



# ASMB8-iKVM

遠端管理卡  
使用手冊



T10970

第二版

2016 年 8 月發行

## 版權說明

© ASUSTeK Computer Inc. All rights reserved. 華碩電腦股份有限公司保留所有權利

本使用手冊包括但不限於其所包含的所有資訊皆受到著作權法之保護，未經華碩電腦股份有限公司（以下簡稱「華碩」）許可，不得任意地仿製、拷貝、謄抄、轉譯或為其他利用。

## 免責聲明

本使用手冊是以「現況」及「以目前明示的條件下」的狀態提供給您。在法律允許的範圍內，華碩就本使用手冊，不提供任何明示或默示的擔保及保證，包括但不限於商業適銷性、特定目的之適用性、未侵害任何他人權利及任何得使用本使用手冊或無法使用本使用手冊的保證，且華碩對因使用本使用手冊而獲取的結果或透過本使用手冊所獲得任何資訊之準確性或可靠性不提供擔保。

台端應自行承擔使用本使用手冊的所有風險。台端明確了解並同意，華碩、華碩之授權人及其各該主管、董事、員工、代理人或關係企業皆無須為您因本使用手冊、或因使用本使用手冊、或因不可歸責於華碩的原因而無法使用本使用手冊或其任何部分而可能產生的衍生、附隨、直接、間接、特別、懲罰或任何其他損失（包括但不限於利益損失、業務中斷、資料遺失或其他金錢損失）負責，不論華碩是否被告知發生上開損失之可能性。

由於部分國家或地區可能不允許責任的全部免除或對前述損失的責任限制，所以前述限制或排除條款可能對您不適用。

台端知悉華碩有權隨時修改本使用手冊。本產品規格或驅動程式一經改變，本使用手冊將會隨之更新。本使用手冊更新的詳細說明請您造訪華碩的客戶服務網 <http://support.asus.com>，或是直接與華碩資訊產品技術支援專線 0800-093-456 聯絡。

於本使用手冊中提及之第三人產品名稱或內容，其所有權及智慧財產權皆為各別產品或內容所有人所有且受現行智慧財產權相關法令及國際條約之保護。

當下列兩種情況發生時，本產品將不再受到華碩之保固及服務：

- (1) 本產品曾經過非華碩授權之維修、規格更改、零件替換或其他未經過華碩授權的行為。
- (2) 本產品序號模糊不清或喪失。

本產品的名稱與版本都會印在主機板/顯示卡上，版本數字的編碼方式是用三個數字組成，並有一個小數點做間隔，如 1.02G、2.03G 等...數字愈大表示版本愈新，而愈左邊位數的數字更動表示更動幅度也愈大。更新的詳細說明請您到華碩的全球資訊網瀏覽或是直接與華碩聯絡。

# 目錄內容

安全性須知.....	vi
電氣方面的安全性 .....	vi
操作方面的安全性 .....	vi
REACH 資訊 .....	vi
產品回收與處理 .....	vi
限用物質名稱及含量列表 .....	vii
關於這本使用手冊 .....	viii
使用手冊的編排方式 .....	viii
提示符號 .....	ix
哪裡可以找到更多的產品資訊 .....	ix
ASMB8-iKVM 規格列表 .....	x

## 第一章：產品介紹

1.1 歡迎加入華碩愛好者的行列！ .....	1-2
1.2 產品包裝 .....	1-2
1.3 功能介紹 .....	1-3
1.4 系統需求 .....	1-4
1.5 網路設定 .....	1-5

## 第二章：安裝

2.1 安裝前 .....	2-2
2.2 硬體安裝 .....	2-2
2.3 韌體升級與 IP 設定 .....	2-4
2.3.1 韌體升級 .....	2-4
2.3.2 設定 BMC IP 來源靜態 IP .....	2-5
2.3.3 設定 BMC IP 來源 DHCP .....	2-6
2.4 BIOS 設定 .....	2-7
2.4.1 設定 BIOS BMC .....	2-7
2.4.2 BMC 網路設定 .....	2-8
2.4.3 系統事件日誌 .....	2-9
2.4.4 IPv6 BMC 網路設定 .....	2-10
2.5 執行 ASMC8 應用程式 .....	2-12
2.5.1 設定 LAN 控制器 .....	2-14
2.5.2 設定使用者名與密碼 .....	2-15

## 第三章：華碩主機管理控制器設定

3.1 華碩主機管理控制器設定（Host Management Controller Setup） .....	3-2
3.1.1 安裝並執行華碩 Host Management Controller Setup 應用程式 .....	3-2
3.1.2 選單欄 .....	3-3
3.1.3 初始化（Initial） .....	3-3
3.1.4 檢視（View） .....	3-3
3.1.5 設定（Set） .....	3-6
3.1.6 監控（Monitor） .....	3-8
3.1.7 幫助（Help） .....	3-9

# 目錄內容

## 第四章：網頁使用者介面

4.1 網頁使用者介面 .....	4-2
4.1.1 登錄應用程式 .....	4-2
4.1.2 使用應用程式 .....	4-3
4.2 系統訊息 ( FRU Information ) .....	4-4
4.3 伺服器狀況 ( Server Health ) .....	4-5
4.3.1 監控訊息 ( Sensor Readings (with Thresholds) ) .....	4-5
4.3.2 事件日誌 ( Event Log ) .....	4-6
4.3.3 審查日誌 ( Audit Log ) .....	4-6
4.3.4 藍屏訊息 ( BSOD Screen ) .....	4-7
4.4 設定 ( Configuration ) .....	4-8
4.4.1 Active Directory .....	4-8
4.4.2 DNS .....	4-11
4.4.3 Event Log .....	4-11
4.4.4 LDAP/E-Directory .....	4-12
4.4.5 滑鼠模式 ( Mouse Mode ) .....	4-15
4.4.6 網路 ( Network ) .....	4-15
4.4.7 Network Bond .....	4-16
4.4.8 NTP .....	4-16
4.4.9 PEF .....	4-17
4.4.10 RADIUS .....	4-24
4.4.11 遠端會話 ( Remote Session ) .....	4-24
4.4.12 服務 ( Services ) .....	4-25
4.4.13 SMTP .....	4-25
4.4.14 SSL .....	4-26
4.4.15 使用者 ( Users ) .....	4-31
4.4.16 虛擬媒體 ( Virtual Media ) .....	4-33
4.5 遠端控制 ( Remote Control ) .....	4-34
4.5.1 Console Redirection .....	4-34
4.5.2 伺服器電源管理 ( Server Power Control ) .....	4-42
4.5.3 Java SOL .....	4-42
4.5.4 機殼識別指令 ( Chassis Identify Command ) .....	4-42
4.5.5 電源按鈕 ( Power Button ) .....	4-43
4.6 自動錄影 ( Auto Video Recording ) .....	4-44
4.6.1 觸發器設定 ( Triggers Configuration ) .....	4-44
4.6.2 已錄製視訊 ( Recorded Video ) .....	4-44
4.7 維護 ( Maintenance ) .....	4-45
4.7.1 保留設定 ( Preserve Configuration ) .....	4-45
4.7.2 恢復出廠預設值 .....	4-45
4.7.3 BMC 重置 ( Reset BMC ) .....	4-46
4.7.4 iKVM 重置 ( Reset iKVM ) .....	4-46

# 目錄內容

- 4.7.5 BIOS 開機自我檢測程序代碼 ( BIOS POST Code ) .....4-46
- 4.8 韌體升級 ( Firmware Update ) .....4-47
  - 4.8.1 韌體升級 ( Firmware Update ) .....4-47
  - 4.8.2 BIOS 升級 ( BIOS Update ) .....4-47

## 附錄：參考訊息

- A.1 BMC 插座.....A-2
- A.2 LAN 接頭.....A-3
- A.3 疑難排解.....A-4
- A.4 監控器表.....A-5
- A.5 華碩 Server System 系列支援 ASMB8-iKVM 之機種型號.....A-11
- A.6 華碩的連絡資訊.....A-12

# 安全性須知

## 電氣方面的安全性

- 為避免可能的電擊造成嚴重損害，在搬動電腦主機之前，請先將電腦電源線暫時從電源插槽中拔掉。
- 當您要加入硬體裝置到系統中或者要移除系統中的硬體裝置時，請務必先連接該裝置的訊號線，然後再連接電源線。可能的話，在安裝硬體裝置之前先拔掉電腦的電源供應器電源線。
- 當您要從主機板連接或拔除任何的訊號線之前，請確定所有的電源線已事先拔掉。
- 在使用擴充卡之前，我們建議您可以先尋求專業人士的協助。這些裝置有可能會干擾接地的迴路。
- 請確定電源供應器的電壓設定已調整到本國/本區域所使用的電壓標準值。若您不確定您所屬區域的供應電壓值為何，那麼請就近詢問當地的電力公司人員。
- 如果電源供應器已損壞，請不要嘗試自行修復。請將之交給專業技術服務人員或經銷商來處理。

## 操作方面的安全性

- 在您安裝主機板以及加入硬體裝置之前，請務必詳加閱讀本手冊所提供的相關資訊。
- 在使用產品之前，請確定所有的排線、電源線都已正確地連接好。若您發現有任何重大的瑕疵，請儘速聯絡您的經銷商。
- 為避免發生電氣短路情形，請務必將所有沒用到的螺絲、迴紋針及其他零件收好，不要遺留在主機板上或電腦主機中。
- 灰塵、濕氣以及劇烈的溫度變化都會影響主機板的使用壽命，因此請盡量避免放置在這些地方。
- 請勿將電腦主機放置在容易搖晃的地方。
- 若在本產品的使用上有任何的技術性問題，請和經過檢定或有經驗的技術人員聯絡。

## REACH 資訊

注意：謹遵守 REACH(Registration, Evaluation, Authorisation, and Restriction of Chemicals) 管理規範，我們會將產品中的化學物質公告在華碩 REACH 網站，詳細請參考 <http://csr.asus.com/english/REACH.htm>。

## 產品回收與處理

華碩與資源回收業者以最高標準相互配合，以保護我們的環境，確保工作者的安全，以及遵從全球有關環境保護的法律規定。我們保證以資源回收的方式回收以往生產的舊裝置，透過多樣的方式保護環境。

如欲了解更多關於華碩產品資源回收資訊與聯絡方式，請連線上網至 CSR (Corporate Social Responsibility) 網頁：<http://csr.asus.com/english/Takeback.htm>。



請勿將本主機板當作一般垃圾丟棄。本產品零組件設計為可回收利用。這個打叉的垃圾桶標誌表示本產品（電器與電子裝置）不應視為一般垃圾丟棄，請依照您所在地區有關廢棄電子產品的處理方式處理。



請勿將內含汞的電池當作一般垃圾丟棄。這個打叉的垃圾桶標誌表示電池不應視為一般垃圾丟棄。

## 限用物質名稱及含量列表

單元	限用物質及其化學符號					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr <sup>+6</sup> )	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
印刷電路板及電子組件	—	○	○	○	○	○
外殼	○	○	○	○	○	○
散熱裝置	—	○	○	○	○	○
電源供應器	—	○	○	○	○	○
其他及其配件	—	○	○	○	○	○
備考 1. "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。 備考 2. "—" 係指該項限用物質為排除項目。						

# 關於這本使用手冊

產品使用手冊包含了所有當您在安裝華碩 ASMB8-iKVM 遠端管理卡時所需用到的訊息。

## 使用手冊的編排方式

使用手冊是由下面幾個章節所組成：

- **第一章：產品介紹**

本章節描述本遠端管理卡的功能和新技術。

- **第二章：安裝**

本章節描述安裝管理卡與應用程式。

- **第三章：華碩遠端控制程式**

本章節介紹華碩遠端控制程式的功能。

- **第四章：網頁使用者介面**

本章節介紹如何使用網頁使用者介面來設定與管理伺服器。

- **附錄：相關訊息**

本附錄中包含 BMC、LAN 接頭訊息與疑難排解訊息等。



## 提示符號

為了能夠確保您正確地完成管理卡設定，請務必注意下面這些會在本手冊中出現的標示符號所代表的特殊含意。



警告：提醒您在進行某一項工作時要注意您本身的安全。



小心：提醒您在進行某一項工作時要注意勿傷害到電腦主機板元件。



重要：此符號表示您必須要遵照手冊所描述之方式完成一項或多項軟硬體  
的安裝或設定。



注意：提供有助於完成某項工作的訣竅和其他額外的訊息。

## 哪裡可以找到更多的產品資訊

您可以經由下面所提供的兩個管道來獲得您所使用的華碩產品資訊以及軟硬體的升級資訊等。

### 1. 華碩網站

您可以到 <http://tw.asus.com> 華碩電腦全球資訊網取得所有關於華碩軟硬體產品的各項資訊。台灣地區以外的華碩網址請參考手冊最後附錄裡的聯絡資訊。

### 2. 其他文件

在您的產品包裝盒中除了本手冊所列舉的標準配件之外，也有可能夾帶其他的文件，譬如經銷商所附的產品保證單據等。

# ASMB8-iKVM 規格列表

晶片組	Aspeed 2400
內建 RAM	系統：224MB 視訊：32MB
內建 ROM	32MB
計時器	32-bit Watchdog Timer
主要功能	相容並支援 IPMI 2.0 支援 KVM over LAN 支援網頁使用者介面（遠端管理） 支援虛擬媒體（Virtual media） 支援 Network Bonding
尺寸	22mm x 17mm

★ 規格若有任何更改，恕不另行通知

# 產品介紹

您可以在本章節中發現諸多華碩所賦予本產品的優異特色，利用簡潔易懂的說明，讓您能很快的掌握本產品的各項特性，當然，在本章節我們也會提及所有能夠應用在本產品的新技術。

# 1

## 1.1 歡迎加入華碩愛好者的行列！

再次感謝您購買此款華碩 ASMB8-iKVM 遠端管理卡。

華碩 ASMB8-iKVM 相容智慧平台管理介面（Intelligent Platform Management Interface，IPMI）2.0，允許您透過本地網路（LAN）中的中心伺服器來監控、控制與管理一台遠端伺服器。將 ASMB8-iKVM 管理卡插入伺服器主機板，就可以即時有效地監控伺服器。此方案幫助您降低 IT 管理成本，也提高了工作效率。

在您拿到本產品包裝盒之後，請馬上檢查下面所列出的各項標準配件是否齊全。

## 1.2 產品包裝

請檢查下面所列出的各項標準配件是否齊全。

- 華碩 ASMB8-iKVM 遠端管理卡
- 驅動程式與公用程式光碟
- 使用手冊



---

若以上列出的任何一項配件有損壞或是短缺的情形，請儘快與您的經銷商連絡。

---

## 1.3 功能介紹

1. IPMI 2.0
  - 系統介面 (KCS)
  - LAN 介面 (支援 RMCP+)
  - 系統事件日誌 (SEL)
  - 傳感資料記錄 (SDR)
  - 現場可更換部件 (FRU)
  - 遠端開機/關機，遠端重新啟動系統系統
  - Serial Over LAN (SOL)
  - 驗證類型：RAKP-HMAC-SHA1
  - 加密 (AES)
  - 平台事件過濾 (PEF)
  - 平台事件陷阱 (PET)
  - 看門狗計時器 (Watchdog Timer)
2. Private I2C 匯流排
  - 自動監控器 (溫度、電壓、風扇速度與記錄事件)
3. PMBus\*
  - 支援 PMBus 裝置電源
4. PSMI\*
  - 支援 PSMI 匯流排裝置電源
5. 網頁使用者介面
  - 監控器，顯示 SDR、SEL、FRU、設定 BMC、LAN
  - 支援 SSL (HTTPS)
  - 多級使用者許可
  - 升級 BMC 韌體
6. 韌體升級
  - DOS 工具
  - 網頁圖形使用者介面 (Windows® XP/Vista/2003/2008、RHEL5.2、SLES10SP2)
7. 提示
  - PET
  - SNMP Trap
  - e-Mail
8. KVM over Internet
  - 網頁遠端控制
9. 遠端更新 BIOS
  - 使用遠端軟碟機更新 BIOS

10. 遠端存儲（虛擬媒體）
  - 支援兩個遠端儲存器，用於 USB/CD-ROM/DVD 與影像
11. 遠端安裝作業系統
  - 使用遠端儲存器遠端安裝作業系統
12. 支援 MIB 文件
  - 管理系統庫（MIB）是一個用來管理通訊網路中實體的資料庫。通常大多數與簡單網路管理協議（SNMP）結合使用。

\* 須支援 PMBus 與 PSMI

\*\* 規格若有變更，恕不另行通知

## 1.4 系統需求

在安裝 ASMB8-iKVM 遠端管理卡之前，請先確認遠端伺服器系統是否達到下列要求：

- 支援底板管理控制器（Baseboard Management Controller，BMC）插座\* 的華碩伺服器主機板
- 支援 RJ-45 網路接頭，用於伺服器管理\*\*
- Microsoft® Internet Explorer 5.5 或更新版本；Firefox



---

\* 請造訪華碩網站（<http://tw.asus.com>）獲取最新支援 ASMB8-iKVM 的伺服器主機板列表。

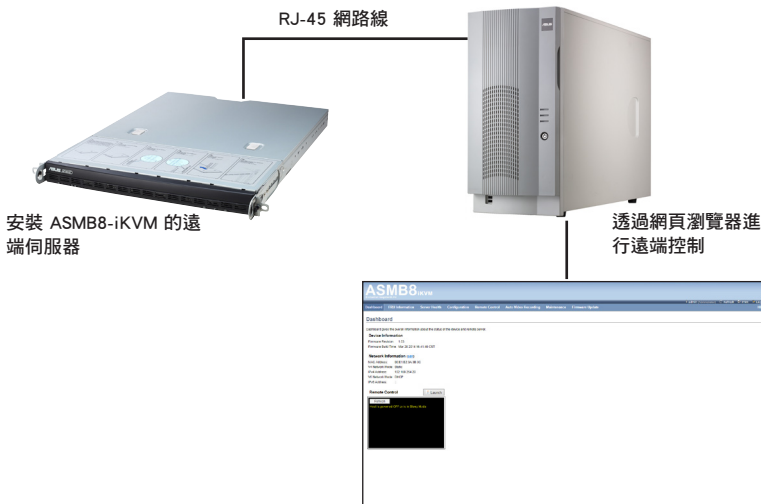
\*\* 詳細訊息請參看附錄。

---

## 1.5 網路設定

安裝在遠端伺服器主機板上的 ASMB8-iKVM 遠端管理卡透過直接 LAN 連線或網路集線器連接到本地 / 中心伺服器。以下是支援的伺服器管理設定：

### 直接 LAN 連線



### 透過網路集線器的 LAN 連線



This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



# 安裝

本章節描述了如何將管理卡安裝到伺服器主機板上，並介紹如何安裝各項應用程式。

# 2

## 2.1 安裝前

在您動手安裝遠端管理卡到伺服器主機板上之前，請務必先作好以下所列出的各項預防措施。

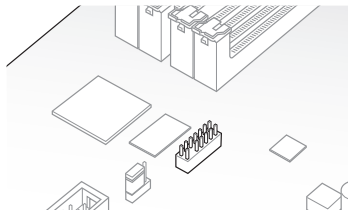


- 在處理伺服器主機板上的任何元件時，請先拔掉系統的電源線。
- 為避免產生靜電，在拿取任何電腦元件時除了可以使用防靜電手環之外，您也可以觸摸一個有接地線的物品或者金屬物品像電源供應器外殼等。
- 拿取整合電路元件時請盡量不要觸碰到元件上的晶片。
- 在您移除任何一個整合電路元件後，請將該元件放置在絕緣墊上以隔離靜電，或者直接放回該元件的絕緣包裝袋中保存。
- 在您安裝或移除任何元件之前，請確認電源供應器的電源開關是切換到關閉（OFF）的位置，而最安全的做法是先暫時拔出電源供應器的電源線，等到安裝/移除工作完成後再將之接回。如此可避免因仍有電力殘留在系統中而嚴重損及主機板、周邊裝置、元件等。

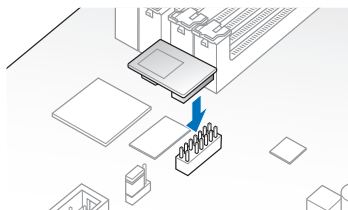
## 2.2 硬體安裝

請依照以下步驟安裝遠端管理卡：

1. 找到主機板上的 ASMB 插座。



2. 將管理卡上的接針插入 ASMB 插座。



主機板結構圖僅供參考。主機板佈局和外觀因型號而異，但安裝步驟是相同的。

3. 按下管理卡，讓它穩穩地安裝在插座上。
4. 將網路線插入 LAN 接頭，以進行伺服器管理。



---

LAN 接頭的位置，請參考附錄說明。

---

5. 若要直接連接 LAN，請將網路線的另一端插入本地 / 中心伺服器的 LAN 接頭。  
若要透過網路集線器或路由器連接，請將網路線的另一端插入集線器或路由器。
6. 確認 VGA、USB、PS/2 線纜都正確連接。然後將電源插頭插入電源插座。



---

每次插入 AC 電源後，請等待 70 秒後再啟動系統。

---

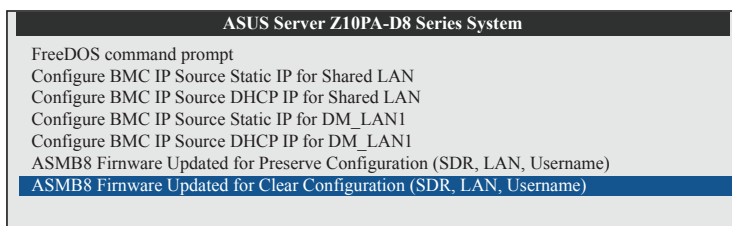
## 2.3 韌體升級與 IP 設定

在開始使用 ASMB8-iKVM 管理卡之前，您需要升級 ASMB8-iKVM 的韌體並設定 IP。

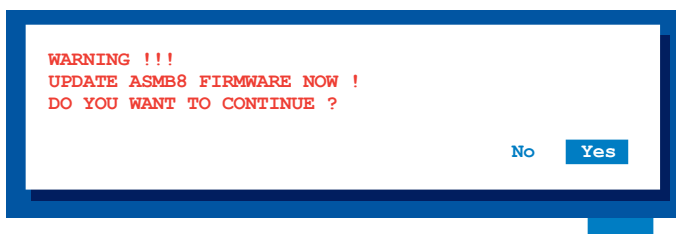
### 2.3.1 韌體升級

請依照以下步驟升級韌體：

1. 將驅動程式與公用程式光碟放入光碟機。
2. 重新啟動系統伺服器，然後在開機自我檢測程序（POST）時按下 <Del>，進入 BIOS 設定。
3. 進入“Boot”選單，將【Boot Device Priority】項目設為 [CD-ROM]。
4. 完成後按下 <F10>，儲存設定並離開 BIOS 設定。
5. 重新啟動系統時，會出現主選單。選擇【ASMB8-iKVM Firmware Update for Preserve Configuration】，然後按下 <Enter> 進入子選單。



6. 此時會出現一條警告訊息，詢問您是否確定要升級韌體，選擇【Yes】進行升級。



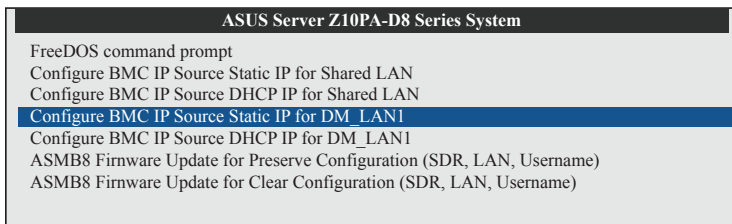
7. 等待韌體升級成功。



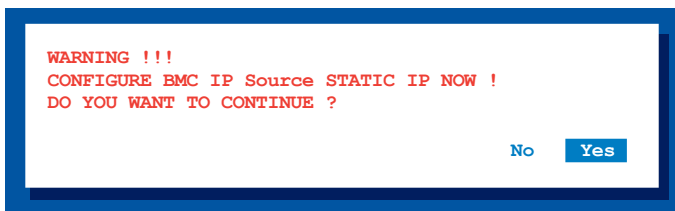
您可以透過網頁使用者介面來升級韌體。請參考“韌體升級”的詳細說明。

### 2.3.2 設定 BMC IP 來源靜態 IP

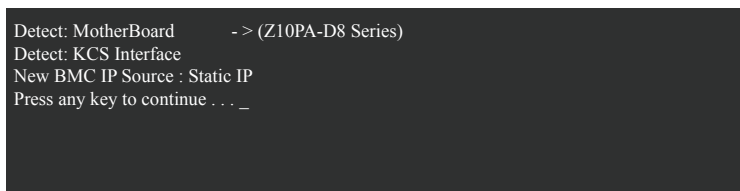
1. 將驅動程式與公程式光碟放入光碟機。
2. 重新啟動系統伺服器，然後在開機自我檢測程序（POST）時按下 <Del>，進入 BIOS 設定。
3. 進入“Boot”選單，將【Boot Device Priority】項目設為 [CD-ROM]。
4. 完成後按下 <F10>，儲存設定並離開 BIOS 設定。
5. 重新啟動系統時，會出現主選單。選擇【Configure BMC IP Source Static IP for Shared LAN（或 DM\_LAN1）】，按下 <Enter> 進入子選單。



6. 此時會出現一條警告訊息，詢問您是否確定要設定 BMC IP 來源靜態 IP，選擇【Yes】繼續。



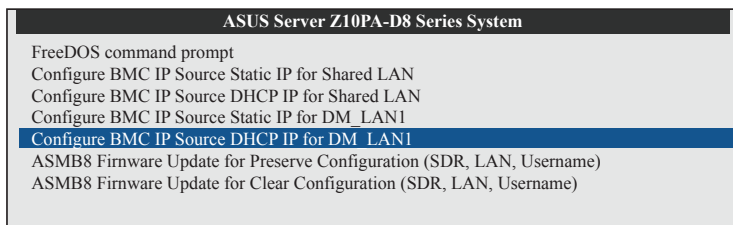
7. 等待設定完成。設定完成後，按任意鍵繼續。



8. 進入 BIOS 選單設定 IP。請參考“2.4 BIOS 設定”部分 IP 設定的說明。

### 2.3.3 設定 BMC IP 來源 DHCP

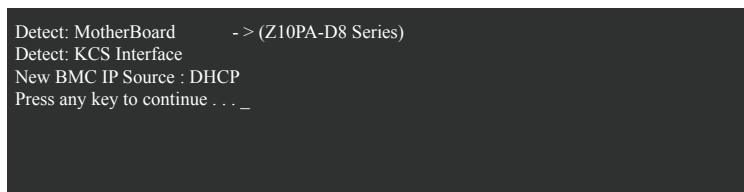
1. 將驅動程式與公用程式光碟放入光碟機。
2. 重新啟動系統伺服器，然後在開機自我檢測程序（POST）時按下 <Del>，進入 BIOS 設定。
3. 進入“Boot”選單，將【Boot Device Priority】項目設為 [CD-ROM]。
4. 完成後按下 <F10>，儲存設定並離開 BIOS 設定。
5. 重新啟動系統時，會出現主選單。選擇【Configure BMC IP Source DHCP for Shared LAN（或 DM\_LAN1）】，按下 <Enter> 進入子選單。



6. 此時會出現一條警告訊息，詢問您是否確定要設定 BMC IP 來源 DHCP，選擇【Yes】繼續。



7. 等待設定完成。設定完成後，按任意鍵繼續。



8. 然後您就可以從 DHCP 伺服器取得 IP。

## 2.4 BIOS 設定

您需要調整遠端伺服器的 BIOS 設定來連接中心伺服器。



- 請根據主機板使用手冊里的說明來升級遠端伺服器的 BIOS。請造訪華碩網站（<http://tw.asus.com>）來下載主機板最新的 BIOS 檔案。
- 本章中的 BIOS 設定畫面僅供參考，可能與您所見到的畫面有所差異。

### 2.4.1 設定 BIOS BMC

請依照以下步驟設定 BMC：

1. 重新啟動遠端伺服器，然後在開機自我檢測程序（POST）時按下 <Del>，進入 BIOS 設定。
2. 進入“Server Mgmt”選單，選擇【BMC network configuration】子選單。使用此選單設定 BMC。
3. 完成後，按下 <F10>，儲存設定並離開 BIOS 設定。

## 2.4.2 BMC 網路設定

此選單中的選項用來設定 BMC LAN 參數。

Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.

MainAdvancedIntelRCSSetupServer MgmtEvent LogsMonitorSecurityBoot ToolExit

BMC Network Configuration

DM\_LAN1

DM LAN1 IP Address in BMC :192.168.254.020

DM LAN1 Subnet Mask in BMC :255.255.255.020

DM LAN1 Gateway Address in BMC :000.000.000.000

DM LAN1 MAC Address in BMC :00.E1.E2.3A020

DM LAN1 MAC Address in BMC :00.E1.E2.3A.3B.3C

Configuration Address Source[Previous State]

Shared LAN

Shared LAN IP Address in BMC :192.168.254.020

Shared LAN Subnet Mask in BMC :255.255.255.020

Shared LAN Gateway Address in BMC000.000.000.000

Shared LAN MAC Address in BMC :00.E1.E2.3A020

Shared LAN MAC Address in BMC :00.E1.E2.3A.3B.3C

Configuration Address Source[Previous State]

Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC)

+ - : Select Screen

↑ ↓ : Select Item

Enter: Selectv

+/- : Change Opt.

F1: General Help

F2: Previous Values

F5: Optimized Defaults

F10: Save & Exit

ESC: Exit

Version 2.15.1236. Copyright (C) 2013 American Megatrends, Inc.

### Configuration Source [Previous State]

本項目用來選擇 IP 地址源類型。將 LAN 通道參數設為靜態或動態。



僅當【Configuration Source】項目設為 [Static] 時，以下項目才會出現。

#### Station IP Address

本項目用來設定 BMC IP 地址。

#### Subnet Mask

本項目用來設定 BMC 子網路遮罩。建議您設定與作業系統的網路相同的子網路遮罩。

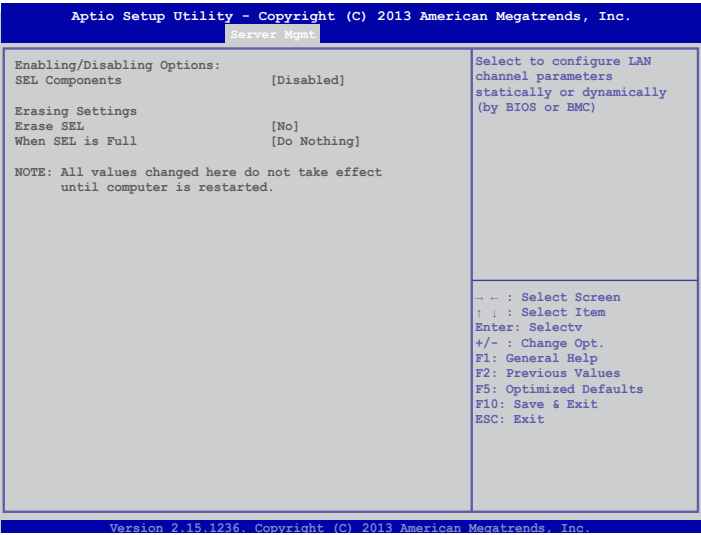
#### Gateway IP Address

本項目用來設定閘道 IP 地址。



2.4.3 系統事件日誌

本項目允許您查看 BMC 事件日誌中的所有事件。讀取所有 BMC SEL 記錄最多會花費 15 秒鐘時間。



SEL Components [Disabled]

本項目用來開啟或關閉啟動時系統事件日誌的所有功能。



僅當【SEL Component】項目設為 [Enabled] 時，以下項目才會出現。

Erase SEL [No]

本項目用來選擇如何清除 SEL。設定值有：[No] [Yes, On next reset] [Yes, On every reset]

When SEL is Full [Do Nothing]

本項目用來選擇您要對全部 SEL 作何操作。設定值有：[Do Nothing] [Erase Immediately]

## 2.4.4 IPv6 BMC 網路設定

顯示 LAN 通道參數，允許您進行 IPv6 BMC LAN 設定。

Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.	
Server Mgmt	
IPv6 BMC Network Configuration	
IPv6 Display Full Field	[Enable]
IPv6 Display Full Formula	[Enable]
IPv6 Display Letter Case	[Upper Case]
IPv6 BMC DM LAN1:	
IPv6 BMC Lan Option	[Enable]
IPv6 BMC Lan IP Address Source	[Previous State]
DM LAN1 IP Address in BMC :	
->	0:0:0:0:0:0:0:0
DM LAN1 Prefix Length in BMC : 0	
DM LAN1 Gateway Address in BMC : 0	
->	0:0:0:0:0:0:0:0
DM LAN1 MAC Address in BMC : 00:E1:E2:3A:3B:3C	
DM LAN1 Address Source in BMC : DHCP Mode	
IPv6 BMC Shared LAN:	
IPv6 BMC Lan Option	[Enable]
IPv6 BMC Lan IP Address Source	[Previous State]
Shared LAN IP Address in BMC :	
->	0:0:0:0:0:0:0:0
Shared LAN Prefix Length in BMC : 0	
Shared LAN Gateway Address in BMC : 0	
->	0:0:0:0:0:0:0:0
Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC)	
-> : Select Screen ! : Select Item Enter: Selectv +/- : Change Opt. F1: General Help F2: Previous Values F5: Optimized Defaults F10: Save & Exit ESC: Exit	
Version 2.15.1236. Copyright (C) 2013 American Megatrends, Inc.	

IPv6 BMC DM LAN1 IP Address Source [Previous State]

本項目用來選擇 IP 地址源類型並將 LAN 通道參數設定為靜態或動態。設定值有：[Previous State] [Static] [Dynamic-Obtained by BMC running DHCP]



---

當您將【IPv6 BMC DM\_LAN1 IP Address Source】設為 [Static] 時，以下項目才會出現。

---

**IPv6 BMC DM\_LAN1 IP Address**

本項目用來設定 IPv6 BMC DM\_LAN1 IP 地址。

**IPv6 BMC DM\_LAN1 IP Prefix Length**

本項目用來設定 IPv6 BMC DM\_LAN1 IP 前綴長度。

**IPv6 BMC DM\_LAN1 Default Gateway**

本項目用來設定 IPv6 BMC DM\_LAN1 閘道 IP 地址。

**IPv6 BMC Shared LAN IP Address Source [Previous State]**

本項目用來選擇 IP 地址源類型並將 LAN 通道參數設為靜態或動態。設定值有：[Previous State] [Static][Dynamic-Obtained by BMC running DHCP]



---

只有當【IPv6 BMC Shared LAN IP Address Source】設為 [Static] 時，以下項目才會出現。

---

**IPv6 BMC Shared LAN IP Address**

本項目用來設定 IPv6 BMC Shared LAN IP 地址。

**IPv6 BMC Shared LAN IP Prefix Length**

本項目用來設定 IPv6 BMC Shared LAN IP 前綴長度。

**IPv6 BMC Shared LAN Default Gateway**

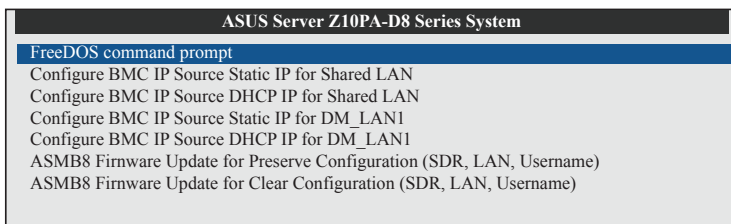
本項目用來設定 IPv6 BMC Shared LAN 閘道 IP 地址。

## 2.5 執行 ASMC8 應用程式

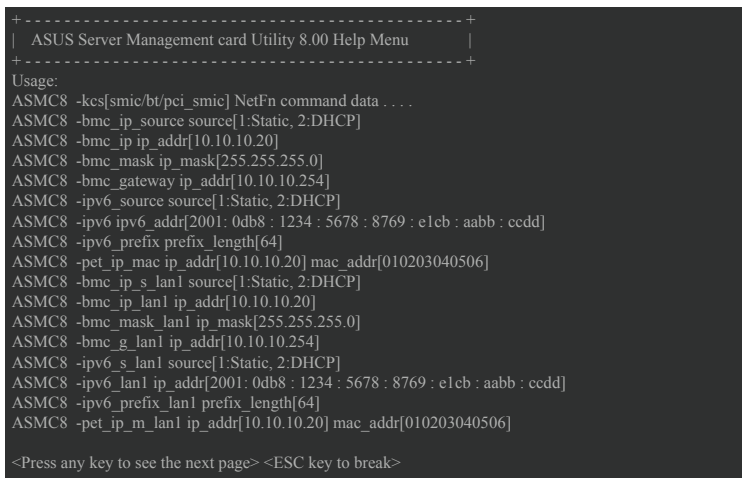
您可以使用 ASMC8 程式來升級 ASMB8-iKVM 韌體、為遠端伺服器設定 LAN，並可在 DOS 環境下變更使用者名 / 密碼。驅動程式與公用程式光碟中包含此程式。

請依照以下步驟執行 ASMC8 應用程式：

1. 將驅動程式與公用程式光碟放入光碟機。
2. 重新啟動遠端伺服器，然後在開機自我檢測程序（POST）時按下 <Del>，進入 BIOS 設定。
3. 進入“Boot”選單，將【Boot Device Priority】項目設為 [CD-ROM]。
4. 完成後按下 <F10>，儲存設定並離開 BIOS 設定。
5. 重新啟動系統時，會出現主選單。選擇【FreeDOS command prompt】然後按下 <Enter> 進入子選單。



6. 當出現 **C:>** 提示符時，輸入 **ASMC8 -?**，然後按下 <Enter> 來顯示 ASMC8 程式幫助選單。畫面如下圖所示。



按任意鍵查看下一頁。

ASMC8 幫助選單項目說明

項目	描述
-kcs[smic/bt/pci_smic] NetFn command data...	發送 IPMI 指令
-bmc_ip_source source[1: Static, 2: DHCP]	設定 IP 來源
-bmc_ip [ip_addr] (e.g., bmc_ip 10.10.10.20)	寫入獨立 LAN 的 BMC IP 地址
-bmc_mask [ip_mask] (e.g., bmc_mask 255.255.255.0)	寫入獨立 LAN 的子網路遮罩
-bmc_gateway [ip_addr] (e.g., bmc_gateway 10.10.10.254)	寫入獨立 LAN 的閘道地址
-pet_ip_mac [ip_addr][mac_addr] (e.g., pet_ip_mac 10.10.10.20 010203040506)	寫入獨立 LAN 的 PET 目標 IP 與 MAC 地址
-bmc_ip_s_lan1 source[1: Static, 2: DHCP]	設定共享 LAN 的 IP 來源
-bmc_ip_lan1 [ip_addr] (e.g., bmc_ip 10.10.10.20)	寫入共享 LAN 的 BMC IP 地址
-bmc_mask_lan1 [ip_mask] (e.g., bmc_mask 255.255.255.0)	寫入共享 LAN 的子網路遮罩
-bmc_g_lan1 [ip_addr] (e.g., bmc_gateway 10.10.10.254)	寫入共享 LAN 的閘道地址
-pet_ip_m_lan1 [ip_addr][mac_addr] (e.g., pet_ip_mac 10.10.10.20 010203040506)	寫入共享 LAN 的 PET 目標 IP 與 MAC 地址
-adm_name new_name_string	變更管理名
-user_name new_name_string	變更使用者名
-adm_password new_adm_password	變更管理密碼
-user_password new_user_password	變更使用者密碼
-sol_baud [baud rate] (e.g., sol_baud 57600)	設定通訊波特率
-bmc_info	顯示 BMC 與 PET IP 與 MAC 地址
-fru -view fru_id	顯示系統 FRU 訊息
-fru -load fru_file	從檔案更新系統 FRU 資料
-fru -save fru_id fru_file	儲存系統 FRU 資料到檔案中
-sel -clear	清除系統事件日誌

## 2.5.1 設定 LAN 控制器

在連接 ASMB8-iKVM 管理卡之前，您必須設定 LAN 接頭，以便讓遠端伺服器連接到本地 / 中心伺服器。

請依照以下步驟設定遠端伺服器的 LAN 接頭：

1. 根據前面部分的說明，執行驅動程式與公用程式光碟中的 ASMC8 應用程式。
2. 設定 IP 來源：
  - (a) 若要設定靜態 IP 地址，請輸入 **ASMC8 -bmc\_ip\_source 1**。
  - (b) 若要從 DHCP 伺服器取得 IP，請輸入 **ASMC8 -bmc\_ip\_source 2**。
3. 輸入 **ASMC8 -bmc\_ip xxx.xxx.xxx.xxx**，然後按下 <Enter> 為遠端伺服器 LAN 接頭指定任何 IP 地址（若有需要）。螢幕會顯示指令與回應緩衝。



---

請將遠端伺服器的 IP 地址寫下來供以後參考。

---

```
c:\>ASMC8 -bmc_ip 10.10.10.243
Detect MotherBoard      -> (Z10PA-D8 Series)
Detect KCS Interface
New BMC IP : 10.10.10.243
c:\>
```

完成後，回到 DOS 畫面。



---

請確認遠端與本地 / 中心伺服器的 IP 地址在同一個子網內。您可以使用作業系統中的網路設定程式來進行確認。

---

4. 若有需要，請設定 (a) 子網路遮罩與 (b) 閘道地址。
  - (a) 輸入 **ASMC8 -bmc\_mask xxx.xxx.xxx.xxx**（您的子網路遮罩在十進制系統中編譯）。
  - (b) 輸入 **ASMC8 -bmc\_gateway xxx.xxx.xxx.xxx**（您的閘道地址在十進制系統中編譯）。
5. 重新啟動遠端伺服器，進入 BIOS 設定，然後從硬碟啟動。
6. 若有需要，請調整本地 / 中心伺服器的網路設定。

## 2.5.2 設定使用者名與密碼

您可以使用 ASMC8 應用程式變更使用者名與密碼。

請依照以下步驟變更使用者名與密碼：

1. 將驅動程式與公用程式光碟放入光碟機。
2. 重新啟動系統伺服器，然後在開機自我檢測程序 (POST) 時按下 <Del>，進入 BIOS 設定。
3. 進入 “Boot” 選單，將【Boot Device Priority】項目設為 [CD-ROM]。
4. 完成後按下 <F10>，儲存設定並離開 BIOS 設定。
5. 重新啟動系統時，會出現主選單。選擇【FreeDOS command prompt】，然後按下 <Enter> 進入子選單。

```
c:\>ASMC8 -user_name super
Detect MotherBoard    -> (Z10PA-D8 Series)
Detect KCS Interface

Change User Name to super
c:\>
```

6. 當 C:> 提示符出現時，輸入 **ASMC8 -user\_name xxxxx**，然後按下 <Enter> 變更使用者名。
7. 輸入 **ASMC8 -user\_password xxxxxxxx** 然後按下 <Enter> 變更密碼。
8. 重新啟動遠端伺服器，進入 BIOS 設定，然後從硬碟啟動。

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



# 華碩主機管理控制器設定

本章介紹如何設定伺服器主機板所支援的華碩主機管理控制器，及如何使用此程式。



## 3.1 華碩主機管理控制器設定 (Host Management Controller Setup)

華碩 Host Management Controller Setup 應用程式能提供準確的設定與基本功能，包括生成 System Event Log (SEL) 與 System Data Record (SDR)。

此應用程式也可用於設定主機介面與系統訊息的即時監控，包括 CPU 溫度、風扇速度與系統電壓。

### 3.1.1 安裝並執行華碩 Host Management Controller Setup 應用程式

請依照以下步驟安裝華碩 Host Management Controller Setup 應用程式：

1. 用驅動程式與公用程式光碟開機進入 DOS 模式。
2. 在彈出的視窗中，輸入 ASMC8，按下 <Enter> 顯示 ASMC8 應用程式幫助選單。畫面如下圖所示。

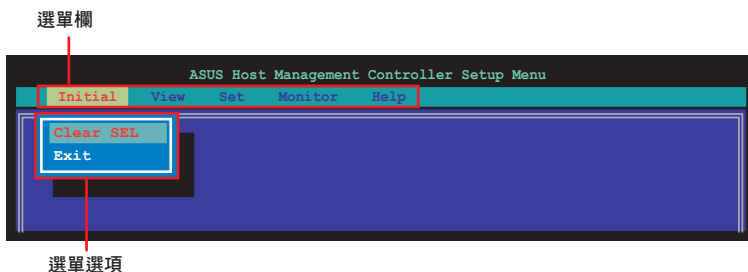
```
C:\>ASMC8
```

3. 程式主畫面出現後，按下 <Enter>。



### 3.1.2 選單欄

應用程式選單欄有五個選單：初始化（Initial）、檢視（View）、設定（Set）、監控（Monitor）與幫助（Help）。您可以使用左 / 右方向鍵進行選擇。進入選單後，使用上 / 下方向鍵顯示設定項目，並按下 <Enter> 進行設定。

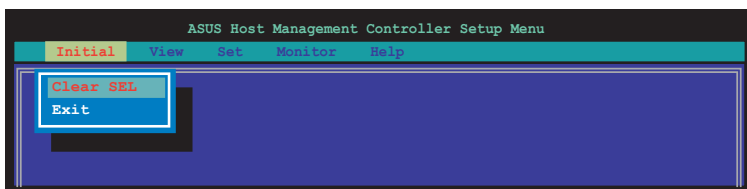


### 3.1.3 初始化（Initial）

【Initial】選項用於清除 SEL 訊息或退出應用程式。

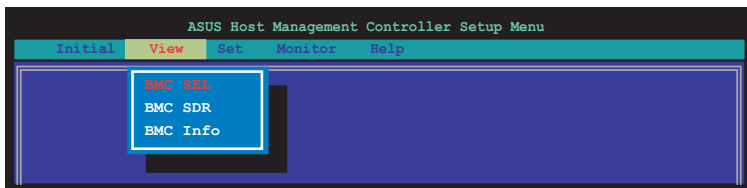
在【Initial】中選擇【Clear SEL】清除所有系統事件日誌訊息。若要建立一個從特定時間開始的新日誌用於監控系統，使用【Clear SEL】。

選擇【Exit】關閉應用程式，並回到 DOS 畫面。



### 3.1.4 檢視（View）

【View】選項顯示底板管理控制器（BMC）資料記錄，包括 System Event Log (SEL)、System Data Record (SDR) 與總體 BMC 訊息。

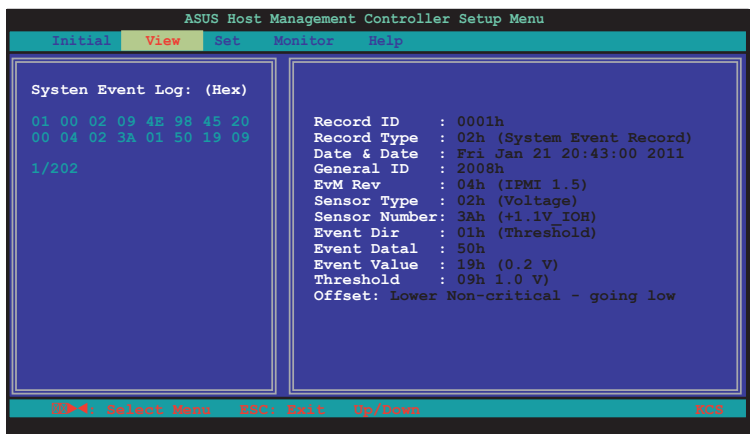


## 查看系統事件日誌（System Event Log，SEL）：

1. 在【View】中選擇【BMC SEL】，按下 <Enter>。左邊顯示系統事件訊息。右邊顯示 SEL 訊息。

視窗左下角的數字表示右邊面板顯示的事件數與遠端主機上系統事件的總數。

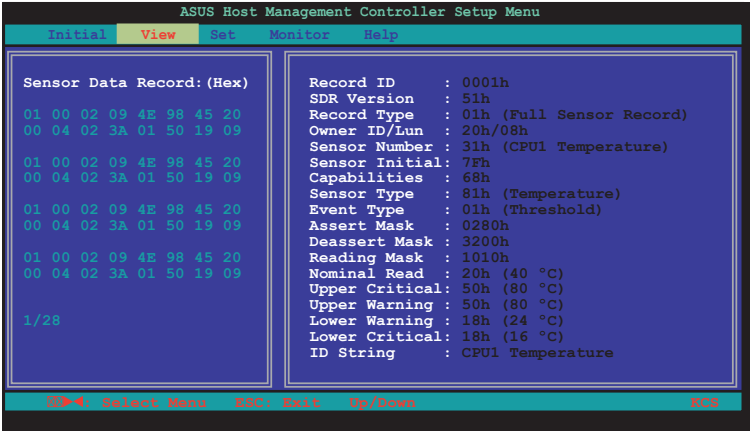
2. 使用向下箭頭往下顯示下一條監控訊息。
3. 完成後按下 <Esc> 回到主畫面。



查看系統資料記錄（System Data Record，SDR）：

- 1. 在【View】中選擇【BMC SDR】，按下 <Enter>。左邊顯示所有資料記錄。右邊顯示監控資料訊息。

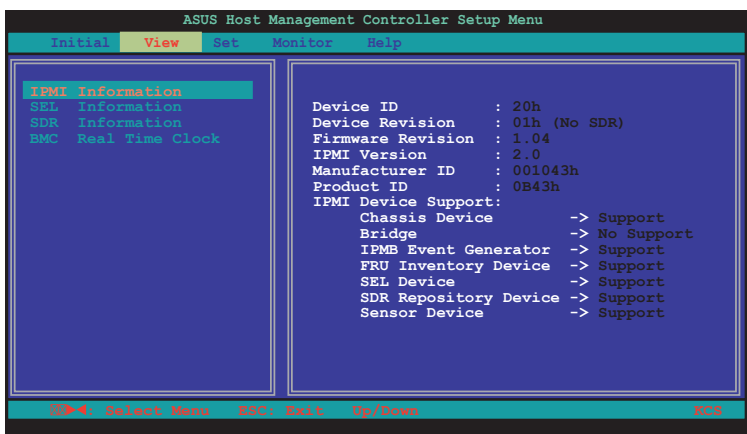
視窗左下角的數字表示右邊面板顯示的資料記錄與遠端主機上監控資料的總數。



- 2. 使用向下箭頭往下顯示下一條監控資料記錄。
- 3. 完成後按下 <Esc> 回到主畫面。

## 查看 BMC 訊息：

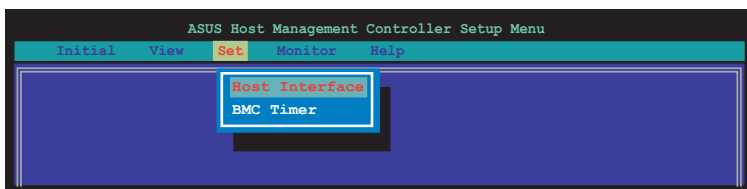
1. 在【View】中選擇【BMC Info】，按下 <Enter>。左邊顯示 BMC 訊息。
2. 使用向下箭頭選擇一條 BMC 訊息，右邊會顯示 BMC 的詳細訊息。



3. 完成後按下 <Esc> 回到主畫面。

## 3.1.5 設定 (Set)

【Set】選項用於控制主機介面類型與正確的 BMC 時間。



### 選擇主機介面：

1. 在【Set】中選擇【Host Interface】，按下 <Enter>。螢幕顯示遠端管理卡支援主機介面。
2. 使用向下箭頭選擇主機介面，按下 <Enter>。



您可以選擇以下主機介面：

KCS Interface	-	鍵盤控制型
SMIC Interface	-	伺服器管理界面晶片
BT Interface	-	Block Transfer
PCI Interface	-	周邊裝置內部接頭
KCS2 Interface	-	鍵盤控制型 2

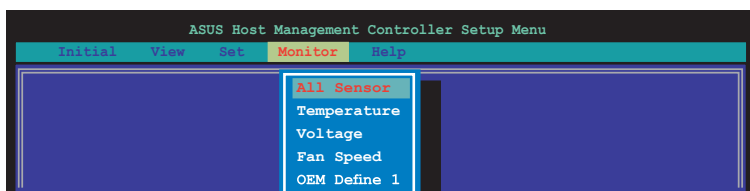
3. 完成後按下 <Esc> 回到主畫面。

### 設定 BMC Timer：

1. 在【Set】中選擇【BMC Timer】，按下 <Enter>。
2. 將 BMC IPMI 時鐘設定為現在的系統時間。
3. 完成後按下 <Esc> 回到主畫面。

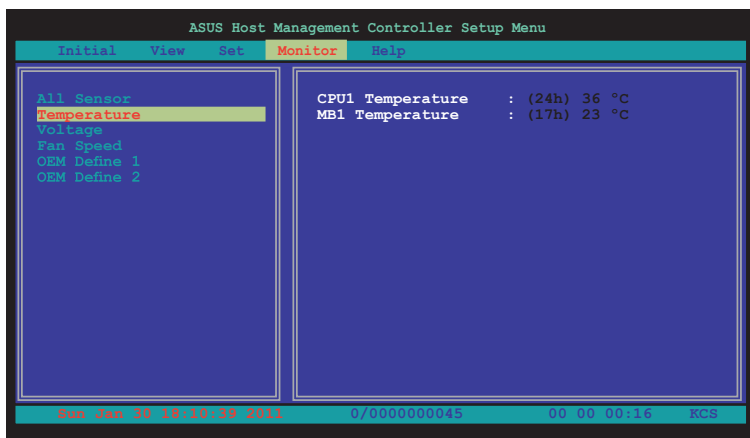
### 3.1.6 監控 (Monitor)

【Monitor】選項顯示遠端伺服器系統的日期與 CPU 溫度、電壓與風扇速度。



顯示遠端伺服器訊息：

1. 在【Monitor】中選擇一個監控器，按下 <Enter>。左邊顯示伺服器訊息。
2. 使用向下箭頭選擇一條監控訊息，右邊會顯示監控的詳細訊息。

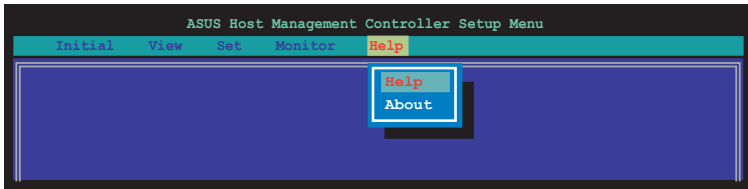


3. 按下 <Esc> 回到主畫面。



### 3.1.7 幫助 (Help)

【Help】選項顯示應用程式選項、版本與版權等訊息。



This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

# 網頁使用者介面

本章介紹如何使用網頁使用者介面來設定與管理伺服器。



## 4.1 網頁使用者介面

網頁使用者介面可幫助您輕鬆地監控遠端伺服器的硬體訊息，包括溫度、風扇速度、電壓與電源。在尚無安裝作業系統的環境下，仍可經由遠端的瀏覽器開啟此圖形介面進行管理的動作。此應用程式也可幫助您快速開啟 / 關閉或重置遠端伺服器。此外，ASMB8-iKVM 所支援之產品皆有提供 ASUS 伺服器管理軟體 ASWM Enterprise，請參閱相關說明書。

按照以下步驟進入網頁使用者介面：

1. 在開機自我檢測程序 (POST) 時進入 BIOS 設定程式。
2. 點選 Advanced > Runtime Error Logging > CPU I/O Bridge Configuration > Launch Storage OpROM，然後按下 <Enter>。
3. 將【Launch Storage OpROM】項目設為 [Enabled]。
4. 點選 Mgmt > BMC network configuration > Configuration Address source，然後按下 <Enter>。
5. 輸入 IP Address in BMC、Subnet Mask in BMC 與 Gateway Address in BMC。
6. 按下 <F10> 儲存更改並離開 BIOS 設定程式。



在使用此網頁管理程式前，請在遠端伺服器上安裝 JRE。您可以在 ASMB8-iKVM 的驅動程式與公用程式光碟中的 JAVA 資料夾中找到 JRE 應用程式。您也可以造訪 <http://www.oracle.com/technetwork/java/javase/downloads/index.html> 來下載 JRE。

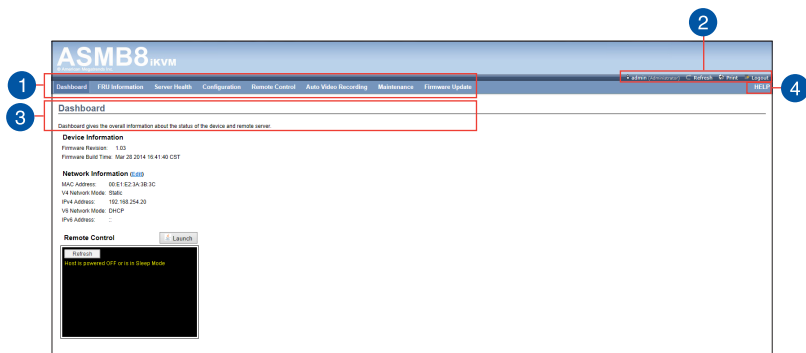
### 4.1.1 登錄應用程式

此網頁圖形介面可支援同時最多 20 位使用者登入，以共同監看與處理問題。

1. 請確認電腦的網路線連接到遠端伺服器的 LAN 接頭中。
2. 打開網頁瀏覽器，輸入與遠端伺服器相同的 IP 地址。
3. 此時出現以下畫面。輸入預設的使用者名 (admin) 和密碼 (admin)。然後點選【Login】(登錄)。

## 4.1.2 使用應用程式

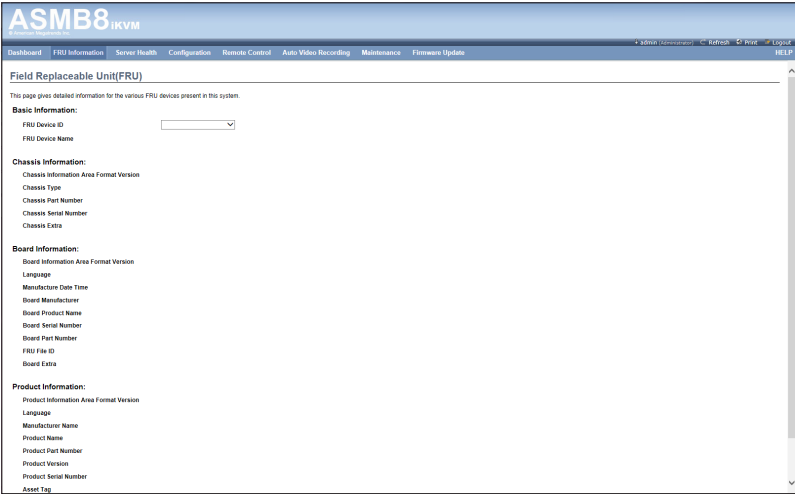
當您成功登錄後，網頁圖形使用者介面將出現。



1. 選單欄：點選選單顯示此選單下的功能列表。
2. 功能列表：點選每個功能鍵開始使用這一功能。
3. 功能名稱：顯示功能名稱。
4. 幫助選單：點選此處顯示所選功能的簡要說明。

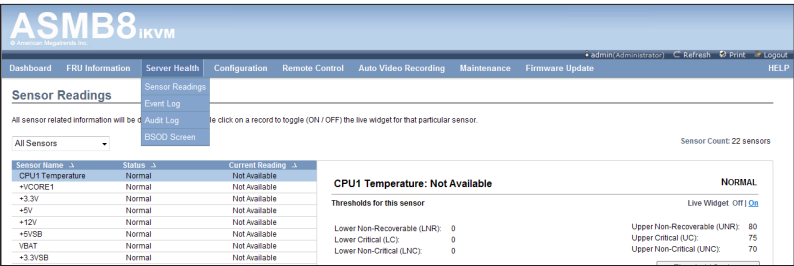
## 4.2 系統訊息（FRU Information）

此部分介紹系統中各個 FRU 裝置的訊息概況。



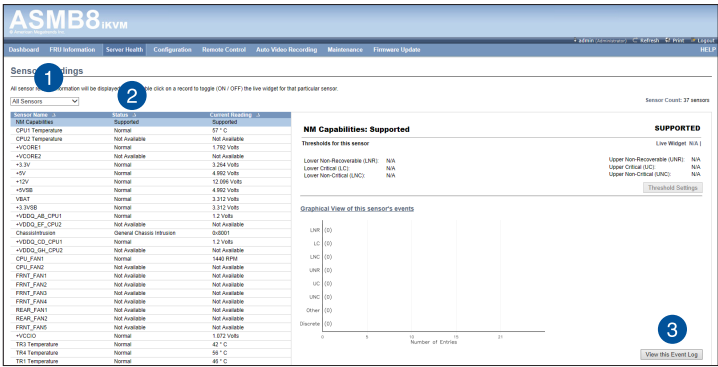
### 4.3 伺服器狀況（Server Health）

此部分顯示與伺服器狀況相關的資料，如監控器訊息與事件日誌。點選每個選項查看此選項的訊息。



#### 4.3.1 監控訊息（Sensor Readings (with Thresholds)）

Sensor Readings 頁面顯示系統監控器訊息，包括監控值與監控狀態。另外，在伺服器主機板或前端面板上有訊息指示燈顯示硬體的異常訊息，可參閱主機板或伺服器相關使用手冊。



- 1. Select a sensor type category：允許您選擇要顯示的監控訊息類型
- 2. Status List：選擇您在下拉列表中選擇的監控訊息列表類型。
- 3. View this Event Log：點選以開啟或關閉 Live Widget 功能。

4.3.2 事件日誌（Event Log）

Event Log 頁面顯示系統事件日誌。當中央處理器、記憶體、背板硬碟等硬體出現異常時，將會記錄在 Event Log 以提示狀況。可參考附錄 A.4 查看讀數的對照表。硬碟訊息所支援之機種型號請見附錄 A.5。

ASMB8iKVM

DashboardFRU InformationServer HealthConfigurationRemote ControlAuto Video RecordingMaintenanceFirmware Update

Event Log

Events generated by the system will be logged here. Double-click on a record to view the description.

All Events

Filter by All Sensors

Event Log: 21 event entries, 1 page(s)

Event ID	Time	Source	Severity	Description
21	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
20	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
19	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
18	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
17	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
16	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
15	04/17/2018 11:52:37	Watchdog 2	Watchdog 2	Timer Expired - Assented
14	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
13	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
12	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
11	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
10	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
9	02/07/2018 01:28:57	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
8	04/16/2018 11:42:26	Watchdog2	Watchdog 2	Timer Expired - Assented
7	01/01/2012 00:07:56	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
6	01/01/2012 00:07:57	Unknown	Microcontroller / Capacitor	Transition to Power Off - Assented
5	02/07/2018 01:28:56	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
4	02/07/2018 01:28:56	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
3	02/07/2018 01:28:56	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
2	02/07/2018 01:28:56	Unknown	Microcontroller / Capacitor	Transition to Running - Assented
1	02/07/2018 01:28:56	Unknown	Microcontroller / Capacitor	Transition to Running - Assented

1

2

Save Event Logs...Clear All Event Logs...

1. Select an event log category：允許您選擇要顯示的事件類型。

2. Clear Event Log：點選清除事件日誌。

4.3.3 審查日誌（Audit Log）

此部分顯示審查事件日誌表。

ASMB8iKVM

DashboardFRU InformationServer HealthConfigurationRemote ControlAuto Video RecordingMaintenanceFirmware Update

Audit Logs

This page displays logs of audit events for this device (if the options have been configured).

Audit Log

UTC Offset: (GMT+08:00)

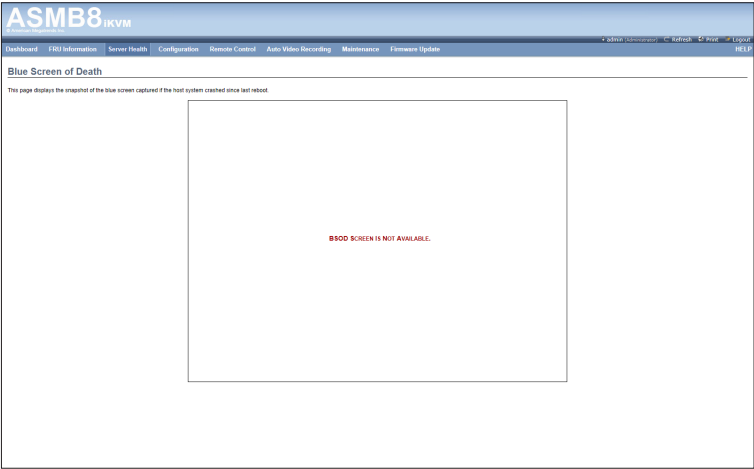
This Filter: 7 event entries

Event ID	Time	Source	Description
1	Jan 1 08:30:16	localhost	webgo: [3014 INF]WEBGUI user admin login successfully from 192.168.254.13
2	Jan 1 08:15:23	localhost	webgo: [3014 INF]WEBGUI logout from 192.168.254.13 user: admin
3	Jan 1 08:49:17	localhost	webgo: [3014 INF]WEBGUI user admin login successfully from 192.168.254.13
4	Jan 1 09:10:11	localhost	webgo: [3014 INF]WEBGUI logout from 192.168.254.13 user: admin
5	Jan 1 10:38:59	localhost	webgo: [3014 INF]WEBGUI user admin login successfully from 192.168.254.13
6	Jan 1 10:39:43	localhost	webgo: [3014 INF]WEBGUI logout from 192.168.254.13 user: admin
7	Jan 1 11:51:01	localhost	webgo: [3014 INF]WEBGUI user admin login successfully from 192.168.254.13



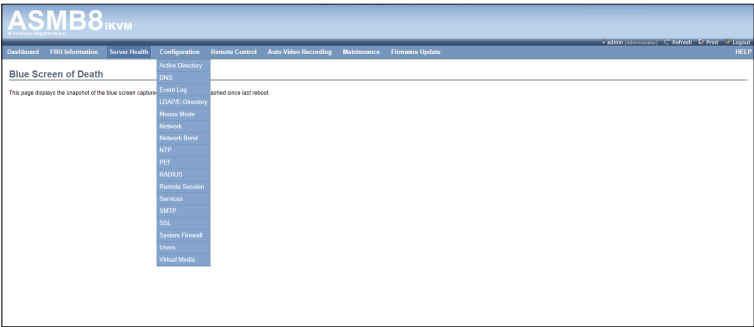
### 4.3.4 藍屏訊息 (BSOD Screen)

此部分顯示當系統崩潰時的藍屏畫面截圖。



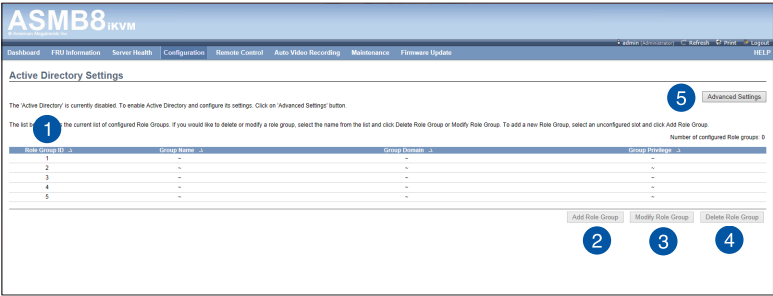
## 4.4 設定（Configuration）

此部分用於對系統進行設定。點選每個選項開始進行設定。



### 4.4.1 Active Directory

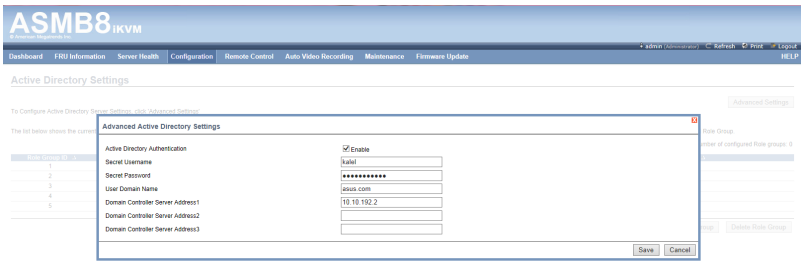
Active Directory 擁有多項功能，包括提供對像訊息、組織對像以便更好地進行造訪、允許使用者與管理員存取、以及允許管理員設定目錄安全。要開啟 Active Directory 設定頁面，從主選單點選【Configuration】>【Active Directory】。Active Directory 設定頁面如下圖所示。



1. Role Group ID：用於識別角色組在 Active Directory 中的的名稱。角色組名稱是一串 255 個數字、字母組成的字串。可使用特殊字符“-”與“\_”。
2. Add Role Group：新增新的角色組至裝置。
3. Modify Role Group：修改角色組。或者，雙擊要設定的插槽。
4. Delete Role Group：刪除已有角色組。
5. Advanced Settings：此項目用來進行 Active Directory 的高級設定。項目有：Enable Active Directory Authentication、User Domain name、Time Out、Domain Controller Server Addresses。

步驟：

- 按以下步驟在 “Advanced Active Directory Settings” 頁面輸入詳細訊息：
1. 點選【Advanced Settings】打開 “Advanced Active Directory Settings” 頁面。



2. 在 “Active Directory Settings” 頁面，輸入以下詳細訊息。
  - Active Directory Authentication：要開啟或關閉 Active Directory，可分別勾選或取消勾選 [Enable]。

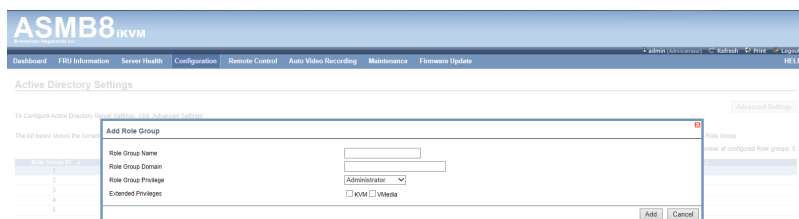


若您已開啟 Active Directory Authentication，請輸入必要的訊息以造訪 Active Directory 伺服器。

- Secret Username：輸入使用者名。
  - Secret Password：輸入密碼。
  - User Domain Name：輸入使用者所在的域名，如 asus.com。
  - IP addresses：在 Domain Controller Server Address1、Domain Controller Server Address2 及 Domain Controller Server Address3 處設定 IP 地址。
3. 點選【Save】儲存設定並返回 “Active Directory Settings” 頁面，或點選【Cancel】取消設定並返回 “Active Directory Settings” 頁面。

## 新增新的角色組 (Role Group)

1. 在 “Active Directory Settings” 頁面，選擇空白行並點選【Add Role Group】打開新增頁面，如下圖所示：



2. 在 “Role Group Name” 區域，輸出角色組在 Active Directory 中的識別名稱。



1. 角色組名稱是一串 255 個字母、數字組成的字符串。
2. 可使用特殊字符 “-” 與 “\_”。

3. 在 “Role Group Domain” 區域，輸入要新增角色組的域名。



1. 域名是一串 255 個字母、數字組成的字符串。
2. 不可使用特殊字符 “-” 與 “\_”。

4. 在 “Role Group Privilege” 區域，輸入該群組的層級。
5. 點選【Add】儲存新的角色組並返回角色組列表。
6. 點選【Cancel】取消設定並返回角色組列表。

## 修改角色組 (Role Group)

1. 在 “Active Directory Settings” 頁面，選擇您要修改的行並點選【Modify Role Group】。
2. 做必要的修改，然後點選【Save】。

## 刪除角色組 (Role Group)

在 “Active Directory Settings” 頁面，選擇您要刪除的行並點選【Delete Role Group】。

### 4.4.2 DNS

此頁面用來管理裝置的 DNS 設定。

ASMB8iKVM

Dashboard | FIDO Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Updates

ASMB8-iKVM-000000000000 | Refresh | GET Ping | Logout | HELP

DNS Server Settings

Manage DNS settings of the device.

Domain Name Service Configuration

DNS Service

☒ Enable

Multicast DNS

mDNS Settings

☐ Enable

Host Configuration

Host Settings

Automatic

Host Name

ASMB8-iKVM-000000000000

Register BMC

DM\_LAN1

☒ Register BMC

☒ Noupdate

☐ DHCP Client FQDN

☐ Hostname

LAN1

☒ Register BMC

☒ Noupdate

☐ DHCP Client FQDN

☐ Hostname

TSG Configuration

TSG Authentication

☐ Enable

Current TSG Private File

Not Available

New TSG Private File

Browse

Domain Name Configuration

Domain Settings

LAN1\_v4

Domain Name

Domain Name Server Configuration

DNS Server Settings

LAN1

IP Priority

☒ IPv4

☐ IPv6

DNS Server1

DNS Server2

DNS Server3

Save | Reset

### 4.4.3 Event Log

此頁面用來設定系統事件記錄訊息。

ASMB8iKVM

Dashboard | FIDO Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Updates

ASMB8-iKVM-000000000000 | Refresh | GET Ping | Logout | HELP

System Event Log

This page is used to configure the System Event log information.

Current Event Log Policy : LINEAR

☐ Enable Linear Event Log Policy

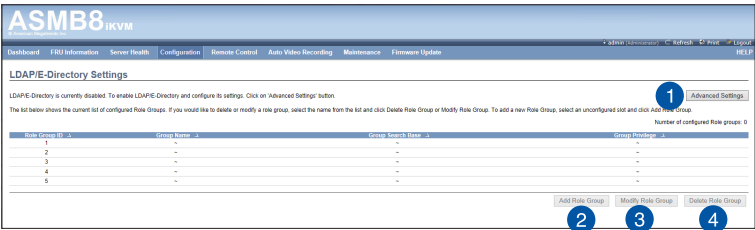
☐ Enable Circular Event Log Policy

Save | Reset

### 4.4.4 LDAP/E-Directory

“Lightweight Directory Access Protocol” (LDAP) 是一項應用協議，用來查詢並修改 Internet Protocol (IP) 網路中的目錄服務的日期。若您的網路中有一台已配置的 LDAP 伺服器，您可以使用它方便地新增、管理並驗證 MegaRAC® 卡使用者。這是透過把登錄請求轉交給 LDAP 伺服器來完成的。這也表示當使用 MegaRAC 卡時無需再定義附加的驗證機製。因為您現有的 LDAP 伺服器保留了驗證功能，您時刻知道哪些使用者在使用網路資源，並且可以方便地定義使用者或群組規則來進行存取控制。

從主選單點選【Configuration】>【LDAP】來打開 LDAP 設定頁面。LDAP 設定頁面如下圖所示。

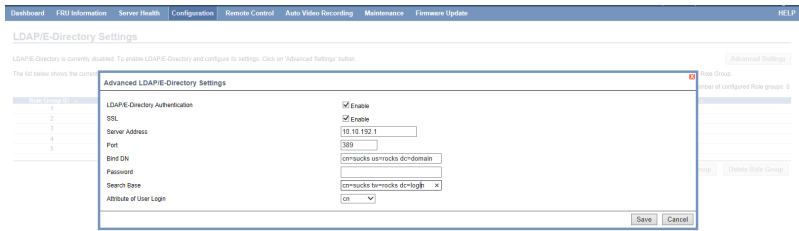


1. Advanced Settings：設定 LDAP 高級設定。項目有：Enable LDAP Authentication、IP Address、Port and Search base。
2. Add Role Group：新增一個新的角色組至裝置。或者，雙擊空的插槽來新增角色組。
3. Modify Role Group：修改指定的角色組。
4. Delete Role Group：從列表中刪除角色組。

步驟：

在 “Advanced LDAP Settings” 頁面輸入詳細訊息：

- 1. 在 LDAP 設定頁面，點選【Advanced Settings】。LDAP 設定頁面如下圖所示。



- 2. 要開啟或關閉 LDAP Authentication，勾選或取消勾選 [Enable]。



在登錄的彈出視窗中，輸入使用者名以 Idap Group 成員登錄。

- 3. 在 “IP Address” 區域輸入 LDAP 伺服器的 IP 地址。



- 1. IP 地址是由 . 分隔的四組數字 “xxx.xxx.xxx.xxx”。
- 2. 每組數字的範圍為 0 至 255。
- 3. 第一組數字必須為 0。
- 4. 支援 IPv4 地址格式與 IPv6 地址格式。

- 4. 在 “Port” 區域設定 LDAP 端口。



預設端口為 389。安全連接預設端口為 636。

- 5. 輸入 Search Base。Search base 告訴 LDAP 伺服器搜索外部目錄樹的哪一部分。search base 與外部目錄的組織、群組類似。
- 6. 點選【Save】儲存設定。
- 7. 點選【Cancel】取消更改。

## 新增新的角色組

1. 在 LDAP 設定頁面，選擇空的行並點選【Add Role Group】打開“Add Role group”頁面。
2. 在“Role Group Name”區域，輸入角色組名稱。
3. 在“Role Group Search Base”區域，輸入角色組的位置路徑。



- 
1. Search Base 是一串 255 個數字、字母組成的字串。
  2. 不可使用特殊字符“-”與“\_”。
- 

4. 在“Role Group Privilege”區域，輸入指定到此群組的權限層級。
5. 點選【Add】儲存新的角色組並返回角色組列表。
6. 點選【Cancel】取消設定並返回角色組列表。

## 修改角色組

1. 在 LDAP 設定頁面，選擇您要修改的行，然後點選【Modify Role Group】。
2. 進行修改，然後點選【Save】。

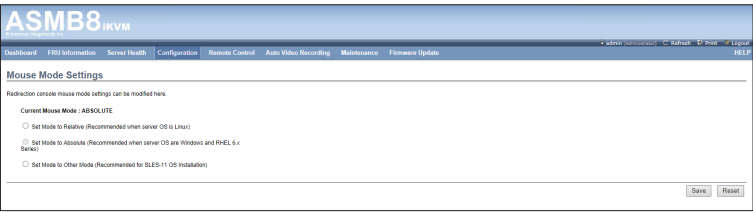
## 刪除角色組

在 LDAP 設定頁面，選擇您要刪除的行，然後點選【Delete Role Group】。



### 4.4.5 滑鼠模式 (Mouse Mode)

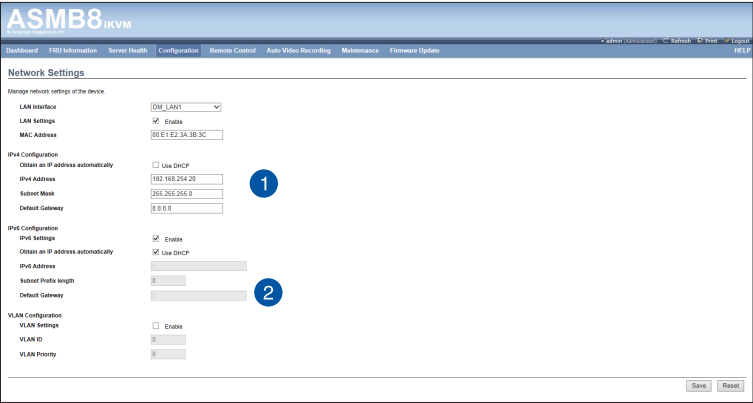
Mouse Mode 頁面用於選擇滑鼠模式。



1. Save：選擇想要的滑鼠模式，然後點選【Save】儲存設定。

### 4.4.6 網路 (Network)

Network 頁面用於設定網路。



1. MAC Address：選擇自動取得或手動設定 IP。
2. IP Address/Subnet Mask/Default Gateway：若您設定靜態 IP，在相關區域內輸入 IP 地址、子網路遮罩與閘道。

### 4.4.7 Network Bond

此頁面用來開啟或關閉 networking bonding 功能，以及設定預設界面。



### 4.4.8 NTP

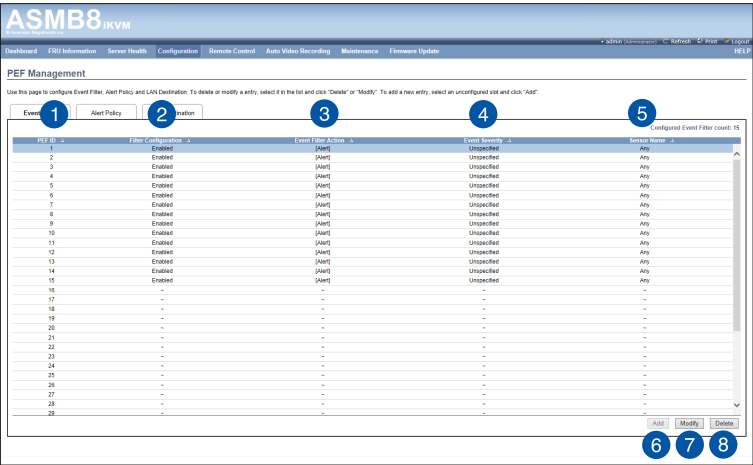
此頁面用來設定 NTP 伺服器或查看並修改裝置的時間與日期設定。



### 4.4.9 PEF

Platform Event Filtering (PEF) 提供一套機制來設定 BMC 以對它收到的或內部生成的事件訊息採取選擇性的動作。這些動作包括如系統關機、重新啟動系統、生成警報等。執行 PEF 需建議在事件過濾表中提供至少 16 個條目。這些條目應先預置以應對常見的系統失敗事件，如系統過熱、系統啟動失敗、風扇錯誤等。

要打開 PEF Management Settings 頁面，從主選單點選【Configurations】>【PEF】。PEF Management Settings 頁面如下圖所示。



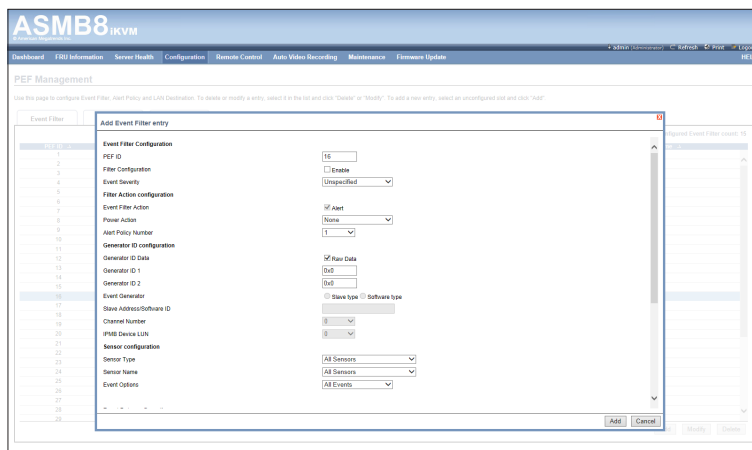
### Event Filter 標籤頁

建議您使用 PEF implementation，在事件過濾表中提供至少 16 個條目。這些條目的子集應針對常見的系統失敗事件（如過熱、供電系統失敗、風扇失敗等）進行預設。

1. PEF ID：此區域顯示新設定的 PEF 條目（只讀）事件的 ID。
2. Filter configuration：勾選以開啟 PEF 設定。
3. Event Filter Action：勾選以開啟 PEF 警報。此項為強制項目。
4. Event Severity：從列表中選擇任一事件嚴重性。
5. Sensor Name：從列表中選擇感應器。
6. Add：新增新的事件過濾條目並返回“Event filter”列表。
7. Modify：修改已有條目。
8. Cancel：取消修改並返回“Event filter”列表。

## 步驟：

1. 點選“Event Filter”標籤頁在可用的插槽上設定事件過濾器。
2. 要新增事件過濾條目，選擇一個空的插槽，然後點選【Add】打開新增事件過濾器頁面。如下圖所示：



3. Event Filter Configuration 部分：
  - PEF ID 顯示設定的 PEF 條目（只讀）的 ID。
  - 在過濾器設定頁面，勾選開啟 PEF 設定。
  - 在“Event Severity”中選擇任一事件嚴重性。
4. Filter Action configuration 部分：
  - Event Filter Action 為強制項目，預設為開啟，開啟 PEF 警報（只讀）。
  - 從下拉列表中選擇任一電源動作：Power down、Power reset 或 Power cycle。
  - 從下拉列表中選擇任一已設定的 Alert Policy 號碼。



點選【Configuration】->【PEF】->【Alert Policy】設定 Alert Policy。

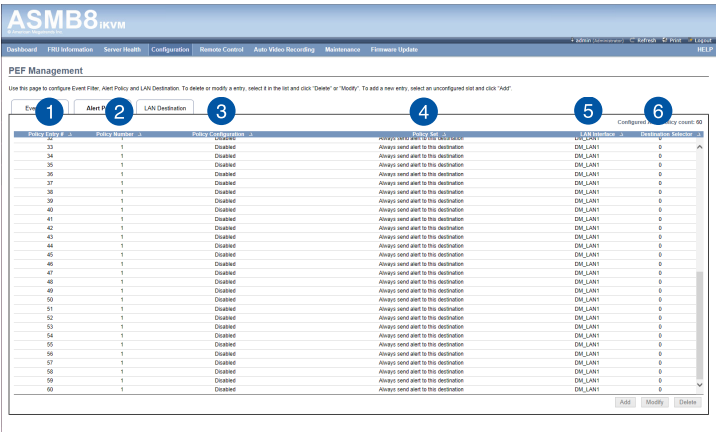
5. Generator ID configuration 部分：
  - 勾選 Generator ID Data 項目用 RAW 資料填充 Generator ID。
  - Generator ID 1 區域用於設定 raw generator ID1 資料。
  - Generator ID 2 區域用於設定 raw generator ID2 資料。



在 RAW 資料的區域，用“0x”設定十六進制值前綴。

Alert Policy 標籤頁

此頁用於設定 Alert Policy 與 LAN destination。您可以在此頁面中新增、刪除或修改條目。



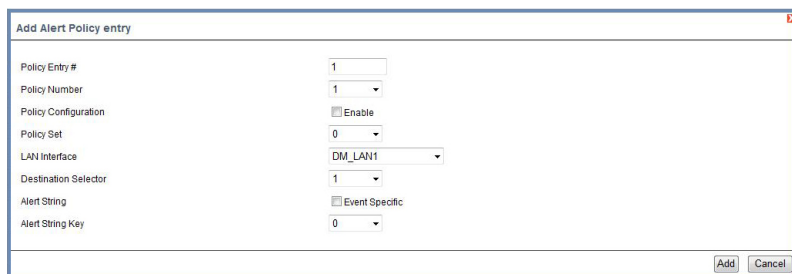
- PEF Management - Alert Policy 標籤頁說明如下。
- 1. Policy Entry #：顯示新設定的 Policy 條目（只讀）編號。
  - 2. Policy Number：顯示設定的 Policy 編號。
  - 3. Policy Configuration：開啟或關閉 Policy 設定。
  - 4. Policy Set：從此列表中選擇任一 Policy 設定。
    - 0 - 總是發送警報至此目的地。
    - 1 - 若發送警報至前一個目的地成功，不需發送警報至此目的地。繼續執行這個 Policy 設定中的下一個條目。
    - 2 - 若發送警報至前一個目的地成功，不需發送警報至此目的地。繼續執行這個 Policy 設定中的其他條目。
    - 3 - 若發送警報至前一個目的地成功，不需發送警報至此目的地。繼續執行這個 Policy 設定中針對不同通道的下一個條目。
    - 4 - 若發送警報至前一個目的地成功，不需發送警報至此目的地。繼續執行這個 Policy 設定中針對不同目的地類型的下一個條目。
  - 5. LAN Interface：從可用的通道列表中選擇一個特定的通道。
  - 6. Destination Selector：從已設定的目的地列表中選擇一個特定的目的地。



進入 Configuration -> PEF -> LAN Destination 設定 LAN Destination。

7. Add：儲存新的警報規則並返回 Alert Policy 列表。
8. Modify：修改已存在的條目。
9. Cancel：取消更改並返回 Alert Policy 列表。

## 步驟：



1. 在 Alert Policy 標籤頁中，選擇您要設定警報規則的插槽。例如，在 Event Filter Entry 頁面中，若您選擇了第 4 條 Alert Policy，您必須設定第四插槽（Policy 編號為 4 的插槽）。
2. 選擇插槽並點選 Add 打開 Add Alert Policy Entry 頁面。
3. Policy Entry # 為只讀區域。
4. 從列表中選擇 Policy Number。
5. 在 Policy Configuration 區域，若您想開啟規則設定則勾選 Enable。
6. 在 Policy Set 區域，從列表中選擇任一 Policy 設定。
7. 在 LAN Interface 區域，從可用的通道列表中選擇特定的通道。
8. 在 Destination Selector 區域，從已設定的目的地列表中選擇特定的目的地。



進入 Configuration -> PEF -> LAN Destination 設定 LAN Destination。例如，在 Alert Policy Entry 頁面中，若您選擇了第 4 個目的地，您必須設定第四插槽（LAN Destination 編號為 4 的插槽）。

9. 在 Alert String 區域，勾選 Event Specific。
10. 在 Alert String Key 區域，選擇任一設定值，用來查看為這個 Alert Policy 發送的 Alert String。
11. 點選 Add 儲存新的警報規則並返回 Alert Policy 列表。
12. 點選 Cancel 取消更改並返回 Alert Policy 列表。
13. 在 Alert Policy 列表中，要更改設定，先選擇要更改的插槽，然後點選 Modify。
14. 在 Modify Alert Policy Entry 頁面中，進行必要的更改，然後點選 Modify。
15. 在 Alert Policy 列表中，要刪除設定，先選擇插槽，然後點選 Delete。

## PEF 管理 LAN Destination 設定頁面

此頁面用來設定 Event filter、Alert Policy 與 LAN destination。設定頁面如下圖所示。

ASMB8iKVM

Dashboard | FRI Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Update

Admin Management | Mailbox | PEF | Logout | Help

PEF Management

Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete an entry, select it in the list and click "Delete" or "Delete". To add a new entry, select an unconfigured slot and click "Add".

Event Filter | Alert Policy | LAN Destination

LAN Interface: LAN1

Configured LAN Destination count: 0

LAN Destination ID	Destination Type	Destination Address
1	-	-
2	-	-
3	-	-
4	-	-
5	-	-
6	-	-
7	-	-
8	-	-
9	-	-
10	-	-
11	-	-
12	-	-
13	-	-
14	-	-
15	-	-

Send Test Alert | Add | Modify | Delete

PEF Management - LAN Destination 標籤頁說明如下。

- LAN Destination：顯示新設定條目（只讀）的目的地編號。
- Destination Type：目的地類型可以是一個 SNMP Trap 或一個 Email 提醒。若是 Email 提醒，需要設定 3 項內容 - 目的地 Email 地址、主題與內容正文。另外還需要新增 SMTP 伺服器訊息 - 進入 Configuration -> SMTP 進行設定。若是 SNMP Trap，只需設定目的地 IP 地址。
- Destination Address：若目的地類型為 SNMP Trap，輸入將收到警報的系統 IP 地址。目的地地址支援以下格式：
  - IPv4 地址格式
  - IPv6 地址格式若目的地類型為 Email 提醒，輸入將收到電子郵件的 Email 地址。
- Subject & Message：若目的地類型為 Email 提醒，則必須設定此項目。發送的郵件將會包含特定主題與正文內容。
- Add：儲存新的 LAN 目的地並返回 LAN Destination 列表。
- Cancel：取消更改並返回 LAN Destination 列表。



## 步驟：



1. 在 LAN Destination 標籤頁中，選擇您要設定的插槽。此插槽必須與您在 Alert Policy Entry- Destination Selector 中選擇的相同。例如，您在 Alert Policy 標籤頁的 Alert Policy Entry 頁面中將 Destination Selector 選擇為 4，那麼您必須設定 LAN Destination 頁面的第四插槽。
2. 選擇插槽並點選 Add 打開 Add LAN Destination Entry 頁面。
3. 在 LAN Destination 區域，會顯示新設定條目的目的地，且為只讀。
4. 在 Destination Type 區域選擇類型。
5. 在 Destination Address 區域，輸入目的地地址。

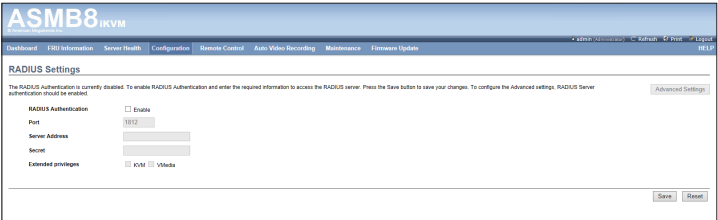


注意：若目的地類型為 Email 提醒，輸入將收到電子郵件的 Email 地址。

6. 從使用者列表中選擇 User Name。
7. 在 Subject 區域，輸入主題。
8. 在 Message 區域，輸入內容。
9. 點選 Add 儲存新的 LAN 目的地並返回 LAN Destination 列表。
10. 點選 Cancel 取消更改並返回 LAN Destination 列表。
11. 在 LAN Destination 標籤頁中，要更改設定，先選擇要更改的行，然後點選 Modify。
12. 在 Modify LAN Destination Entry 頁面中，進行必要的更改，然後點選 Modify。
13. 在 LAN Destination 標籤頁中，要刪除設定，先選擇插槽，然後點選 Delete。

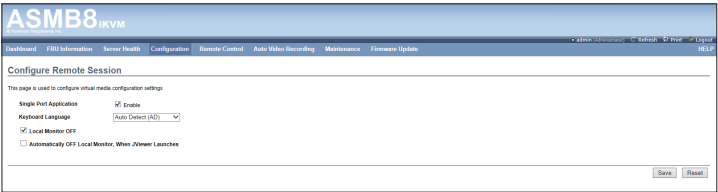
### 4.4.10 RADIUS

此頁面用來開啟或關閉 RADIUS 驗證，並輸入所需訊息來造訪 RADIUS 伺服器。



### 4.4.11 遠端會話（Remote Session）

Remote Session 頁面用來開啟或關閉 KVM 或重定向會話時的資料加密。



1. Single Port Application：勾選以開啟。
2. Keyboard Language：從下拉列表中選擇鍵盤語言。
3. Local Monitor OFF：勾選以開啟或關閉。
4. Automatically OFF Local Monitor, When JViewer Launches：勾選以開啟或關閉。
5. Save：儲存當前更改。



若出現任何問題，它將自動關閉當前存在的 KVM 或虛擬媒體會話的遠端重定向。

6. Reset：重置更改的內容。

### 4.4.12 服務 (Services)

此頁面中列出了在 BMC 上執行的服務。顯示服務的當前狀態和其他基本訊息。點選【Modify】修改服務設定。

ASMB8iKVM

Dashboard | FPD Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Update

Services

Below is a list of services running on the BMC. It shows current status and other basic information about the services. Select a slot and press "Modify" button to modify the services configuration.

Number of Services: 7

Slot	Service Name	Current State	User Name	Access Point IP	Service Port	Endpoint IP	Message	Response	Action
1	web	Active	both	80	443	192.168.1.1	200	200	Modify
2	ssh	Active	both	22	22	192.168.1.1	200	200	Modify
3	ipmi	Active	both	600	600	192.168.1.1	200	200	Modify
4	ipmi	Active	both	600	600	192.168.1.1	200	200	Modify
5	ipmi	Active	both	600	600	192.168.1.1	200	200	Modify
6	ipmi	Active	both	600	600	192.168.1.1	200	200	Modify
7	ipmi	Inactive	both	600	600	192.168.1.1	200	200	Modify

### 4.4.13 SMTP

SMTP 頁面用來設定 SMTP 郵件伺服器。輸入郵件伺服器的 IP 地址，然後點選【Save】應用設定。

ASMB8iKVM

Dashboard | FPD Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Update

SMTP Settings

Manage SMTP settings of the device.

LAN Channel Number

1

Sender Address

Machine Name

Primary SMTP Server

SMTP Support

☒ Enable

Port

25

Server Address

☐ SMTP Server requires Authentication

User Name

Password

Secondary SMTP Server

SMTP Support

☐ Enable

Port

25

Server Address

☐ SMTP Server requires Authentication

User Name

Password

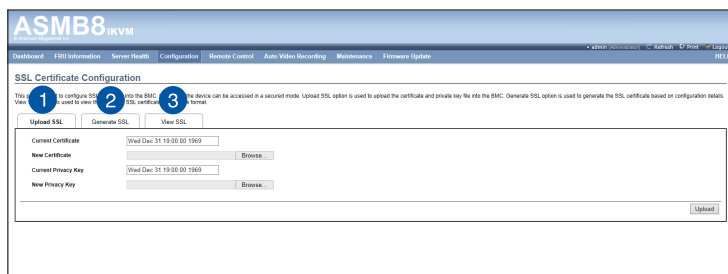
Save

Reset

## 4.4.14 SSL

SSL (Secure Socket Layer) 協議為 Netscape 所研發，用以保障網路伺服器與瀏覽器之間的傳輸。協議使用第三方 CA (Certificate Authority) 認證來識別傳輸的一端或兩端。

從主選單點選【Configuration】>【SSL】打開“SSL Certificate Configuration”頁面。此頁面有三個標籤頁。



1. 【Upload SSL】項目可用於上傳證書與私人密鑰文件至 BMC。
2. 【Generate SSL】項目用於依據設定訊息生成 SSL 證書。
3. 【View SSL】項目用於查看已上傳的 SSL 證書。

**ASMB8 iKVM**  
Remote Access

Dashboard | FRU Information | Server Health | **Configuration** | Remote Control | Auto Video Recording | Maintenance | Firmware Update

admin (Administrator) | Refresh | CF Drive | Logout | HELP

### SSL Certificate Configuration

This page is used to configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode. Upload SSL option is used to upload the certificate and private key file into the BMC. Generate SSL option is used to generate the SSL certificate based on configuration details. View SSL option is used to view the uploaded SSL certificate in readable format.

Upload SSL | **Generate SSL** | View SSL

Current Certificate	Wed Dec 31 19:00:00 1969
New Certificate	<input type="text"/> Browse
Current Privacy Key	Wed Dec 31 19:00:00 1969
New Privacy Key	<input type="text"/> Browse

SSL Certificate Configuration - Upload SSL 標籤頁說明如下。

1. Current Certificate：顯示當前證書訊息（只讀）。
2. New Certificate：要上傳的證書，證書須為 pem 類型。
3. Current Privacy Key：顯示當前隱私密鑰訊息（只讀）。
4. New Privacy Key：新隱私密鑰，須為 pem 類型。
5. Upload：上傳 SSL 證書與隱私密鑰至 BMC。



上傳成功後，HTTPS 服務將會使用新上傳的 SSL 證書開啟。

**ASMB8 iKVM**  
Remote Access

Dashboard | FRU Information | Server Health | **Configuration** | Remote Control | Auto Video Recording | Maintenance | Firmware Update

admin (Administrator) | Refresh | CF Drive | Logout | HELP

### SSL Certificate Configuration

This page is used to configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode. Upload SSL option is used to upload the certificate and private key file into the BMC. Generate SSL option is used to generate the SSL certificate based on configuration details. View SSL option is used to view the uploaded SSL certificate in readable format.

Upload SSL | **Generate SSL** | View SSL

Common Name(CN)	<input type="text"/>
Organization(O)	<input type="text"/>
Organization Unit(OU)	<input type="text"/>
City or Locality(L)	<input type="text"/>
State or Province(ST)	<input type="text"/>
Country(C)	<input type="text"/>
Email Address	<input type="text"/>
Valid for	<input type="text"/> days
Key Length	512 bits

SSL Certificate Configuration - Generate SSL 標籤頁說明如下。

1. Common Name(CN)：證書生成名稱。
  - 最長 64 字符。
  - 不可使用特殊字符 “#” 與 “\$”。

2. Organization(O)：生成證書的組織名稱。
  - 最長 64 字符。
  - 不可使用特殊字符 “#” 與 “\$”。
3. Organization Unit(OU)：生成證書的組織單位。
  - 最長 64 字符。
  - 不可使用特殊字符 “#” 與 “\$”。
4. City or Locality(L)：組織所在城市（必填）。
  - 最長 64 字符。
  - 不可使用特殊字符 “#” 與 “\$”。
5. State or Province(ST)：組織所在州/省（必填）。
  - 最長 64 字符。
  - 不可使用特殊字符 “#” 與 “\$”。
6. Country(C)：組織所在國家代碼（必填）。
  - 僅允許兩個字符。
  - 不可使用特殊字符。
7. Email Address：組織電子郵件地址（必填）。
8. Valid for：證書有效期。
  - 有效期為 1 至 3650 天。
9. Key Length：證書位長。
10. Generate：生成新的 SSL 證書。



---

HTTPS 服務將會使用新上傳的 SSL 證書開啟。

---

**ASMB8 iKVM**

Dashboard FQDN Information Service Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update

### SSL Certificate Configuration

This page is used to configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode. Upload SSL option is used to upload the certificate and private key file into the BMC. Generate SSL option is used to generate the SSL certificate based on configuration details. View SSL option is used to view the uploaded SSL certificate in readable format.

Upload SSL Generate SSL View SSL

<b>Basic Information</b>	
Version	3
Serial Number	89F7D4C2D5A4A4EC2
Signature Algorithm	sha1024RSAEncryption
Public Key	(1024 bit)
<b>Issued From</b>	
Common Name(CN)	ASB
Organization(O)	American Megatrends Inc.
Organization Unit(OU)	Service Processors
City or Locality(L)	Atlanta
State or Province(ST)	Georgia
Country(C)	US
Email Address	support@ami.com
<b>Validity Information</b>	
Valid From	Sep 12 09:36:47 2009 GMT
Valid To	Jan 29 09:36:47 2010 GMT
<b>Issued To</b>	
Common Name(CN)	ASB
Organization(O)	American Megatrends Inc.
Organization Unit(OU)	Service Processors
City or Locality(L)	Atlanta
State or Province(ST)	Georgia

SSL Certificate Configuration - Generate SSL 標籤頁說明如下。

1. Basic Information：此部分顯示有關已上傳 SSL 認證的基本訊息，有以下內容：
  - Version
  - Serial Number
  - Signature Algorithm
  - Public Key
2. Issued From：此部分描述認證方訊息。
  - Common Name(CN)
  - Organization(O)
  - Organization Unit(OU)
  - City or Locality(L)
  - State or Province(ST)
  - Country(C)
  - Email Address
3. Validity Information：此部分顯示已上傳認證的有效期。
  - Valid From
  - Valid To

4. Issued To：此部分顯示認證方訊息。

- Common Name(CN)
- Organization(O)
- Organization Unit(OU)
  - City or Locality(L)
  - State or Province(ST)
  - Country(C)
  - Email Address

### 步驟：

1. 點選 Upload SSL 標籤頁，瀏覽 New Certificate 與 New Privacy key。
2. 點選 Upload 上傳新的證書與隱私密鑰。
3. 在 Generate SSL 標籤頁中輸入以下詳細訊息。
  - Common Name，證書名稱
  - Name of the Organization，組織名稱
  - Overall Organization Section Unit，組織單位
  - City or Locality，組織所在城市
  - State or Province，組織所在州（省）
  - Country，組織所在國家
  - email address，組織電子郵件地址
  - Valid For，證書有效時間
4. 選擇 Key Length，設定證書的位元值。
5. 點選 Generate 生成證書。
6. 點選 View SSL 標籤頁以使用者可讀的格式查看已上傳 SSL 證書。

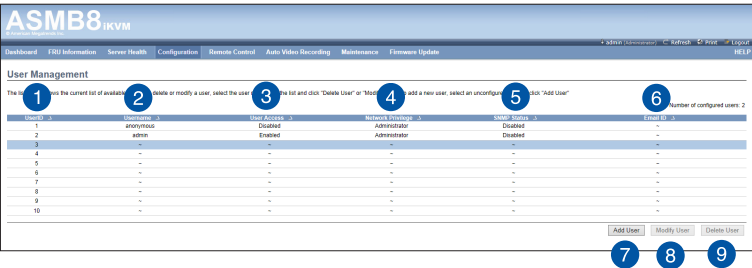


- 
1. 上傳或生成證書後，僅開啟 HTTP 服務。
  2. 您現在可以安全地造訪您的 MegaRAC® SP，請使用以下鏈接：  
`https://<您的 MegaRAC® SP 的 IP 地址>`
  3. 例如，若您的 MegaRAC® SP 的 IP 地址為 192.168.0.30，則輸入  
`https://192.168.0.30`
  4. 請注意 <http> 後的 <s>。在造訪 MegaRAC® SP 前，您必須接受證書。
-



### 4.4.15 使用者 (Users)

“User Management” 頁面中可查看伺服器的當前使用者插槽。您可以新增使用者、修改或刪除已存在的使用者。“User Management” 頁面如下圖所示。



1. User ID：顯示使用者的 ID 號碼。注意：列表最多只能包含 10 個使用者。
2. User Name：顯示使用者名稱。
3. User Access：開啟或關閉使用者的存取權限。
4. Network Privilege：顯示使用者的網路存取權限。
5. SNMP Status：顯示使用者的 SNMP 狀態是否為開啟或關閉。
6. Email ID：顯示使用者的電子郵件地址。
7. Add User：新增一個新使用者。
8. Modify User：修改已存在的使用者。
9. Delete User：刪除已存在的使用者。

#### 新增新使用者：

1. 要新增一個新使用者，選擇一個空的插槽並點選【Add User】。
2. 在“User Name”區域輸入使用者的名稱。
3. 在“Password”與“Confirm Password”區域，輸入並確認您的密碼。
4. 密碼長度必須為 8-20 個字符，且不可使用空格。

- 5 開啟或關閉 User Access Privilege.
6. 在“Network Privilege”區域，輸入使用者的網路權限：Administrator（管理員）、Operator（操作員）、User（使用者）或 No Access（無權限）。
7. 勾選“SNMP Status”復選框為使用者開啟 SNMP 權限。注意：若 SNMP Status 開啟，則必須設定密碼。
8. 從“SNMP Access”下拉選單中為使用者選擇 SNMP 存取層級：Read Only（只讀）或 Read Write（讀寫）。
9. 從下拉列表中選擇 SNMP 設定使用的 Authentication Protocol。注意：若 Authentication 協議改變，則必須設定密碼。
10. 從“Privacy protocol”下拉選單中選擇 SNMP 設定使用的 Encryption algorithm。
11. 在“Email ID”區域，輸入使用者的電子郵件帳號。若使用者忘記密碼，新密碼會透過郵件的方式寄至此電子郵件帳號。  
AMI-Format：此郵件格式的主題為“Alert from (your Hostname)”。此郵件的內容顯示游標訊息：游標類型與描述。  
Fixed-Subject Format：此格式會依據使用者設定顯示相關訊息。您必須設定郵件警告的主題與訊息。
12. 在“New SSH Key”區域，點選【Browse】並選擇 SSH 密鑰文件。注意：SSH 密鑰文件應為 pub 類型。
13. 點選【Add】儲存新使用者並返回使用者列表頁面。
14. 點選【Cancel】取消修改並返回使用者列表頁面。

### 修改已有使用者

1. 從列表中選擇一個使用者，並點選【Modify User】。
2. 編輯需要的內容。
3. 要改變密碼，開啟【Change Password】項目。
4. 修改完成後，點選【Modify】返回使用者列表頁面。

### 刪除已有使用者

要刪除使用者，先從列表中選擇使用者，然後點選【Delete User】。

### 4.4.16 虛擬媒體 (Virtual Media)

以下選項可讓您設定虛擬媒體裝置。您可以選擇支援各種虛擬媒體裝置的數量。

ASMB8iKVM

Dashboard | F80 Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Update

ASMB8-iKVM v1.0000 | Help

Virtual Media Devices

The following option will allow to configure virtual media devices. Below, you can select the number of instances that are supported for each type of virtual media device.

Floppy Drives

2

CD/DVD devices

2

Hard disk devices

2

Power Save Mode

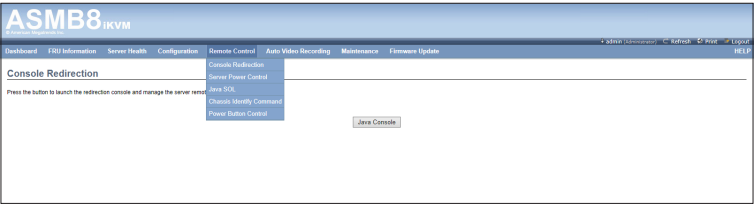
☒ Enable

Save

Reset

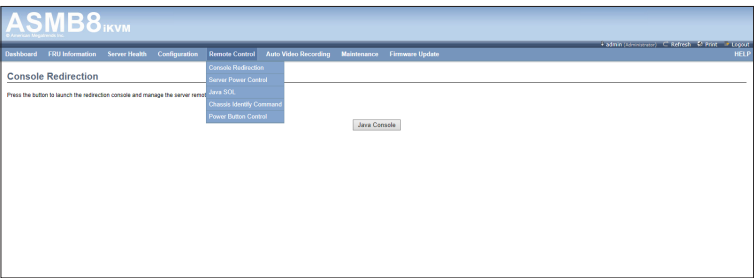
## 4.5 遠端控制（Remote Control）

此部分允許您對伺服器進行遠端操作。點選每個選項開始進行設定。



### 4.5.1 Console Redirection

遠端控制台應用程式，使用網頁圖形使用者介面，可遠端控制伺服器的作業系統、使用螢幕、滑鼠與鍵盤，以及重定向本地 CD/DVD、磁片與硬碟/USB 隨身碟，如同這些裝置是直接連接在伺服器上。此遠端控制台可以支援同時 2 位使用者開啟畫面，由優先開啟的使用者取得鍵盤與滑鼠控制，並可選擇是否轉移控制權給另一位使用者。



### 瀏覽器設定

若開啟 KVM，需解除對彈出視窗的阻止。若使用 Internet explorer，從設定中開啟下載文件項目。

## Java Console：

這是一個獨立於作業系統的插件，可在 JRE 的輔助下在 Windows 與 Linux 中使用。客戶端系統中需安裝 JRE。您可以從以下鏈接安裝 JRE：<http://www.java.com/en/download/manual.jsp>

兩種方法開啟 Java Console：

1. 打開 Dashboard 頁面，在 Remote control 部分點選 Launch for Java Console。
2. 打開 Remote Control > Console Redirection 頁面，點選 Java Console。

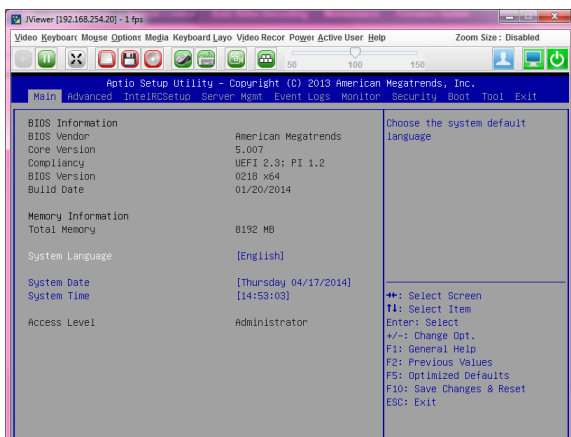
將從 BMC 下載 .jnlp 文件。

要開啟 .jnlp 文件，使用適當的 JRE 版本（Javaws）下載完成後，Console Redirection 視窗開啟。

Console Redirection 主選單包含以下項目：

- 視訊（Video）
- 鍵盤（Keyboard）
- 滑鼠（Mouse）
- 選項（Options）
- 媒體（Media）
- 鍵盤概觀（Keyboard Layout）
- 視訊記錄（Video Record）
- 電源（Power）
- 活動中的使用者（Active User）
- 幫助（Help）

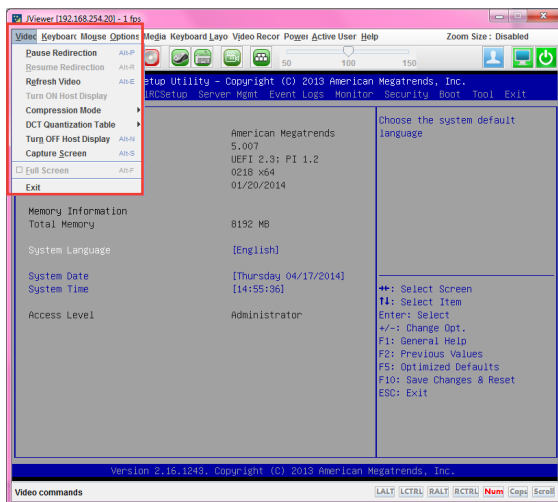
關於這些選單的詳細說明請參考以下部分。



## 視訊 (Video)

此選單包含以下子項目：

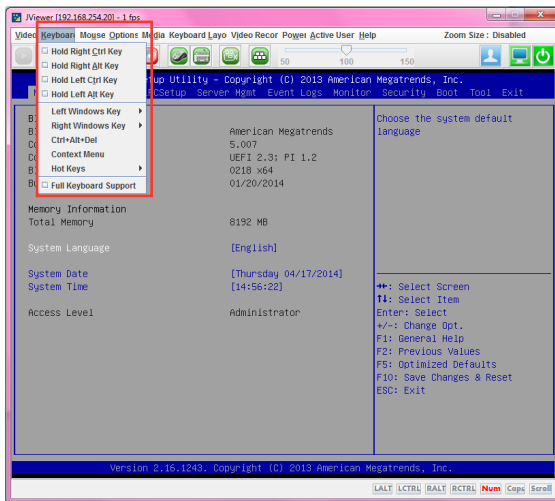
1. Pause redirection：此項目用來暫停 Console Redirection。
2. Resume Redirection：此項目用來當會話暫停時重新開始 Console Redirection。
3. Refresh Video：此項目用來更新 Console Redirection 視窗的顯示內容。
4. Turn ON Host display：若您開啟此選項，顯示畫面將回到伺服器螢幕。
5. Compression Mode：此項目用來設定視訊中的壓縮設定。
6. DCT Quantization Table：此項目用來設定質量，範圍從 0（最差）到 7（最佳質量）。
7. Turn OFF Host display：若您開啟此選項，伺服器顯示將為空白，但您可以在 Console Redirection 中查看螢幕。
8. Capture Screen：本項目可讓您截取 console redirection 畫面。
9. Exit：此項目用來退出 console redirection 畫面。



## 鍵盤 (Keyboard)

此選單包含以下子項目：

1. Hold Right Ctrl Key：在 Console Redirection 中此項目實現右邊 <CTRL> 鍵功能。
2. Hold Right Alt Key：在 Console Redirection 中此項目實現右邊 <ALT> 鍵功能。
3. Hold Left Ctrl Key：在 Console Redirection 中此項目實現左邊 <CTRL> 鍵功能。
4. Hold Left Alt Key：在 Console Redirection 中此項目實現左邊 <ALT> 鍵功能。
5. Left Windows Key：在 Console Redirection 中此項目實現左邊 <WIN> 鍵功能。您也可以決定按鍵的方式：長按或按下後放開。
6. Right Windows Key：在 Console Redirection 中此項目實現右邊 <WIN> 鍵功能。您也可以決定按鍵的方式：長按或按下後放開。
7. Alt+Ctrl+Del：此項目等同於當您在重定向時同時按下伺服器上的 <CTRL>、<ALT> 與 <DEL> 鍵。
8. Context menu：在 Console Redirection 中此項目實現 context 選單功能。
9. Hot Keys：本選單項目可讓您將常用的鍵新增為熱鍵。
10. Full Keyboard support：勾選本項目以支援完全鍵盤。

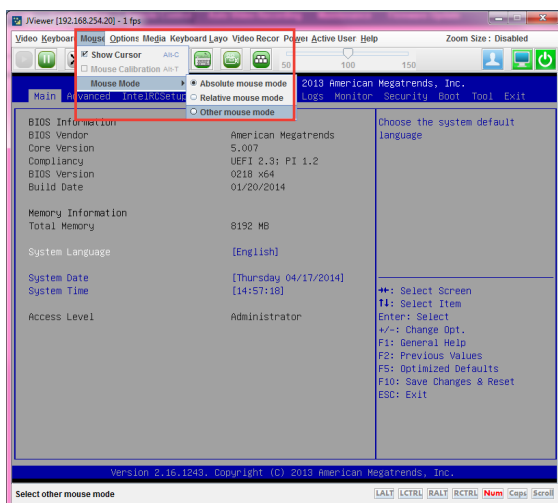


## 滑鼠 (Mouse)

1. Show Cursor：此項目用來顯或隱藏遠端客戶端系統中的本地滑鼠游標。
2. Mouse Calibration：只有當滑鼠模式時此項目才可用。

在此步驟中，遠端伺服器上的滑鼠閾值設定會被發現。本地滑鼠的游標以紅色顯示，遠端游標為遠端視訊畫面中的一部分。兩個游標都會在一開始便同步。請使用“+”或“-”鍵來改變閾值設定，直到兩個游標不同步。請偵測第一個使兩個游標不同步的閾值。偵測到後，使用 'ALT-T' 儲存閾值。

3. Mouse Mode：此選單項目可讓您選擇滑鼠支援的模式或類型。





## 選項 (Options)

Band width：Bandwidth Usage 項目用來調整頻寬。您可以選擇以下項目：

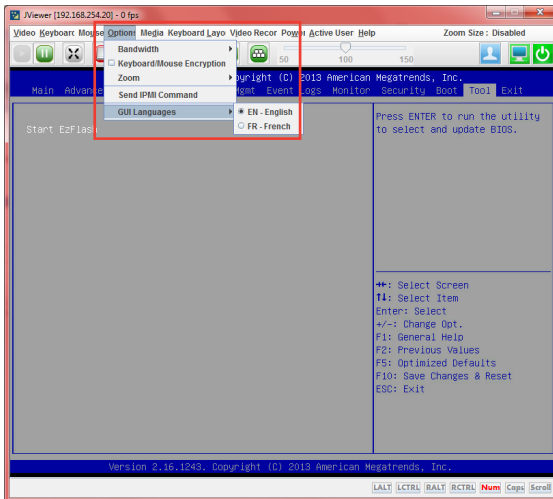
1. Auto Detect：此項目用來自動偵測客戶端鍵盤分布，並依據偵測到的訊息發送主要事件至主機。
2. 256Kbps
3. 512Kbps
4. 1Mbps
5. 10Mbps
6. 100Mbps

Keyboard/Mouse Encryption：此項目用來加密鍵盤輸入和滑鼠移動。

## 縮放 (Zoom)：

只有當 Java Console 開啟時此項目才可用。

1. Zoom In：放大畫面尺寸。放大範圍為 100% 到 150%，以 10% 為增量。
2. Zoom Out：縮小畫面尺寸。縮小範圍為 100% 到 50%，以 10% 為增量。



## 媒體（Media）

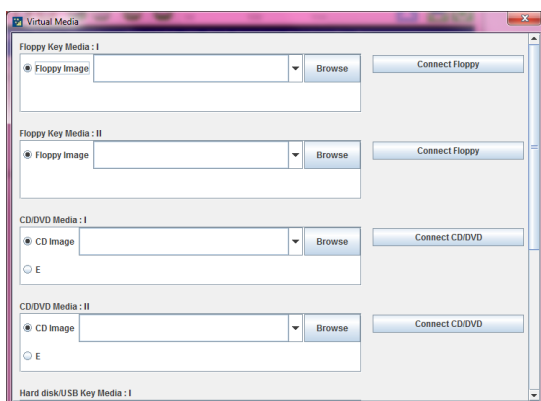
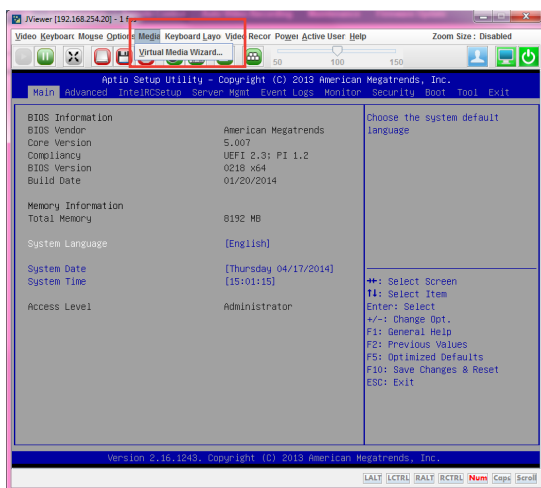
Virtual Media Wizard：

要新增或修改媒體，選擇並點選 Virtual Media Wizard 按鈕，然後會彈出一個名為“Virtual Media”的視窗，可以設定媒體。Virtual Media 畫面如下圖所示。

Floppy Key Media：此項目用來開始或停止物理軟碟機裝置與軟碟機圖片類型（如 img）的重定向。

CD/DVD Media：此項目用來開始或停止物理 DVD/CD-ROM 光碟機與 cd 圖片類型（如 iso）的重定向。

Hard disc/USB Key Media：此項目用來開始或停止 Hard Disk/USB 與 USB 圖片（如 img）的重定向。

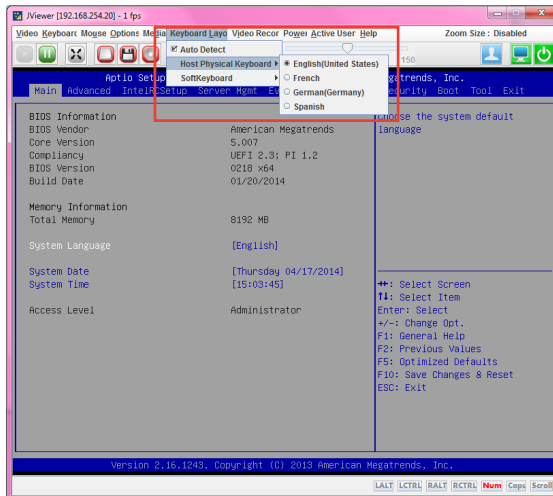


虛擬媒體向導

## 鍵盤概觀（Keyboard Layout）

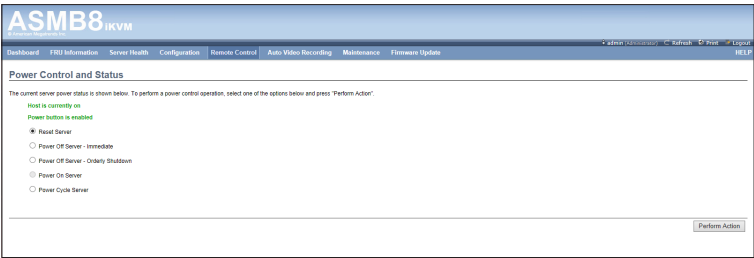
**Auto Detect：**此項目用來自動偵測鍵盤分布。語言自動支援 英語 - 法語 - 西班牙語 - 德語 - 日語。若客戶端與主機的語言相同，那麼除英語外，以上所有語言都必須選擇此項目以避免輸入錯誤。

**Soft Keyboard：**此項目用來選擇鍵盤分布。螢幕中會顯示一個如鍵盤一樣的對話框。若客戶端與主機的語言不同，那麼除英語外，以上所有語言都必須在 JViewer 中的列表中選擇適當的語言並使用軟鍵盤以避免輸入錯誤。注意：軟鍵盤只適用於 JViewer 應用程式，並不適用於客戶端系統。



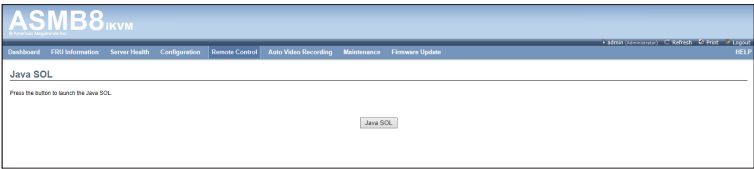
### 4.5.2 伺服器電源管理（Server Power Control）

“Server Power Control” 頁面顯示現在伺服器電源狀態，並允許您變更當前的設定。請選擇您想要的項目，然後點選【Perform Action】執行選擇的操作。



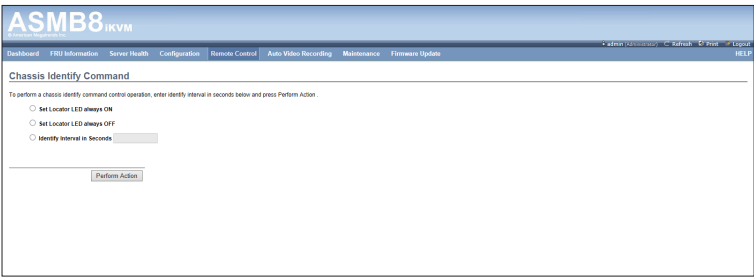
### 4.5.3 Java SOL

“Java SOL” 頁面可讓您開啟 Java SOL 應用程式。



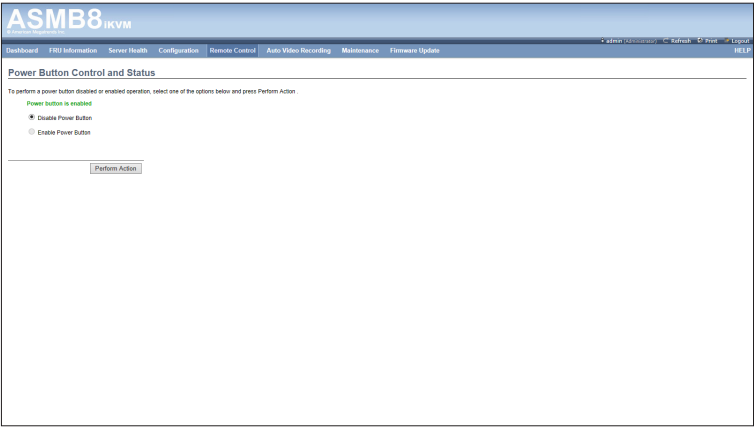
### 4.5.4 機殼識別指令（Chassis Identify Command）

在 “Chassis Identify Command” 頁面中您可以執行控制機殼識別指令。點選【Perform Action】執行命令。



### 4.5.5 電源按鈕（Power Button）

“Power Button” 頁面允許您開啟或關閉電源按鈕，然後點選【Perform Action】確認選擇。



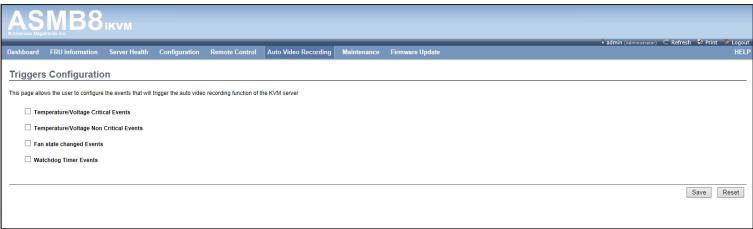
## 4.6 自動錄影（Auto Video Recording）

此部分允許您設定可以觸發 KVM 伺服器自動錄影功能的事件，並將已錄製的視訊文件顯示在 BMC 中。



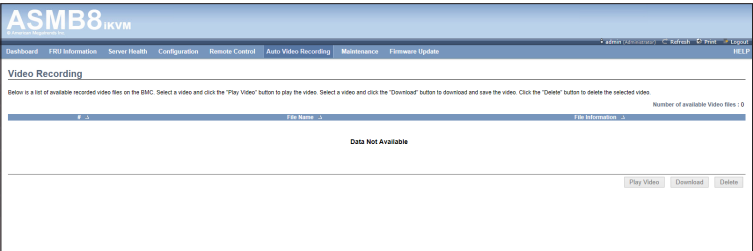
### 4.6.1 觸發器設定（Triggers Configuration）

本頁面允許您設定可觸發 KVM 伺服器自動錄影功能的事件。



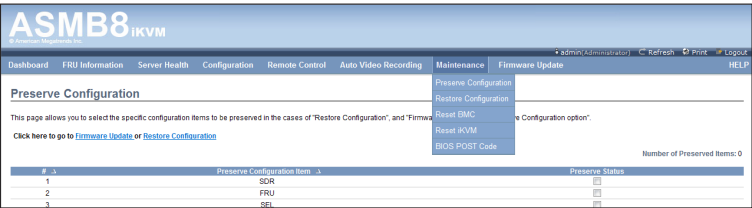
### 4.6.2 已錄製視訊（Recorded Video）

此部分在 BMC 中顯示已錄製視訊文件列表，並可播放、下載、儲存或刪除選定的視訊。



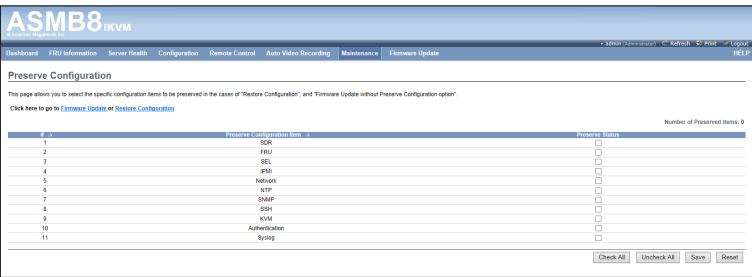
## 4.7 維護（Maintenance）

此部分用來為遠端伺服器進行保留設定，恢復出廠預設值，或進行韌體升級。



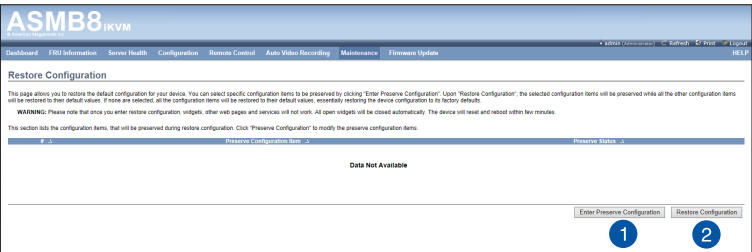
### 4.7.1 保留設定（Preserve Configuration）

本頁面可讓您選擇特定的項目作為保留設定，當執行恢復出廠設定或韌體升級時，這些設定會被保留。



### 4.7.2 恢復出廠預設值

此部分用來恢復所有出廠預設值。



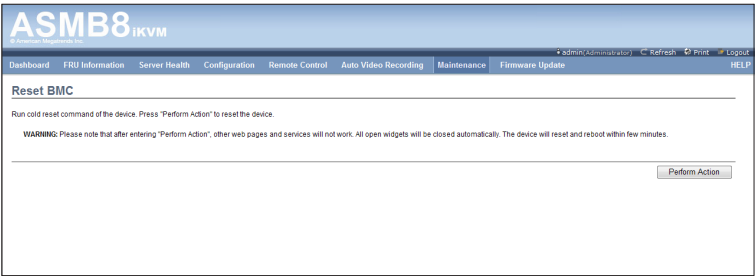
1. Enter Preserve Configuration：點選以選擇需保留的設定。
2. Restore Configuration：已選擇的設定將被保留，其他設定將被恢復為預設值。若您沒有選擇保留設定，則所有設定將恢復成它們的預設值，裝置將完全恢復為出廠預設狀態。

### 4.7.3 BMC 重置 (Reset BMC)

本頁面可讓您執行裝置的冷啟動命令。



注意：進入【Perform Action】後，其他網頁及服務將無法使用。所有開啟的小部件將自動關閉。裝置將重置並在數分鐘內重新啟動。

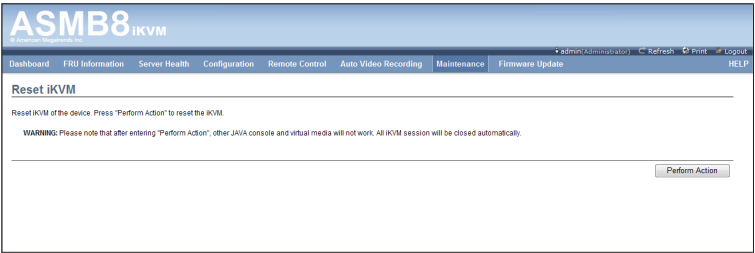


### 4.7.4 iKVM 重置 (Reset iKVM)

本頁下面可讓您重置裝置的 iKVM。

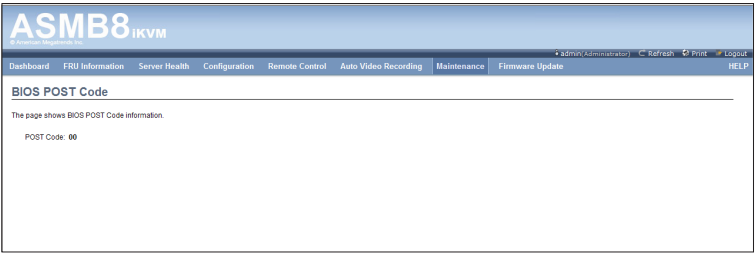


注意：進入【Perform Action】後，其他 JAVA 終端與虛擬媒體將無法使用。所有的 iKVM 會話將被自動關閉。



### 4.7.5 BIOS 開機自我檢測程序代碼 (BIOS POST Code)

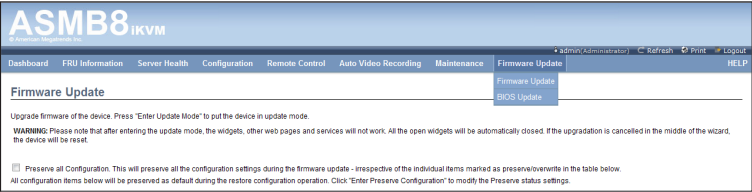
本頁面顯示上一次的 BIOS 開機自我檢測程序代碼訊息。





# 4.8 韌體升級 (Firmware Update)

此部分可進入升級模式並升級 ASMB8 的韌體。

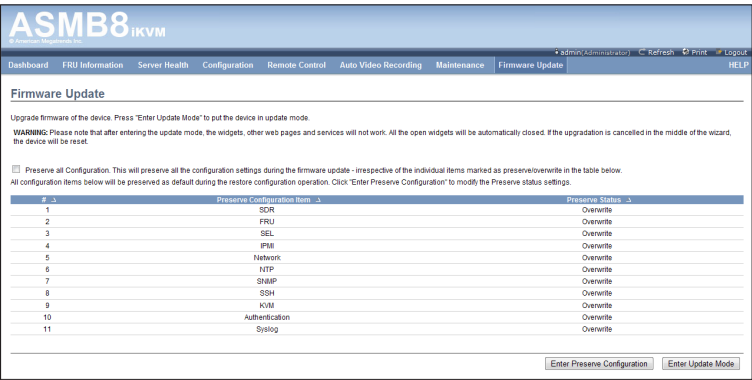


## 4.8.1 韌體升級 (Firmware Update)

本頁面可讓您遠端更新裝置的韌體。



注意：進入【Enter Update Mode】後，小部件、其他網頁及服務將無法使用。所有開啟的小部件將自動關閉。若中途取消升級，裝置將會重置。

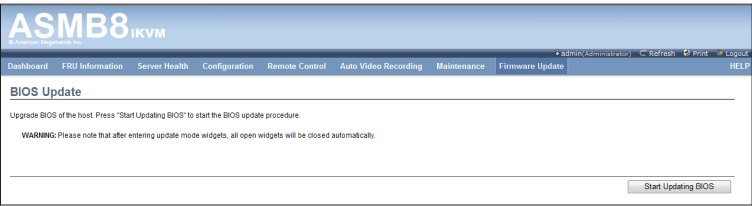


## 4.8.2 BIOS 升級 (BIOS Update)

本頁面可讓您遠端更新主機的 BIOS。



注意：進入【Start Updating BIOS】後，小部件將無法使用。所有開啟的小部件將自動關閉。



This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## 參考訊息

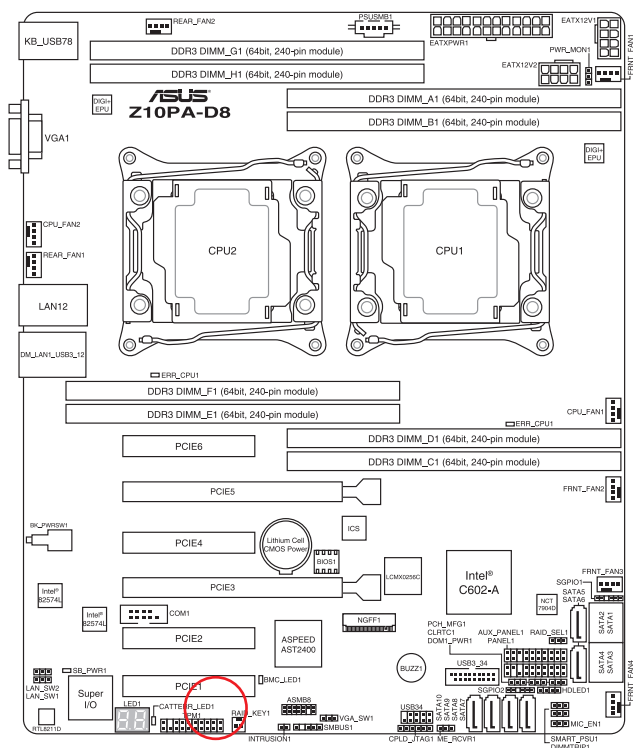
本章附錄介紹了 BMC 與 LAN 接頭在主機板上的位置，並提供了在安裝與使用管理卡的過程中出現的常見問題的解決方法。



## A.1 BMC 插座

華碩伺服器主機板支援具有底板管理控制器（Baseboard Management Controller，BMC）接頭的 ASMB8-iKVM 遠端管理卡。

BMC 插座的位置請參考下列圖示。

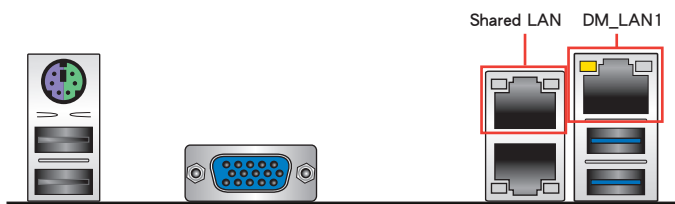


主機板圖示僅供參考。主機板外觀可能因型號而異。

## A.2 LAN 接頭

華碩伺服器主機板支援具有三個 LAN (RJ-45) 網路接頭的 ASMB8-iKVM 遠端管理卡：一個用於網路連接，另兩個用於伺服器管理。用於伺服器管理的接頭標示為 Shared LAN 與 DM\_LAN1。您必須使用 Shared LAN 與 DM\_LAN1 接頭將遠端伺服器連接到本地 / 中心主機（直接 LAN 連線）或網路集線器或路由器。

Shared LAN 與 DM\_LAN1 接頭的位置請參考下列圖示。



Shared LAN 與 DM\_LAN1 的具體位置請參考主機板使用手冊。

### A.3 疑難排解



疑難排解部分提供了一些在您安裝 / 使用華碩 ASMB8-iKVM 管理卡時常見問題的解決方法，幫助您輕鬆解決問題。若嘗試了此部分的方法仍未解決問題或有其他問題，請連絡技術支援部門。

問題	解決方法
本地 / 中心伺服器無法連接到 ASMB8-iKVM 遠端管理卡	<ol style="list-style-type: none"><li>1. 檢查網路線是否正確插入 LAN 接頭。</li><li>2. 請確認遠端與本地 / 中心伺服器的 IP 地址在同一個子網內。 （請參考第二章的說明） 在本地 / 中心伺服器上嘗試“ping xx.xx.xx.xx”（遠端伺服器 IP），並確認遠端伺服器 可回復 ping 請求。</li><li>3. 檢查 IP 來源是否設定為 [DHCP]。若設為 [DHCP]，您無法設定 IP 地址。</li></ol>
所有 SEL（系統事件日誌）無法顯示	最大 SEL 數為 900 個事件。
SEL（系統事件日誌）中顯示的的日期 / 時間不正確	請參考 4.4.9 的說明，檢查時區是否設定錯誤。
ASMB8-iKVM 在防火牆環境下無法連接網路	請 MIS 在防火牆中新增以下接頭數： 5123（虛擬軟碟機）（TCP） 5120（虛擬 CDROM）（TCP） 623（IPMI）（TCP & UDP） 80（HTTP）（TCP） 7578（iKVM）（TCP） 443（HTTPs）（TCP） 161（SNMP）（UDP）
Java 重定向畫面無法正常顯示	點選【Refresh Page】鍵更新重定向螢幕。



ASMB JAVA console 僅適用於內建的顯示卡，在其他的視訊卡上可能無法正常顯示。

## A.4 監控器表

### 記憶體 ECC

編號	名稱	類型	類型編碼	設定值或事件類型	事件日期 3
0xD1	CPU1_ECC1	Memory ECC Sensor	0xC	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03: DIMM_A4, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B4, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0A: DIMM_C3, 0x0B: DIMM_C4, 0x0C: DIMM_D1, 0x0D: DIMM_D2, 0x0E: DIMM_D3, 0x0F: DIMM_D4
0xD3	CPU2_ECC1	Memory ECC Sensor	0xC	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05: DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x0A: DIMM_F3, 0x0B: DIMM_F4, 0x0C: DIMM_G1, 0x0D: DIMM_G2, 0x0E: DIMM_G3, 0x0F: DIMM_G4, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_H3, 0x13: DIMM_H4, 0x14: DIMM_C1, 0x15: DIMM_C2, 0x16: DIMM_C3, 0x17: DIMM_C4

### CPU CATERR

編號	名稱	類型	類型編碼	設定值或事件類型
0xDA	CPU_CATERR	Processor	07h	Discrete (6Fh) 0x01: IERR

### 記憶體錯誤

編號	名稱	類型	類型編碼	設定值或事件類型	事件日期 3
0xDB	Memory_Train_ERR	OEM Type	0xC5	Discrete (6Fh) 0x01: Memory Train Error	[7:0] - Memory module/device 0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0A: DIMM_C3, 0x0C: DIMM_D1, 0x0D: DIMM_D2, 0x0E: DIMM_D3, 0x10: DIMM_E1, 0x11: DIMM_E2, 0x12: DIMM_E3, 0x14: DIMM_F1, 0x15: DIMM_F2, 0x16: DIMM_F3, 0x18: DIMM_G1, 0x19: DIMM_G2, 0x1A: DIMM_G3, 0x1C: DIMM_H1, 0x1D: DIMM_H2, 0x1E: DIMM_H3

## Backplane HD

編號	名稱	類型	類型編碼	設定值或事件類型
0x68	Backplane1 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x69	Backplane1 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6A	Backplane1 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6B	Backplane1 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6C	Backplane1 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6D	Backplane1 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6E	Backplane1 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6F	Backplane1 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x78	Backplane2 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x79	Backplane2 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7A	Backplane2 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7B	Backplane2 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7C	Backplane2 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7D	Backplane2 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7E	Backplane2 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7F	Backplane2 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild



## 電源

編號	名稱	類型	類型編碼	設定值或事件類型
0x81	PSU1 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critical - going high
0x82	PSU1 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x83	PSU1 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x92	PSU1 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x93	PSU1 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x94	PSU1 AC	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x95	PSU1 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x96	PSU1 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x97	PSU1 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected
0x84	PSU2 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critical - going high
0x85	PSU2 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x86	PSU2 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x9A	PSU2 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9B	PSU2 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x9C	PSU2 AC Lost	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x9D	PSU2 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9E	PSU2 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9F	PSU2 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected

## 硬體監控

編號	名稱	類型	類型編碼	設定值或事件類型
0x31	CPU1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x32	CPU2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCC	TR1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCD	TR2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x34	VCORE1	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x35	VCORE2	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x36	+3.3V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x37	+5V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x38	+12V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x39	+1.5V_I <sub>CH</sub> (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3A	+1.1V_I <sub>OH</sub> (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3B	+5VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3C	VBAT	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3D	P1VTT (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3E	+1.5V_P1DDR3 (For Intel platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high

0x3F	P2VTT (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x40	+3.3VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x41	+1.5V_P2DDR3 (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	P1DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	+1.5V (For Intel UP platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x43	P2DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x44	P1_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x45	P2_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x46	P1_VDDNB (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x47	+1.8V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x48	+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x49	+1.1V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x4A	VTT (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0xA0	CPU_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA1	CPU_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low

0xA2	FRNT_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA3	FRNT_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA4	FRNT_FAN3	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA5	FRNT_FAN4	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA6	REAR_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA7	REAR_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA8	FRNT_FAN5	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xA9	FRNT_FAN6	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0xAA	FRNT_FAN7	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low
0x4F	Chassis Intrusion	Physical Security (Chassis Intrusion)	0x05	Discrete(0x6F) 0x01: General Chassis Intrusion 0x02: Drive Bay Intrusion

# A.5 華碩 Server System 系列支援 ASMB8-iKVM 之機種型號

Rack	Tower	GPU Server
RS7 Series E8	TS7 Series E8	ESC8000 G3
RS5 Series E8	TS5 Series E8	ESC4000 G3
RS3 Series E9	TS3 Series E9	ESC4000 G3S

## A.6 華碩的連絡資訊

### 華碩電腦公司 ASUSTeK COMPUTER INC. (台灣)

#### 市場訊息

地址：台灣臺北市北投區立德路 150 號 4 樓  
電話：+886-2-2894-3447  
傳真：+886-2-2890-7798  
電子郵件：info@asus.com.tw  
全球資訊網：http://tw.asus.com

#### 技術支援

電話：+886-2-2894-3447 (0800-093-456)  
線上支援：<http://support.asus.com/techserv/techserv.aspx>

### 華碩電腦公司 ASUSTeK COMPUTER INC. (亞太地區)

#### 市場訊息

地址：台灣臺北市北投區立德路 150 號 4 樓  
電話：+886-2-2894-3447  
傳真：+886-2-2890-7798  
電子郵件：info@asus.com.tw  
全球資訊網：http://tw.asus.com

#### 技術支援

電話：+86-21-38429911  
傳真：+86-21-58668722, ext. 9101#  
線上支援：<http://support.asus.com/techserv/techserv.aspx>

### ASUS COMPUTER INTERNATIONAL (美國)

#### 市場訊息

地址：800 Corporate Way, Fremont, CA 94539, USA  
電話：+1-510-739-3777  
傳真：+1-510-608-4555  
電子郵件：<http://vip.asus.com/eservice/techserv.aspx>

#### 技術支援

電話：+1-812-282-2787  
傳真：+1-812-284-0883  
線上支援：<http://support.asus.com/techserv/techserv.aspx>

### ASUS COMPUTER GmbH (德國/奧地利)

#### 市場訊息

地址：Harkort Str. 21-23, D-40880 Ratingen, Germany  
傳真：+49-2102-959911  
全球資訊網：<http://www.asus.de>  
線上連絡：<http://www.asus.de/sales> (僅回答市場相關事務的問題)

#### 技術支援

電話：+49-1805-010923 (元件)  
電話：+49-1805-010920 (系統/筆記型電腦/Eee 系列產品/LCD)  
傳真：+49-2102-9599-11  
線上支援：<http://support.asus.com/techserv/techserv.aspx>



This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.