# Dell EMC PowerEdge R750xa

## BIOS and UEFI Reference Guide

Part Number: E71S
Regulatory Type: E71S001
July 2021
Rev. A02

## 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。**

# Contents

# 1

# 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

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：www.dell.com/poweredgemanuals。 |
| **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 磁碟機，您必須將此欄位與 **SATA Settings (SATA 設定)** 選單中的 **Embedded SATA (嵌入式 SATA)** 欄位設為 **RAID** 模式。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 (非 RAID)** 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。<br>您可以在 **Device Settings (裝置設定)** 選單管理傳統網路設定。<br>**註:** 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 **Enabled** 和 **Disabled**。此選項預設為**已停用**。 |
| **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 **Optimizer Mode**。 |
| **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 **Enabled (啟用)**，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**已停用**。 |
| **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**啟用**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 **Disabled (已停用)**。 |
| **記憶體訓練** | 此選項設為**快速**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**下次開機時重新訓練**以強制進行一次完整記憶體訓練步驟，之後再回復為**快速**。<br><br>此選項設為**下次開機時重新訓練**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。<br><br>此選項設為**啟用**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。 |
| **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**已啟用**。 |
| **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**停用**，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**已啟用**，則 BIOS 會顯示所有邏輯處理器。如果此選項設為**已停用**，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**已啟用**。 |
| **CPU Interconnect Speed** | 可讓您管理系統中各處理器間的通訊連結頻率。<br>**註:** 標準和基本等級的處理器支援的連結頻率較低。 |

### 表 5. Processor Settings 詳細資料 (續)

| 選項 | 說明 |
|---|---|
| | 可用選項包含**最大資料速率**、**11.2 GT/秒**、**10.4 GT/秒** 及 **9.6 GT/秒**。此選項預設為**最大資料速率**。<br><br>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。<br><br>為發揮最佳效能，您應選取**最大資料速率**。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。<br><br>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。 |
| **Virtualization Technology** | 啟用或停用處理器的虛擬化技術。此選項預設為**已啟用**。 |
| **目錄模式** | 啟用或停用目錄模式。此選項預設為**已啟用**。 |
| **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**已啟用**。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**已啟用**。 |
| **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**已啟用**。 |
| **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**已啟用**。 |
| **Sub NUMA Cluster** | 啟用或停用子 NUMA 叢集。此選項預設為**已停用**。 |
| **MADT Core Enumeration** | 指定 MADT Core Enumeration。此選項預設為**循環制**。 |
| **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**已啟用**。 |
| **XPT 預先擷取** | 此選項預設為**已啟用**。 |
| **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**已啟用**。 |
| **截止線 LLC 分配** | 啟用或停用截止線 LLC 分配。此選項預設為**已啟用**。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**已停用**。 |
| **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 **Disabled (停用)**。<br>**註:** 「CPU 電源管理」設為**最大效能**時，系統不支援此功能。 |
| **AVX P1** | 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 **Normal**。 |

### 表 5. Processor Settings 詳細資料 (續)

| 選項 | 說明 |
|---|---|
| | **註:** 此選項僅存在於特定的處理器庫存單元 (SKU)。 |
| **動態 SST 效能設定檔** | 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**已停用**。 |
| **SST-Performance Profile** | 可讓您使用快速選取技術重新設定處理器。 |
| **Intel SST-BF** | 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**已停用**。 |
| **Intel SST-CP** | 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**已停用**。 |
| **x2APIC Mode** | 啟用或停用 x2APIC 模式。此選項預設為**已啟用**。<br>**註:** 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)。 |
| **AVX ICCP 預先授予授權** | 啟用或停用 AVX ICCP 預先授予授權。此選項預設為**已停用**。 |
| **AVX ICC 預先授予等級** | 可讓您選取 Intel 提供的不同 AVX ICC 轉換等級。此選項預設為 **128 高強度**。 |
| **Dell Controlled Turbo** | |
| **Dell Controlled Turbo 設定** | 控制渦輪加速介入方式。僅可在「系統設定檔」設為**效能**或**自訂**，且「CPU 電源管理」設為**效能**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**已停用**。<br>**註:** 視安裝的處理器數量而定，最多可能會有二個處理器清單。 |
| **Dell AVX Scaling Technology** | 可讓您設定 Dell AVX 調整技術。此選項預設為 **0**。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。 |
| **Optimizer Mode (最佳化模式)** | 啟用或停用 CPU 效能。此選項設為**自動**時，會將「CPU 電源管理」設為「最大效能」。設為**已啟用**時，會啟用「CPU 電源管理」設定。設為**已停用**時，會停用「CPU 電源管理」選項。此選項預設為 **Auto (自動)**。 |
| **Number of Cores per Processor** | 控制每個處理器中啟用的核心數目。此選項預設為 **All (全部)**。 |
| **Processor Core Speed** | 指定處理器最大核心頻率。 |
| **Processor Bus Speed** | 指定處理器的匯流排速度。<br>**註:** 兩個處理器皆安裝時，才會顯示處理器匯流排速度選項。 |
| **本機電腦檢查例外狀況** | 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**已停用**。 |
| **Processor n** | **註:** 視處理器的數量而定，最多可能會列出 n 顆處理器。<br>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 **Off**、**AHCI mode** 或 **RAID modes**。此選項預設為 **AHCI Mode (AHCI 模式)**。<br>**註:**<br>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。<br>2. 在 RAID 模式下，不支援 ESXi 和 Ubuntu 作業系統。 |
| **Security Freeze Lock** | 在 POST 期間，將 **Security Freeze Lock (安全凍結鎖定)** 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。<br>在 **AHCI 模式**或 **RAID 模式**中，BIOS 支援一律為啟用。<br>**表 8. Port n**<br>**選項** / **說明**<br>**Model** — 指定選取裝置的磁碟機機型。<br>**Drive Type** — 指定連接 SATA 連接埠的磁碟機類型。<br>**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。 |

### 表 9. NVMe 設定詳細資料 (續)

| 選項 | 說明 |
|---|---|
| **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**。<br>**警示: 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。**<br>**註:** 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。<br>**註:** 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。 |

#### 表 11. UEFI 開機設定

| 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。

   **警示: 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。

## 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 |
|---|---|
| **UEFI PXE Settings** | 可讓您控制 UEFI PXE 裝置的組態。 |
| **PXE Device n** (n = 1 至 4) | 啟用或停用裝置。啟用時，系統會為裝置建立 UEFI PXE 開機選項。 |
| **PXE Device n Settings** (n = 1 至 4) | 可讓您控制 PXE 裝置的組態。 |
| **UEFI HTTP Settings** | 可讓您控制 UEFI HTTP 裝置的組態。 |
| **HTTP Device n** (n = 1 至 4) | 啟用或停用裝置。啟用時，系統會為裝置建立 UEFI HTTP 開機選項。 |
| **HTTP Device n Settings** (n = 1 至 4) | 可讓您控制 HTTP 裝置的組態。 |
| **UEFI iSCSI Settings** | 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 |
|---|---|
| **介面** | 指定用於此 PXE 裝置的 NIC 介面。 |
| **Protocol (通訊協定)** | 指定用於 PXE 裝置的通訊協定。此選項可設為 **IPv4** 或 **IPv6**。此選項預設為 **IPv4**。 |
| **Vlan** | 啟用 PXE 裝置的 Vlan。此選項可設為 **Enable** 或 **Disable**。此選項預設為 **Disable (停用)**。 |

### 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 **Disabled (已停用)**。 |
| **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 **Disable (停用)**。 |
| **連線 2** | 啟用或停用 iSCSI 連線。此選項預設為 **Disable (停用)**。 |
| **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** | 設定使用者可存取的 USB 連接埠。選取**僅開啟背面連接埠**可停用正面 USB 連接埠；選取**關閉所有連接埠**可停用所有正面和背面 USB 連接埠；選取**關閉所有連接埠 (動態)** 可於 POST 期間停用所有正面和背面 USB 連接埠。此選項預設為**開啟所有連接埠**。<br>使用者可存取的 USB 連接埠設為**關閉所有連接埠 (動態)** 時，會啟用**僅啟用正面連接埠**選項。<br>• **僅啟用正面連接埠**：在作業系統執行階段啟用或停用正面 USB 連接埠。 |
| | 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。 |
| **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**開啟**或**關閉**。若設為 **OFF (關閉)**，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「開啟」。 |
| **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「開啟」。 |
| **Internal SD Card Redundancy** | 設定內部雙 SD 模組 (IDSDM) 的備援模式。設為 **Mirror (鏡像)** 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。<br>當「內部 SD 卡備援」設為**已停用**時，作業系統只會顯示主要 SD 卡。此選項預設為**已停用**。 |
| **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 **Disabled (OS)**，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 NIC1 和 NIC2** 選項。 |
| **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** | 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 **Enabled (啟用)**，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 **停用**，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**。<br>**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。 |
| **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。 |
| **Current State of Embedded Video Controller** | 顯示嵌入式影像控制器目前的狀態。**Current State of Embedded Video Controller (嵌入式影像控制器的目前狀態)** 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 **Enabled (啟用)**，作業系統會初始化計時器。若此選項設為**停用** (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 **12 TB**，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 **512 GB**，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 **56 TB**。 |
| **Slot Disablement** | 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。 |
| | **Slot n**：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**。 |
| **插槽分支** | **Auto Discovery Bifurcation Settings** 可讓您設定 **Platform Default Bifurcation**、 及 **Manual bifurcation Control**。 |
| | 此選項預設為**平台預設分支**。設為 **Manual bifurcation Control** 時，插槽分支欄位可供存取；設為 **Platform Default Bifurcation** 時，欄位會呈灰色，無法使用。<br>**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。 |

## 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** | 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。<br>沒有 COM 序列埠 (DB9) 之系統可用的選項為**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**。此選項預設為「關閉」。<br>有 COM 序列埠 (DB9) 之系統可用的選項為**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**。此選項預設為 **Auto (自動)**。 |
| **Serial Port Address** | 可讓您設定序列裝置的連接埠位址。此選項預設為 **Serial Device1=COM2, Serial Device 2=COM1**。<br>**註:** 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。<br>**註:** 每次系統開機時，BIOS 會與儲存在 iDRAC 的序列 MUX 設定同步。您可在 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。 |
| **External Serial Connector** | 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 **Serial Device 1 (序列裝置 1)**。<br>**註:** 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。<br>**註:** 每次系統開機時，BIOS 會與儲存在 iDRAC 的序列 MUX 設定同步。您可在 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。 |
| **Failsafe Baud Rate** | 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 **115200**。 |
| **Remote Terminal Type** | 設定遠端主控台終端機類型。此選項預設為 **VT100/VT220**。 |
| **Redirection After Boot** | 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**。 |

## 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** | 設定系統設定檔。如果您將 System Profile (系統設定檔) 選項設為 **Custom (自訂)** 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 **Performance Per Watt (DAPC) (每瓦效能最佳化 (DAPC))**。其他選項包括**效能**、**每瓦效能 (OS)**、**工作站效能**及**自訂**。<br>**註: System Profile (系統設定檔)** 選項設為 **Custom (自訂)** 時，才能獲得系統設定檔設定畫面的所有參數。 |

### 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 **Enabled** (作業系統控制) 或設為 **Autonomous** (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 **Standard (標準)**。 |
| **Memory Refresh Rate** | 設定 1x 或 2x 的記憶體重新整理頻率。此選項預設為 **1x**。 |
| **Uncore Frequency** | 可讓您選取**非核心頻率**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。**能源效率原則**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**能源效率原則**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 **Balanced Performance (平衡的效能)**。 |
| **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**。<br>**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。<br>**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。 |
| **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**。 |
| **處理器 EIST** | 啟用或停用 PCI **處理器 EIST**。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**模式 0**。 |
| **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 **BW 最佳化**，則效能會針對 DDR 與 DDRT 頻寬最佳化。若此選項設為 **Latency Optimized**，則在效能方面，DDR 延遲的情況會較為理想。此選項預設為 **BW 最佳化**。 |

## System Security

To view the **System Security** screen, power on the system, press F2, and click **System Setup Main Menu** > **System BIOS** > **System Security**.

### Table 19. System Security details

| Option | Description |
|---|---|
| **CPU AES-NI** | Improves the speed of applications by performing encryption and decryption by using the Advanced Encryption Standard Instruction Set (AES-NI). This option is set to **Enabled** by default. |
| **System Password** | Sets the 系統 password. This option is set to **Enabled** by default and is read-only if the password jumper is not installed in the 系統. |

### Table 19. System Security details (continued)

| Option | Description |
|---|---|
| **Setup Password** | Sets the setup password. This option is read-only if the password jumper is not installed in the system. |
| **Password Status** | Locks the 系統 password. This option is set to **Unlocked** by default. |
| **TPM Information** | Indicates the type of Trusted Platform Module, if present. |

### Table 20. TPM 1.2 security information

| Option | Description |
|---|---|
| **TPM Information** | |
| **TPM Security** | **NOTE:** The TPM menu is available only when the TPM module is installed.<br>Enables you to control the reporting mode of the TPM. The **TPM Security** option is set to **Off** by default. You can only modify the TPM Status, and TPM Activation if the **TPM Status** field is set to either **On with Pre-boot Measurements** or **On without Pre-boot Measurements**.<br>When TPM 1.2 is installed, the **TPM Security** option is set to **Off**, **On with Pre-boot Measurements**, or **On without Pre-boot Measurements**. |
| **TPM Information** | Changes the operational state of the TPM. This option is set to **No Change** by default. |
| **TPM Firmware** | Indicates the firmware version of the TPM. |
| **TPM Status** | Specifies the TPM status. |
| **TPM Command** | Controls the Trusted Platform Module (TPM). When set to **None**, no command is sent to the TPM. When set to **Activate**, the TPM is enabled and activated. When set to **Deactivate**, the TPM is disabled and deactivated. When set to **Clear**, all the contents of the TPM are cleared. This option is set to **None** by default. |

### Table 21. TPM 2.0 security information

| Option | Description |
|---|---|
| **TPM Information** | |
| **TPM Security** | **NOTE:** The TPM menu is available only when the TPM module is installed.<br>Enables you to control the reporting mode of the TPM. The **TPM Security** option is set to **Off** by default. You can only modify the TPM Status, and TPM Activation if the **TPM Status** field is set to either **On with Pre-boot Measurements** or **On without Pre-boot Measurements**.<br>When TPM 2.0 is installed, the **TPM Security** option is set to **On** or **Off**. This option is set to **Off** by default. |
| **TPM Information** | Changes the operational state of the TPM. This option is set to **No Change** by default. |
| **TPM Firmware** | Indicates the firmware version of the TPM. |
| **TPM Hierarchy** | Enables, disables, or clears the storage and endorsement hierarchies. When set to **Enabled**, the storage and endorsement hierarchies can be used.<br>When set to **Disabled**, the storage and endorsement hierarchies cannot be used.<br>When set to **Clear**, the storage and endorsement hierarchies are cleared of any values, and then reset to **Enabled**. |
| **TPM Advanced Settings** | Specifies TPM Advanced Settings details. |

### Table 22. System Security details

| Option | Description |
|---|---|
| **Intel(R) TXT** | Enables you to set the Intel Trusted Execution Technology (TXT) option. To enable the **Intel TXT** option, virtualization technology and TPM Security must be enabled with Pre-boot measurements. This option is set to **Off** by default. |
| **Memory Encryption** | Enables or disables the Intel Total Memory Encryption (TME). When option is set to **Disabled**, BIOS disables both TME and MK-TME technology. When option is set to **Enabled**, BIOS enables the TME technology. This option is set to **Disabled** by default. |
| **Intel(R) SGX** | Enables you to set the Intel Software Guard Extension (SGX) option. To enable the **Intel SGX** option, processor must be SGX capable, memory population must be compatible (minimum x8 identical DIMM1 to DIMM8 per CPU socket), memory operating mode must be set at optimizer mode, memory encryption must be enabled and node interleaving must be disabled. This option is set to **Off** by default. When this option is to **Off**, BIOS disables the SGX technology. When this option is to **On**, BIOS enables the SGX technology. |
| **SGX Package Info In-Band Access** | Enables you to access the Intel Software Guard Extension (SGX) package info in-band option. This option is set to **Off** by default. |
| **PPMRR Size** | Sets the PPMRR size. |
| **SGX QoS** | Enables or disables the SGX quality of service. |
| **Select Owner EPOCH input type** | Enables you to select **Change to New random Owner EPOCHs** or **Manual User Defined Owner EPOCHs**. Each EPOCH is 64-bit. After generating new EPOCH by selecting **Change to New random Owner EPOCHs**, the selection reverts back to **Manual User Defined Owner EPOCHs**. |
| | **Software Guard Extensions Epoch n**: Sets the Software Guard Extensions Epoch values. |
| **Enable writes to SGXLEPUBKEYHASH[3:0] from OS/SW** | Enables or disables the Enable writes to SGXLEPUBKEYHASH[3:0] from OS/SW. |
| | **SGX LE Public Key Hash0**: Sets the bytes from 0-7 for SGX Launch Enclave Public Key Hash. |
| | **SGX LE Public Key Hash1**: Sets the bytes from 8-15 for SGX Launch Enclave Public Key Hash. |
| | **SGX LE Public Key Hash2**: Sets the bytes from 16-23 for SGX Launch Enclave Public Key Hash. |
| | **SGX LE Public Key Hash3**: Sets the bytes from 24-31 for SGX Launch Enclave Public Key Hash. |
| **Enable/Disable SGX Auto MP Registration Agent** | Enables are disables the SGX Auto MP Registration. The MP registration agent is responsible to register the platform. |
| **SGX Factory Reset** | Enables you to reset the SGX option to factory settings. This option is set to **Off** by default. |
| **Power Button** | Enables or disables the power button on the front of the 系統. This option is set to **Enabled** by default. |
| **AC Power Recovery** | Sets how the system behaves after AC power is restored to the 系統. This option is set to **Last** by default.<br>**NOTE:** The host system will not power on up until iDRAC Root of Trust (RoT) is completed, host power on will be delayed by minimum 90 seconds after the AC applied. |
| **AC Power Recovery Delay** | Sets the time delay for the system to power up after AC power is restored to the 系統. This option is set to **Immediate** by default. When this option is set to **Immediate**, there is no delay for power up. When this option is set to **Random**, the system creates a random delay for power up. When this option is set to **User Defined**, the system delay time is manually to power up. |

### Table 22. System Security details (continued)

| Option | Description |
|---|---|
| **User Defined Delay (60 s to 600 s)** | Sets the **User Defined Delay** option when the **User Defined** option for **AC Power Recovery Delay** is selected. |
| **UEFI Variable Access** | Provides varying degrees of securing UEFI variables. When set to **Standard** (the default), UEFI variables are accessible in the operating system per the UEFI specification. When set to **Controlled**, selected UEFI variables are protected in the environment and new UEFI boot entries are forced to be at the end of the current boot order. |
| **In-Band Manageability Interface** | When set to **Disabled** , this setting hides the Management Engine's (ME), HECI devices, and the system's IPMI devices from the operating system. This prevents the operating system from changing the ME power capping settings, and blocks access to all in-band management tools. All management should be managed through out-of-band. This option is set to **Enabled** by default.<br>**NOTE:** BIOS update requires HECI devices to be operational and DUP updates require IPMI interface to be operational. This setting needs to be set to Enabled to avoid updating errors. |
| **SMM Security Migration** | Enables or disables the UEFI SMM security migration protections. |
| **Secure Boot** | Enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is set to **Disabled** by default. |
| **Secure Boot Policy** | When Secure Boot policy is set to **Standard**, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot policy is set to **Custom**, the BIOS uses the user-defined key and certificates. Secure Boot policy is set to **Standard** by default. |
| **Secure Boot Mode** | Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx).<br>If the current mode is set to **Deployed Mode**, the available options are **User Mode** and **Deployed Mode**. If the current mode is set to **User Mode**, the available options are **User Mode**, **Audit Mode**, and **Deployed Mode**. |
| **Secure Boot Policy Summary** | Specifies the list of certificates and hashes that secure boot uses to authenticate images. |
| **Secure Boot Custom Policy Settings** | Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to **Custom** option. |

#### Table 23. Secure Boot Mode

| Options | Descriptions |
|---|---|
| **User Mode** | In **User Mode**, PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects.<br>The BIOS allows unauthenticated programmatic transitions between modes. |
| **Audit mode** | In **Audit Mode**, PK is not present. BIOS does not authenticate programmatic update to the policy objects and transitions between modes. The BIOS performs a signature verification on pre-boot images and logs the results in the image Execution Information Table, but executes the images whether they pass or fail verification.<br>**Audit Mode** is useful for programmatic determination of a working set of policy objects. |
| **Deployed Mode** | **Deployed Mode** is the most secure mode. In **Deployed Mode**, PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects.<br>**Deployed Mode** restricts the programmatic mode transitions. |

## 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

1. 若要進入 System Setup，請在開啟或重新啟動系統後，立即按下 F2 鍵。
2. 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。**
3. 在 **系統安全性** 畫面中，確認 **Password Status** 已設為 **Unlocked。**
4. 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。
5. 重新輸入系統密碼，然後按一下 **OK。**
6. 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。
7. 重新輸入設定密碼，然後按一下 **OK（確定）**。
8. 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)** 設定為 **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：<br>• **無**<br>• **IDSDM**<br>• **SATA Ports in AHCI mode**<br>• **BOSS PCIe Cards (Internal M.2 Drives)**<br>• **內建 USB**<br>**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。<br>• **內部 SD 卡** |
| **Redundant OS State** | **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。<br>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)**。<br>**註:** BIOS 會停用硬體中的裝置，使作業系統無法加以存取。 |
| **Redundant OS Boot** | **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。<br>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」。<br>**註:** 此選項不適用於 84 鍵的鍵盤。 |
| **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。