



Dominion KX II-101

使用指南

2.0 版

Copyright © 2008 力登電腦股份有限公司版權所有
KX2101-0A-CHT
2008 年 2 月
255-62-4031-00

本文件所有的資訊均受到版權保護。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。

©Copyright 2008, Raritan, Inc.、CommandCenter®、Dominion®、Paragon® 及 Raritan 公司標誌都是力登電腦股份有限公司的商標或註冊商標並保留一切權利。Java® 是 Sun Microsystems, Inc. 的註冊商標。Internet Explorer® 是 Microsoft Corporation 的註冊商標。Netscape® 與 Netscape Navigator® 是 Netscape Communication Corporation 的註冊商標。所有其他商標或註冊商標為各所有人所有。

FCC 資訊

本設備依據 FCC 法規標準第 15 節進行測試，證實符合 Class A 數位裝置的限制。這些限制的設計是爲了提供適當的保護，防止對商用系統設備造成有害的干擾。本設備會產生、使用而且可能放射電磁波能量，請務必按照指示說明進行安裝及使用，否則可能會對無線電通訊造成有害的干擾。在住宅區環境操作本設備可能會造成有害的干擾。

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。

力登對於因意外、災害、誤用、濫用、非力登指示的產品修改、或力登合理控制之外的其他事件或不在正常操作下所引起的狀況，而對本產品造成之損害不負任何責任。



目錄

簡介	1
<hr/>	
Dominion KX II-101 概覽	1
產品圖片	2
產品特色	3
介面	3
網路組態	3
系統管理功能	3
管理功能	3
使用者功能	4
電源	4
視訊解析度	4
裝載	4
產品包裝內容	4
專有名詞	5
選用附件	5
重要資訊	6
<hr/>	
登入	6
預設 IP 位址	6
Service Pack	6
安裝與組態	7
<hr/>	
設定目標伺服器	7
設定伺服器視訊解析度	8
滑鼠模式	10
連接 KX II-101	14
連接目標伺服器	16
連接網路	19
開啓 KX II-101 電源	19
使用管理連接埠	19
使用本機使用者連接埠	20
設定網路防火牆組態	20
設定 KX II-101	20
使用遠端主控台	21
使用終端機模擬程式	26

連接 KX II-101	31
語言支援.....	31
Java Runtime Environment (JRE).....	31
啓動 KX II-101	31
啓用直接連接埠存取.....	33
KX II-101 主控台配置.....	33
KX II-101 主控台瀏覽方式.....	34
KX II-101 遠端主控台功能表導覽.....	35
登出.....	35
管理我的最愛.....	36
管理我的最愛功能表.....	37
我的最愛清單.....	38
探查裝置 - 本機子網路.....	40
探查裝置 - KX II-101 子網路.....	42
新增我的最愛.....	43
連接埠存取頁面.....	44
使用者、群組以及存取權限	45
使用者.....	45
群組.....	45
使用者與群組之間的關聯性.....	46
使用者管理.....	46
使用者管理功能表.....	46
遠端驗證.....	58
CC-SG 使用者注意事項.....	58
支援的通訊協定.....	58
Microsoft Active Directory 注意事項.....	58
驗證與授權.....	58
驗證設定.....	59
更新 LDAP 架構.....	66
虛擬 KVM 用戶端	76
概覽.....	77
選項.....	78
功能表樹狀目錄.....	78
工具列.....	79
滑鼠指標同步.....	80
滑鼠同步提示.....	80
連線功能表.....	81
內容對話方塊.....	81

連線資訊.....	83
結束.....	84
鍵盤功能表.....	84
傳送 Ctrl+Alt+Delete.....	84
鍵盤巨集.....	84
建立鍵盤巨集.....	85
執行鍵盤巨集.....	87
修改鍵盤巨集.....	87
移除鍵盤巨集.....	87
視訊功能表.....	88
重新整理畫面.....	88
自動感應視訊設定.....	88
校準色彩.....	89
視訊設定.....	89
滑鼠功能表.....	92
同步化滑鼠.....	92
單滑鼠游標.....	92
標準.....	93
智慧.....	94
絕對.....	95
VKC 虛擬媒體.....	95
工具功能表.....	96
選項.....	96
檢視功能表.....	97
檢視工具列.....	97
縮放比例.....	97
目標螢幕解析度.....	98
說明功能表.....	98
關於 Raritan 虛擬 KVM 用戶端.....	98
虛擬媒體.....	99
<hr/>	
概覽.....	100
使用虛擬媒體的必要條件.....	102
使用虛擬媒體.....	103
開啓 KVM 階段作業.....	104
連接虛擬媒體.....	105
本機磁碟機.....	105
無法使用讀取/寫入的情況.....	106
CD-ROM/DVD-ROM/ISO 映像檔.....	107

目錄

中斷虛擬媒體的連線.....	108
檔案伺服器設定 (僅限檔案伺服器 ISO 映像檔).....	109
裝置管理	111
裝置設定功能表.....	111
Network Settings (網路設定).....	112
網路基本設定.....	113
LAN 介面設定.....	114
裝置服務.....	116
鍵盤/滑鼠設定.....	118
序列連接埠設定.....	119
日期/時間設定.....	120
事件管理.....	121
SNMP 組態.....	122
Syslog 組態.....	123
事件管理 - 目的地.....	124
SNMP 代理組態.....	126
SNMP 設限組態.....	126
連接埠組態.....	128
電源控制	130
概覽.....	130
連接電源插座.....	131
命名電源插座裝置 (電源插座裝置的連接埠頁面).....	132
建立 KVM 目標伺服器與插座的關聯 (連接埠頁面).....	133
顯示插座關聯.....	137
控制電源插座裝置.....	138
安全性設定	140
安全性設定功能表.....	140
安全性設定.....	141
登入限制.....	142
強固密碼.....	143
使用者封鎖.....	144
加密與共用.....	145
檢查瀏覽器是否支援 AES 加密功能.....	147

IP 存取控制.....	147
維護	150
維護功能表.....	150
稽核記錄.....	151
裝置資訊.....	152
備份與還原.....	153
韌體升級.....	155
升級歷程記錄.....	156
重新開機.....	157
命令行介面 (CLI)	159
概覽.....	159
使用 CLI 存取 KX II-101.....	160
KX II-101 的 SSH 連線.....	160
Windows 電腦的 SSH 存取方法.....	160
UNIX 工作站的 SSH 存取方法.....	161
登入.....	161
瀏覽 CLI.....	161
CLI 提示.....	162
自動完成指令.....	162
CLI 語法 - 祕訣與快速鍵.....	162
所有命令行介面層級的常見指令.....	163
CLI 指令.....	163
診斷.....	164
組態.....	165
Listports 指令.....	167
Userlist 指令.....	167

目錄

診斷	168
診斷功能表.....	168
網路介面頁面.....	169
網路統計資料頁面.....	169
偵測 (Ping) 主機頁面.....	172
追蹤主機路由頁面.....	173
裝置診斷.....	174
CC 解除管理	176
概覽.....	176
從 CC-SG 移除對 KX II-101 的管理.....	177
在 Proxy 模式下使用 CC-SG.....	178
規格	179
KX II-101.....	179
接頭.....	180
Raritan 遠端用戶端軟體.....	180
安裝機架	181
各式 AC-DC 變壓器插頭.....	181
識別插頭類型.....	181
移除 AC-DC 變壓器的外罩附件.....	182
AC-DC 變壓器的轉接插頭.....	182
托架安裝.....	183
KX II-101 托架零件.....	184
裝上托架水平裝載 KX II-101.....	185
裝上托架垂直裝載 KX II-101.....	185
索引	187

本章內容

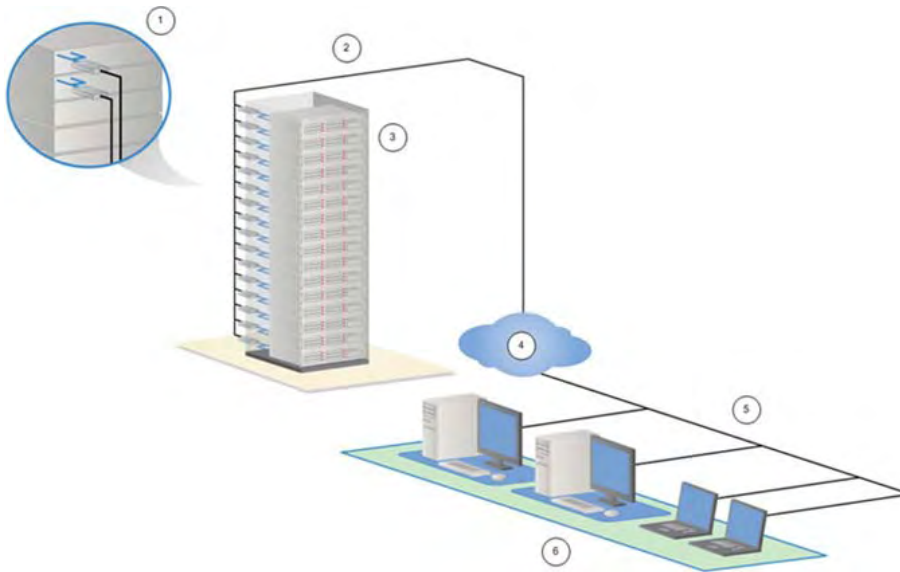
Dominion KX II-101 概覽.....	1
產品圖片	2
產品特色	3
產品包裝內容	4
專有名詞	5

Dominion KX II-101 概覽

感謝您購買 Dominion KX II-101。KX II-101 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 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 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 裝置都有自己的 IP 位址。每部裝置均是透過乙太網路供電 (PoE, Power-over-Ethernet) 或外部電源模組來提供電源。

Dominion KX II-101 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) 管理設備，整合為單一邏輯解決方案。



- 1 KX II-101
- 2 LAN

產品圖片

- 3 Windows、Linux 以及 Sun 伺服器。
- 4 TCP/IP
- 5 LAN
- 6 遠端 (網路) 存取

產品圖片



產品特色

介面

- 整合式 PS/2 KVM 連線
- 可取得控制與虛擬媒體的選用 USB 連線。
- 可供初始裝置設定與診斷使用和供外接式數據機存取的序列管理連接埠
- 可支援 10/100-base-T 自動感應、全雙工的乙太網路 LAN 連接埠
- LED 網路活動指示燈與狀態
- 背光 LED 電源開啓指示燈

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
- 可管理設定的時鐘或利用網路時間通訊協定 (NTP/SNTP) 同步處理
- 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 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) 管理設備相整合

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)
- 可有多位遠端使用者的「PC Share」(PC 共用) 模式
- TCP 通訊
- 英文使用者介面
- 虛擬媒體存取
- 滑鼠絕對同步
- 隨插即用
- 256 位元加密的完整 KVM 訊號，包括視訊及虛擬媒體

電源

- 透過 Class 2 乙太網路供電 (PoE) 技術提供電源
- 透過外部 AC-DC 電源模組提供替代電源

視訊解析度

- 解析度最高可達 1600X1200 (60 Hz)

裝載

- 機架安裝托架
如需詳細資訊，請參閱 <安裝機架> (請參閱 "安裝機架" p. 181)。

產品包裝內容

每部 KX II-101 裝置出貨時均附有：

- 主要裝置 KX II-101 - KVM over IP 硬體鎖
- USB Type A 對 Type B 迷你接頭
- 充電器組 - AC-DC 6VDC
- 可在全球使用的三個額外電源插頭
- Mini-DIN 對 DB9 序列纜線
- 安裝托架組
- Raritan 使用手冊與快速安裝指南 CD-ROM
- 印刷版快速安裝指南
- 印刷版應用程式注意事項 (適用的話)
- 印刷版技術注意事項 (適用的話)

專有名詞

目標伺服器	要透過 KX II-101 與其連接的 KVM 組態存取的伺服器。
遠端電腦	Windows、Linux、Solaris 或 Apple Macintosh® 電腦，用以存取和控制連接到 KX II-101 的目標伺服器。
管理 (Admin) 序列連接埠	KX II-101 提供了管理 (Admin) 序列連接埠。請使用隨附的 Mini-DIN 對 DB9 纜線，將電腦上的序列連接埠連接到 KX II-101 的管理序列連接埠。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	此連接埠可讓使用者不需要拔除 KX II-101，臨機使用目標伺服器原本的鍵盤與滑鼠。
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。

選用附件

- DB15 對 PS/2 與 VGA 本機使用者纜線
如需詳細資訊，請參閱 <連接附件> (請參閱 "接頭" p. 180)。

本章內容

登入	6
預設 IP 位址	6
Service Pack	6

登入

- 預設的 KX II-101 登入使用者名稱爲 **admin**，而密碼爲 **raritan**。此使用者具有管理權限。
- 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。
- 預設密碼 **raritan** 必須全以小寫字母輸入。
- 爲確保安全性，請儘快變更預設密碼。

預設 IP 位址

KX II-101 出貨時附有預設的靜態 IP 位址 192.168.0.192。在未沒有 DHCP 伺服器的網路上，您必須使用 KX II-101 序列管理主控台或 KX II-101 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 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. 22)。如需使用序列管理主控台設定 IP 位址的詳細資訊，請參閱 [〈使用本機序列主控台〉](#) (請參閱 "使用終端機模擬程式" p. 26)。

Service Pack

- 使用 Microsoft Internet Explorer 5.01 版或 Windows 2000 的 KX II-101 使用者必須將升級至 Service Pack 4 (SP4) 或以上的版本。

本章內容

設定目標伺服器	7
連接 KX II-101.....	14
設定網路防火牆組態	20
設定 KX II-101.....	20

 設定目標伺服器

本章說明如何安裝和設定 KX II-101。安裝與設定步驟如下：

1. **設定目標伺服器** (p. 7)。
2. **設定網路防火牆組態** (p. 20)。
3. **連接 KX II-101** (p. 14)。
4. **設定 KX II-101** (p. 20)。

安裝 KX II-101 之前，請執行下述步驟，先設定您想要透過 KX II-101 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 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界面的目標伺服器，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 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 支援下列視訊解析度：

文字模式庖

640x480 @ 60Hz	1024x768 @ 60Hz
640x480 @ 72Hz	1024x768 @ 70Hz
640x480 @ 75Hz	1024x768 @ 75Hz
640x480 @ 85Hz	1024x768 @ 85Hz
800x600 @ 56Hz	1152x864 @ 60Hz
800x600 @ 60Hz	1152x864 @ 75Hz
800x600 @ 72Hz	1280x1024 @ 60Hz
800x600 @ 75Hz	1600x1200 @ 60Hz
800x600 @ 85Hz	

設定 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 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. 8)。

注意：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同步訊號。

指令行解析度

- 若要檢查指令行解析度：
 - 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 支援的任一解析度。

2. 重新啓動電腦。

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 支援的任一解析度。

2. 重新啓動電腦。

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
```

其中 1024x768x75 可以是 KX II-101 支援的任一解析度。

2. 重新啓動電腦。

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
```

其中 1024x768x75 可以是 KX II-101 支援的任一解析度。

2. 重新啓動電腦。

滑鼠模式

KX II-101 可在數種滑鼠模式下操作： Absolute Mouse Synchronization™ (滑鼠絕對同步)、智慧滑鼠模式 (請勿使用動畫滑鼠) 以及標準滑鼠模式。 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，則必須將滑鼠參數設為特定的值，這部份會在本節的各個段落中加以說明。

本節說明不同系統所需的滑鼠組態。

Windows Vista

➤ 若要設定滑鼠：

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

➤ 若要停用動畫與淡化特效：

1. 從 Windows「開始」功能表，選擇「控制台」>「系統」>「進階」系統設定。 隨即會開啓「系統內容」對話方塊。
2. 按一下「進階」索引標籤。
3. 選取「效能」群組的「設定」按鈕。 隨即會開啓「效能選項」對話方塊。
4. 取消選取「自訂」選項下的以下核取方塊：
 - 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
 - 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
5. 按一下「確定」。
6. 關閉「控制台」。

Windows XP 設定

在執行 Microsoft Windows XP 的 KVM 目標伺服器上，停用「增強指標的準確性」選項，然後將滑鼠移動速度設定在剛好中間速度的位置。您可以在「控制台」>「滑鼠」>「指標設定」找到這些參數。

注意：對於執行 Windows 2000 或 XP 的目標伺服器，您可能希望建立一個使用者名稱，僅供透過 KX II-101 從遠端連線時使用。這可讓您只為 KX II-101 連線保留目標伺服器的慢速滑鼠指標速度/加速設定，而其他使用者仍可保有較快速的滑鼠速度。

注意：Windows XP 與 2000 登入畫面會回復到預設的滑鼠參數，而這些與最佳 KX II-101 效能的建議參數不同；因此，這些畫面無法達到最佳的滑鼠同步效果。如果您瞭解如何調整 Windows 目標伺服器的登錄，您可以使用 Windows 登錄編輯程式來變更下列設定，改善登入畫面的 KX II-101 滑鼠同步：預設使用者滑鼠 motion speed = 0; mouse threshold 1 = 0; mouse threshold 2 = 0。

Windows 2000 設定

在執行 Microsoft Windows 2000 的目標伺服器上，請將滑鼠指標加速設為「無」，並且將滑鼠移動速度設定在剛好中間速度的位置。您可以在「控制台」>「滑鼠」找到這些參數。

Linux 設定

在執行 Linux 圖形介面的目標伺服器上，請將滑鼠加速設為剛好 1，並且將臨界值設為剛好 1。

如上所述，請確保執行 Linux 的目標伺服器都使用 KX II-101 支援的解析度，並且採用標準的 VESA 解析度與螢幕更新頻率。Linux 目標伺服器也應該將遮沒時間 (blanking time) 設在 VESA 標準值的 +/- 40% 範圍內。

➤ 若要檢查這些參數：

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

注意：在許多 Linux 圖形環境裡，Ctrl+Alt+(加號) 指令會變更視訊解析度，此指令會輪流切換 XF86Config 檔案中仍然啟動的所有解析度。

Sun Solaris 設定

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

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

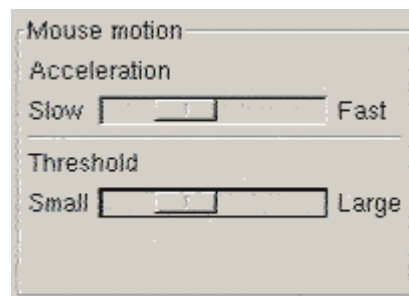
執行 Solaris 作業系統的目標伺服器必須輸出 VGA 視訊 (水平同步與垂直同步訊號，而不是複合同步訊號)。若要將您的 Sun 視訊卡輸出從複合同步訊號變更為非預設的 VGA 輸出，請先發出 Stop+A 指令，降到 bootprom 模式。然後，發出指令：

```
# eeprom output-device=screen:r1024x768x75
```

即可變更輸出解析度。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 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 使用，採用分離同步輸出的 HD15 Sun 需要使用 APKMSUN Raritan Guardian 轉換器。KX101 只支援 PS/2 版本與 APSUSB 介面卡搭配使用 (不支援複合同步訊號)。

在執行 Solaris 作業系統的目標伺服器上，將滑鼠加速設為剛好 1，並且將臨界值設為剛好 1。請在圖形使用者介面進行此項設定 (見下圖)，或使用指令行 `xset mouse a t`，其中的 `a` 代表加速，而 `t` 代表基準值。



Apple® Macintosh 設定

使用 Absolute Mouse Synchronization (滑鼠絕對同步) 模式。

連接 KX II-101

連接 KX II-101

KX II-101 的實體連線如下圖所示：



- 1 連接的監視器與 PS/2 纜線 (請參閱項目 3)。
- 2 Mini-USB 連接埠。 用以將裝置連接到目標伺服器；如果未使用連接的 PS/2 纜線，則是使用隨附的 USB 纜線。 要使用「滑鼠絕對同步」或「虛擬媒體」功能時，才必須使用 USB 連線。
- 3 連接的監視器與 PS/2 纜線。 用以將裝置連接到監視器以及目標伺服器 (如果未使用 USB 纜線)。
- 4 LOCAL USER 連接埠。 用以將本機鍵盤、視訊以及滑鼠直接連接到目標伺服器；使用選用的 PS/2 纜線。
- 5 乙太網路 LAN/PoE 連接埠。 可在使用 PoE LAN 連線時，提供 LAN 連線與電源。
- 6 電源接頭。 可在不使用 PoE (乙太網路供電) LAN 連線時，連接電源供應裝置。
- 7 背光 LED 電源開啓與開機指示燈。 對裝置的運作狀態提供回應。
- 8 Admin 連接埠。 用以執行下列其中一項動作：
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。
連接外接式數據機以撥入裝置。

連接目標伺服器

KX II-101 可以使用整合式 PS/2 纜線或隨附的 USB 纜線，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與螢幕更新頻率，然後再接連接纜線，如 **<設定伺服器視訊解析度>** (請參閱 "設定伺服器視訊解析度" p. 8)所述。

PS/2 組態

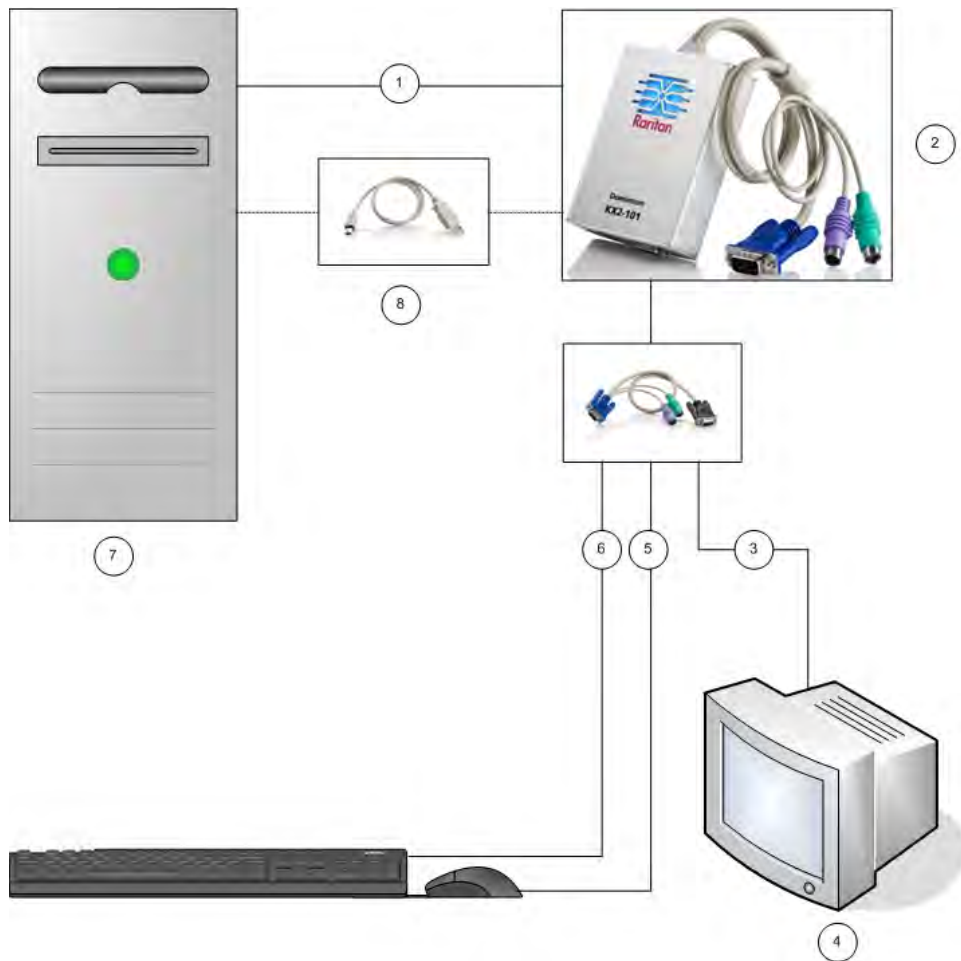
➤ 若要設定 KX II-101 以搭配 PS/2 目標伺服器使用：

1. 使用所附的 PS/2 鍵盤、視訊以及滑鼠纜線，將 KX II-101 連接到目標伺服器。
2. 使用選用的 PS/2 纜線，將本機鍵盤、視訊以及滑鼠連接到 KX II-101 的本機使用者連接埠。

注意： KX II-101 必須已開啓電源，本機使用者連接埠才能夠運作。

3. 如果您需要虛擬媒體 (VM) 連線，請將 mini-USB 接頭連接到 KX II-101，然後將 USB 接頭連接到目標伺服器上的任何 USB 連接埠。

完成後，連線應該如下圖所示。



- 1 從 KX II-101 連到目標伺服器的整合式 PS/2 鍵盤、視訊以及滑鼠連線。
- 2 KX II-101。
- 3 本機監視器的視訊連線 (選用纜線)。
- 4 本機監視器。
- 5 從 KX II-101 連到滑鼠的 PS/2 連線 (選用纜線)。
- 6 從 KX II-101 連到鍵盤的 PS/2 連線 (選用纜線)。
- 7 目標伺服器。
- 8 以隨附的 mini-USB 對 USB 接頭從 KX II-101 連到目標伺服器，藉以取得虛擬媒體連線。

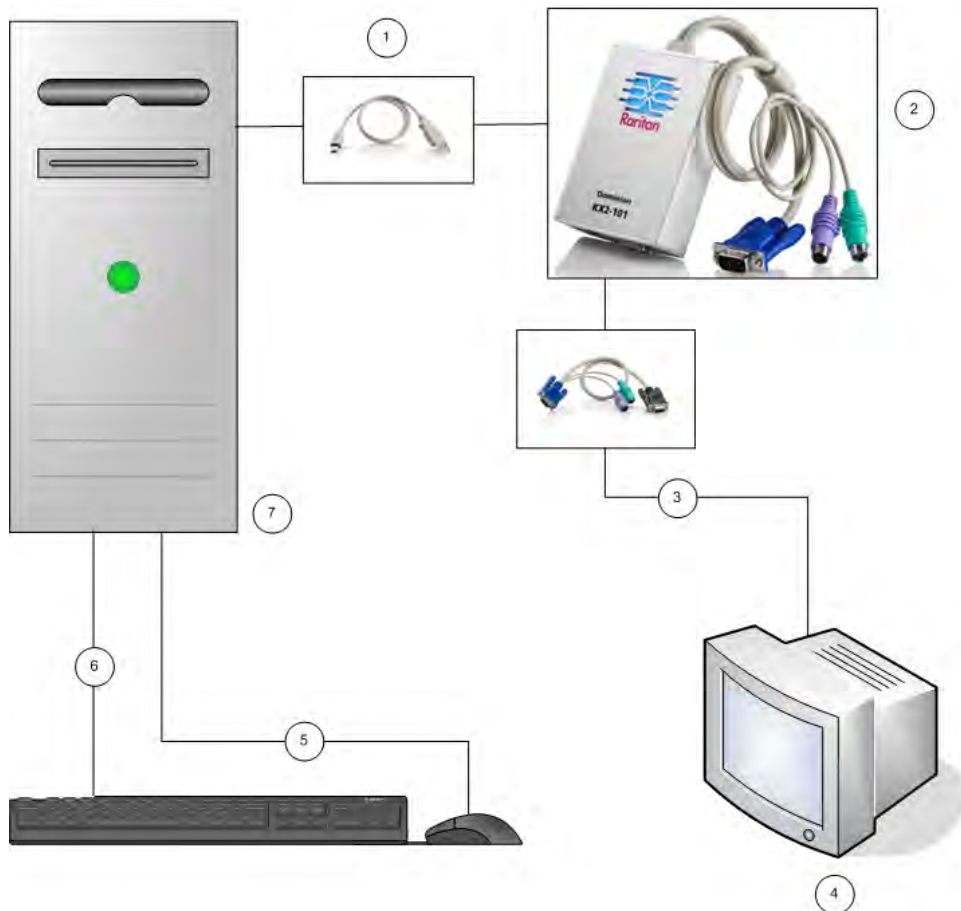
USB 組態

➤ 若要設定 KX II-101 以搭配 USB 目標伺服器使用：

1. 將 mini-USB 接頭連接到 KX II-101，然後將 USB 接頭連接到目標伺服器上的 USB 連接埠。
2. 使用隨附的 PS/2 DKX2-101-LPKVMC 纜線，只將本機視訊連接到 KX II-101 的本機使用者連接埠。

注意：KX II-101 必須已開啓電源，本機使用者連接埠才能夠運作。

3. 使用 USB 纜線，將鍵盤與滑鼠直接連接到目標伺服器。
- 完成後，連線應該如下圖所示。



- 1 以隨附的 mini-USB 對 USB 纜線從 KX II-101 連到目標伺服器。
- 2 KX II-101。
- 3 本機監視器的視訊連線 (選用纜線)。

- 4 本機監視器。
- 5 從目標伺服器連到滑鼠的 USB 連線。
- 6 從目標伺服器連到鍵盤的 USB 連線。
- 7 目標伺服器。

連接網路

將標準乙太網路纜線從標示為 LAN 的網路連接埠，連接到乙太網路切換器、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 正在使用時會閃爍黃光，代表正以 10Mbps 傳輸 IP 流量。綠光則代表連線速度為 100Mbps。

開啓 KX II-101 電源

KX II-101 可以利用標準的 AC 電源模組或透過 PoE (乙太網路供電) 提供電源。

- 如需標準 AC 電源，請將隨附的 AC 電源變壓器組插入電源插孔，然後將另一端插入附近的 AC 電源插座。
- 如需 PoE，請將 10/100Mbps 纜線連接到 LAN 連接埠，然後將另一端插入提供 PoE 的 LAN 插孔。

在開啓 KX II-101 的電源之後，便會進入開機順序，Raritan 標誌處的 LED 會持續閃爍藍光，期間約 45 秒。順利完成開機後，背光 LED 會一直亮著。

使用管理連接埠

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 執行設定工作。請將隨附的序列纜線有 min-DIN 的那端插入 KX II-101 的管理 (Admin) 連接埠，然後將 DB9 端插入電腦或膝上型電腦的序列連接埠。序列連接埠的通訊組態應該設定為：115,200 傳輸速率、8 個資料位元、1 個停止位元、無同位檢查以及無流量控制。

如需使用 ADMIN 連接埠設定 KX II-101 的詳細資訊，請參閱〈使用終端機模擬程式〉。

使用本機使用者連接埠

KX II-101 可以使用選用的視訊與 PS/2 纜線，讓您透過 LOCAL USER 連接埠，將鍵盤與滑鼠連接到目標伺服器。LOCAL USER 連接埠可作為通往 KX II-101 所連接目標伺服器的途徑，並無其他用途。KX II-101 必須已開啓電源，LOCAL USER 連接埠才能夠使用。

注意：本機連接埠上僅支援 PS/2 主控介面連線，而且您必須在使用 PS/2 接頭連接 KX II-101 之後，重新啓動目標伺服器。

設定網路防火牆組態

若要透過網路防火牆存取 KX II-101，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 使用您自行指定的另一個 TCP 連接埠。

若要運用 KX II-101 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 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。

設定 KX II-101

KX II-101 能以兩種方法進行設定：

- 使用網頁型 KX II-101 遠端主控台，這種方法在裝置與工作站之間需要網路連線。
- 使用像是 HyperTerminal 的終端機模擬程式，這種方法需要從裝置的 ADMIN 連接埠直接連接到工作站。KX II-101 中已隨附可用於此連線的纜線。

本節說明設定 KX II-101 的兩種方法。

使用遠端主控台

KX II-101 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 之前，您必須將工作站與裝置連線到網路。

若要設定 KX II-101，您可以：

- 設定新的密碼取代預設密碼。
- 指派 IP 位址
- 命名目標伺服器
- 建立使用者與群組

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。

1. 登入與 KX II-101 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。 隨即會開啓「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) 欄位中輸入新的密碼，在「Confirm New Password」(確認新密碼) 欄位中再輸入一次新密碼。 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「確定」。 隨即會開啓「Port Access」(連接埠存取) 頁面。

指派 IP 位址

1. 在 KX II-101 遠端主控台中，選擇「Device Settings」(裝置設定) > 「Network Settings」(網路設定)。隨即會開啓「Network Basic Settings」(網路基本設定) 頁面。

Home > Device Settings > Network Settings

Network Basic Settings

Device Name *
DominionKX2-101

IP auto configuration
DHCP

Preferred host name (DHCP only)

IP address
192.168.50.241

Subnet mask
255.255.255.0

Gateway IP address
192.168.50.126

Primary DNS server IP address
192.168.50.114

Secondary DNS server IP address
192.168.50.112

2. 在「Device Name」(裝置名稱) 欄位中，為 KX II-101 裝置指定有意義的名稱，最多可有 16 個英數字元與特殊字元，不得包含空格。
3. 從「IP auto configuration」(IP 自動組態) 下拉式清單中選取 IP 組態：
 - None (無) (靜態 IP)。此為預設與建議選項，因為 KX II-101 是基礎結構裝置，因此其 IP 位址不應變更。此選項需要手動指定網路參數。
 - DHCP。使用此選項，KX II-101 每次開機時，都會由 DHCP 伺服器指定網路參數。

設定直接連接埠存取

➤ 若要設定直接連接埠存取：

1. 選擇「Device Settings」(裝置設定) > 「Device Services」(裝置服務)。隨即會出現「Device Services」(裝置服務)。
2. 選取「Enable Direct Port Access via URL」(透過 URL 啓用直接連接埠存取) 核取方塊。

3. 啟用全域 Telnet 或 SSH 存取。
 - 選取「Enable TELNET Access」(啟用 TELNET 存取) 核取方塊，啟用 TELNET 存取。
 - 選取「Enable SSH Access」(啟用 TELNET 存取) 核取方塊，啟用 SSH 存取。
4. 為選取的存取類型指定有效的 TCP 連接埠。例如，透過 Telnet 的直接連接埠存方式，可以將 TCP 連接埠設為 7770。

Home > Device Settings > Device Services

Services

Discovery Port *
5000

Enable TELNET Access

TELNET Port
23

Enable SSH Access

SSH Port
22

Enable Direct Port Access via URL

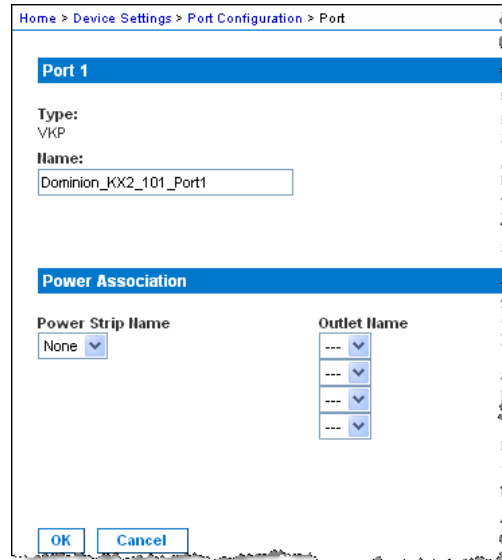
OK Reset To Defaults Cancel

5. 按一下「OK」(確定) 即可儲存此項資訊。

命名目標伺服器

1. 如 <連接 KX II-101> (請參閱 "連接 KX II-101" p. 31) 中所述，將 KX II-101 連接到目標伺服器 (如果您尚未這麼做)。
2. 選擇「Device Settings」(裝置設定) > 「Port Configuration」(連接埠組態)。隨即會開啓「Port Configuration」(連接埠組態) 頁面。

- 按一下目標伺服器的「Port Name」(連接埠名稱)。 隨即會開啓「Port」(連接埠) 頁面。



- 輸入名稱 (最多可有 32 個英數字元與特殊字元)。
- 按一下「OK」(確定)。

建立使用者與群組

本機與遠端驗證皆會利用使用者群組 (透過 RADIUS 或 LDAP)。 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。

➤ 若要建立使用者群組：

- 請使用下列其中一種方法，開啓「Group」(群組) 頁面：
 - 選擇「User Management」(使用者管理) > 「Add New User Group」(新增使用者群組)，或
 - 按一下「User Group List」(使用者群組清單) 頁面的「Add」(新增) 按鈕。
- 在「Groupname」(群組名稱) 欄位中，輸入新使用者群組的敘述性名稱。
- 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，勾選核取方塊。

4. 設定「Port Permissions」(連接埠權限)(存取、VM 存取以及電源控制)。指定此群組下使用者可存取的伺服器連接埠與存取類型。請注意，VM (虛擬媒體) 存取權的預設值跟所有連接埠權限一樣，都是「off」(關閉)。若要使用虛擬媒體，即必須啓用權限。
 5. 按一下「OK」(確定)。
- 若要建立新的使用者：
1. 請使用下列其中一種方法，開啓「User」(使用者) 頁面：
 - a. 選擇「User Management」(使用者管理) > 「Add New User」(新增使用者)，或
 - b. 按一下「User List」(使用者清單) 頁面的「Add」(新增) 按鈕。
 2. 在「Username」(使用者名稱) 欄位中，輸入唯一的名稱 (最多 16 個字元)。
 3. 在「Full Name」(全名) 欄位中，輸入該人員的全名 (最多 64 個字元)。
 4. 在「Password」(密碼) 欄位中輸入密碼，在「Confirm Password」(確認密碼) 欄位中再輸入一次密碼 (最多 64 個字元)。
 5. 從「User Group」(使用者群組) 下拉式清單中選取群組。除系統提供的預設群組之外 (Admin、<Unknown>、Individual Group)，此清單還包含您已建立的所有群組。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」。
 6. 按一下「OK」(確定)。

使用終端機模擬程式

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 的下列組態參數：

- IP 位址
- 子網路遮罩位址
- 閘道位址
- IP 存取控制
- LAN 速度
- LAN 介面模式

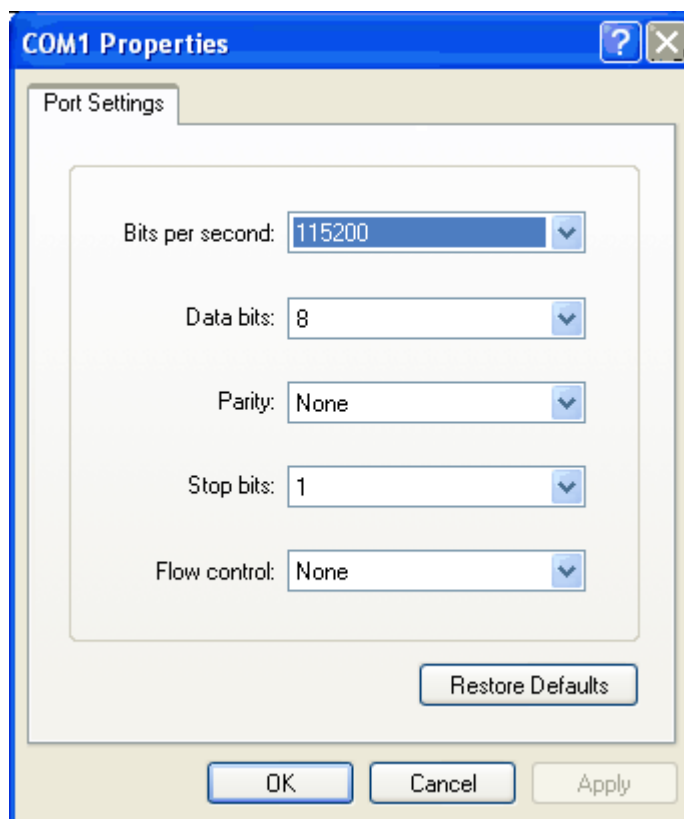
若要使用終端機模擬程式搭配 KX II-101，您必須先以隨附的 RS-232 序列纜線，從 KX II-101 的管理連接埠連接到電腦上的 COM1 連接埠。如需詳細資訊，請參閱 [〈使用管理連接埠〉](#) (請參閱 "使用管理連接埠" p. 19)。

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：*

1. 使用隨附的 RS-232 序列纜線，將 KX II-101 連接到本機電腦。
連接 KX II-101 上的管理連接埠與電腦上的 COM1 連接埠。
2. 啟動您想要用以設定 KX II-101 的終端機模擬程式。
3. 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



4. 連接 KX II-101。
隨即會出現登入畫面。



5. 輸入管理員使用者名稱，然後按下 Enter。

設定 KX II-101

系統會提示您，要求輸入密碼。

```
Login: admin
Password: _
```

- 輸入您的密碼，然後按下 Enter。
- 隨即會出現「Admin Port」(管理連接埠) 提示。

```
Login: admin
Password: MACADDR: 00:0d:5d:03:5d:23

-----
Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC         FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153        Idle Timeout: 30min
-----

Port Port          Port Port   Port
No.  Name          Type Status Availability
1 - Dominion_KXII-101_Port KVM up idle

Current Time: Fri Dec 28 19:44:16 2007

Admin Port >
```

- 在「Admin Port>」(管理連接埠) 提示，輸入 config，然後按下 Enter。
- 在「Config>」(設定) 提示，輸入 network，然後按下 Enter。
- 若要檢視目前的各項介面設定，請在「Interface>」(介面) 提示，輸入 interface，然後按下 Enter。

隨即會出現目前的各項介面設定。

```

Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC         FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153        Idle Timeout: 30min
-----
Port No.   Port Name                Port Type   Status   Availability
1 - Dominion_KXII-101_Port KUM      up       idle

Current Time: Fri Dec 28 19:52:26 2007

Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface

IP auto configuration: dhcp
IP address: 192.168.50.153
Netmask: 255.255.255.0
Gateway: 192.168.50.126
Ethernet mode: Autodetect

Admin Port > Config > Network > _

```

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	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： interface ipauto none ip 192.168.50.12 dhcp - 於啟動時自動將 IP 位址指派給裝置。
ip	IP 位址	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。
mask	subnetmask	子網路遮罩的 IP 位址。
gw	IP 位址	閘道的 IP 位址
mode	mode	乙太網路模式：您有下列選擇： auto - 根據網路，自動設定速度與介面模式。 10hdx - 10 Mbps，半雙工。 10fdx - 10 Mbps，全雙工。 100hdx - 100 Mbps，半雙工。 100fdx - 100 Mbps，全雙工。

設定 KX II-101

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.
```

1. 完成設定 KX II-101 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

語言支援	31
Java Runtime Environment (JRE)	31
啓動 KX II-101	31
管理我的最愛	36
連接埠存取頁面	44

語言支援

KX II-101 提供下列語言的鍵盤支援： 美式英文、繁體中文、簡體中文、日文、韓文、法文以及德文。

注意： 中文、日文及韓文鍵盤僅供顯示之用，「KX II-101 遠端主控台」功能目前不支援本機語言輸入。

Linux 上的語言組態

如需在 Linux 上設定外國語言鍵盤的詳細資訊，請參閱《KVM 與序列存取用戶端使用指南》中的「**鍵盤類型**」。

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 文件及《Raritan 多平台用戶端 (MPC) 與 Raritan 遠端用戶端 (RRC) 使用指南》。

「KX II-101 遠端主控台」與 MPC 都需要有 JRE 才能運作。 KX II-101 遠端主控台會檢查 Java 版本；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 Java Runtime Environment (JRE) 1.5 版以達最佳效能，但 KX II-101 遠端主控台與 MPC 亦可與 JRE 1.4.2_05 版或更高的版本搭配運作 (JRE 1.5.0_02 除外)。

注意： 爲了讓多語言鍵盤能在「KX II-101 遠端主控台」(虛擬 KVM 用戶端) 中運作，請安裝 Java Runtime Environment (JRE) 的多語言版本。

啓動 KX II-101

重要： 無論使用何種瀏覽器，您都必須允許來自 Dominion 裝置之 IP 位

址的快顯視窗，才能啓動 KX II-101 遠端主控台。

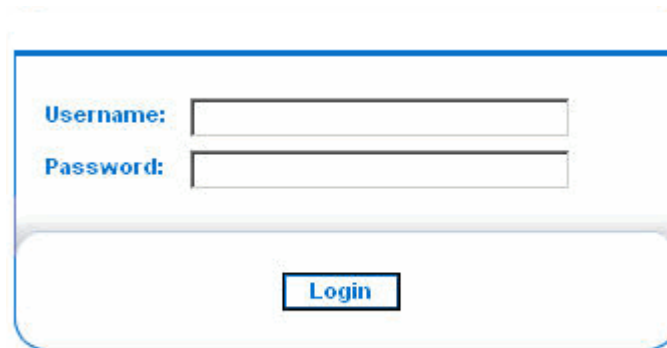
根據您的瀏覽器與安全性設定，您可能會看到各種不同的安全性及認證警告。必須接受這些警告才能啓動 KX II-101 遠端主控台。

勾選這些安全性與認證警告訊息上的下列選項，您便可減少以後登入時的警告訊息數量：

- In the future, do not show this warning (以後不顯示這個警告)。
- Always trust content from this publisher (自動信任來自此發行者的內容)。

➤ 若要啓動 KX II-101 遠端主控台：

1. 登入與 KX II-101 裝置有網路連線的任何工作站，然後安裝 Java Runtime Environment v1.4.2_05 或更高的版本 (JRE 可自 <http://java.sun.com/> <http://java.sun.com> 取得)。
2. 啓動支援的網頁瀏覽器，例如 Internet Explorer (IE) 或 Firefox。請參閱〈支援的瀏覽器〉。
3. 輸入下列 URL：`http://IP-ADDRESS`，此處的 IP-ADDRESS 是您指派給 KX II-101 裝置的 IP 位址。您也可以使用 `https`，即管理員指派給 KX II-101 的 DNS 名稱 (假設已配置 DNS 伺服器)，或僅在瀏覽器中輸入 IP 位址 (KX II-101 一律會將 IP 位址從 HTTP 重新導向至 HTTPS)。隨即會開啓「Login」(登入) 頁面。



The image shows a login form with a blue border. It contains two input fields: 'Username:' and 'Password:'. Below the input fields is a blue button labeled 'Login'.

4. 輸入您的使用者名稱與密碼。若是第一次登入，請使用出廠預設的使用者名稱與密碼登入 (`admin` 及 `raritan`，全部小寫)；之後會提示您，要求變更預設密碼。如需詳細資訊，請參閱〈變更預設的密碼〉。
5. 按一下「Login」(登入)。

啟用直接連接埠存取

直接連接埠存取可讓您存取 KX II-101 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 遠端主控台。
2. 選擇「Device Settings」(裝置設定) > 「Device Services」(裝置服務)。隨即會開啓「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) 以儲存設定。

➤ 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 的連接埠編號。

如果您只有一個 KVM 連接埠，便不需要連接埠編號。

直接連接埠存取 URL 的格式如下：

```
https://[IP
address]/dpa.asp?username=[username]&password=[password]&port=[port number]
```

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 主控台配置

KX II-101 遠端主控台介面提供 HTML (如同網頁) 介面，以供進行組態設定與管理以及列出和選擇目標伺服器。選項會歸類到各種索引標籤中。

成功登入之後，隨即會開啓「Port Access」(連接埠存取) 頁面，顯示連接埠、其狀態以及可用性。

KX II-101 主控台瀏覽方式

KX II-101 遠端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，隨即會開啓可用選項的頁面。
- 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」)。

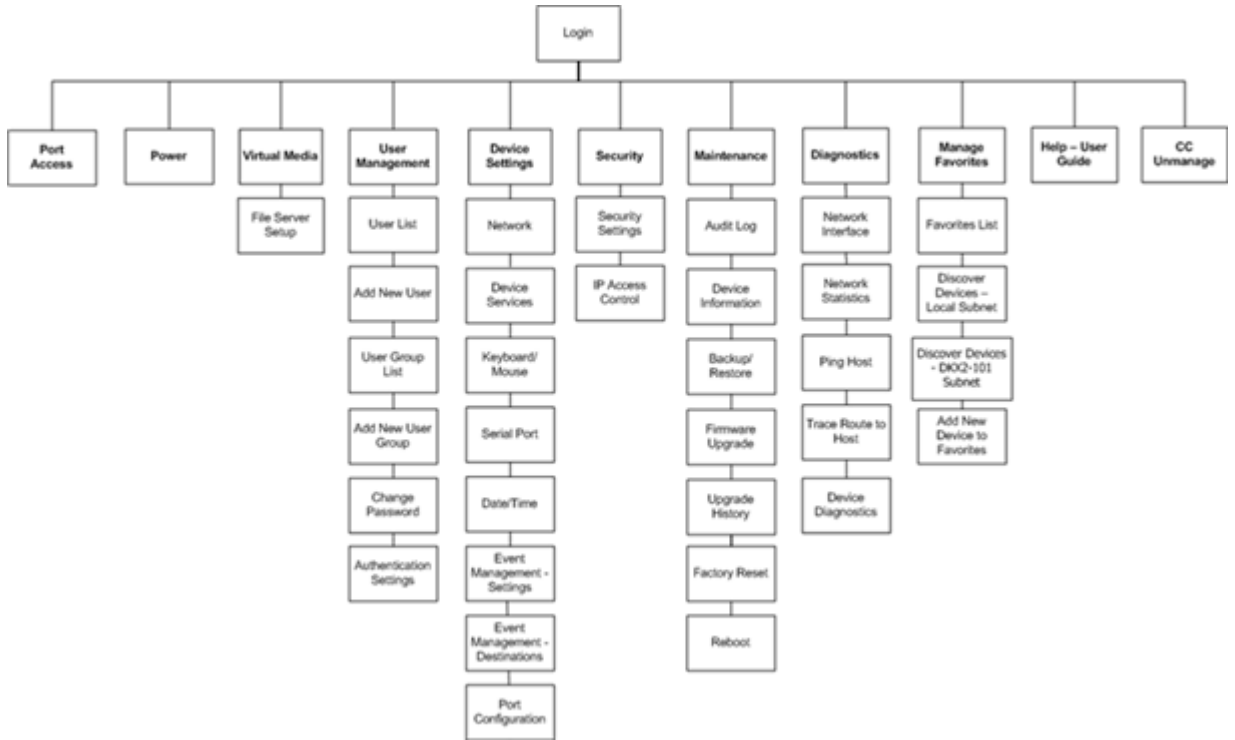
Category	Event	SNMP	Syslog	Audit Log
Device Operation		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Factory/Reset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End OC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

➤ 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，或
- 使用右側的捲軸

KX II-101 遠端主控台功能表導覽

下圖顯示 KX II-101 遠端主控台提供的所有功能表選項：



登出

➤ 若要結束 KX II-101 遠端主控台：

- 按一下頁面右上角的「Logout」(登出)。

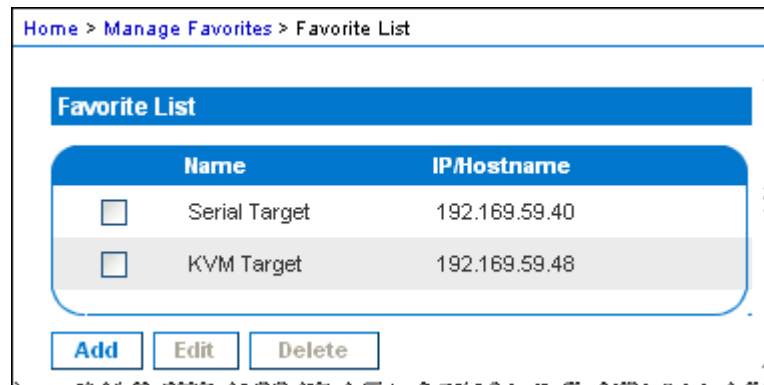
注意：登出也會關閉所有開啓的「虛擬 KVM 用戶端」與序列用戶端階段作業。

管理我的最愛

「Favorites」(我的最愛) 功能可讓您組織及快速存取常用裝置。

「Favorite Devices」(愛用裝置) 區段位於「Port Access」(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的清單
- 快速存取常用的裝置
- 依名稱或 IP 位址列出「Favorites」(我的最愛)
- 在子網路探查 KX II-101 裝置 (登入之前與之後)
- 從連線的裝置擷取探查到的 KX II-101 裝置 (登入之後)



- 若要存取愛用的 KX II-101 裝置：
 - 按一下該裝置的名稱 (列在「Favorite Devices」(愛用裝置) 下)。隨即會為該裝置開啓新的瀏覽器視窗。
- 若要切換依名稱及 IP 位址顯示的「Favorite Devices」(愛用裝置) 清單：

若要依 IP 位址顯示「Favorites」(我的最愛)：
 按一下「Display by IP」(依 IP 顯示) 按鈕。

若要依名稱顯示「Favorites」(我的最愛)：
 按一下「Display by Name」(依名稱顯示) 按鈕。

「Favorite Devices」(愛用裝置) 目前會依 IP 位址顯示；按一下「Display by Name」(依名稱顯示) 即可切換。

「Favorite Devices」(愛用裝置) 目前會依名稱顯示；按一下「Display by IP」(依 IP 顯示) 即可切換。



管理我的最愛功能表

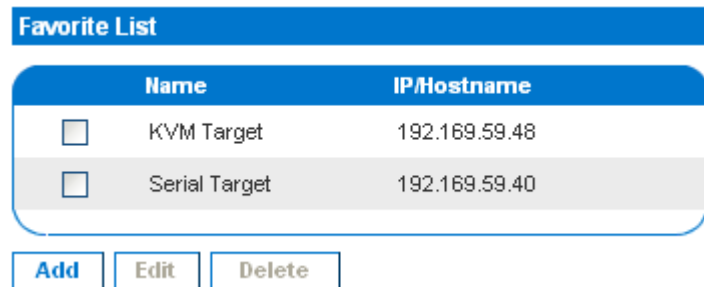
- 若要開啓「Manage Favorites」(管理我的最愛) 功能表：
 - 按一下「Manage」(管理) 按鈕。隨即會開啓「Manage Favorites」(管理我的最愛) 頁面，而且上面包含下列選項：

使用：	執行：
Favorites List (我的最愛清單)	管理愛用裝置的清單。
Discover Devices - Local Subnet (探查裝置 - 本機子網路)	探查本機子網路上的裝置。
Discover Devices - KX II-101 Subnet (探查裝置 - KX II-101 子網路)	探查 KX II-101 裝置子網路上的裝置。
Add New Device to Favorites (新增裝置到我的最愛)	在「Favorites」(我的最愛) 清單中新增、編輯和刪除裝置。

我的最愛清單

您可以從「Favorites List」(我的最愛清單) 頁面，在「Favorites」(我的最愛) 清單內新增、編輯和刪除裝置。

- 若要開啓「Favorites List」(我的最愛清單) 頁面：
 - 選擇「Manage」(管理) > 「Favorites List」(我的最愛清單)。 隨即會開啓「Favorites List」(我的最愛清單) 頁面：



Favorite List		
	Name	IP/Hostname
<input type="checkbox"/>	KVM Target	192.169.59.48
<input type="checkbox"/>	Serial Target	192.169.59.40

- 若要新增「Favorite」(我的最愛)：
 - 按一下「Add」(新增) 按鈕。 隨即會開啓「Add New Favorite」(新增我的最愛) (請參閱 "新增我的最愛" p. 43) 頁面。
- 若要刪除「Favorite」(我的最愛)：

重要： 移除愛用項目時務必謹慎小心，因為系統不會顯示提示要求您確認刪除。

1. 選取適當 KX II-101 裝置旁邊的核取方塊。
 2. 按一下「Delete」(刪除) 按鈕。 隨即會從我的最愛清單中移除該愛用項目。
- 若要編輯「Favorite」(我的最愛)：
 1. 從「Favorites List」(我的最愛清單) 頁面，選取適當 KX II-101 裝置旁邊的核取方塊。

- 按一下「Edit」(編輯) 按鈕。隨即會開啓「Edit」(編輯) 頁面：

Edit: 192.169.59.48

All fields are required

Description

KVM Target

IP Address

192.169.59.48

Port

5000

Product Type

Dominion KSX G1

OK Cancel

- 視需要更新欄位：
 - Description (說明)。輸入有意義的內容。
 - IP Address (IP 位址)。輸入 KX II-101 切換器裝置的 IP 位址。
 - Port (連接埠)。變更探查連接埠 (如有需要)。
 - Product Type (產品類型)。
- 按一下「OK」(確定)。

探查裝置 - 本機子網路

本選項會在本機子網路上 (亦即，正在執行「KX II-101 遠端主控台」的子網路) 探查裝置，直接從此頁面存取這些裝置，或將其新增到我的最愛清單。

	Name	IP/Hostname
<input type="checkbox"/>	DKX2-101	192.168.50.68
<input type="checkbox"/>	KX_KIM-0050	192.168.50.12
<input type="checkbox"/>	shoalb-sx	192.168.50.239
<input type="checkbox"/>	shoalbkx2	192.168.50.234

➤ 若要探查本機子網路上的裝置：

1. 選擇「Favorites」(我的最愛) > 「Discover Devices - Local Subnet」(探查裝置 - 本機子網路)。隨即會開啓「Discover Devices - Local Subnet」(探查裝置 - 本機子網路) 頁面。
2. 選取適當的探查連接埠 (如需探查連接埠的詳細資訊，請參閱 <網路其他設定 >)：
 - 若要使用預設的探查連接埠，請選取「Use Default Port 5000」(使用預設連接埠 5000) 選項。
 - 若要使用其他探查連接埠：
 - a. 取消選取「Use Default Port 5000」(使用預設連接埠 5000) 選項。
 - b. 在「Discover on Port」(執行探查的連接埠) 欄位輸入連接埠編號。
 - c. 按一下「Save」(儲存)。
3. 按一下「Refresh」(重新整理)。隨即會重新整理本機子網路的裝置清單。

➤ 若要將裝置新增到「Favorites List」(我的最愛清單)：

1. 選取裝置名稱/IP 位址旁邊的核取方塊。
2. 按一下「Add」(新增)。

祕訣：使用「Select All」(全選) 及「Deselect All」(取消全選) 按鈕，快速選取 (或取消全選) 遠端主控台子網路的全部裝置。

- 若要存取探查到的裝置：
 - 按一下該裝置的名稱或 IP 位址。隨即會為該裝置開啓新的瀏覽器視窗。

探查裝置 - KX II-101 子網路

本選項會在裝置子網路上 (亦即, KX II-101 裝置 IP 位址本身的子網路) 探查裝置, 直接從此頁面存取這些裝置, 或將其新增到我的最愛清單。

此功能可讓多台 KX II-101 裝置自動交互操作與擴充。 KX II-101 遠端主控台可自動探查 KX II-101 的子網路中的 KX II-101 裝置。



➤ 若要探查裝置子網路上的裝置：

1. 選擇「Favorites」(我的最愛) > 「Discover Devices - KX II-101 Subnet」(探查裝置 - KX II-101 子網路)。隨即會開啓「Discover Devices - KX II-101 Subnet」(探查裝置 - KX II-101 子網路) 頁面。

2. 按一下「Refresh」(重新整理)。隨即會重新整理本機子網路的裝置清單。

➤ 若要將裝置新增到「Favorites List」(我的最愛清單)：

1. 選取裝置名稱/IP 位址旁邊的核取方塊。
2. 按一下「Add」(新增)。

祕訣：使用「Select All」(全選) 及「Deselect All」(取消全選) 按鈕快速選取 (或取消選取) KX II-101 裝置子網路的全部裝置。

➤ 若要存取探查到的裝置：

- 按一下該裝置的名稱或 IP 位址。隨即會為該裝置開啓新的瀏覽器視窗。

新增我的最愛

➤ 若要將裝置新增到「Favorites List」(我的最愛清單)：

1. 選取「Manage Favorites」(管理我的最愛) > 「Add New Device to Favorites」(新增裝置到我的最愛)。隨即會開啓「Add New Favorite」(新增我的最愛) 頁面：
2. 輸入有意義的說明。
3. 輸入裝置的「IP Address」(IP 位址)。
4. 變更探查連接埠 (如有需要)。
5. 按一下「OK」(確定)。

此裝置即會新增到我的最愛清單。

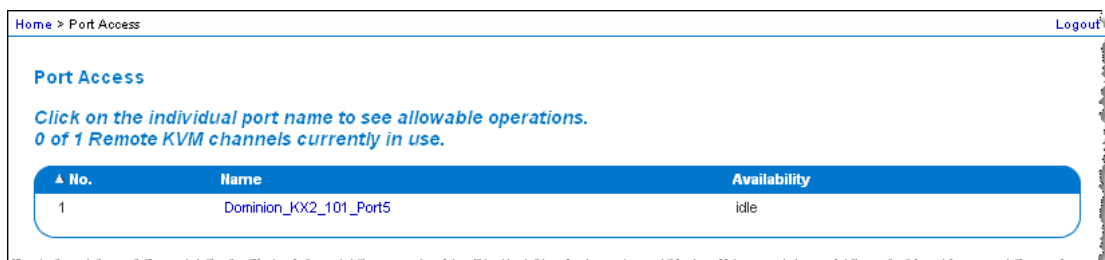
連接埠存取頁面

成功登入「KX II-101 遠端主控台」之後，隨即會開啓「Port Access」(連接埠存取) 頁面。此頁面會顯示 KX II-101 連接埠、其狀態以及可用性。「Port Access」(連接埠存取) 頁面可讓您存取已連接到 KX II-101 的 KVM 目標伺服器。KVM 目標伺服器是您想要透過 KX II-101 裝置來控制的伺服器；其是使用裝置上連接的 PS/2 接頭連接到 KX II-101。

注意：每個 KVM 目標伺服器連線都會開啓一個新的「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗。

➤ 若要使用「Port Access」(連接埠存取) 頁面：

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



The screenshot shows a web browser window with the URL 'Home > Port Access' and a 'Logout' link. The page title is 'Port Access'. Below the title, there is a blue instruction: 'Click on the individual port name to see allowable operations. 0 of 1 Remote KVM channels currently in use.' A table with a blue header and one data row is displayed. The table has three columns: 'No.', 'Name', and 'Availability'. The data row contains the values '1', 'Dominion_KX2_101_Port5', and 'idle'.

No.	Name	Availability
1	Dominion_KX2_101_Port5	idle

- No. (編號)。KX II-101 只有一個連接埠可用。
 - Name (名稱)。KX II-101 連接埠的名稱；初始設定為 Dominion_KX101G2_Port1，但您可將其變更為較具敘述性的名稱。
 - Availability (可用性)。「Availability」(可用性) 可為「Idle」(閒置)、「Connected」(已連線)、「Busy」(忙碌) 或「Unavailable」(無法使用)。
2. 若要連線到目標伺服器，請按一下裝置/目標伺服器的名稱，然後按一下「Connect」(連線) 快顯選項。隨即會開啓「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗，然後其可用性會變成「Busy」(忙碌)。
 3. 若要與目標伺服器中斷連線，請按一下裝置/目標伺服器的名稱，然後按一下「Disconnect」(中斷連線) 快顯選項。隨即會關閉「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗，然後其可用性會變成「Idle」(閒置)。

本章內容

使用者	45
群組	45
使用者與群組之間的關聯性	46
使用者管理	46
遠端驗證	58

使用者

KX II-101 會在內部儲存所有使用者與群組名稱的清單，以決定存取授權與權限。這項資訊是以加密格式儲存於內部。共有多種驗證形態，而這一種則稱之為「本機驗證」。所有使用者皆須經過驗證，若 KX II-101 被設定為使用 LDAP 或 RADIUS，則會先處理驗證，再處理本機驗證。

您必須有使用者名稱與密碼，才能存取 KX II-101 裝置。此項資訊是用以驗證嘗試存取 KX II-101 裝置的使用者。如需新增和編輯使用者的詳細資訊，請參閱 [〈使用者管理〉](#) (請參閱 "使用者管理" p. 46)。

群組

每台 KX II-101 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	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 使用者必須身為 Admin 群組的成員。
Unknown	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 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。

使用者與群組之間的關聯性

除系統所提供的預設群組之外，您也可以建立群組，並指定適當的權限以符合您的需求。如需建立和編輯使用者群組的詳細資訊，請參閱〈使用者管理〉。

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 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「Group」(群組) 資訊判斷使用者的權限，決定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。

使用者管理

使用者管理功能表

「User Management」(使用者管理) 功能表的組織架構如下：

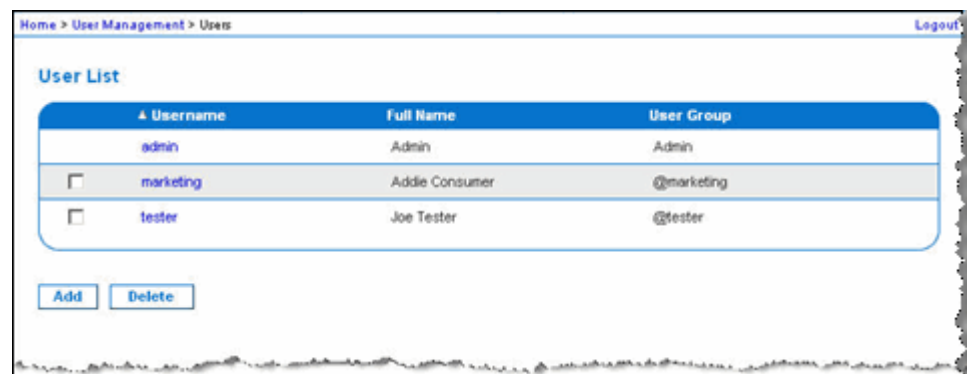
使用：	執行：
User List (使用者清單)	顯示按字母順序排列所有使用者的清單，還可以新增、修改或刪除使用者。
Add New User (新增使用者)	可新增使用者以及修改使用者資訊。
User Group List (使用者群組清單)	顯示按字母順序排列所有使用者群組的清單，還可以新增、修改或刪除使用者群組。
Add New User Group (新增使用者群組)	新增使用者群組以及修改使用者群組資訊。
Change Password (變更密碼)	變更特定使用者的密碼。
Authentication Settings (驗證設定)	設定用以存取 KX II-101 的驗證類型。

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。您也可以在此「User List」(使用者清單) 頁面新增、修改或刪除使用者。

➤ 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)。隨即會開啓「User List」(使用者清單) 頁面。



➤ 若要新增使用者：

- 按一下「Add」(新增) 按鈕。隨即會開啓「User」(使用者) 頁面。如需有關「User」(使用者) 頁面的完整資訊，請參閱 <新增使用者> (請參閱 "新增使用者" p. 48)。

➤ 若要修改現有的使用者：

1. 請從列出的項目中找出該使用者。
2. 按一下使用者名稱。隨即會開啓「User」(使用者) 頁面。如需有關編輯使用者的完整資訊，請參閱 <修改現有使用者> (請參閱 "修改現有的使用者" p. 49)。

➤ 若要刪除使用者：

1. 請選取使用者名稱左側的核取方塊，從列出的項目中選取使用者。
2. 按一下「Delete」(刪除)。隨即會出現提示要求您確認刪除。
3. 按一下「OK」(確定)。

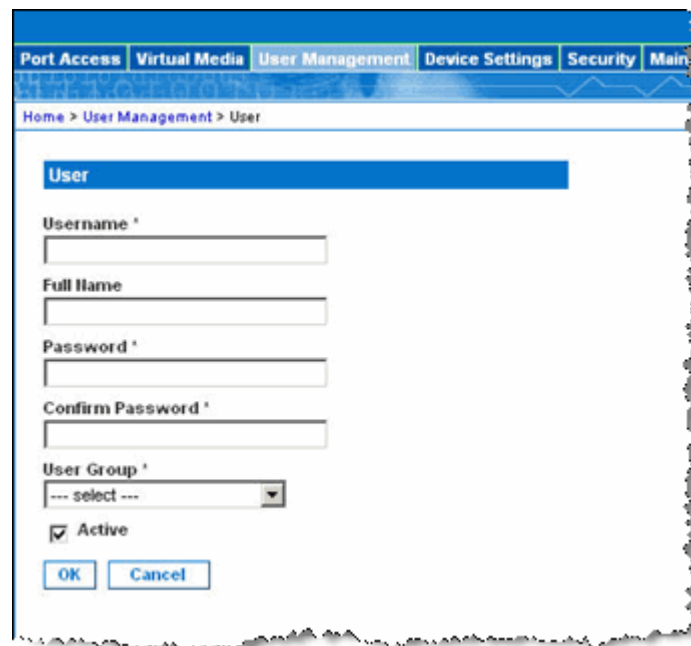
新增使用者

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 使用者。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。

注意： 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 (在取消選取「Active」(使用中) 核取方塊的情況下)。如需詳細資訊，請參閱〈安全性設定〉。

➤ 若要新增使用者：

1. 請使用下列其中一種方法，開啓「User」(使用者) 頁面：
 - 選擇「User Management」(使用者管理) > 「Add New User」(新增使用者)，或
 - 按一下「User List」(使用者清單) 頁面的「Add」(新增) 按鈕。



The screenshot shows a web browser window with a navigation bar at the top containing 'Port Access', 'Virtual Media', 'User Management', 'Device Settings', 'Security', and 'Main'. Below the navigation bar is a breadcrumb trail: 'Home > User Management > User'. The main content area is titled 'User' and contains a form with the following fields: 'Username *' (text input), 'Full Name' (text input), 'Password *' (text input), 'Confirm Password *' (text input), 'User Group *' (dropdown menu with '--- select ---'), and a checked 'Active' checkbox. At the bottom of the form are 'OK' and 'Cancel' buttons.

2. 在「Username」(使用者名稱) 欄位中，輸入唯一的名稱 (最多 16 個字元)。
3. 在「Full Name」(全名) 欄位中，輸入該人員的全名 (最多 64 個字元)。
4. 在「Password」(密碼) 欄位中輸入密碼，在「Confirm Password」(確認密碼) 欄位中再輸入一次密碼 (最多 64 個字元)。

5. 從「User Group」(使用者群組) 下拉式清單中選擇群組。除系統提供的預設群組之外 (<Unknown> (預設值)、Admin、Individual Group)，此清單還包含您已建立的所有群組。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擇「Individual Group」。

注意：Admin 使用者必須身為 Admin 群組的成員。

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. 52)。

6. 若要啟動此使用者，請選取「Active」(使用中) 核取方塊。預設值為啟動 (啓用)。
7. 按一下「OK」(確定)。

修改現有的使用者

➤ 若要修改現有的使用者：

1. 請在「User」(使用者) 頁面中，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. 48)。
2. 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。如需詳細資訊，請參閱 <使用者封鎖> (請參閱 "使用者封鎖" p. 144)。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：

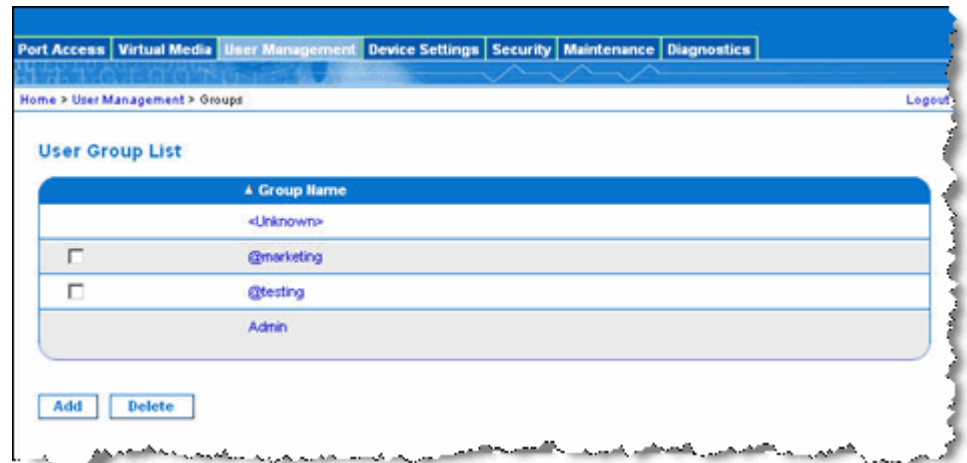
1. 選擇「User Management」(使用者管理) > 「User」(使用者)。隨即會開啓「User」(使用者) 頁面。
2. 選取或取消選取「Active」(使用中) 核取方塊。
 - 如果選取，會讓使用者處於使用中，並取得 KX II-101 的存取權。
 - 如果取消選取，會讓使用者處於非使用中，而且無法存取 KX II-101。
3. 按一下「OK」(確定)。即會更新使用者的使用中狀態。

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。

「User Group List」(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「Group Name」(群組名稱) 欄標題即可以遞增或遞減的順序來排序清單。您也可以在「User Group List」(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「User Management」(使用者管理) > 「User Group List」(使用者群組清單)。隨即會開啓「User Group List」(使用者群組清單) 頁面。



- 若要新增使用者群組：
 - 按一下「Add」(新增) 按鈕。隨即會開啓「Group」(群組) 頁面。如需有關「Group」(群組) 頁面的完整資訊，請參閱 <新增使用者群組 >。
- 若要修改現有的使用者群組：
 1. 請從列出的項目中找出該使用者群組。
 2. 按一下「Group Name」(群組名稱)。隨即會開啓「Group」(群組) 頁面。如需有關編輯群組的完整資訊，請參閱 <修改現有使用者群組 > (請參閱 "修改現有的使用者群組" p. 56)。
- 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> 使用者群組。

祕訣：若要判斷使用者是否屬於特定群組，請依「User Group」(使用者群組) 排序「User List」(使用者清單)。

1. 請選擇「Group Name」(群組名稱) 左側的核取方塊，從列出的項目中選取群組。
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)。

新增使用者群組

➤ 若要新增使用者群組：

1. 請使用下列其中一種方法，開啓「Group」(群組) 頁面：
 - 選擇「User Management」(使用者管理) > 「Add New User Group」(新增使用者群組)，或
 - 按一下「User Group List」(使用者群組清單) 頁面的「Add」(新增) 按鈕。

The screenshot shows the 'Group' configuration page. It includes a 'Group Name' input field, a 'Permissions' section with checkboxes for Device Settings, Diagnostics, Maintenance, PC-Share, Security, and User Management, a 'Port Permissions' section with a table for 'Port', 'Access', 'VM Access', and 'Power Control', and an 'IP ACL' section with a table for 'Rule #', 'Starting IP', 'Ending IP', and 'Action'. At the bottom are 'OK' and 'Cancel' buttons.

「Group」(群組) 頁面會分組歸類為以下類別： Group (群組)、Permissions (權限)、Port Permissions (連接埠權限) 以及 IP ACL。

2. 在「Group Name」(群組名稱) 欄位中，輸入新使用者群組的敘述性名稱。
3. 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。如需詳細資訊，請參閱 <設定權限> (請參閱 "設定權限" p. 52)。
4. 設定「Port Permissions」(連接埠權限)。指定要授與給 KVM 與電源連接埠的存取類型。如需詳細資訊，請參閱 <設定連接埠權限>。
5. 設定 IP ACL (選用)。此功能以指定 IP 位址的方式，來限制 KX II-101 裝置的存取權；本功能僅適用於隸屬特定群組的使用者 (具有優先權)，不像 <IP 存取控制> (請參閱 "IP 存取控制" p. 147) 清單功能適用於所有對裝置的存取嘗試。
6. 按一下「OK」(確定)。

注意：MPC 內提供了數項管理功能，但只有預設 ADMIN 群組的成員才能夠使用這些功能。

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 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。
Diagnostics (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 診斷。
Maintenance (維護)	備份和還原資料庫、韌體升級、出廠重設、重新開機。
PC-Share (電腦共用)	多位使用者可同時存取相同目標。
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/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使用者。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)。隨即會開啓「Group」(群組) 頁面。
3. 選取適當的權限。
4. 按一下「OK」(確定)。

設定連接埠權限

您可以為伺服器連接埠指定存取類型、虛擬媒體的存取類型以及電源控制。請注意，所有權限的預設設定皆為停用。

Access (存取)		VM Access (VM 存取)		Power Control (電源控制)	
選項	說明	選項	說明	選項	說明
None* (無)	完全拒絕存取	Deny* (拒絕)	完全拒絕連接埠的虛擬媒體權限	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)	Deny* (拒絕)	完全拒絕連接埠的虛擬媒體權限	Deny* (拒絕)	完全拒絕存取
Control (控制)	控制所連接的目標伺服器	虛擬媒體存取僅限讀取存取權	僅限讀取存取權。虛擬媒體的完全存取權 (讀取、寫入)	Access (存取)	完全存取
Control (控制)	控制所連接的目標伺服器	Read-Write (讀寫)	虛擬媒體的完全存取權 (讀取、寫入)	Access (存取) 或 Deny (拒絕)	完全存取權或完全拒絕存取

* 預設設定

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 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 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。如需詳細資訊，請參閱 **<IP 存取控制>**（請參閱 "IP 存取控制" p. 147）。

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。

Rule #	Starting IP	Ending IP	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT

Buttons: Append, Insert, Replace, Delete

➤ 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「Action」（動作）：
 - Accept (接受)。指定為接受的 IP 位址，才可以存取 KX II-101 裝置。
 - Drop (捨棄)。指定為捨棄的 IP 位址，都會被拒絕存取 KX II-101 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。
5. 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「Rule #」（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. 從下拉式清單中選擇「Action」（動作）。
4. 按一下「Insert」（插入）。若剛才輸入的「Rule #」（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「Rule #」（規則編號）。
2. 輸入「Starting IP」（起始 IP）與「Ending IP」（結束 IP）欄位。
3. 從下拉式清單中選取「Action」（動作）。

4. 按一下「Replace」(取代)。新規則會取代具有相同規則編號的原始規則。

➤ 若要刪除規則：

1. 指定要刪除的「Rule #」(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。

IP ACL			
Rule #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP
<input type="text"/>	<input type="text"/>	<input type="text"/>	ACCEPT ▾
<input type="button" value="Append"/> <input type="button" value="Insert"/> <input type="button" value="Replace"/> <input type="button" value="Delete"/>			

祕訣： 規則編號可讓您對規則的建立順序擁有較多的控制。

修改現有的使用者群組

注意：Admin (管理) 群組會啓用所有權限，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。

Home > User Management > Group

Group

Group Name *

Permissions

- Device Settings
- Diagnostics
- Maintenance
- PC-Share
- Security
- User Management

Port Permissions

Port	Access	VM Access	Power Control
Dominion_KX2_101_Port1	Deny	Deny	Deny
Power Port 1	Deny		Deny

IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Append Insert Replace Delete

OK Cancel

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。如需詳細資訊，請參閱 <設定權限> (請參閱 "設定權限" p. 52)。
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。如需詳細資訊，請參閱 <設定連接埠權限>。
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 裝置的存取權。如需詳細資訊，請參閱 <分組的 IP 存取控制>。
5. 按一下「OK」(確定)。

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)。隨即會開啓「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) 欄位中輸入新的密碼，在「Confirm New Password」(確認新密碼) 欄位中再輸入一次新密碼。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)。

注意： 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<安全性設定 - 強固密碼> (請參閱“強固密碼” p. 143)。

驗證設定

驗證設定會在稍後於本章中討論遠端驗證時說明。如需詳細資訊，請參閱<驗證設定>。

遠端驗證

CC-SG 使用者注意事項

當 KX II-101 是由 CommandCenter Secure Gateway 控制時，CC-SG 會驗證使用者與群組，但本機使用者除外（需具有本機連接埠存取權）。當 CC-SG 正在控制 KX II-101 時，會以 KX II-101 上設定的本機使用者資料庫或遠端驗證伺服器 (LDAP/LDAPS or RADIUS) 驗證本機連接埠使用者，而不是以 CC-SG 使用者資料庫驗證。

如需 CC-SG 驗證的詳細資訊，請參閱 CommandCenter Secure Gateway 的《使用指南》、《管理員指南》或《部署指南》，網址為：
<http://www.raritan.com/support/> <http://www.raritan.com/support>。

支援的通訊協定

為了簡化使用者名稱與密碼管理，KX II-101 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 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。

驗證與授權

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 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。

驗證設定

您可從「Authentication Settings」(驗證設定) 頁面設定用以存取 KX II-101 的驗證類型。如需驗證與授權如何操作與其不同之處的詳細資訊，請參閱 <驗證與授權> (請參閱 "驗證與授權" p. 58)。

注意：即使選取遠端驗證 (LDAP 或 RADIUS)，還是會使用本機驗證。

➤ 若要設定驗證：

1. 選擇「User Management」(使用者管理) > 「Authentication Settings」(驗證設定)。隨即會開啓「Authentication Settings」(驗證設定) 頁面：

2. 選擇想要使用的驗證通訊協定選項 (「Local Authentication」(本機驗證)、「LDAP」或「RADIUS」)。選擇「LDAP」選項會啓用其餘的 LDAP 欄位；選取「RADIUS」選項則會啓用其餘的 RADIUS 欄位。
3. 如果選擇「Local Authentication」(本機驗證)，請進入步驟 6。

遠端驗證

4. 如果選擇「LDAP」，請參閱「執行 LDAP 遠端驗證」一節，即可取得填寫「Authentication Settings」(驗證設定) 頁面上「LDAP」區段之各欄位的詳細資訊。
5. 如果選擇「RADIUS」，請參閱<執行 RADIUS 遠端驗證> (請參閱"執行 RADIUS 遠端驗證" p. 64) 一節，即可取得填寫「Authentication Settings」(驗證設定) 頁面上「RADIUS」區段之各欄位的詳細資訊。
6. 按一下「OK」(確定) 即可儲存。
 - 若要取消而不儲存變更：
 - 按一下「Cancel」(取消)。
 - 若要回復出廠預設值：
 - 按一下「Reset to Defaults」(重設為預設值) 按鈕。

執行 LDAP 遠端驗證

輕量型目錄存取通訊協定 (LDAP) 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 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 驗證伺服器。

➤ 若要使用 LDAP 驗證通訊協定，請輸入下列資訊：

1. 在「Primary LDAP Server」(主要 LDAP 伺服器) 欄位中，輸入 LDAP 遠端驗證伺服器的 IP 位址或 DNS 名稱。已選取「Enable Secure LDAP」選項時，便必須使用 DNS 名稱。

2. (選用) 在「Secondary LDAP Server」(次要 LDAP 伺服器) 欄位中，輸入備份 LDAP 伺服器的 IP 位址或 DNS 名稱。已選取「Enable Secure 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。
3. 在「Secret Phrase」(通關密碼) 欄位中，輸入以遠端驗證伺服器執行驗證時所需的伺服器密碼，然後在「Confirm Secret Phrase」(確認通關密碼) 欄位中，再輸入一次。請不要變更現有的架構。使用 LDAP 伺服器上使用中的字串。
4. 如果想要使用 SSL，請選取「Enable Secure LDAP」(啓用安全的 LDAP) 核取方塊，便會啓用「Secure LDAP Port」(安全的 LDAP 連接埠) 欄位。安全通訊端層 (SSL) 是一種加密通訊協定，允許 KX II-101 與 LDAP 伺服器安全地進行通訊。
5. 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。
6. 「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。選取「Enable Secure LDAP」(啓用安全的 LDAP) 核取方塊時，便會啓用此欄位。
7. Certificate File (認證檔)。請聯絡驗證伺服器管理員，以為 LDAP 伺服器取得 Base64 編碼 X-509 格式的 CA 認證檔。使用「Browse」(瀏覽) 按鈕瀏覽認證檔。選取「Enable Secure LDAP」(啓用安全的 LDAP) 選項時即會啓用此欄位。
8. DN of administrative User (管理使用者的 DN)。管理使用者的識別名稱，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”。
9. User Search DN (使用者搜尋 DN)。此範例描述利用 LDAP 所繫結的名稱，以及要在資料庫中開始搜尋所指定基本 DN 的位置。
「Base Search」(基本搜尋) 值範例如下：
“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. Type of external LDAP server (外部 LDAP 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 目錄服務，以供在 Windows 環境下使用。
11. Active Directory Domain (Active Directory 網域)。輸入 Active Directory 網域的名稱。

從 Active Directory 伺服器傳回使用者群組資訊

KX II-101 支援對 Active Directory (AD) 進行使用者驗證，而不需要在 KX II-101 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 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。

注意：如果您是 Raritan, Inc. 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 仍將支援此組態，您無須執行下列作業。如需更新 AD LDAP 架構的詳細資訊，請參閱 <更新 LDAP 架構> (請參閱 "更新 LDAP 架構" p. 66)。

➤ 若要在 KX II-101 上啟用 AD 伺服器：

1. 使用 KX II-101 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、KVM_Operator。
2. 在您的 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 使用者指派給在步驟 2 中建立的群組。
4. 在 KX II-101 上，適當地啟用和設定您的 AD 伺服器。請參閱 <執行 LDAP 遠端驗證>。

重要注意事項：

- 群組名稱須區分大小寫。
- KX II-101 提供下列無法變更或刪除的預設群組：Admin 與 <Unknown>。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 群組組態，KX II-101 便會自動對驗證成功的使用者指派 <Unknown> 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：

The screenshot shows a configuration window titled "RADIUS". It contains two main sections for "Primary Radius Server" and "Secondary Radius Server". Each section has input fields for "Shared Secret", "Authentication Port" (set to 1812), "Accounting Port" (set to 1813), "Timeout (in seconds)" (set to 1), and "Retries" (set to 3). At the bottom, there is a "Global Authentication Type" dropdown menu currently set to "PAP".

1. 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 (選用) 次要遠端驗證伺服器的 IP 位址。
2. 在「Shared Secret」(共用密碼) 欄位中，輸入可供驗證使用的伺服器密碼。共用密碼是 KX II-101 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。
3. Authentication Port (驗證連接埠)。預設的驗證連接埠是 1812，請視需要加以變更。

4. Accounting Port (帳戶處理連接埠)。預設的帳戶處理連接埠是 1813，請視需要加以變更。
5. Timeout (in seconds) (逾時 (秒))。預設的逾時為 1 秒鐘，請視需要加以變更。逾時是 KX II-101 傳送其他驗證要求之前，等候 RADIUS 伺服器回應的時間長度。
6. Retries (重試)。預設的重試次數是 3，請視需要加以變更。這是 KX II-101 向 RADIUS 伺服器傳送驗證要求的次數。
7. Global Authentication Type (全域驗證類型)。選擇下拉式清單中的選項：
 - 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。

透過 RADIUS 傳回使用者群組資訊

當 RADIUS 驗證嘗試成功時，KX II-101 裝置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 裝置會傳送下列 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 切換器裝置的 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。

屬性	資料
登入	
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 切換器裝置的 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。
NAS-IP-Address (4)	KX II-101 切換器裝置的 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。

更新 LDAP 架構

注意：本章中的程序應交由經驗豐富的使用者執行。

傳回使用者群組資訊

順利完成驗證之後，請立即使用本章中的資訊，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 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，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啓用此屬性。

從 Microsoft Active Directory

注意：此工作應交由經驗豐富的 Active Directory 管理員執行。

從 Windows 2000 Server 版的 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。

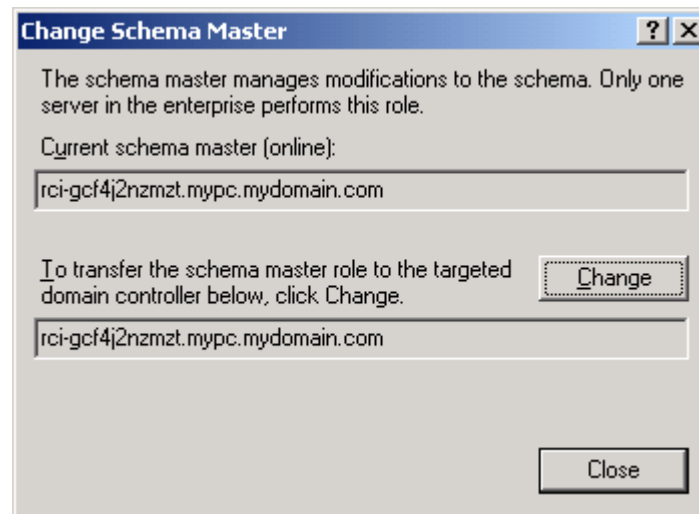
1. 安裝適用於 Active Directory 的架構外掛程式 – 如需說明指示，請參閱 Microsoft Active Directory 文件。
2. 執行 Active Directory 主控台，然後選取「Active Directory Schema」(Active Directory 架構)。

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. (選用) 選取「The Schema may be modified on this Domain Controller」(可在此網域控制站修改架構) 前的核取方塊。
3. 按一下「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)。

- 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。

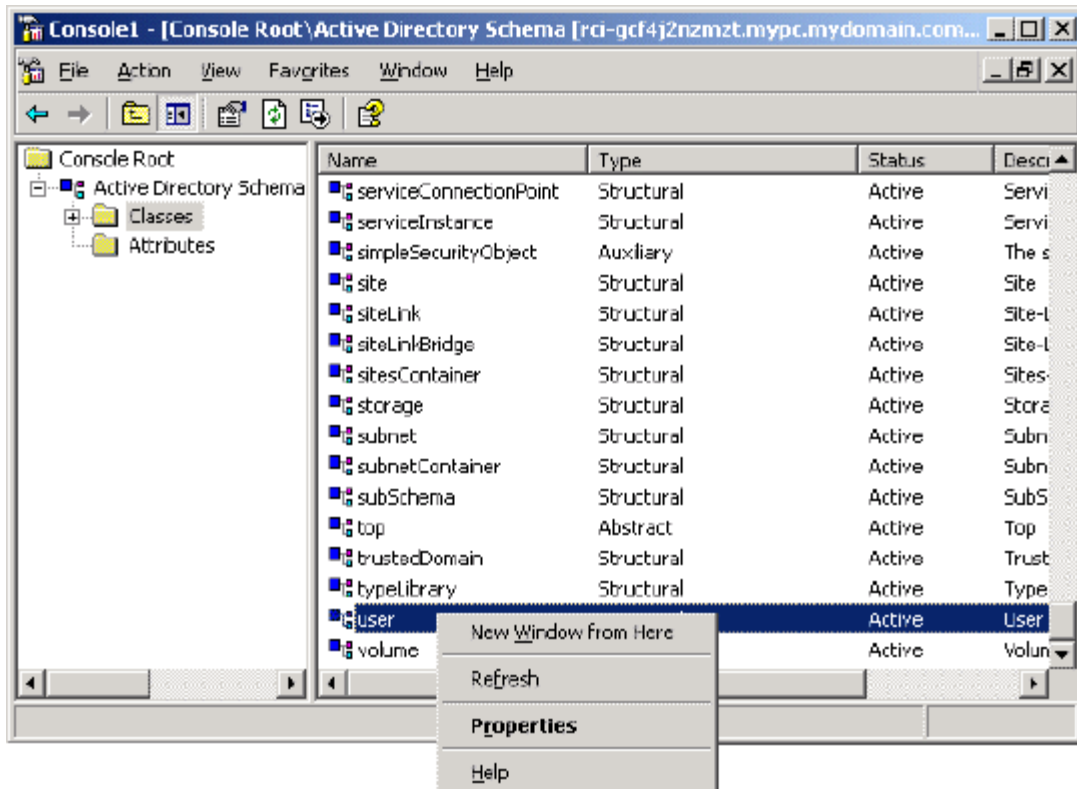
- 在「Common Name」(一般名稱) 欄位中，輸入 *rciusergroup*。
- 在「LDAP Display Name」(LDAP 顯示名稱) 欄位中，輸入 *rciusergroup*。
- 在「Unique x5000 Object ID」(唯一的 x5000 物件 ID) 欄位中，輸入 *1.3.6.1.4.1.13742.50*。
- 在「Description」(說明) 欄位中，輸入有意義的說明。
- 按一下「Syntax」(語法) 下拉箭頭，然後從清單中選取「Case Insensitive String」(字串不區分大小寫)。
- 在「Minimum」(最小值) 中，輸入 *1*。
- 在「Maximum」(最大值) 中，輸入 *24*。
- 按一下「OK」(確定) 即可建立新的屬性。

將屬性新增至類別

➤ 若要將屬性新增至類別：

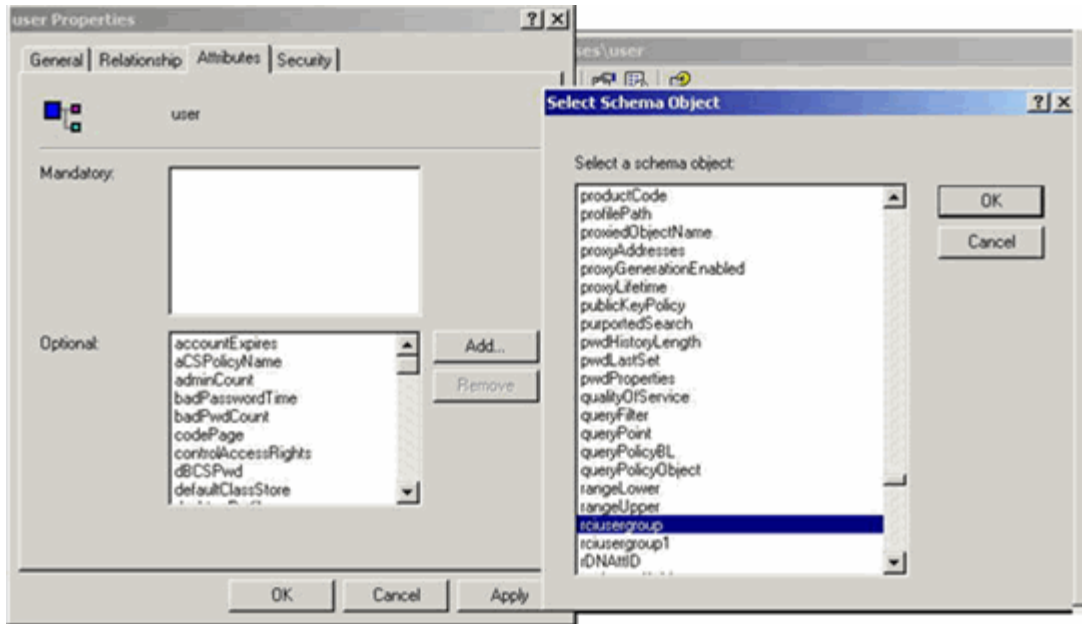
- 在視窗的左窗格中，按一下「Classes」(類別)。

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) 視窗。

- 按一下以開啓「Attributes」(屬性) 索引標籤。



- 按一下「Add」(新增)。
- 從「Select Schema Object」(選取架構物件) 清單中選擇「rciusergroup」。
- 在「Select Schema Object」(選取架構物件) 對話方塊中，按一下「OK」(確定)。
- 在「User Properties」(User 內容) 對話方塊中，按一下「OK」(確定)。

更新架構快取

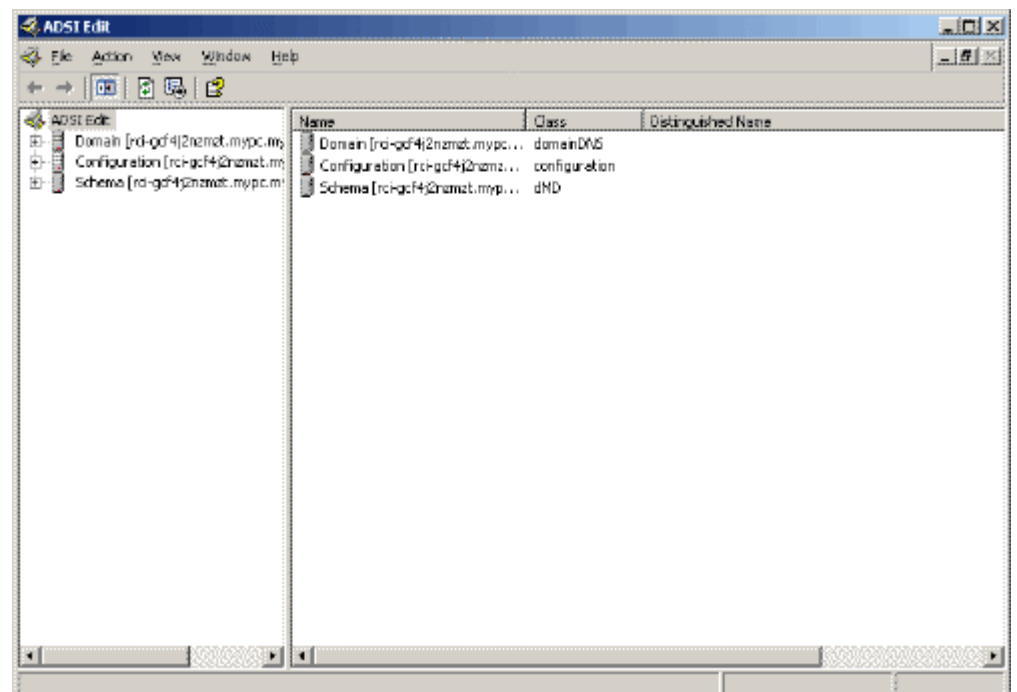
- 若要更新架構快取：
 - 在視窗的左窗格中，以滑鼠右鍵按一下「Active Directory Schema」(Active Directory 架構)，然後從快顯功能表中選取「Reload the Schema」(重新載入架構)。
 - 將「Active Directory Schema MMC」(Active Directory 架構 MMC) 主控台縮到最小。

編輯使用者成員的 rclusergroup 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。

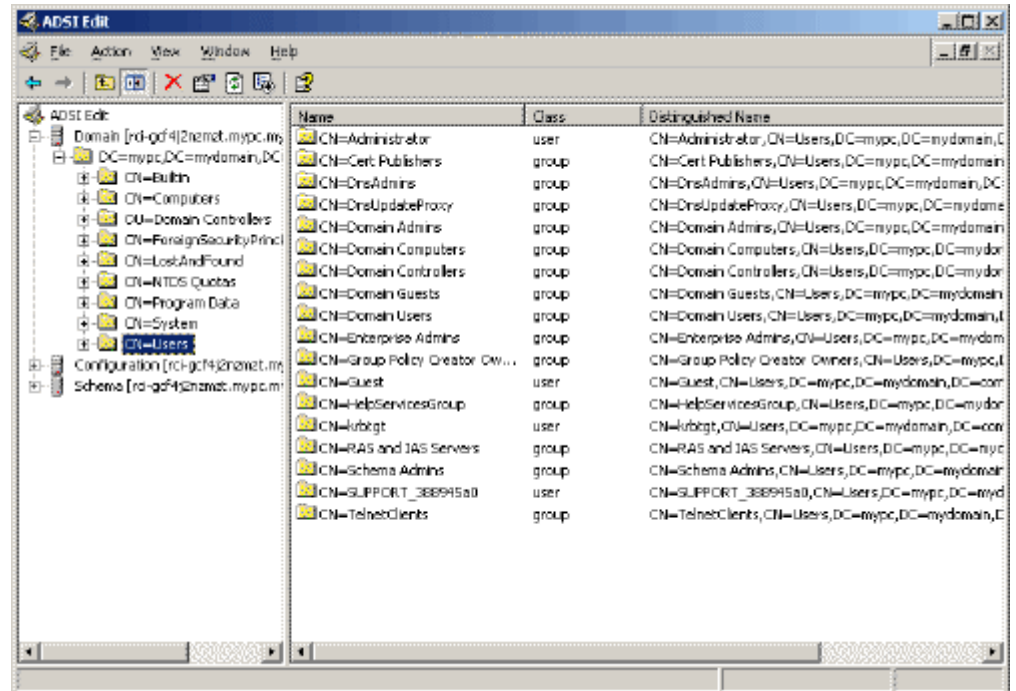
➤ 若要編輯 rclusergroup 群組內個別的使用者屬性：

1. 從安裝光碟中選擇「Support」(支援) > 「Tools」(工具)。
2. 按兩下 SUPTOOLS.MSI，安裝支援工具。
3. 移至已安裝支援工具的目錄。
4. 執行 adsiedit.msc，隨即會開啓「ADSI Edit」(ADSI 編輯) 視窗。



5. 開啓「Domain」(網域)。

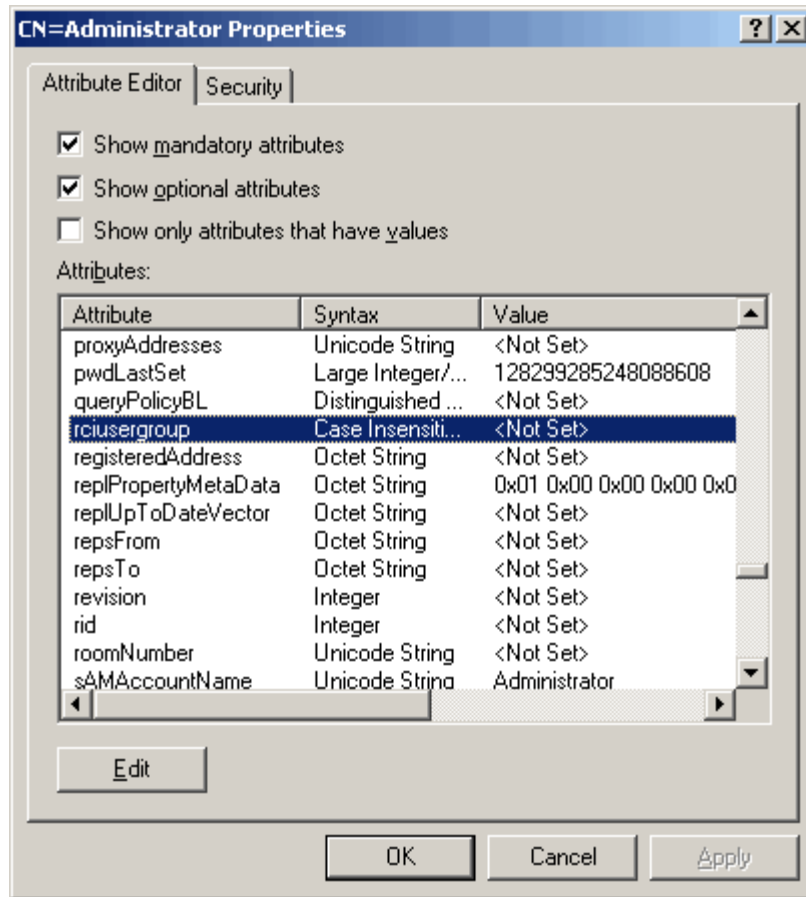
6. 在視窗的左窗格中，選取「CN=User」資料夾。



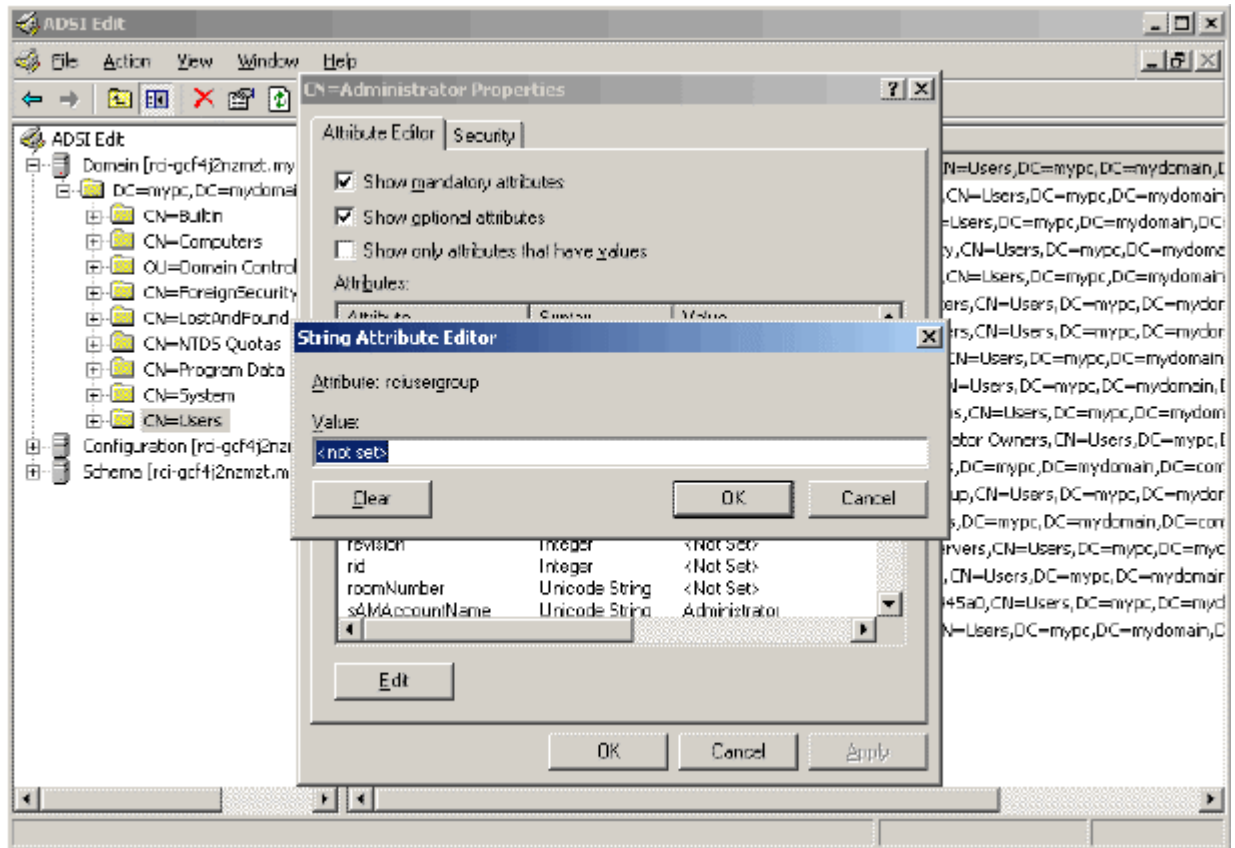
7. 在右窗格中，找出要調整其內容的使用者名稱。 在使用者名稱上按一下滑鼠右鍵，然後選取「Properties」(內容)。

8. 按一下「Attribute Editor」(屬性編輯器) 索引標籤 (如果尚未開啓)。

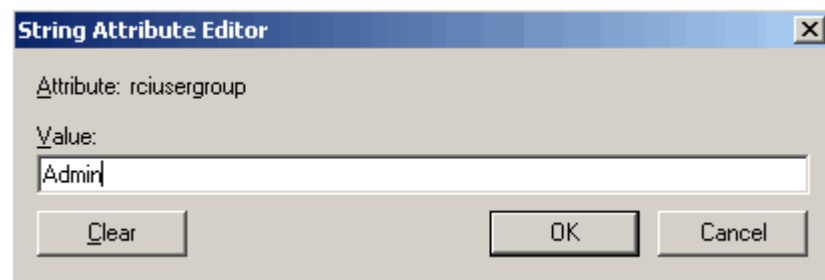
9. 從「Attributes」(屬性) 清單中選擇 rcusergroup。



- 按一下「Edit」(編輯)。隨即會開啓「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 Dominion KX II-101)。



- 按一下「OK」(確定)。

本章內容

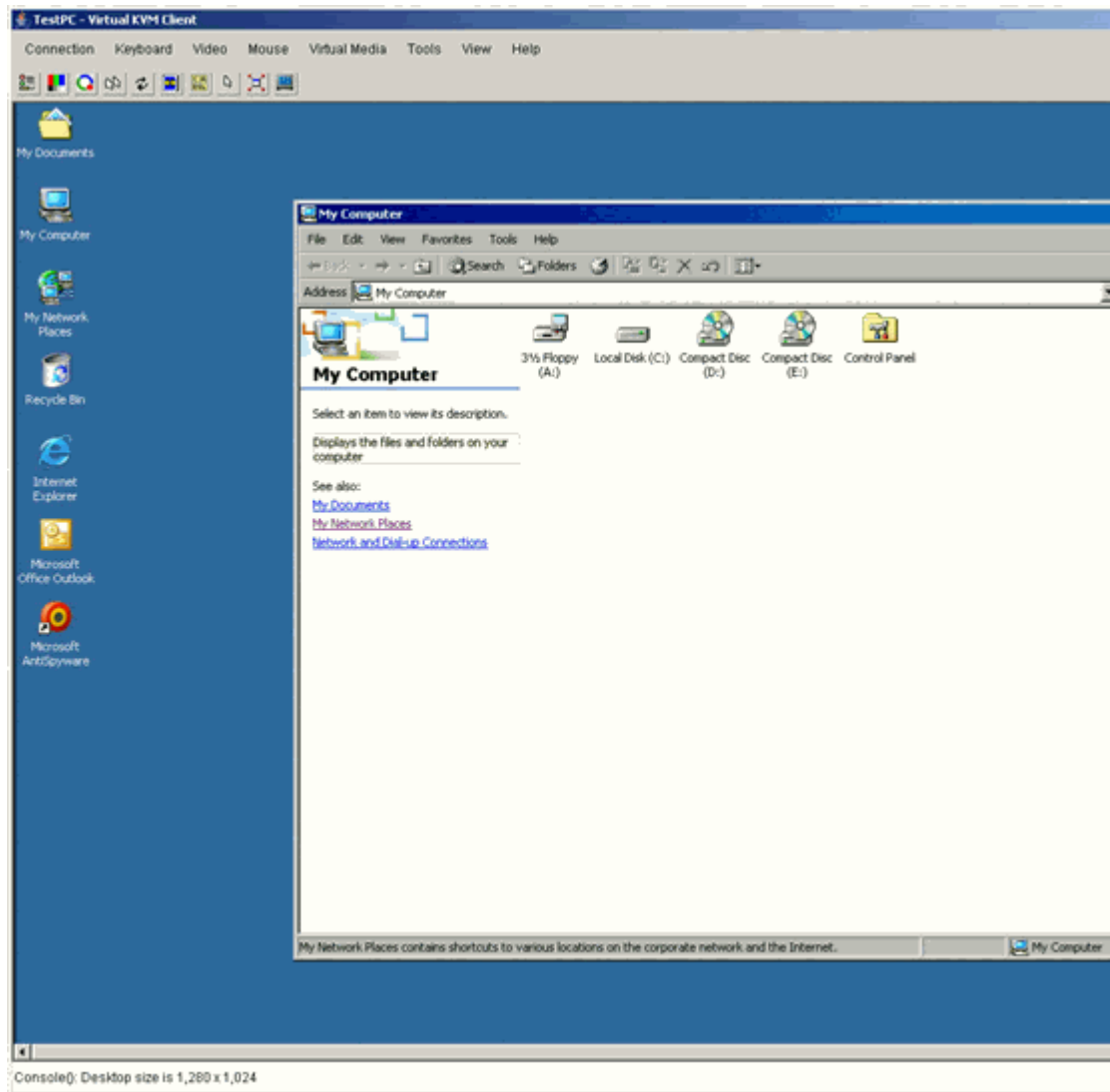
概覽	77
選項	78
滑鼠指標同步	80
連線功能表	81
鍵盤功能表	84
視訊功能表	88
滑鼠功能表	92
VKC 虛擬媒體	95
工具功能表	96
檢視功能表	97
說明功能表	98

概覽

每當您使用「KX II-101 遠端主控台」存取目標伺服器時，即會開啓「Virtual KVM Client」(虛擬 KVM 用戶端) 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。

注意：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。



選項

您可透過功能表與工具列來存取「虛擬 KVM 用戶端」所提供的功能。

功能	說明
功能表列	指令與設定的下拉式功能表。
工具列	常用功能與指令的快速鍵按鈕。
目標伺服器視訊視窗	目標裝置顯示畫面。
狀態列	有關連線參數、目標伺服器視窗大小、同時連線數、Caps Lock 指示燈與 Num Lock 指示燈的即時資訊。

選項

功能表樹狀目錄

下表包含虛擬 KVM 用戶端提供的所有功能表與功能表項目。

- Connection (連線) 功能表：
 - Properties (內容)
 - Connection Info (連線資訊)
 - Exit (結束)
- Keyboard (鍵盤) 功能表：
 - Send Ctrl + Alt + Delete (傳送 Ctrl + Alt + Delete)
 - Keyboard Macros (鍵盤巨集)
 - Keyboard Macros (鍵盤巨集) 選項
 - 使用者建立的巨集 (選用)
- Video (視訊) 功能表：
 - Refresh Screen (重新整理畫面)
 - Auto-Sense Video Settings (自動感應視訊設定)
 - Calibrate Color (校準色彩)
 - Video Settings (視訊設定)
- Mouse (滑鼠) 功能表：
 - Synchronize Mouse (同步化滑鼠)
 - Single Mouse Cursor (單滑鼠游標)
 - Absolute (絕對)

- Intelligent (智慧)
- Standard (標準)
- Virtual Media (虛擬媒體) 功能表：
 - Connect Drive (連接磁碟機)
 - Connect CD-ROM/ISO Image (連接 CD-ROM/ISO 映像檔)
- Tools (工具) 功能表：
 - Options (選項)
- View (檢視) 功能表：
 - View Toolbar (檢視工具列)
 - Scaling (縮放比例)
 - Target Screen Resolution (目標螢幕解析度)
- Help (說明) 功能表：
 - About Raritan Virtual KVM Client (關於 Raritan 虛擬 KVM 用戶端)

工具列

按鈕	說明
	內容
	視訊設定
	校準色彩
	同步化目標滑鼠游標
	重新整理畫面
	自動感應視訊
	傳送 Ctrl+Alt+Delete
	單滑鼠游標
	全螢幕
	將視訊調整為螢幕大小

滑鼠指標同步

從遠端檢視使用滑鼠的目標伺服器時，會看到兩個滑鼠指標：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。




在快速的 LAN 連線中，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）。如需有可用滑鼠模式的詳細資訊，請參閱〈[滑鼠功能表](#)〉（請參閱 "滑鼠功能表" p. 92）。

滑鼠同步提示

要進行滑鼠同步化時，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 KX II-101 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 KX II-101 裝置所見的實際值〈支援的視訊解析度〉。
2. 確認纜線長度並未超過所選取視訊解析度的特定限制。如需詳細資訊，請參閱裝置使用指南中的〈目標伺服器連接距離與視訊解析度〉。
3. 確認已在進行安裝程序時，正確設定滑鼠與視訊。如需完整說明指示，請參閱裝置使用指南中的〈安裝與組態〉。
4. 按一下虛擬 KVM 用戶端的「Auto-sense video」(自動感應視訊) 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. 開啓終端機視窗。
 - b. 輸入 `xset mouse 1 1 command`。
 - c. 關閉終端機視窗。
6. 按一下虛擬 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。

連線功能表

內容對話方塊

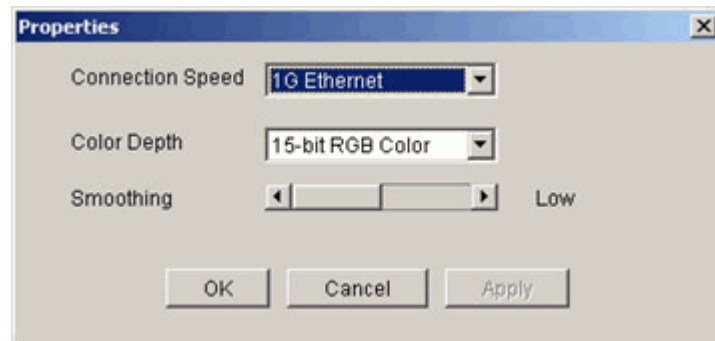
KX II-101 動態視訊壓縮演算法可在不同的頻寬限制下維護 KVM 主控台的可用性。KX II-101 裝置不僅可為 LAN 用途最佳化 KVM 輸出，WAN 用途亦可蒙受此益處。這些裝置還可以控制色彩濃度與限制視訊輸出，在視訊品質與系統對所有頻寬的回應之間取得最佳平衡。

	連線內容	手動調整頻寬的相關選項 (連線速度、色彩濃度等)。
---	------	---------------------------

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。

➤ 若要設定連線內容：

1. 選擇「Connection」(連線) > 「Properties」(內容)。隨即會開啓「Properties」(內容)對話方塊。



連線功能表

2. 從下拉式清單中選擇「Connection Speed」(連線速度)。 KX II-101 可自動偵測可用的頻寬但不限制頻寬使用；但您也可根據頻寬限制調整此用法。

Auto (自動)

1G Ethernet (1G 乙太網路)

100 Mb Ethernet (100 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)

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」(色彩濃度)。 KX II-101 可動態調整傳送給遠端使用者的色彩濃度，以充分利用頻寬達到最大的使用。

15-bit RGB Color (15
位元 RGB 色彩)

8-bit RGB Color (8 位
元 RGB 色彩)

4-bit Color (4 位元色
彩)

4-bit Gray (3 位元灰
階)

3-bit Gray (3 位元灰
階)

2-bit Gray (2 位元灰階)

Black and White (黑白)

重要：在大部分的管理工作中 (伺服器監控、重新配置等) 並不需使用多數視訊圖形卡所提供的 24 位元或 32 位元全彩色譜。嘗試以如此高的色彩濃度進行傳輸，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。
- 若要取消而不儲存變更：
- 按一下「Cancel」(取消)。

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) > 「Connection Info」(連線資訊)。隨即會開啓「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)。KX II-101 裝置的名稱。
- IP Address (IP 位址)。KX II-101 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)。螢幕的水平解析度。
- 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取的程式中。

結束


- 若要關閉虛擬 KVM 用戶端 (目前存取的目標)：
 - 選擇「Connection」(連線) > 「Exit」(結束)。

鍵盤功能表

傳送 Ctrl+Alt+Delete

因為使用頻繁，「虛擬 KVM 用戶端」內已預先程式化 Ctrl+Alt+Delete 巨集。

此按鍵組合會傳送至目前連線的目標伺服器。反之，若您在使用「虛擬 KVM 用戶端」時實際按下 Ctrl+Alt+Delete 鍵，因作業系統結構之故，您的電腦會先攔截此指令，而不會將此按鍵結合傳送至預定的目標伺服器。

	傳送 Ctrl+Alt+Delete	將 Ctrl+Alt+Delete 按鍵組合傳送至目標伺服器
---	--------------------	--------------------------------

- 若要將 Ctrl+Alt+Delete 按鍵組合傳送至目標伺服器：
 - 選擇「Keyboard」(鍵盤) > 「Send Ctrl+Alt+Delete」(傳送 Ctrl+Alt+Delete)，或
 - 按一下工具列上的「Send Ctrl+Alt+Delete」(傳送 Ctrl+Alt+Delete) 按鈕。

鍵盤巨集

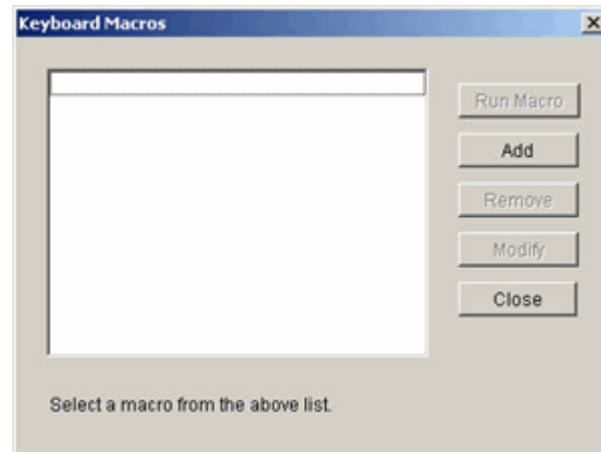
鍵盤巨集可確保所要傳送至目標伺服器的按鍵組合，必會傳送至該目標伺服器，而且只能由該目標伺服器進行轉譯。否則，其可能會由正在執行「虛擬 KVM 用戶端」的電腦 (即用戶端電腦) 所轉譯。

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 MPC 中使用，反之亦然。

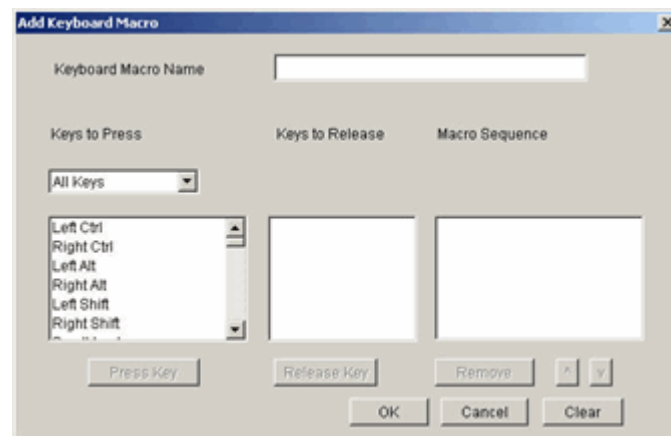
建立鍵盤巨集

➤ 若要建立鍵盤巨集 (新增巨集)：

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. 按一下「Add」(新增)，隨即會出現「Add Keyboard Macros」(新增鍵盤巨集) 對話方塊。

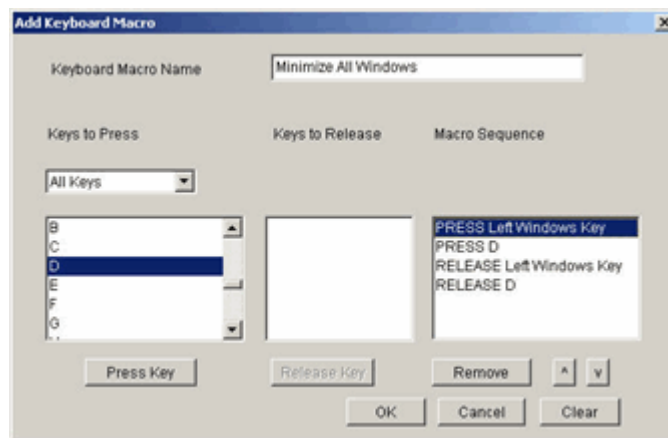


3. 在「Keyboard Macro Name」(鍵盤巨集名稱) 欄位中輸入名稱。這是在建立巨集之後，顯示在虛擬 KVM 用戶端功能表列的名稱。在本範例中，則是輸入「Minimize All Windows」(最小化所有視窗)。
4. 在「Keys to Press」(按鍵) 下拉式清單中：

- a. 捲動瀏覽並選取要模擬按鍵動作的各個鍵 (請依按鍵順序選擇)。
- b. 在每個選項之後按一下「Press Key」(按下按鍵)。每個選取的按鍵都會顯示在「Keys to Release」(要發送的按鍵) 欄位中。

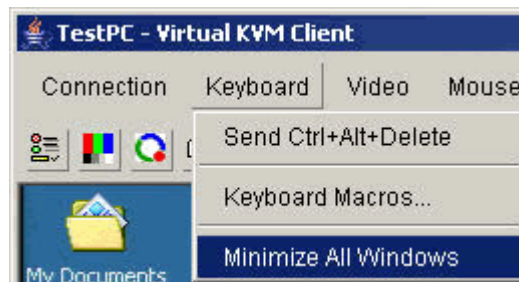
在此範例中，請選取兩個按鍵：Windows 按鍵與字母 D 鍵。

5. 在「Keys to Release」(要發送的按鍵) 欄位中：
 - a. 選擇要模擬發送按鍵的每個鍵 (請依其發送順序選擇)。
 - b. 在每個選項之後按一下「Release Key」(發送按鍵)。在此範例中，也必須發送按下的兩個鍵。
6. 檢閱「Macro Sequence」(巨集組合) – 已使用「Keys to Press」(按鍵) 及「Keys to Release」(要發送的按鍵) 選項自動產生。確認「Macro Sequence」(巨集組合) 確實是您所需的按鍵組合。(若要移除組合中的步驟，請選取該步驟，然後按一下「Remove」(移除)。



祕訣：使用 ^ 及 v 鍵重新排列按鍵組合。

7. 在「Add Keyboard Macro」(新增鍵盤巨集) 視窗中，按一下「OK」(確定) 以儲存巨集。
8. 在「Keyboard Macros」(鍵盤巨集) 視窗中，按一下「Close」(關閉)。建立的鍵盤巨集現已列為「Keyboard」(鍵盤) 功能表的選項：



- 若要清除所有欄位重新來過：
- 按一下「Clear」(清除) 按鈕。

執行鍵盤巨集

鍵盤巨集一旦建立，在「Keyboard」(鍵盤) 功能表中按一下其名稱即可執行。

➤ 若要執行巨集 (使用本範例)：

- 選擇「Keyboard」(鍵盤) > 「Minimize All Windows」(最小化所有視窗)。

另一個方法是從「Keyboard Macros」(鍵盤巨集) 視窗中選取巨集。

➤ 若要執行巨集：

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. 從列出的項目中選取巨集。
3. 按一下「Run Macro」(執行巨集)。

修改鍵盤巨集

➤ 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)。隨即會開啓「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)。

移除鍵盤巨集

➤ 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。

視訊功能表

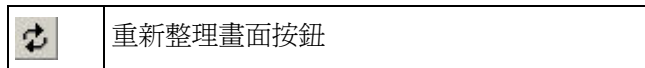
有數種方法可自動重新整理視訊設定：

- 「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) 選項會自動偵測目標伺服器的視訊設定
- 「Calibrate Color」(校準色彩) 選項會校準視訊以增強顯示的色彩品質

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

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。

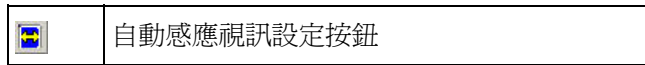


➤ 若要重新整理視訊設定，請執行下列其中一項動作：

- 選擇「Video」(視訊) > 「Refresh Screen」(重新整理畫面)。
- 按一下工具列的「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) 選項會強制重新感應視訊設定 (解析度、螢幕更新頻率) 並重繪視訊螢幕。




➤ 若要自動偵測視訊設定，請執行下列其中一項動作：

- 選擇「Video」(視訊) > 「Auto-sense Video Settings」(自動感應視訊設定)。
- 按一下工具列中的「Auto-Sense Video Settings」(自動偵測視訊設定) 按鈕。

隨即會顯示訊息，表示正在進行自動調整。

校準色彩

使用「Calibrate Color」(校準色彩) 指令可最佳化所傳送視訊影像的色彩層次 (色調、亮度、飽和度)。每部目標伺服器的 KX II-101 色彩設定都不相同。

	校準色彩	調整色彩設定，以最佳化視訊顯示畫面。
---	------	--------------------

注意：「Calibrate Color」(校準色彩) 選項僅適用於目前的連線。

➤ 若要校準色彩：

1. 對執行圖形化使用者介面的任一目標伺服器開啓遠端 KVM 連線。
2. 選擇「Video」(視訊) > 「Calibrate Color」(校準色彩)；或按一下「Calibrate Color」(校準色彩) 按鈕。目標裝置螢幕即會更新其色彩校準。

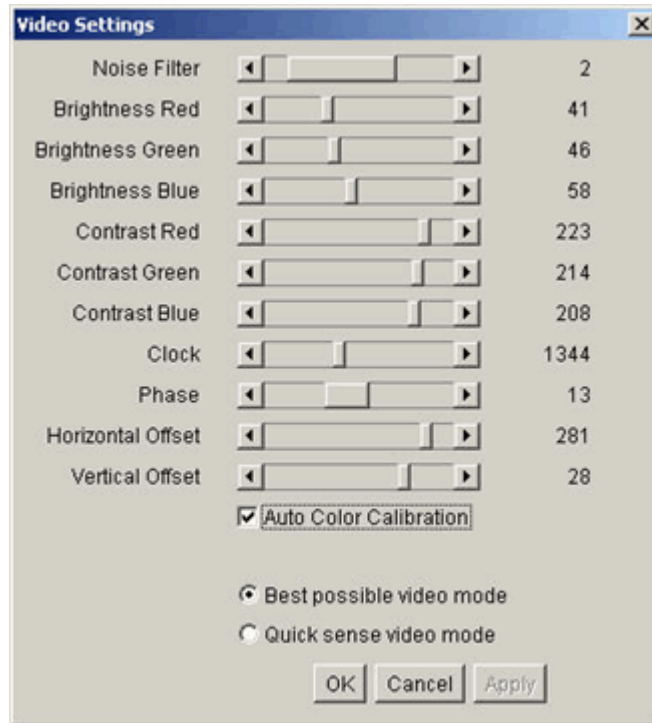
視訊設定

使用「Video Settings」(視訊設定) 選項可手動調整視訊設定。

	視訊設定	開啓「Video Settings」(視訊設定) 以手動調整視訊參數。
--	------	-------------------------------------

➤ 若要變更視訊設定：

1. 選擇「Video」(視訊) > 「Video Settings」(視訊設定)。隨即會出現顯示目前設定的「Video Settings」(視訊設定) 對話方塊：



2. 使用滑桿調整設定以取得所要的結果 (您可在調整設定時立即看到效果)：

- Noise Filter (過濾雜訊)。 KX II-101 可濾除圖形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。
- Brightness (亮度)：使用此設定可調整目標伺服器顯示畫面的亮度。
 - Red (紅色)。控制紅色訊號的亮度。
 - Green (綠色)。控制綠色訊號的亮度。
 - Blue (藍色)。控制藍色訊號的亮度。
- Color Contrast Settings (色彩對比設定)：控制對比調整。

- Contrast Red (紅色對比)。 控制紅色訊號。
- Contrast Green (綠色對比)。 控制綠色訊號。
- 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「時脈」與「相位」設定時請務必謹慎小心，因為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。

- Clock (時脈)。 控制視訊像素透過視訊畫面顯示的速度。 變更時脈設定會造成視訊影像水平拉長或縮短；建議使用奇數設定值。 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。
- Offset (位移)： 控制螢幕畫面的位置：
 - 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。
 - 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。
- Auto Color Calibration (自動色彩校準)。 如果希望自動校準色彩，請選取此選項。
- Video Sensing (視訊感應)： 選取視訊感應模式：
 - 最佳可用視訊模式： KX II-101 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。
 - Quick sense video mode (快速感應視訊模式)： 選取此選項，會使 KX II-101 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 配置，此選項特別有幫助。

3. 按一下「Apply」(套用)。 隨即會變更「Video Settings」(視訊設定)。

注意： 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。

滑鼠功能表

控制目標伺服器時，KX II-101 選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。您可在單滑鼠模式或雙滑鼠模式中操作。在雙滑鼠模式中只要正確設定，兩個滑鼠游標即會對齊。滑鼠同步化若發生問題，請參閱〈控制目標伺服器〉。

當有兩個滑鼠游標時，KX II-101 會提供數種滑鼠模式：

- 絕對 (滑鼠同步)
- 智慧 (滑鼠模式)
- 標準 (滑鼠模式)

同步化滑鼠

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

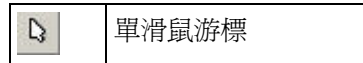


➤ 若要同步化滑鼠，請執行下列其中一項動作：

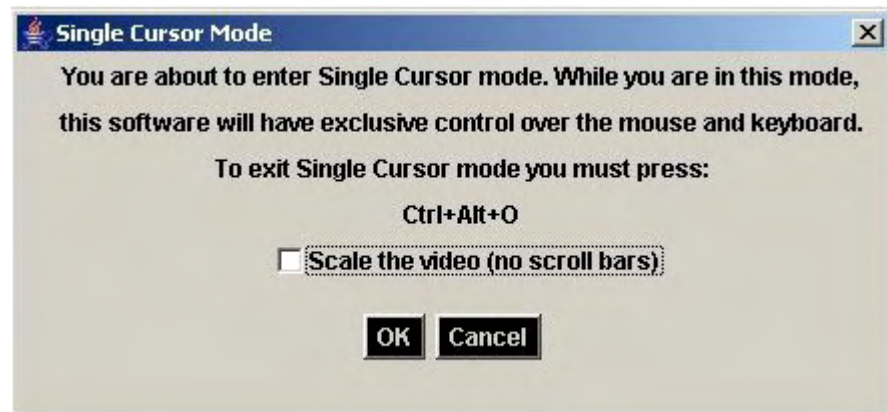
- 選擇「Mouse」(滑鼠) > 「Synchronize Mouse」(同步化滑鼠)。
- 按一下工具列中的「Synchronize Mouse」(同步化滑鼠) 按鈕。

單滑鼠游標

「Single Mouse Cursor」(單滑鼠游標) 會進入單滑鼠模式，處於此模式便只會顯示目標伺服器的滑鼠游標，本機電腦滑鼠指標將不再出現於螢幕畫面中。處於單滑鼠模式時，因為不需要同步化一個滑鼠游標，所以會停用「Synchronize Mouse」(同步化滑鼠) 選項。



- 若要進入單滑鼠模式，請執行下列其中一項動作：
 - 選擇「Mouse」(滑鼠) > 「Single Mouse Cursor」(單滑鼠游標)。
 - 按一下工具列中的「Single/Double Mouse Cursor」(單/雙滑鼠游標) 按鈕。
- 若要結束單滑鼠模式：
 1. 進入單滑鼠模式時，會顯示下列訊息。按一下「OK」(確定)。



2. 在鍵盤上按 **Ctrl+Alt+O**，結束單滑鼠模式。

標準

這是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。標準滑鼠模式為預設值。

- 若要進入標準滑鼠模式：
 - 選擇「Mouse」(滑鼠) > 「Standard」(標準)。

智慧

在智慧滑鼠模式中，KX II-101 可偵測目標滑鼠設定並據以同步化滑鼠指標，允許目標上的滑鼠加速設定。在此模式中，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。

如需智慧滑鼠模式的詳細資訊，請參閱《Raritan 多平台用戶端使用指南》之附錄 B：〈智慧滑鼠同步的條件〉(位於 Raritan 網站

<http://www.raritan.com/support/productdocumentation>，或參閱 KX II-101 所附之 Raritan 使用手冊與快速安裝手冊 CD ROM。

➤ 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

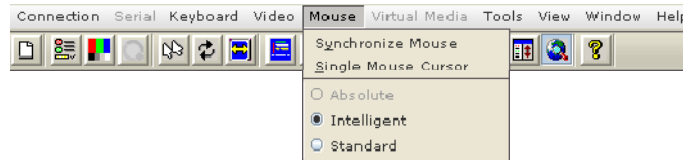
您可以使用「Mouse」(滑鼠) 功能表提供的「Intelligent Mouse Synchronization」(智慧滑鼠同步) 指令，在滑鼠不在使用中時自動重新同步化滑鼠游標。不過，要讓此功能正常運作，必須符合下列條件：

- 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

注意：絕對滑鼠同步僅限用於具虛擬媒體功能的 USB CIM (D2CIM-VUSB)。

此模式使用絕對座標讓用戶端與目標指標保持同步，即使目標滑鼠設定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，滑鼠在目標伺服器上會移動到確實的位置。

- 若要進入絕對滑鼠模式：
 - 選擇「Mouse」(滑鼠) > 「Absolute」(絕對)。

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. 99) 一章。

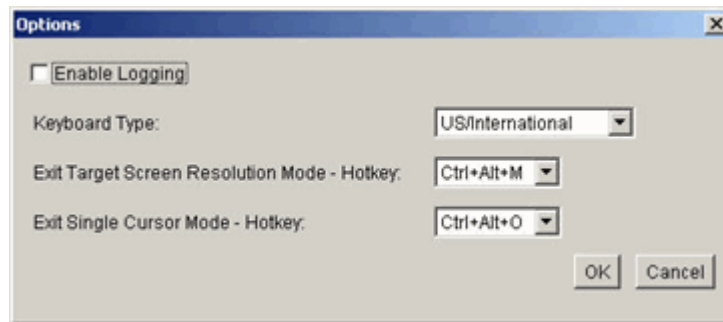
工具功能表

選項

您可在「Tools」(工具) 功能表指定特定選項，以使用「虛擬 KVM 用戶端」：在雙滑鼠模式中同步化滑鼠、啓用記錄、鍵盤類型及退出目標螢幕解析度模式快速鍵。

➤ 若要設定工具選項：

1. 選擇「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」(啓用記錄) 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：
 - US/International (美式鍵盤/國際通用)
 - French (France) (法文鍵盤 (法國))
 - German (Germany) (德文鍵盤 (德國))
 - Japanese (日文鍵盤)
 - United Kingdom (英式鍵盤)
 - Korean (Korea) (韓文鍵盤 (南韓))
 - Belgian (比利時文鍵盤)
 - Norwegian (挪威文鍵盤)
 - Danish (丹麥文鍵盤)
 - Swedish (瑞典文鍵盤)

4. **Exit Target Screen Resolution Mode - Hotkey** (結束目標螢幕解析度模式 - 快速鍵)。當您進入目標螢幕解析度模式時，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，請從下拉式清單中選取。
5. **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，請從下拉式清單中選取。
6. 按一下「OK」(確定)。

檢視功能表

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 (開啓和關閉)：
 - 選擇「View」(檢視) > 「View Toolbar」(檢視工具列)。

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 (開啓和關閉)：
 - 選擇「View」(檢視) > 「Scaling」(縮放比例)。

目標螢幕解析度

當您進入目標螢幕解析度模式時，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。結束此模式所使用的快速鍵是在「Options」(選項) 對話方塊中指定 (預設值為 Ctrl+Alt+M)。

- 若要進入目標螢幕解析度模式：
 - 選擇「View」(檢視) > 「Target Screen Resolution」(目標螢幕解析度)。
- 若要結束目標螢幕解析度模式：
 - 按下在「Tools」(工具) > 「Options」(選項) 對話方塊中設定的快速鍵。預設值為 Ctrl+Alt+M。

CC-SG 使用者注意事項：目標螢幕解析度已停用；只有不受 CC-SG 管理的 KX II-101 裝置，才能使用全螢幕模式。

說明功能表

關於 Raritan 虛擬 KVM 用戶端

此功能表選項提供「虛擬 KVM 用戶端」的版本資訊，以備您要求 Raritan 技術支援協助之需。

- 若要取得版本資訊：
 - 請選取「Help」(說明) > 「About Raritan Virtual KVM Client」(關於 Raritan 虛擬 KVM 用戶端)。

本章內容

概覽	100
使用虛擬媒體的必要條件	102
使用虛擬媒體	103
開啓 KVM 階段作業	104
連接虛擬媒體	105
中斷虛擬媒體的連線	108
檔案伺服器設定 (僅限檔案伺服器 ISO 映像檔)	109

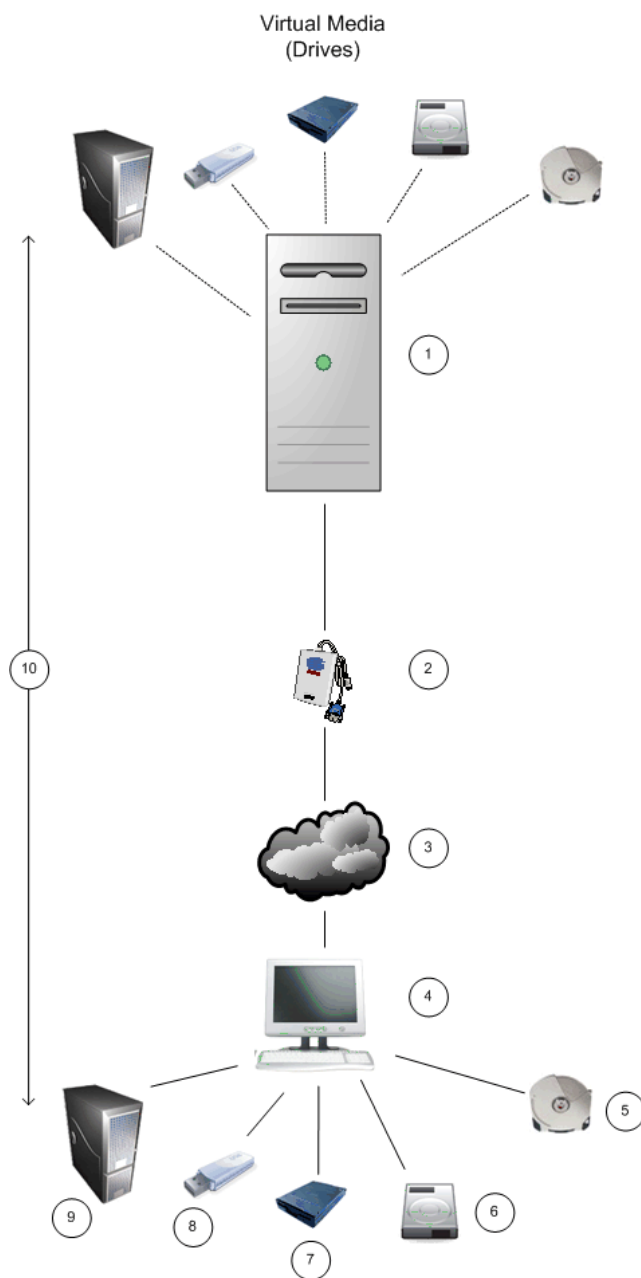
概覽

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。



- 1 目標伺服器。
- 2 KX II-101
- 3 從 KX II-101 到本機工作站的 IP 網路連線。
- 4 本機工作站。
- 5 CD/DVD 光碟機。
- 6 硬碟映像檔。

使用虛擬媒體的必要條件

- 7 軟碟機。
- 8 USB 隨身碟。
- 9 遠端檔案伺服器 (ISO 映像檔)。
- 10 虛擬連線

使用虛擬媒體的必要條件

若要使用虛擬媒體，必須符合下列條件：

KX II-101

- 對於需要存取虛擬媒體的使用者，必須設定 KX II-101 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)。連接埠權限是在群組層級設定，如需詳細資訊，請參閱裝置使用指南的〈設定連接埠權限〉。
- KX II-101 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)，還必須在「Security Settings」(安全性設定) 頁面中啟用「PC Share Mode」(電腦共用模式)(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。如需選擇 USB 設定檔的詳細資訊，請參閱裝置使用指南中的〈設定 USB 設定檔〉。

用戶端電腦

- 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)。

注意：如果您是使用 Microsoft Vista 關閉「使用者帳戶控制」：「控制台」>「使用者帳戶」>「使用者帳戶控制」> 關閉。

如果您不想要變更 Vista 帳戶權限，請以管理員的身分執行 Internet Explorer。若要這樣做，請按一下「開始」功能表，找到 IE，在其上按一下滑鼠右鍵，然後選取「以系統管理員身分執行」。

- USB 2.0 連接埠不僅速度快，在此也是較好的選擇。

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。

使用虛擬媒體

使用 KX II-101 虛擬媒體功能，您最多可裝載兩部不同類型的磁碟機。這些磁碟機可在 VM 階段作業期間提供存取。

➤ 若要使用虛擬媒體：

1. 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。
2. 驗證是否符合正確的**必要條件** (請參閱 "使用虛擬媒體的必要條件" p. 102)。
3. (僅限檔案伺服器 ISO 映像檔) 如果您計劃存取檔案伺服器 ISO 映像檔，請透過「KX II-101 遠端主控台」的「**File Server Setup**」(**檔案伺服器設定**) 頁面 (請參閱 "檔案伺服器設定 (僅限檔案伺服器 ISO 映像檔)" p. 109)，識別這些檔案伺服器與映像檔。

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

4. 以適當的目標伺服器開啓 KVM 階段作業。
5. 連接虛擬媒體。

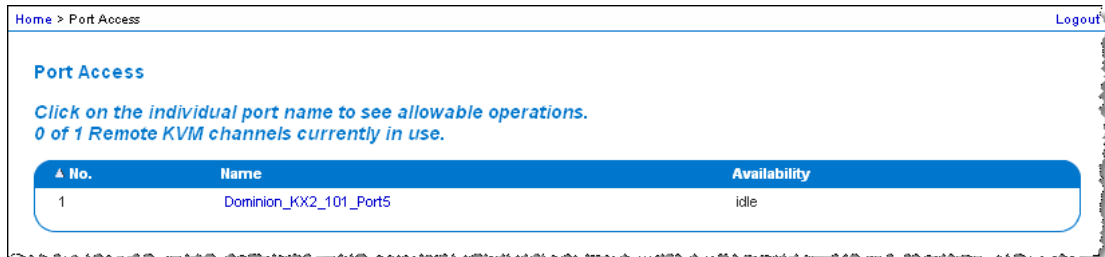
若為：	選取此 VM 選項：
本機磁碟機	Connect Drive (連接磁碟機) (請參閱 "本機磁碟機" p. 105)
本機 CD/DVD 光碟機	Connect CD-ROM/ISO Image (連接 CD-ROM/ISO 映像檔) (請參閱 "CD-ROM/DVD-ROM/ISO 映像檔" p. 107)
ISO 映像檔	Connect CD-ROM/ISO Image (連接 CD-ROM/ISO 映像檔)
檔案伺服器 ISO 映像檔	Connect CD-ROM/ISO Image (連接 CD-ROM/ISO 映像檔)

工作完成後，請**中斷虛擬媒體的連線** (p. 108)。

開啓 KVM 階段作業

➤ 若要開啓 KVM 階段作業：

1. 請從 KX II-101 遠端主控台開啓「Port Access」(連接埠存取) 頁面。



2. 從「Port Access」(連接埠存取) 頁面連線到目標伺服器：
 - a. 按一下目標伺服器的「Name」(名稱)。
 - b. 從快顯功能表選取「Connect」(連線)。



隨即會在「Virtual KVM Client」(虛擬 KVM 用戶端) 視窗中開啓目標伺服器。

連接虛擬媒體

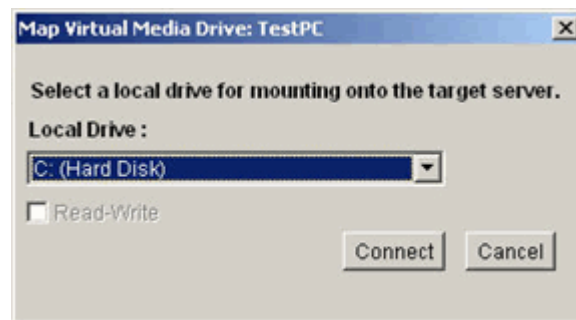
本機磁碟機

此選項可裝載整部磁碟機；整部磁碟機會虛擬裝載於目標伺服器上。此選項僅適用於硬碟與外接磁碟機；其中不含網路磁碟機、CD-ROM 或 DVD-ROM 光碟機。這是唯一可進行讀取/寫入的選項。

注意：當執行特定 Windows 作業系統版本的 KVM 目標伺服器被重新導向回 NTFS 格式的分割區（例如，本機的 C 磁碟機）時，可能無法接受新的大量儲存裝置連線。如果發生這種情況，請關閉 KX II-101 遠端主控台，然後在重新連線後，重新導向到其他虛擬媒體裝置。若有其他使用者連接到相同的目標伺服器，也必須關閉其目標伺服器連線。

➤ 若要存取用戶端電腦上的磁碟機：

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



2. 選擇「Local Drive」(本機磁碟機) 下拉式清單中的磁碟機。
3. 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. 106)。選取此選項後，即可讀取或寫入連接的 USB 磁碟。

警告： 啓用「讀寫」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「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。

注意：如果目標伺服器沒有 USB 連線，您會看見以下警告訊息：
「已設定虛擬媒體功能，但無法使用，除非已經連接 USB 纜線或開啓目標的電源。請檢查您的 USB 連線，或查看是否已開啓目標的電源。」請在解決這個問題後，再次連接磁碟機。

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：

- 用於所有硬碟時。
- 磁碟機有防寫保護時。
- 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)

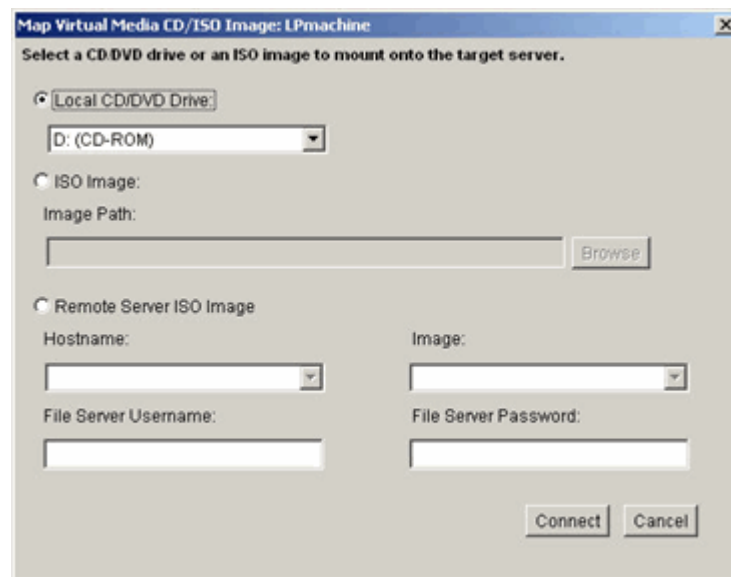
CD-ROM/DVD-ROM/ISO 映像檔

此選項可裝載 CD-ROM、DVD-ROM 與 ISO 映像檔。

注意：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)。隨即會開啓「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」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) 按鈕。

中斷虛擬媒體的連線

- 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 KX II-101 的「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。
 - 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。

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)。

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

檔案伺服器設定 (僅限檔案伺服器 ISO 映像檔)

注意：只有使用虛擬媒體存取檔案伺服器 ISO 映像檔時，才需要此功能。

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

使用 KX II-101 遠端主控台的「File Server Setup」(檔案伺服器設定) 頁面，透過使用 KX II-101 虛擬媒體，指定想要存取的檔案伺服器與映像檔路徑。此處所指定的檔案伺服器 ISO 映像檔，會成為「Remote Server ISO Image Hostname」(遠端伺服器 ISO 映像檔主機名稱) 與「Image」(映像檔) 下拉式清單中的可用選項 (位於「Map Virtual Media CD/ISO Image」(對應虛擬媒體 CD/ISO 映像檔) 對話方塊 (請參閱「CD-ROM/DVD-ROM/ISO 映像檔」p. 107))。

➤ 若要指定虛擬媒體存取所需的檔案伺服器 ISO 映像檔：

1. 從 KX II-101 遠端主控台中選擇虛擬媒體。隨即會開啓「File Server Setup」(檔案伺服器設定) 頁面。

Selected	Host Name/IP Address	Image Path
<input checked="" type="checkbox"/>	192.168.1.193	/images/disk1.iso
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

2. 輸入所要存取之檔案伺服器 ISO 映像檔的相關資訊：

檔案伺服器設定 (僅限檔案伺服器 ISO 映像檔)

- Host Name/IP Address (主機名稱/IP 位址)。 檔案伺服器的主機名稱或 IP 位址。
 - Image Path (映像檔路徑)。 ISO 映像檔位置的完整路徑名稱。
3. 針對所有要當作虛擬媒體以供存取的媒體，選取其「Selected」(已選取)核取方塊。
 4. 按一下「Save」(儲存)。 此處所指定的所有媒體，這時都將會成為「Map Virtual Media CD/ISO Image」(對應虛擬媒體 CD/ISO 映像檔)對話方塊中的選項。

本章內容

裝置設定功能表	111
Network Settings (網路設定).....	112
裝置服務	116
鍵盤/滑鼠設定	118
序列連接埠設定	119
日期/時間設定	120
事件管理	121
連接埠組態	128

裝置設定功能表

「Device Settings」(裝置設定) 功能表的組織架構如下： 網路、裝置服務、鍵盤/滑鼠、序列連接埠、日期/時間、事件管理 - 設定、事件管理 - 目的地，以及連接埠組態。

使用：	執行：
Network (網路)	自訂 KX II-101 的網路組態。
Device Services (裝置服務)	設定 KX II-101 網路連接埠，以及啓用 TELNET 與 SSH 存取權。
Keyboard/Mouse (鍵盤/滑鼠)	設定目標伺服器如何看待 KX II-101 傳送的鍵盤與滑鼠訊號。
Serial Port (序列連接埠)	選取和設定 KX II-101 序列連接埠的功能。
Date/Time (日期/時間)	設定日期、時間、時區及網路時間通訊協定 (NTP)。
Event Management - Settings (事件管理 - 設定)	設定 SNMP 與 Syslog。
Event Management - Destinations (事件管理 - 目的地)	選取要追蹤的系統事件與此資訊傳送的目的地。
Port Configuration (連接埠組態)	設定 KVM 連接埠與插座。

Network Settings (網路設定)

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

基本上，有兩種方法可以設定 IP 組態：

- None (無)。(預設值) 此為建議選項 (靜態 IP)。因為 KX II-101 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。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)。隨即會開啓「Network Settings」(網路設定) 頁面。

Home > Device Settings > Network Settings

Network Basic Settings

Device Name *
DKX2-101

IP auto configuration
DHCP

Preferred host name (DHCP only)
[]

IP address
192.168.50.74

Subnet mask
255.255.255.0

Gateway IP address
192.168.50.126

Primary DNS server IP address
192.168.50.114

Secondary DNS server IP address
192.168.50.112

LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX2-101 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX2-101 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Current LAN interface parameters:
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex
Autodetect

Bandwidth Limit
No Limit

Set System ACL

OK Reset To Defaults Cancel

2. 更新「Network Basic Settings」(網路基本設定)。如需有關各欄位的詳細資訊，請參閱〈網路基本設定〉。
3. 更新「LAN Interface Settings」(LAN 介面設定)。如需有關各欄位的詳細資訊，請參閱〈LAN 介面設定〉。
4. 按一下「OK」(確定) 設定上述組態。變更如需重新開機裝置方能生效，即會出現重新開機的訊息。

- 若要取消而不儲存變更：
 - 按一下「Cancel」(取消)。

- 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

Network Basic Settings

Device Name *
DKX2-101

IP auto configuration
DHCP

Preferred host name (DHCP only)
[Empty text box]

IP address
192.168.59.99

Subnet mask
255.255.255.0

Gateway IP address
192.168.59.126

Primary DNS server IP address
192.168.59.2

Secondary DNS server IP address
192.168.51.10

OK Reset To Defaults Cancel

- Device Name (裝置名稱)。輸入不重複的裝置名稱 (最多 16 個字元，不得包含空格)。命名裝置以利識別。KX II-101 裝置的預設名稱為：“DKX2-101”。遠端使用者也會看到此名稱。但是，如果 MPC 使用者為此裝置建立了連線設定檔，則該使用者會在設定檔中看到「Description」(說明) 欄位。
- IP auto configuration (IP 自動組態)。選取下拉式清單中可用的選項：
 - None (無)。若不要自動 IP 組態，且偏好自行設定 IP 位址 (靜態 IP)，請使用此選項。此為預設及建議選項。

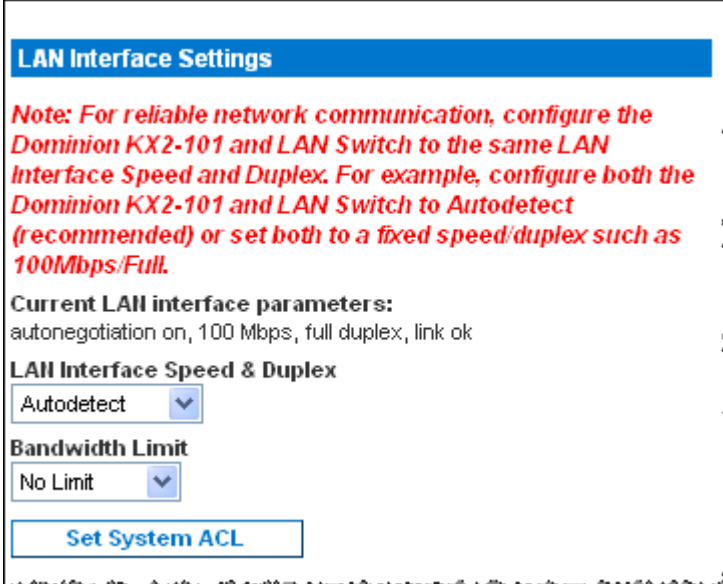
Network Settings (網路設定)

如果在「IP auto configuration」(IP 自動組態) 中選取此選項，即會啓用下列網路基本設定欄位，讓您手動設定 IP 組態。

- IP Address (IP 位址)。預設的 IP 位址為 192.168.0.192。
- Subnet Mask (子網路遮罩)。預設的子網路遮罩為 255.255.255.0。
- Gateway IP Address (閘道 IP 位址)。閘道的 IP 位址 (若使用的話)。
- Primary DNS Server IP Address (主要 DNS 伺服器 IP 位址)。用以將名稱轉譯為 IP 位址的主要網域名稱伺服器。
- Secondary DNS Server IP Address (次要 DNS 伺服器 IP 位址)。用以將名稱轉譯為 IP 位址的次要網域名稱伺服器 (若使用的話)。
- DHCP。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。

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。

LAN 介面設定



LAN Interface Settings

Note: For reliable network communication, configure the Dominion KX2-101 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX2-101 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full.

Current LAN interface parameters:
autonegotiation on, 100 Mbps, full duplex, link ok

LAN Interface Speed & Duplex
Autodetect

Bandwidth Limit
No Limit

[Set System ACL](#)

- Set System ACL (設定系統 ACL)。按一下此按鈕可為 KX II-101 設定全域層級的「存取控制清單」，確保裝置不會回應來傳自不允許之 IP 位址的封包。隨即會開啓「IP Access Control」(IP 存取控制) (請參閱 "IP 存取控制" p. 147) 頁面。

注意：這些是全域的 ACL 值，會影響整台 KX II-101 裝置。您也可根據群組層級建立 ACL。例如，您可建立「外包廠商」使用者群組，僅允許其從指定的 IP 位址範圍存取 KX II-101 (如需如何建立群組專屬「存取控制清單」的詳細資訊，請參閱〈分組的 IP ACL〉。

裝置服務

使用「Device Services」(裝置服務) 頁面，指定 KX II-101 的連線選項。

Home > Device Settings > Device Services

Services

Discovery Port *
5000

Enable TELNET Access

TELNET Port
23

Enable SSH Access

SSH Port
22

Enable Direct Port Access via URL

OK Reset To Defaults Cancel

- 若要設定探查連接埠：
 1. 選擇「Device Settings」(裝置設定) > 「Device Services」(裝置服務)。隨即會開啓「Device Services」(裝置服務) 頁面。
 2. 輸入 KX II-101 用以與用戶端電腦通訊的網路連接埠。
 3. 按一下「Save」(儲存) 以儲存設定。

➤ 若要啓用 TELNET 存取權：

1. 選擇「Device Settings」(裝置設定) > 「Device Services」(裝置服務)。隨即會開啓「Device Services」(裝置服務) 頁面。
2. 選取「Enable TELNET Access」(啓用 TELNET 存取權)。
3. 輸入可供 KX II-101 的 TELNET 存取權使用的網路連接埠。
4. 按一下「Save」(儲存) 以儲存設定。

➤ 若要啓用 SSH 存取權：

1. 選擇「Device Settings」(裝置設定) > 「Device Services」(裝置服務)。隨即會開啓「Device Services」(裝置服務) 頁面。
2. 選取「Enable SSH Access」(啓用 SSH 存取權)。
3. 輸入可供 KX II-101 的 SSH 存取權使用的網路連接埠。
4. 按一下「Save」(儲存) 以儲存設定。

啓用直接連接埠存取

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

➤ 若要啓用直接連接埠存取：

1. 選擇「Device Settings」(裝置設定) > 「Device Services」(裝置服務)。隨即會開啓「Device Services」(裝置服務) 頁面。
2. 選取「Enable Direct Port Access via URL」(透過 URL 啓用直接連接埠存取) 核取方塊。
3. 按一下「Save」(儲存) 以儲存設定。

➤ 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 的連接埠編號。如果您只有一個 KVM 連接埠，便不需要連接埠編號。

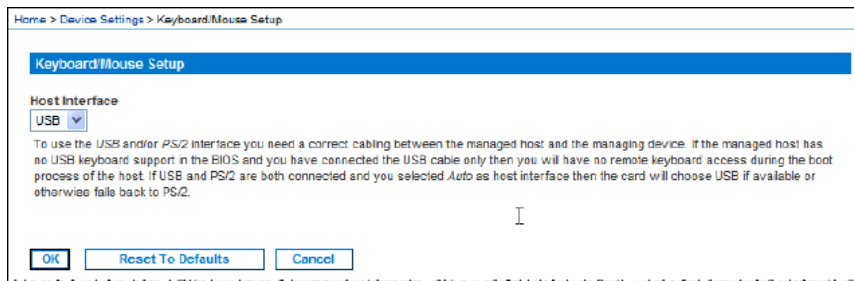
直接連接埠存取 URL 的格式如下：

```
https://[IP  
address]/dpa.asp?username=[username]&password=[password]&port=[port number]
```

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。

鍵盤/滑鼠設定

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



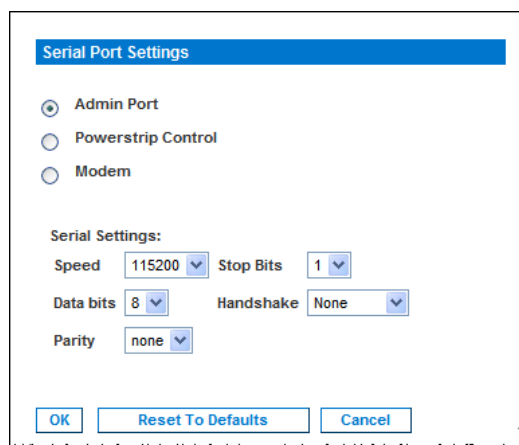
- Host Interface (主機介面)。選取 KX II-101 會透過 PS/2 或 USB 連線，傳送鍵盤與滑鼠資料。
 - Auto (自動)。使用此設定，如果有 USB 連線可用，KX II-101 會優先採用，沒有 USB 連線，則會恢復為使用 PS/2 連線。
 - USB。強制 KX II-101 使用 USB 連線，將鍵盤與滑鼠資料傳送給主機裝置。
 - PS/2。強制 KX II-101 使用 PS/2 連線，將鍵盤與滑鼠資料傳送給主機裝置。
- 若要重設出廠預設值：
 - 按一下「Reset to Defaults」(重設為預設值)。

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 如何使用其整合式序列連接埠。

➤ 若要設定序列連接埠：

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. 選擇想要使用的序列連接埠功能：
 - Admin 連接埠。選擇此選項，可從用戶端電腦直接連接 KX II-101，以存取進階組態。
 - PowerStrip Control (電源插座控制)。當 KX II-101 連接到序列控制的電源插座時，便可以選擇此選項。
 - Modem (數據機)。將外接數據機連接到 KX II-101 以提供撥號存取時，便可以選擇此選項。
3. 對於「Modem」(數據機) 選項，可以如下設定數據機使用設定：
 - a. 從「Serial line speed」(序列線路速度) 下拉式清單中，選取 KX II-101 與數據機之間的資料速度。
 - b. 輸入「Modem init string」(數據機初始字串)。
 - c. 輸入「Modem server IP address」(數據機伺服器 IP 位址)。上述即為在透過數據機連線之後，使用者輸入以存取 KX II-101 網頁介面的位址。
 - d. 輸入「Modem client IP address」(數據機用戶端 IP 位址)。上述即為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)。

日期/時間設定

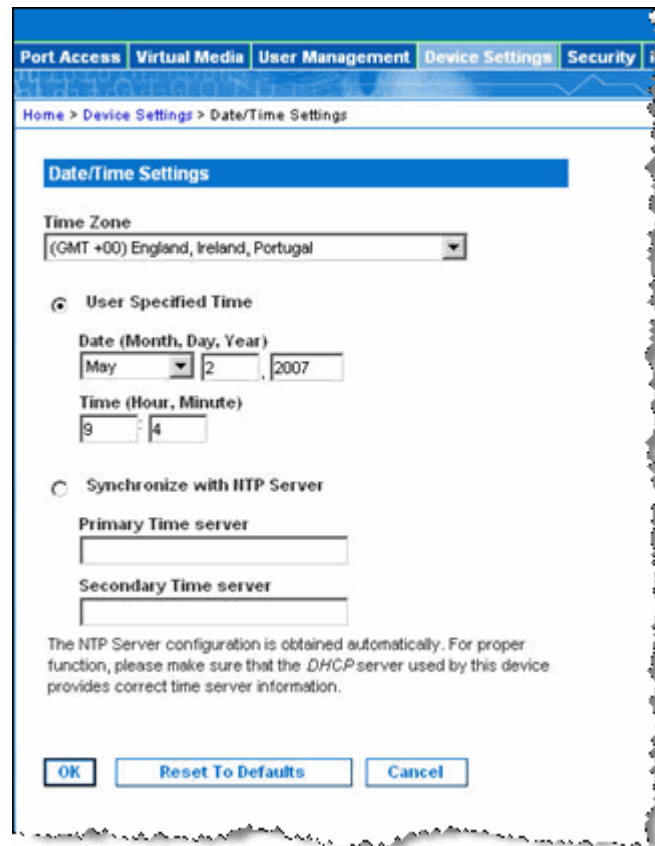
使用「Date/Time Settings」(日期/時間設定) 頁面可指定 KX II-101 的日期與時間。執行此作業的方法有兩種：

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

注意：KX II-101 不支援日光節約時間。

➤ 若要設定日期與時間：

1. 選擇「Device Settings」(裝置設定) > 「Date/Time」(日期/時間)。隨即會開啓「Date/Time Settings」(日期/時間設定) 頁面：



2. 從「Time Zone」(時區) 下拉式清單中選擇時區。
3. 選擇要用以設定日期與時間的方法：
 - User Specified Time (使用者指定的時間)。選擇此選項可手動輸入日期與時間。

- Synchronize with NTP Server (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。
4. 對於「User Specified Time」(使用者指定的時間) 選項，請輸入日期與時間如下：
 - a. 從下拉式清單中選擇「Month」(月份)。
 - b. 輸入該月份的「Day」(天)。
 - c. 以 yyyy 格式輸入「Year」(年份)。
 - d. 以 hh:mm 格式輸入「Time」(時間)(請使用 24 小時制)。
 5. 對於「Synchronize with NTP Server」(與 NTP 伺服器同步) 選項：
 - a. 輸入「Primary Time server」(主要時間伺服器) 的 IP 位址。
 - b. (選用) 輸入「Secondary Time server」(次要時間伺服器) 的 IP 位址。
 6. 按一下「OK」(確定)。

事件管理

KX II-101 的事件管理功能提供一組畫面，讓您啓用與停用將系統事件散佈到 SNMP 管理員、Syslog 以及稽核記錄的功能。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。

SNMP 組態

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。 KX II-101 透過事件管理提供 SNMP 代理支援。 如需 SNMP 代理與設限的詳細資訊，請參閱〈SNMP 代理組態〉 (請參閱 "SNMP 代理組態" p. 126)與〈SNMP 設限組態〉 (請參閱 "SNMP 設限組態" p. 126)。

➤ 若要設定 SNMP (啓用 SNMP 記錄)：

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

Home > Device Settings > Event Management - Settings

SNMP Configuration

SNMP Logging Enabled

Name
sai-Dlx2101

Contact
SAI

Location
FSD

Agent Community String

Type
Read-Write

Destination IP	Port #	Community
192.168.51.150	162	public
	162	public
	162	public
	162	public
	162	public

[Click here to view the Dominion KX2-101 SNMP MIB](#)

SysLog Configuration

Enable Syslog Forwarding

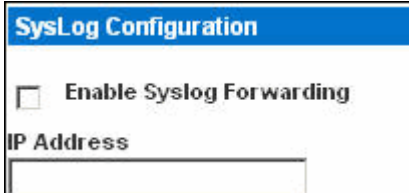
IP Address

OK **Reset To Defaults** **Cancel**

2. 選取「Enable SNMP Logging」(啓用 SNMP 記錄) 選項，這會啓用其餘的 SNMP 欄位。
3. 在「Name」(名稱)、 「Contact」(聯絡人) 及「Location」(位置) 欄位中，分別輸入 SNMP 代理 (屬於此 Dominion 裝置) 出現在 KX II-101 主控台界面的名稱、與此裝置相關的聯絡人姓名，以及 Dominion 裝置實際所在位置。

4. 輸入「Agent Community String」(代理社群字串) (Dominion 裝置的字串)。SNMP 社群是執行 SNMP 裝置及管理站隸屬之群組，有助於定義資訊傳送之目的位置。社群名稱用以識別群組，SNMP 裝置或代理可能同時屬於多個 SNMP 社群。
5. 請使用「Type」(類型) 下拉式清單，將社群組指定為「Read-Only」(唯讀) 或「Read-Write」(讀寫)。
6. 指定其「Destination IP」(目的地 IP)、「Port #」(連接埠編號) 以及「Community」(社群)，最多可設定五個 SNMP 管理員。
7. 按一下「Click here to view the KX II-101 SNMP MIB」(按此處檢視 KX II-101 SNMP MIB) 連結以存取「SNMP Management Information Base」(SNMP 管理資訊庫)。
8. 按一下「OK」(確定)。

Syslog 組態



- 若要設定 Syslog (啟用 Syslog 轉寄功能)：
 1. 選擇「Enable Syslog Forwarding」(啟用 Syslog 轉寄功能) 選項，將裝置訊息記錄在遠端的 Syslog 伺服器中。
 2. 在「IP Address」(IP 位址) 欄位中輸入 Syslog 伺服器的 IP 位址。
 3. 按一下「OK」(確定)。
- 若要取消而不儲存變更：
 - 按一下「Cancel」(取消)。
- 若要重設出廠預設值：
 - 按一下「Reset To Defaults」(重設為預設值) 按鈕。

事件管理 - 目的地

系統事件若已啓用，會產生 SNMP 通知事件 (設限) 或記錄到 Syslog 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。

注意：只有選取「SNMP Logging Enabled」(SNMP 記錄已啓用) 選項才會產生 SNMP 設限 (SNMP trap)；只有選取「Enable Syslog Forwarding」(啓用 Syslog 轉寄功能) 選項才會產生 Syslog 事件。這兩個選項都位在「Event Management - Settings」(事件管理 - 設定) 頁面。請參閱<事件管理 - 設定>。

➤ 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)。隨即會開啓「Event Management - Destinations」(事件管理 - 目的地) 頁面：

Home > Device Settings > Event Management - Destinations

Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Similarly, Syslog events will only be generated if the "Syslog Forwarding" option is checked. These options can be found on the "Event Management - Settings" page on the Device Settings page.

Category	Event	SNMP	Syslog
Device Operation	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware File Discarded	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Validation Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Backed Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Restored	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Port Connection Denied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Security	Password Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Login Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity	Port Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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. 選取要啓用或停用之「Event」(事件) 明細項目的核取方塊，以及傳送資訊的位置。

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

3. 按一下「OK」(確定)。
 - 若要取消而不儲存變更：
 - 按一下「Cancel」(取消)。
 - 若要重設出廠預設值：
 - 按一下「Reset To Defaults」(重設為預設值) 按鈕。

警告：透過 UDP 使用 SNMP 設限時，若 KX II-101 已重新開機，KX II-101 與其所連接的路由器可能會同步化失敗，而使得 SNMP 設限不會記錄「已完成重新開機」。

SNMP 代理組態

稱為代理的 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。使用「Event Logging」(事件記錄) 頁面，設定 KX II-101 (SNMP 代理) 與 SNMP 管理員之間的 SNMP 連線。

SNMP 設限組態

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

設限名稱	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 已透過 RFP 檔案完成更新。
deviceUpgradeStarted	KX II-101 已透過 RFP 檔案開始更新。
factoryReset	已將裝置重設為原廠預設值。
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 系統。
groupDeleted	已從系統刪除群組。
groupModified	已修改群組。
ipConflictDetected	偵測到 IP 位址衝突。

設限名稱	說明
ipConflictResolved	已解決 IP 位址衝突。
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。
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。
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。
portStatusChange	連接埠變為無法使用。
powerNotification	電源插座狀態通知： 1= 使用中，0= 非使用中。
powerOutletNotification	電源插座裝置的插座狀態通知。
rebootCompleted	KX II-101 已完成重新開機。
rebootStarted	KX II-101 已開始重新開機，其是透過對系統重新開啓電源，或是從作業系統重新暖開機。
securityViolation	安全性違規。
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	擁有使用中階段作業的使用者遇到異常階段作業終止情況。
userDeleted	使用者帳戶已刪除。
userLogin	使用者已成功登入 KX II-101 並經過驗證。
userLogout	使用者已成功正確登出 KX II-101。
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	擁有使用中階段作業的使用者因逾時而導致階段作業終止。
vmImageConnected	使用者嘗試在使用虛擬媒體的目標上掛載裝置或影像。每次嘗試對應 (裝載) 裝置/映像檔時都會產生此事件。

連接埠組態

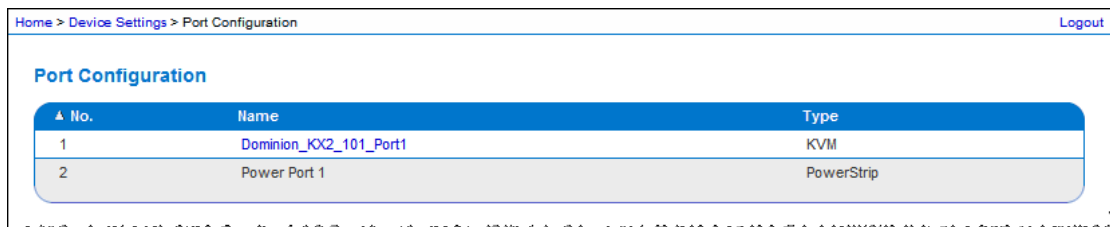
設限名稱	說明
vmImageDisconnected	使用者嘗試在使用虛擬媒體的目標上卸載裝置或映像檔。

連接埠組態

「Port Configuration」(連接埠組態) 頁面會顯示 KX II-101 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)。隨即會開啓「Port Configuration」(連接埠組態) 頁面：



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 Number (連接埠編號)。KX II-101 裝置的可用連接埠總數，從 1 起編號。
- 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。

注意：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)	PowerStrip (電源插座)
-------------------	-------------------

KVM	KVM 目標
-----	--------

2. 對要編輯的連接埠，按一下「Port Name」(連接埠名稱)。
 - 若為 KVM 連接埠，隨即會開啓「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，隨即會開啓電源插座的「Port」(連接埠)頁面。您可以在此頁面命名電源插座。命名其電源插座與插座。

注意：只有當 Raritan 電源插座已連接到 KX II-101 並完成設定時，「Power Port 1」(電源連接埠 1) 連結才會啓用。否則，該連結會處於停用。

本章內容

概覽	130
連接電源插座	131
命名電源插座裝置 (電源插座裝置的連接埠頁面)	132
建立 KVM 目標伺服器與插座的關聯 (連接埠頁面)	133
顯示插座關聯	137
控制電源插座裝置	138

 概覽

KX II-101 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* 電源控制功能：

1. 將電源插座連接到目標伺服器。
2. 命名電源插座。
3. 將電源插座裝置中的插座關聯到目標伺服器。
4. 在「*Powerstrip Device*」(電源插座裝置) (請參閱 "控制電源插座裝置" p. 138) 頁面上，開啓和關閉電源插座裝置上的插座電源。

連接電源插座



- 1 從 KX II-101 到 Raritan 電源插座裝置的 DKX2-101-SPDUC 接頭 (未隨附)。
- 2 Raritan 電源插座裝置。

➤ 若要將 KX II-101 連接到 Raritan 電源插座裝置：

1. 將 DKX2-101-SPDUC 纜線的 Mini DIM9M 接頭連接到 KX II-101 的 Admin(管理) 連接埠。
2. 將 DKX2-101-SPDUC 纜線的 RJ45M 接頭連接到 Raritan 電源插座裝置上的序列連接埠接頭。
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. 開啓 Raritan 電源插座裝置的電源。

命名電源插座裝置 (電源插座裝置的連接埠頁面)

當您從「Port Configuration」(連接埠組態) 頁面選取連接到 Raritan 遠端電源插座裝置的連接埠時，隨即會開啓此「Port」(連接埠) 頁面。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：插座的「Number」(編號)、「Name」(名稱) 及「Port Association」(連接埠關聯)。

使用本頁面命名電源插座裝置與其插座；所有名稱最多可有 32 個英數字元且可包含特殊字元。

Home > Device Settings > Port Configuration > Port

Port 1

Type:
KVM

Name:
Dominion_KX2_101_Port1

Power Association

Power Strip Name: None

Outlet Name: ---

Target Server Settings

- Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices
- Absolute mouse scaling for MAC server (applies only if USB is active Keyboard/Mouse Interface)
- USB SUN Keyboard support (applies only if USB is active Keyboard/Mouse Interface)

OK Cancel

注意：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）：

注意：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。（插座名稱預設為其插座編號。）
3. 按一下「OK」（確定）。

➤ 若要取消而不儲存變更：

- 按一下「Cancel」（取消）。

建立 KVM 目標伺服器與插座的關聯（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，隨即會開啓此「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）頁面開啓電源、關閉電源以及重新開啓伺服器電源，如下所示。



建立 KVM 目標伺服器與插座的關聯 (連接埠頁面)

注意：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。如需詳細資訊，請參閱<連接電源插座裝置> (請參閱“連接電源插座” p. 131)。

➤ 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)：

注意：當目標伺服器 (連接埠) 與電源插座裝置產生關聯時，便會以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。

有兩個插座關聯的電源插座裝置，如下所示。

The screenshot shows a web interface for configuring a port. The breadcrumb trail is "Home > Device Settings > Port Configuration > Port".

Port 1

Type: KVM

Name: Dominion_KX2_101_Port1

Power Association

Power Strip Name: Power Port 1

Outlet Name: Dominion_KX2_101_Port1(7), Dominion_KX2_101_Port1(8), None, None

Target Server Settings

- Use Full Speed - Useful for BIOS that cannot handle High Speed USB devices
- Absolute mouse scaling for MAC server (applies only if USB is active Keyboard/Mouse Interface)
- USB SUN Keyboard support (applies only if USB is active Keyboard/Mouse Interface)

Buttons: OK, Cancel

➤ 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。
2. 按一下「OK」(確定)。

建立 KVM 目標伺服器與插座的關聯 (連接埠頁面)

- 若要取消而不儲存變更：
 - 按一下「Cancel」(取消)。

- 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。

顯示插座關聯

- 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。

Home > Device Settings > Port Configuration > Port

Port 2

Type:
PowerStrip

Name:

Outlets

Number	Name	Port Association
1	<input type="text" value="Outlet 1"/>	
2	<input type="text" value="Outlet 2"/>	
3	<input type="text" value="Outlet 3"/>	
4	<input type="text" value="Outlet 4"/>	
5	<input type="text" value="Outlet 5"/>	
6	<input type="text" value="Outlet 6"/>	
7	<input type="text" value="Dominion_KX2_101_Port1"/>	Dominion_KX2_101_Port1
8	<input type="text" value="Dominion_KX2_101_Port1"/>	Dominion_KX2_101_Port1

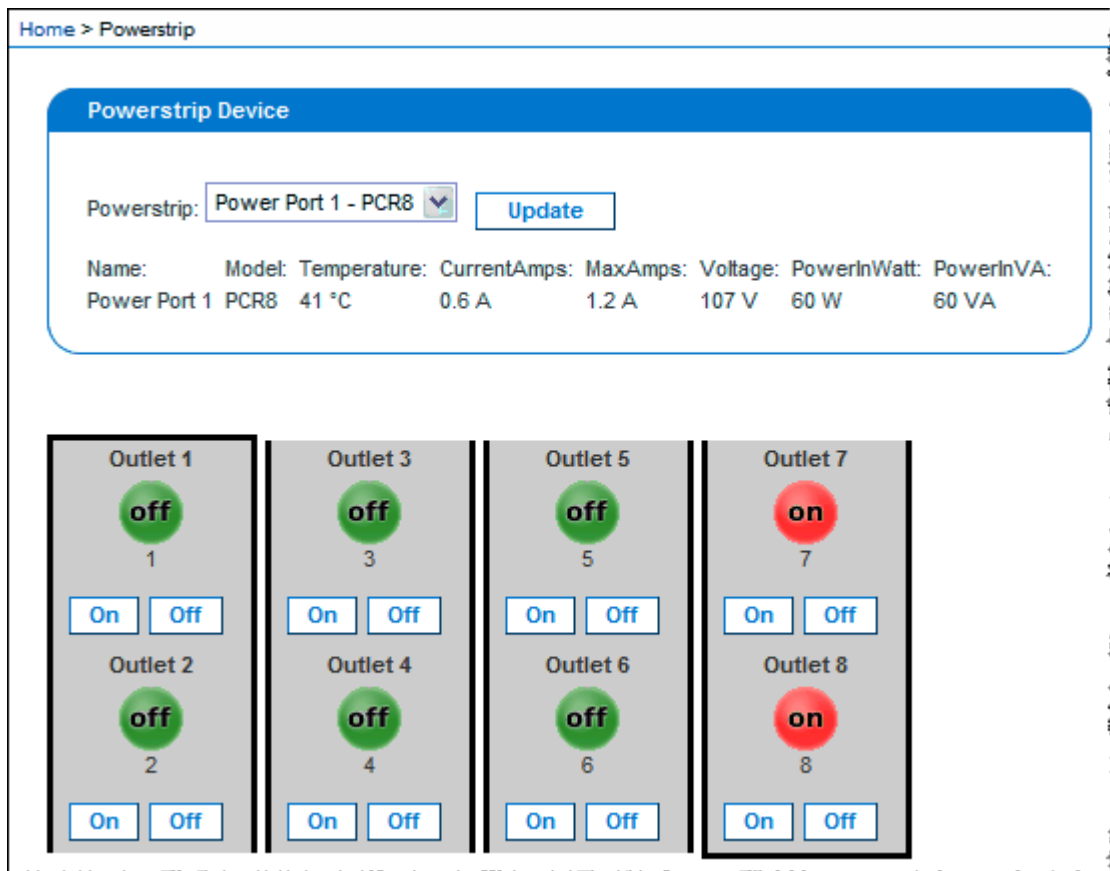
控制電源插座裝置

➤ 若要編輯電源連接埠組態：

- 透過編輯「Port 2」(連接埠 2) > 「Name」(名稱) 欄位，來變更電源連接埠名稱。
- 透過編輯關聯的「Outlets」(插座) > 「Name」(名稱) 欄位，來變更插座名稱。插座名稱會顯示在「Powerstrip Settings」(電源插座裝置) 頁面中。如需詳細資訊，請參閱 <控制電源插座裝置> (請參閱 "控制電源插座裝置" p. 138)。
- 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。如需詳細資訊，請參閱 <建立 KVM 目標伺服器與插座的關聯 (連接埠頁面)> (請參閱 "建立 KVM 目標伺服器與插座的關聯 (連接埠頁面)" p. 133)。

控制電源插座裝置

您可以使用「Powerstrip Settings」(電源插座裝置) 頁面，控制電源插座裝置。此頁面可讓您開啓和關閉電源插座裝置上的插座電源。



- 若要控制 *KX II-101* 所連接的電源插座裝置：
1. 選擇「Home」(首頁) > 「Powerstrip」(電源插座)。
隨即會開啓「Powerstrip 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，以開啓或關閉該插座。
 3. 當系統提示要求您確認選擇時，按一下「OK」(確定)。
隨即會開啓或關閉該電源插座的電源。

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

本章內容

安全性設定功能表	140
安全性設定	141
IP 存取控制	147

 安全性設定功能表

「Security」(安全性) 功能表的組織架構如下：安全性設定 與 IP 存取控制。

使用：	執行：
Security Settings (安全性設定)	設定登入限制、強固密碼、使用者封鎖以及加密與共用的安全性設定。
IP Access Control (IP 存取控制)	控制對 KX II-101 裝置的存取。設定全域存取控制清單，確保裝置不會回應傳自不允許之 IP 位址的封包。

安全性設定

在「Security Settings」(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。

Raritan SSL 認證是用於進行公開金鑰與私密金鑰的交換，並提供其他層級的安全性。Raritan 網頁伺服器認證是自行簽署的，而 Java Applet 憑證則是由 VeriSign 認證所簽署。加密可保證資料免遭竊聽的安全，而這些認證則確保可信任此實體為 Raritan, Inc.。

➤ 若要設定安全性設定：

1. 選擇「Security」(安全性) > 「Security Settings」(安全性設定)。隨即會開啓「Security Settings」(安全性設定) 頁面。

The screenshot shows the 'Security Settings' configuration page with the following details:

- Login limitations:**
 - Enable Single Login Limitation
 - Enable Password Aging
 - Password Aging Interval (days):
 - Log Out Idle Users
 - After (minutes):
- User Blocking:**
 - Disabled
 - Timer Lockout
 - Attempts:
 - Lockout Time:
 - Deactivate User-ID
 - Failed Attempts:
- Strong passwords:**
 - Enable strong passwords
 - Minimum length of strong password:
 - Maximum length of strong password:
 - Enforce at least one lower case character
 - Enforce at least one upper case character
 - Enforce at least one numeric character
 - Enforce at least one printable special character
 - Number of restricted passwords based on history:
- Encryption & Share:**
 - Encryption Mode:
 - Apply Encryption Mode to KVM and Virtual Media
 - PC Share Mode:
 - VM Share Mode
 - Disable Local Port Output
 - Local Device Reset Mode:

Buttons at the bottom:

欄位會分類為下列群組：Login Limitations (登入限制)、Strong Passwords (強固密碼)、User Blocking (使用者封鎖) 及 Encryption & Share (加密與共用)。

2. 適當更新「Login Limitations」(登入限制) (請參閱 "登入限制" p. 142) 設定。

3. 適當更新「**Strong Passwords**」(強固密碼) (請參閱 "強固密碼" p. 143) 設定。
 4. 適當更新「**User Blocking**」(使用者封鎖) (請參閱 "使用者封鎖" p. 144) 設定。
 5. 適當更新「**Encryption & Share**」(加密與共用)設定。
 6. 按一下「OK」(確定)。
- 若要關閉頁面而不儲存任何變更：
 - 按一下「Cancel」(取消)。
 - 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 (啓用單次登入限制)。	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。
Enable Password Aging (啓用密碼使用期限)。	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。 Password Aging Interval (days) (密碼使用期限間隔 (天))。選取「 Enable Password Aging 」(啓用密碼使用期限) 核取方塊時，即會啓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。
Log Out Idle Users (登出閒置的使用者)。	選取此核取方塊，會在經過特定的非使用中時間後，自動中斷使用者階段作業的連線。在「 After 」(之後) 欄位中鍵入時間量。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。 After (minutes) (之後 (分鐘))。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) 選項時即會啓用此欄位。

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，您可以指定準則以定義有效的 KX II-101 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。

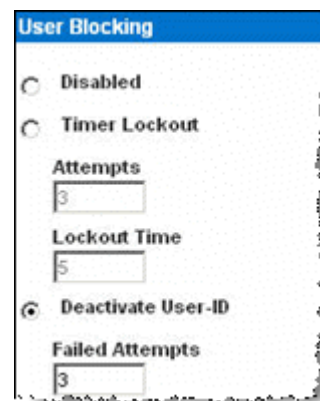
- **Enable strong passwords (啓用強固密碼)**。強固密碼會要求使用者建立的密碼長度下限為 8 個字元，包含至少一個字母字元及一個非字母字元 (標點符號字元或數字)。此外，密碼前四個字元不得與使用者名稱相同。
選取此選項時，即會執行強固密碼規則。密碼不符強固密碼準則的使用者於下次登入時，系統會自動要求變更密碼。取消選取此選項時，僅會執行標準格式的驗證。選取此選項時，即會啓用下列欄位且為必要欄位：
 - **Minimum length of strong password (強固密碼的長度下限)**。密碼長度至少為 8 個字元。預設值為 8 個，但最多可有 63 個。
 - **Maximum length of strong password (強固密碼的長度上限)**。預設值為 16，但最多可至 64 個字元長。
 - **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，由之前密碼不得重複的位數。範圍為 1-12，預設值為 5。

使用者封鎖

「User Blocking」(使用者封鎖) 選項指定的準則，規定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：

- Disabled (停用)。預設選項，無論驗證失敗幾次，都不會封鎖使用者。
- Timer Lockout (計時器鎖定)。超過指定的失敗登入嘗試次數之後，拒絕使用者存取系統的指定時間量。選取此選項時，即會啓用下列欄位：
 - Attempts (嘗試次數)。失敗登入嘗試次數，在此次數之後即封鎖該使用者。有效範圍為 1 - 10，預設值為 3 次。
 - Lockout Time (鎖定時間)。封鎖使用者的時間量。有效範圍為 1 - 1440 分鐘，預設值為 5 分鐘。
- Deactivate User-ID (停用使用者 ID)。選取此項目時，選項會指定達到「Failed Attempts」(失敗次數) 欄位中指定的失敗登入嘗試次數之後，便封鎖該使用者：
 - Failed Attempts (失敗次數)。失敗登入嘗試次數，在此次數之後即停用使用者 ID。選取「Deactivate User-ID」(停用使用者 ID) 選項時即會啓用此欄位。有效範圍為 1 - 10。



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「User」(使用者) (請參閱 "新增使用者" p. 48) 頁面選取「Active」(使用中) 核取方塊，來變更使用者密碼和啓動使用者帳戶。

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 重設按鈕時所執行的重設類型。

Encryption & Share

Encryption Mode
 Auto

Apply Encryption Mode to KVM and Virtual Media

PC Share Mode
 PC-Share

VM Share Mode
 Disable Local Port Output

Local Device Reset Mode
 Enable Local Factory Reset

- Encryption Mode (加密模式)。從下拉式清單中選擇其中一個選項。選取加密模式時，若瀏覽器不支援所選取的模式便會顯示警告，同時也無法連線至 KX II-101：

Encryption & Share

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 Dominion KX2-101.

Encryption Mode
 RC4

Apply Encryption Mode to KVM and Virtual Media

PC Share Mode
 Private

VM Share Mode
 Disable Local Port Output

Local Device Reset Mode
 Enable Local Factory Reset

- Auto (自動)。此為建議選項，KX II-101 會自動交涉可能的最高級加密方法。

- 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 裝置及遠端電腦之間的私人通訊通道。
- 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 **<檢查瀏覽器是否支援 AES 加密功能>** (請參閱 "檢查瀏覽器是否支援 AES 加密功能" p. 147)。
- 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 **<檢查瀏覽器是否支援 AES 加密功能>** (請參閱 "檢查瀏覽器是否支援 AES 加密功能" p. 147)。
- 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。
- 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，並可同時檢視與控制相同的目標伺服器。按下拉式清單以選取下列其中一個選項：
 - Private (獨占)：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，若某位使用者不停鍵入或移動滑鼠，則會發生控制不平衡的狀況。
- VM Share Mode (VM 共用模式)。唯有啓用「PC-Share Mode」(電腦共用模式) 時才會啓用此選項。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。
- Local Device Reset Mode (本機裝置重設模式)。此選項會指定按下硬體重設按鈕 (位於裝置背面) 時所執行的動作。如需詳細資訊，請參閱 **<重設按鈕>**。選取下列任一選項：
 - Enable Local Factory Reset (啓用本機出廠重設，預設值)。將 KX II-101 裝置回復到出廠預設值。
 - Enable Local Admin Password Reset (啓用本機管理員密碼重設)。僅重設本機管理員密碼。密碼會重設為 raritan。

- Disable All Local Resets (停用所有本機重設)。不執行任何重設動作。

檢查瀏覽器是否支援 AES 加密功能

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下列網站：

<https://www.fortify.net/sslcheck.html>。此網站可偵測瀏覽器的加密方法，並顯示偵測結果的報表。

注意：IE6 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 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

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：

- JRE1.4.2 - <http://java.sun.com/j2se/1.4.2/download.html>
- JRE1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

IP 存取控制

使用「IP Access Control」(IP 存取控制) 可控制對 KX II-101 裝置的存取。設定全域存取控制清單 (ACL)，確保裝置不會回應傳自不允許之 IP 位址的封包。「IP Access Control」(IP 存取控制) 是全域選項，可影響整台 KX II-101 裝置，但也可以在群組層級控制對裝置的存取。如需有關群組層級控制的詳細資訊，請參閱分組的 <IP 存取控制>。

重要：KX II-101 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 本機連接埠。

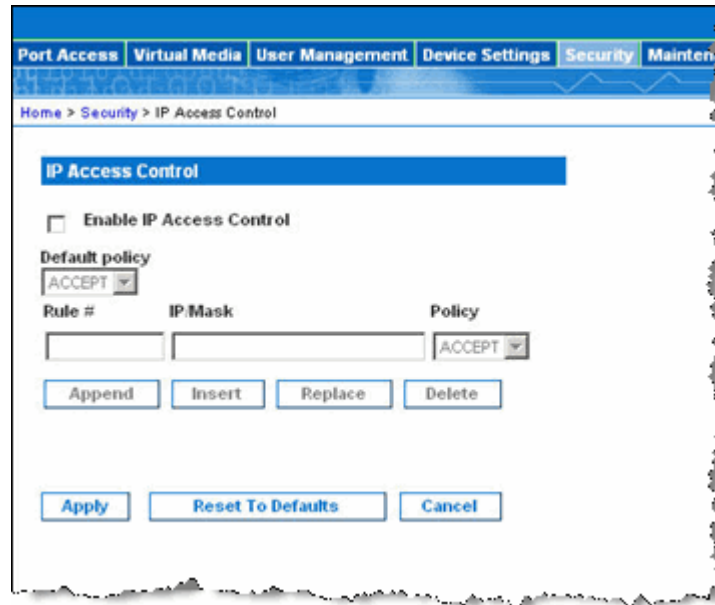
➤ 若要使用 IP 存取控制：

1. 請使用下列方法之一開啓「IP Access Control」(IP 存取控制) 頁面：
 - 選取「Security」(安全性) > 「IP Access Control」(IP 存取控制)，或

IP 存取控制

- 按一下「Network Settings」(網路設定) 頁面的「Set System ACL」(設定系統 ACL) 按鈕。

隨即會開啓「IP Access Control」(IP 存取控制) 頁面。



2. 選取「Enable IP Access Control」(啓用 IP 存取控制) 核取方塊，可啓用 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 裝置的 IP 位址。
 - Drop (捨棄)。拒絕其存取 KX II-101 裝置的 IP 位址。
- 若要新增 (附加) 規則：
1. 在「IP/Mask」(IP/遮罩) 欄位中，輸入 IP 位址與子網路遮罩。
 2. 從下拉式清單中選擇「Policy」(原則)。
 3. 按一下「Append」(附加)。將規則加入為規則清單的最後一筆記錄。
 4. 請為每個要輸入的規則重複步驟 1 到 3。
- 若要插入規則：
1. 輸入「Rule #」(規則編號)。使用「Insert」(插入) 指令時必須要有規則編號。
 2. 在「IP/Mask」(IP/遮罩) 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「Rule #」(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「Rule #」(規則編號)。
2. 在「IP/Mask」(IP/遮罩) 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)。新規則會取代具有相同規則編號的原始規則。

➤ 若要刪除規則：

1. 指定要刪除的「Rule #」(規則編號)。
2. 按一下「Delete」(刪除)。
3. 隨即會出現提示要求您確認刪除。按一下「OK」(確定)。

祕訣：規則編號可讓您對規則的建立順序擁有較多的控制。

本章內容

維護功能表	150
稽核記錄	151
裝置資訊	152
備份與還原	153
韌體升級	155
升級歷程記錄	156
重新開機	157

維護功能表

「Maintenance」(維護) 功能表包含下列選項：「Audit Log」(稽核記錄)、
「Device Information」(裝置資訊)、「Backup/Restore」(備份/還原)、
「Firmware Upgrade」(韌體升級)、「Factory Reset」(出廠重設)、
「Upgrade History」(升級歷程記錄) 以及「Reboot」(重新開機)。

稽核記錄

因 KX II-101 系統事件所建立的記錄。

➤ 若要檢視 KX II-101 裝置的稽核記錄：

1. 選擇「Maintenance」(維護) > 「Audit Log」(稽核記錄)。隨即會開啓「Audit Log」(稽核記錄) 頁面：

Home > Maintenance > Audit Log Logout

Audit Log

[Older]

Date	Event	Description
11/13/2007 12:51:53	Access Logout	User 'admin' from host '192.168.61.209' logged out.
11/13/2007 12:28:01	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'available'.
11/13/2007 12:28:01	Port Disconnected	Port 'Dominion_KX2_101_Port5' disconnected by user 'admin'.
11/13/2007 12:27:56	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'connected'.
11/13/2007 12:27:56	Port Connected	Port 'Dominion_KX2_101_Port5' connected by user 'admin'.
11/13/2007 11:39:00	Access Login	User 'admin' from host '192.168.61.209' logged in.
11/13/2007 10:55:30	Access Login	User 'admin' from host '192.168.50.54' logged in.
11/13/2007 10:55:15	Login Failed	Authentication failed for user 'admin' from host '192.168.50.54'.
11/12/2007 17:53:55	Access Logout	User 'admin' from host '192.168.32.40' logged out.
11/12/2007 17:53:28	Access Login	User 'admin' from host '192.168.32.40' logged in.
11/12/2007 17:53:13	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:53:13	End CC Control	CC management stopped by user 'CC admin' from host '192.168.59.246'.
11/12/2007 17:50:19	Access Logout	User 'CC user session' from host '192.168.59.246' logged out.
11/12/2007 17:48:21	Access Login	User 'CC user session' from host '192.168.59.246' logged in.
11/12/2007 17:48:16	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:15	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:14	Access Login	User 'CC admin' from host '192.168.59.246' logged in.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.
11/12/2007 17:48:08	Begin CC Control	CC management started by user 'admin' from host '192.168.59.246'.
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.

[Save To File](#)

裝置資訊

「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：

注意：僅「KX II-101 遠端主控台」提供稽核記錄儲存功能，「本機主控台」則否。

1. 按一下「Save to File」(另存檔案) 按鈕。隨即會開啓「Save File」(儲存檔案) 對話方塊。
2. 選取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。

➤ 若要翻閱稽核記錄：

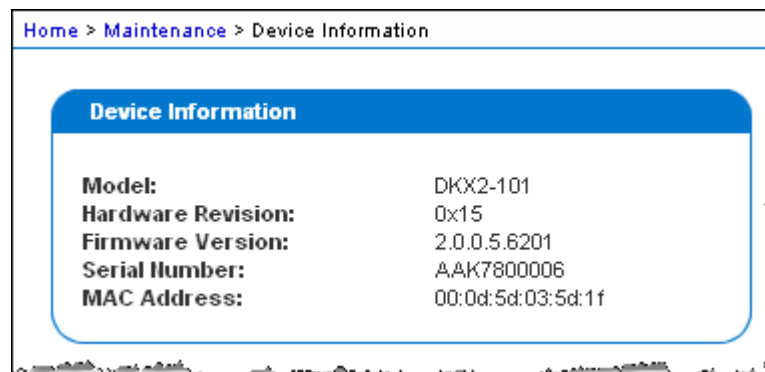
- 使用 [Older] (較早) 與 [Newer] (較新) 連結。

裝置資訊

「Device Information」(裝置資訊) 頁面提供有關 KX II-101 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 的相關資訊：

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

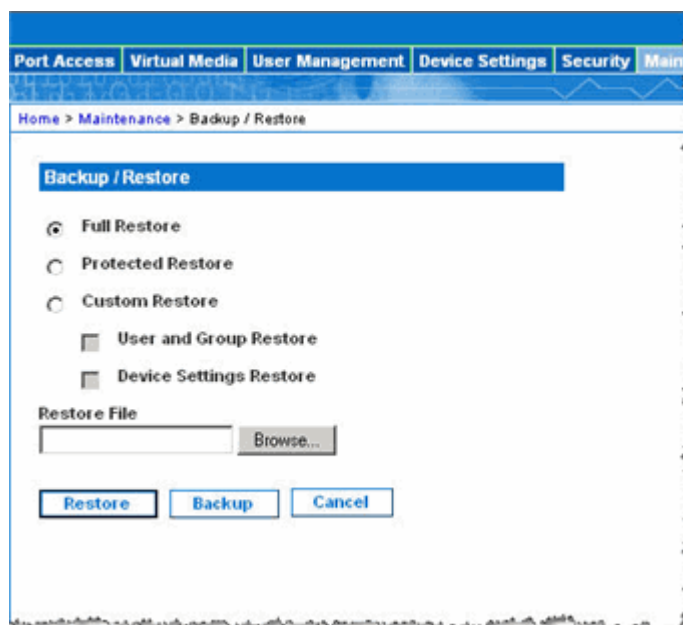


下列提供 KX II-101 的相關資訊：「Model」(機型)、「Hardware Revision」(硬體修訂版)、「Firmware Version」(韌體版本)、「Serial Number」(序號) 以及「MAC Address」(MAC 位址)。

備份與還原

您可從「Backup/Restore」(備份/還原) 頁面，備份與還原 KX II-101 的設定與組態。備份與還原除了可運用在商業運作的延續上，還可使用此功能作為節省時間的機制。例如，您可以從使用中的 KX II-101 備份使用者的各項設定，再將這些組態還原至新的 KX II-101 上，而從其他 KX II-101 對小組快速提供存取。您也可以設定一台 KX II-101，再將其組態複製到多台 KX II-101 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)。隨即會開啓「Backup/Restore」(備份/還原) 頁面。



注意：備份一律為完整的系統備份。還原則可根據您的選擇進行完整或部分執行。

- 若要備份 KX II-101：
 1. 按一下「Backup」(備份)。隨即會出現「File Download」(下載檔案) 對話方塊。
 2. 按一下「Save」(儲存)。就會出現「Save As」(另存新檔) 對話方塊。

3. 選擇位置、指定檔案名稱，然後按一下「Save」(儲存)。隨即會出現「Download Complete」(下載完成) 對話方塊。
4. 按一下「Close」(關閉)。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。

➤ 若要還原 KX II-101：

警告：將 KX II-101 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 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上。
 - Protected Restore (保護還原)。還原各項設定，但除裝置特有資訊以外，例如序號、MAC 位址、IP 位址、名稱等等。使用此選項，您可以設定一台 KX II-101，再將其組態複製到多台 KX II-101 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。選取適當的核取方塊：
 - 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。使用此選項可讓您快速設定不同 KX II-101 的使用者。
 - Device Settings Restore (裝置設定還原)。此選項僅包含裝置設定。使用此選項可快速複製裝置資訊。
2. 按一下「Browse」(瀏覽) 按鈕。隨即會開啓「Choose file」(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「Open」(開啓)。選取的檔案會列在「Restore File」(還原檔案) 欄位中。
4. 按一下「Restore」(還原)。隨即會還原配置 (以選取的還原類型為準)。

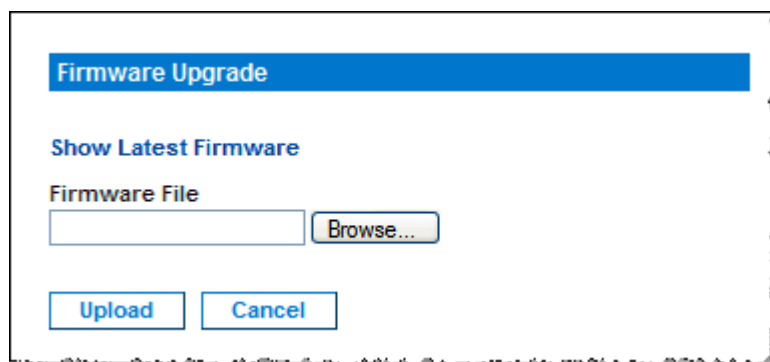
韌體升級

使用「Firmware Upgrade」(韌體升級) 頁面，以升級 KX II-101 裝置的韌體。此頁面僅供「KX II-101 遠端主控台」使用。

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

➤ 若要升級 KX II-101 裝置：

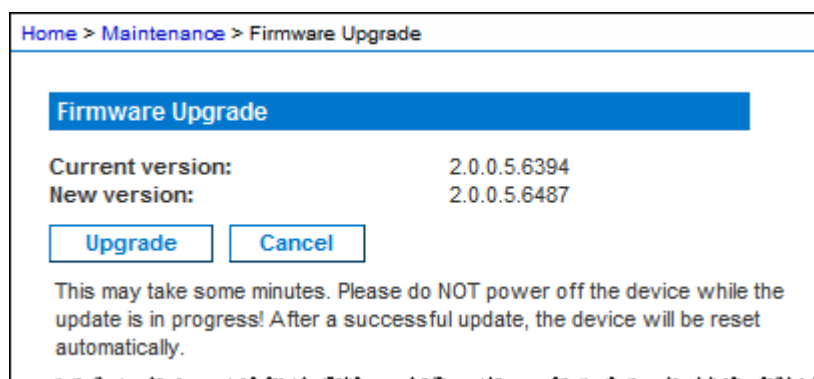
1. 選取「Maintenance」(維護) > 「Firmware Upgrade」(韌體升級)。隨即會開啓「Firmware Upgrade」(韌體升級) 頁面：



2. 在「Firmware Upgrade」(韌體升級) > KX II-101 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。

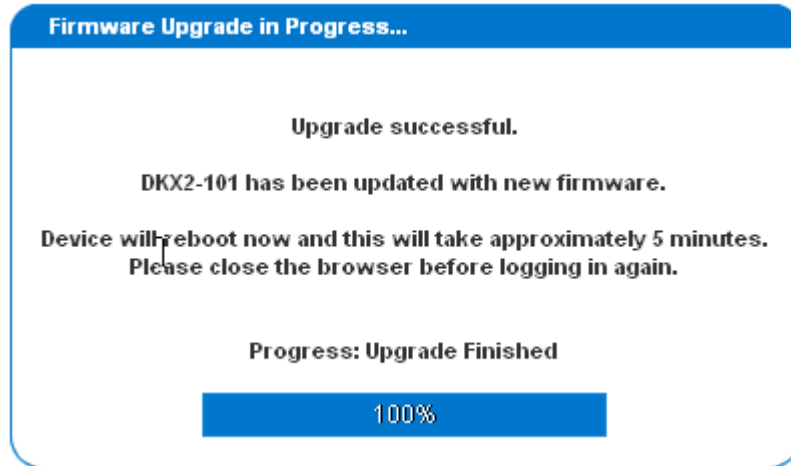
注意：請先將韌體更新檔複製到本機電腦上，再進行上傳。請勿從網路磁碟機載入檔案。按一下「Browse」(瀏覽) 按鈕，瀏覽解壓縮升級檔案所在的目錄。

4. 按一下「Firmware Upgrade」(韌體升級) 頁面的「Upload」(上傳)。顯示有關升級與版本號碼的資訊，供您確認之用：



注意：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。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《Raritan 多平台用戶端 (MPC) 使用指南》。

升級歷程記錄

KX II-101 提供在 KX II-101 裝置與附掛的 CIM 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)。隨即會開啓「Upgrade History」(升級歷程記錄) 頁面：

Home > Upgrade History Logout

Upgrade History

Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	Result
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:30	January 09, 2000 20:32	2.0.0.5.6236	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:18	January 09, 2000 20:20	2.0.0.5.6191	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.65	January 06, 2000 17:58	January 06, 2000 18:01	2.0.0.1.6126	2.0.0.5.6191	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 2000 00:02	January 01, 2000 00:04	99.99.99.2.9999	2.0.0.1.6126	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 1970 00:06	January 01, 1970 00:09	2.0.0.1.5974	99.99.99.2.9999	Successful
Full Firmware Upgrade						2.0.0.1.5974	Failed

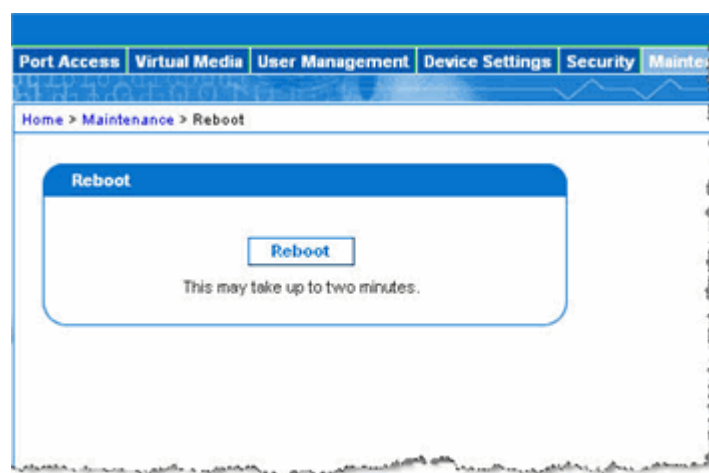
重新開機

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

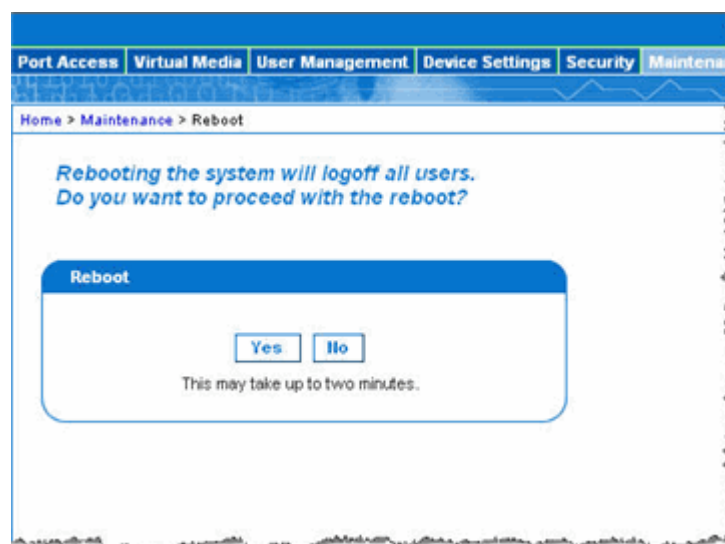
重要：系統會關閉所有 KVM 與序列連線，並登出所有使用者。

➤ 若要將 KX II-101 重新開機：

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



2. 按一下「Reboot」(重新開機) 按鈕。隨即會出現提示要求您確認動作：



3. 按一下「Yes」(是) 繼續重新開機作業。

重新開機

- 若要結束但不重新開機：
 - 按一下「No」(否)。

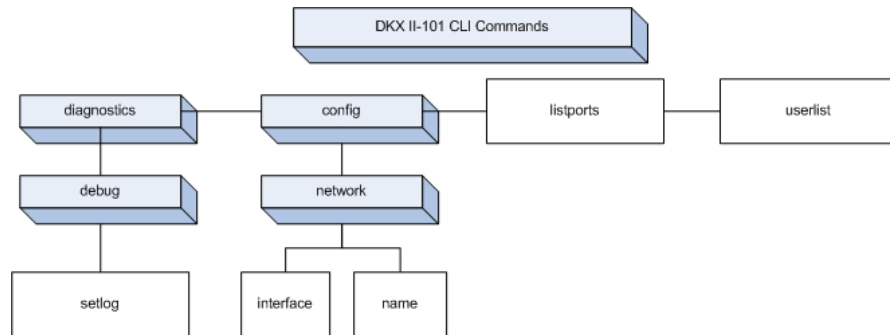
本章內容

概覽	159
使用 CLI 存取 KX II-101	160
KX II-101 的 SSH 連線	160
登入	161
瀏覽 CLI	161
CLI 指令	163

概覽

本章提供可與 KX II-101 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. 163)。

下圖提供 CLI 指令概覽：



注意：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

使用下列任一種方法來存取 KX II-101：

- 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多種可用的 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.netbeans.org/ssh
<http://www.netbeans.org/ssh>
- OpenSSH 用戶端 - www.openssh.org <http://www.openssh.org>

注意：透過 SSH 或 TELNET 存取 CLI，需要在 KX II-101 遠端用戶端的「Device Services」(裝置服務) 頁面中設定存取權。如需詳細資訊，請參閱〈裝置服務〉(請參閱 "裝置服務" p. 116)。

KX II-101 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。如需詳細資訊，請參閱〈裝置服務〉(請參閱 "裝置服務" p. 116)。

注意：基於安全性考量，KX II-101 不支援 SSH V1 連線。

Windows 電腦的 SSH 存取方法

➤ 若要從 Windows 電腦開啓 SSH 階段作業：

1. 啓動 SSH 用戶端軟體，例如 PuTTY。
2. 輸入 KX II-101 伺服器的 IP 位址 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」(開啓) 按鈕。
5. 隨即出現下列提示：
login as:

如需登入資訊，請參閱〈登入〉一節。

UNIX 工作站的 SSH 存取方法

- 若要從 UNIX/Linux 工作站開啓 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
```

然後便會出現「密碼」提示：

如需登入資訊，請參閱〈登入〉一節。

登入

- 若要登入，請輸入使用者名稱 *admin*，如下所示：

Login: admin

隨即會出現密碼提示：變更預設的密碼：raritan

Password:

隨即會顯示歡迎訊息。現在您已經以管理員的身分登入。

```

Login: admin
Passuord:
-----
Device Type: Dominion KX2-101      Model: DKX2-101
Device Name: DKX2-101-DOC         FW Version: 2.0.0.5.6394      SN: AAK7800010
IP Address: 192.168.50.153        Idle Timeout: 30min
-----
Port No.  Name                               Port Type  Status  Availability
1 - Dominion_KXII-101_Port  KVM up    idle
Current Time: Wed Dec 26 14:37:00 2007
Admin Port > _

```

在檢閱下面的〈[瀏覽 CLI](#)〉（請參閱 "瀏覽 CLI" p. 161）一節之後，您便可以如〈[使用管理序列主控台](#)〉（請參閱 "使用終端機模擬程式" p. 26）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。此外，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 Port > Config > Network >
```

對於 TELNET/SSH，指令的根目錄部份則是 admin：

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

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。
- 如果找到多個可能的相符項目，CLI 也會有效的項目。
- 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。
- 垂直線 (|) 代表其中的選項為選用，或需要設定關鍵字或引數。

快速鍵

- 按向上箭頭，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，使用 Ctrl/C，可終止指令或取消指令。
- 使用 Enter 鍵，可執行指令。
- 按下 Tab，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 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。
<i>diagnostics</i> (請參閱 "診斷" p. 164)	切換到「Diagnostics」(診斷) 功能表。
<i>debug</i> (請參閱 "除錯" p. 164)	切換到「Debug」(除錯) 功能表。
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 網路介面。
<i>listports</i> (請參閱 "Listports 指令" p. 167)	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。
logout	登出目前的 CLI 階段作業。
<i>name</i> (請參閱 "Name 指令" p. 166)	設定裝置名稱。
<i>network</i> (請參閱 "網路" p. 165)	顯示網路組態以及讓您設定網路設定。
quit	返回前一個指令。

<i>setlog</i> (請參閱 "Setlog 指令" p. 164)	設定裝置記錄選項。
<i>top</i>	切換到根目錄功能表。
<i>userlist</i> (請參閱 "Userlist 指令" p. 167)	列出使用中的使用者數目、使用者名稱、連接埠以及狀態。

診斷

「Diagnostics」(診斷) 功能表可讓您為不同的 KX II-101 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 的記錄選項。

Setlog 指令

Setlog 指令可讓您對不同的 KX II-101 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。

指令選項	說明
level	診斷層級： err warn info debug trace
vflag	詳細資訊旗標的類型： timestamp module thread fileline
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 網路介面與裝置名稱。

指令	說明
interface	設定 KX II-101 裝置網路介面。
name	設定裝置名稱。

Name 指令

name 指令是用來設定裝置與主機名稱。

裝置名稱的語法如下：

```
name devicename<>
```

主機名稱的語法如下：

```
name hostname<>
```

name 指令範例

下列指令設定了裝置名稱：

```
Admin Port > Config > Network > name devicename <device name>
```

下列指令設定了主機名稱：

```
Admin Port > Config > Network > name hostname <host name>
```

Interface 指令

interface 指令是用來設定 KX II-101 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。如需詳細資訊，請參閱 [〈安裝與組態〉](#) (請參閱 "安裝與組態" p. 7)。

interface 指令的語法如下：

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

interface 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 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 100Mbps 全雙工 (100fdx)

Interface 指令範例

下列指令設定了 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
```

Listports 指令

Listports 指令 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_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

```
-----
--
```

```
admin      | Admin Port | active
```

本章內容

診斷功能表	168
網路介面頁面	169
網路統計資料頁面	169
偵測 (Ping) 主機頁面	172
追蹤主機路由頁面	173
裝置診斷	174

診斷功能表

「Diagnostics」(診斷) 頁面是用於疑難排解，主要供 KX II-101 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)，所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。

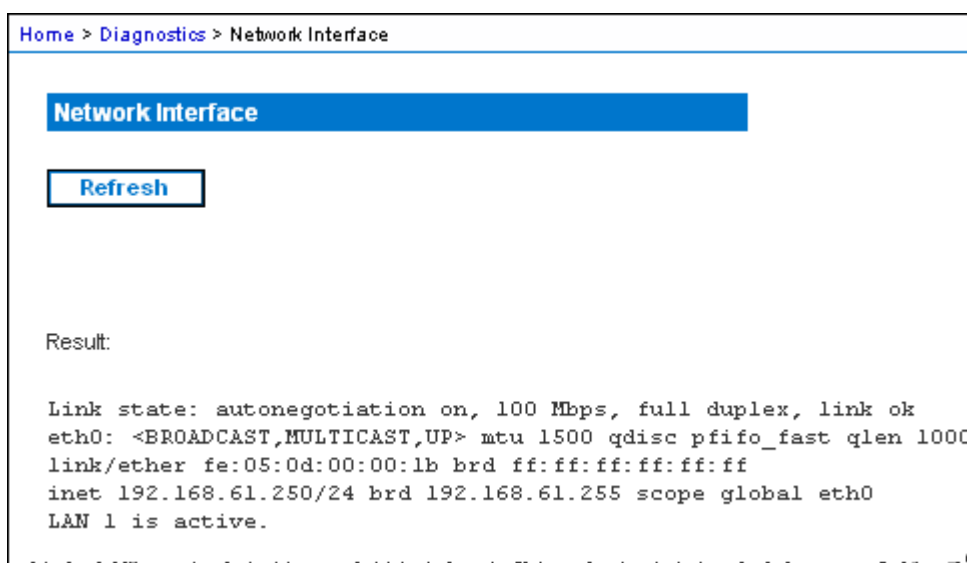
共有三個選項可用：

使用：	執行：
Network Interface (網路介面)	取得網路介面的狀態。
Network Statistics (網路統計資料)	取得網路相關統計資料。
Ping Host (偵測 (Ping) 主機)	判斷是否可以連到 IP 網路上的特定主機。
Trace Route to Host (追蹤主機路由)	判斷所選取主機的路由歷程。
Device Diagnostics (裝置診斷)	必須有 Raritan 技術支援人員的指導，方可使用此選項 (僅限遠端主控台)。

網路介面頁面

KX II-101 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)。隨即會開啓「Network Interface」(網路介面) 頁面：



顯示下列資訊：

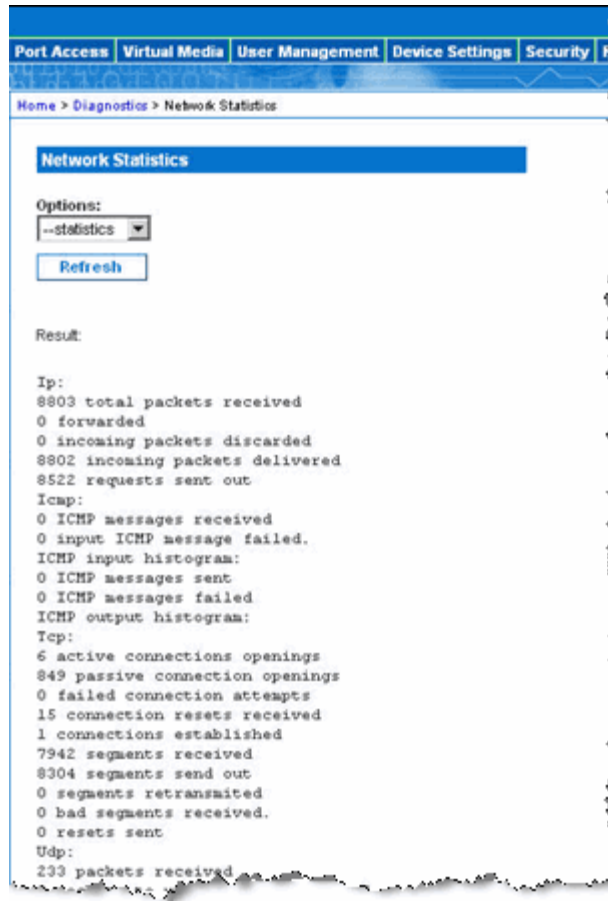
- 乙太網路介面處於開啓或關閉。
 - 是否可偵測 (ping) 到閘道。
 - 目前使用中的 LAN 連接埠。
- 若要重新整理此項資訊：
 - 按一下「Refresh」(重新整理) 按鈕。

網路統計資料頁面

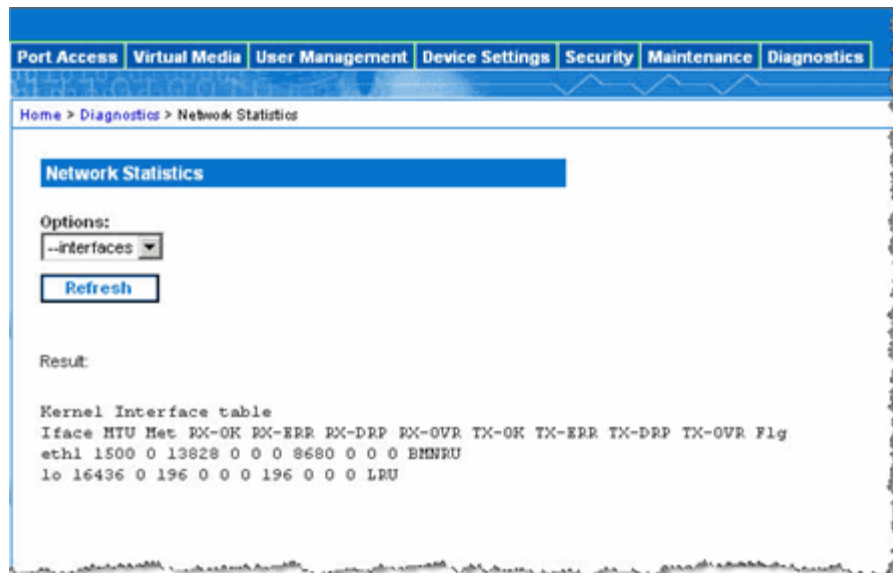
KX II-101 提供有關網路介面狀態的統計資料。

- 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)。隨即會開啓「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：

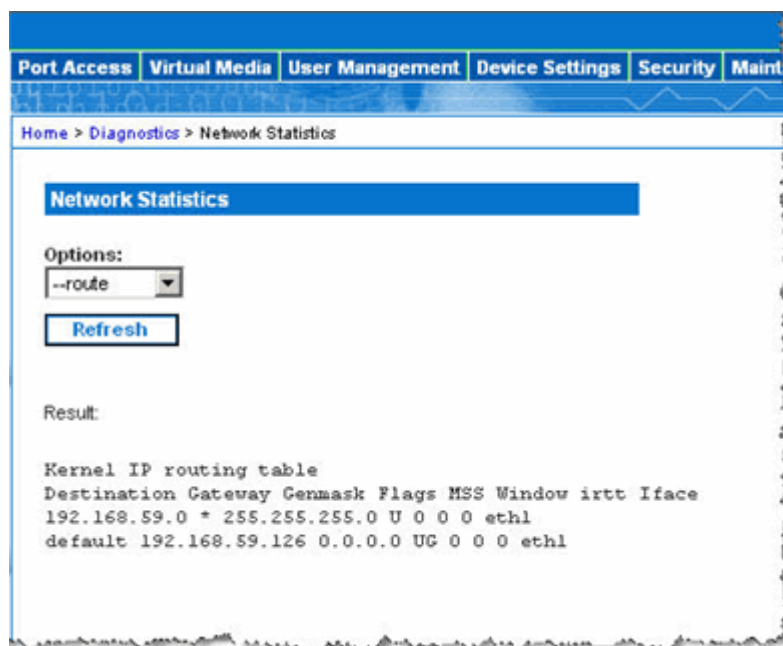
- Statistics (統計資料)。產生與下圖相似的頁面：



- 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：



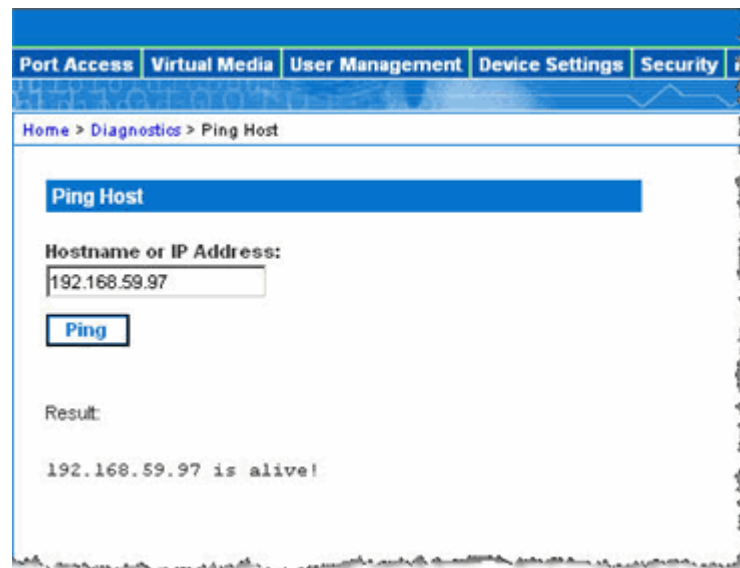
- 按一下「Refresh」(重新整理) 按鈕。
隨即會在「Result」(結果) 欄位中顯示相關資訊。

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 (Ping) 主機) 頁面可判斷目標伺服器或其他 KX II-101 裝置是否可供存取。

➤ 若要偵測 (ping) 主機：

1. 請選取「Diagnostics」(診斷) > 「Ping Host」(偵測 (Ping) 主機)。隨即會開啓「Ping Host」(偵測 (Ping) 主機) 頁面。



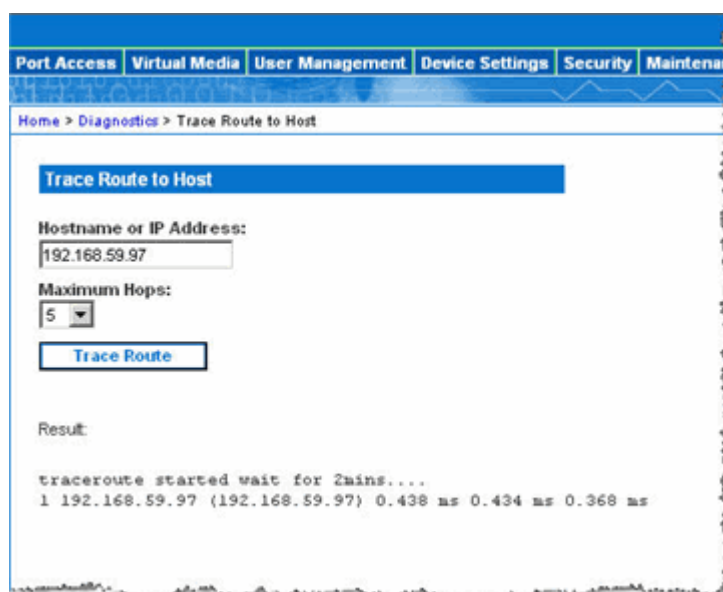
2. 在「Hostname or IP Address」(主機名稱或 IP 位址) 欄位中輸入主機名稱或 IP 位址。
3. 按一下「Ping」(偵測)。隨即會在「Result」(結果) 欄位中顯示偵測結果。

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)。隨即會開啓「Trace Route to Host」(追蹤主機路由) 頁面。



2. 在「Hostname or IP Address」(主機名稱或 IP 位址) 欄位中輸入主機名稱或 IP 位址。
3. 從下拉式清單中選擇「Maximum Hops」(最大躍點) (5 到 50，增量為 5)：
4. 按一下「Trace Route」(追蹤路由) 按鈕。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

注意：本頁面適合 Raritan 客服工程師或在「Raritan 技術支援」的指導下使用。

「Device Diagnostics」(裝置診斷) 頁面會將診斷資訊從 KX II-101 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。

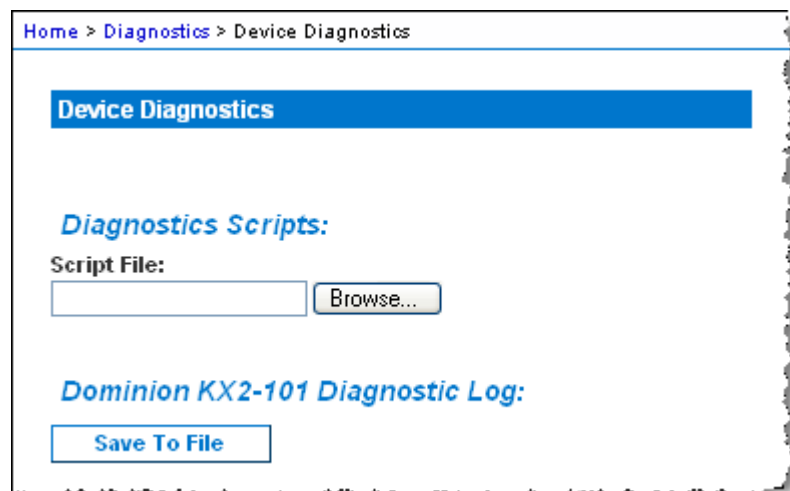
請使用下列設定：

- **Diagnostics Scripts** (診斷指令檔，選用)。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。
- **Device Diagnostic Log** (裝置診斷記錄)。將 KX II-101 裝置的診斷訊息快照集下載到用戶端。此加密檔案會傳送至「Raritan 技術支援部門」，亦只有 Raritan 能夠轉譯此檔案。

注意：只有擁有管理權限的使用者才可存取本頁面。

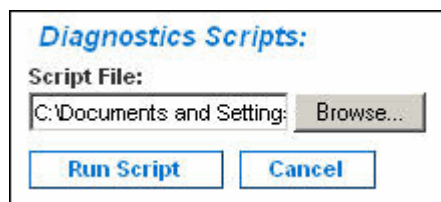
➤ 若要執行 KX II-101 系統診斷：

1. 選擇「Diagnostics」(診斷) > 「Device Diagnostics」(裝置診斷)。隨即會開啓「Device Diagnostics」(裝置診斷) 頁面。

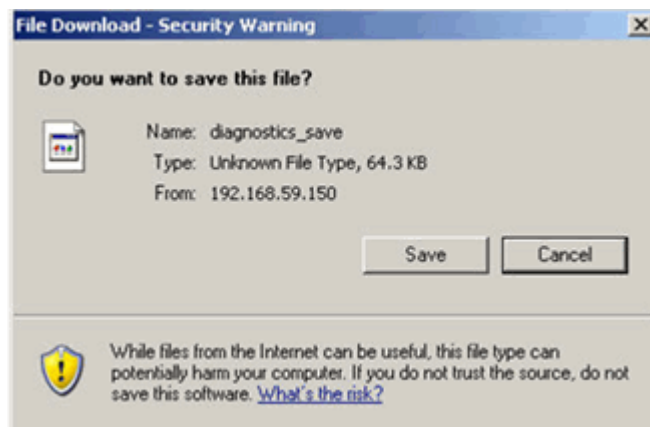


2. (選用) 如果您已收到「Raritan 技術支援部門」提供的診斷指令檔，請執行下列步驟。否則，請跳至步驟 3。
 - a. 擷取 Raritan 提供的診斷檔案，請在必要時將檔案解壓縮。

- b. 使用「Browse」(瀏覽) 按鈕。隨即會開啓「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」(開啓)。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) 按鈕。隨即會開啓「File Download」(下載檔案) 對話方塊：



- b. 按一下「Save」(儲存)。隨即會開啓「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.....	176
從 CC-SG 移除對 KX II-101 的管理.....	177
在 Proxy 模式下使用 CC-SG.....	178

概覽

當 KX II-101 裝置受 CommandCenter Secure Gateway 控制，而您嘗試直接使用「KX II-101 遠端主控台」存取裝置時，會顯示下列訊息 (在輸入有效的使用者名稱及密碼後)：

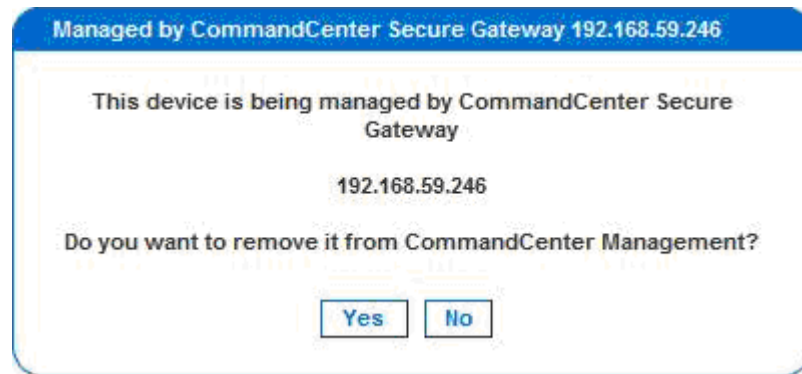


從 CC-SG 移除對 KX II-101 的管理

除非 CC-SG 釋放對 KX II-101 的控制，否則您無法直接存取裝置。但如果 KX II-101 未接獲 CommandCenter 的活動訊號訊息 (例如 CommandCenter 不在網路中)，爲了存取裝置，您可以解除 CC-SG 對 KX II-101 的控制。此項作業要使用「CC Unmanage」(CC 解除管理) 功能完成。

注意：必須具有維護權限才能使用此功能。

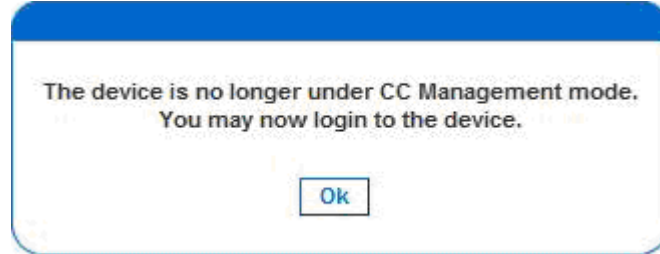
未接獲活動訊號訊息時，直接存取裝置會顯示下列訊息：



- 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) 按鈕。隨即會出現提示要求您確認動作：

在 Proxy 模式下使用 CC-SG

- 按一下「Yes」(是) 按鈕。隨即會顯示訊息，確認裝置不再受 CC 管理：



- 按一下「Yes」(是)。隨即會開啓 KX II-101 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) 啓動虛擬 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，若計劃要使用多平台用戶端 (MPC)，請不要使用 CC-SG Proxy 模式。

A

規格

本章內容

KX II-101.....	179
接頭.....	180
Raritan 遠端用戶端軟體.....	180

KX II-101

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 公厘
重量	0.6292 英磅；0.286 公斤
電源	AC/DC (100-240V~/6VDC) 變壓器 或 乙太網路供電 (PoE) Mid-Span Power Insertion Signal-Pair Power Insertion
作業溫度	0° - 40°C (32° - 104°F)
濕度	20% - 85% RH
指示燈： 藍色 RARITAN 背光標誌 網路連接埠	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 功能、數據機連線以及 Dominion PX 連線的多功能序列連接埠。

接頭

遠端連線： 網路通訊協定	一個 10/100 乙太網路 (RJ45) 連接埠 TCP/IP、HTTP、HTTPS、UDP、RADIUS、LDAP、SNTP、DHCP
螢幕解析度： 電腦圖形模式 SUN® 視訊模式	720x400 (用於 DOS) 640 X 480 @ 60/72/75/85Hz， 800 X 600 @ 56/60/72/75/85Hz， 1024 X 768 @ 60/70/75/85Hz， 1152 X 864 @ 60/75Hz， 1280 X 1024 @ 60Hz， 1600 X 1200 @ 60Hz
認證：	UL/CUL、FCC Class A、CB、CE Class A 以及 VCCI Class A

接頭

介面類型	長度 (英吋；公分)	說明
視訊	15 英吋；38 公分	整合式纜線
PS/2	15 英吋；38 公分	整合式纜線
MiniUSB 對 USB(M)	17.7 英吋；45 公分	USB 纜線
MiniDin9(M) 對 DB9(F)	72 英吋；182 公分	序列纜線
DKX2-101-LPKVMC	3.9 英吋；10 公分	本機連接埠整合式纜線
DKX2-101-SPDUC	70.86 英吋；180 公分	連接 Dominion PX 的纜線

Raritan 遠端用戶端軟體

作業系統需求：Windows XP / NT / ME / 2000

B

安裝機架

KX II-101 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 產品組內隨附的托架與螺釘。

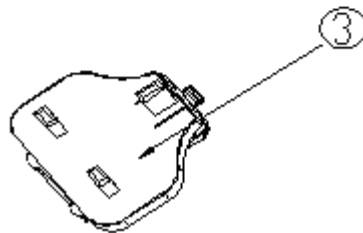
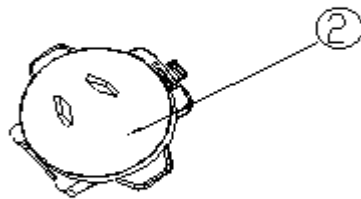
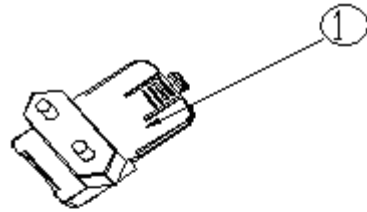
本章內容

各式 AC-DC 變壓器插頭	181
托架安裝	183

各式 AC-DC 變壓器插頭

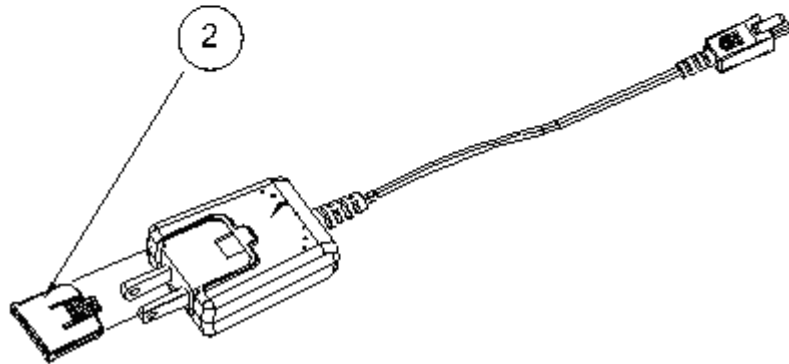
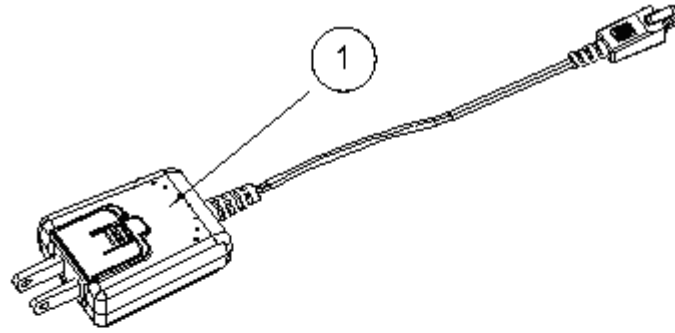
識別插頭類型

1. 歐規插頭
2. 澳規插頭
3. 英規插頭



移除 AC-DC 變壓器的外罩附件

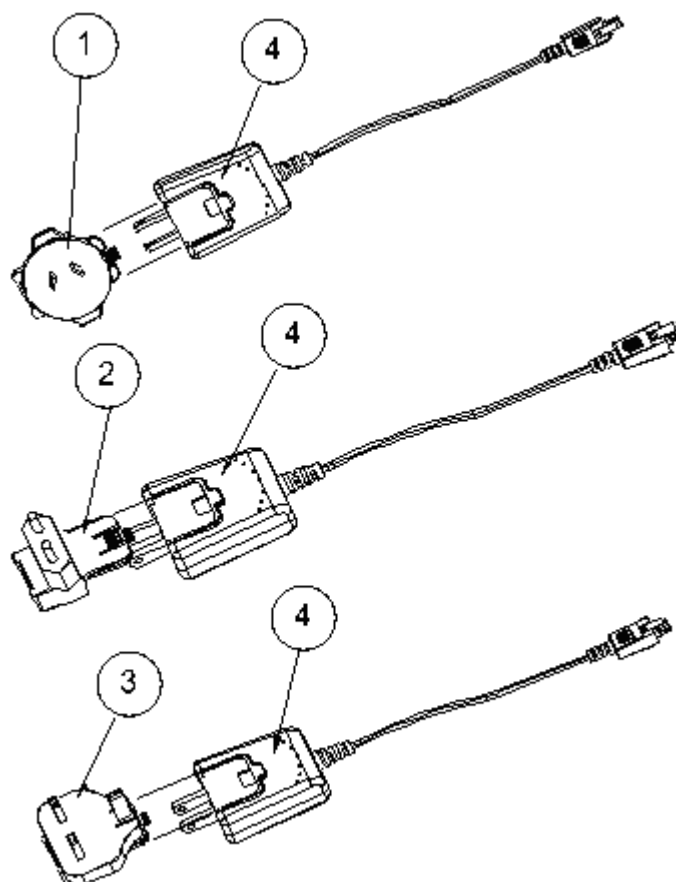
1. AC/DC 變壓器
2. 外罩附件。一推即可移除。



AC-DC 變壓器的轉接插頭

1. 澳規插頭
2. 歐規插頭
3. 英規插頭

4. 變壓器

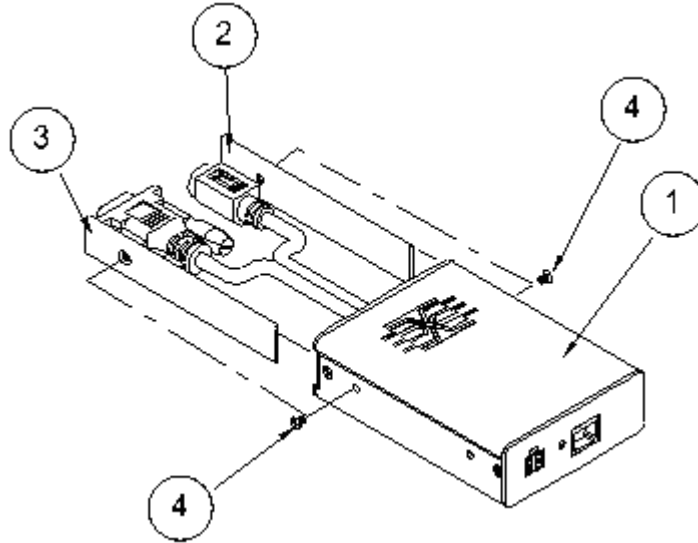


托架安裝

1. KX II-101 裝置
2. 右面板
3. 左面板
4. 螺釘

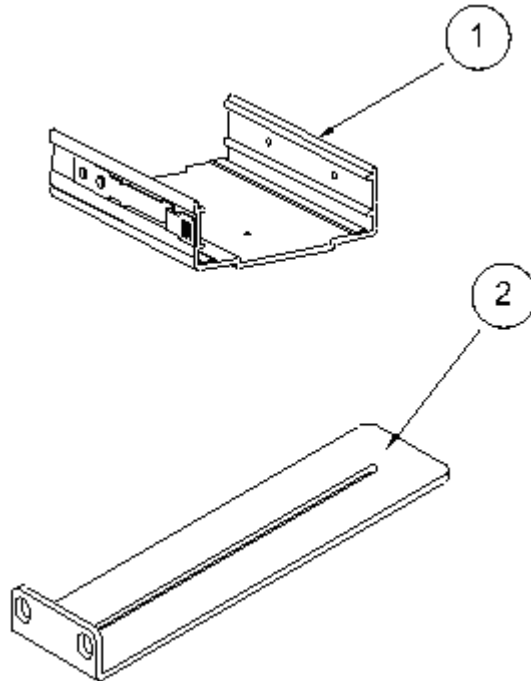
托架安裝

- 移除 KX II-101 裝置的螺釘。
- 滑開 KX II-101 裝置的左右側面板。



KX II-101 托架零件

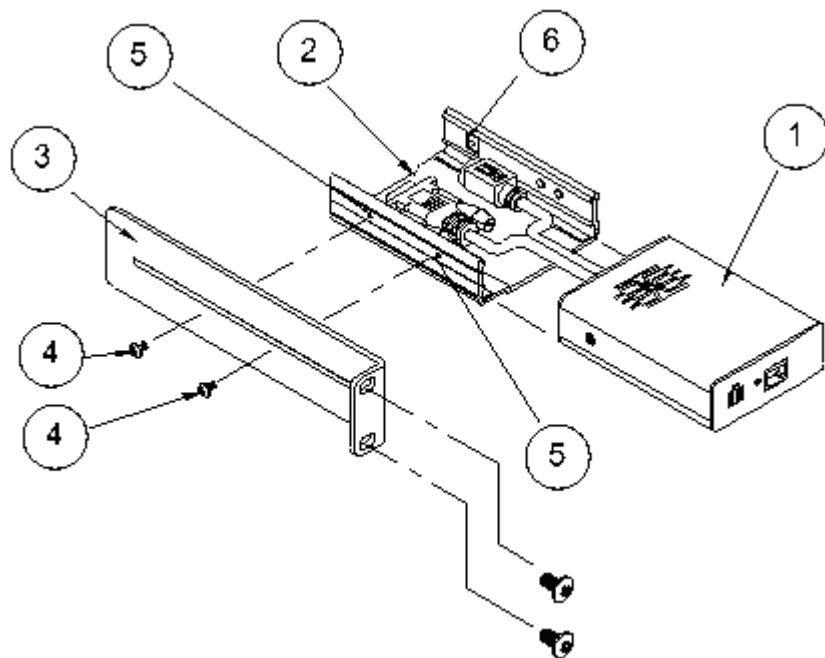
1. U 型托架
2. L 型托架



裝上托架水平裝載 KX II-101

1. KX II-101 裝置
 2. U 型托架
 3. L 型托架
 4. 螺釘
 5. 裝載孔
 6. 門鎖拉柄
- 使用隨附的螺釘裝上 U 型托架與 L 型托架。調整托架位置後再鎖緊螺釘。
 - 以機架用的螺釘 (機架製造商所提供) 將 U 型與 L 型托架附件裝到機架上。
 - 讓 KVM 纜線面向目標，將 KX II-101 裝置滑入 U 型托架。推入並鬆開門鎖拉柄，將 KX II-101 裝置與 U 型托架鎖緊。

下圖顯示在左側裝載 KX II-101。若要在右側裝載 KX II-101，請遵循上述指示進行，但要將托架裝在 KX II-101 裝置的右側。



裝上托架垂直裝載 KX II-101

1. KX II-101 裝置
2. U 型托架

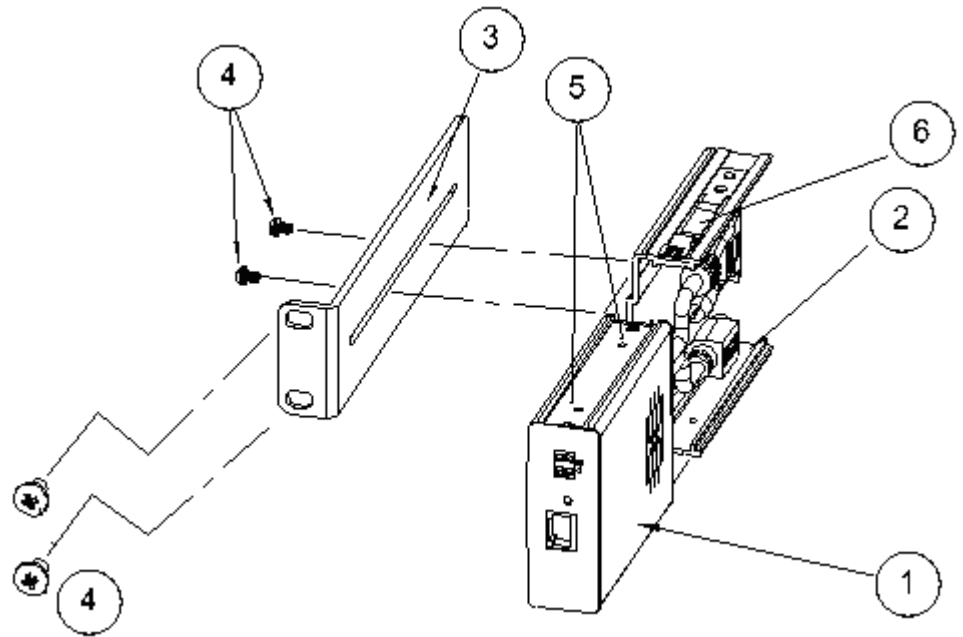
托架安裝

3. L 型托架
4. 螺釘
5. 裝載孔
6. 門鎖拉柄

使用隨附的螺釘裝上 U 型托架與 L 型托架。調整托架位置後再鎖緊螺釘。

以機架用的螺釘 (機架製造商所提供) 將 U 型與 L 型托架附件裝到機架上。

讓 KVM 纜線面向目標，將 KX II-101 裝置滑入 U 型托架。推入並鬆開門鎖拉柄，將 KX II-101 裝置與 U 型托架鎖緊。



索引

A

AC-DC 變壓器的轉接插頭 - 182
AppleR Macintosh 設定 - 13

C

CC 解除管理 - 176
CC-SG 使用者注意事項 - 58
CD-ROM/DVD-ROM/ISO 映像檔 - 103, 107, 109
CLI 指令 - 159, 163
CLI 提示 - 162
CLI 語法 - 祕訣與快速鍵 - 162

D

Dominion KX II-101 概覽 - 1

I

Interface 指令 - 166
IP 存取控制 - 52, 54, 116, 147

J

Java Runtime Environment (JRE) - 31

K

KX II-101 - 179
KX II-101 主控台配置 - 33
KX II-101 主控台瀏覽方式 - 34
KX II-101 托架零件 - 184
KX II-101 的 SSH 連線 - 160
KX II-101 遠端主控台功能表導覽 - 35

L

LAN 介面設定 - 114
Linux 設定 - 11
Listports 指令 - 163, 167

M

Microsoft Active Directory 注意事項 - 58

N

Name 指令 - 163, 166

Network Settings (網路設定) - 112

P

PS/2 組態 - 16

R

RADIUS 通訊交換規格 - 65
Raritan 遠端用戶端軟體 - 180

S

Service Pack - 6
Setlog 指令 - 164
SNMP 代理組態 - 122, 126
SNMP 組態 - 122
SNMP 設限組態 - 122, 126
Sun Solaris 設定 - 12
Syslog 組態 - 123

U

UNIX 工作站的 SSH 存取方法 - 161
USB 組態 - 18
Userlist 指令 - 164, 167

V

VKC 虛擬媒體 - 95

W

Windows 2000 設定 - 11
Windows Vista - 10
Windows XP 設定 - 11
Windows 電腦的 SSH 存取方法 - 160

三劃

工具功能表 - 96
工具列 - 79

四劃

中斷虛擬媒體的連線 - 103, 108
介面 - 3
內容對話方塊 - 81
分組的 IP ACL (存取控制清單) - 53
升級歷程記錄 - 156

索引

支援的通訊協定 - 58
日期/時間設定 - 120

五劃

加密與共用 - 145
功能表樹狀目錄 - 78
本機磁碟機 - 103, 105
目標螢幕解析度 - 98

六劃

同步化滑鼠 - 92
各式 AC-DC 變壓器插頭 - 181
在 Proxy 模式下使用 CC-SG - 178
安全性設定 - 140, 141
安全性設定功能表 - 140
安裝與組態 - 7, 166
安裝機架 - 4, 181
托架安裝 - 183
自動完成指令 - 162
自動感應視訊設定 - 88

七劃

序列連接埠設定 - 119
我的最愛清單 - 38
更新 LDAP 架構 - 63, 66
更新架構快取 - 71
系統管理功能 - 3

八劃

事件管理 - 121
事件管理 - 目的地 - 124
使用 CLI 存取 KX II-101 - 160
使用本機使用者連接埠 - 20
使用者 - 45
使用者、群組以及存取權限 - 45
使用者功能 - 4
使用者封鎖 - 49, 142, 144
使用者清單 - 47
使用者群組清單 - 50
使用者管理 - 45, 46
使用者管理功能表 - 46
使用者與群組之間的關聯性 - 46
使用終端機模擬程式 - 6, 26, 161
使用虛擬媒體 - 103

使用虛擬媒體的必要條件 - 102, 103
使用管理連接埠 - 19, 26
使用遠端主控台 - 21
命名目標伺服器 - 23
命名電源插座裝置 (電源插座裝置的連接埠頁面) - 132
所有指令行介面層級的常見指令 - 163

九劃

封鎖和解除封鎖使用者 - 49
建立 KVM 目標伺服器與插座的關聯 (連接埠頁面) - 133, 138
建立使用者與群組 - 24
建立新屬性 - 68
建立鍵盤巨集 - 85
指令行介面 (CLI) - 159
指派 IP 位址 - 6, 22
重要資訊 - 6
重新開機 - 157
重新整理畫面 - 88

十劃

修改現有的使用者 - 47, 49
修改現有的使用者群組 - 50, 56
修改鍵盤巨集 - 87
校準色彩 - 89
追蹤主機路由頁面 - 173
除錯 - 163, 164

十一劃

偵測 (Ping) 主機頁面 - 172
執行 LDAP 遠端驗證 - 61
執行 RADIUS 遠端驗證 - 60, 64
執行鍵盤巨集 - 87
專有名詞 - 5
將屬性新增至類別 - 69
強固密碼 - 57, 142, 143
從 Active Directory 伺服器傳回使用者群組資訊 - 63
從 CC-SG 移除對 KX II-101 的管理 - 177
從 LDAP - 67
從 Microsoft Active Directory - 67
控制電源插座裝置 - 130, 138
探查裝置 - KX II-101 子網路 - 42

探查裝置 - 本機子網路 - 40
 接頭 - 5, 180
 啓用直接連接埠存取 - 33
 啓動 KX II-101 - 31
 產品包裝內容 - 4
 產品特色 - 3
 產品圖片 - 2
 移除 AC-DC 變壓器的外罩附件 - 182
 移除鍵盤巨集 - 87
 組態 - 165
 規格 - 179
 設定 KX II-101 - 7, 20
 設定 Sun 視訊解析度 - 8
 設定目標伺服器 - 7
 設定伺服器視訊解析度 - 8, 16
 設定直接連接埠存取 - 22
 設定個別群組的權限 - 49, 52
 設定連接埠權限 - 53
 設定登錄允許對架構進行寫入作業 - 68
 設定新密碼 - 21
 設定網路防火牆組態 - 7, 20
 設定權限 - 52, 56
 連接 KX II-101 - 7, 14, 23, 31
 連接目標伺服器 - 16
 連接埠存取頁面 - 44
 連接埠組態 - 128
 連接虛擬媒體 - 105
 連接電源插座 - 131, 134
 連接網路 - 19
 連線功能表 - 81
 連線資訊 - 83
 透過 RADIUS 傳回使用者群組資訊 - 65

十二劃

備份與還原 - 153
 單滑鼠游標 - 92
 智慧 - 94
 無法使用讀取/寫入的情況 - 105, 106
 登入 - 6, 161
 登入限制 - 141, 142
 登出 - 35
 結束 - 84
 絕對 - 95
 虛擬 KVM 用戶端 - 76

虛擬媒體 - 95, 99
 視訊功能表 - 88
 視訊設定 - 89
 視訊解析度 - 4
 診斷 - 163, 164, 168
 診斷功能表 - 168
 開啓 KVM 階段作業 - 104
 開啓 KX II-101 電源 - 19
 韌體升級 - 155

十三劃

傳回使用者群組資訊 - 66
 傳送 Ctrl+Alt+Delete - 84
 新增我的最愛 - 38, 43
 新增使用者 - 47, 48, 49, 144
 新增使用者群組 - 51
 概覽 - 77, 100, 130, 159, 176
 滑鼠功能表 - 80, 92
 滑鼠同步提示 - 80
 滑鼠指標同步 - 80
 滑鼠模式 - 10
 群組 - 45
 裝上托架水平裝載 KX II-101 - 185
 裝上托架垂直裝載 KX II-101 - 185
 裝置服務 - 116, 160
 裝置設定功能表 - 111
 裝置診斷 - 174
 裝置資訊 - 152
 裝置管理 - 111
 裝載 - 4
 電源 - 4
 電源控制 - 130
 預設 IP 位址 - 6

十四劃

管理功能 - 3
 管理我的最愛 - 36
 管理我的最愛功能表 - 37
 網路 - 163, 165
 網路介面頁面 - 169
 網路基本設定 - 113
 網路統計資料頁面 - 169
 網路組態 - 3
 維護 - 150

索引

維護功能表 - 150
語言支援 - 31
說明功能表 - 98
遠端驗證 - 58

十五劃

標準 - 93
稽核記錄 - 151
編輯使用者成員的 rciusergroup 屬性 - 72

十六劃

選用附件 - 5
選項 - 78, 96

十七劃

檔案伺服器設定 (僅限檔案伺服器 ISO 映像檔)
- 103, 109
檢查瀏覽器是否支援 AES 加密功能 - 146, 147
檢視工具列 - 97
檢視功能表 - 97
縮放比例 - 97
鍵盤/滑鼠設定 - 118
鍵盤功能表 - 84
鍵盤巨集 - 84

十八劃

瀏覽 CLI - 161
簡介 - 1

十九劃

識別插頭類型 - 181
關於 Raritan 虛擬 KVM 用戶端 - 98

二十三劃

變更密碼 - 57
顯示插座關聯 - 137
驗證設定 - 57, 59
驗證與授權 - 58, 59



➤ 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：+81-3-3523-5994

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 p.m. GMT+1 CET

電話：+49-20-17-47-98-0

➤ 韓國

週一至週五

當地時間 9 a.m. - 6 p.m.

電話：+82-2-5578730

➤ 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：tech.rap@raritan.com