

# Dell EMC PowerEdge R750xa

## BIOS 與 UEFI 參考指南

## 註、警示與警告

 **註:** 「註」表示可以幫助您更有效地使用產品的重要資訊。

 **警示:** 「警示」表示有可能會損壞硬體或導致資料遺失，並告訴您如何避免發生此類問題。

 **警告:** 「警告」表示可能的財產損失、人身傷害或死亡。

<b>章 1: 預裝作業系統管理應用程式.....</b>	<b>4</b>
系統設定.....	4
系統 BIOS.....	4
iDRAC 設定公用程式.....	20
裝置設定.....	21
Dell Lifecycle Controller.....	21
嵌入式系統管理.....	21
開機管理程式.....	21
PXE 啟動.....	21

# 預裝作業系統管理應用程式

您可以管理系統基本設定和功能，無須使用系統韌體開機至作業系統。

## 管理預裝作業系統應用程式的選項

您可以使用下列任一選項來管理預裝作業系統應用程式：

- 系統設定
- Dell Lifecycle Controller
- 開機管理程式
- 開機前執行環境 (PXE)

主題：

- [系統設定](#)
- [Dell Lifecycle Controller](#)
- [開機管理程式](#)
- [PXE 啟動](#)

## 系統設定

使用 **System Setup** 畫面，您可以配置系統的 BIOS 設定、iDRAC 設定和裝置設定。

您可以使用下列任何其中一種介面存取系統設定：

- 圖形使用者介面：若要存取，請前往 iDRAC 操作介面，依序按一下 **設定** > **BIOS 設定**。
- 文字瀏覽器：若要使用文字瀏覽器，請使用「主控台重新導向」。

若要檢視 **System Setup**，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu**。

 **註：**如果在您按下 F2 鍵之前，作業系統便已開始載入，請讓系統完成開機，然後再重新啟動系統並重試。

 **註：**Intel 第 3 代 Xeon 可擴充高核心數 (HCC) 處理器要求最低 BIOS 修訂版 1.2.x。

下表說明 **系統設定主選單** 畫面中的選項：

**表 1. 系統設定主功能表**

選項	說明
系統 BIOS	可讓您配置 BIOS 設定。
iDRAC Settings	可讓您進行 iDRAC 設定。iDRAC 設定公用程式是使用 UEFI (整合可延伸韌體介面) 來設定及配置 iDRAC 參數的介面。您可以使用 iDRAC 設定公用程式來啟用或停用各種 iDRAC 參數。如需此公用程式的詳細資訊，請參閱《Integrated Dell Remote Access Controller User's Guide》(Integrated Dell Remote Access Controller 使用者指南)，網址為： <a href="http://www.dell.com/poweredgemanuals">www.dell.com/poweredgemanuals</a> 。
裝置設定	可讓您設定儲存控制器或網路卡等裝置的設定。

## 系統 BIOS

若要檢視 **System BIOS** 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu** > **System BIOS**。

表 2. 系統 BIOS 詳細資料

選項	說明
系統資訊	提供系統的相關資訊，例如系統型號、BIOS 版本、產品服務編號等。
Memory Settings	指定與已安裝記憶體相關的資訊及選項。
處理器設定	指定與處理器相關的資訊和選項，例如速度、快取記憶體大小等。
SATA 設定	指定啟用或停用內建 SATA 控制器和連接埠的選項。
NVMe Settings	可指定變更 NVMe 設定的選項。如果系統包含您要在 RAID 陣列中設定的 NVMe 硬碟機，您必須將此欄位與 <b>SATA Settings (SATA 設定)</b> 選單中的 <b>Embedded SATA (嵌入式 SATA)</b> 欄位設為 RAID 模式。您可能還需要將 <b>Boot Mode (開機模式)</b> 設定變更為 UEFI。否則，您應該將此欄位設為 <b>Non-RAID (非 RAID)</b> 模式。
Boot Settings	可指定用來指定開機模式 (BIOS 或 UEFI) 的選項。可讓您修改 UEFI 和 BIOS 開機設定。
網路設定	可指定管理 UEFI 網路設定與開機通訊協定的選項。 您可以在 <b>Device Settings (裝置設定)</b> 選單管理傳統網路設定。  <b>註:</b> BIOS 開機模式不支援 Network Settings。
整合式裝置	指定管理整合裝置控制器與連接埠的選項，並指定相關的功能及選項。
序列通訊	可指定管理序列埠的選項，以及其相關功能和選項。
系統設定檔設定	可指定變更處理器電源管理設定、記憶體頻率的的選項。
系統安全性	可指定設定系統安全性設定的選項，例如系統密碼、設定密碼、可信賴平台模組 (TPM) 安全性及 UEFI Secure Boot。此選項也可以管理系統的電源按鈕。
Redundant OS Control	可設定備援作業系統控制項的備援作業系統資訊。
其他設定	可指定變更系統日期和時間的選項。

## 系統資訊

若要檢視 **System Information** 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > System Information**。

表 3. System Information 詳細資料

選項	說明
System Model Name	指定系統型號名稱。
System BIOS Version	指定安裝在系統上的 BIOS 版本。
System Management Engine Version	指定 Management Engine 韌體的目前版本。
System Service Tag	指定系統產品服務編號。
System Manufacturer	指定系統製造商名稱。
System Manufacturer Contact Information	指定系統製造商的聯絡資訊。
System CPLD Version	指定系統複雜的可程式化邏輯裝置 (CPLD) 韌體的目前版本。
UEFI Compliance Version	指定系統韌體的 UEFI 遵循等級。

## Memory Settings

若要檢視 **Memory Settings** 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > Memory Settings**。

表 4. 記憶體設定詳細資料

選項	說明
System Memory Size	指定系統記憶體大小。
System Memory Type	可指定系統中安裝的記憶體類型。
System Memory Speed	指定系統記憶體速度。
System Memory Voltage	指定系統記憶體電壓。
影像記憶體	指定影像記憶體大小。
System Memory Testing	可指定在系統開機期間是否執行系統記憶體測試。此兩者可用選項為 <b>Enabled</b> 和 <b>Disabled</b> 。此選項預設為 <b>已停用</b> 。
記憶體作業模式	可指定記憶體作業模式。此可用選項預設為 <b>Optimizer Mode</b> 。
Current State of Memory Operating Mode	可指定記憶體作業模式的目前狀態。
Node Interleaving	啟用或停用節點交錯選項。指定是否支援非統一記憶體架構 (NUMA)。若將此欄位設為 <b>Enabled (啟用)</b> ，則安裝對稱式記憶體組態時支援記憶體交錯。若將此欄位設為「已停用」，則系統支援 NUMA (非對稱) 記憶體組態。此選項預設為 <b>已停用</b> 。
ADDDC 設定	啟用或停用 ADDDC Setting (ADDDC 設定) 功能。若啟用「適應性雙重 DRAM 裝置校正」(ADDDC)，系統會動態對應出故障的 DRAM。此選項設為 <b>啟用</b> 時，在特定工作負荷下可能會對系統效能造成影響。此功能僅適用於 x4 DIMM。此選項預設為 <b>Disabled (已停用)</b> 。
記憶體訓練	此選項設為 <b>快速</b> 且記憶體組態不變時，系統會使用先前儲存的記憶體訓練參數來訓練記憶體子系統，且系統開機時間也會縮短。如果記憶體組態變更，系統會自動啟用 <b>下次開機時重新訓練</b> 以強制進行一次完整記憶體訓練步驟，之後再回復為 <b>快速</b> 。  此選項設為 <b>下次開機時重新訓練</b> 時，系統會在下次開機時，強制執行一次完整記憶體訓練步驟，且開機時間會變長。  此選項設為 <b>啟用</b> 時，系統會在每次開機時強制執行完整記憶體訓練步驟，且每次開機的時間都會變長。
記憶體對應輸出	此選項可控制系統中的 DIMM 插槽。此選項預設為 <b>已啟用</b> 。其可用來停用系統已安裝的 DIMM。
可修正錯誤記錄	啟用或停用可修正錯誤記錄。此選項預設為 <b>已啟用</b> 。
隱藏記憶體：可用總記憶體	啟用或停用「隱藏記憶體」功能。「隱藏記憶體」功能可讓軟體變更記憶體大小。此選項預設為 <b>停用並隱藏</b> ，顯示的選項須由個人化模組啟用。

## 持續性記憶體詳細資料

您可以在《PMem User's Guide》(PMem 使用者指南) 中找到 **持續性記憶體** 畫面的詳細資料，網址為：<https://www.dell.com/poweredgemanuals>。

## 處理器設定

若要檢視 **Processor Settings** 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > Processor Settings**。

表 5. Processor Settings 詳細資料

選項	說明
Logical Processor	每個處理器核心支援最多兩個邏輯處理器。如果此選項設為 <b>已啟用</b> ，則 BIOS 會顯示所有邏輯處理器。如果此選項設為 <b>已停用</b> ，則 BIOS 會針對每個核心僅顯示一個邏輯處理器。此選項預設為 <b>已啟用</b> 。

表 5. Processor Settings 詳細資料 (續)

選項	說明
CPU Interconnect Speed	<p>可讓您管理系統中各處理器間的通訊連結頻率。</p> <p> 註: 標準和基本等級的處理器支援的連結頻率較低。</p> <p>可用選項包含<b>最大資料速率、11.2 GT/秒、10.4 GT/秒及 9.6 GT/秒</b>。此選項預設為<b>最大資料速率</b>。</p> <p>最大資料速率代表 BIOS 以處理器所支援的最高頻率執行通訊連結。您也可以選取處理器支援的特定頻率，可選頻率可能依處理器而有所不同。</p> <p>為發揮最佳效能，您應選取<b>最大資料速率</b>。若是通訊連結頻率有任何降低情形，都會影響到非本機記憶體存取及快取一致性流量的效能。另外也有可能減慢從特定處理器存取非本機 I/O 裝置的速度。</p> <p>然而，若您更注重省電而非效能，請降低處理器通訊連結的頻率。降低頻率前，您必須將記憶體與 I/O 存取作業移至最近的 NUMA 節點，以有效降低對系統效能的影響。</p>
Virtualization Technology	啟用或停用處理器的虛擬化技術。此選項預設為 <b>已啟用</b> 。
目錄模式	啟用或停用目錄模式。此選項預設為 <b>已啟用</b> 。
直接記憶體存取保護	此選項預設為 <b>已停用</b> 。此選項應啟用，以支援 Windows 2022 上的「安全啟動」(韌體保護)。
Adjacent Cache Line Prefetch	針對需要大量使用循序記憶體存取功能的應用程式，進行系統最佳化。此選項預設為 <b>已啟用</b> 。您可以針對需要大量使用隨機記憶體存取功能的應用程式來停用此選項。
Hardware Prefetcher	啟用或停用硬體預先擷取器。此選項預設為 <b>已啟用</b> 。
DCU Streamer Prefetcher	啟用或停用資料快取裝置 (DCU) 資料流預先擷取器。此選項預設為 <b>已啟用</b> 。
DCU IP Prefetcher	啟用或停用資料快取裝置 (DCU) IP 預先擷取器。此選項預設為 <b>已啟用</b> 。
Sub NUMA Cluster	啟用或停用子 NUMA 叢集。此選項預設為 <b>已停用</b> 。
MADT Core Enumeration	指定 MADT Core Enumeration。此選項預設為 <b>循環制</b> 。
UPI Prefetch	可讓您取得 DDR 匯流排上提早啟動的記憶體讀取。Ultra Path Interconnect (UPI) Rx 路徑會將推測性記憶體讀取直接繁衍至整合式記憶體控制器 (iMC)。此選項預設為 <b>已啟用</b> 。
XPT 預先擷取	此選項預設為 <b>已啟用</b> 。
LLC 預先擷取	啟用或停用所有執行緒上的 LLC 預先擷取功能。此選項預設為 <b>已啟用</b> 。
截止線 LLC 分配	啟用或停用截止線 LLC 分配。此選項預設為 <b>已啟用</b> 。您可以啟用此選項，即可輸入 LLC 中的截止線；或者，停用選項，則無須輸入 LLC 中的截止線。
目錄 AtoS	啟用或停用目錄 AtoS。AtoS 最佳化可減少重複讀取存取的遠端讀取延遲，無須介入寫入。此選項預設為 <b>已停用</b> 。
Logical Processor Idling	可讓您提高系統的能源效率。其採用作業系統核心暫止演算法，駐留系統中的部分邏輯處理器，讓對應的處理器核心轉換為低電力閒置狀態。只有在作業系統支援時，才能啟用這個選項。此選項預設為 <b>Disabled (停用)</b> 。

表 5. Processor Settings 詳細資料 (續)

選項	說明
	<p><b>註:</b> 「CPU 電源管理」設為<b>最大效能</b>時，系統不支援此功能。</p>
AVX P1	<p>讓您在 POST 期間，根據系統的電源和熱傳導能力，重新設定處理器的散熱設計功率 (TDP) 等級。TDP 會驗證冷卻系統所需的最大散熱量。此選項預設為 <b>Normal</b>。</p> <p><b>註:</b> 此選項僅存在於特定的處理器庫存單元 (SKU)。</p>
動態 SST 效能設定檔	<p>可讓您使用動態或靜態 Speed Select Technology 重新設定處理器。此選項預設為<b>已停用</b>。</p>
SST-Performance Profile	<p>可讓您使用快速選取技術重新設定處理器。</p>
Intel SST-BF	<p>啟用 Intel SST-BF。此選項會在系統設定檔選取「每瓦效能」(作業系統)或「自訂」(須啟用 OSPM)時顯示。此選項預設為<b>已停用</b>。</p>
Intel SST-CP	<p>啟用 Intel SST-CP。此選項會在系統設定檔選取「每瓦效能」(作業系統)或「自訂」(須啟用 OSPM)時顯示。每個系統設定檔模式均會顯示此選項讓您選取。此選項預設為<b>已停用</b>。</p>
x2APIC Mode	<p>啟用或停用 x2APIC 模式。此選項預設為<b>已啟用</b>。</p> <p><b>註:</b> 若為兩顆處理器 64 核心的組態，如果已啟用 256 個執行緒，則不可切換 x2APIC 模式 (BIOS 設定：已啟用所有 CCD、核心及邏輯處理器)。</p>
AVX ICCP 預先授予授權	<p>啟用或停用 AVX ICCP 預先授予授權。此選項預設為<b>已停用</b>。</p>
AVX ICC 預先授予等級	<p>可讓您選取 Intel 提供的不同 AVX ICC 轉換等級。此選項預設為<b>128 高強度</b>。</p>
<b>Dell Controlled Turbo</b>	
Dell Controlled Turbo 設定	<p>控制渦輪加速介入方式。僅可在「系統設定檔」設為<b>效能</b>或<b>自訂</b>，且「CPU 電源管理」設為<b>效能</b>的情況下啟用此選項。每個系統設定檔模式都可讓您選取此項目。此選項預設為<b>已停用</b>。</p> <p><b>註:</b> 視安裝的處理器數量而定，最多可能會有二個處理器清單。</p>
Dell AVX Scaling Technology	<p>可讓您設定 Dell AVX 調整技術。此選項預設為 <b>0</b>。輸入 0 到 12 個間隔值。Dell Controlled Turbo 功能啟用時，輸入的值會減少「Dell AVX 調整技術」頻率。</p>
Optimizer Mode (最佳化模式)	<p>啟用或停用 CPU 效能。此選項設為<b>自動</b>時，會將「CPU 電源管理」設為「最大效能」。設為<b>已啟用</b>時，會啟用「CPU 電源管理」設定。設為<b>已停用</b>時，會停用「CPU 電源管理」選項。此選項預設為 <b>Auto (自動)</b>。</p>
Number of Cores per Processor	<p>控制每個處理器中啟用的核心數目。此選項預設為 <b>All (全部)</b>。</p>
Processor Core Speed	<p>指定處理器最大核心頻率。</p>
Processor Bus Speed	<p>指定處理器的匯流排速度。</p> <p><b>註:</b> 兩個處理器皆安裝時，才會顯示處理器匯流排速度選項。</p>
本機電腦檢查例外狀況	<p>啟用或停用本機電腦檢查例外狀況。這是 MCA 復原機制的擴充功能，可將未修正可復原 (UCR) 軟體可復原動作所需 (SRAR) 錯誤，傳遞給一或多個接收先前中毒或損壞資料的特定邏輯處理器執行緒。啟用後，僅會提供「UCR SRAR 電腦檢查例外狀況」給受影響的執行緒，而非廣播到系統中所有執行緒。此功能支援在附近偵測到多個可復原錯誤情況的作業系統復原，這些錯誤可能會導致嚴重電腦檢查事件。僅具備進階 RAS 功能的處理器提供此功能。此選項預設為<b>已停用</b>。</p>

表 5. Processor Settings 詳細資料 (續)

選項	說明
Processor n	 註: 視處理器的數量而定，最多可能會列出 n 顆處理器。 系統會針對每顆處理器顯示下列設定：

表 6. 處理器 n 詳細資料

選項	說明
Family-Model-Stepping	按照 Intel 的定義，指定處理器的系列、型號和步進。
Brand	指定品牌名稱。
Level 2 Cache	指定 L2 快取記憶體總大小。
Level 3 Cache	指定 L3 快取記憶體總大小。
核心數目	指定每個處理器的核心數目。
Maximum Memory Capacity	指定每個處理器的最大記憶體容量。
Microcode	指定處理器微碼版本。

## SATA 設定

若要檢視 SATA Settings 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > SATA Settings**。

表 7. SATA Settings 詳細資料

選項	說明								
Embedded SATA	可讓嵌入式 SATA 選項設為 <b>Off</b> 、 <b>AHCI mode</b> 或 <b>RAID modes</b> 。此選項預設為 <b>AHCI Mode (AHCI 模式)</b> 。  註: 1. 您可能還需要將 Boot Mode (開機模式) 設定變更為 UEFI。否則，您應該將此欄位設為 Non-RAID mode。 2. 在 RAID 模式下，不支援 ESXi 和 Ubuntu 作業系統。								
Security Freeze Lock	在 POST 期間，將 <b>Security Freeze Lock (安全凍結鎖定)</b> 命令傳送至嵌入式 SATA 磁碟機。此選項僅適用於 AHCI 模式。此選項預設為已啟用。								
Write Cache	在 POST 期間，啟用或停用嵌入式 SATA 磁碟機的命令。此選項預設為已停用。								
Port n	可設定所選裝置的磁碟機類型。 在 <b>AHCI 模式</b> 或 <b>RAID 模式</b> 中，BIOS 支援一律為啟用。 <b>表 8. Port n</b>								
<table border="1"> <thead> <tr> <th>選項</th> <th>說明</th> </tr> </thead> <tbody> <tr> <td>Model</td> <td>指定選取裝置的磁碟機機型。</td> </tr> <tr> <td>Drive Type</td> <td>指定連接 SATA 連接埠的磁碟機類型。</td> </tr> <tr> <td>容量</td> <td>指定磁碟機總容量。對於卸除式媒體裝置 (例如光碟機) 並不會定義此欄位。</td> </tr> </tbody> </table>		選項	說明	Model	指定選取裝置的磁碟機機型。	Drive Type	指定連接 SATA 連接埠的磁碟機類型。	容量	指定磁碟機總容量。對於卸除式媒體裝置 (例如光碟機) 並不會定義此欄位。
選項	說明								
Model	指定選取裝置的磁碟機機型。								
Drive Type	指定連接 SATA 連接埠的磁碟機類型。								
容量	指定磁碟機總容量。對於卸除式媒體裝置 (例如光碟機) 並不會定義此欄位。								

## NVMe Settings

此選項可設定 NVMe 磁碟機模式。如果系統包含您要在 RAID 陣列中設定的 NVMe 磁碟機，則必須將此欄位和 SATA Settings 選單中的 Embedded SATA 欄位設為 RAID Mode。您可能還需要將 Boot Mode 設定變更為 UEFI。

若要檢視 NVMe 設定畫面，請開啟系統電源並按下 F2，然後按一下系統設定主選單 > 系統 BIOS > NVMe 設定。

表 9. NVMe 設定詳細資料

選項	說明
NVMe 模式	啟用或停用開機模式。此選項預設為 Non-RAID 模式。
BIOS NVMe 驅動程式	設定啟動 NVMe 驅動程式的磁碟機類型。可用選項為 Dell 認證磁碟機和所有磁碟機。此選項預設為 Dell 認證磁碟機。

## Boot Settings

您可以使用「開機設定」畫面，將開機模式設為 BIOS 或 UEFI。亦可指定開機順序。

- **UEFI**：整合可延伸韌體介面 (UEFI) 是作業系統及平台韌體之間的新介面。此介面包含了具平台相關資訊的資料表，以及作業系統及其載入器可用的開機及執行階段服務呼叫。只有在「開機模式」設為 UEFI 時，才能發揮以下優點：
  - 支援大於 2TB 的磁碟機分割區。
  - 增強型安全性 (例如「UEFI 安全開機」)。
  - 加快開機時間。

**註**：若要從 NVMe 磁碟機開機，您只能使用 UEFI 開機模式。

- **BIOS**：BIOS Boot Mode (BIOS 開機模式) 是傳統的開機模式，並保留下來作為回溯相容性。

若要檢視 Boot Settings 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 System Setup Main Menu > System BIOS > Boot Settings。

表 10. 開機設定詳細資料

選項	說明
Boot Mode	可讓您設定系統的開機模式。如果作業系統支援 UEFI，您可以將此選項設為 UEFI。將此欄位設為 BIOS 則可與非 UEFI 作業系統相容使用。此選項預設為 UEFI。 <b>警告</b> ：如果未在相同的開機模式中安裝作業系統，切換開機模式可能會使系統無法啟動。 <b>註</b> ：將此欄位設為 UEFI 可停用 BIOS Boot Settings 選單。
Boot Sequence Retry	啟用或停用「開機順序重試」功能或重設系統。如果此選項設為已啟用，而系統無法開機時，系統會在 30 秒後重新嘗試開機順序。此選項設為重設且系統無法開機時，系統會立即重新開機。此選項預設為已啟用。
Hard-disk Failover	啟用或停用硬碟容錯移轉功能。此選項預設為已停用。
Generic USB Boot	啟用或停用一般 USB 開機預留位置。此選項預設為已停用。
Hard-disk Drive Placeholder	啟用或停用硬碟預留位置。此選項預設為已停用。
清除所有 Sysprep 順序和變數	此選項設為無時，BIOS 將不會執行任何動作。若設為是，BIOS 將會刪除 Sysprep #### 和 SysprepOrder 的變數；此選項為一次性選項，會在刪除變數後重設為「無」。只有在 UEFI 開機模式中才會提供此設定。此選項預設為「無」。
UEFI 開機設定	指定 UEFI 開機順序。啟用或停用 UEFI 開機選項。 <b>註</b> ：此選項可控制 UEFI 開機順序。系統會先嘗試使用清單中的第一個選項。

  

選項	說明
UEFI Boot Sequence	可讓您變更開機裝置順序。
Boot Options Enable/Disable	可讓您選取已啟用或停用的開機裝置。

## 選擇系統開機模式

系統設定可讓您指定下列其中一個開機模式以安裝您的作業系統：

- UEFI 開機模式 (預設值) 是增強型 64 位元開機介面。

如果您將系統設定為開機進入 UEFI 模式，此設定將取代系統 BIOS。

1. 從 **System Setup Main Menu (系統設定主選單)**，按一下 **Boot Settings (開機設定)**，然後選取 **Boot Mode (開機模式)**。
2. 選取您要讓系統開機進入的 UEFI 開機模式。

 **警告:** 如果未在相同的開機模式中安裝作業系統，切換開機模式可能會使系統無法啟動。

3. 在系統以指定的開機模式開機後，繼續從該模式安裝您的作業系統。

 **註:** 作業系統必須與 UEFI 相容，才能從 UEFI 開機模式安裝。DOS 與 32 位元作業系統不支援 UEFI，只能從 BIOS 開機模式安裝。

 **註:** 如需有關支援作業系統的最新資訊，請前往 [www.dell.com/ossupport](http://www.dell.com/ossupport)。

## 變更開機順序

### 關於此工作

如果您想要從 USB 隨身碟或光碟機開機，您可能需要變更開機順序。如果您選取 **BIOS** 作為 **Boot Mode (開機模式)**，下列指示可能會有所不同。

 **註:** 變更磁碟機開機順序僅支援 BIOS 開機模式。

### 步驟

1. 在 **System Setup Main Menu** 畫面中，按一下 **System BIOS > Boot Settings > UEFI Boot Settings > UEFI Boot Sequence**。
2. 使用方向鍵選取開機裝置，然後使用加號 (+) 和減號 (-) 鍵順序向上或向下移動裝置的排序。
3. 按一下 **結束**，然後按一下 **是**，以在結束時儲存設定值。

 **註:** 您亦可視需要啟用或停用開機順序裝置。

## 網路設定

若要檢視 **Network Settings** 畫面，請開啟系統電源並按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > Network Settings**。

 **註:** BIOS 開機模式不支援 Network Settings。

表 12. Network Settings 詳細資料

選項	說明
<b>UEFI PXE Settings</b>	可讓您控制 UEFI PXE 裝置的組態。
<b>PXE Device n (n = 1 至 4)</b>	啟用或停用裝置。啟用時，系統會為裝置建立 UEFI PXE 開機選項。
<b>PXE Device n Settings (n = 1 至 4)</b>	可讓您控制 PXE 裝置的組態。
<b>UEFI HTTP Settings</b>	可讓您控制 UEFI HTTP 裝置的組態。
<b>HTTP Device n (n = 1 至 4)</b>	啟用或停用裝置。啟用時，系統會為裝置建立 UEFI HTTP 開機選項。
<b>HTTP Device n Settings (n = 1 至 4)</b>	可讓您控制 HTTP 裝置的組態。
<b>UEFI iSCSI Settings</b>	可讓您控制 iSCSI 裝置的組態。

表 13. PXE Device n Settings 詳細資料

選項	說明
<b>介面</b>	指定用於此 PXE 裝置的 NIC 介面。
<b>Protocol (通訊協定)</b>	指定用於 PXE 裝置的通訊協定。此選項可設為 <b>IPv4</b> 或 <b>IPv6</b> 。此選項預設為 <b>IPv4</b> 。
<b>Vlan</b>	啟用 PXE 裝置的 Vlan。此選項可設為 <b>Enable</b> 或 <b>Disable</b> 。此選項預設為 <b>Disable (停用)</b> 。

表 13. PXE Device n Settings 詳細資料 (續)

選項	說明
Vlan ID	顯示 PXE 裝置的 Vlan ID。
Vlan Priority	顯示 PXE 裝置的 Vlan 優先順序。

表 14. UEFI iSCSI Settings 畫面詳細資訊

選項	說明
iSCSI Initiator Name	指定 IQN 格式的 iSCSI Initiator 名稱。
iSCSI Device1	啟用或停用 iSCSI 裝置。停用時，系統會自動為 iSCSI 裝置建立 UEFI 開機選項。此選項預設為 <b>Disabled (已停用)</b> 。
iSCSI Device1 Settings	可讓您控制 iSCSI 裝置的組態。

表 15. iSCSI Device1 Settings 畫面詳細資訊

選項	說明
Connection 1	啟用或停用 iSCSI 連線。此選項預設為 <b>Disable (停用)</b> 。
連線 2	啟用或停用 iSCSI 連線。此選項預設為 <b>Disable (停用)</b> 。
Connection 1 Settings	可讓您控制 iSCSI 連線的組態。
連線 2 設定	可讓您控制 iSCSI 連線的組態。
Connection Order	可讓您控制系統嘗試使用 iSCSI 連線的順序。

## 整合式裝置

若要查看 **Integrated Devices** 畫面，請開啟系統電源，按下 F2，然後按一下 **System Setup Main Menu > System BIOS > Integrated Devices**。

表 16. Integrated Devices 詳細資訊

選項	說明
User Accessible USB Ports	<p>設定使用者可存取的 USB 連接埠。選取<b>僅開啟背面連接埠</b>可停用正面 USB 連接埠；選取<b>關閉所有連接埠</b>可停用所有正面和背面 USB 連接埠；選取<b>關閉所有連接埠 (動態)</b>可於 POST 期間停用所有正面和背面 USB 連接埠。此選項預設為<b>開啟所有連接埠</b>。</p> <p>使用者可存取的 USB 連接埠設為<b>關閉所有連接埠 (動態)</b>時，會啟用<b>僅啟用正面連接埠</b>選項。</p> <ul style="list-style-type: none"> <li><b>僅啟用正面連接埠</b>：在作業系統執行階段啟用或停用正面 USB 連接埠。</li> </ul> <p>在開機程序執行期間，USB 鍵盤和滑鼠仍可在某些 USB 連接埠運作，視選項而定。開機程序完成後，USB 連接埠會根據設定啟用或停用。</p>
iDRAC Direct USB Port	iDRAC Direct USB 連接埠完全由 iDRAC 管理，主機無法檢視。此選項可設為 <b>開啟</b> 或 <b>關閉</b> 。若設為 <b>OFF (關閉)</b> ，iDRAC 不會偵測到安裝在此受管理連接埠的任何 USB 裝置。此選項預設為「 <b>開啟</b> 」。
Internal SD Card Port	啟用或停用內部雙 SD 模組 (iDSDM) 的內部 SD 卡連接埠。此選項預設為「 <b>開啟</b> 」。
Internal SD Card Redundancy	<p>設定內部雙 SD 模組 (iDSDM) 的備援模式。設為 <b>Mirror (鏡像)</b> 模式時，資料會同時寫入至兩張 SD 卡。若卡故障或是未能更換故障的卡，則在系統開機期間，作用中的卡的資料會複製到離線的卡。</p> <p>當「<b>內部 SD 卡備援</b>」設為<b>已停用</b>時，作業系統只會顯示主要 SD 卡。此選項預設為<b>已停用</b>。</p>
Internal SD Primary Card	依預設會選取主要 SD 卡作為 SD 卡 1。如果 SD 卡 1 未顯示，則控制器會選取 SD 卡 2 作為主要 SD 卡。

表 16. Integrated Devices 詳細資訊 (續)

選項	說明
內嵌 NIC1 和 NIC2	啟用或停用嵌入式 NIC1 和 NIC2。若設為 <b>Disabled (OS)</b> ，則可能仍可透過內嵌管理控制器使用 NIC 以存取共用網路。請使用系統的 NIC 管理公用程式來設定內嵌 <b>NIC1 和 NIC2</b> 選項。此選項預設為已啟用。
I/OAT DMA Engine	啟用或停用 I/O 加速技術 (I/OAT) 選項。I/OAT 是一套 DMA 功能，旨在提高網路流量並降低 CPU 使用率。只有在硬體和軟體支援該功能時，才會啟用此選項。此選項預設為已停用。
Embedded Video Controller	<p>啟用或停用將 Embedded Video Controller (嵌入式影像控制器) 作為主要顯示器。若設為 <b>Enabled (啟用)</b>，即使已安裝附加顯示卡，系統仍會以內嵌影像控制器作為主要顯示器。若設為 <b>停用</b>，則系統會將附加顯示卡當作主要顯示器。BIOS 在 POST 期間和開機前環境中會將顯示輸出至主要附加影像和嵌入式影像。之後，內嵌影像會在作業系統開機前立即停用。此選項預設為已啟用。</p> <p>① 註：若系統安裝多張附加顯示卡，則 PCI 列舉期間探索到的第一張卡會獲選作為主要影像裝置。您可能必須重新安排插槽內的插卡，以控制要以哪一張卡作為主要影像裝置。</p>
I/O 監測延遲回應	選取 PCI I/O 可保留 CPU 監測要求的週期數，以保留完成其寫入 LLC 所需的時間。此項設定可以協助改善工作負載的效能，其傳輸量和延遲極為重要。可用的選項為 <b>256 週期數、512 週期數、1K 週期數、2K 週期數、4K 週期數、8K 週期數、16K 週期數、32K 週期數、64K 週期數及 128K 週期數</b> 。此選項預設為 <b>256 週期數</b> 。
Current State of Embedded Video Controller	顯示嵌入式影像控制器目前的狀態。 <b>Current State of Embedded Video Controller (嵌入式影像控制器的目前狀態)</b> 選項是唯讀欄位。如果「嵌入式影像控制器」是系統中唯一的顯示功能 (也就是說，未安裝任何附加顯示卡)，即使「嵌入式影像控制器」設定設為「已停用」「已啟用」，也會自動使用「嵌入式影像控制器」作為主要顯示器。
SR-IOV Global Enable	啟用或停用 Single Root I/O Virtualization (SR-IOV) (單一根 I/O 虛擬化) 裝置的 BIOS 組態。此選項預設為已停用。
OS Watchdog Timer	如果系統停止回應，此 Watchdog Timer 可協助作業系統回復。若此選項設為 <b>Enabled (啟用)</b> ，作業系統會初始化計時器。若此選項設為 <b>停用</b> (預設值)，計時器將不會對系統造成任何影響。
Empty Slot Unhide	啟用或停用 BIOS 和作業系統可以使用的所有空插槽的根連接埠。此選項預設為已停用。
Memory Mapped I/O above 4 GB	啟用或停用對需要大量記憶體之 PCIe 裝置的支援。僅可為 64 位元作業系統啟用此選項。此選項預設為已啟用。
Memory Mapped I/O Base	若設為 <b>12 TB</b> ，系統會將 MMIO 基礎對應至 12 TB。請為需要 44 位元 PCIe 定址的作業系統啟用此選項。若設為 <b>512 GB</b> ，系統會將 MMIO 基礎對應至 512 GB，並將支援的記憶體上限減少至低於 512 GB。僅可針對 4 GPU DGMA 問題啟用此選項。此選項預設為 <b>56 TB</b> 。
Slot Disablement	<p>可啟用或停用系統上可用的 PCIe 插槽。插槽停用功能可控制已安裝在指定插槽的 PCIe 卡組態。只有在已安裝的周邊應用裝置擴充卡導致作業系統無法開機，或是導致系統啟動延遲時，才能停用插槽。如果停用插槽，Option ROM 和 UEFI 驅動程式也都會停用。只有出現在系統上的插槽可受到控制。</p> <p><b>Slot n</b>：啟用或停用 PCIe 插槽 n，或僅停用 PCIe 插槽 n 的開機驅動程式。此選項預設為已啟用。</p>
插槽分支	<p><b>Auto Discovery Bifurcation Settings</b> 可讓您設定 <b>Platform Default Bifurcation</b>、及 <b>Manual bifurcation Control</b>。</p> <p>此選項預設為平台預設分支。設為 <b>Manual bifurcation Control</b> 時，插槽分支欄位可供存取；設為 <b>Platform Default Bifurcation</b> 時，欄位會呈灰色，無法使用。</p> <p>① 註：插槽分支僅支援 PCIe 插槽，不支援切換卡轉擴充板及薄型連結器轉擴充板插槽類型。</p>

## 序列通訊

若要檢視 **Serial Communication** 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > Serial Communication**。

**註:** PowerEdge R750xa 系統可選配序列埠。只有在系統安裝 COM 序列埠後，才可使用「序列通訊」選項。

表 17. Serial Communication 詳細資料

選項	說明
序列通訊	<p>啟用序列通訊選項。在 BIOS 中選取序列通訊裝置 (序列裝置 1 和序列裝置 2)。您也可以啟用 BIOS 主控台重新導向功能及指定連接埠位址。</p> <p>沒有 COM 序列埠 (DB9) 之系統可用的選項為<b>不使用主控台重新導向開啟、使用主控台重新導向開啟、關閉</b>。此選項預設為「關閉」。</p> <p>有 COM 序列埠 (DB9) 之系統可用的選項為<b>不使用主控台重新導向開啟、透過 Com1 使用主控台重新導向開啟、透過 Com2 使用主控台重新導向開啟、關閉、自動</b>。此選項預設為 <b>Auto (自動)</b>。</p>
Serial Port Address	<p>可讓您設定序列裝置的連接埠位址。此選項預設為 <b>Serial Device1=COM2, Serial Device 2=COM1</b>。</p> <p><b>註:</b> 只有序列裝置 2 才能用於 Serial Over LAN (SOL) 功能。若要使用 SOL 主控台重新導向，請對主控台重新導向和序列裝置設定相同的連接埠位址。</p> <p><b>註:</b> 每次系統開機時，BIOS 會與儲存在 iDRAC 的序列 MUX 設定同步。您可以在 iDRAC 中單獨變更序列 MUX 設定。從 BIOS 設定公用程式載入 BIOS 預設設定，不一定都能將序列 MUX 設定還原成序列裝置 1 的預設設定。</p>
External Serial Connector	<p>可讓您使用此選項將外接式序列連接器與序列裝置 1、序列裝置 2 或遠端存取裝置建立關聯。此選項預設為 <b>Serial Device 1 (序列裝置 1)</b>。</p> <p><b>註:</b> 只有 Serial Device 2 (序列裝置 2) 可用於 Serial Over LAN (SOL)。若要使用 SOL 主控台重新導向，請對主控台重新導向和序列裝置設定相同的連接埠位址。</p> <p><b>註:</b> 每次系統開機時，BIOS 會與儲存在 iDRAC 的序列 MUX 設定同步。您可以在 iDRAC 中單獨變更序列 MUX 設定。從 BIOS 設定公用程式載入 BIOS 預設設定，不一定都能將此設定還原成序列裝置 1 的預設設定。</p>
Failsafe Baud Rate	<p>指定主控台重新導向的故障防護傳輸速率。BIOS 會自動嘗試決定傳輸速率。只有嘗試失敗時，才會使用這個故障防護傳輸速率，而且此值不得更改。此選項預設為 <b>115200</b>。</p>
Remote Terminal Type	<p>設定遠端主控台終端機類型。此選項預設為 <b>VT100/VT220</b>。</p>
Redirection After Boot	<p>可在作業系統載入時，啟用或停用 BIOS 主控台重新導向。此選項預設為已啟用。</p>

## 系統設定檔設定

若要檢視 **System Profile Settings** 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > System Profile Settings**。

表 18. System Profile Settings 詳細資料

選項	說明
System Profile	<p>設定系統設定檔。如果您將 System Profile (系統設定檔) 選項設為 <b>Custom (自訂)</b> 以外的模式，BIOS 會自動設定其餘的選項。只有在模式設定為「自訂」時，您才能變更其餘選項。此選項預設為 <b>Performance Per Watt (DAPC) (每瓦效能最佳化 (DAPC))</b>。其他選項包括效能、每瓦效能 (OS)、工作站效能及自訂。</p> <p><b>註:</b> System Profile (系統設定檔) 選項設為 <b>Custom (自訂)</b> 時，才能獲得系統設定檔設定畫面的所有參數。</p>

表 18. System Profile Settings 詳細資料 (續)

選項	說明
CPU Power Management	設定 CPU 電源管理。此選項預設為系統 DBPM (DAPC)。其他選項包括最大效能、OS DBPM。
Memory Frequency ( 記憶體頻率 )	設定系統記憶體的速度。您可以選取最大效能、最大可靠性或特定速度。此選項預設為 Maximum Performance (最高效能)。
Turbo Boost	啟用或停用處理器，以渦輪加速模式運作。此選項預設為已啟用。
C1E	啟用或停用處理器，讓處理器閒置時切換至最低效能狀態。此選項預設為已啟用。
C States	啟用或停用處理器，在所有可用的電源狀態下運作。C States 可讓處理器閒置時進入低電源狀態。設為 <b>Enabled</b> (作業系統控制) 或設為 <b>Autonomous</b> (若支援硬體控制) 後，處理器能在所有可用的電源狀態下運作以節省電源，但可能會增加記憶體延遲或頻率抖動的可能性。此選項預設為已啟用。
Memory Patrol Scrub	設定記憶體巡查清除模式。此選項預設為 <b>Standard (標準)</b> 。
Memory Refresh Rate	設定 1x 或 2x 的記憶體重新整理頻率。此選項預設為 <b>1x</b> 。
Uncore Frequency	可讓您選取 <b>非核心頻率</b> 選項。「動態模式」可讓處理器在執行期間，最佳化核心和非核心之間的電源資源。 <b>能源效率原則</b> 選項的設定，會影響以省電或效能最佳化為目的而進行的非核心頻率最佳化作業。
Energy Efficient Policy	可讓您選取 <b>能源效率原則</b> 選項。CPU 會使用設定來控制處理器的內部行為，並決定是否針對更高效能或更佳省電效果。此選項預設為 <b>Balanced Performance (平衡的效能)</b> 。
Monitor/Mwait	啟用處理器中的 Monitor/Mwait 指令。所有系統設定檔 (自訂除外) 中都會將此選項預設為已啟用。 <i>i</i> 註: 只有在 Custom (自訂) 模式中的 C States (C 狀態) 選項設定為已停用時，才能停用此選項。 <i>i</i> 註: 在 Custom (自訂) 模式中，C States (C 狀態) 設為 Enabled (啟用) 時，變更 Monitor/Mwait 設定不會影響系統電源或效能。
工作負荷設定檔	此選項可讓使用者指定伺服器的目標工作負荷。其可依據工作負荷類型最佳化效能。此選項預設為未設定。
CPU Interconnect Bus Link Power Management	啟用或停用 CPU 互連匯流排連結電源管理。此選項預設為已啟用。
PCI ASPM L1 Link Power Management	啟用或停用 PCI ASPM L1 連結電源管理。此選項預設為已啟用。
Intel Persistent Memory CR QoS	可讓您選取 QoS 旋鈕的調整方法 1，並且建議用於 Active Directory 中的 2-2-2 記憶體組態；QoS 旋鈕的方法 2 則是建議用於 Active Directory 中的其他記憶體組態；而 QoS 旋鈕的方法 3 則是建議用於每個通道 1 條 DIMM 的組態。此選項預設為 <b>模式 0</b> 。
Intel Persistent Memory Performance Setting	可讓您根據工作負荷行為選取 NVMe 效能設定。若此選項設為 <b>BW 最佳化</b> ，則效能會針對 DDR 與 DDRT 頻寬最佳化。若此選項設為 <b>Latency Optimized</b> ，則在效能方面，DDR 延遲的情況會較為理想。此選項預設為 <b>BW 最佳化</b> 。

## 系統安全性

若要檢視 System Security 畫面，請啟動系統電源，按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > System Security**。

表 19. System Security 詳細資料

選項	說明
CPU AES-NI	使用「進階加密標準指令集」來執行加密和解密，以提高應用程式的速度。此選項預設為已啟用。
系統密碼	設定系統密碼。此選項預設為「已啟用」，如果系統未安裝密碼跳線，此選項將為唯讀。
Setup Password	設定設定密碼。如果系統未安裝密碼跳線，此選項將為唯讀。

表 19. System Security 詳細資料 (續)

選項	說明
Password Status	鎖定系統密碼。此選項預設為「已解除鎖定」。
TPM Information	表示可信賴平台模組類型 (若有)。

表 20. TPM 1.2 security 資訊

選項	說明
TPM Information	
TPM Security	<p> 註: 只有當 TPM 模組已安裝時, 才能使用 TPM 功能表。</p> <p>可讓您控制 TPM 的報告模式。「TPM 安全性」選項預設為「關閉」。如果 <b>TPM Status (TPM 狀態)</b> 欄位設為 <b>On with Pre-boot Measurements (開啟並使用開機前測量)</b> 或 <b>On without Pre-boot Measurements (開啟但不使用開機前測量)</b>, 則您只能修改 TPM Status (TPM 狀態) 和 TPM Activation (TPM 啟動)。</p> <p>若已安裝 TPM 1.2, 「TPM 安全性」選項可設為「關閉」、「使用開機前測量開啟」或「不使用開機前測量開啟」。</p>
TPM Information	變更 TPM 的作業狀態。此選項預設為「無變更」。
TPM Firmware	指出 TPM 的韌體版本。
TPM Status	指定 TPM 狀態。
TPM Command	控制可信賴平台模組 (TPM)。設為「無」時, 不會有任何命令傳送至 TPM。設為「啟動」時, 會啟用並啟動 TPM。設為「停用」時, 會停用 TPM。設為「清除」時, 會清除 TPM 的所有內容。此選項預設為「無」。

表 21. TPM 2.0 security 資訊

選項	說明
TPM Information	
TPM Security	<p> 註: 只有當 TPM 模組已安裝時, 才能使用 TPM 功能表。</p> <p>可讓您控制 TPM 的報告模式。「TPM 安全性」選項預設為「關閉」。如果 <b>TPM Status (TPM 狀態)</b> 欄位設為 <b>On with Pre-boot Measurements (開啟並使用開機前測量)</b> 或 <b>On without Pre-boot Measurements (開啟但不使用開機前測量)</b>, 則您只能修改 TPM Status (TPM 狀態) 和 TPM Activation (TPM 啟動)。</p> <p>若已安裝 TPM 2.0 時, 「TPM 安全性」選項可設為「開啟」或「關閉」。此選項預設為「關閉」。</p>
TPM Information	變更 TPM 的作業狀態。此選項預設為「無變更」。
TPM Firmware	指出 TPM 的韌體版本。
TPM Hierarchy	<p>啟用、停用或清除儲存與背書階層。設為「已啟用」時, 可使用儲存和背書階層。</p> <p>設為「已停用」時, 則無法使用儲存與背書階層。</p> <p>設為「清除」時, 將清除儲存和背書階層的任何值, 然後重設為「已啟用」。</p>
TPM Advanced Settings	指定 TPM 進階設定詳細資料。

表 22. System Security 詳細資料

選項	說明
Intel(R) TXT	可讓您設定 Intel 可信賴執行技術 (TXT) 選項。若要啟用 <b>Intel TXT</b> 選項, 必須使用開機前測量將虛擬化技術和 TPM 安全性設為已啟用。此選項預設為「關閉」。此選項已設為開啟, 以支援 Windows 2022 上的「安全啟動」(韌體保護)。
記憶體加密	啟用或停用 Intel 全記憶體加密 (TME) 和多租用戶 (Intel® TME-MT)。選項設為 <b>已停用</b> 時, BIOS 會停用 TME 和 MK-TME 技術。選項設為 <b>單一金鑰</b> 時, BIOS 會啟用 TME 技術。選項設為 <b>多重金鑰</b> 時, BIOS 會啟用 TME-MT 技術。此選項預設為 <b>已停用</b> 。

表 22. System Security 詳細資料 (續)

選項	說明
Intel(R) SGX	可讓您設定 Intel Software Guard Extensions (SGX) 選項。若要啟用 <b>Intel SGX</b> 選項，處理器必須支援 SGX、記憶體安裝方式必須相容 (至少每 CPU 插槽 8 條完全相同的 DIMM1 至 DIMM8，不支援持續性記憶體組態)、記憶體運作模式必須設為最佳化模式、記憶體加密必須啟用，且節點交錯必須停用。此選項預設為 <b>關閉</b> 。此選項設為 <b>關閉</b> 時，BIOS 會停用 SGX 技術。此選項設為 <b>開啟</b> 時，BIOS 會啟用 SGX 技術。
SGX 套件資訊頻內存取	可讓您存取 Intel Software Guard Extensions (SGX) 套件資訊頻內選項。此選項預設為 <b>關閉</b> 。
PPMRR 大小	設定 PPMRR 大小。
SGX GoS	啟用或停用 SGX 服務品質。
選取擁有者 EPOCH 輸入類型	可讓您選取變更為 <b>新隨機擁有者 EPOCH</b> 或 <b>手動使用者定義擁有者 EPOCH</b> 。每個 EPOCH 均為 64 位元。選取變更為 <b>新隨機擁有者 EPOCH</b> ，產生新 EPOCH 後，選項會變更為 <b>手動使用者定義擁有者 EPOCH</b> 。 <b>Software Guard Extensions Epoch n</b> ：設定 Software Guard Extensions Epoch 值。
可從 OS/SW 寫入 SGXLEPUBKEYHASH[3:0]	啟用或停用 [可從 OS/SW 寫入 SGXLEPUBKEYHASH[3:0]]。 <b>SGX LE 公開金鑰雜湊 0</b> ：為 SGX 啟動飛地公開金鑰雜湊設定位元組 (0 至 7)。 <b>SGX LE 公開金鑰雜湊 1</b> ：為 SGX 啟動飛地公開金鑰雜湊設定位元組 (8 至 15)。 <b>SGX LE 公開金鑰雜湊 2</b> ：為 SGX 啟動飛地公開金鑰雜湊設定位元組 (16 至 23)。 <b>SGX LE 公開金鑰雜湊 3</b> ：為 SGX 啟動飛地公開金鑰雜湊設定位元組 (24 至 31)。
啟用/停用 SGX 自動 MP 註冊代理程式	啟用或停用 [SGX 自動 MP 註冊]。MP 註冊代理程式負責註冊平台。
SGX 原廠重設	可讓您將 SGX 選項重設為原廠設定。此選項預設為 <b>關閉</b> 。
電源按鈕	啟用或停用系統正面的電源按鈕。此選項預設為 <b>已啟用</b> 。
AC Power Recovery	可設定系統在 AC 電源恢復後的行為。此選項預設為 [持續]。 <b>i 註</b> ：完成 iDRAC Root of Trust (RoT) 前，主機系統不會開啟電源，會在接上 AC 電源後延遲至少 90 秒才開啟主機電源。
AC Power Recovery Delay	設定系統在 AC 電源恢復後延遲多久才啟動。此選項預設為 [立即]。此選項設為 <b>立即</b> 時，不會延遲開啟電源。此選項設為 <b>隨機</b> 時，系統會隨機延遲開啟電源。此選項設為 <b>使用者定義</b> 時，系統延遲時間為手動開啟電源。
User Defined Delay (60 s to 600 s)	於 <b>AC Power Recovery Delay (交流電源恢復延遲)</b> 選取 <b>User Defined (使用者定義)</b> 選項，設定 <b>User Defined Delay (使用者定義延遲)</b> 。實際的 AC 復原時間必須加上 iDRAC Root of Trust 時間 (約 50 秒)。
UEFI Variable Access	提供不同等級的 UEFI 變數安全性。若設為 [標準] (預設值)，在作業系統中會依照 UEFI 規格存取 UEFI 變數。若設為 <b>Controlled (管制)</b> ，則選取的 UEFI 變數在環境中會受到保護，且新的 UEFI 開機項目會強制列在目前開機順序的最後面。
In-Band Manageability Interface	設為 <b>已停用</b> 時，此設定會在作業系統中隱藏管理引擎 (ME)、HECI 裝置及系統的 IPMI 裝置。這可以防止作業系統變更 ME 的用電控制設定，並封鎖對所有頻內管理工具的存取行為。所有管理應透過頻外來管理。此選項預設為 <b>已啟用</b> 。 <b>i 註</b> ：BIOS 更新需要可運作的 HECI 裝置，而 DUP 更新需要可運作的 IPMI 介面。此設定須設為 [已啟用]，以避免更新錯誤。
SMM 安全性遷移	啟用或停用 UEFI SMM 安全性遷移保護。此選項應啟用以支援 Windows 2022。
Secure Boot (安全開機)	啟用 [安全開機]，其中 BIOS 會使用 [安全啟動原則] 中的憑證來驗證每個開機前映像。[安全開機] 預設為 [已停用]。
Secure Boot Policy	若 Secure Boot 原則設為 <b>標準</b> ，BIOS 會使用系統製造商的金鑰和憑證來驗證開機前映像。當 [安全開機原則] 設為 [標準] 時，BIOS 則會使用使用者定義的金鑰和憑證。[安全開機原則] 預設為 [標準]。
Secure Boot Mode	設定 BIOS 如何使用 Secure Boot 原則物件 (PK、KEK、db、dbx)。

表 22. System Security 詳細資料 (續)

選項	說明								
	<p>如果目前的模式設為「部署模式」，則可用的選項為「使用者模式」和「部署模式」。如果目前的模式設為「使用者模式」，則可用的選項為「使用者模式」、「稽核模式」和「部署模式」。</p> <p><b>表 23. Secure Boot Mode</b></p> <table border="1"> <thead> <tr> <th>選項</th> <th>說明</th> </tr> </thead> <tbody> <tr> <td><b>User Mode</b></td> <td> <p>在 <b>User Mode (使用者模式)</b> 中必須安裝 PK，然後 BIOS 會執行簽章驗證，並以編程的方式嘗試更新原則物件。</p> <p>BIOS 可讓您在模式之間進行未驗證的編程轉換。</p> </td> </tr> <tr> <td><b>稽核模式</b></td> <td> <p>在 <b>稽核模式</b> 中，PK 不存在。BIOS 不會驗證原則物件的編程更新以及模式之間的轉換。BIOS 會執行開機前映像的簽章驗證，並將結果記錄在映像執行資訊表中，但無論驗證通過或失敗都會執行映像。</p> <p>在以編程的方式確定可正常運作的原則物件時，<b>Audit Mode (稽核模式)</b> 非常實用。</p> </td> </tr> <tr> <td><b>Deployed Mode</b></td> <td> <p>「部署模式」是最安全的模式。在「部署模式」中必須安裝 PK，然後 BIOS 會執行簽章驗證，並以編程的方式嘗試更新原則物件。</p> <p>「部署模式」會限制編程模式轉換。</p> </td> </tr> </tbody> </table>	選項	說明	<b>User Mode</b>	<p>在 <b>User Mode (使用者模式)</b> 中必須安裝 PK，然後 BIOS 會執行簽章驗證，並以編程的方式嘗試更新原則物件。</p> <p>BIOS 可讓您在模式之間進行未驗證的編程轉換。</p>	<b>稽核模式</b>	<p>在 <b>稽核模式</b> 中，PK 不存在。BIOS 不會驗證原則物件的編程更新以及模式之間的轉換。BIOS 會執行開機前映像的簽章驗證，並將結果記錄在映像執行資訊表中，但無論驗證通過或失敗都會執行映像。</p> <p>在以編程的方式確定可正常運作的原則物件時，<b>Audit Mode (稽核模式)</b> 非常實用。</p>	<b>Deployed Mode</b>	<p>「部署模式」是最安全的模式。在「部署模式」中必須安裝 PK，然後 BIOS 會執行簽章驗證，並以編程的方式嘗試更新原則物件。</p> <p>「部署模式」會限制編程模式轉換。</p>
選項	說明								
<b>User Mode</b>	<p>在 <b>User Mode (使用者模式)</b> 中必須安裝 PK，然後 BIOS 會執行簽章驗證，並以編程的方式嘗試更新原則物件。</p> <p>BIOS 可讓您在模式之間進行未驗證的編程轉換。</p>								
<b>稽核模式</b>	<p>在 <b>稽核模式</b> 中，PK 不存在。BIOS 不會驗證原則物件的編程更新以及模式之間的轉換。BIOS 會執行開機前映像的簽章驗證，並將結果記錄在映像執行資訊表中，但無論驗證通過或失敗都會執行映像。</p> <p>在以編程的方式確定可正常運作的原則物件時，<b>Audit Mode (稽核模式)</b> 非常實用。</p>								
<b>Deployed Mode</b>	<p>「部署模式」是最安全的模式。在「部署模式」中必須安裝 PK，然後 BIOS 會執行簽章驗證，並以編程的方式嘗試更新原則物件。</p> <p>「部署模式」會限制編程模式轉換。</p>								
<b>Secure Boot Policy Summary</b>	指定安全啟動用來驗證映像的認證和雜湊清單。								
<b>Secure Boot Custom Policy Settings</b>	設定「安全開機原則」。若要啟用此選項，請將 Secure Boot Policy (Secure Boot 原則) 設為 <b>Custom (自訂)</b> 選項。								

## 建立系統及設定密碼

### 事前準備作業

確認密碼跳線已啟用。密碼跳線可啟用或停用系統密碼和設定密碼功能。如需詳細資訊，請參閱「系統跳線設定」一節。

**註:** 如果密碼跳線設定停用，將會刪除現有的系統密碼和設定密碼，而您不需要輸入系統密碼即可啟動系統。

### 步驟

- 若要進入 System Setup，請在開啟或重新啟動系統後，立即按下 F2 鍵。
- 在 **System Setup Main Menu (系統設定主選單)** 畫面上，按一下 **系統 BIOS >** 的系統安全性。
- 在 **系統安全性** 畫面中，確認 **Password Status** 已設為 **Unlocked**。
- 在 **System Password** 欄位中，輸入您的系統密碼，然後按下 Enter 或 Tab 鍵。  
指定系統密碼時，請遵循以下準則：
  - 密碼長度不超過 32 個字元。

畫面會出現訊息，提示您重新輸入系統密碼。
- 重新輸入系統密碼，然後按一下 **OK**。
- 在 **Setup Password** 欄位中，輸入您的設定密碼，然後按下 Enter 或 Tab 鍵。  
出現訊息提示您重新輸入設定密碼。
- 重新輸入設定密碼，然後按一下 **OK (確定)**。
- 按下 Esc 鍵返回系統 BIOS 畫面。再次按下 Esc 鍵。  
出現訊息提示您儲存變更。

**註:** 在系統重新啟動前，密碼保護不會生效。

## 使用系統密碼來保護系統

### 關於此工作

如果已指定設定密碼，系統將接受您的設定密碼作為替代系統密碼。

### 步驟

1. 開啟或重新啟動系統。
2. 輸入系統密碼，然後按下 Enter 鍵。

### 後續步驟

如果 **Password Status** 設為 **Locked**，重新開機後出現提示時，請輸入系統密碼並按下 Enter 鍵。

**註:** 如果輸入的系統密碼不正確，系統會顯示訊息，提示您重新輸入密碼。您有三次機會可嘗試輸入正確密碼。第三次嘗試失敗後，系統會顯示錯誤訊息，說明系統已經停止運作，必須關閉。即使您關閉並重新啟動系統，錯誤訊息仍會持續顯示於畫面上，直到您輸入正確的密碼為止。

## 刪除或變更系統與設定密碼

### 事前準備作業

**註:** 如果「密碼狀態」設為「鎖定」，您便無法刪除或變更現有的系統或設定密碼。

### 步驟

1. 若要進入系統設定，請在開啟或重新啟動系統後，立即按 F2 鍵。
2. 在 **System Setup Main Menu** 畫面中，按一下 **System BIOS > System Security**。
3. 在 **System Security (系統安全性)** 畫面，確認 **Password Status (密碼狀態)** 設為 **Unlocked (解除鎖定)**。
4. 在 **System Password** 欄位中，變更或刪除現有的系統密碼，然後按下 Enter 或 Tab 鍵。
5. 在 **設定密碼** 欄位中，變更或刪除現有的設定密碼，然後按下 Enter 或 Tab 鍵。  
如果您變更系統與設定密碼，則會出現訊息提示您重新輸入新密碼。如果您刪除系統與設定密碼，則會出現訊息提示您確認是否刪除。
6. 按下 Esc 鍵返回「系統 BIOS」畫面。再次按下 Esc 鍵，之後會出現訊息提示您儲存變更。
7. 選取「設定密碼」，變更或刪除現有的設定密碼，並按下 Enter 或 Tab 鍵。  
**註:** 若您變更系統密碼或設定密碼，之後會出現訊息提示您重新輸入新密碼。若您刪除系統密碼或設定密碼，之後會出現訊息提示您確認是否刪除。

## 在啟用設定密碼的情況下作業

如果 **Setup Password (設定密碼)** 設為 **Enabled (啟用)**，則必須先輸入正確的設定密碼，才能修改系統設定選項。

如果您在三次嘗試機會內輸入的密碼皆不正確，系統會顯示下列訊息：

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted! Must power down.
```

即使您關閉並重新啟動系統，錯誤訊息仍會持續顯示，直到您輸入正確的密碼為止。下列選項為例外情形：

- 如果 **System Password (系統密碼)** 並未設為 **Enabled (啟用)**，也未透過 **Password Status (密碼狀態)** 選項鎖定，您可以指定系統密碼。如需詳細資訊，請參閱「系統安全性設定畫面」一節。
- 您無法停用或變更現有的系統密碼。

**註:** 您可以使用密碼狀態選項和設定密碼選項來保護系統密碼，以防止未經授權的變更。

## Redundant OS Control

若要檢視 Redundant OS Control 畫面，請開啟系統電源並按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > Redundant OS Control**。

表 24. Redundant OS Control 詳細資料

選項	說明
Redundant OS Location	可讓您從下列裝置選取備份磁碟： <ul style="list-style-type: none"><li>● 無</li><li>● IDSDM</li><li>● SATA Ports in AHCI mode</li><li>● BOSS PCIe Cards (Internal M.2 Drives)</li><li>● 內建 USB<ul style="list-style-type: none"><li>① 註: RAID 組態與 NVMe 卡並未包含在內，因為 BIOS 無法在這些組態中區分個別磁碟機。</li></ul></li><li>● 內部 SD 卡</li></ul>
Redundant OS State	<ul style="list-style-type: none"><li>① 註: 如果 Redundant OS Location (備援作業系統位置) 設為 None (無)，則會停用此選項。</li></ul> 設為 Visible (可見) 時，開機清單和作業系統中會顯示備份磁碟。設為 Hidden (隱藏) 時，備份磁碟會停用，且不會顯示於開機清單和作業系統中。此選項預設為 Visible (可見)。 <ul style="list-style-type: none"><li>① 註: BIOS 會停用硬體中的裝置，使作業系統無法加以存取。</li></ul>
Redundant OS Boot	<ul style="list-style-type: none"><li>① 註: 如果 Redundant OS Location (備援作業系統位置) 設為 None (無)，或 Redundant OS State (備援作業系統狀態) 設為 Hidden (隱藏)，則會停用此選項。</li></ul> 設為 Enabled (已啟用) 時，BIOS 會開機進入 Redundant OS Location (備援作業系統位置) 所指定的裝置。設為 Disabled (已停用) 時，BIOS 會保留目前的開機清單設定。此選項預設為已停用。

## 其他設定

若要檢視 Miscellaneous Settings 畫面，請開啟系統電源並按下 F2 鍵，然後按一下 **System Setup Main Menu > System BIOS > Miscellaneous Settings**。

表 25. Miscellaneous Settings 詳細資訊

選項	說明
系統時間	可讓您設定系統的時間。
系統日期	可讓您設定系統的日期。
資產標籤	指定資產標籤，可讓您基於安全和追蹤等目的加以修改。
Keyboard NumLock	可讓您設定在系統開機時 NumLock 為啟用或停用。此選項預設為「開啟」。 <ul style="list-style-type: none"><li>① 註: 此選項不適用於 84 鍵的鍵盤。</li></ul>
F1/F2 Prompt on Error	啟用或停用 F1/F2 Prompt on Error (出現錯誤時顯示 F1/F2 提示)。此選項預設為已啟用。F1/F2 提示亦包含鍵盤錯誤。
Load Legacy Video Option ROM	啟用或停用 Load Legacy Video Option ROM 選項。此選項預設為已停用。
Dell Wyse P25/P45 BIOS Access	啟用或停用 Dell Wyse P25/P45 BIOS 存取。此選項預設為已啟用。
Power Cycle Request	啟用或停用 Power Cycle Request (重新啟動電源要求)。此選項預設為「無」。

## iDRAC 設定公用程式

iDRAC 設定公用程式是使用 UEFI 來設定及配置 iDRAC 參數的介面。您可以使用 iDRAC 設定公用程式來啟用或停用各種 iDRAC 參數。

**註:** 在 iDRAC 設定公用程式使用部分功能，需要 iDRAC Enterprise 授權升級。

如需有關使用 iDRAC 的詳細資訊，請參閱《Integrated Dell Remote Access Controller User's Guide》(Integrated Dell Remote Access Controller 使用者指南)，網址為：<https://www.dell.com/idracmanuals>。

## 裝置設定

**Device Settings** 可讓您設定裝置參數，例如儲存控制器或網路卡。

## Dell Lifecycle Controller

Dell Lifecycle Controller (LC) 提供進階內嵌系統管理功能，包括系統部署、組態設定、更新、維護及診斷。LC 屬於 iDRAC 頻外解決方案和 Dell 系統內嵌整合可延伸韌體介面 (UEFI) 應用程式的一部分。

## 嵌入式系統管理

Dell Lifecycle Controller 可以在系統的整個生命週期期間提供進階內嵌系統管理功能。Dell Lifecycle Controller 可在開機順序期間啟動，且可獨立於作業系統外運作。

**註:** 某些平台組態可能不支援 Dell Lifecycle Controller 提供的完整功能集。

如需有關設定 Dell Lifecycle Controller、設定硬體與韌體，以及部署作業系統的詳細資訊，請參閱 Dell Lifecycle Controller 說明文件，網址為：<https://www.dell.com/idracmanuals>。

## 開機管理程式

**Boot Manager** 選項可讓您選取開機選項和診斷公用程式。

若要進入 **Boot Manager**，請開啟系統電源，然後按下 F11 鍵。

表 26. Boot Manager 詳細資料

選項	說明
繼續正常開機	系統會從開機順序的第一個項目開始嘗試啟動到裝置。如果開機嘗試失敗，系統會繼續嘗試開機順序的下個項目，直到開機成功或找不到任何開機選項為止。
單次啟動選單	讓您存取開機功能表，您可以在其中選取用於開機的單次開機裝置。
啟動系統設定	可讓您使用系統設定。
啟動 Lifecycle Controller	退出開機管理員，並叫出 Dell Lifecycle Controller 程式。
系統公用程式	可讓您啟動系統公用程式選單，例如 Launch Diagnostics、BIOS Update File Explorer、Reboot System。

## PXE 啟動

您可以使用開機前執行環境 (PXE) 選項，以從遠端開機並設定已連線至網路的系統。

若要存取 **PXE boot (PXE 開機)** 選項，請啟動系統並在 POST 期間按下 F12，而非從 BIOS Setup (BIOS 設定) 使用標準開機順序。這麼做不會叫出任何選單也無法管理網路裝置。