 且無法封鎖

請使用「Group」(群組) 頁面的「IP ACL」區段，針對各個群組範圍，新增、插入、取代以及刪除 IP 存取控制規則。

▶ **若要新增 (附加) 規則：**

1. 請在「Starting IP」(起始 IP) 欄位中輸入起始的 IP 位址。
2. 在「Ending IP」(結束 IP) 欄位中輸入結束的 IP 位址。
3. 從可用的選項中選擇動作：
 - Accept (接受) - 設定為「Accept」(接受) 的 IP 位址，才可以存取 KX II-101-V2 裝置。
 - Drop (捨棄) - 拒絕設定為「Drop」(捨棄) 的 IP 位址存取 KX II-101-V2 裝置。
4. 按一下「Append」(附加)。將規則加入為規則清單的最後一筆記錄。請為每個要輸入的規則重複步驟 1 到 4。

▶ **若要插入規則：**

1. 輸入規則編號 (#)。使用「Insert」(插入) 指令時必須要有規則編號。
2. 輸入「Starting IP」(起始 IP) 與「Ending IP」(結束 IP) 欄位。
3. 從「Action」(動作) 下拉式清單中選擇動作。
4. 按一下「Insert」(插入)。若剛才輸入的規則編號等於現有的規則編號，則新規則會放在現有規則的前面，而清單中所有規則都會向下移。

▶ **若要取代規則：**

1. 指定要取代的規則編號。
2. 輸入「Starting IP」(起始 IP) 與「Ending IP」(結束 IP) 欄位。

3. 從下拉式清單中選擇「Action」(動作)。
4. 按一下「Replace」(取代)。新規則會取代規則編號相同的原規則。

▶ **若要刪除規則：**

1. 指定要刪除的規則編號。
2. 按一下「Delete」(刪除)。
3. 當出現提示要求您確認刪除時，請按一下「OK」(確定)。

重要：ACL 規則的列出順序即為評估順序。例如，在此處的範例中，如果顛倒兩個 ACL 規則的順序，Dominion 即完全不接受任何通訊。

```
Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT
Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP
```

祕訣：規則編號可讓您對規則的建立順序擁有較多的控制。

設定權限

重要：選取「User Management」(使用者管理) 核取方塊，允許群組成員變更所有使用者的權限 (包括自己在內)。授權時請三思。

權限	說明
Device Access While Under CC-SG Management (受 CC-SG 管理時的裝置存取)	<p>在 CC-SG 針對裝置啟用「本機存取」功能時，允許擁有此權限使用者與使用者群組使用 IP 位址直接存取 KX II-101-V2。您可以從遠端主控台、MPC、VKC 及 AKC 存取該裝置。</p> <p>直接存取受 CC-SG 管理的裝置時，會在 KX II-101-V2 記錄存取與連線活動。根據 KX II-101-V2 驗證設定來執行使用者驗證。</p> <p><i>附註：根據預設，Admin (管理) 使用者群組會擁有此權限。</i></p>
Device Settings (裝置設定)	網路設定、日期/時間設定、連接埠組態 (通道名稱、電源關聯)、事件管理 (SNMP、Syslog)、虛擬媒體檔案伺服器設定
診斷	網路介面狀態、網路統計資料、偵測 (ping) 主機、追蹤主機路由、KX II-101-V2 診斷
維護	備份與還原資料庫、韌體升級、重設工廠預設值、

權限	說明
	重新開機
Modem Access (數據機存取)	使用數據機連線到 KX II-101-V2 裝置的權限。
PC-Share (電腦共用)	多位使用者同時存取相同目標
Security (安全性)	SSL 憑證、安全性設定 (VM 共用、電腦共用)、IP ACL
User Management (使用者管理)	使用者與群組管理、遠端驗證 (LDAP/LDAPS/RADIUS)、登入設定

設定個別群組的權限

▶ 若要設定個別使用者群組的權限：

1. 請從列出的群組中找出該群組。在「Group Name」(群組名稱) 中會以 @ 來識別個別群組。
2. 按一下「Group Name」(群組名稱)。隨即會開啟「Group」(群組) 頁面。
3. 選取適當的權限。
4. 按一下「OK」(確定)。

修改現有的使用者群組

附註：「Admin」(管理) 群組會啟用所有權限，而且無法變更。

▶ 若要修改現有的使用者群組：

1. 從「Group」(群組) 頁面變更適當的欄位，然後設定適當的權限。
2. 設定群組的「Permissions」(權限)。在要指派給此群組下所有使用者的權限前方，選取核取方塊。請參閱 <設定權限> (請參閱 "設定權限" p. 84)。
3. 設定「Port Permissions」(連接埠權限)。指定隸屬此群組的使用者可以存取的伺服器連接埠與存取類型。請參閱 <設定連接埠權限> (請參閱 "設定連接埠權限" p. 82)。
4. 設定「IP ACL」(選用)。此功能以指定 IP 位址的方式，來限制 KX II-101-V2 裝置的存取權。請參閱 <分組的 IP ACL (存取控制清單)> (請參閱 "分組的 IP ACL (存取控制清單)" p. 82)。

5. 按一下「OK」(確定)。

▶ **若要刪除使用者群組：**

重要：如果您刪除仍含有使用者的群組，系統便會將那些使用者自動指派給 **<unknown>** (不明) 使用者群組。

*祕訣：*若要判斷使用者是否屬於特定群組，請按照「使用者群組」排序「使用者清單」。

1. 請選擇「群組名稱」左邊的核取方塊，從列出的項目中選取群組。
2. 按一下「刪除」。
3. 當出現提示要求您確認刪除時，請按一下「確定」。

使用者

使用者必須有使用者名稱與密碼，才能存取 KX II-101-V2。此項資訊是用來驗證嘗試存取 KX II-101-V2 的使用者。

檢視 KX II-101-V2 使用者清單

「User List」(使用者清單) 頁面會顯示所有使用者的清單，包括其使用者名稱、全名以及使用者群組。按一下欄名稱，即可依任一欄排序此清單。您可以在「User List」(使用者清單) 頁面新增、修改或刪除使用者。

若要檢視每個使用者連線的目標連接埠，請參閱〈按連接埠檢視使用者〉。

▶ **若要檢視使用者清單：**

- 選擇「User Management」(使用者管理) > 「User List」(使用者清單)。隨即會開啟「User List」(使用者清單) 頁面。

按連接埠檢視使用者

「User By Ports」(按連接埠列出使用者) 頁面會列出所有經過驗證的本機與遠端使用者，以及他們所連線的連接埠。只列出有永久連線的連接埠。

如果同一個使用者從多個用戶端登入，頁面上由他們建立的每個連線都會顯示其使用者名稱。例如，如果使用者從兩 (2) 個不同的用戶端登入，他們的名稱就會列出兩次。

此頁面包含下列使用者與連接埠資訊：

- **Port Number** (連接埠編號) - 指派給使用者連線之連接埠的連接埠編號
- **Port Name** (連接埠名稱) - 指派給使用者連線之連接埠的連接埠名稱

附註：如果使用者未連線到目標，就會在「Port Name」(連接埠名稱) 下方，顯示「Local Console」(本機主控台) 或「Remote Console」(遠端主控台)。

- **Username** (使用者名稱) - 用於使用者登入與目標連線的使用者名稱
- **Access From** (存取來源) - 使用者所存取 KX II-101-V2 的 IP 位址
- **Status** (狀態) - 目前的連線狀態：「Active」(作用中) 或「Inactive」(閒置)

▶ 若要按連接埠檢視使用者：

- 選擇「User Management」(使用者管理) > 「User by Port」(按連接埠列出使用者)。隨即會開啟「User by Port」(按連接埠列出使用者) 頁面。

與連接埠的使用者中斷連線

與使用者中斷連線，會從目標連接埠與使用者中斷連線，而不會將他們登出 KX II-101-V2。

附註：將使用者登出，會從目標連接埠與使用者中斷連線，並將他們登出 KX II-101-V2。如需將使用者強制登出的資訊，請參閱<將使用者登出 KX II-101-V2 (強制登出)> (請參閱 "將使用者登出 KX II-101-V2 (強制登出)" p. 88)。

▶ 若要與連接埠的使用者中斷連線：

1. 選擇「User Management」(使用者管理) > 「Users by Port」(按連接埠列出使用者)。隨即會開啟「User by Port」(按連接埠列出使用者) 頁面。
2. 選取您要從目標與之中斷連線的人員使用者名稱旁邊的核取方塊。
3. 按一下「Disconnect User from Port」(與連接埠的使用者中斷連線)。

4. 在確認訊息上，按一下「OK」(確定)，來與使用者中斷連線。
5. 一則確認訊息會隨即顯示，指出已經與使用者中斷連線。

將使用者登出 KX II-101-V2 (強制登出)

如果您是管理員，可以將登入 KX II-101-V2 的任何驗證使用者登出。您也可以將連接埠層級與使用者中斷連線。請參閱 [〈與連接埠的使用者中斷連線〉](#) (請參閱 "與連接埠的使用者中斷連線" p. 87)。

▶ **若要將使用者登出 KX II-101-V2：**

1. 選擇「User Management」(使用者管理) > 「Users by Port」(按連接埠列出使用者)。隨即會開啟「User by Port」(按連接埠列出使用者) 頁面。
2. 選取您要從目標與之中斷連線的人員使用者名稱旁邊的核取方塊。
3. 按一下「Force User Logoff」(強制登出使用者)。
4. 在「Logoff User」(登出使用者) 確認訊息上，按一下「OK」(確定)。

新增使用者

因為當您新增使用者時，必須將該使用者指定給現有的使用者群組，所以最好先定義使用者群組，然後再建立 KX II-101-V2 使用者。請參閱 [〈新增使用者群組〉](#)。

您可以從「User」(使用者) 頁面新增使用者、修改使用者資訊以及重新啟動已停用的使用者。

附註：登入嘗試失敗次數超過「Security Settings」(安全性設定) 頁面中設定的登入嘗試次數上限時，該使用者名稱便會遭到停用。請參閱 [〈安全性設定〉](#) (請參閱 "安全性設定" p. 137)。

▶ **若要新增使用者：**

1. 選取「使用者管理」>「新增使用者」，或是在「使用者清單」頁面按一下「新增」。
2. 在「使用者名稱」欄位中，輸入唯一的名稱 (最多 16 個字元)。
3. 在「完整名稱」欄位中，輸入該人員的全名 (最多 64 個字元)。
4. 在「密碼」欄位中輸入密碼，並在「確認密碼」欄位再次輸入密碼 (最多 64 個字元)。
5. 從「使用者群組」下拉式清單中選擇群組。

如果不希望此使用者與現有的使用者群組產生關聯，請從下拉式清單中選取「Individual Group」(個別群組)。如需有關「Individual Group」(個別群組) 權限的相關資訊，請參閱 [〈設定個別群組的權限〉](#) (請參閱 "設定個別群組的權限" p. 85)。

- 若要啟動新使用者，請選取「作用中」核取方塊。按一下「確定」。

修改現有使用者

▶ **若要修改現有的使用者：**

- 選擇「User Management」(使用者管理) > 「User List」(使用者清單) 來開啟「User List」(使用者清單) 頁面。
- 請從「User List」(使用者清單) 頁面上列出的項目中找出該使用者。
- 按一下使用者名稱。隨即會開啟「User」(使用者) 頁面。
- 請在「User」(使用者) 頁面上，變更適當的欄位。如需如何存取「User」(使用者) 頁面的詳細資訊，請參閱 [〈新增使用者〉](#) (請參閱 "新增使用者" p. 88)。
- 若要刪除使用者，請按一下「Delete」(刪除)：隨即會出現提示要求您確認刪除。
- 按一下「OK」(確定)。

封鎖和解除封鎖使用者

管理員可以封鎖使用者對系統的存取權，或者根據安全性設定自動封鎖。請參閱 [〈使用者封鎖〉](#) (請參閱 "封鎖使用者" p. 140)。遭到封鎖的使用者會變成非使用中，而管理員只要讓使用者再次成為使用中，便可以解除封鎖。

▶ **若要封鎖或解除封鎖使用者：**

- 選擇「User Management」(使用者管理) > 「User List」(使用者清單)。隨即會開啟「User List」(使用者清單) 頁面。
- 選取或取消選取「Active」(使用中) 核取方塊。
 - 如果選取，會讓使用者處於使用中，並取得 KX II-101-V2 的存取權。
 - 如果取消選取，會讓使用者處於非使用中，而且無法存取 KX II-101-V2。
- 按一下「OK」(確定)。即會更新使用者的使用中狀態。

驗證設定

驗證是確認使用者所宣稱身分的程序。使用者一經驗證，使用者群組即可用以決定其系統與連接埠權限。使用者獲指派的權限可決定所允許的存取類型。此即稱之為授權。

當您設定 KX II-101-V2 進行遠端驗證時，外部驗證伺服器主要是用於驗證而非用於授權。

附註：選取遠端驗證 (LDAP/LDAPS 或 RADIUS) 時，如果找不到使用者，也將核對本機驗證資料庫。

▶ **若要設定驗證：**

1. 選擇「使用者管理」>「驗證設定」。隨即會開啟「驗證設定」頁面。
2. 選擇想要使用的驗證通訊協定選項 (本機驗證、LDAP/LDAPS 或 RADIUS)。選擇「LDAP」選項會啟用其餘的 LDAP 欄位；選取「RADIUS」選項則會啟用其餘的 RADIUS 欄位。
3. 如果選擇「本機驗證」，請進入步驟 6。
4. 如果選擇「LDAP/LDAPS」，請參閱〈實作 LDAP 遠端驗證〉一節，即可取得填寫「驗證設定」頁面上「LDAP」區段的各欄位詳細資訊。
5. 如果選擇「RADIUS」，請參閱〈執行 RADIUS 遠端驗證〉一節，即可取得填寫「驗證設定」頁面上「RADIUS」區段的各欄位詳細資訊。
6. 按一下「確定」即可儲存。

▶ **若要回復工廠預設值：**

- 按一下「重設為預設值」。


執行 LDAP/LDAPS 遠端驗證

輕量型目錄存取通訊協定 (LDAP/LDAPS) 是一種網路通訊協定，用於查詢和修改透過 TCP/IP 執行的目錄服務。用戶端連線到 LDAP/LDAPS 伺服器時，即會開始 LDAP 階段作業 (預設的 TCP 連接埠為 389)。接著，用戶端會向伺服器傳送作業要求，伺服器則會傳回回應。

提醒：Microsoft Active Directory 原本就是當作 LDAP/LDAPS 驗證伺服器。

▶ **若要使用 LDAP 驗證通訊協定：**

1. 按一下「User Management」(使用者管理) >「Authentication Settings」(驗證設定)，即會開啟「Authentication Settings」(驗證設定) 頁面。

2. 選取「LDAP」選擇鈕，以啟用頁面的「LDAP」區段。
3. 按一下  圖示，以展開頁面的「LDAP」區段。

伺服器組態設定

4. 在「Primary LDAP Server」(主要 LDAP 伺服器) 欄位中，輸入 LDAP/LDAPS 遠端驗證伺服器的 IP 位址或 DNS 名稱 (最多 256 個字元)。已選取「Enable Secure LDAP」(啟用安全的 LDAP) 選項與「Enable LDAPS Server Certificate Validation」(啟用 LDAPS 伺服器認證驗證) 選項時，便必須使用 DNS 名稱，以符合 LDAP 伺服器認證的 CN。
5. 在「Secondary LDAP Server」(次要 LDAP 伺服器) 欄位中，輸入備用 LDAP/LDAPS 伺服器的 IP 位址或 DNS 名稱 (最多 256 個字元)。已選取「Enable Secure LDAP」(啟用安全的 LDAP) 選項時，便必須使用 DNS 名稱。請注意，其餘欄位會與「Primary LDAP Server」(主要 LDAP 伺服器) 欄位共用相同設定。**選用**
6. 外部 LDAP 伺服器類型。
7. 選取外部 LDAP/LDAPS 伺服器類型。從可用的選項中選取：
 - Generic LDAP Server (一般 LDAP 伺服器)。
 - Microsoft Active Directory。Active Directory 是由 Microsoft 執行的 LDAP/LDAPS 目錄服務，以供在 Windows 環境下使用。
8. 如果選取 Microsoft Active Directory，請輸入 Active Directory 網域的名稱。例如 *acme.com*。請聯絡 Active Directory 管理員以取得特定網域名稱。
9. 在「User Search DN」(使用者搜尋 DN) 欄位中，輸入要開始搜尋使用者資訊的 LDAP 資料庫所在的伺服器識別名稱。最多可以使用 64 個字元。基本搜尋值的範例如下：
`cn=Users,dc=raritan,dc=com`。請聯絡驗證伺服器管理員，以取得可輸入這些欄位的適當值。
10. 在「DN of Administrative User」(管理使用者的 DN) 欄位中輸入管理使用者的識別名稱 (最多 64 個字元)。如果 LDAP 伺服器只允許管理員使用管理使用者角色來搜尋使用者資訊，請完成此欄位。請聯絡驗證伺服器管理員，以取得可輸入此欄位的適當值。「DN of Administrative User」(管理使用者的 DN) 值的範例如下：
`cn=Administrator,cn=Users,dc=testradius,dc=com`。**選用**

11. 如果您已輸入管理使用者的識別名稱，便必須輸入密碼，用來在遠端驗證伺服器驗證管理使用者的 DN。在「Secret Phrase」（通關密碼）欄位中輸入密碼，然後在「Confirm Secret Phrase」（確認通關密碼）欄位中再次輸入密碼（最多 128 個字元）。

Authentication Settings

Local Authentication

LDAP

RADIUS

▼ LDAP

Server Configuration

Primary LDAP Server
192.168.59.187

Secondary LDAP Server (optional)
192.168.51.214

Type of External LDAP Server
Microsoft Active Directory ▼

Active Directory Domain
testradius.com

User Search DN
cn=users,dc=testradius,dc=com

DN of Administrative User (optional)
cn=Administrator,cn=users,dc=testrac

Secret Phrase of Administrative User
●●●●●●●●

Confirm Secret Phrase

LDAP/LDAP 安全

12. 如果想要使用 SSL，請選取「Enable Secure LDAP」（啟用安全的 LDAP）核取方塊。如此便會啟用「Enable LDAPS Server Certificate Validation」（啟用 LDAPS 伺服器認證驗證）核取方塊。安全通訊端層 (SSL) 是一種加密通訊協定，允許 KX II-101-V2 與 LDAP/LDAPS 伺服器安全地進行通訊。
13. 預設連接埠為 389。請使用標準 LDAP TCP 連接埠或指定其他連接埠。

14. 「Secure LDAP Port」(安全的 LDAP 連接埠) 的預設連接埠為 636。請使用預設的連接埠或指定其他連接埠。只有在選取「Enable Secure LDAP」(啟用安全的 LDAP) 核取方塊時，才能使用此欄位。
15. 選取「Enable LDAPS Server Certificate Validation」(啟用 LDAPS 伺服器憑證驗證) 核取方塊，以使用先前上傳的 CA 憑證檔來驗證伺服器提供的憑證。如果您不想要使用先前上傳的根 CA 憑證檔，請不要選取此核取方塊。停用此功能，相當於接受由未知憑證授權單位簽署的憑證。只有在啟用「Enable Secure LDAP」(啟用安全的 LDAP) 核取方塊時，才能使用此核取方塊。

附註：選取「Enable LDAPS Server Certificate Validation」(啟用 LDAPS 伺服器認證驗證) 選項時，除了要使用根 CA 認證進行驗證外，伺服器主機名稱也必須符合伺服器認證中提供的一般名稱。

16. 視需要上載「根 CA 認證檔案」。選取「啟用安全 LDAP」選項時即會啟用此欄位。請洽詢驗證伺服器管理員，以取得 LDAP/LDAPS 伺服器 Base64 編碼 X-509 格式的 CA 認證檔案。使用「瀏覽」按鈕瀏覽到認證檔案。如果您以新的認證取代 LDAP/LDAPS 伺服器的認證，則必須重新啟動 KX II-101-V2 裝置，新的認證才會生效。

LDAP / Secure LDAP

Enable Secure LDAP

Port

Secure LDAP Port

Enable LDAPS Server Certificate Validation

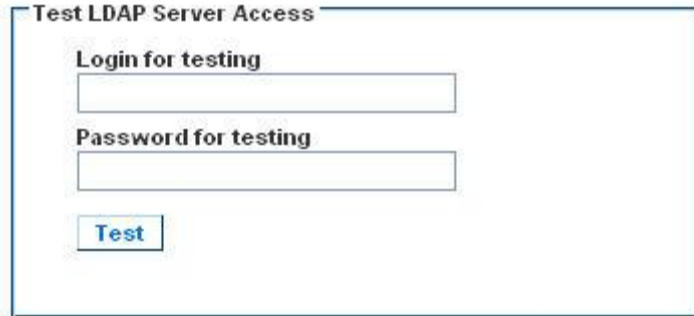
Root CA Certificate File

Note: Reboot device after certificate file is uploaded.

測試 LDAP 伺服器存取權

17. KX II-101-V2 能夠讓您從「Authentication Settings」(驗證設定) 頁面測試 LDAP 組態，因為要成功地設定 LDAP 伺服器與 KX II-101-V2 以進行遠端驗證，有時候會很複雜。若要測試 LDAP 組態，請在「Login for testing」(登入進行測試) 欄位與「Password for testing」(進行測試的密碼) 欄位中，分別輸入登入名稱與密碼。這就是您輸入以存取 KX II-101-V2 以及 LDAP 伺服器用來驗證您身分的使用者名稱與密碼。按一下「Test」(測試)。

測試完成之後，便會顯示一則訊息讓您得知測試成功，或者若測試失敗，則會顯示詳細的錯誤訊息。上面會顯示成功結果，或在失敗時顯示詳細的錯誤訊息。成功時，也會顯示為測試使用者從遠端 LDAP 伺服器擷取的群組資訊。



The image shows a dialog box titled "Test LDAP Server Access". Inside the dialog, there are two text input fields. The first is labeled "Login for testing" and the second is labeled "Password for testing". Below these fields is a button labeled "Test".

從 Active Directory 伺服器傳回使用者群組資訊

KX II-101-V2 支援對 Active Directory® (AD) 進行使用者驗證，而不需要在 KX II-101-V2 本機上定義使用者。如此即可專門在 AD 伺服器上保存 Active Directory 使用者帳戶與密碼。授權與 AD 使用者權限是透過標準 KX II-101-V2 原則與使用者群組權限 (於本機套用到 AD 使用者群組) 來控制與管理。

重要：如果您是力登電腦股份有限公司現有的客戶，而且已透過變更 AD 架構來設定 Active Directory 伺服器，則 KX II-101-V2 仍支援此組態，您無須執行下列作業。如需更新 AD LDAP/LDAPS 架構的詳細資訊，請參閱〈更新 LDAP 架構〉。

▶ 若要在 KX II-101-V2 啟用 AD 伺服器：

1. 使用 KX II-101-V2 建立特殊的群組，並為這些群組指派適當的權限。例如，您可以建立下列群組：KVM_Admin 與 KVM_Operator。
2. 在 Active Directory 伺服器上，使用前一步驟中的群組名稱建立同名的新群組。
3. 在 AD 伺服器上，將 KX II-101-V2 使用者指派給在步驟 2 建立的群組。
4. 在 KX II-101-V2 上，適當地啟用和設定您的 AD 伺服器。請參閱〈執行 LDAP/LDAPS 遠端驗證〉 (請參閱 "執行 LDAP/LDAPS 遠端驗證" p. 90)。

重要注意事項

- 群組名稱須區分大小寫。
- KX II-101-V2 提供下列無法變更或刪除的預設群組：Admin (管理) 與 <Unknown> (不明)。請確認您的 Active Directory 伺服器並未使用相同的群組名稱。
- 從 Active Directory 伺服器傳回的群組資訊若不符合 KX II-101-V2 群組組態設定，KX II-101-V2 便會自動將驗證成功的使用者指派給 <Unknown> (不明) 群組。

執行 RADIUS 遠端驗證

遠端驗證撥入使用者服務 (RADIUS) 是一種 AAA (驗證、授權與帳戶管理) 通訊協定，可供網路存取應用程式使用。

▶ 若要使用 RADIUS 驗證通訊協定：

1. 按一下「User Management」(使用者管理) >「Authentication Settings」(驗證設定)，即會開啟「Authentication Settings」(驗證設定) 頁面。
2. 按一下「RADIUS」選擇鈕，以啟用頁面的「RADIUS」區段。
3. 按一下  圖示，以展開頁面的「RADIUS」區段。
4. 分別在「Primary Radius Server」(主要 Radius 伺服器) 與「Secondary Radius Server」(次要 Radius 伺服器) 欄位中，輸入主要與所選用次要遠端驗證伺服器的 IP 位址 (最多 256 個字元)。
5. 在「Shared Secret」(共用密碼) 欄位中，輸入可供驗證使用的伺服器密碼 (最多 128 個字元)。

共用密碼是 KX II-101-V2 及 RADIUS 伺服器都必須知道的字元字串，如此兩者才能安全地進行通訊。它其實就是密碼。

6. 「Authentication Port」(驗證連接埠) 的預設連接埠是 1812，但是可視需要加以變更。
7. 「Accounting Port」(帳戶處理連接埠) 的預設連接埠是 1813，但是可視需要加以變更。
8. 「Timeout」(逾時) 是以秒為單位來記錄，而預設的逾時值為 1 秒，但是可視需要加以變更。

逾時是 KX II-101-V2 傳送其他驗證要求之前，等候 RADIUS 伺服器回應的時間長度。

9. 預設的重試次數是 3。

這是 KX II-101-V2 向 RADIUS 伺服器傳送驗證要求的次數。

10. 從下拉式清單的選項之中選擇「Global Authentication Type」(全域驗證類型)：

- PAP - 使用 PAP，以純文字格式傳送密碼。PAP 不是互動形式。一旦建立連線，使用者名稱與密碼即會當成一個資料封包傳送，而非伺服器傳送登入提示並等候回應。
- CHAP - 使用 CHAP，伺服器可隨時要求驗證。CHAP 提供的安全性比 PAP 高。

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication
 LDAP
 RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Secondary RADIUS Server

Shared Secret

Authentication Port
1812

Accounting Port
1813

Timeout (in seconds)
1

Retries
3

Global Authentication Type
PAP ▼

OK Reset To Defaults Cancel

透過 RADIUS 傳回使用者群組資訊

當 RADIUS 驗證嘗試成功時，KX II-101-V2 會根據使用者群組的權限，決定特定使用者的權限。

遠端 RADIUS 伺服器可透過傳回屬性 (以 RADIUS FILTER-ID 執行)，提供這些使用者群組的名稱。FILTER-ID 的格式如下：

Raritan:G{GROUP_NAME}，此處的 GROUP_NAME 為一個字串，代表使用者所屬群組的名稱。

RADIUS 通訊交換規格

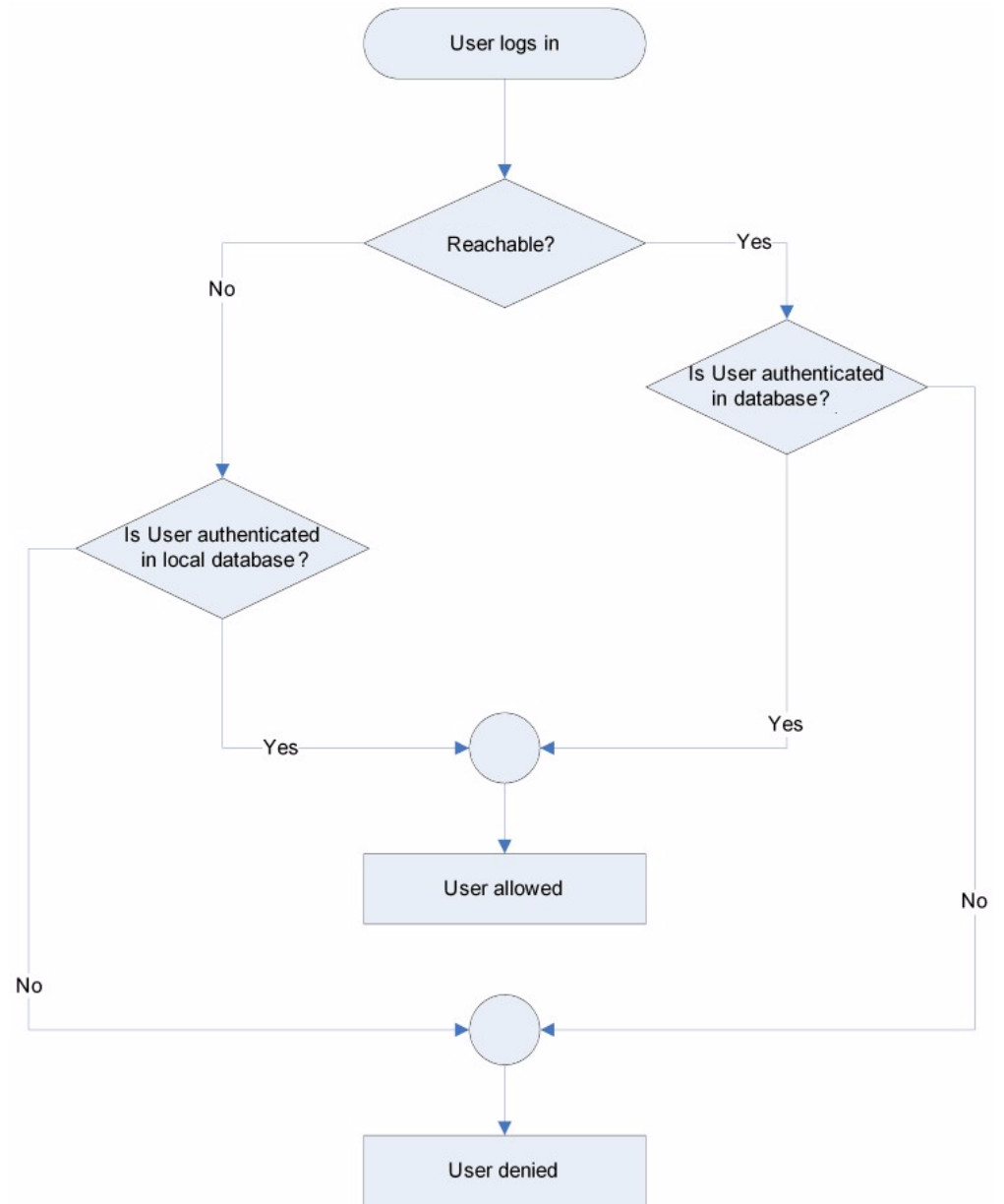
KX II-101-V2 會傳送下列 RADIUS 屬性給 RADIUS 伺服器：

屬性	資料
登入	
Access-Request (1)	
NAS-Port-Type (61)	用於網路連線的 VIRTUAL (5)。
NAS-IP-Address (4)	KX II-101-V2 的 IP 位址。
User-Name (1)	於登入畫面輸入的使用者名稱。
Acct-Session-ID (44)	用於帳戶處理的階段作業 ID。
User-Password(2)	加密的密碼。
Accounting-Request(4)	
Acct-Status (40)	Start(1) - 啟動帳戶處理。
NAS-Port-Type (61)	用於網路連線的 VIRTUAL (5)。
NAS-Port (5)	一律為 0。
NAS-IP-Address (4)	KX II-101-V2 的 IP 位址。
User-Name (1)	於登入畫面輸入的使用者名稱。
Acct-Session-ID (44)	用於帳戶處理的階段作業 ID。
登出	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - 停止帳戶處理
NAS-Port-Type (61)	用於網路連線的 VIRTUAL (5)。
NAS-Port (5)	一律為 0。

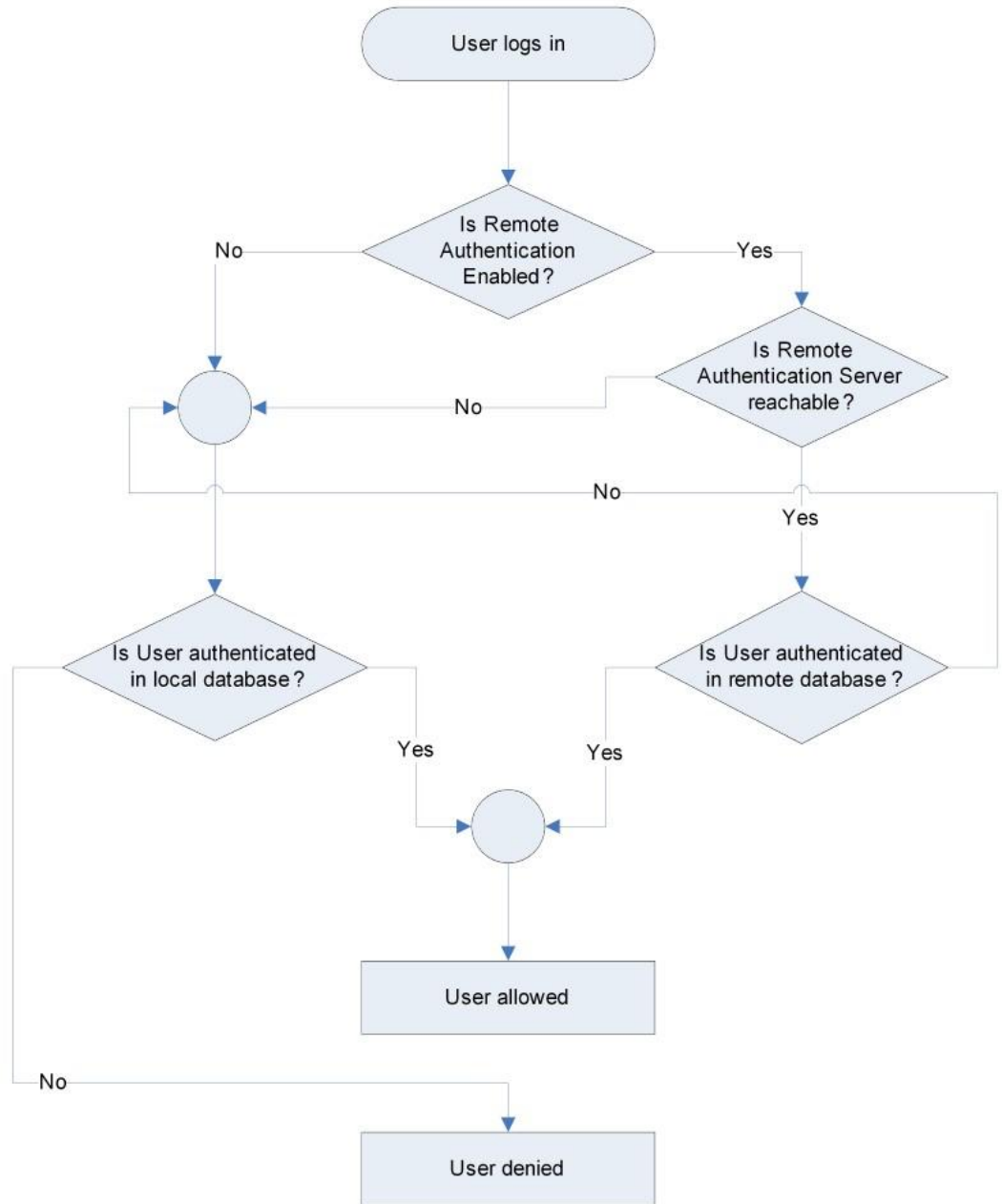
屬性	資料
NAS-IP-Address (4)	KX II-101-V2 的 IP 位址。
User-Name (1)	於登入畫面輸入的使用者名稱。
Acct-Session-ID (44)	用於帳戶處理的階段作業 ID。

使用者驗證程序

設定裝置來驗證和授權本機使用者時，驗證使用者認證的順序是依照下列程序進行：



依照下列流程圖中指定的程序進行遠端驗證：



變更密碼

▶ 若要變更密碼：

1. 選擇「User Management」(使用者管理) > 「Change Password」(變更密碼)。隨即會開啟「Change Password」(變更密碼) 頁面。
2. 在「Old Password」(舊密碼) 欄位中輸入目前的密碼。
3. 在「New Password」(新密碼) 欄位中輸入新密碼。在「Confirm New Password」(確認新密碼) 欄位中再次輸入新密碼。密碼長度最多可有 64 個字元，其中可包含英文的英數字元與特殊字元。
4. 按一下「OK」(確定)。
5. 您會收到已順利變更密碼的確認訊息。按一下「OK」(確定)。

附註：如果使用強固密碼，此頁面會顯示密碼所需格式的相關資訊。如需密碼與強固密碼的詳細資訊，請參閱<強固密碼> (請參閱 "強固密碼" p. 139)。

The screenshot shows a web interface for changing a password. At the top, there is a breadcrumb trail: "Home > User Management > Change Password". Below this is a blue header bar with the text "Change Password". The form contains three input fields: "Old Password", "New Password", and "Confirm New Password". At the bottom of the form, there are two buttons: "OK" and "Cancel".

本章內容

網路設定	102
裝置服務	107
鍵盤/滑鼠設定	111
序列連接埠設定	111
設定日期/時間設定	113
事件管理	114
連接埠組態.....	122
類比 KVM 切換器	130
使用「Reset」(重設) 按鈕重設 KX II-101-V2	131
變更預設的 GUI 語言設定	132

網路設定

使用「Network Settings」(網路設定) 頁面為 KX II-101-V2 裝置自訂網路組態 (如 IP 位址、探查連接埠及 LAN 介面參數)。

有兩個選項可以用來設定 IP 組態：

- None (default) (無 (預設值)) - 此為建議選項 (靜態 IP)。因為 KX II-101-V2 是網路基礎結構的一部分，一般都不希望其 IP 位址頻繁變更。此選項允許您設定網路參數。
- DHCP - 使用此選項，便會由 DHCP 伺服器自動指派 IP 位址。

▶ **若要變更網路組態：**

1. 選擇「Device Settings」(裝置設定) > 「Network」(網路)。隨即會開啟「Network Settings」(網路設定) 頁面。
2. 更新「Network Basic Settings」(網路基本設定)。請參閱 <網路基本設定> (請參閱 "網路基本設定" p. 103)。
3. 更新「LAN Interface Settings」(LAN 介面設定)。請參閱 <LAN 介面設定> (請參閱 "LAN 介面設定" p. 106)。
4. 按一下「OK」(確定) 設定上述組態。如果您的變更需要將裝置重新開機方能生效，便會出現重新開機的訊息。

▶ **若要重設出廠預設值：**

- 按一下「Reset to Defaults」(重設為預設值)。

網路基本設定

下列程序會說明如何使用「Network Settings」(網路設定) 頁面指派 IP 位址。如需有關此頁面全部欄位及作業的完整資訊，請參閱 <網路設定> (請參閱 "網路設定" p. 102)。

▶ 若要指派 IP 位址：

1. 選擇「Device Settings」(裝置設定) > 「Network」(網路)。隨即會開啟「Network Settings」(網路設定) 頁面。
2. 為 KX II-101-V2 裝置指定有意義的「Device Name」(裝置名稱)。最多可有 32 個英數字元，可包含有效的特殊字元，但不可包含空格。
3. 在 IPv4 區段中，輸入或選取適當的 IPv4 特定網路設定：
 - a. 視需要輸入「IP Address」(IP 位址)。預設的 IP 位址為 192.168.0.192。
 - b. 輸入「Subnet Mask」(子網路遮罩)。預設的子網路遮罩為 255.255.255.0。
 - c. 如果「IP Auto Configuration」(IP 自動組態) 下拉式清單選取「None」(無)，請輸入「Default Gateway」(預設閘道)。
 - d. 如果「IP Auto Configuration」(IP 自動組態) 下拉式清單選取「DHCP」，請輸入「Preferred DHCP Host Name」(慣用 DHCP 主機名稱)。
 - e. 選取「IP Auto Configuration」(IP 自動組態)。有以下選項可用：
 - None (無，靜態 IP) - 此選項需要手動指定網路參數。
此為建議選項，因為 KX II-101-V2 是基礎結構裝置，因此其 IP 位址不應變更。
 - DHCP - 由網路電腦 (用戶端) 使用動態主機設定通訊協定，從 DHCP 伺服器取得唯一的 IP 位址與其他參數。
使用此選項，則由 DHCP 伺服器指定網路參數。如果使用 DHCP，請輸入「Preferred host name」(慣用主機名稱，僅限 DHCP)。最多 63 個字元。
4. 如果使用 IPv6，請在 IPv6 區段中輸入或選取適當的 IPv6 特定網路設定：
 - a. 選取 IPv6 核取方塊以啟動該區段中的欄位。
 - b. 輸入「Global/Unique IP Address」(全域/唯一 IP 位址)。這是指派給 KX II-101-V2 的 IP 位址。
 - c. 輸入「Prefix Length」(首碼長度)。這是 IPv6 位址中使用的位元數目。

- d. 輸入「Gateway IP Address」(閘道 IP 位址)。
- e. Link-Local IP Address (連結本機 IP 位址)。這是自動指派給裝置的位址。用來進行芳鄰探索或是在沒有路由器存在時使用。**唯讀**
- f. Zone ID (區域 ID)。這會以相關聯的位址來識別裝置。**唯讀**
- g. 選取「IP Auto Configuration」(IP 自動組態設定)。有以下選項可用：
 - None (無) - 若不要自動 IP 組態，而偏好自行設定 IP 位址 (靜態 IP)，請使用此選項。此為預設及建議選項。

如果在「IP auto configuration」(IP 自動組態設定) 中選取「None」(無)，即會啟用下列網路基本設定欄位：「Global/Unique IP Address」(全域/唯一 IP 位址)、「Prefix Length」(首碼長度) 及「Gateway IP Address」(閘道 IP 位址)，讓您手動設定 IP 組態。
 - Router Discovery (路由器探索) - 除了只適用於直接連接之子網路的「連結本機」IPv6 位址以外，若要自動指派「全域」或「唯一」的本機 IPv6 位址，請使用此選項。
5. 如果選取「DHCP」，同時已啟用「Obtain DNS Server Address」(取得 DNS 伺服器位址)，請選取「Obtain DNS Server Address Automatically」(自動取得 DNS 伺服器位址)。選取「Obtain DNS Server Address Automatically」(自動取得 DNS 伺服器位址) 後，就會使用由 DHCP 伺服器提供的 DNS 資訊。
6. 如果選取「Use the Following DNS Server Addresses」(使用下列的 DNS 伺服器位址)，不論是否選取「DHCP」，都會使用在此區段中輸入的位址來連線到 DNS 伺服器。

如果選取「Use the Following DNS Server Addresses」(使用下列的 DNS 伺服器位址) 選項，請輸入下列資訊。若因為連線中斷而使主要 DNS 伺服器連線中斷，就會使用以下的主要與次要 DNS 位址。

 - a. Primary DNS Server IP Address (主要 DNS 伺服器 IP 位址)
 - b. Secondary DNS Server IP Address (次要 DNS 伺服器 IP 位址)
7. 完成後，請按一下「OK」(確定)。

如需在「Network Settings」(網路設定) 頁面中設定此區段的詳細資訊，請參閱 <LAN 介面設定> (請參閱 "LAN 介面設定" p. 106)。

附註：在某些環境中，「LAN Interface Speed & Duplex」(LAN 介面速度與雙工) 設定的「Autodetect」(自動偵測，自動交涉程式)，並不會正確設定網路參數，因而引發網路問題。在執行實例中，將 KX II-101-V2 的「LAN Interface Speed & Duplex」(LAN 介面速度與雙工) 欄位設為「100 Mbps/Full Duplex」(100 Mbps/全雙工) 或適合您網路的其他選項，即可解決此問題。如需詳細資訊，請參閱「Network Settings」(網路設定) (請參閱 "網路設定" p. 102) 頁面。

Basic Network Settings

Device Name *
se-kx2-232

IPv4 Address

IP Address: 192.168.51.55
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.51.126
Preferred DHCP Host Name:
IP Auto Configuration: DHCP

IPv6 Address

Global Unique IP Address: / Prefix Length:
Gateway IP Address:
Link-Local IP Address: N/A Zone ID: %1
IP Auto Configuration: None

Obtain DNS Server Address Automatically
 Use the Following DNS Server Addresses

Primary DNS Server IP Address: 192.168.59.2
Secondary DNS Server IP Address: 192.168.51.10

OK Reset To Defaults Cancel

LAN 介面設定

目前的參數設定會在「Current LAN interface parameters」(目前的 LAN 介面參數) 欄位中指出。

- 選取「LAN Interface Speed & Duplex」(LAN 介面速度與雙工)。
 - Autodetect (自動偵測，預設選項)
 - 10 Mbps/Half (半雙工) - 黃色 LED 指示燈會閃爍
 - 10 Mbps/Full (全雙工) - 黃色 LED 指示燈會閃爍
 - 100 Mbps/Half (半雙工) - 黃色 LED 指示燈會閃爍且綠色 LED 指示燈一直亮著
 - 100 Mbps/Full (全雙工) - 黃色 LED 指示燈會閃爍且綠色 LED 指示燈一直亮著

半雙工可提供雙向通訊，但一次一方 (不是同時)。

全雙工允許同時雙向通訊。

附註：採用半雙工或全雙工以 10 Mbps 的速度執行時，偶爾會發生問題。如果發生問題，請嘗試其他速度與雙工。

請參閱 <網路速度設定> (see "**Network Speed Settings**" p. 188)。

- 選取「Bandwidth Limit」(頻寬限制)。
 - 無限制
 - 128 KB
 - 256 KB
 - 512 KB
 - 2 MB
 - 5 MB
 - 10 MB
 - 100 MB

需要新的螢幕擷取畫面

裝置服務

您可以在「Device Services」(裝置服務) 頁面設定下列功能：

- 啟用 SSH 存取
- 輸入探查連接埠
- 啟用直接連接埠存取功能
- 啟用 Telnet 存取功能
- 設定 HTTP 與 HTTPS 設定
- 設定 SNMP 代理程式

啟用 Telnet

如果您想要使用 Telnet 來存取 KX II-101-V2，請先從 CLI 或瀏覽器存取 KX II-101-V2。

▶ 若要啟用 Telnet：

1. 選取「Device Settings」(裝置設定) > 「Device Services」(裝置服務)，然後選取「Enable TELNET Access」(啟用 TELNET 存取) 核取方塊。
2. 輸入 Telnet 連接埠。
3. 按一下「OK」(確定)。

啟用 Telnet 存取權之後，便可用來存取 KX II-101-V2 以及設定其餘參數。

啟用 SSH

「Enable SSH Access」(啟用 SSH 存取) 可讓管理員透過 SSH v2 應用程式存取 KX II-101-V2。

▶ 若要啟用 SSH 存取：

1. 選擇「裝置設定」> 「Device Services」(裝置服務)。就會開啟「Device Service Settings」(裝置服務設定) 頁面。
2. 選取「Enable SSH Access」(啟用 SSH 存取)。
3. 輸入「SSH Port」(SSH 連接埠) 資訊。標準的 SSH TCP 連接埠號碼為 22，但您可以變更該連接埠號碼，以提供更高層級的安全性作業。
4. 按一下「OK」(確定)。

HTTP 與 HTTPS 連接埠設定

您能夠設定 KX II-101-V2 使用的 HTTP 及 (或) HTTPS 連接埠。例如，如果您將預設 HTTP 連接埠 80 用於其他用途，變更連接埠可確保裝置不會嘗試使用該連接埠。

▶ 若要變更 HTTP 及 (或) HTTPS 連接埠設定：

1. 選擇「裝置設定」>「Device Services」(裝置服務)。就會開啟「Device Service Settings」(裝置服務設定) 頁面。
2. 在「HTTP Port」(HTTP 連接埠) 及 (或)「HTTPS Port」(HTTPS 連接埠) 欄位中，輸入新的連接埠。
3. 按一下「OK」(確定)。

輸入探查連接埠

KX II-101-V2 會透過單一的可設定 TCP 連接埠進行探查。預設的連接埠為 5000，不過您可設定使用任何 TCP 連接埠，但 80 及 443 除外。若要通過防火牆存取 KX II-101-V2 裝置，防火牆設定必須能夠透過預設連接埠 5000 或此處設定之非預設連接埠進行雙向通訊。

▶ 若要啟用探查連接埠：

1. 選擇「裝置設定」>「Device Services」(裝置服務)。就會開啟「Device Service Settings」(裝置服務設定) 頁面。
2. 輸入「Discovery Port」(探查連接埠)。
3. 按一下「OK」(確定)。

透過 URL 啟用直接連接埠存取

直接連接埠存取功能讓使用者不需要使用裝置的「Login」(登入) 對話方塊與「Port Access」(連接埠存取) 頁面。如果 URL 中未包含使用者名稱與密碼，此功能也可讓您直接輸入使用者名稱與密碼，然後繼續執行目標。

下列是有關直接連接埠存取功能的重要 URL 資訊：

如果使用 VKC 與直接連接埠存取功能：

- `https://IPaddress/dpa.asp?username=username&password=password&port=port number`

▶ 若要啟用直接連接埠存取：

1. 選擇「裝置設定」>「Device Services」(裝置服務)。就會開啟「Device Service Settings」(裝置服務設定) 頁面。

2. 如果您要讓使用者以 URL 傳送必要的參數，透過 Dominion 裝置來直接存取目標，請選取「Enable Direct Port Access via URL」(透過 URL 啟用直接連接埠存取)。
3. 按一下「OK」(確定)。

設定 SNMP 代理程式

稱為代理程式的 SNMP 相容裝置，會儲存有關其在管理資訊庫 (MIB) 中的資料，並將此資料傳回給 SNMP 管理員。如需檢視 KX II-101-V2 MIB 的資訊，請參閱 <檢視 KX II-101-V2 MIB> (請參閱 "檢視 KX II-101-V2 MIB" p. 119)。

KX II-101-V2 支援 SNMP v1/v2c 和 (或) v3 的 SNMP 記錄功能。SNMP v1/v2c 定義 SNMP 記錄功能啟用時的訊息格式與通訊協定操作。SNMP v3 是 SNMP 安全性擴充功能，可提供使用者驗證、密碼管理以及加密。

▶ 若要設定 SNMP 代理程式：

1. 選擇「裝置設定」>「Device Services」(裝置服務)。就會開啟「Device Service Settings」(裝置服務設定) 頁面。
2. 請提供 MIB-II 系統群組元件的下列 SNMP 代理程式識別碼資訊：
 - a. System Name (系統名稱) - SNMP 代理程式的名稱/裝置名稱
 - b. System Contact (系統連絡人) - 與裝置相關的連絡人名稱
 - c. System Location (系統位置) - 裝置的位置
3. 選取「Enable SNMP v1/v2c」(啟用 SNMP v1/v2c) 與「Enable SNMP v3」(啟用 SNMP v3)，或其中之一。您必須至少選取其中一個選項。<必要>
4. 完成下列的 SNMP v1/v2c 欄位 (視需要)：
 - a. Community (社群) - 裝置的社群字串
 - b. Community Type (社群類型) - 將「Read-Only」(唯讀) 或「Read-Write」(讀寫) 存取權授與社群使用者

附註：SNMP 社群是執行 SNMP 的裝置與管理工作站隸屬的群組。其可協助定義要傳送資訊的位置。社群名稱可使用來識別群組。SNMP 裝置或代理可能同時屬於多個 SNMP 社群。

5. 完成下列的 SNMP v3 欄位 (視需要)：
 - a. 如有必要，請選取「Use Auth Passphrase」(使用驗證密碼密語)。如果需要「Privacy Passphrase」(隱私權密碼密語)，「Use Auth Passphrase」(使用驗證密碼密語) 可讓兩者都使用相同的密碼密語，而不必再次輸入驗證密碼密語。

- b. **Security Name** (安全性名稱) - 與 **SNMP** 代理程式通訊的實體使用者名稱或服務帳戶名稱 (最多可有 32 個字元)
 - c. **Authentication Protocol** (驗證通訊協定) - **SNMP v3** 代理程式使用的 **MD5** 或 **SHA** 驗證通訊協定
 - d. **Authentication Passphrase** (驗證密碼密語) - 存取 **SNMP v3** 代理程式所需的密碼密語 (最多可有 64 個字元)
 - e. **Privacy Protocol** (隱私權通訊協定) - 適用的話, **AES** 或 **DES** 演算法可用來加密 **PDU** 與內容資料
 - f. **Privacy Passphrase** (隱私權密碼密語) - 用以存取隱私權演算法的密碼密語 (最多可有 64 個字元)
6. 按一下「OK」(確定), 啟動 **SNMP** 代理程式服務。

您可以按一下 **SNMP** 設陷組態設定的連結, 快速存取「事件管理 - 設定」頁面, 來設定 **SNMP** 設陷。如需建立 **SNMP** 設陷的資訊, 請參閱〈設定 **SNMP** 設陷〉, 而如需可用的 **KX II-101-V2 SNMP** 設陷清單, 請參閱〈**KX II-101-V2 SNMP** 設陷清單〉。

請在「**Event Management - Destination**」(事件管理 - 目的地) 頁面選取要在設定 **SNMP** 設陷後擷取的事件。請參閱〈設定事件管理 - 目的地〉。

SNMP Agent Configuration

Enable SNMP Daemon

System Name: DominionKX System Contact: System Location:

Enable SNMP v1/v2c;

Community: Community Type: Read-Only

Enable SNMP v3 Use Auth Passphrase

Security Name: Auth Protocol: MD5 Auth Passphrase: Privacy Protocol: None Privacy Passphrase:

[Link to SNMP Trap Configuration](#)

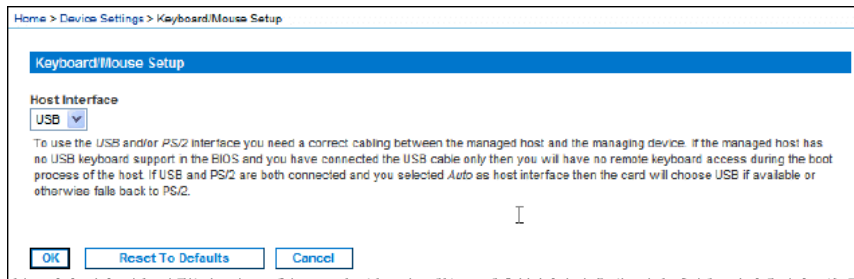
▶ **若要重設出廠預設值：**

- 按一下「**Reset to Defaults**」(重設為預設值)。頁面上的所有項目都會重設為預設值。

警告：透過 **UDP** 使用 **SNMP** 設陷時, 若 **KX II-101-V2** 已重新開機, **KX II-101-V2** 與其所連接的路由器可能會同步化失敗, 以防止記錄重新開機所完成的 **SNMP** 設陷。

鍵盤/滑鼠設定

使用「Keyboard/Mouse Setup」(鍵盤/滑鼠設定) 頁面，設定 KX II-101-V2 與主機裝置之間的鍵盤與滑鼠介面。



1. 按一下「Device Settings」(裝置設定) > 「Keyboard/Mouse」(鍵盤/滑鼠)。
2. 選取「Network Interface」(網路介面)。此選項可判斷 <ProductName> 是透過 PS/2 或 USB 連線，傳送鍵盤與滑鼠資料。
 - Auto (自動) - 使用此設定，如果有 USB 連線可用，KX II-101-V2 會優先採用，否則會預設為使用 PS/2 連線。
 - USB - 強制 KX II-101-V2 使用 USB 連線，將鍵盤與滑鼠資料傳送給主機裝置。
 - PS/2 - 強制 KX II-101-V2 使用 PS/2 連線，將鍵盤與滑鼠資料傳送給主機裝置。

附註：如果在搭配使用 KX II-101-V2 的前端上使用 Raritan 切換器，您必須將「Host Interface」(主機介面) 設定為 PS/2，組態設定才能正常運作。請參閱<類比 KVM 切換器> (請參閱“類比 KVM 切換器” p. 130)。

3. 按一下「OK」(確定)。
- ▶ 若要重設出廠預設值：
- 按一下「Reset to Defaults」(重設為預設值)。

序列連接埠設定

使用「Serial Port Settings」(序列連接埠設定) 頁面，設定 KX II-101-V2 如何使用其整合式序列連接埠。

Admin 連接埠

▶ 若要設定管理 (admin) 序列連接埠：

1. 選擇「Device Settings」(裝置設定) > 「Serial Port」(序列連接埠)。隨即會出現「Serial Port Settings」(序列連接埠設定) 頁面：
2. 選取「Admin Port」(管理連接埠) 選擇鈕。
3. 選擇其中一個選項，從用戶端電腦直接連接到 KX II-101-V2，並透過像是 Hyperterminal 的程式存取指令行介面。請參閱 <指令行介面 (CLI)> (請參閱 "指令行介面 (CLI)" p. 169)。
4. 在「Serial Settings」(序列設定) 區段中，設定下列欄位：
 - Speed (速度)
 - Stop Bits (停止位元)
 - Data Bits (資料位元)
 - Handshake (交握)
 - Parity (同位檢查)
5. 按一下「OK」(確定)。

Raritan 電源插座裝置控制

▶ 若要設定電源插座裝置序列連接埠：

1. 選擇「Device Settings」(裝置設定) > 「Serial Port」(序列連接埠)。隨即會開啟「Serial Port Settings」(序列連接埠設定) 頁面。
2. 選取「PowerStrip Control」(電源插座裝置控制) 選擇鈕。當 KX II-101-V2 連接到 Raritan 電源插座裝置時，便可以選擇此選項。
3. 按一下「OK」(確定)。

數據機

▶ 若要設定數據機序列連接埠：

1. 選擇「Device Settings」(裝置設定) > 「Serial Port」(序列連接埠)。隨即會開啟「Serial Port Settings」(序列連接埠設定) 頁面。
2. 選取「Modem」(數據機) 選擇鈕。將外接數據機連接到 KX II-101-V2 以提供撥接存取時，便可以選擇此選項。
3. 在「Modem Settings」(數據機設定) 區段中，設定下列欄位：
 - Serial line speed (序列線路速度)

- Modem init string (數據機 init 字串) - 啟用數據機存取必須使用欄位中顯示的預設字串。
 - Modem server IP address (數據機伺服器 IP 位址) - 在透過數據機連線之後，使用者輸入以存取 KX II-101-V2 網頁介面的位址。
 - Modem client IP address (數據機用戶端 IP 位址) - 在透過數據機連線之後，指派給使用者的位址。
4. 按一下「OK」(確定)。

請參閱 <數據機存取纜線連線> (請參閱 "數據機存取纜線連線" p. 113)，瞭解數據機存取適用之纜線連線的詳細資訊，並參閱 <經過認證的數據機> (請參閱 "經過認證的數據機" p. 184)，瞭解經過認證可與 KX II-101-V2 一起使用之數據機的詳細資訊。如需透過數據機連線到 KX II-101-V2 時使用哪些設定可達到最佳效能的詳細資訊，請參閱《KVM 與序列用戶端指南》中的 <在 MPC 中建立、修改及刪除設定檔>。

數據機存取纜線連線

使用下列纜線連線組態，將 KX II-101-V2 連接到數據機：

1. 連接管理 (admin) 序列纜線與 KX II-101-V2。
2. 連接 9 針腳公/公轉接頭與管理 (admin) 序列纜線。
3. 連接虛擬數據機纜線與轉接頭的另一端。
4. 連接 9 針腳公/公轉接頭與數據機纜線的另一端。
5. 在虛擬數據機纜線與數據機之間連接 DB9 對 DB25 (公) 數據機纜線。

設定日期/時間設定

使用「Date/Time Settings」(日期/時間設定) 頁面可指定 KX II-101-V2 的日期與時間。執行此作業的方法有兩種：

- 手動設定日期與時間。
- 與網路時間通訊協定 (NTP) 伺服器同步日期與時間。

▶ 若要設定日期與時間：

1. 選擇「裝置設定」>「日期/時間」。隨即會開啟「日期/時間設定」頁面。
2. 從「時區」下拉式清單中選擇時區。
3. 若要調整日光節約時間，請勾選「調整日光節約時間」核取方塊。
4. 選擇要用以設定日期與時間的方法：

- 使用者指定的時間 - 選擇此選項可手動輸入日期與時間。請對「使用者指定的時間」選項輸入日期與時間。時間請使用 hh:mm 格式 (使用 24 小時制)。
 - 與 NTP 伺服器同步 - 選擇此選項可與網路時間通訊協定 (NTP) 伺服器同步日期與時間。
5. 對於「與 NTP 伺服器同步」選項：
 - a. 輸入「主要時間伺服器」的 IP 位址。
 - b. 輸入「次要時間伺服器」的 IP 位址。**選擇性且非必要**
 6. 按一下「確定」。

事件管理

KX II-101-V2 事件管理功能可讓您啟用和停用將系統事件發送到 SNMP 管理程式、系統記錄及稽核記錄的功能。這些事件皆經過分類，而且您可針對每個事件，決定是否將其傳送到一或多個目的地。

設定事件管理 - 設定

在「Event Management - Settings」(事件管理 - 設定) 頁面設定 SNMP 設陷與系統記錄組態設定。請參閱〈設定 SNMP 設陷〉。

設定之後，請在「Event Management - Destinations」(事件管理 - 目的地) 頁面上，啟用 SNMP 設陷。請參閱〈設定事件管理 - 目的地〉。

設定 SNMP 設陷

簡易網路管理通訊協定 (SNMP) 是掌控網路管理以及監控網路裝置與其功能的通訊協定。透過網路送出 SNMP 設陷來收集資訊。在「Event Management - Settings」(事件管理 - 設定) 頁面上設定設陷。如需 KX II-101-V2 SNMP 設陷清單，請參閱〈KX II-101-V2 SNMP 設陷清單〉。

稱為代理程式的 SNMP 相容裝置，會儲存有關其在管理資訊庫 (MIB) 中的資料，並回應 SNMP 設陷。在「Device Services」(裝置服務) 頁面上，設定 SNMP 代理程式。如需設定 SNMP 代理程式的資訊，請參閱〈設定 SNMP 代理程式〉(請參閱 "設定 SNMP 代理程式" p. 109)，而如需檢視 KX II-101-V2 MIB 的資訊，請參閱〈檢視 KX II-101-V2 MIB〉(請參閱 "檢視 KX II-101-V2 MIB" p. 119)。

▶ 若要設定 SNMP (啟用 SNMP 記錄)：

1. 選擇「Device Settings」(裝置設定) > 「Event Management - Settings」(事件管理 - 設定)。隨即會開啟「Event Management - Settings」(事件管理 - 設定) 頁面：

2. 選取「已啟用 SNMP 記錄」以啟用其餘的核取方塊。<必要>
3. 選取「SNMP v1/v2c Traps Enabled」(已啟用 SNMP v1/v2c 設陷) 與「SNMP Trap v3 Enabled」(已啟用 SNMP 設陷 v3), 或是其中之一。您必須至少選取其中一個選項。選取之後, 就會啟用所有相關的欄位。<必要>
4. 完成下列的 SNMP v1/v2c 欄位 (視需要) :
 - a. Destination IP/Hostname (目的地 IP/主機名稱) - SNMP 管理員的 IP 或主機名稱。最多可以建立五 (5) 個 SNMP 管理員

附註：主機名稱的 IPv6 位址長度不可超過 80 個字元。

- b. Port Number (連接埠編號) - SNMP 管理員使用的連接埠編號
- c. Community (社群) - 裝置的社群字串

附註：SNMP 社群是執行 SNMP 的裝置與管理工作站隸屬的群組。其可協助定義要傳送資訊的位置。社群名稱可使用來識別群組。SNMP 裝置或代理可能同時屬於多個 SNMP 社群。

5. 如果尚未啟用, 請選取「SNMP Trap v3 Enabled」(已啟用 SNMP 設陷 v3) 核取方塊, 來啟用下列欄位。完成下列的 SNMP v3 欄位 (視需要) :
 - a. Destination IP/Hostname (目的地 IP/主機名稱) - SNMP 管理員的 IP 或主機名稱。最多可以建立五 (5) 個 SNMP 管理員
-
- 附註：主機名稱的 IPv6 位址長度不可超過 80 個字元。*
-
- b. Port Number (連接埠編號) - SNMP 管理員使用的連接埠編號
 - c. Security Name (安全性名稱) - 與 SNMP 代理程式通訊的實體使用者名稱或服務帳戶名稱 (最多可有 32 個字元)
 - d. Authentication Protocol (驗證通訊協定) - SNMP v3 代理程式使用的 MD5 或 SHA 驗證通訊協定
 - e. Authentication Passphrase (驗證密碼密語) - 存取 SNMP v3 代理程式所需的密碼密語 (最多可有 64 個字元)
 - f. Privacy Protocol (隱私權通訊協定) - 適用的話, AES 或 DES 演算法可用來加密 PDU 與內容資料
 - g. Privacy Passphrase (隱私權密碼密語) - 用以存取隱私權演算法的密碼密語 (最多可有 64 個字元)
6. 按一下「OK」(確定) 即可建立 SNMP 設陷。

使用「Link to SNMP Agent Configuration」(連至 SNMP 代理程式組態設定的連結)，以快速瀏覽到「Event Management - Settings」(事件管理 - 設定) 頁面。

請在「Event Management - Destination」(事件管理 - 目的地) 頁面選取要在設定 SNMP 設陷後擷取的事件。請參閱〈設定事件管理 - 目的地〉。

*KX II-101-V2 支援 SNMP v1/v2c 和 (或) v3 的 SNMP 記錄功能。
SNMP v1/v2c 定義 SNMP 記錄功能啟用時的訊息格式與通訊協定操作。
SNMP v3 是 SNMP 安全性擴充功能，可提供使用者驗證、密碼管理以及加密。*

▶ **若要編輯現有的 SNMP 設陷：**

1. 選擇「Device Settings」(裝置設定) > 「Event Management - Settings」(事件管理 - 設定)。隨即會開啟「Event Management - Settings」(事件管理 - 設定) 頁面：
2. 視需要進行變更，然後按一下「OK」(確定) 以儲存變更。

附註：如果您在任何時間停用 **SNMP** 設定，都會保留 **SNMP** 資訊，您若要重新啟用設定，就不必重新輸入。

▶ 若要刪除 **SNMP** 設陷：

- 清除所有 **SNMP** 設陷欄位，然後儲存。

使用重設為出廠預設值功能，來移除 **SNMP** 組態設定，以及將 **KX II-101-V2** 設定為其原始的出廠預設值。

警告：透過 **UDP** 使用 **SNMP** 設陷時，若 **KX II-101-V2** 已重新開機，**KX II-101-V2** 與其所連接的路由器可能會同步化失敗，以防止記錄重新開機所完成的 **SNMP** 設陷。

Home > Device Settings > Event Management - Settings

SNMP Traps Configuration

SNMP Logging Enabled SNMP v1/v2c Traps Enabled SNMP Trap v3 Enabled

SNMP v1/v2 Trap

Destination IP/Hostname	Port #	Community
	162	public
	162	public
	162	public
	162	public
	162	public

SNMP v3 Trap

Engine ID: 80001f8803000d5d03ca3b

Destination IP/Hostname	Port #	Security Name	Auth Protocol	Auth Passphrase	Privacy Protocol	Privacy Passphrase
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	
	162		MD5		None	

[Link to SNMP Agent Configuration](#)

[Click here to view the Dominion KX2 SNMP MIB](#)

KX II-101-V2 SNMP 設陷清單

SNMP 讓您可以傳送設陷或通知，警告管理員已符合一或多個條件。下表列出 **KX II-101-V2** 的 **SNMP** 設陷：

設陷名稱	說明
configBackup	已備份裝置的各項設定。
configRestore	已還原裝置的各項設定。
deviceUpdateFailed	裝置更新失敗。
deviceUpgradeCompleted	KX II-101-V2 已透過 RFP 檔案完成更新。
deviceUpgradeStarted	KX II-101-V2 已透過 RFP 檔案開始更新。

設陷名稱	說明
factoryReset	已將裝置重設為出廠預設值。
firmwareFileDiscarded	韌體檔案遭捨棄。
firmwareUpdateFailed	韌體更新失敗。
firmwareValidationFailed	韌體驗證失敗。
groupAdded	群組已新增至 KX II-101-V2 系統。
groupDeleted	已從系統刪除某個群組。
groupModified	已修改群組。
networkFailure	產品的乙太網路介面無法再透過網路進行通訊。
networkParameterChanged	已變更網路參數。
networkParameterChangedv2	已變更 KX II-101-V2 網路參數。
passwordSettingsChanged	已變更強固密碼設定。
portConnect	之前驗證過的使用者已開始 KVM 階段作業。
portConnectv2	先前驗證的 KX II-101-V2 使用者已開始 KVM 階段作業。
portConnectionDenied	對目標連接埠的連線遭拒絕。
portDisconnect	忙於 KVM 階段作業的使用者正確關閉階段作業。
portDisconnectv2	忙於 KVM 階段作業的 KX II-101-V2 使用者正確關閉階段作業。
portStatusChange	連接埠變為無法使用。
powerNotification	電源插座狀態通知：1= 作用中，0= 非作用中。
powerOutletNotification	電源插座裝置的插座狀態通知。
rebootCompleted	KX II-101-V2 已完成重新開機。
rebootStarted	KX II-101-V2 已開始重新開機，其是透過對系統重新開啟電源，或是從作業系統重新暖開機。
securityBannerAction	已接受或拒絕安全性標題。
securityBannerChanged	已變更安全性標題。
securityViolation	安全性違規。
setDateTime	已設定裝置的日期和時間。
setFIPSMODE	已啟用 FIPS 模式。

設陷名稱	說明
startCCManagement	裝置已處於 CommandCenter 管理之下。
stopCCManagement	裝置已從 CommandCenter 管理中移除。
userAdded	使用者已新增至系統。
userAuthenticationFailure	使用者嘗試登入，但沒有正確的使用者名稱及/或密碼。
userConnectionLost	擁有作用中階段作業的使用者遇到異常階段作業終止情況。
userDeleted	已刪除某個使用者帳戶。
userForcedLogout	管理員強制登出使用者
userLogin	使用者已成功登入 KX II-101-V2 並經過驗證。
userLogout	使用者已適當地成功登出 KX II-101-V2。
userModified	已修改使用者帳戶。
userPasswordChanged	若修改任何裝置使用者的密碼，便會觸發此事件。
userSessionTimeout	擁有作用中階段作業的使用者因逾時而導致階段作業終止。
userUploadedCertificate	使用者已載入 SSL 憑證。
vmlImageConnected	使用者嘗試在使用虛擬媒體的目標上裝載裝置或映像檔。每次嘗試對應 (裝載) 裝置/映像檔時都會產生此事件。
vmlImageDisconnected	使用者嘗試在使用虛擬媒體的目標上卸載裝置或映像檔。

檢視 KX II-101-V2 MIB

▶ 若要檢視 KX II-101-V2 MIB：

1. 選擇「Device Settings」(裝置設定) > 「Event Management - Settings」(事件管理 - 設定)。隨即會開啟「Event Management - Settings」(事件管理 - 設定) 頁面：
2. 按一下「Click here to view the Dominion KX2 SNMP MIB」(按此處即可顯示 Dominion KX2 SNMP MIB) 連結。使用瀏覽器視窗開啟 MIB 檔案。

附註：如果您擁有 MIB 檔案的「Read-Write」(讀寫) 權限，請使用 MIB 編輯器來變更檔案。

```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps
-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort

-- 07/08/11 H.
-- Corrected description for portStatusChange

-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList

-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction

-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateAndTime, setFIPSMODE
-- Also added defn for sysDateAndTime, fipsModeStatus

-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

系統記錄組態設定

▶ 若要設定系統記錄 (啟用系統記錄轉寄功能)：

1. 選取「Enable Syslog Forwarding」(啟用系統記錄轉寄功能)，將裝置訊息記錄在遠端的系統記錄伺服器中。
2. 在「IP Address/Hostname」(IP 位址/主機名稱) 欄位中輸入系統記錄伺服器的 IP 位址。
3. 按一下「OK」(確定)。

附註：主機名稱的 IPv6 位址長度不可超過 80 個字元。

使用重設為出廠預設值功能，來移除系統記錄組態設定，以及將 KX II-101-V2 設定為其原始的出廠預設值。

▶ 若要重設出廠預設值：

1. 按一下「Reset to Defaults」(重設為預設值)。

設定事件管理 - 目的地

系統事件若已啟用，會產生 SNMP 通知事件 (設陷) 或記錄到系統記錄或稽核記錄。使用「Event Management - Destinations」(事件管理 - 目的地) 頁面，選取要追蹤的系統事件以及此資訊的傳送目的地。

附註：只有選取「SNMP Logging Enabled」(SNMP 記錄已啟用)，才會產生 SNMP 設陷。只有選取「Enable Syslog Forwarding」(啟用系統記錄轉寄功能) 選項才會產生系統記錄事件。這兩個選項都位在「Event Management - Settings」(事件管理 - 設定) 頁面。請參閱〈設定事件管理 - 設定〉(請參閱 "設定事件管理 - 設定" p. 114)。

▶ 若要選取事件與其目的地：

1. 選擇「Device Settings」(裝置設定) > 「Event Management - Destinations」(事件管理 - 目的地)。隨即會開啟「Event Management - Destinations」(事件管理 - 目的地) 頁面。

系統事件依「Device Operation」(裝置作業)、「Device Management」(裝置管理)、「Security」(安全性)、「User Activity」(使用者活動) 以及「User Group Administration」(使用者群組管理) 分類。

2. 選取要啟用或停用之事件明細項目的核取方塊，以及要傳送資訊的位置。

祕訣：分別選取或清除「Category」(類別) 核取方塊，可啟用或停用整個類別。

3. 按一下「OK」(確定)。

▶ 若要重設出廠預設值：

- 按一下「Reset to Defaults」(重設為預設值)。

警告：透過 UDP 使用 SNMP 設陷時，若 KX II-101-V2 已重新開機，KX II-101-V2 與其所連接的路由器可能會同步化失敗，以防止記錄重新開機所完成的 SNMP 設陷。

連接埠組態

「Port Configuration」(連接埠組態) 頁面會顯示 KX II-101-V2 連接埠的清單。連接 KVM 目標伺服器或電源插座的連接埠會以藍色顯示，而且可供編輯。

▶ 若要變更連接埠組態：

1. 選擇「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態)。隨即會開啟「Port Configuration」(連接埠組態) 頁面。

排序

本頁最初是依連接埠號碼顯示，但按一下欄標題即可依任一欄位排序。

- **Port Name** (連接埠名稱) - 指派給連接埠的名稱。顯示空白的連接埠名稱表示您無法變更名稱，且該連接埠無法編輯；以藍色顯示的連接埠名稱才可編輯。

附註：連接埠名稱不得使用省略符號。

- **Port Type** (連接埠類型) - 連接到連接埠的目標類型：

連接埠類型	說明
PowerStrip (電源插座裝置)	電源插座裝置/PDU
KVM	KVM 目標

▶ 若要編輯連接埠名稱：

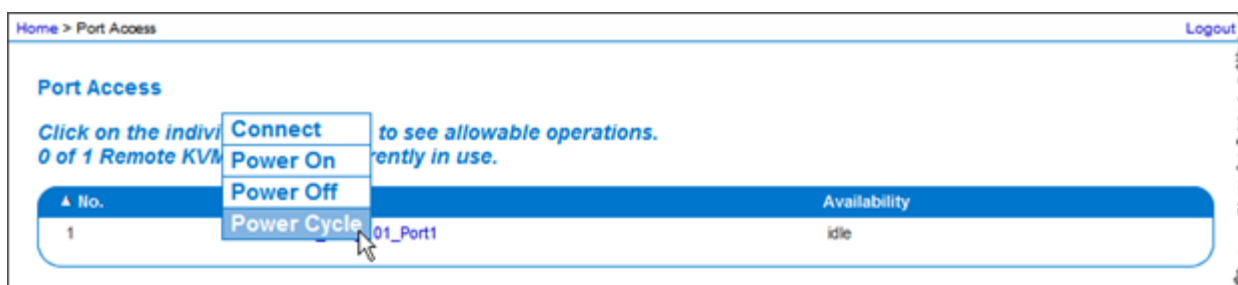
1. 對要編輯的連接埠，按一下「Port Name」(連接埠名稱)。
 - 若為 KVM 連接埠，隨即會開啟「Port」(連接埠) 頁面。您可在此頁面命名連接埠、建立電源關聯以及設定目標伺服器設定。
 - 若為電源插座裝置，隨即會開啟電源插座裝置的「Port」(連接埠) 頁面。您可在此頁面命名電源插座裝置及其插座。請參閱 < **電源控制** > (請參閱 "**電源控制**" p. 125)。

附註：只有當 Raritan 電源插座裝置已連接到 KX II-101-V2 並完成設定時，「Power Port 1」(電源連接埠 1) 連結才會啟用。否則，該連結會處於停用。

管理 KVM 目標伺服器 (連接埠頁面)

當您從「Port Configuration」(連接埠組態) 頁面選取連接到目標伺服器的連接埠時，隨即會開啟此「Port」(連接埠) 頁面。您可以在此頁面中，建立電源關聯，以及將「Port Name」(連接埠名稱) 變更為較具敘述性的名稱。

伺服器最多可有四個電源插頭，可分別與電源插座裝置建立關聯。您可以在此頁面中定義這些關聯，如此便可從「Port Access」(連接埠存取) 頁面開啟電源、關閉電源以及重新開啟伺服器電源，如下所示。



附註：若要使用此功能，您必須將 Raritan Dominion PX 電源插座裝置連接到裝置。請參閱〈連接電源插座裝置〉。

▶ 若要存取連接埠組態：

1. 選擇「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態)。隨即會開啟「Port Configuration」(連接埠組態) 頁面。
2. 對要編輯的連接埠，按一下「Port Name」(連接埠名稱)。

附註：只有當 Raritan 電源插座裝置已連接到 KX II-101-V2 並完成設定時，「Power Port 1」(電源連接埠 1) 連結才會啟用。否則，該連結會處於停用。

重新命名連接埠

▶ 若要變更連接埠名稱：

1. 輸入敘述姓名稱，例如目標伺服器的名稱。名稱最多可有 32 個英數字元，並可包含特殊字元。

附註：連接埠名稱不得使用省略符號。

2. 按一下「OK」(確定)。

有效的特殊字元

字元	說明	字元	說明
!	驚歎號	;	分號
"	雙引號	=	等號
#	井字號	>	大於符號
\$	貨幣符號	?	問號
%	百分比符號	@	@ 符號
&	連字號	[左角括號
(左括弧	\	反斜線
)	右括弧]	右角括號
*	星號	^	插入號
+	加號	_	底線
,	逗號	`	重音符號
-	破折號	{	左大括弧
.	句號		豎直線符號
/	正斜線	}	右大括弧
<	小於符號	~	波狀符號
:	冒號		

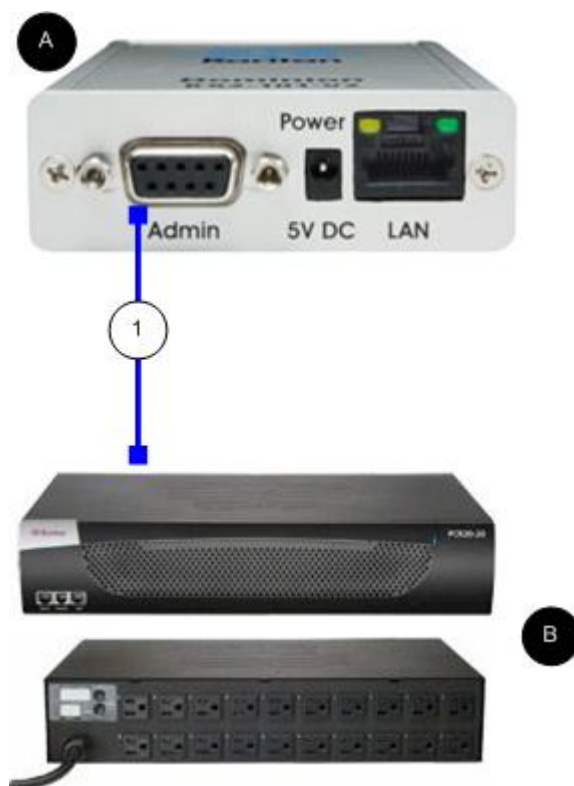
電源控制

KX II-101-V2 提供目標伺服器的遠端電源控制。若要使用此功能，您必須要有 Raritan 遠端電源插座裝置。

▶ 若要使用 KX II-101-V2 電源控制功能：

- 使用 DKX2-101-V2-PDU 接頭(未隨附，但可向經銷商或力登取得)將電源插座裝置連接到目標伺服器。請參閱〈[連接電源插座裝置](#)〉。
- 命名電源插座裝置(未隨附，但可向經銷商或力登取得)。請參閱〈[命名電源插座裝置\(電源插座裝置的連接埠頁面\)](#)〉 (see "[命名電源插座裝置 \(電源插座裝置的連接埠頁面\)](#)" p. 127)。
- 將電源插座裝置的插座關聯到目標伺服器。請參閱〈[管理 KVM 目標伺服器\(連接埠頁面\)](#)〉 (see "[管理 KVM 目標伺服器 \(連接埠頁面\)](#)" p. 123)。
- 在「Power Strip Device」(電源插座裝置) 頁面上，開啟和關閉電源插座裝置上的插座電源。請參閱〈[控制電源插座裝置](#)〉。

連接電源插座裝置



圖解	
	KX II-101-V2
	Raritan 電源插座裝置。
	從 KX II-101-V2 到 Raritan 電源插座裝置的 DKX2-101-V2-PDU (DB9-RJ45 轉接頭) 接頭 (未隨附)。

▶ 若要將 **KX II-101-V2** 連接到 **Raritan 電源插座裝置**：

1. 將 DKX2-101-V2-PDU (DB9-RJ45 轉接頭) 纜線連接到 KX II-101-V2 的 Admin (管理) 連接埠。
2. 使用 Cat5 纜線將 DKX2-101-V2-PDU 連接到 Raritan 電源插座裝置的序列連接埠接頭。
3. 將 AC 電源線接到目標伺服器以及電源插座裝置上的可用插座。
4. 將電源插座裝置接上 AC 電源。
5. 開啟 Raritan 電源插座裝置的電源。
6. 按一下「Device Settings」(裝置設定) > 「Serial Port」(序列連接埠)，隨即會開啟「Serial Port」(序列連接埠) 頁面。
7. 選取「Power Strip Control」(電源插座裝置控制) 選擇鈕，然後按一下「OK」(確定)。完成此動作後，便可以在遠端主控台上使用「Power」(電源) 功能表。

命名電源插座裝置 (電源插座裝置的连接埠頁面)

KX II-101-V2 一旦連接到 Raritan 遠端電源插座裝置時，該連接埠隨即會顯示在「Port」(連接埠) 頁面，而您可以從「Port Configuration」(連接埠組態) 頁面來開啟該連接埠。系統已預先填入「Type」(類型) 與「Name」(類型) 欄位。電源插座裝置中的各插座會顯示下列資訊：「Outlet Number」(插座編號)、「Name」(名稱) 及「Port Association」(連接埠關聯)。

使用此頁面命名電源插座裝置與其插座：所有名稱最多可有 32 個英數字元，並可包含特殊字元。

附註：當電源插座裝置與目標伺服器 (連接埠) 相關聯時，插座名稱即會由目標伺服器名稱所取代 (即使您對插座已指派其他名稱亦然)。

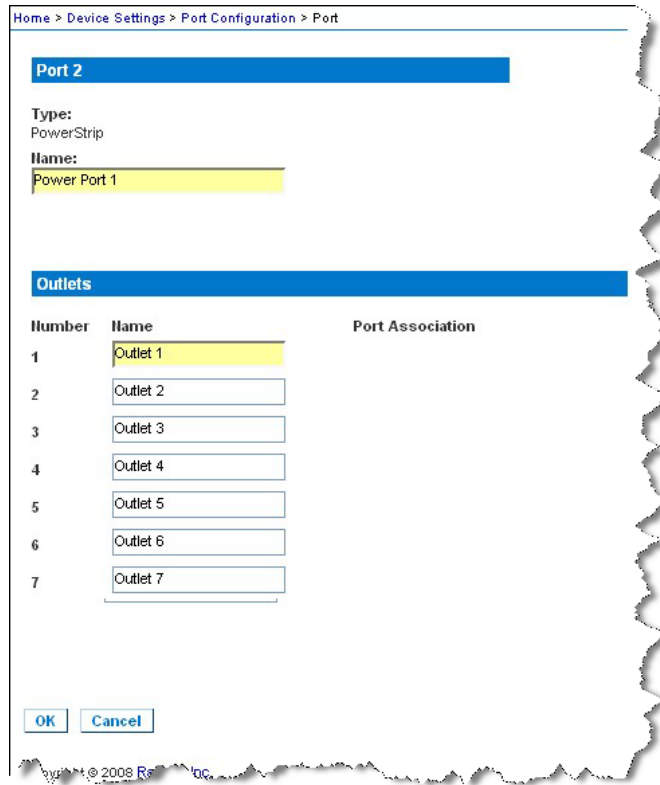
▶ 若要命名電源插座裝置 (與插座)：

附註：CommandCenter Service Gateway 無法辨識包含空格的電源插座裝置名稱。

1. 請將電源插座裝置名稱變更為您容易記住的文字。
2. 請視需要變更 (插座) 名稱。(插座名稱預設為插座編號。)
3. 按一下「OK」(確定)。

▶ 若要取消而不儲存變更：

- 按一下「Cancel」(取消)。



管理電源關聯

▶ 若要建立電源關聯 (讓電源插座裝置的插座與目標伺服器產生關聯)：

附註：當目標伺服器 (連接埠) 與電源插座裝置產生關聯時，便會已連接埠名稱取代插座名稱。您可以在「Port 2」(連接埠 2) 頁面中變更此名稱。

1. 從「Power Strip Name」(電源插座裝置名稱) 下拉式清單中選擇電源插座裝置。
2. 從「Outlet Name」(插座名稱) 下拉式清單中選擇插座。
3. 針對每個想要的電源關聯，重複執行步驟 1 與 2。
4. 按一下「OK」(確定)。隨即會顯示確認訊息。

▶ **若要移除電源插座裝置關聯：**

1. 從「Power Strip Name」(電源插座裝置名稱) 下拉式清單中選取適當的電源插座裝置。
2. 從「Outlet Name」(插座名稱) 下拉式清單中為此電源插座裝置選取適當的插座。
3. 從「Outlet Name」(插座名稱) 下拉式清單中選取「None」(無)。
4. 按一下「OK」(確定)。便會移除該電源插座裝置/插座關聯。隨即會顯示確認訊息。

▶ **若要顯示電源連接埠組態：**

- 選擇「Home」(首頁) > 「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態) > [power port name]。電源插座裝置的插座關聯會顯示在「Outlets」(插座) 下方。

▶ **若要編輯電源連接埠組態：**

1. 透過編輯連接埠的「Name」(名稱) 欄位，來變更電源連接埠名稱。
2. 透過編輯相關插座的「Name」(名稱) 欄位，來變更插座名稱。插座名稱會顯示在「Power Strip Device」(電源插座裝置) 頁面中。請參閱 < 控制電源插座裝置 >。
3. 按一下插座名稱旁邊的「Port Association」(連接埠關聯) 連結文字，在「Port 1」(連接埠 1) 頁面中加以編輯，變更插座關聯。

控制電源插座裝置

使用「Power Strip Device」(電源插座裝置) 頁面控制電源插座裝置。此頁面可讓您開啟和關閉電源插座裝置上的插座電源。

▶ **若要控制 KX II-101-V2 所連接的電源插座裝置：**

1. 選擇「Home」(首頁) > 「Powerstrip」(電源插座)。隨即會開啟「Power Strip Device」(電源插座裝置) 頁面。
2. 按一下每個插座的「On」(開) 或 「Off」(關) 按鈕，以開啟或關閉該插座。
3. 當系統提示要求您確認選擇時，按一下「OK」(確定)。

附註：KX II-101-V2 只能控制一台電源插座裝置。您無法從「Powerstrip」(電源插座裝置) 功能表選擇其他電源插座裝置。

類比 KVM 切換器

您可以設定 Raritan 類比 KVM 切換器以和 KX II-101-V2 一起使用。

KX II-101-V2 與下列 Raritan KVM 切換器的相容性已經過驗證：

- SwitchMan SW2、SW4 及 SW8
- Master Console MX416 與 MXU

可能會與來自 Raritan 或其他廠商的類似產品相容，但不保證支援。

附註：為了讓 KX II-101-V2 能和類比 KVM 切換器一起使用，可讓您切換目標的切換器快速鍵必須設定為 Scroll Lock (預設)。

▶ 若要設定 Raritan 類比 KVM 切換器：

1. 在「Keyboard/Mouse Setup」(鍵盤/滑鼠設定) 頁面上，將「Host Interface」(主機介面) 設定為 PS/2。如果您未執行此動作，便嘗試設定類比 KVM 切換器，「Analog KVM Switch Configuration」(類比 KVM 切換器組態) 頁面上會收到錯誤「PS/2 is needed to access the KVM Switch. Please enable PS/2 first!」(必須有 PS/2 才能存取 KVM 切換器。請先啟用 PS/2)。請參閱 <鍵盤/滑鼠設定> (請參閱 "鍵盤/滑鼠設定" p. 111)。
2. 按一下「Device Settings」(裝置設定) > 「Analog KVM Switch」(類比 KVM 切換器)。隨即會開啟「Analog KVM Switch」(類比 KVM 切換器) 頁面。
3. 選取「Use Analog KVM Switch」(使用類比 KVM 切換器) 核取方塊以啟用該欄位。
4. 從「Switch Type」(切換器類型) 下拉式清單中選取 Raritan 切換器類型：
 - Raritan MCC
 - Raritan MX
 - Raritan MXU
 - Raritan Switchman
5. 在「Port Count」(連接埠數目) 欄位中，根據選取的切換器類型輸入可用的連接埠數目。視需要變更連接埠數目，或使用預設的數目。切換器選項預設值與預設的連接埠數目分別如下：
 - Raritan MCC - 8
 - Raritan MX - 16
 - Raritan MXU - 16
 - Raritan Switchman - 2

6. 選取「Security Setting」(安全性設定) 核取方塊以啟用安全性。
7. 輸入用以存取 KVM 切換器的密碼。
8. 按一下「OK」(確定) 以設定類比 KVM 切換器。

▶ 若要還原類比 KVM 切換器預設值：

- 按一下「Reset to Defaults」(重設為預設值)。

使用「Reset」(重設) 按鈕重設 KX II-101-V2

在裝置的上方有一個「Reset」(重設) 按鈕。為防止意外重設而設計成凹陷式 (需要尖銳的物體才能按下此按鈕)。

按下「Reset」(重設) 按鈕所執行的動作定義於圖形化使用者介面中。請參閱〈加密與共用〉。

▶ 若要重設裝置：

1. 關閉 KX II-101-V2 的電源。
2. 使用尖銳的物體按住「重設」按鈕。
3. 按住「重設」按鈕，同時開啟 KX II-101-V2 裝置的電源。
4. 持續按住「重設」按鈕 10 秒。

5. 放開「Reset」(重設) 按鈕，然後 KX II-101-V2 便會重新開機。這通常需要花費三分鐘的時間。

附註：如果設定在重設時將 KX II-101-V2 還原為出廠預設值，便會據以設定 IP 位址、使用者名稱及其他選項。



變更預設的 GUI 語言設定

KX II-101-V2 GUI 支援下列翻譯語言：

- 日文
- Simplified Chinese (簡體中文鍵盤)
- Traditional Chinese (繁體中文鍵盤)

▶ 若要變更 GUI 語言：

1. 選取「Device Settings」(裝置設定) > 「Language」(語言)。隨即會開啟「Language Settings」(語言設定) 頁面。
2. 從「Language」(語言) 下拉式清單中選取您要套用至 GUI 的語言。
3. 按一下「Apply」(套用)。按一下「Reset Defaults」(重設為預設值) 即可恢復為「English」(英文)。

附註：在您套用新語言之後，也會翻譯線上說明，以符合您的語言選擇。

本章內容

概覽.....	133
USB 連線設定	134
進階 USB 連線設定	135

概覽

為了利用不同的 KVM 目標伺服器來擴充 KX II-101-V2 的相容性，Raritan 提供 USB 組態設定檔選項的使用者定義即時選項，供範圍廣泛的作業系統與 BIOS 層級伺服器實作使用。

預設的 USB 連線設定即符合大多數 KVM 目標伺服器部署組態的需要。亦提供其他組態項目以滿足其他經常部署之伺服器組態的特定需求 (例如，Linux® 與 Mac OS X)。還有一些組態項目 (依平台名稱與 BIOS 修訂版指定) 可增強與目標伺服器的虛擬媒體功能相容性，例如在 BIOS 層級運作。

您可以在 KX II-101-V2 遠端主控台的「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態) > 「Port」(連接埠) 頁面上設定 USB 設定檔。裝置管理員可以利用最符合使用者與目標伺服器組態需求的設定檔來設定連接埠。

警告：根據您在「Advanced USB Connection Settings」(進階 USB 連線設定) 區段中所設的選項，可能會在 KX II-101-V2 與目標伺服器之間造成組態問題。

因此，Raritan 強烈建議您參閱最新的「User Defined KX II-101-V2 USB Profile Configuration Table」(使用者定義的 KX II-101-V2 USB 設定檔組態表格)，您可以在「Port」(連接埠) 頁面上，從「Advanced USB Connection Settings」(進階 USB 連線設定) 區段中的超連結直接存取。您可以在 <已知 USB 設定檔> 中找到此書出版當時的可用資訊。

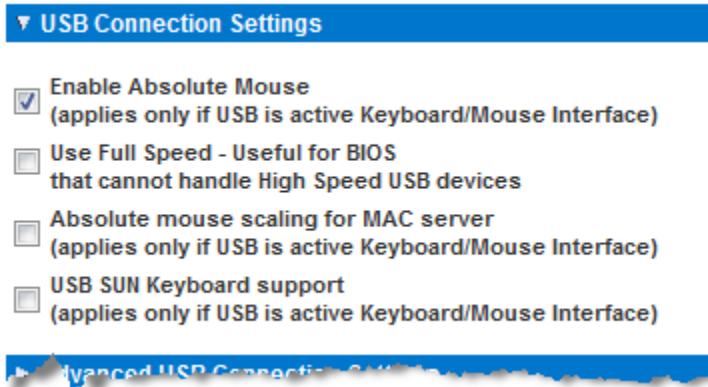
連線到 KVM 目標伺服器的使用者可以根據 KVM 目標伺服器的運作狀態，在這些 USB 連線設定之中選擇。例如，如果伺服器正在執行中，而使用者想要使用 Windows® 作業系統，此時最好使用預設值。但是如果使用者想要變更 BIOS 功能表中的設定，或是從虛擬媒體磁碟機開機，此時可能較適合使用不同的 USB 連線設定，視目標伺服器機型而定。

萬一 Raritan 提供的 USB 連線設定全不適用於特定 KVM 目標，請聯絡「Raritan 技術支援部門」以尋求協助。

USB 連線設定

▶ 若要定義目標伺服器的 **USB 連線**：

1. 按一下「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態)，以開啟「Port Configuration」(連接埠組態) 頁面。按一下要設定的連接埠。
2. 按一下「USB Connection Settings」(USB 連線設定) 以展開「USB Connection Settings」(USB 連線設定) 區段。
3. 選取要使用的 USB 連線設定：
 - Enable Absolute Mouse (啟用絕對滑鼠) - 只有當作用中的鍵盤/滑鼠介面是 USB 時才適用
 - Use Full Speed (使用全速) - 對於無法裝載高速 USB 裝置的 BIOS 十分有用
 - Absolute mouse scaling for MAC server (為 MAC 伺服器調整絕對滑鼠) - 只有當作用中的鍵盤/滑鼠介面是 USB 時才適用
 - USB Sun Keyboard support (USB Sun 鍵盤支援) - 只有當作用中的鍵盤/滑鼠介面是 USB 時才適用
4. 按一下「OK」(確定)。



進階 USB 連線設定

警告：根據您在「Advanced USB Connection Settings」(進階 USB 連線設定) 區段中所設的選項，可能會在 KX II-101-V2 與目標伺服器之間造成組態問題。因此，Raritan 強烈建議您參閱<已知 USB 設定檔> 或「User Defined KX II-101-V2 USB Profiles Connection Configuration Table」(使用者定義的 KX II-101-V2 USB 設定檔組態表格)，其在「Port」(連接埠) 頁面的「Advanced USB Connection Settings」(進階 USB 連線設定) 區段上，按一下其對應連結便可存取。

▶ 若要定義目標伺服器的進階 USB 連線：

1. 按一下「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態)，以開啟「Port Configuration」(連接埠組態) 頁面。按一下要設定的連接埠。
2. 按一下「Advanced USB Connection Settings」(進階 USB 連線設定) 以展開該區段。
3. 按一下「User Defined KX II-101 USB Profile Configuration Table」(使用者定義的 KX II-101 USB 設定檔組態表格) 連結，存取建議的組態以套用至「Advanced USB Connection Settings」(進階 USB 連線設定) 區段。
4. 視需要設定下列項目：
 - a. Virtual Media Interface #1 Type (虛擬媒體介面 #1 類型)
 - b. 勾選「Remove Unused VM Interface #1 From Device Configuration」(從裝置組態移除未使用的 VM 介面 #1) 核取方塊，以移除指定的 VM 類型介面 (#1)。
 - c. Virtual Media Interface #2 Type (虛擬媒體介面 #2 類型)
 - d. 勾選「Remove Unused VM Interface #2 From Device Configuration」(從裝置組態移除未使用的 VM 介面 #2) 核取方塊，以移除指定的 VM 類型介面 (#2)。

5. 按一下「OK」(確定)。

▼ Advanced USB Connection Settings

IMPORTANT: Please follow the reference guide provided at this link.

User Defined KX II-101 USB Profile Configuration Table

Virtual Media Interface #1 Type

CD-ROM ▼

Remove Unused VM Interface #1 From Device Configuration
(useful for BIOS that cannot accommodate empty drives)

Virtual Media Interface #2 Type

Removable Disk ▼

Remove Unused VM Interface #2 From Device Configuration
(useful for BIOS that cannot accommodate empty drives)

本章內容

安全性設定.....	137
設定 IP 存取控制.....	146
SSL 憑證.....	149
安全性標題.....	151

安全性設定

在「安全性設定」頁面中可以指定登入限制、使用者封鎖、密碼規則以及加密與共用設定。

▶ **若要設定安全性設定：**

1. 選擇「Security」(安全性) > 「Security Settings」(安全性設定)。隨即會開啟「Security Settings」(安全性設定) 頁面。
2. 適當更新「**Login Limitations**」(**登入限制**) (請參閱 "**登入限制**" p. 137) 設定。
3. 適當更新「**Strong Passwords**」(**強固密碼**) (請參閱 "**強固密碼**" p. 139) 設定。
4. 適當更新「**User Blocking**」(**使用者封鎖**) (請參閱 "**封鎖使用者**" p. 140) 設定。
5. 適當更新「Encryption & Share」(加密與共用)設定。
6. 按一下「OK」(確定)。

▶ **若要重設為預設值：**

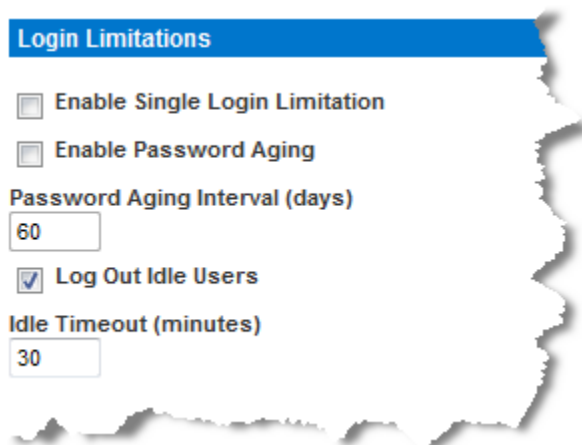
- 按一下「Reset to Defaults」(重設為預設值)。

登入限制

您可以使用「Login Limitations」(登入限制) 指定單次登入的限制、密碼使用期限以及登出閒置的使用者。

限制	說明
Enable Single Login Limitation (啟用單次登入限制)	選取此選項時，無論任何時間每個使用者名稱都只允許登入一次。取消選取此選項時，特定的使用者名稱/密碼組合可同時從數個用戶端工作站連入裝置。

限制	說明
Enable Password Aging (啟用密碼使用期限)。	<p>選取此選項時，會根據「Password Aging Interval」(密碼使用期限間隔) 欄位指定的天數，要求所有使用者定期變更密碼。</p> <p>選取「Enable Password Aging」(啟用密碼使用期限) 核取方塊時，即會啟用此欄位且為必要欄位。輸入必須變更密碼的間隔天數。預設值為 60 天。</p>
Log out idle users, After (1-365 minutes) (登出閒置的使用者，之後 (1-365 分鐘))	<p>選取「Log off idle users」(登出閒置的使用者) 核取方塊，在經過您於「After (1-365 minutes)」(之後 (1-365 分鐘)) 欄位中指定的時間之後便自動中斷連線。如果期間沒有任何鍵盤或滑鼠活動，便會登出所有階段作業與所有資源。如果有虛擬媒體階段作業在進行中，則該階段作業不會逾時。</p> <p>「After」(之後) 欄位是用來設定時間量 (以分鐘計)，在此時間之後即登出閒置使用者。選取「Log Out Idle Users」(登出閒置的使用者) 選項時即會啟用此欄位。可輸入做為欄位值的分鐘數最多為 365。</p>



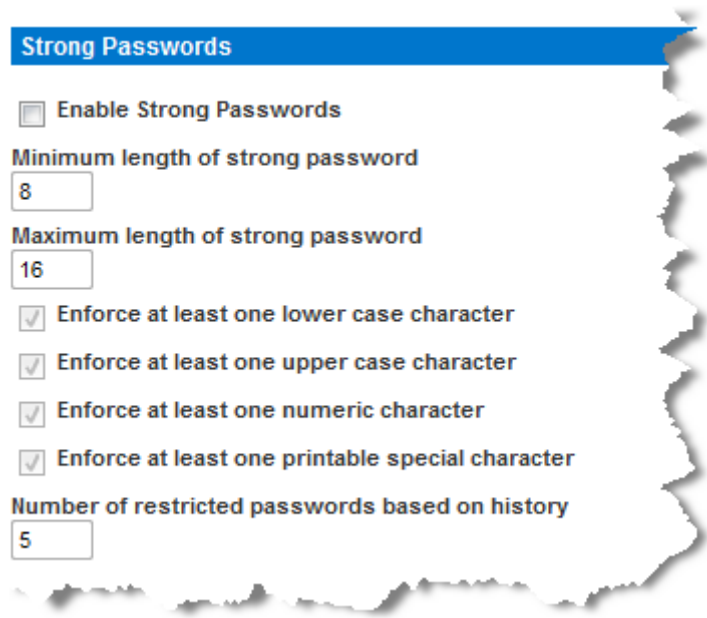
強固密碼

強固密碼為系統提供較為安全的本機驗證。使用強固密碼，您可以指定有效的 KX II-101-V2 本機密碼格式，如長度的最小值與最大值、必要的字元及密碼歷程記錄保留等。

強固密碼會要求使用者建立的密碼長度下限為 8 個字元，包含至少一個字母字元及一個非字母字元（標點符號字元或數字）。此外，密碼前四個字元不得與使用者名稱相同。

選取此選項時，即會執行強固密碼規則。密碼不符強固密碼準則的使用者於下次登入時，系統會自動要求變更密碼。取消選取此選項時，僅會執行標準格式的驗證。選取此選項時，即會啟用下列欄位且為必要欄位：

欄位	說明
Minimum length of strong password (強固密碼的長度下限)	密碼長度至少為 8 個字元。預設值為 8，但管理員可將下限變更為 63 個字元。
Maximum length of strong password (強固密碼的長度上限)	預設的長度下限為 8，但管理員可將預設的上限值設定為 16 個字元。預設的強固密碼長度上限為 63 個字元。
Enforce at least one lower case character (強制要求至少要有一個小寫字元)	選取此選項時，密碼中至少必須有一個小寫字元。
Enforce at least one upper case character (強制要求至少要有一個大寫字元)	選取此選項時，密碼中至少必須有一個大寫字元。
Enforce at least one numeric character (強制要求至少要有一個數字字元)	選取此選項時，密碼中至少必須有一個數字字元。
Enforce at least one printable special character (強制要求至少要有一個可列印的特殊字元)	選取此選項時，密碼中至少必須有一個特殊字元（可列印）。
Number of restricted passwords based on history (根據歷程所限制的密碼數)	此欄位表示密碼歷程深度。亦即，不得與之前的密碼重複的次數。範圍為 1-12，而預設值為 5。



封鎖使用者

「封鎖使用者」選項指定的準則規定在達到指定的失敗登入嘗試次數之後，即封鎖使用者不得存取系統。

以下三個選項互斥：

選項	說明
已停用	預設選項。無論驗證失敗幾次，都不會封鎖使用者。

選項	說明
鎖定計時器	<p>超過指定的登入失敗次數之後，拒絕使用者存取系統的指定時間量。選取此選項時，即會啟用下列欄位：</p> <ul style="list-style-type: none"> 嘗試次數 - 登入失敗的次數，在達到此次數之後，隨即封鎖該使用者。有效範圍為 1 - 10，而預設值為 3 次。 鎖定時間 - 封鎖使用者的時間量。有效範圍為 1 - 1440 分鐘，而預設值為 5 分鐘。 <p><i>附註：身為管理員角色的使用者則不受計時器鎖定的限制。</i></p>
停用使用者 ID	<p>選取此項目時，選項會指定達到「失敗次數」欄位中指定的登入失敗次數之後，便封鎖該使用者：</p> <ul style="list-style-type: none"> 失敗次數 - 登入失敗的次數，在達到此次數之後，隨即停用使用者 ID。選取「停用使用者 ID」選項時，隨即會啟用此欄位。有效範圍為 1 - 10。 <p>當使用者 ID 超過指定的失敗次數而遭停用時，管理員必須在「使用者」頁面選取「作用中」核取方塊，來變更使用者密碼和啟動使用者帳戶。</p>

User Blocking

Disabled

Timer Lockout

Attempts

Lockout Time

Deactivate User-ID

Failed Attempts

加密與共用

使用「Encryption & Share」(加密與共用) 設定可指定使用的加密類型、電腦與 VM 共用模式，以及按下 KX II-101-V2 「Reset」(重設) 按鈕時所執行的重設類型。

警告：如果您的瀏覽器不支援選取的加密模式，即無法從瀏覽器存取 KX II-101-V2。

▶ **若要設定加密與共用：**

1. 從「Encryption Mode」(加密模式) 下拉式清單中選擇其中一個選項。
選取加密模式時，若顯示一個警告，表示瀏覽器不支援所選取的模式，您便無法連線至 KX II-101-V2。該警告指出「When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the KX II-101-V2」(指定「加密模式」時，請確定瀏覽器支援此加密模式；否則您便無法連線至 KX II-101-V2)。

加密模式	說明
自動	此為建議選項。KX II-101-V2 會儘可能自動交涉為最高加密等級。 您必須選取「Auto」(自動)，裝置及用戶端才能成功溝通使用的 FIPS 相容演算法。
RC4	保護使用者名稱、密碼以及 KVM 資料，包括使用 RSA RC4 加密方法的視訊傳輸。此為 128 位元的安全通訊端層 (SSL) 通訊協定，於初始連線驗證期間提供 KX II-101-V2 裝置及遠端電腦之間的私人通訊通道。 如果您啟用 FIPS 140-2 模式，並已選取 RC4，則將會收到一則錯誤訊息。處於 FIPS 140-2 模式時，無法使用 RC4。
AES-128	進階加密標準 (AES) 是美國國家標準與技術局的電子資料加密規格。鍵值長度為 128。指定 AES-128 時，請確定瀏覽器可支援此值，否則將無法連線。如需詳細資訊，請參閱 <檢查瀏覽器是否具 AES 加密功能> (請參閱 "檢查瀏覽器是否支援 AES 加密功能" p. 144)。
AES-256	進階加密標準 (AES) 是美國國家標準與技術局的電子資料加密規格。鍵值長度為 256。指

加密模式	說明
	定 AES-256 時，請確定瀏覽器可支援此值，否則將無法連線。如需詳細資訊，請參閱 <檢查瀏覽器是否具 AES 加密功能> (請參閱 " 檢查瀏覽器是否支援 AES 加密功能 " p. 144)。

附註：MPC 永遠會交涉為最高加密等級，並在「加密模式」設定不是設定為「自動」時與該設定相符。

附註：如果在執行 Windows XP® 作業系統 (包含 Service Pack 2)，Internet Explorer® 7 即無法使用 AES-128 加密從遠端連線到 KX II-101-V2 裝置。

2. Apply Encryption Mode to KVM and Virtual Media (對 KVM 與虛擬媒體套用加密模式)。選取此選項時，即會將選取的加密模式套用到 KVM 及虛擬媒體。驗證過後，KVM 與虛擬媒體資料也會使用 128 位元加密傳輸。
3. 若為政府機構與其他高安全性環境，請選取「Enable FIPS 140-2」(啟用 FIPS 140-2) 核取方塊，來啟用 FIPS 140-2 模式。如需啟用 FIPS 140-2 的詳細資訊，請參閱 **<啟用 FIPS 140-2>** (請參閱 " **啟用 FIPS 140-2**" p. 145)。
4. PC Share Mode (電腦共用模式) - 決定全域並行的遠端 KVM 存取，透過此裝置最多可讓八位遠端使用者同時登入一台 KX II-101-V2，並可同時檢視與控制相同的目標伺服器。按一下下拉式清單以選取下列其中一個選項：
 - Private (獨佔) - 不共用電腦。此為預設模式。每部目標伺服器一次僅允許一位使用者單獨存取。
 - PC-Share (電腦共用) - KVM 目標伺服器一次可讓最多八位使用者同時存取 (管理員或非管理員)。每位遠端使用者對鍵盤與滑鼠的控制都相同，但請注意，若某位使用者不停打字或移動滑鼠，則會發生控制不平衡的狀況。
5. 如有需要，可選取「VM Share Mode」(VM 共用模式)。唯有啟用「電腦共用」模式時才會啟用此選項。選取此選項時，允許多位使用者共用虛擬媒體，亦即數位使用者可存取相同的虛擬媒體階段作業。預設為停用。
6. 如有需要，可選取「Local Device Reset Mode」(本機裝置重設模式)。此選項會指定按下硬體「Reset」(重設) 按鈕 (位於裝置背面) 時所執行的動作。如需詳細資訊，請參閱 **<重設 KX II-101-V2 使用「Reset」(重設) 按鈕>** (請參閱 " **使用「Reset」(重設) 按鈕重設 KX II-101-V2**" p. 131)。選擇下列其中一個選項：

本機裝置重設模式	說明
Enable Local Factory Reset (啟用重設本機出廠值，預設值)	將 KX II-101-V2 裝置回復到出廠預設值。
Enable Local Admin Password Reset (啟用重設本機管理員密碼)	僅重設本機管理員密碼。密碼會重設為 raritan。
Disable All Local Resets (停用重設所有本機預設值)	不執行任何重設動作。

檢查瀏覽器是否支援 AES 加密功能

KX II-101-V2 支援 AES-256。如果不知道瀏覽器是否使用 AES，請聯絡瀏覽器製造商，或使用具有要選取之加密方法的瀏覽器瀏覽 <https://www.fortify.net/sslcheck.html> 網站。此網站可偵測瀏覽器的加密方法，並顯示偵測結果的報表。

附註：Internet Explorer® 6 不支援 AES 128 或 256 位元加密方法。

AES 256 必要條件與支援組態

只有下列網頁瀏覽器可支援 AES 256 位元加密方法：

- Firefox® 2.0.0.x 與 3.0.x (及更新版本)
- Internet Explorer 7 及 8

除了瀏覽器支援之外，AES 256 位元加密方法還需要安裝 Java™ Cryptography Extension® (JCE®) Unlimited Strength Jurisdiction Policy 檔案。

各版 JRE™ 的 Jurisdiction 檔案可在以下連結的「other downloads」(其他下載項目) 區段取得：

- JRE1.7 - javase/downloads/jce-7-download-432124.html

啟用 FIPS 140-2

若為政府機構及其他高安全性環境，可能會想要啟用 FIPS 140-2 模式。按照《FIPS 140-2 實作指引》G.5 節的準則，KX II-101-V2 會使用在 Linux® 平台執行的內建 FIPS 140-2 驗證加密模組。啟用此模式之後，用以產生 SSL 憑證的私密金鑰必須在內部產生；其無法加以下載或匯出。

▶ 若要啟用 FIPS 140-2：

1. 存取「Security Settings」(安全性設定) 頁面。
2. 在「Security Settings」(安全性設定) 頁面的「Encryption & Share」(加密與共用) 區段中，選取「Enable FIPS 140-2」(啟用 FIPS 140-2) 核取方塊來啟用 FIPS 140-2 模式。一旦進入 FIPS 140-2 模式，您將會利用 FIPS 140-2 核可的演算法進行外部通訊。FIPS 加密模組是用來加密 KVM 階段作業流量，其包含視訊、鍵盤、滑鼠、虛擬媒體及智慧卡資料。
3. 將 KX II-101-V2 重新開機。<必要>

啟動 FIPS 模式之後，便會在畫面左面板的「Device Information」(裝置資訊) 區段中，顯示「FIPS Mode: Enabled」(FIPS 模式：已啟用)。

如需額外的安全性，您也可以啟動 FIPS 模式後，建立新的「憑證簽署要求」。這將會使用必要的金鑰加密方式建立。在憑證完成簽署或建立自我簽署憑證之後加以上載。SSL 憑證狀態便會從「Not FIPS Mode Compliant」(與 FIPS 模式不相容) 更新成「FIPS Mode Compliant」(與 FIPS 模式相容)。

啟動 FIPS 模式時，無法下載或上載金鑰檔案。內部會讓最新建立的 CSR 與金鑰檔案建立關聯。再者，不會將來自 CA 的 SSL 憑證與其私密金鑰納入可完整還原的備份檔案中。您無法從 KX II-101-V2 匯出金鑰。

FIPS 140-2 支援需求

KX II-101-V2 支援使用 FIPS 140-20 核可加密演算法。當用戶端設定為只限 FIPS 140-2 模式時，這可讓 SSL 伺服器與用戶端成功交涉加密階段作業使用的 cipher 套裝軟體。

下列是使用 FIPS 140-2 搭配 KX II-101-V2 的建議：

KX II-101-V2

- 在「Security Settings」(安全性設定) 頁面上，將「Encryption & Share」(加密與共用) 設定為「Auto」(自動)。請參閱<加密與共用>。

Microsoft 用戶端

- 您應該在用戶端電腦與 Internet Explorer 中啟用 FIPS 140-2。

▶ 若要在 Windows 用戶端上啟用 FIPS 140-2 :

1. 選取「Control Panel」(控制台) > 「Administrative Tools」(系統管理工具) > 「Local Security Policy」(本機安全性原則), 來開啟「Local Security Settings」(本機安全性原則) 對話方塊。
2. 從瀏覽樹狀結構中, 選取「Local Policies」(本機原則) > 「Security Options」(安全性選項)。
3. 啟用「System Cryptography: Use FIPS compliant algorithms for encryption, hashing and signing」(系統加密編譯: 使用 FIPS 相容演算法於加密, 雜湊, 以及簽章)。
4. 將用戶端電腦重新開機。

▶ 若要在 Internet Explorer 中啟用 FIPS 140-2 :

1. 在 Internet Explorer 中, 選取「Tools」(工具) > 「Internet Options」(網際網路選項), 然後按一下「Advanced」(進階) 索引標籤。
2. 選取「Use TLS 1.0」(使用 TLS 1.0) 核取方塊。
3. 重新啟動瀏覽器。

設定 IP 存取控制

使用 IP 存取控制可控制對 KX II-101-V2 裝置的存取。設定全域存取控制清單 (ACL), 確保裝置不會回應從不允許的 IP 位址所傳出的封包。

重要: KX II-101-V2 本機連接埠使用的 IP 位址為 127.0.0.1。建立「IP 存取控制清單」時, 若 127.0.0.1 位於封鎖的 IP 位址範圍內, 即不能存取 KX II-101-V2 本機連接埠。

▶ 若要使用 IP 存取控制 :

1. 選取「Security」(安全性) > 「IP Access Control」(IP 存取控制), 即可開啟「IP Access Control」(IP 存取控制) 頁面。隨即會開啟「IP Access Control」(IP 存取控制) 頁面。
2. 選取「Enable IP Access Control」(啟用 IP 存取控制) 核取方塊, 可啟用 IP 存取控制及頁面上其餘欄位。
3. 選擇「Default Policy」(預設原則)。此為針對不在指定範圍內之 IP 位址所執行的動作。
 - Accept (接受) - 允許存取 KX II-101-V2 裝置的 IP 位址。
 - Drop (捨棄) - 被拒絕存取 KX II-101-V2 裝置的 IP 位址。

▶ **若要新增 (附加) 規則：**

1. 在「IPv4/Mask」(IPv4/遮罩) 或「IPv6/Prefix Length」(IPv6/首碼長度) 欄位中，輸入 IP 位址與子網路遮罩。

附註：應使用 CIDR (無類別網域間路由選擇) 標記法來輸入 IP 位址，CIDR 標記法包含兩個部分。佔最大部分的是網路位址，可以識別整個網路或子網路。佔最小部分的是識別碼。位於/後面的首碼長度可以識別子網路遮罩的長度。

2. 從下拉式清單中選擇「Policy」(原則)。
3. 按一下「Append」(附加)。將規則加入成為規則清單的最後一筆記錄。

▶ **若要插入規則：**

1. 輸入規則編號 (#)。使用「Insert」(插入) 指令時必須要有規則編號。
2. 在「IPv4/Mask」(IPv4/遮罩) 或「IPv6/Prefix Length」(IPv6/首碼長度) 欄位中，輸入 IP 位址與子網路遮罩。
3. 從下拉式清單中選擇「Policy」(原則)。
4. 按一下「Insert」(插入)。若剛才輸入的規則編號等於現有的規則編號，則新規則會放在現有規則的前面，而清單中所有規則都會向下移。

祕訣：規則編號可讓您對規則的建立順序擁有較多的控制。

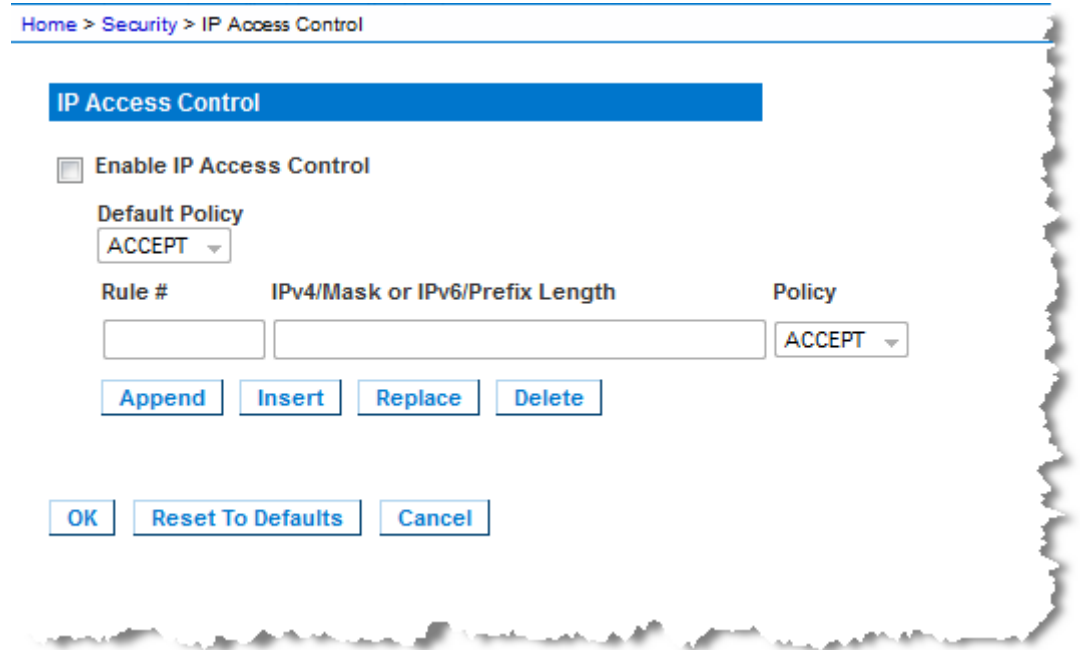
▶ **若要取代規則：**

1. 指定要取代的規則編號。
2. 在「IPv4/Mask」(IPv4/遮罩) 或「IPv6/Prefix Length」(IPv6/首碼長度) 欄位中，輸入 IP 位址與子網路遮罩。
3. 從下拉式清單中選擇「Policy」(原則)。
4. 按一下「Replace」(取代)。新規則會取代規則編號相同的原規則。

▶ **若要刪除規則：**

1. 指定要刪除的規則編號。
2. 按一下「Delete」(刪除)。

- 隨即會出現提示要求您確認刪除。按一下「OK」(確定)。



若只允許存取一個 IP 位址並封鎖其他位址，請將規則的子網路遮罩變更為 /32。例如，您正嘗試排除來自 '192.168.51' 子網路的所有存取，而預設原則為「Accept」(接受)，您可以附加「IP/Mask」(IP/遮罩) 設定為 192.168.51.00/24 的一個規則與原則「DROP」(捨棄)。或者，如果您正嘗試排除來自 192.168.51 子網路的所有存取，除某特定 IP 位址 (192.168.51.105) 除外，而預設原則為「Accept」(接受)，您可以：

- 附加「IP/Mask」(IP/遮罩) 設定為 192.168.51.105/32 的「Rule 1」(規則 1) 以及「Accept」(接受) 原則。
- 附加「IP/Mask」(IP/遮罩) 設定為 192.168.51.0/24 的「Rule 2」(規則 2) 以及「Drop」(捨棄) 原則。

如果顛倒「Rule 1」(規則 1) 與「Rule 2」(規則 2) 的順序，192.168.51.105 也會無法存取 KX II-101-V2，因為發生的第一個規則已經將其捨棄。

SSL 憑證

KX II-101-V2 在自己與連線的用戶端間使用安全通訊端層 (SSL) 通訊協定，用於任何加密的網路流量。建立連線時，KX II-101-V2 必須使用加密憑證向用戶端自行表明身分。

您可以在 KX II-101-V2 上產生「憑證簽署要求 (CSR)」以及安裝由憑證授權單位 (CA) 簽署的憑證。CA 會驗證 CSR 建立者的身分識別。然後 CA 會將內含其簽名的憑證傳回給建立者。帶有知名 CA 簽名的憑證是用來證明憑證提供者的身分識別。

重要：請務必正確設定 KX II-101-V2 日期/時間。

建立自我簽署憑證時，會使用 KX II-101-V2 日期與時間來計算有效期間。如果 KX II-101-V2 日期與時間不準確，會使憑證的有效日期範圍不正確，而導致憑證驗證失敗。請參閱 [〈設定日期/時間設定〉](#) (請參閱 "設定日期/時間設定" p. 113)。

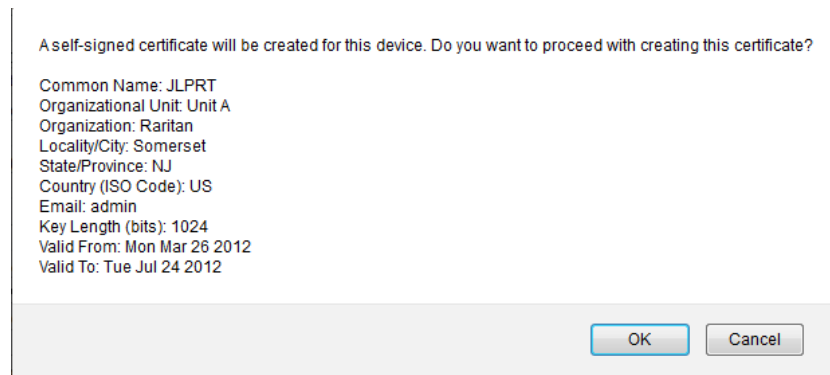
附註：CSR 必須在 KX II-101-V2 上產生。

附註：升級韌體時，不會取代作用中的憑證與 CSR。

▶ **若要建立與安裝 SSL 憑證：**

1. 選取「安全性」>「憑證」。
2. 填寫下列欄位：
 - a. Common name (一般名稱) - 在您的網路安裝 KX II-101-V2 之後的網路名稱，(通常是完整網域名稱)。一般名稱和利用網頁瀏覽器來存取 KX II-101-V2 的名稱完全相同，只是沒有首碼 "http://"。此處指定的名稱若與實際的網路名稱不同，瀏覽器便會在使用 HTTPS 存取 KX II-101-V2 時，顯示安全性警告。
 - b. Organizational unit (組織單位) - 此欄位是用來指定 KX II-101-V2 隸屬於組織內的哪個部門。
 - c. Organization (組織) - KX II-101-V2 所屬的組織名稱。
 - d. Locality/City (地區/城市) - 組織所在的城市。
 - e. State/Province (州/省) - 組織所在的州或省。
 - f. Country (ISO code) (國家，ISO 碼) - 組織所在的國家。這是兩個字母的 ISO 碼，例如 DE 代表德國或 US 代表美國。
 - g. Challenge Password (挑戰密碼) - 一些憑證授權單位需要挑戰密碼，才能授權之後對憑證進行變更 (例如撤銷憑證)需要時，請加以輸入。
 - h. Confirm Challenge Password (確認挑戰密碼) - 確認挑戰密碼。

- i. **Email** (電子郵件) - 負責 KX II-101-V2 與其安全性的聯絡人電子郵件地址。
 - j. **Key length** (金鑰長度) - 所產生金鑰的長度 (位元)。預設值為 1024。
3. 請執行下列其中一項動作：
- a. 如果您需要產生自我簽署憑證，請選取「**Create a Self-Signed Certificate**」(建立自我簽署憑證) 核取方塊。當您選取此選項時，KX II-101-V2 會根據您的項目產生憑證，然後做為負責簽署的憑證授權單位。不需要匯出和使用 CSR 來產生簽署的憑證。
 - b. 指定有效天數的範圍。請確定 KX II-101-V2 日期與時間正確無誤，否則會使用無效的日期來建立憑證的有效日期範圍。
 - c. 按一下「**Create**」(建立)。
 - d. 隨即會顯示確認對話方塊。按一下「**OK**」(確定) 即可加以關閉。
 - e. 重新啟動 KX II-101-V2 以啟動自我簽署憑證。



或

- f. 指定有效天數的範圍。請確定 KX II-101-V2 日期與時間正確無誤，否則會使用無效的日期來建立憑證的有效日期範圍。
- g. 按一下「**Create**」(建立)。
- h. 就會出現一個對話方塊，其中含有您輸入的所有資訊以及憑證的有效日期範圍。如果資訊正確無誤，按一下「**OK**」(確定) 即可產生 CSR。
- i. 重新啟動 KX II-101-V2 以將儲存的 CSR 傳送給 CA 進行 SSL 憑證。

► **若要下載 CSR 憑證：**

1. 按一下「**Download**」(下載)，即可下載產生憑證時會使用的 CSR 與包含私密金鑰的檔案。

附註：CSR 與私密金鑰檔案彼此相符且視為一對。如果簽署的憑證與用以產生原始 CSR 的私密金鑰不相符，其即為無效憑證。這適用於上傳及下載 CSR 與私密金鑰檔案。

- 將儲存的 CSR 傳送給 CA 進行驗證。您會從 CA 取得新的憑證。

▶ **若要上傳簽署憑證：**

- 按一下「Upload」(上傳)，即可將憑證上傳至 KX II-101-V2。

附註：CSR 與私密金鑰檔案彼此相符且視為一對。如果簽署的憑證與用以產生原始 CSR 的私密金鑰不相符，其即為無效憑證。這適用於上傳及下載 CSR 與私密金鑰檔案。

Certificate Signing Request (CSR)	Certificate Upload
<p>The following CSR is pending:</p> <pre>countryName = US stateOrProvinceName = DC localityName = Washington organizationName = ACME Corp. organizationalUnitName = Marketing Dept. commonName = John Doe emailAddress = johndoe@acme.com</pre> <p style="text-align: center;"> <input type="button" value="Download"/> <input type="button" value="Delete"/> </p>	<p>SSL Certificate File</p> <p><input type="text"/> <input type="button" value="Browse..."/></p> <p><input type="button" value="Upload"/></p>

完成上述三個步驟之後，KX II-101-V2 即可擁有自己的憑證，可用於向用戶端識別其身分。

重要：如果將 KX II-101-V2 上的 CSR 刪除，即不可能重新取得該 CSR。萬一您意外將其刪除，您必須重複進行上述的三個步驟。為了避免發生這種狀況，請使用下載功能，來取得 CSR 與其私密金鑰的副本。

安全性標題

KX II-101-V2 可讓您將安全性標題新增至 KX II-101-V2 登入程序。此功能會要求使用者在存取 KX II-101-V2 之前，先接受或拒絕安全性協議書。在使用者利用其登入憑證來存取 KX II-101-V2 之後，便會在「Restricted Service Agreement」(限制服務協議書) 對話方塊中顯示在安全性標題提供的資訊。

您可以自訂安全性標題的文字標題與內容，或是使用預設文字。此外，您可以設定安全性標題，要求使用者在接受安全性協議書後，才能存取 KX II-101-V2，或是只在登入程序結束後顯示。如果啟用接受或拒絕功能，便會在稽核記錄中記錄使用者的選擇。

▶ **若要設定安全性標題：**

- 按一下「Security」(安全性) > 「Banner」(標題)，隨即會開啟「Banner」(標題) 頁面。

2. 選取「**Display Restricted Service Banner**」(顯示限制服務標題) 以啟用該功能。
3. 如果您想要求使用者先認可該標題後，才繼續進行登入程序，請選取「**Require Acceptance of Restricted Service Banner**」(需要接受限制服務標題)。使用者須選取一個核取方塊來認可標題。如果您未啟用此設定，則只會在使用者登入後才顯示安全性標題，而不會要求使用者加以認可。
4. 請視需要變更標題文字。此資訊會做為標題的一部分向使用者顯示。最多可使用 **64** 個字元。
5. 在「**Restricted Services Banner Message**」(限制服務標題訊息) 文字方塊編輯資訊。最多可以輸入或從文字檔案上載 **6000** 個字元。若要這樣做，請執行下列其中一項動作：
 - a. 在文字方塊中手動輸入來編輯文字。按一下「**OK**」(確定)。
6. 選取「**Restricted Services Banner File**」(限制服務標題檔案) 選擇鈕，然後使用「**Browse**」(瀏覽) 功能來找到並上載檔案，即可上載 **.txt** 檔案中的資訊。按一下「**OK**」(確定)。上載檔案之後，該檔案中的文字便會顯示在「**Restricted Services Banner Message**」(限制服務標題訊息) 文字方塊中。

本章內容

稽核記錄	153
裝置資訊	154
Backup and Restore (備份與還原)	155
升級韌體	157
升級歷程記錄	158
出廠重設	158
將 KX II-101-V2 重新開機	159
停止 CC-SG 管理	160

稽核記錄

因 KX II-101-V2 系統事件所建立的記錄。稽核記錄在開始覆寫最舊的項目之前，最多可包含大約 2K 的資料。若要避免失去稽核記錄資料，請將資料匯出到 Syslog 伺服器或 SNMP 管理員。您可以從「Device Settings」(裝置設定) > 「Event Management」(事件管理) 頁面，設定 Syslog 伺服器或 SNMP 管理員。

▶ **若要檢視 KX II-101-V2 的稽核記錄：**

1. 選擇「Maintenance」(維護) > 「Audit Log」(稽核記錄)。隨即會開啟「Audit Log」(稽核記錄) 頁面。
 「Audit Log」(稽核記錄) 頁面會依日期與時間顯示事件 (先列出最近期的事件)。「Audit Log」(稽核記錄) 提供下列資訊：
 - Date (日期) - 事件發生的日期與時間，使用 24 小時制。
 - Event (事件) - 事件名稱與「Event Management」(事件管理) 頁面所列者相同。
 - Description (說明) - 事件的詳細說明。

▶ **若要儲存稽核記錄：**

1. 按一下「Save to File」(另存檔案)。隨即會出現「Save File」(儲存檔案) 對話方塊。
2. 選擇想要的檔案名稱與位置，然後按一下「Save」(儲存)。稽核記錄會以指定的名稱及位置，儲存在本機用戶端機器內。

▶ **若要翻閱稽核記錄：**

- 使用 [Older] (較早) 與 [Newer] (較新) 連結。

裝置資訊

「Device Information」(裝置資訊) 頁面提供有關 KX II-101-V2 裝置的詳細資訊。如需聯絡 Raritan 技術支援部門，此項資訊會很有幫助。

▶ 若要檢視 **KX II-101-V2** 的相關資訊：

- 選擇「Maintenance」(維護) > 「Device Information」(裝置資訊)。隨即會開啟「Device Information」(裝置資訊) 頁面。

下列提供 KX II-101-V2 的相關資訊：

- Model (型號)
- Hardware Revision (硬體修訂版本)
- Firmware Version (韌體版本)
- Serial Number (序號)
- MAC Address (MAC 位址)

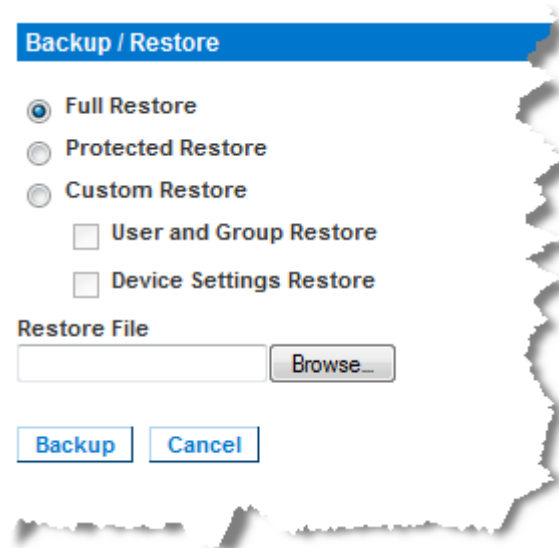
Backup and Restore (備份與還原)

您可以從「備份/還原」頁面來備份與還原 KX II-101-V2 裝置的設定與組態。

備份和還原除了可用來延續商業營運，還可使用此功能做為節省時間的機制。例如，您可以從使用中的 KX II-101-V2 裝置備份使用者的各項設定，再將這些組態還原至新的 KX II-101-V2 裝置，而可從其他 KX II-101-V2 裝置向您的小組快速提供存取。您也可以設定一台 KX II-101-V2 裝置，再將其組態複製到多台 KX II-101-V2 裝置。

▶ 若要存取「Backup/Restore」(備份/還原) 頁面：

- 選擇「Maintenance」(維護) > 「Backup/Restore」(備份/還原)。隨即會開啟「Backup/Restore」(備份/還原) 頁面。



附註：備份一律為進行完整的系統備份。還原則可根據您的選擇進行完整或部分還原。

▶ 如果使用 Internet Explorer 7 或更新版本，若要備份您的 KX II-101-V2：

1. 按一下「Backup」(備份)。隨即會開啟有「Open」(開啟) 按鈕的「File Download」(下載檔案) 對話方塊。請不要按一下「Open」(開啟)。

在 IE 6 (及更新版本) 中，用來開啟檔案的預設應用程式就是 IE，因此會提示您開啟檔案與儲存檔案。為了避免這種情況，您必須將用來開啟檔案的預設應用程式變更為 WordPad®。

2. 若要執行此作業：

- a. 儲存備份檔案。備份檔案會以指定的名稱與位置，儲存在本機用戶端機器內。
- b. 在儲存後，找到該檔案並於其上按一下滑鼠右鍵。選取「Properties」(內容)。
- c. 在「General」(一般) 索引標籤中，按一下「Change」(變更)，然後選取 WordPad。

▶ **若要還原 KX II-101-V2：**

警告：將 KX II-101-V2 還原為較舊版本時，務請謹慎執行作業。使用者名稱與密碼會還原到備份當時所使用的內容。如果不記得舊的管理使用者名稱與密碼，便會遭到 KX II-101-V2 封鎖。

此外，備份時若使用其他 IP 位址，也會還原到該 IP 位址。組態若使用 DHCP，請僅在能夠存取本機連接埠時才執行此作業，以於更新後檢查 IP 位址。

1. 選擇您要執行的還原類型：
 - **Full Restore (完整還原)** - 完整還原整個系統。通常用於傳統備份與還原用途。
 - **Protected Restore (保護還原)** - 還原各項設定，但除裝置特有資訊以外，例如 IP 位址、名稱等等。使用此選項，您可以設定一台 KX II-101-V2，再將其組態複製到多台 KX II-101-V2 裝置。
 - **Custom Restore (自訂還原)** - 使用此選項，您可以選取「User and Group Restore」(使用者與群組還原)、「Device Settings Restore」(裝置設定還原) 或兩者皆選：
 - **User and Group Restore (使用者與群組還原)** - 此選項僅包含使用者與群組資訊。此選項不會還原憑證與私密金鑰檔案。使用此選項可讓您快速設定不同 KX II-101-V2 的使用者。
 - **Device Settings Restore (裝置設定還原)** - 此選項僅包含裝置設定、例如電源關聯、USB 設定檔、與刀峰機架相關的組態參數以及「連接埠群組」指派。使用此選項可快速複製裝置資訊。
2. 按一下「瀏覽」。隨即會開啟「選擇檔案」對話方塊。
3. 瀏覽並選取適當的備份檔案，然後按一下「開啟」。選取的檔案會列在「還原檔案」欄位中。
4. 按一下「還原」。隨即會還原組態設定 (以選取的還原類型為準)。

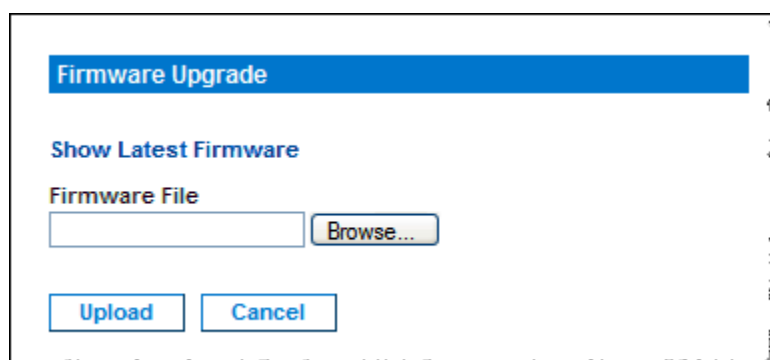
升級韌體

使用「Firmware Upgrade」(韌體升級) 頁面，以升級 KX II-101-V2 的韌體。

重要：升級進行時請勿關閉 KX II-101-V2 裝置，因為如此做可能會損害裝置。

► 若要升級 KX II-101-V2 裝置：

1. 選取「Maintenance」(維護) > 「Firmware Upgrade」(韌體升級)。隨即會開啟「Firmware Upgrade」(韌體升級) 頁面。



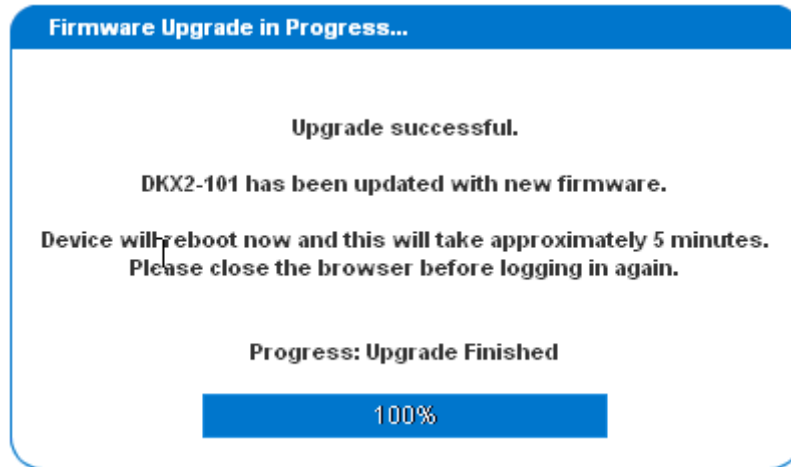
2. 在「Firmware Upgrade」(韌體升級) > KX II-101-V2 頁面中找到適當的 Raritan 韌體散佈檔案 (*.RFP)，然後下載檔案。
3. 將檔案解壓縮，並在升級前，詳閱韌體 ZIP 檔案所附的所有指示。

附註：請先將韌體更新檔複製到本機電腦上，再進行上傳。請勿從網路磁碟機載入檔案。按一下「瀏覽」，瀏覽解壓縮升級檔案所在的目錄。

4. 按一下「Firmware Upgrade」(韌體升級) 頁面的「Upload」(上傳)。隨即會顯示升級與版本號碼的相關資訊。

附註：此時會登出已連線的使用者，並封鎖新的登入嘗試。

5. 按一下「Upgrade」(升級)。請靜候升級完成。升級過程中會顯示狀態資訊與進度列。完成升級之後，裝置便會重新開機。



6. 出現提示時，請關閉瀏覽器並稍候約 5 分鐘，再次登入 KX II-101-V2。如需有關升級使用多平台用戶端之裝置韌體的詳細資訊，請參閱《KVM 與序列存取用戶端指南》。

升級歷程記錄

KX II-101-V2 提供在 KX II-101-V2 裝置上執行升級的相關資訊。

▶ **若要檢視升級歷程記錄：**

- 選擇「Maintenance」(維護) > 「Upgrade History」(升級歷程記錄)。隨即會開啟「Upgrade History」(升級歷程記錄) 頁面。

出廠重設

附註：建議您先儲存稽核記錄，再執行重設工廠預設值作業。執行重設工廠預設值作業時會刪除稽核記錄，重設事件也不會記錄在稽核記錄中。如需儲存稽核記錄的詳細資訊，請參閱〈稽核記錄〉。

▶ **若要執行重設工廠預設值作業：**

1. 選擇「維護」> 「重設工廠預設值」。隨即會開啟「重設工廠預設值」頁面。
2. 從下列選項之中選擇適當的重設選項：

- 重設完整工廠預設值 - 移除整個組態設定，並將裝置完全重設回工廠預設值。請注意，任何與 **CommandCenter** 相關的管理關聯皆會中斷。因為這是全面性的重設作業，所以會出現提示向您確認是否執行重設工廠預設值作業。
 - 重設網路參數 - 將裝置的網路參數重設回預設值 (按一下「裝置設定」>「網路設定」即可存取此資訊)：
3. 按一下「重設」繼續。因為所有網路設定都將永久遺失，所以會出現提示向您確認是否執行重設工廠預設值作業。
 4. 按一下「確定」繼續。完成時，KX II-101-V2 裝置會自動重新啟動。

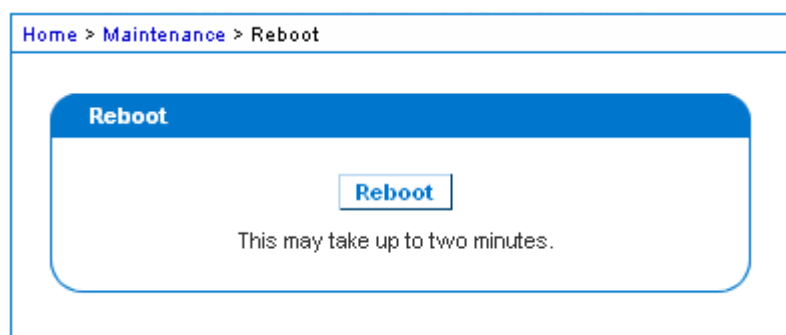
將 KX II-101-V2 重新開機

「Reboot」(重新啟動) 頁面提供安全且受控制的方式，讓您重新開機 KX II-101-V2 裝置。此為建議的重新開機方法。

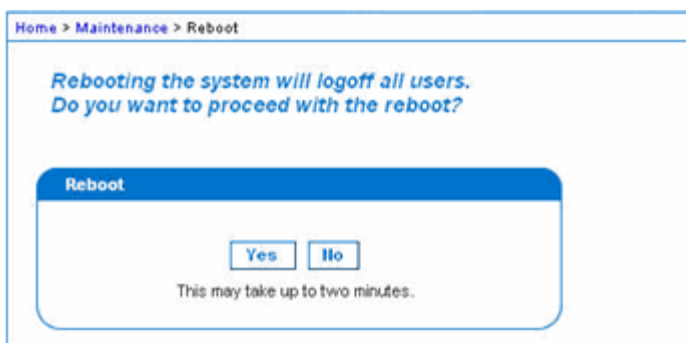
重要：系統會關閉所有 KVM 與序列連線，並登出所有使用者。

▶ 若要將 KX II-101-V2 重新開機：

1. 選擇「Maintenance」(維護) > 「Reboot」(重新開機)。隨即會開啟「Reboot」(重新開機) 頁面。



2. 按一下「Reboot」(重新開機)。隨即會出現提示要求您確認動作：按一下「Yes」(是) 繼續重新開機作業。



停止 CC-SG 管理

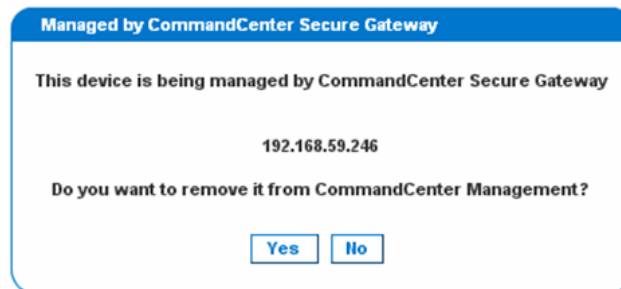
當 KX II-101-V2 受 CC-SG 管理時，如果您嘗試直接存取該裝置，系統會通知您該裝置受 CC-SG 管理。

如果您是透過 CC-SG 管理 KX II-101-V2，且在經過指定的時間間隔 (通常是 10 分鐘) 之後會中斷 CC-SG 與 KX II-101-V2 之間的連線，即可以從 KX II-101-V2 主控台結束 CC-SG 管理階段工作。

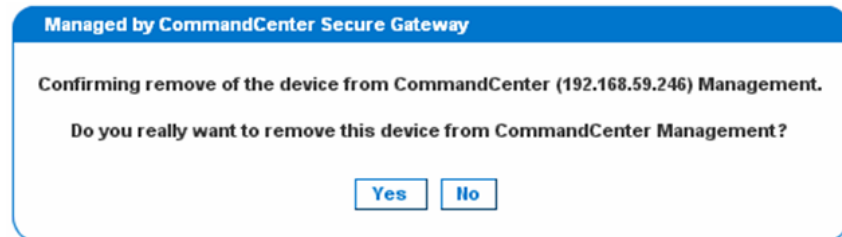
附註：您必須擁有適當的權限，才能結束 CC-SG 對 KX II-101-V2 的管理。此外，除非目前使用 CC-SG 來管理 KX II-101-V2，否則不會提供「Stop CC-SG Management」(停止 CC-SG 管理) 選項。

▶ 若要停止 CC-SG 對 KX II-101-V2 的管理：

1. 按一下「Maintenance」(維護) > 「Stop CC-SG Management」(停止 CC-SG 管理)。顯示的訊息指出該裝置是由 CC-SG 管理。還會顯示一個選項，供您移除 CC-SG 對裝置的管理。



2. 按一下「Yes」(是)，即可開始移除 CC-SG 對裝置的管理。之後會顯示確認訊息，要求您確認想要移除 CC-SG 對裝置的管理。



3. 按一下「Yes」(是),即可移除 CC-SG 對裝置的管理。結束 CC-SG 管理之後,便會顯示確認訊息。



「Diagnostics」(診斷) 頁面是用於疑難排解，主要供 KX II-101-V2 裝置的管理員使用。所有的「Diagnostics」(診斷) 頁面都執行標準的網路指令(「Device Diagnostics」(裝置診斷) 除外)，而顯示的資訊即是這些指令的輸出結果。「Diagnostics」(診斷) 功能表選項可幫助助您除錯與設定網路組態：

「Device Diagnostics」(裝置診斷) 選項是要與「Raritan 技術支援部門」聯合運用。

本章內容

網路介面頁面	162
Network Statistics (網路統計資料) 頁面	163
偵測 (Ping) 主機頁面	165
Trace Route to Host (追蹤主機路由) 頁面	165
裝置診斷	167

網路介面頁面

KX II-101-V2 提供有關網路介面狀態的資訊。

▶ 若要檢視網路介面的相關資訊：

- 選擇「Diagnostics」(診斷) > 「Network Interface」(網路介面)。隨即會開啟「Network Interface」(網路介面) 頁面。

顯示的資訊如下：

- 乙太網路介面處於開啟或關閉。
- 閘道是否可偵測 (ping)。
- 目前作用中的 LAN 連接埠。

▶ 若要重新整理此項資訊：

- 按一下「Refresh」(重新整理)。

Network Statistics (網路統計資料) 頁面

KX II-101-V2 提供有關網路介面狀態的統計資料。

▶ 若要檢視網路介面的統計資料：

1. 選擇「Diagnostics」(診斷) > 「Network Statistics」(網路統計資料)。
隨即會開啟「Network Statistics」(網路統計資料) 頁面。
2. 從「Options」(選項) 下拉式清單中選擇適當的選項：
 - Statistics (統計資料) - 產生與下圖相似的頁面。



```
Home > Diagnostics > Network Statistics

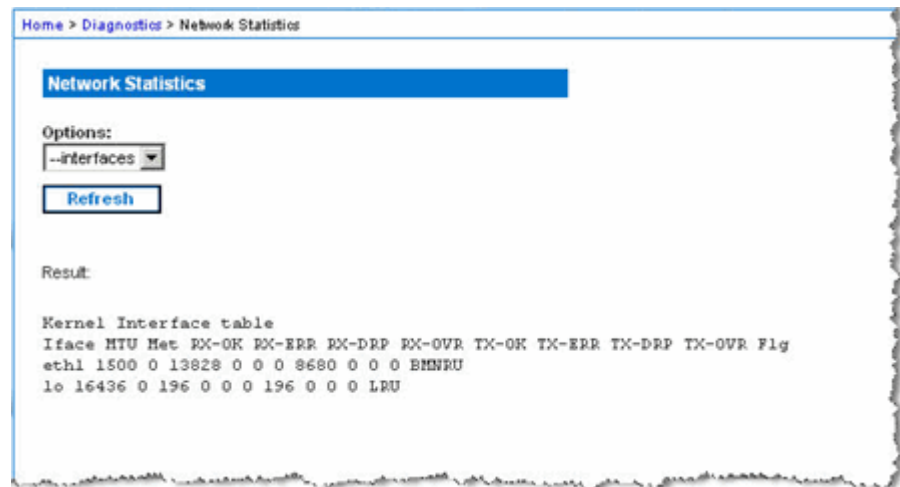
Network Statistics

Options:
--statistics
Refresh

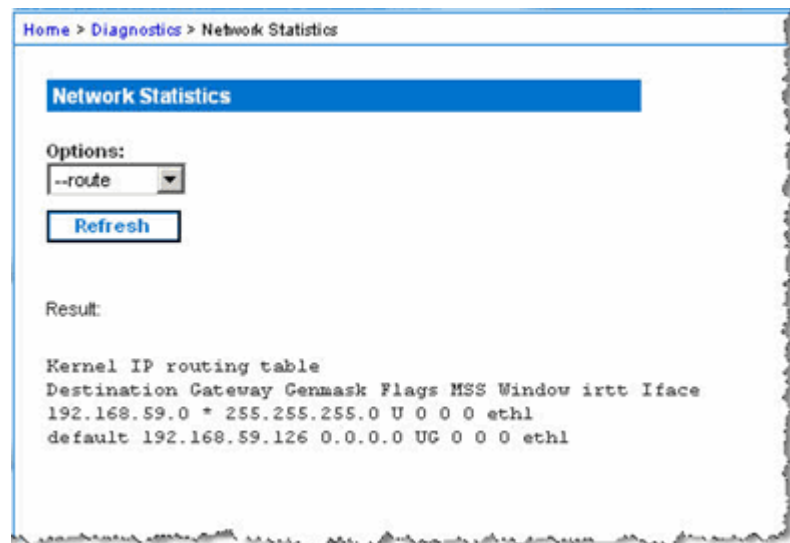
Result:

Ip:
8803 total packets received
0 forwarded
0 incoming packets discarded
8802 incoming packets delivered
8522 requests sent out
Icmp:
0 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
0 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
Tcp:
6 active connections openings
849 passive connection openings
0 failed connection attempts
15 connection resets received
1 connections established
7942 segments received
8304 segments send out
0 segments retransmited
0 bad segments received.
0 resets sent
Udp:
233 packets received
```

- Interfaces (介面) - 產生與下圖相似的頁面。



- Route (路由) - 產生與下圖相似的頁面。



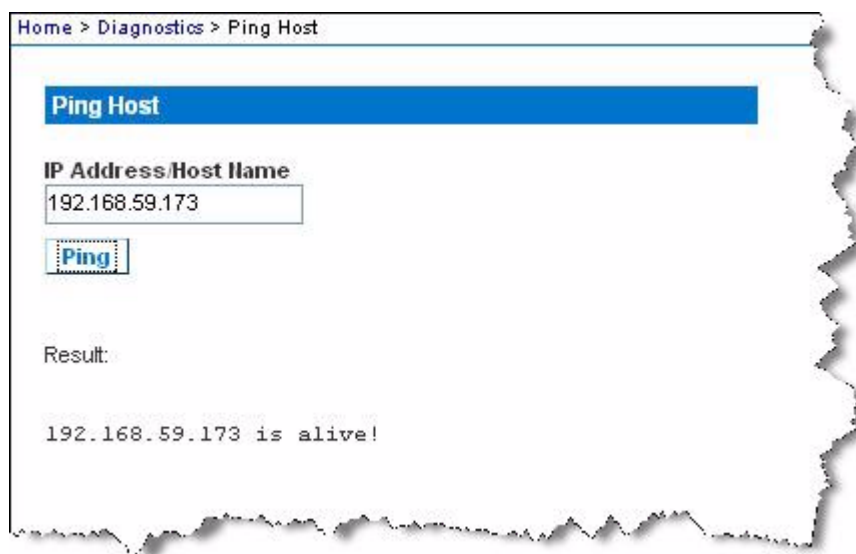
3. 按一下「Refresh」(重新整理)。隨即會在「Result」(結果) 欄位中顯示相關資訊。

偵測 (Ping) 主機頁面

Ping 是一種網路工具，用以測試可否連到 IP 網路上的特定主機或 IP 位址。使用「Ping Host」(偵測主機) 頁面可判斷目標伺服器或其他 KX II-101-V2 是否可供存取。

▶ 若要偵測 (ping) 主機：

1. 選擇「Diagnostics」(診斷) > 「Ping Host」(偵測主機)。隨即會開啟「Ping Host」(偵測主機) 頁面。



2. 在「IP Address/Host Name」(IP 位址/主機名稱) 欄位中輸入主機名稱或 IP 位址。

附註：主機名稱的長度不可超過 232 個字元。

3. 按一下「Ping」(偵測)。隨即會在「Result」(結果) 欄位中顯示偵測結果。

Trace Route to Host (追蹤主機路由) 頁面

Trace Route 是一種網路工具，用以判斷所指定主機名稱或 IP 位址的路由歷程。

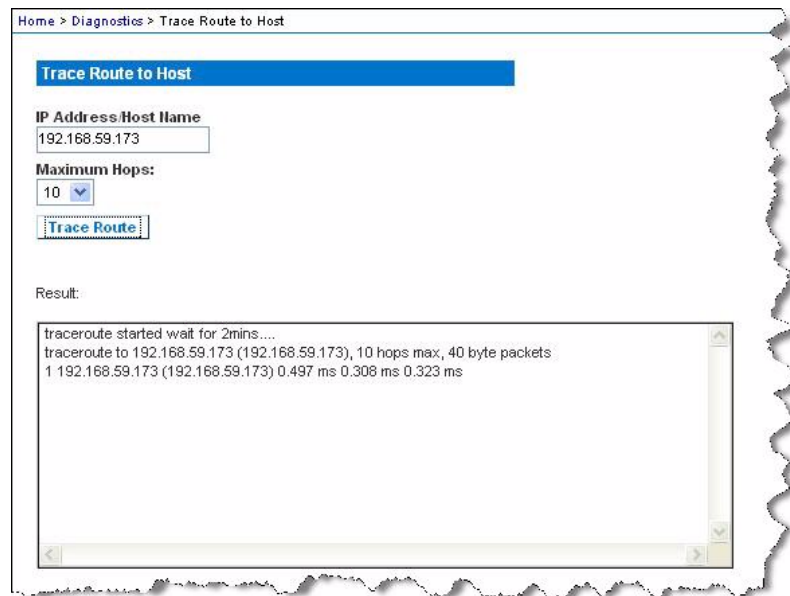
▶ 若要追蹤主機路由：

1. 選擇「Diagnostics」(診斷) > 「Trace Route to Host」(追蹤主機路由)。隨即會開啟「Trace Route to Host」(追蹤主機路由) 頁面。

2. 在「IP Address/Host Name」(IP 位址/主機名稱) 欄位中輸入 IP 位址或主機名稱。

附註：主機名稱的長度不可超過 232 個字元。

3. 從下拉式清單中選擇最大躍點 (5 到 50，增量為 5)。
4. 按一下「Trace Route」(追蹤路由)。如此即會針對指定的主機名稱或 IP 位址以及最大躍點，執行追蹤路由指令。並在「Result」(結果) 欄位中顯示追蹤路由的結果。



裝置診斷

附註：本頁面適合 *Raritan* 客服工程師或在「*Raritan* 技術支援部門」人員的指導下使用。

「Device Diagnostics」(裝置診斷) 頁面會將診斷資訊從 KX II-101-V2 下載到用戶端電腦。您可以選擇要執行或不執行「*Raritan* 技術支援部門」提供的選用診斷指令檔，來產生裝置診斷記錄檔。診斷指令檔可產生更多資訊，以供診斷問題。

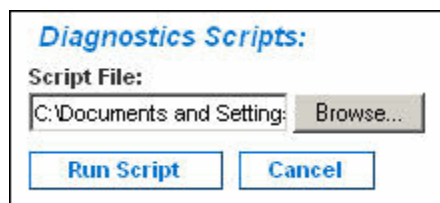
請使用下列設定：

- **Diagnostics Scripts** (診斷指令檔) - 在嚴重錯誤偵測階段作業過程中，載入「*Raritan* 技術支援部門」提供的特殊指令檔。此指令檔會上傳至裝置執行。**選用**
- **Device Diagnostic Log** (裝置診斷記錄) - 將診斷訊息快照集從 KX II-101-V2 裝置下載到用戶端。接下來，將此加密檔案傳送給「*Raritan* 技術支援部門」。只有 *Raritan* 才能轉譯此檔案。

附註：只有擁有管理權限的使用者才可存取本頁面。

▶ 若要執行 KX II-101-V2 系統診斷：

1. 選擇「Diagnostics」(診斷) > 「Device Diagnostics」(裝置診斷)。隨即會開啟「Device Diagnostics」(裝置診斷) 頁面。
2. (選用) 如果您已收到「*Raritan* 技術支援部門」提供的診斷指令檔，請執行下列步驟。否則，請跳至步驟 3。
 - a. 擷取 *Raritan* 提供的診斷檔案，請在必要時將檔案解壓縮。
 - b. 按一下「Browse」(瀏覽)。隨即會開啟「Choose file」(選擇檔案) 對話方塊。
 - c. 找到並選取此診斷檔案。
 - d. 按一下「Open」(開啟)。隨即會在「Script File」(指令檔) 欄位中顯示檔案：



- e. 按一下「Run Script」(執行指令檔)。
3. 建立診斷檔案並傳送給「*Raritan* 技術支援部門」：

- a. 按一下「Save to File」(另存檔案)。隨即會出現「File Download」(下載檔案) 對話方塊。



- b. 按一下「Save」(儲存)。隨即會出現「Save As」(另存新檔) 對話方塊。
 - c. 瀏覽到所要的目錄，然後按一下「Save」(儲存)。
4. 依照「Raritan 技術支援部門」的指示，以電子郵件傳送此檔案。

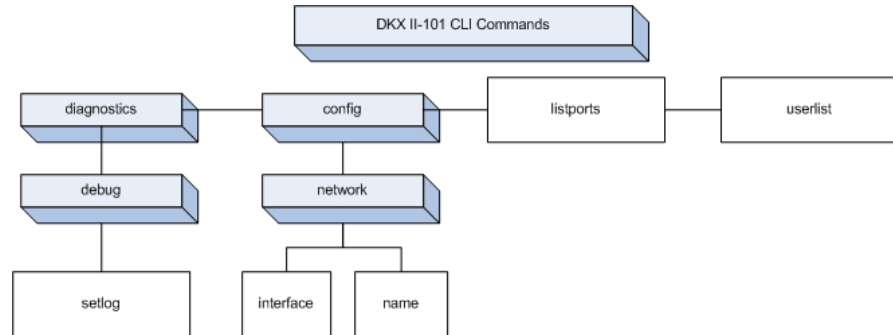
本章內容

概覽.....	169
使用 CLI 存取 KX II-101-V2.....	170
KX II-101-V2 的 SSH 連線	170
登入.....	171
瀏覽 CLI	171
CLI 指令	173

概覽

本章提供可與 KX II-101-V2 一起使用的 CLI 指令概覽。如需指令與定義清單以及在本章中提供這些指令範例之各小節的連結，請參閱 **<CLI 指令 >** (請參閱 "**CLI 指令**" p. 173)。

下圖提供 CLI 指令概覽：



附註：從 CLI 的所有層級到上述的功能，均可以使用下列常見的指令：*top*、*history*、*logout*、*quit* 以及 *help*。

使用 CLI 存取 KX II-101-V2

使用下列任一種方法來存取 KX II-101-V2：

- TELNET，透過 IP 連線
- SSH (Secure Shell)，透過 IP 連線
- 多功能管理序列連接埠，透過 RS-232 序列介面使用提供的纜線以及像是 HyperTerminal 的終端機模擬程式。

您可以從下列位置取得數種可用的 SSH/TELNET 用戶端：

- PuTTY - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- SSH 用戶端，來自 ssh.com - www.ssh.com <http://www.ssh.com>
- Applet SSH 用戶端 - www.netspace.org/ssh
<http://www.netspace.org/ssh>
- OpenSSH 用戶端 - www.openssh.org <http://www.openssh.org>

附註：透過 SSH 或 TELNET 存取 CLI，需要在 KX II-101-V2 遠端用戶端的「Device Services」(裝置服務) 頁面中設定存取權。請參閱〈裝置服務〉(請參閱 "裝置服務" p. 107)。

KX II-101-V2 的 SSH 連線

使用可支援 SSHv2 的任何 SSH 用戶端，來與裝置連線。您必須啟用「Device Services」(裝置服務) 頁面中的 SSH 存取權。請參閱〈裝置服務〉(請參閱 "裝置服務" p. 107)。

附註：基於安全性考量，KX II-101-V2 不支援 SSH V1 連線。

Windows 電腦的 SSH 存取方法

► 若要從 Windows® 電腦開啟 SSH 階段作業：

1. 啟動 SSH 用戶端軟體。
2. 輸入 KX II-101-V2 伺服器的 IP 位址。例如 192.168.0.192。
3. 選擇 SSH，然後使用預設的組態連接埠 22。
4. 按一下「Open」(開啟)。
5. 隨即會出現 login as: 提示

UNIX/Linux 工作站的 SSH 存取方法

- ▶ 若要從 UNIX®/Linux® 工作站開啟 SSH 階段作業，而且要以 admin 使用者的身分登入，請輸入下列指令：

```
ssh -l admin 192.168.30.222
```

隨即會出現密碼提示。

登入

- ▶ 若要登入：

1. Login: admin
2. 隨即會出現密碼提示。變更預設的密碼：*raritan*。

隨即會出現歡迎訊息。現在您已經以管理員的身分登入。

在檢閱下面的 <瀏覽 CLI> (請參閱 "瀏覽 CLI" p. 171) 一節之後，您便可以如 <設定 KX II-101-V2 使用終端機模擬程式 (選用)> (請參閱 "設定 KX II-101-V2 使用終端機模擬程式 (選用)" p. 31) 中所述，執行初始組態設定工作。

瀏覽 CLI

使用 CLI 之前，最好可以瞭解 CLI 的瀏覽方式與語法。還有一些按鍵組合可以簡化 CLI 的使用。

CLI 提示

指令行介面提示可指出目前的指令層級。提示的根目錄部份為登入名稱。對於使用終端機模擬應用程式的直接管理序列連接埠連線，指令的根目錄部份則是 Admin Port。

```
admin >
```

對於 Telnet/SSH，指令的根目錄部份則是 admin：

```
admin > config > network >
```

0

自動完成指令

CLI 支援自動完成只輸入部分的指令。在輸入項目的前幾個字元之後，按下 **Tab** 鍵。如果字元可找到唯一相符的項目，CLI 便會完成該項目。

- 如果找不到符合的項目，CLI 便會顯示該層級的有效項目。
- 如果找到多個符合的項目，CLI 便會顯示所有的有效項目。

繼續輸入文字以構成唯一的項目，然後按下 **Tab** 鍵，以自動完成該項目。

CLI 語法 - 祕訣與快速鍵

祕訣：

- 指令是以英數字元順序列出。
- 指令不區分大小寫。
- 參數名稱是沒有底線的單字。
- 使用未加上引數的指令，預設會顯示該指令的目前設定。
- 在指令後面輸入問號 (?)，可產生該指令的說明。
- 豎直線符號 (|) 代表其中的選項為選用，或需要設定關鍵字或引數。

快速鍵

- 按下向上鍵，可顯示上一個項目。
- 按下 **Backspace** 鍵，可刪除上一個輸入的字元。
- 如果您輸入錯誤的參數，按下 **Ctrl + C**，可終止指令或取消指令。
- 按下 **Enter** 鍵，可執行指令。
- 按下 **Tab** 鍵，可完成指令。例如，Admin Port > Conf。然後系統便會顯示 Admin Port > Config > 提示。

所有指令行介面層級的常見指令

CLI 指令一節會列出所有 CLI 層級可用的指令。這些指令也可協助瀏覽 CLI。

指令	說明
top	返回 CLI 階層的最上層，或返回「使用者名稱」提示。
history	顯示使用者最近輸入 KX II-101-V2 CLI 的 200 個指令。
help	顯示 CLI 語法的概覽。
quit	讓使用者回到上一層。
logout	登出使用者階段作業。

CLI 指令

下表列出和說明所有可用 CLI 指令。

指令	說明
config	切換到「Configuration」(組態) 功能表。
diagnostics	切換到「Diagnostics」(診斷) 功能表。請參閱 <診斷> (請參閱 "診斷" p. 174)。
debug	切換到「Debug」(偵錯) 功能表。請參閱 <偵錯> (請參閱 "除錯" p. 174)。
help	顯示 CLI 語法的概覽。
history	顯示目前階段作業的指令行歷程記錄。
interface	設定 KX II-101-V2 網路介面。
ipv6_interface	設定/取得 IPv6 網路參數。
listports	列出連接埠、連接埠名稱、連接埠類型、連接埠狀態以及連接埠可用性。請參閱 <Listports 指令> (請參閱 "Listports 指令" p. 177)。
logout	登出目前的 CLI 階段作業。
name	設定裝置名稱。請參閱 <Name 指令> (請參閱 "Name 指令" p. 176)。
network	顯示網路組態以及讓您設定網路設定。請參閱 <網路> (請參閱 "網路" p. 175)。
quit	返回前一個指令。
setlog	設定裝置記錄選項。請參閱 <Setlog 指令> (請參閱 "Setlog 指令" p. 174)。
top	切換到根目錄功能表。
userlist	列出作用中的使用者數目、使用者名稱、連接埠以及狀態。請參閱 <Userlist 指令> (請參閱 "Userlist 指令" p. 177)。

診斷

「Diagnostics」(診斷) 功能表可讓您為不同的 KX II-101-V2 模組設定記錄選項。您應只有在 Raritan 技術支援工程師的指導下，方可設定記錄選項。這些記錄選項可讓支援工程師，取得可用於偵測與疑難排解用途的正確資訊。支援工程師指導您這樣做時，會告訴您如何設定記錄選項，以及如何產生記錄檔，以傳送給 Raritan 技術支援部門。

重要：只有在 Raritan 技術支援工程師的監督指導之下，方可設定記錄選項。

除錯

「Diagnostics」(診斷) > 「Debug」(除錯) 功能表可讓您選擇 Setlog 指令，設定 KX II-101-V2 的記錄選項。

Setlog 指令

Setlog 指令可讓您對不同的 KX II-101-V2 模組設定記錄層級，以及檢視每個模組目前的記錄層級。Setlog 指令的語法如下：

```
setlog [module <module>] [level <level>] [vflag <vflag>] [verbose <on|off>]
Set/Get diag log level
```

Setlog 指令選項如下表所述：Raritan 技術支援人員會告訴您如何設定這些設定。

指令選項	說明
module	模組名稱。
level	診斷層級： <ul style="list-style-type: none"> ▪ err ▪ warn ▪ info ▪ debug ▪ trace
vflag	詳細資訊旗標的類型： <ul style="list-style-type: none"> ▪ timestamp ▪ module ▪ thread ▪ fileline

指令選項	說明
verbose [on off]	開啟和關閉詳細資訊記錄功能。

Setlog 指令範例

下列 **Setlog** 指令設定了記錄層級，利用為 **libpp_serial** 模組而記錄的詳細資訊進行除錯。

```
Setlog module libpp_serial level debug verbose on
```

組態

「**Configuration**」(組態) 功能表可讓您存取網路指令，用以設定網路介面以及設定裝置名稱。

網路

「**Configuration**」(組態) > 「**Network**」(網路) 指令是用來設定 **KX II-101-V2** 網路介面與裝置名稱。

指令	說明
interface	設定 KX II-101-V2 裝置網路介面。
name	設定裝置名稱。
ipv6_interface	設定/取得 IPv6 網路參數。

Interface 指令

interface 指令是用來設定 **KX II-101-V2** 網路介面。在接受此指令之後，裝置會捨棄 **HTTP/HTTPS** 連線，然後初始化新的網路連線。所有 **HTTP/HTTPS** 使用者必須使用新的 **IP** 位址以及正確的使用者名稱與密碼，重新連線到該裝置。請參閱〈安裝與組態〉。

interface 指令的語法如下：

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask <subnetmask>] [gw <ipaddress>] [mode <auto/10hdx/10fdx/100hdx/100fdx>]
```

network 指令選項如下表所述：

指令選項	說明
ipauto	靜態或動態 IP 位址
ip ipaddress	指派給 KX II-101-V2 以供從 IP 網路存取的 IP 位址
mask subnetmask	從 IP 管理員處取得的子網路遮罩
gw ipaddress	從 IP 管理員處取得的閘道 IP 位址
mode <auto 100fdx>	將「乙太網路模式」設定為自動偵測，或強制使用 100 Mb/s 全雙工 (100fdx)

Interface 指令範例

下列指令可設定 IP 位址、遮罩以及閘道位址，還將模式設定為自動偵測。

```
Admin Port > Config > Network > interface ipauto none
ip 192.168.50.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

Name 指令

name 指令是用來設定裝置與主機名稱。

語法

```
name [unitname name] [domain name] [force <true|false>]
```

name 指令範例

下列指令可設定裝置名稱：

```
Admin Port > Config > Network > name unitname <unit name>
domain <host name> force trues
```

IPv6 指令

使用 IPv6 指令可設定 IPv6 網路參數以及擷取現有 IPv6 參數。

```
Ipv6_interface mode enable ipauto none ip
2001:db8:290c:1291::17 prefixlen 128 gw
2001:db8:290c:1291::1
```

Listports 指令

Listports 指令可列出使用中的使用者數目、使用者名稱、連接埠以及狀態。

Listports 指令範例

```
Admin Port > listports
Port Port                Port Port  Port
No.  Name                  Type Status Availability
1 - Dominion_KXII-101_V2_Port KVM  up      idle
```

Userlist 指令

Userlist 指令列出連接埠、連接埠名稱、連接埠類型、連接埠狀態以及連接埠可用性。

Userlist 指令範例

```
Admin Port > Userlist
Active user number:1
User Name | From          | Status
-----
-
admin     | Admin Port | active
```

本章內容

概覽.....	178
從 CC-SG 移除對 KX II-101-V2 的管理.....	179
在 Proxy 模式下使用 CC-SG.....	180

概覽

CC-SG 能夠管理 KX II-101-V2。一旦受 CC-SG 管理，就支援從 iPad® 或 iPhone® 行動裝置存取 KX II-101-V2。如需將 KX II-101-V2 新增至 CC-SG 以讓 CC-SG 能夠管理裝置，以及設定裝置行動存取功能的詳細資訊，請參閱 CC-SG 文件。

當 KX II-101-V2 裝置受 CommandCenter Secure Gateway 控制，而您嘗試直接使用「KX II-101-V2 遠端主控台」存取裝置時，在輸入有效的使用者名稱及密碼後，隨即會顯示下列訊息：

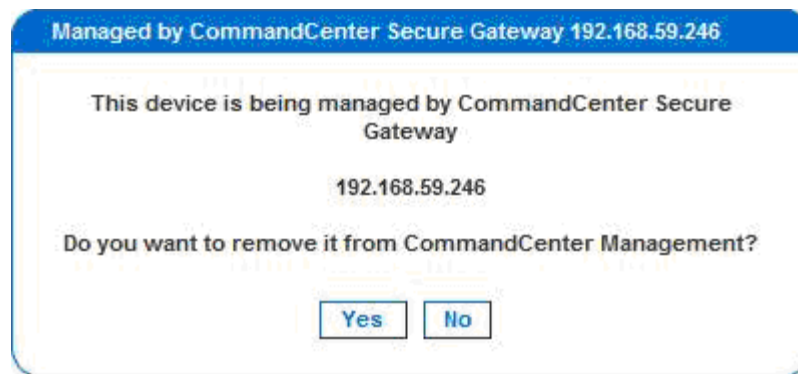


從 CC-SG 移除對 KX II-101-V2 的管理

除非 CC-SG 釋放對 KX II-101-V2 的控制，否則您無法直接存取裝置。但如果 KX II-101-V2 未接獲 CommandCenter 的活動訊號訊息 (例如 CommandCenter 不在網路中)，為了存取裝置，您可以解除 CC-SG 對 KX II-101-V2 的控制。此項作業要使用 CC 解除管理功能完成。

附註：必須具有維護權限才能使用此功能。

若未接獲活動訊號訊息，直接存取裝置時會出現下列訊息：

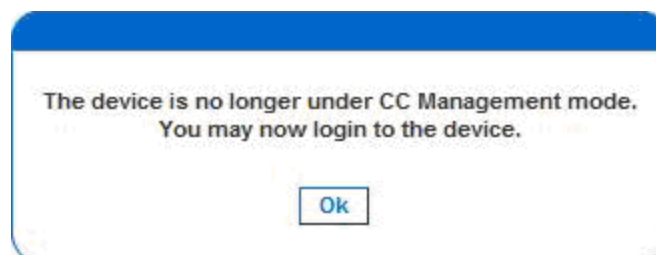


▶ 若要移除 CC-SG 對裝置的管理 (使用 CC 解除管理功能)：

1. 按一下「Yes」(是)。隨即會出現提示要求您確認動作：



2. 按一下「Yes」(是)。隨即會出現一則訊息，確認裝置不再受 CC 管理。



3. 按一下「OK」(確定)。隨即會開啟 KX II-101-V2 登入頁面。

在 Proxy 模式下使用 CC-SG

CC-SG Proxy 模式無法得知虛擬 KVM 用戶端的版本

在 Proxy 模式下，從 CommandCenter Secure Gateway (CC-SG) 啟動虛擬 KVM 用戶端時，無法得知虛擬 KVM 用戶端版本。在「About Raritan Virtual KVM Client」(關於 Raritan 虛擬 KVM 用戶端) 對話方塊中，版本會顯示為「Version Unknown」(版本不明)。

Proxy 模式與 MPC

如果您是在 CC-SG 組態下使用 KX II-101-V2，若計劃要使用多平台用戶端 (MPC)，請不要使用 CC-SG Proxy 模式。

本章內容

實物規格	181
支援的作業系統 (用戶端)	182
支援的瀏覽器	183
接頭.....	184
經過認證的數據機.....	184
支援的視訊解析度.....	184
支援的鍵盤語言	185
使用的 TCP 及 UDP 連接埠	186
Network Speed Settings	188
9 針腳.....	189

實物規格

KX II-101-V2...	說明
外型規格	零 U 式外型；可垂直或水平裝載機架 (隨附托架組)
尺寸(長 x 寬 x 高)	4.055 x 2.913 x 1.063 英吋；103 x 74 x 27 公釐
重量	0.6498 英磅或 0.295 公斤
電源	AC/DC (100-240V~/ 6VDC) 變壓器或乙太網路供電 (PoE)；與 IEEE 802.3af 相容 Mid-Span Power Insertion Signal-Pair Power Insertion Class 2 PoE 供電裝置 (7 瓦以下)
操作溫度	0° - 40°C (32° - 104°F)
濕度	20% -85% RH
指示燈： 藍色 RARITAN 背光標誌 黃色與綠色 LED 指示燈	開機與電源指示燈 網路活動與連線速度指示燈
本機連線：	1 個 Mini USB 連接埠，可用於鍵盤 / 滑鼠以及連至目標的虛擬媒體連線 1 個 MiniDIN9 連接埠，可用於全面性 RS-232

KX II-101-V2...	說明
	功能、數據機連線以及 Dominion PX 連線的多功能序列連接埠
遠端連線：網路通訊協定	1 個有活動狀態指示燈的乙太網路 (RJ45) 連接埠 TCP/IP、TELNET、SSH、HTTP、HTTPS、安全 LDAP、RADIUS、LDAP、SNMP v2 與 v3、DHCP 及 SNTP，雙重堆疊：IPv4 與 IPv6
保固期	為期兩年並提供進階更換服務*

支援的作業系統 (用戶端)

虛擬 KVM 用戶端及多平台用戶端 (MPC) 支援下列作業系統：

用戶端作業系統	用戶端是否支援虛擬媒體 (VM) ?
Windows 7®	是
Windows XP®	是
Windows 2008®	是
Windows Vista®	是
Windows 2000® SP4 Server	是
Windows 2003® Server	是
Windows 2008® Server	是
Red Hat® Desktop 5.0	是
Red Hat Desktop 4.0	是
Open SUSE 10、11	是
Fedora® 13 與 14	是
Mac® OS	是
Solaris™	否
Linux®	是，只有 ISO 映像檔

JRE™ 外掛程式可在 Windows® 32 位元與 64 位元作業系統使用。MPC 與 VKC 只能從 32 位元瀏覽器或 64 位元 IE7 或 IE8 瀏覽器啟動。

下列是 Java™ 32 位元與 64 位元 Windows 作業系統需求。

模式	作業系統	瀏覽器
Windows x64 32 位元模式	Windows XP®	<ul style="list-style-type: none"> Internet Explorer® 6.0 SP1+ 或 7.0、IE 8 Firefox® 1.06 - 4 或更新版本
	Windows Server 2003®	<ul style="list-style-type: none"> Internet Explorer 6.0 SP1++、IE 7、IE 8 Firefox 1.06 - 3
	Windows Vista®	<ul style="list-style-type: none"> Internet Explorer 7.0 或 8.0
	Windows 7®	<ul style="list-style-type: none"> Internet Explorer 9.0 Firefox 1.06 - 4 或更新版本
Windows x64 64 位元模式	Windows XP	64 位元作業系統，32 位元瀏覽器：
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	64 位元模式，64 位元瀏覽器：
	Windows Server 2003	
	Windows Server 2008	<ul style="list-style-type: none"> Internet Explorer 7.0 或 8.0
	Windows 7	

支援的瀏覽器

KX II-101-V2 支援下列瀏覽器：

- Internet Explorer® 7 至 9
- Firefox® 4 或更新版本
- Safari® 3 或更新版本

接頭

介面類型	長度		說明
	英吋	公分	
KVM 纜線搭配 PS/2 及 USB	15"	38 cm	整合式纜線
MiniDin9(M) 對 DB9(F)	72"	182 cm	序列纜線
DKX2-101-V2-PDU (選用)	70.86"	180 cm	連接 Dominion PX 的纜線

經過認證的數據機

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

支援的視訊解析度

確認 KX II-101-V2 能支援每部目標伺服器的視訊解析度與螢幕更新頻率，同時訊號為非交錯式。

視訊解析度與纜線長度是取得滑鼠同步的重要因素。

KX II-101-V2 支援以下解析度：

解析度	
640x350 @70Hz	1024x768@85
640x350 @85Hz	1024x768 @ 75Hz
640x400 @56Hz	1024x768 @ 90Hz
640x400 @84Hz	1024x768 @ 100Hz
640x400 @85Hz	1152x864 @ 60Hz
640x480 @ 60Hz	1152x864 @ 70Hz
640x480 @ 66.6Hz	1152x864 @ 75Hz

解析度	
640x480 @ 72Hz	1152x864 @ 85Hz
640x480 @ 75Hz	1152x870 @ 75.1Hz
640x480 @ 85Hz	1152x900 @ 66Hz
720x400 @ 70Hz	1152x900 @ 76Hz
720x400 @ 84Hz	1280x720 @ 60Hz
720x400 @ 85Hz	1280x960 @ 60Hz
800x600 @ 56Hz	1280x960 @ 85Hz
800x600 @ 60Hz	1280x1024 @ 60Hz
800x600 @ 70Hz	1280x1024 @ 75Hz
800x600 @ 72Hz	1280x1024 @ 85Hz
800x600 @ 75Hz	1360x768 @ 60Hz
800x600 @ 85Hz	1366x768 @ 60Hz
800x600 @ 90Hz	1368x768 @ 60Hz
800x600 @ 100Hz	1400x1050 @ 60Hz
832x624 @ 75.1Hz	1440x900 @ 60Hz
1024x768 @ 60Hz	1600x1200 @ 60Hz
1024x768 @ 70	1680x1050 @ 60Hz
1024x768 @ 72	1920x1080 @ 60Hz

附註：「複合式同步訊號」與「綠色視訊同步」需有額外的介面卡。

附註：預設可能無法使用一些解析度。如果未看到解析度，請先插入監視器，移除監視器，然後再插入 CIM。

附註：如果目標伺服器的顯示卡支援 1440x900 與 1680x1050 解析度，但卻未顯示，則可能需要 DDC-1440 或 DDC-1680 介面卡。

支援的鍵盤語言

KX II-101-V2 可為下表列出的語言提供鍵盤支援：

語言	地區	鍵盤配置
美式英文	美國與大部分英語系國家：例如，加拿大、澳洲以及紐西蘭。	美式鍵盤配置
國際通用英文	美國與大部分英語系國家：例如，	美式鍵盤配置

語言	地區	鍵盤配置
	荷蘭。	
英式英文	英國	英式鍵盤配置
繁體中文	香港特別行政區、中華民國 (台灣)	繁體中文鍵盤
簡體中文	中華人民共和國 (大陸)	簡體中文鍵盤
韓文	南韓	韓文鍵盤
日文	日本	JIS 鍵盤
法文	法國	法文 (AZERTY) 鍵盤配置。
德文	德國與奧地利	德文鍵盤 (QWERTZ 配置)
法文	比利時	比利時文鍵盤
挪威文	挪威	挪威文鍵盤
丹麥文	丹麥	丹麥文鍵盤
瑞典文	瑞典	瑞典文鍵盤
匈牙利文	匈牙利	匈牙利文鍵盤
斯洛維尼亞文	斯洛維尼亞	斯洛維尼亞文鍵盤
義大利文	義大利	義大利文鍵盤
西班牙文	西班牙與大部分西語系國家	西班牙文鍵盤
葡萄牙文	葡萄牙	葡萄牙文鍵盤

使用的 TCP 及 UDP 連接埠

連接埠	說明
HTTP (連接埠 80)	您可以視需要來設定此連接埠。請參閱 <HTTP 與 HTTPS 連接埠設定> (請參閱 "HTTP 與 HTTPS 連接埠設定" p. 108)。根據預設，KX II-101-V2 透過 HTTP (連接埠 80) 所接獲的所有要求都會自動轉寄到 HTTPS 以取得全面安全性。KX II-101-V2 為方便使用者所以仍會回應連接埠 80，讓使用者不必明確在 URL 欄位中輸入也能存取 KX II-101-V2，但仍保有全面安全性。
HTTPS (連接埠 443)	您可以視需要來設定此連接埠。請參閱 <HTTP 與 HTTPS 連接埠設定> (請參閱 "HTTP 與 HTTPS 連接埠設定" p. 108)。根據預設，此連接埠可用於多種用途，包括 HTML 用戶端的網頁伺服器、將用戶端軟體 (MPC/VKC) 下載至用戶端的主機，以及將 KVM 與虛擬媒體資料流傳輸到用戶端。
KX II-101-V2 (Raritan KVM-over-IP) 通訊協定(可設定連接埠 Port 5000)	此連接埠可用於探查其他 Dominion 裝置，以及讓力登裝置與系統進行通訊，包括可使用 CC-SG 管理的裝置適用的 CC-SG。預設會設為連接埠 5000，但您可設定為使用目前不在使用中的任何 TCP 連接埠。如需如何設定此設定的詳細資訊，請參閱 <網路設定> (請參閱 "網路設定" p. 102)。
SNTP (時間伺服器)，位於可設定 UDP 連接埠 123	KX II-101-V2 提供可與中央時間伺服器同步其內部時鐘的選用功能。此功能需要使用 UDP 連接埠 123 (SNTP 標準項目)，但也可設定為使用任何指定的連接埠。 選用
LDAP/LDAPS (位於可設定連接埠 389 或 636)	如果 KX II-101-V2 設定為透過 LDAP/LDAPS 通訊協定從遠端驗證使用者登入，即會使用連接埠 389 及 636，但系統也可設定為使用任何指定的連接埠。 選用
RADIUS (位於可設定連接埠 1812)	如果 KX II-101-V2 設定為透過 RADIUS 通訊協定從遠端驗證使用者登入，即會使用連接埠 1812，但系統也可設定為使用任何指定的連接埠。 選用
RADIUS 帳戶管理 (位於可設定連接埠 1813)	如果 KX II-101-V2 設定為透過 RADIUS 通訊協定從遠端驗證使用者登入，同時也使用 RADIUS 帳戶管理來記錄事件，則會使用連接埠 1813 或您指定的其他連接埠來傳送記錄通知。
SYSLOG (位於可設定 UDP 連接埠 514)	如果 KX II-101-V2 設定為將訊息傳送至 Syslog 伺服器，則會使用指定的連接埠進行通訊，即 UDP 連接埠 514。
SNMP 預設 UDP 連接埠	連接埠 161 是用於連入/連出讀取/寫入 SNMP 存取，而連接埠 162 則用於 SNMP 設陷連出流量。 選用
TCP 連接埠 22	連接埠 22 是用於 KX II-101-V2 指令行介面 (當您與「Raritan 技術支援部門」人員一起工作時)。

網路速度設定


KX II-101-V2 網路速度設定

網路交換器 連接埠設定	自動	100/全雙工	100/半雙工	10/全雙工	10/半雙工
自動	最快可用速度	KX II-101-V2 : 100/全雙工 交換器: 100/半雙工	100/半雙工	KX II-101-V2 : 10/全雙工 交換器: 10/半雙工	10/半雙工
100/全雙工	KX II-101-V2 : 100/半雙工 交換器: 100/全雙工	100/全雙工	KX II-101-V2 : 100/半雙工 交換器: 100/全雙工	無通訊	無通訊
100/半雙工	100/半雙工	KX II-101-V2 : 100/全雙工 交換器: 100/半雙工	100/半雙工	無通訊	無通訊
10/全雙工	KX II-101-V2 : 10/半雙工 交換器: 10/全雙工	無通訊	無通訊	10/全雙工	KX II-101-V2 : 10/半雙工 交換器: 10/全雙工
10/半雙工	10/半雙工	無通訊	無通訊	KX II-101-V2 : 10/全雙工 交換器: 10/半雙工	10/半雙工


圖例：

 運作不如預期

 支援

 可運作，但不建議

 乙太網路規格並不支援；產品可通訊，但會發生衝突

 根據乙太網路規格，這些應為「無通訊」，不過請注意，KX II-101-V2 的行為超出預期。

附註：對於可靠的網路通訊，則可將 KX II-101-V2 與 LAN 交換器設成相同的「LAN Interface Speed and Duplex」(LAN 介面速度與雙工)。例如，將 KX II-101-V2 與 LAN 交換器同時設定為「Autodetect」(自動偵測，建議使用)，或將兩者設定為固定速度/雙工，例如 100MB/s/Full (全雙工)。

9 針腳

針腳定義	
1	DTR (輸出)
2	TXD (輸出)
3	RXD (輸入)
4	DCD/DSR (輸入) *
5	GND
6	DTR (輸出)
7	CTS (輸入)
8	RTS (輸出)
9	RI (輸入)

附註：本章中的程序應交由經驗豐富的使用者執行。

本章內容

傳回使用者群組資訊	190
設定登錄允許對架構進行寫入作業	191
建立新屬性.....	191
新增類別的屬性	193
更新結構描述快取.....	194
編輯使用者成員的 <code>rciusergroup</code> 屬性.....	194

傳回使用者群組資訊

順利完成驗證之後，請立即使用本節中的資訊，傳回使用者群組資訊（以及協助授權）。

從 LDAP

當 LDAP/LDAPS 驗證成功時，KX II-101-V2 會根據使用者群組的權限，決定特定使用者的權限。遠端 LDAP 伺服器可透過傳回具有下列名稱的屬性，來提供這些使用者群組的名稱：

`rciusergroup` 屬性類型：字串

LDAP/LDAPS 伺服器上需要有架構擴充功能。請聯絡驗證伺服器管理員以啟用此屬性。

從 Microsoft Active Directory

附註：此工作應交由經驗豐富的 *Active Directory*[®] 管理員執行。

從 Windows 2000[®] 作業系統伺服器的 Microsoft[®] Active Directory 傳回使用者群組資訊，需要更新 LDAP/LDAPS 架構。如需詳細資訊，請參閱 Microsoft 文件。

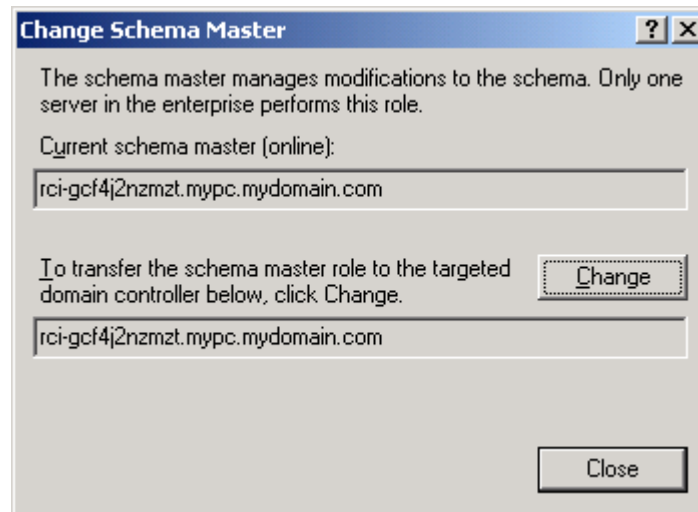
1. 安裝 Active Directory 的架構外掛程式。如需相關指示，請參閱 Microsoft Active Directory 文件。
2. 執行 Active Directory 主控台，然後選取「Active Directory Schema」（Active Directory 架構）。

設定登錄允許對架構進行寫入作業

若要允許網域控制站寫入架構，您必須設定允許架構更新的登錄項目。

▶ 若要允許對架構進行寫入作業：

1. 在視窗的左窗格中，以滑鼠右鍵按一下「Active Directory® Schema」(Active Directory 架構) 根節點，然後按一下「Operations Master」(操作主機)。隨即會出現「Change Schema Master」(變更架構主機)。



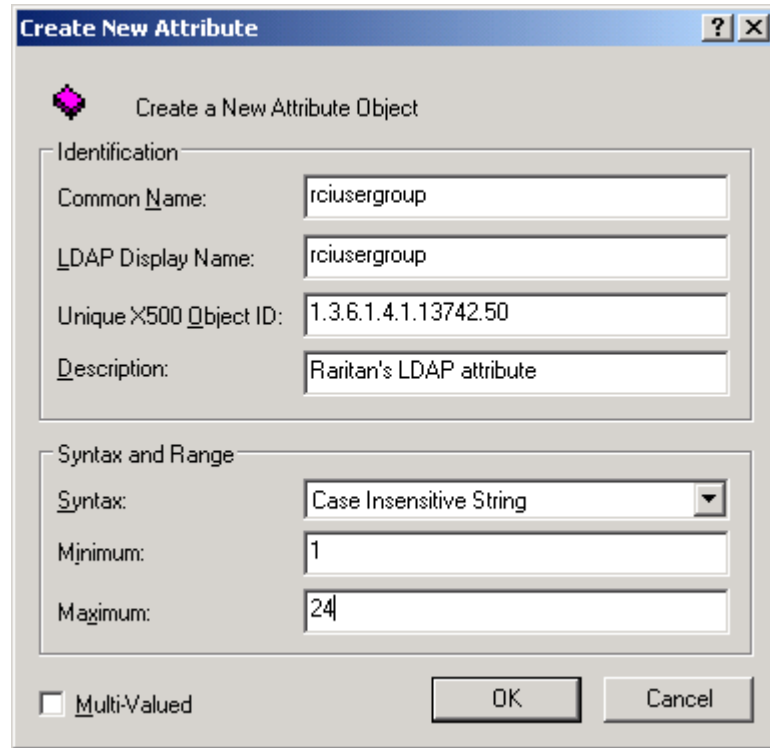
2. 選取「The Schema may be modified on this Domain Controller」(可在此網域控制站修改架構) 核取方塊。選用
3. 按一下「OK」(確定)。

建立新屬性

▶ 若要建立 `rciusergroup` 類別的新屬性：

1. 在視窗的左窗格中，按一下「Active Directory® Schema」(Active Directory 架構) 前的 + 號。
2. 以滑鼠右鍵按一下左窗格中的「Attributes」(屬性)。

3. 按一下「New」(新增)，然後選擇「Attribute」(屬性)。出現警告訊息時，按一下「Continue」(繼續) 即會顯示「Create New Attribute」(建立新屬性) 視窗。

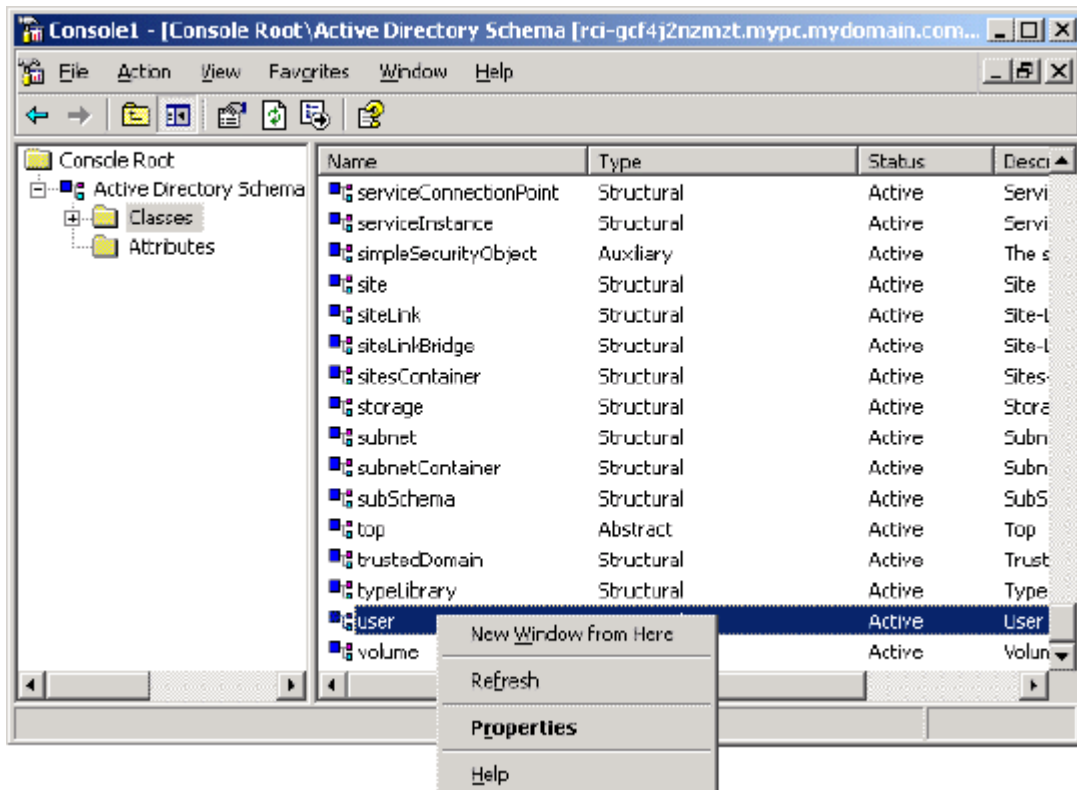


4. 在「Common Name」(一般名稱) 欄位中，輸入 *rciusergroup*。
5. 在「LDAP Display Name」(LDAP 顯示名稱) 欄位中，輸入 *rciusergroup*。
6. 在「Unique x5000 Object ID」(唯一的 x5000 物件 ID) 欄位中，輸入 *1.3.6.1.4.1.13742.50*。
7. 在「Description」(說明) 欄位中，輸入有意義的說明。
8. 按一下「Syntax」(語法) 下拉箭頭，然後從清單中選取「Case Insensitive String」(字串不區分大小寫)。
9. 在「Minimum」(最小值) 中，輸入 *1*。
10. 在「Maximum」(最大值) 中，輸入 *24*。
11. 按一下「OK」(確定) 即可建立新的屬性。

新增類別的屬性

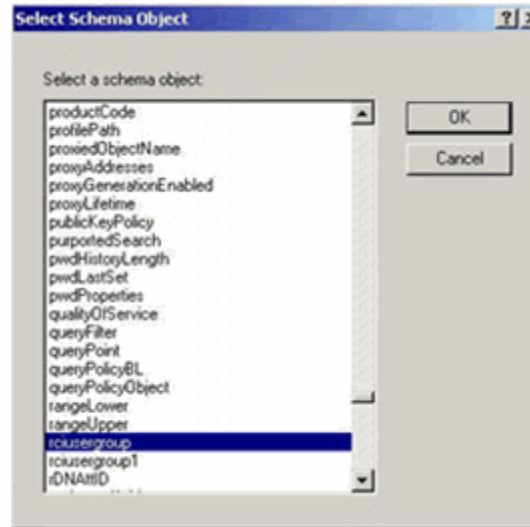
▶ 若要新增類別的屬性：

1. 在視窗的左窗格中，按一下「Classes」(類別)。
2. 在右窗格中捲動到 `user` 類別，然後在其上按一下滑鼠右鍵。



3. 從功能表中選取「Properties」(內容)。隨即會顯示「user Properties」(user 內容) 對話方塊。
4. 按一下以開啟「Attributes」(屬性) 索引標籤。
5. 按一下「Add」(新增)。

6. 從「Select Schema Object」(選取架構物件) 清單中選擇「rciusergroup」。



7. 在「Select Schema Object」(選取架構物件) 對話方塊中，按一下「OK」(確定)。
8. 在「User Properties」(User 內容) 對話方塊中，按一下「OK」(確定)。

更新結構描述快取

▶ 若要更新架構快取：

1. 在視窗的左窗格中，以滑鼠右鍵按一下「Active Directory® Schema」(Active Directory 架構)，然後選取「Reload the Schema」(重新載入架構)。
2. 將「Active Directory Schema MMC」(Active Directory 架構 MMC (Microsoft® Management Console)) 主控台縮到最小。

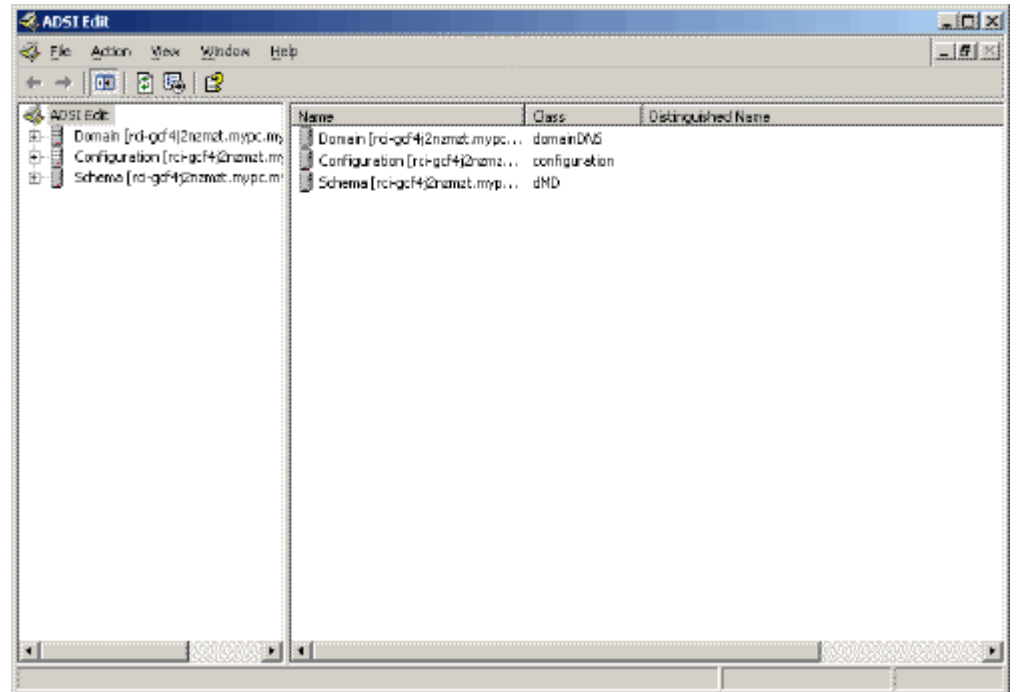
編輯使用者成員的 rciusergroup 屬性

若要在 Windows 2003® 伺服器上執行 Active Directory® 指令檔，請使用 Microsoft® 提供的指令檔 (可在 Windows 2003 伺服器安裝光碟上找到)。這些指令檔會隨 Microsoft® Windows 2003 安裝載入系統。ADSI (Active Directory 服務介面) 的作用如同低階 Active Directory 編輯器，可讓您執行一般的管理工作，如使用目錄服務新增、刪除及移動物件。

▶ 若要編輯 rciusergroup 群組內個別的使用者屬性：

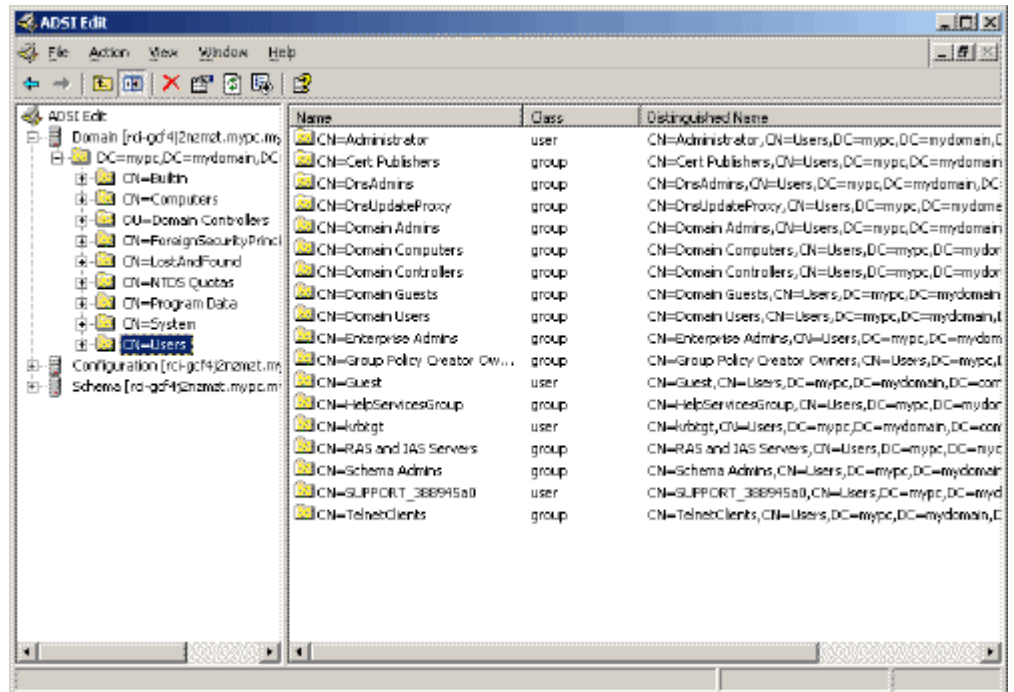
1. 從安裝光碟中選擇「Support」(支援) > 「Tools」(工具)。

- 按兩下 SUPTOOLS.MSI，安裝支援工具。
- 移至已安裝支援工具的目錄。執行 `adsiedit.msc`，隨即會開啟「ADSI Edit」(ADSI 編輯) 視窗。



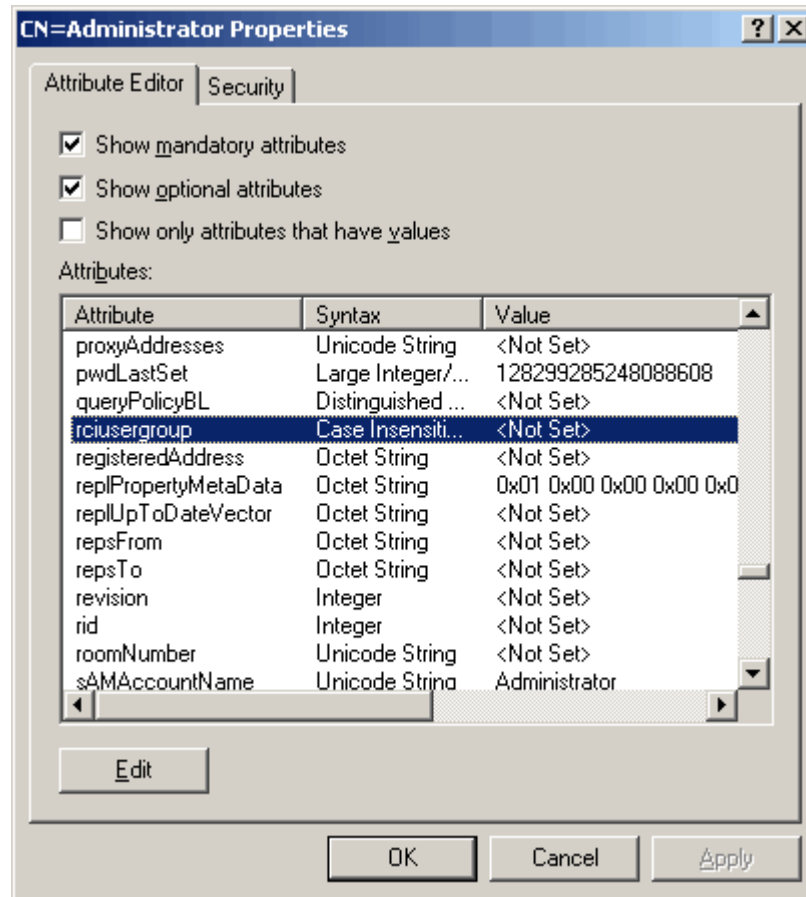
- 開啟「Domain」(網域)。

5. 在視窗的左窗格中，選取「CN=User」資料夾。

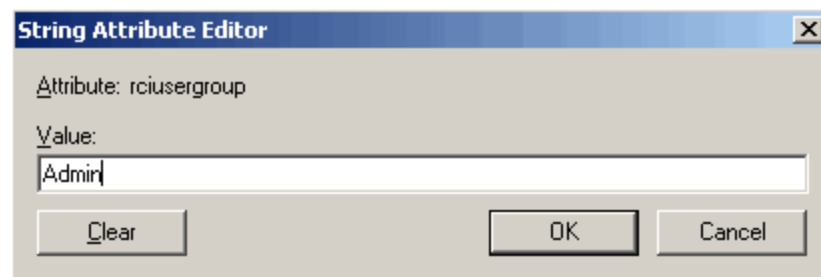


6. 在右窗格中，找出要調整其內容的使用者名稱。在使用者名稱上按一下滑鼠右鍵，然後選取「Properties」(內容)。

- 按一下「Attribute Editor」(屬性編輯器) 索引標籤 (如果尚未開啟)。從「Attributes」(屬性) 清單中選擇 `rciusergroup`。



- 按一下「Edit」(編輯)。隨即會開啟「String Attribute Editor」(字串屬性編輯器) 對話方塊。
- 在「Edit Attributes」(編輯屬性) 欄位中，輸入使用者群組 (建立於 KX II-101-V2)。按一下「OK」(確定)。



KX II-101-V2 裝置能夠在伺服器機架的任一側、面向前面或後面，以垂直或水平方式裝載。請使用 KX II-101-V2 產品組內隨附的托架與螺釘。

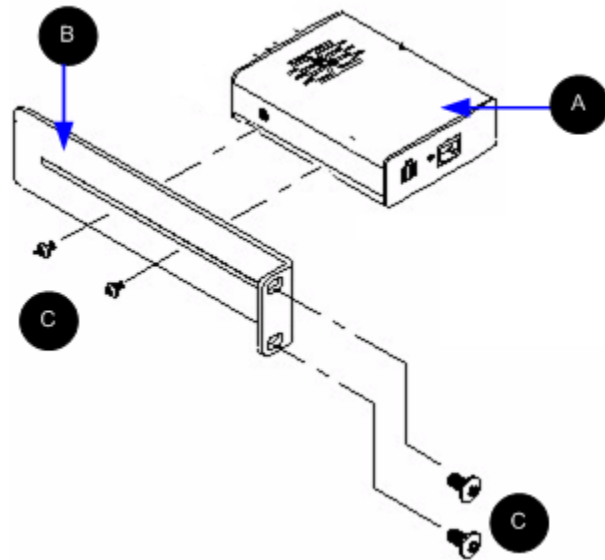
本章內容

裝上 L 型托架水平裝載 KX II-101-V2198

裝上 L 型托架水平裝載 KX II-101-V2

1. 使用隨附的螺釘裝上 L 型托架與 KX II-101-V2。調整托架位置後再鎖緊螺釘。
2. 以機架用的螺釘（機架製造商所提供）將 L 型托架附件裝到機架上。

此圖顯示在左側裝載 KX II-101-V2。若要在右側裝載 KX II-101-V2，請遵循上述指示進行，但要將托架裝在 KX II-101-V2 的右側。



圖解

A	KX II-101-V2
B	L 型托架
C	螺釘

本章內容

Java Runtime Environment (JRE)	200
IPv6 支援注意事項	201
鍵盤、視訊以及滑鼠注意事項	201
CC-SG	203

Java Runtime Environment (JRE)

重要：建議您停用 **Java™** 快取處理並清除 **Java** 快取。如需詳細資訊，請參閱 **Java** 文件或《**KVM** 與序列存取用戶端指南》。

因為遠端主控台會檢查 **Java** 版本，所以 **LX**、**KX II**、**KX II-101** 及 **KX II-101-V2** 遠端主控台與 **MPC** 需要 **Java Runtime Environment™** (**JRE™**) 才能運作。如果版本不正確或已過時，系統便會提示您，要求下載相容的版本。

Raritan 建議使用 **JRE 1.7** 版以達最佳效能，但遠端主控台與 **MPC** 亦可與 **JRE 1.6.x** 及更新的版本搭配運作 (**JRE 1.6.2** 除外)。

*附註：*為了讓多語言鍵盤能在 **LX**、**KX II**、**KX II-101** 及 **KX II-101-V2** 遠端主控台 (虛擬 **KVM** 用戶端) 中運作，請安裝 **JRE** 的多語言版本。

IPv6 支援注意事項

作業系統 IPv6 支援注意事項

Java

Java™ 1.6 支援下列各項使用 IPv6：

- Solaris™ 10 (及更新的版本)
- Linux® 核心 2.1.2 (及更新的版本)/RedHat 6.1 (及更新的版本)

Java 不支援下列 IPv6 組態：

- J2SE 在 Microsoft® Windows® 上不支援 IPv6。

Linux

- 使用 IPv6 時，建議您使用 Linux 核心 2.4.0 或更新版本。
- 必須安裝已啟用 IPv6 的核心，否則需要在啟用 IPv6 選項後重建核心。
- 使用 IPv6 時，Linux 還需要安裝數項網路公用程式。如需詳細資訊，請參閱 <http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html>

Windows

- Windows XP 與 Windows 2003 使用者需要安裝 Microsoft IPv6 Service Pack 以啟用 IPv6。

Mac Leopard

- 適用於 Mac® Leopard® 的 KX II 2.0.20 版不支援 IPv6。

鍵盤、視訊以及滑鼠注意事項

下列設備有一些鍵盤、視訊或滑鼠限制。若適用時則會提供因應措施。

Sun Blade 視訊、鍵盤及滑鼠支援限制

視訊

如果透過 KX II-101-V2 存取 Sun™ Blade 100，當 Sun Blade 正在開機時，本機連接埠上的視訊或遠端連線可能無法正常運作。為了避免發生此問題，請務必使用 Sun Open Boot 韌體 4.17.1 或以上版本。

鍵盤與滑鼠

因為 Sun Blades 不支援多個鍵盤，亦未提供本機鍵盤或滑鼠連接埠，所以無法同時使用 KX II-101-V2 與本機鍵盤。不過，Sun Blades 可以使用遠端鍵盤與滑鼠。

從本機鍵盤存取 BIOS 的限制

使用絕對滑鼠同步模式時，需要有 USB 連線。不過，本節中提及的鍵盤不支援以 USB 與本機鍵盤連線。若要經由本機連接埠透過 BIOS 或虛擬媒體存取本機鍵盤，請依照這些組態設定：

鍵盤	可用組態設定
Dell® OptiPlex™ GX280 - BIOS A03	<p>使用 Newlink USB 對 PS/2 轉接頭，本機與遠端鍵盤便可以存取 BIOS 與虛擬媒體。</p> <p>在「Keyboard/Mouse Setup」(鍵盤/滑鼠設定) 頁面上，將「Host Interface」(主機介面) 設定為 PS/2。請參閱 <鍵盤/滑鼠設定> (請參閱 "鍵盤/滑鼠設定" p. 111)。</p>
Dell Dimension 2400– BIOS A05	<p>在「Keyboard/Mouse Setup」(鍵盤/滑鼠設定) 頁面上，將「Host Interface」(主機介面) 設定為 PS/2。請參閱 <鍵盤/滑鼠設定> (請參閱 "鍵盤/滑鼠設定" p. 111)。</p>
Dell Optiplex 170L - BIOS A07	<p>PS/2 加上 PS/2 對 USB 轉接頭。</p> <p>在「Keyboard/Mouse Setup」(鍵盤/滑鼠設定) 頁面上，將「Host Interface」(主機介面) 設定為 PS/2。請參閱 <鍵盤/滑鼠設定> (請參閱 "鍵盤/滑鼠設定" p. 111)。</p>
Dell Server 1850	<p>為了讓 BIOS A06 版能辨識裝載於卸除式 USB 快閃磁碟機的虛擬媒體，請在 Dell 伺服器與 KX II-101-V2 之間採用 PS/2 與 USB 連線。</p> <p>在「Keyboard/Mouse Setup」(鍵盤/滑鼠設定) 頁面上，將「Host Interface」(主機介面) 設定為 PS/2。請參閱 <鍵盤/滑鼠設定> (請參閱 "鍵盤/滑鼠設定" p. 111)。</p>

HP UX RX 1600 鍵盤與滑鼠組態

如果使用 HP® UX RX 1600 執行 UNIX®，請執行下列動作以將裝置連接到目標伺服器：

- 確認您在使用 KX II-101-V2 韌體 2.0.20.5.6964 或以上版本。
- 使用 KX II-101-V2 提供的 USB 纜線。
- 在「Keyboard/Mouse Setup」(鍵盤/滑鼠設定) 頁面上，將「Host Interface」(主機介面) 欄位設定為 USB。請參閱 <鍵盤/滑鼠設定> (請參閱 "鍵盤/滑鼠設定" p. 111)。
- 確認並未在「Port」(連接埠) 頁面上，選取「Enable Absolute Mouse」(啟用絕對滑鼠) 與「Use Full Speed」(使用全速) 核取方塊。
- 使用智慧或標準滑鼠模式。請勿使用絕對滑鼠模式。

Compaq Alpha 與 IBM P 伺服器滑鼠模式限制

透過 KX II-101-V2 連接到 Compaq® Alpha 伺服器或 IBM® P 伺服器時，您必須使用單滑鼠模式。請參閱 <使用目標伺服器> (請參閱 "使用目標伺服器" p. 34)。

Windows 2000 與 Windows 2003 Server 鍵盤限制

由於作業系統限制，使用 Windows 2000® 作業系統與 Windows 2003® 伺服器時，下列鍵盤按鍵組合在美式國際通用鍵盤上沒有作用。

- 右邊 Alt+D
- 右邊 Alt+I
- 右邊 Alt+L

附註：在按鍵上明確標出為美式國際通用的鍵盤上，右邊 Alt 可能會標示為 AltGr。

CC-SG

Proxy 模式與 MPC

如果您是在 CC-SG 組態下使用 KX II，若計劃要使用多平台用戶端 (MPC)，請不要使用 CC-SG Proxy 模式。

本章內容

一般常見問題集	204
IPv6 網路功能	205

一般常見問題集

問題	回答
Dominion KX II-101-V2 與上一代 Dominion KX II-101 之間有何差異？	Dominion KX II-101-V2 是價格經濟實惠的最新一代機型。V2 事實上可支援上一代 KX II-101 產品的所有功能，還另外提供許多有趣的功能。V2 版不支援乙太網路供電 (PoE) 或 PS2 本機連接埠。
Dominion KX II-101-V2 如何運作？	Dominion KX II-101-V2 連接到伺服器的鍵盤、視訊及滑鼠連接埠。其會先行擷取、數位化和壓縮視訊訊號，然後再使用 Raritan 功能強大的畫面 Grabber 與壓縮技術，將其傳輸給遠端用戶端電腦。Dominion KX II-101-V2 透過直覺式使用者介面提供一組豐富的功能。還能透過 CommandCenter® Secure Gateway 使用其他管理裝置來加以集中管理。
Dominion KX II-101-V2 能夠從遠端管理哪些電腦類型？	無論目標伺服器的硬體、作業系統或應用程式，存取目標伺服器的主要輸入/輸出裝置 - 鍵盤、視訊及滑鼠為何，Dominion KX II-101-V2 均可運作。因此，支援標準電腦鍵盤與滑鼠介面以及標準電腦視訊 (VGA) 的任何硬體均可以和 Dominion KX II-101-V2 一起使用。
是否具備安全性功能可保護我的目標伺服器，防止未經授權的遠端連線？	是。KX II-101-V2 可在遠端階段作業期間，提供多層安全性 - 連線驗證與資料傳輸安全性。利用使用者名稱、密碼及私密金鑰來驗證使用者。Dominion KX II-101-V2 能以位在 Dominion KX II-101-V2 的本機資料庫，或是以外部的 AAA 伺服器 (LDAP、Active Directory® 或 RADIUS) 來驗證使用者。最多可以使用 256 位元 AES 方法，加密所有鍵盤、視訊及滑鼠資料。
Dominion KX II-101-V2 支援哪些虛擬媒體類型？	KX II-101-V2 支援下列媒體類型：內部及 USB 連接的 CD/DVD 光碟機、USB 大量儲存裝置、電腦硬碟及遠端磁碟機映像檔。
虛擬媒體安全嗎？	是。虛擬媒體階段作業使用 256 位元 AES 加密方法保護安全。
KX2-101-V2 是否有本機連接埠？	是，有一個 VGA/USB 本機連接埠，但不需要本機連接埠纜線。若要在本機存取連接的伺服器，請將 LCD 監視器連接到 KX2-101-V2 的「本機 VGA」連接埠。將 USB 鍵盤與滑鼠直接連接到目標伺服器。

問題	回答
最新的版本中提供哪些新功能？	<p>3.5 版 (及以上) 目前提供下列功能：</p> <ul style="list-style-type: none"> • 1920x1080 視訊解析度 • iPad/iPhone 存取 (需要 CC-SG) • 雙重堆疊 IPv6 • FIPS 140-2 加密模組 • 登出使用者和中斷連接埠連線 • SNMPv3 • 另外從 Linux 與 Mac 用戶端支援虛擬媒體 • 支援日文、繁體中文及簡體中文使用者介面 • 說明功能表 • 登入標題 • 上載客戶 SSL 憑證 • 可設定連接埠編號

IPv6 網路功能

問題	回答
什麼是 IPv6 ？	<p>IPv6 是「Internet Protocol Version 6」(網際網路通訊協定第 6 版) 的縮寫,其是將會取代目前 IP 第 4 版 (IPv4) 通訊協定的下一代 IP 通訊協定。</p> <p>IPv6 可解決 IPv4 中的一些問題,例如 IPv4 位址的數目有限。還可以在路由與網路自動組態方面改善 IPv4。IPv6 預計會逐漸取代 IPv4,同時在數年間兩者會同時存在。</p> <p>IPv6 可設定和維護 IP 網路,從管理員的觀點來看 - 這是 IP 網路最讓人頭痛的部分之一。</p>
KX II-101-V2 為何支援 IPv6 網路功能？	<p>美國政府機構與國防部目前均指定採購 IPv6 相容的產品。此外,許多企業與其他國家 (例如中國) 即將在未來的數年逐漸轉移到 IPv6。</p>

問題	回答
什麼是「雙重堆疊」？為何需要它？	雙重堆疊是可同時支援 IPv4 與 IPv6 通訊協定的能力。由於會逐漸由 IPv4 轉移到 IPv6，雙重堆疊也成為支援 IPv6 的基本需求。
我該如何在 KX II-101-V2 啟用 IPv6？	您可以使用「Device Settings」(裝置設定) 索引標籤的「Network Settings」(網路設定) 頁面。啟用 IPv6 定址並選擇手動或自動設定組態。如需相關資訊，請參閱使用指南。
若我有具有 IPv6 位址的外部伺服器且想與 KX II-101-V2 一起使用，該怎麼辦？	KX II-101-V2 可透過其 IPv6 位址存取外部服務，例如 SNMP 管理員、系統記錄伺服器或 LDAP 伺服器。 使用 KX II-101-V2 的雙重堆疊架構，即可透過以下方式來存取這些外部伺服器：(1) IPv4 位址、(2) IPv6 位址或 (3) 主機名稱。因此 KX II-101-V2 可支援許多客戶未來會有的混合式 IPv4/IPv6 環境。
如果我的網路不支援 IPv6，該怎麼辦？	KX II-101-V2 出廠時預設的網路功能設定為僅用於 IPv4。當您準備好要使用 IPv6，接下來請依照上面的指示來啟用 IPv4/IPv6 雙重堆疊作業。
我可以在哪裡取得 IPv6 的詳細資訊？	如需 IPv6 的一般資訊，請參閱 www.ipv6.org 。KX II-101-V2 使用指南說明 KX II-101-V2 的 IPv6 支援。

索引

9

9 針腳 - 189

A

A：電源 - 23

Admin 連接埠 - 112

Apple Macintosh 設定 - 20

B

B：目標伺服器 - 23

Backup and Restore (備份與還原) - 155

C

C

網路 - 26

CC-SG - 203

CC-SG 使用者注意事項 - 30

CC-SG 管理 - 178

CLI 指令 - 169, 173

CLI 提示 - 171

CLI 語法 - 祕訣與快速鍵 - 172

Compaq Alpha 與 IBM P 伺服器滑鼠模式限制 - 203

D

D：Admin 連接埠 - 26

E

E：本機使用者 (Local User) 連接埠 - 26

F

FIPS 140-2 支援需求 - 145

H

HP UX RX 1600 鍵盤與滑鼠組態 - 203

HTTP 與 HTTPS 連接埠設定 - 108, 187

I

IBM AIX 設定 - 21

Interface 指令 - 175

IPv6 支援注意事項 - 201

IPv6 指令 - 176

IPv6 網路功能 - 205

J

Java Runtime Environment (JRE) - 200

K

KX II-101-V2 SNMP 設陷清單 - 117

KX II-101-V2 主控台瀏覽方式 - 35

KX II-101-V2 的 SSH 連線 - 170

KX II-101-V2 概覽 - 2

KX II-101-V2 說明 - 3

KX II-101-V2 遠端主控台介面 - 34

L

LAN 介面設定 - 29, 102, 105, 106

Linux 設定 (Red Hat 4 與 5 以及 Fedora 14) - 17

Linux 設定 (適用於標準滑鼠模式) - 18

Linux 環境的虛擬媒體 - 74

Listports 指令 - 173, 177

M

Mac 環境的虛擬媒體 - 75

Microsoft Active Directory 注意事項 - 30

N

Name 指令 - 173, 176

Network Speed Settings - 106, 188

Network Statistics (網路統計資料) 頁面 - 163

P

Proxy 模式與 MPC - 203

PS/2 組態 - 25

R

RADIUS 通訊交換規格 - 97

Raritan 電源插座裝置控制 - 112

S

Setlog 指令 - 173, 174

SSL 憑證 - 149

Sun Blade 視訊、鍵盤及滑鼠支援限制 - 201
Sun Solaris 設定 - 19
Sun 視訊解析度 - 11

T

Trace Route to Host (追蹤主機路由) 頁面 - 165

U

UNIX/Linux 工作站的 SSH 存取方法 - 171
USB 組態 - 23
USB 連線設定 - 134
Userlist 指令 - 173, 177

V

VKC 虛擬媒體 - 62

W

Windows 2000 設定 - 16
Windows 2000 與 Windows 2003 Server 鍵盤限制 - 203
Windows 7 與 Windows Vista 設定 - 14
Windows XP 環境的虛擬媒體 - 73
Windows XP、Windows 2003 及 Windows 2008 設定 - 13
Windows 電腦的 SSH 存取方法 - 170

一劃

一般常見問題集 - 204
一般設定 - 62

三劃

工具列按鈕與狀態列圖示 - 44
工具選項 - 62, 67

四劃

中斷 KVM 目標伺服器連線 - 46
中斷虛擬媒體的連線 - 77, 79
介面 - 5, 34
分組的 IP ACL (存取控制清單) - 82, 85
升級韌體 - 157
升級歷程記錄 - 158
支援的作業系統 (用戶端) - 182
支援的通訊協定 - 30

支援的視訊解析度 - 184
支援的鍵盤語言 - 185
支援的瀏覽器 - 183

五劃

以 VKC 與 AKC 設定掃描設定 - 66
出廠重設 - 158
加密與共用 - 142
左面板 - 35
本機磁碟機 - 77
用戶端啟動設定 - 65
目標伺服器的電源控制 - 45

六劃

全螢幕模式 - 67
在 Proxy 模式下使用 CC-SG - 180
多平台用戶端 (MPC) - 43
安全性設定 - 88, 137
安全性管理 - 137
安全性標題 - 151
安裝與組態 - 9
安裝機架 - 198
自動完成指令 - 172
自動感應視訊設定 - 54

七劃

作業系統 IPv6 支援注意事項 - 201
序列連接埠設定 - 111
快速入門 - 10
更新 LDAP 架構 - 190
更新結構描述快取 - 194
步驟 1：設定目標伺服器 - 9, 10
步驟 2：設定網路防火牆設定 - 9, 21
步驟 3：連接設備 - 9, 22
步驟 4：設定 KX II-101-V2 - 9, 26
系統記錄組態設定 - 120
系統管理功能 - 6

八劃

事件管理 - 114
使用 CLI 存取 KX II-101-V2 - 170
使用「Reset」(重設) 按鈕重設 KX II-101-V2 - 131, 143
使用目標伺服器 - 34, 203
使用目標的螢幕擷取畫面 - 57

使用的 TCP 及 UDP 連接埠 - 186
 使用者 - 86
 使用者功能 - 7
 使用者群組 - 80
 使用者群組清單 - 81
 使用者管理 - 31, 80
 使用者與群組之間的關聯性 - 81
 使用者驗證程序 - 99
 使用虛擬媒體 - 76
 使用虛擬媒體的必要條件 - 72, 76
 命名目標伺服器 - 29
 命名電源插座裝置 (電源插座裝置的連接埠頁面) - 125, 127
 所有指令行介面層級的常見指令 - 172

九劃

封鎖使用者 - 89, 137, 140
 封鎖和解除封鎖使用者 - 89
 建立使用者群組與使用者 - 31
 建立新屬性 - 191
 建置鍵盤巨集 - 51
 指令行介面 (CLI) - 112, 169
 指派 IP 位址 - 10, 27
 按連接埠檢視使用者 - 87
 相關文件 - 4
 重要注意事項： - 200
 重新命名連接埠 - 123
 重新整理畫面 - 54

十劃

修改和移除鍵盤巨集 - 53
 修改現有使用者 - 89
 修改現有的使用者群組 - 85
 套件內容 - 8
 除錯 - 173, 174

十一劃

停止 CC-SG 管理 - 160
 偵測 (Ping) 主機頁面 - 165
 啟用 FIPS 140-2 - 143, 145
 啟用 SSH - 107
 啟用 Telnet - 107
 啟用直接連接埠存取 - 34
 執行 LDAP/LDAPS 遠端驗證 - 90, 94
 執行 RADIUS 遠端驗證 - 95

執行鍵盤巨集 - 53
 將 KX II-101-V2 重新開機 - 159
 將使用者登出 KX II-101-V2 (強制登出) - 87, 88
 常見問題集 - 204
 強固密碼 - 101, 137, 139
 從 Active Directory 伺服器傳回使用者群組資訊 - 94
 從 CC-SG 移除對 KX II-101-V2 的管理 - 179
 從 LDAP - 190
 從 Microsoft Active Directory - 190
 從本機鍵盤存取 BIOS 的限制 - 202
 探查 KX II-101-V2 子網路的 Raritan 裝置 - 41
 探查本機子網路上的 Raritan 裝置 - 40
 接頭 - 184
 控制電源插座裝置 - 129
 產品功能 - 5
 產品圖片 - 5
 組態 - 175
 術語 - 7
 規格 - 181
 設定 IP 存取控制 - 146
 設定 KX II-101-V2 使用終端機模擬程式 (選用) - 10, 27, 31, 171
 設定 KX II-101-V2 使用遠端主控台 - 27
 設定 SNMP 代理程式 - 109, 114
 設定 SNMP 設陷 - 114
 設定日期/時間設定 - 113, 149
 設定伺服器視訊解析度 - 10, 11
 設定事件管理 - 目的地 - 121
 設定事件管理 - 設定 - 114, 121
 設定個別群組的權限 - 85, 89
 設定連接埠權限 - 82, 85
 設定登錄允許對架構進行寫入作業 - 191
 設定新密碼 - 27
 設定權限 - 82, 84, 85
 透過 RADIUS 傳回使用者群組資訊 - 97
 透過 URL 啟用直接連接埠存取 - 108
 連接埠存取頁面 - 37
 連接埠動作功能表 - 38
 連接埠組態 - 20, 122
 連接虛擬媒體 - 77
 連接電源插座裝置 - 125
 連線內容 - 46
 連線到 KVM 目標伺服器 - 43

連線資訊 - 48

十二劃

智慧滑鼠模式 - 61
無法使用讀取/寫入的情況 - 76, 77
登入 - 171
登入限制 - 137
登出 - 42
絕對滑鼠模式 - 62
虛擬 KVM 用戶端 (VVC) - 38, 43
虛擬媒體 - 62, 69
視訊內容 - 54
視訊解析度 - 7
診斷 - 162, 173, 174
進階 USB 連線設定 - 135

十三劃

傳回使用者群組資訊 - 190
匯入/匯出鍵盤巨集 - 49
愛用裝置清單頁面 - 40, 41
新增、編輯和刪除我的最愛 - 41
新增使用者 - 88, 89
新增使用者群組 - 81
新增類別的屬性 - 193
概覽 - 9, 43, 70, 133, 169, 178
滑鼠指標同步 - 59
滑鼠設定 - 13
滑鼠選項 - 58
經過認證的數據機 - 113, 184
裝上 L 型托架水平裝載 KX II-101-V2 - 198
裝置服務 - 107, 170
裝置診斷 - 167
裝置資訊 - 154
裝置管理 - 102
裝載 - 7
裝載 CD-ROM/DVD-ROM/ISO 映像檔 - 78
電源 - 7
電源控制 - 122, 125
預設登入資訊 - 9

十四劃

實物規格 - 181
管理 KVM 目標伺服器 (連接埠頁面) - 123, 125
管理 USB 連線 - 133

管理功能 - 6
管理我的最愛 - 39
管理愛用裝置頁面 - 40
管理電源關聯 - 128
維護 - 153
網路 - 173, 175
網路介面頁面 - 162
網路基本設定 - 102, 103
網路組態 - 5
網路設定 - 27, 29, 102, 103, 105, 187
與連接埠的使用者中斷連線 - 87, 88
說明的新增內容 - 4
說明選項 - 68
遠端驗證 - 30

十五劃

數據機 - 112
數據機存取纜線連線 - 113
標準滑鼠模式 - 60
稽核記錄 - 153
編輯使用者成員的 rcigroup 屬性 - 194
調整視訊設定 - 54

十六劃

輸入探查連接埠 - 108

十七劃

檢查瀏覽器是否支援 AES 加密功能 - 142, 144
檢視 KX II-101-V2 MIB - 109, 114, 119
檢視 KX II-101-V2 使用者清單 - 86
檢視工具列 - 66
檢視狀態列 - 67
檢視選項 - 66
縮放比例 - 67
鍵盤、視訊以及滑鼠注意事項 - 201
鍵盤/滑鼠設定 - 111, 130, 202, 203
鍵盤巨集 - 49
鍵盤限制 - 64
鍵盤選項 - 49

十八劃

瀏覽 CLI - 171
簡介 - 1

十九劃

類比 KVM 切換器 - 111, 130

二十三劃

變更密碼 - 101

變更最大螢幕更新頻率 - 58

變更預設的 GUI 語言設定 - 132

驗證設定 - 90

▶ 美國/加拿大/拉丁美洲

週一至週五

8 a.m. - 8 p.m. ET

電話：800-724-8090 或 732-764-8886

若為 CommandCenter NOC：按 6，再按 1

若為 CommandCenter Secure Gateway：按 6，再按 2

傳真：732-764-8887

CommandCenter NOC 的電子郵件：tech-ccnoc@raritan.com

其他所有產品的電子郵件：tech@raritan.com

▶ 中國

北京

週一至週五

當地時間 9 a.m. - 6 p.m.

電話：+86-10-88091890

上海

週一至週五

當地時間 9 a.m. - 6 p.m.

電話：+86-21-5425-2499

廣州

週一至週五

當地時間 9 a.m. - 6 p.m.

電話：+86-20-8755-5561

▶ 印度

週一至週五

當地時間 9 a.m. - 6 p.m.

電話：+91-124-410-7881

▶ 日本

週一至週五

當地時間 9:30 a.m. - 5:30 p.m.

電話：+81-3-3523-5991

電子郵件：support.japan@raritan.com

▶ 歐洲

歐洲

週一至週五

8:30 a.m. - 5 p.m. GMT+1 CET

電話：+31-10-2844040

電子郵件：tech.europe@raritan.com

英國

週一至週五

8:30 a.m. to 5 p.m. GMT+1 CET

電話 +44-20-7614-77-00

法國

週一至週五

8:30 a.m. - 5 p.m. GMT+1 CET

電話：+33-1-47-56-20-39

德國

週一至週五

8:30 a.m. - 5:30 p.m. GMT+1 CET

電話：+49-20-17-47-98-0

電子郵件：rg-support@raritan.com

▶ 墨爾本，澳洲

週一至週五

當地時間 9:00 a.m. - 6 p.m.

電話：+61-3-9866-6887

▶ 台灣

週一至週五

9 a.m. - 6 p.m. GMT -5 標準 -4 日光

電話：+886-2-8919-1333

電子郵件：support.apac@raritan.com