

# INTEL-SA-00075 偵測與安全防護 工具指南

Intel® 主動管理技術 (Intel® AMT)、Intel® 標準管理功能 (ISM) 以及  
Intel® 小型企業技術 (SBT)

## 偵測和安全防護 INTEL-SA-00075 的說明

修訂版本 1.1 – 2017 年 7 月 20 日

---

### 簡介

本文件會逐步帶領您進行偵測和防護 INTEL-SA-00075 中所述的安全性弱點的多個處理序。如需詳細資訊，請參閱在 <https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr> 的公共安全諮詢。

**如果您是一台電腦的使用者，而您希望判斷其狀態：**我們提供 INTEL-SA-00075 偵測圖形使用者介面的應用程式 (Intel-SA-00075-gui.exe) 來進行單一或獨立系統的本機分析。

**如果您想要判斷的狀態及/或套用多部電腦的防護功能：**我們提供 INTEL-SA-00075 偵測與安全工具主控台 (Intel-SA-00075-console.exe) 應用程式。此工具可以執行探索並寫入其結果到本機 Windows 登錄，以及（選擇性）到 XML 檔案，供後續收集和分析用。主控台應用程式也可以協助實作安全防護。如需詳細資訊，請參閱第 2 頁的 *使用 INTEL-SA-00075 偵測與安全防護工具*。

**如果您是網路管理員且已經在使用 Intel® 安裝及組態軟體 (Intel® SCS)：**Intel® SCS 套件包含一個替代方案、主控台工具、Intel® SCS 系統探索公用程式。如果您已經熟悉 Intel® SCS 工具，或是想要進一步瞭解 Intel® 主動管理技術的詳細資料，我們建議您使用此工具請參閱第 111 頁的 *使用 Intel® SCS 系統探索公用程式*。

## 安全防護

本文件所述的安全防護步驟旨在避免未經授權的啟動，而且使用可管理的 Intel Sku、Intel® 主動管理技術 (Intel® 主動管理技術)、Intel® 標準管理功能 (ISM)，以及 Intel® 小型企業技術 (小型企業技術)，套用解決弱點的韌體更新。

IT 從業人員可以使用這些指示做為指令碼的基礎，或安全防護步驟的大規模部署的管理主控台內的作業。實作安全防護程序的步驟如下：

1. 解除佈建 Intel 管理性 SKU 用戶端來防禦取得系統權限的無權限網路攻擊者
2. 停用或移除本機管理性服務 (LMS) 來防禦無權限本機攻擊者取得系統的權限
3. 選擇性設定本機管理性設定的限制

Intel 強烈建議所有安全防護路徑中的第一個步驟是解除佈建 Intel 管理性 SKU，以處理網路權限提升弱點問題。對於已佈建的系統，必須在停用或移除 LMS 之前先執行取消佈建。等待更新的 Intel 管理性 SKU 韌體推出時，Intel 強烈建議透過移除或停用 LMS 來防護本機權限提升。（選擇性）做為防止不小心重新安裝或重新啟用 LMS 的第二層防禦，部分透過作業系統執行的管理性組態選項，可以額外透過作業系統 (OS) 停用；不過，這些額外的本機管理性設定限制對於如何允許其反向作業有所約束。

**附註：** AMT 6.0.x 不支援主機端佈建/用戶端控制模式，因此無法透過本機作業系統介面使用 INTEL-SA-00075 偵測與安全防護工具解除佈建。對於使用管理性韌體 6.0.x.x 或 6.1.x.x 的平台，需要完整使用 Intel SCS 套件的 ACUConfig /full 或透過系統 MEBx 來完整解除佈建

如需協助您實作本文件所提供的安全防護步驟，請聯絡 [Intel 客戶支援](#)。從「技術」區段選取 Intel® 主動管理技術 (Intel® AMT)。

## 使用 INTEL-SA-00075 偵測與安全防護工具

### INTEL-SA-00075 偵測與安全防護工具是什麼？

INTEL-SA-00075 偵測與安全防護工具可供本機使用者或 IT 管理員用來判斷系統是否容易受到攻擊，以記載於 Intel 的安全諮詢 INTEL-SA-00075。主控台版本的工具可用來進行安全防護步驟。

偵測與安全防護工具提供兩種版本。

- 第一個是互動式圖形使用者介面工具，執行時可探索裝置的硬體和軟體詳細資訊，並提供風險評估的指示。想要進行系統的本機評估時，建議使用此版本。
- 第二個版本是可以執行風險評估和執行建議安全防護步驟的主控台可執行檔。探索資訊可以選擇性地儲存到 Windows\* 登錄檔和（或）到 XML 檔。此版本對於想要在多部電腦中執行大量探索和安全防護作業的 IT 管理員來說更加便利。

## 取得 INTEL-SA-00075 偵測與安全防護工具

INTEL-SA-00075 偵測與安全防護工具下載套件位於：

<https://www.intel.com/content/www/tw/zh/support/technologies/000024133.html>。

## 系統需求

- Microsoft Windows\* 7、8、8.1 或 10
- 本機作業系統管理員存取權

## 安裝工具

### 互動式安裝

執行 INTEL-SA-00075 Detection and Mitigation Tool.msi，並依照螢幕上的提示進行。

### 無訊息安裝

msiexec.exe /i INTEL-SA-00075 Detection and Mitigation Tool.msi /qn

如此將會將「INTEL-SA-00075 偵測與安全防護工具安裝在預設目錄中。

C:\Program Files (x86)\Intel\Intel-SA-00075 Detection and Mitigation Tool\

## 解除安裝工具

### 互動式解除安裝

執行 INTEL-SA-00075 Detection and Mitigation Tool.msi，並依照螢幕上的提示進行。

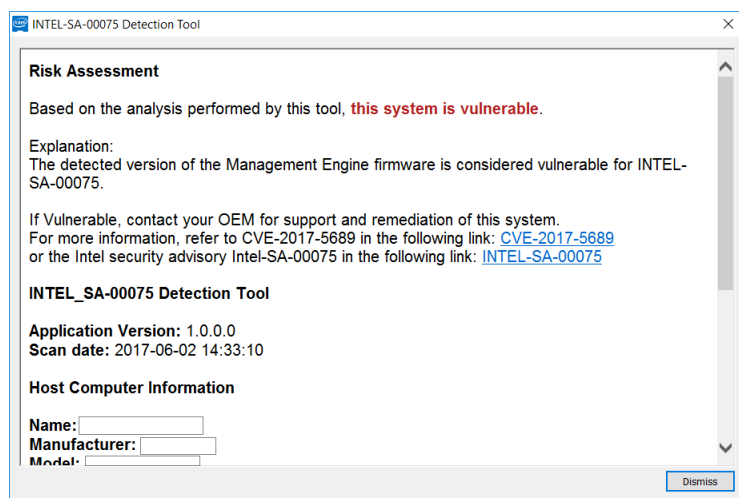
### 無訊息解除安裝

msiexec.exe /x INTEL-SA-00075 Detection and Mitigation Tool.msi /qn

## 執行 GUI 工具

INTEL-SA-00075-GUI.exe 可在單一系統上執行。執行時，工具會輸出探索資訊到螢幕。

圖 1. INTEL-SA-00075-GUI 輸出畫面範例



## 執行主控台工具

請從命令提示字元使用管理員權限執行 INTEL-SA-00075-console.exe。

使用方法：

```
Intel-SA-00075-console.exe [[command] | [option...]]
```

一次只能執行一個指令。如果沒有提供指令，則會執行探索指令。

表 1. INTEL-SA-00075 主控台指令行參數

指令行指令	功能
-Discover	輸出結果至主控台，並將資料寫入登錄檔。
-Unprovision [password], -u [password]	移除所有的 Intel 主動管理技術設定及停用 Intel 主動管理技術功能，可使用並且可能需要 Intel 主動管理技術裝置的管理使用者密碼。 注意：叫用這個指令而不使用密碼僅適用於受 INTEL-SA-00075 影響的韌體版本 (6.1.x.x–11.6.x.x 且組建編號小於 3000)。如果使用的韌體版本 6.1.x.x–11.6.x.x 擁有大於 3000 的組建編號，解除佈建將僅適用於提供密碼時。
-DisableClientControlMode, -DisableCCM	永久停用 Intel 主動管理技術裝置中的用戶端控制模式選項。執行此指令之後，裝置不能置於用戶端控制模式中。注意：沒有 CLI 指令可回復此動作。 警告：並非所有的平台都可以在停用後重新啟用 CCM。
-DisableLMS	停用 LMS 服務。

指令行選項	功能
-n, -noregistry	避免將結果寫入登錄
-c, -noconsole	避免主控台上顯示結果
-d, -delay <seconds>	延遲在開始執行之前的秒數。如果未指定值，此工具將不會延遲。
-f, -writefile	指定將結果寫入檔案。檔案名稱的格式如下：<computername>.xml
-p <filepath>, -filepath <filepath>	儲存輸出檔案的路徑。如果沒有指定路徑，檔案就會被寫入執行此工具的目錄。
-h, -help, -?	顯示這些指令行參數及其功能

### -Discover

探索指令輸出搜尋資訊道主控台。依預設它也會將探索資料寫入登錄。如果沒有提供指令到「主控台」工具，就會執行探索指令。

### -Unprovision

移除所有的 Intel 主動管理技術設定，並停用 Intel 主動管理技術功能，可能會使用 Intel 主動管理技術裝置的可選用管理員使用者密碼。

設定時，Intel® 主動管理技術與 ISM 會自動透過您的電腦網聆聽管理流量。易受已知權限提升問題攻擊的系的應該使用 unprovision 指令解除佈建，以防止未經授權存取管理性功能。

叫用這個指令而不使用密碼僅適用於受 INTEL-SA-00075 影響的韌體版本 (6.1.x.x–11.6.x.x 且組建編號小於 3000)。如果使用的韌體版本 6.1.x.x–11.6.x.x 擁有大於 3000 的組建編號，解除佈建將僅適用於提供密碼時。

### -DisableClientControlMode

-DisableClientControlMode 設定限制是選擇性步驟，客戶需要第二層來防禦取得作業系統系統管理員權限的無權限攻擊者所進行的安全防護反轉。反轉這些選項很難，電腦製造商可能不支援，並且可能需要實體存取系統。如果您選擇要執行這項額外的設定限制，就必須在停用 LMS 服務之前執行。

### 若要重新啟用 CCM

如果您的製造商支援，您可以重設 BIOS 的 Intel 管理性 SKU，它會重新啟用 CCM。請洽詢您的製造商，以瞭解是否支援此功能，以及要遵循的步驟。

**附註：**您的製造廠商可能會提供工具，可讓您透過作業系統設定 BIOS 設定。這些工具，如果有的話，可能會讓您重設 BIOS 中的 Intel 管理性 SKU，而不需實際碰觸電腦。請洽詢您的製造商，以瞭解他們提供的工具是否搭載這項功能。

### -DisableLMS

DisableLMS 指令停用 LMS 服務做為安全防護步驟。

### 什麼是 LMS？

Intel® 管理和安全性應用程式本機管理服務 (LMS) 是一項服務，可讓執行 Intel® 主動管理技術的本機應用程式、Intel® 小型企業優勢工具或 Intel® 標準管理功能支援的裝置，使用通用 SOAP 與 WS 管理功能。它會聆聽 Intel® 管理引擎 (ME) 連接埠 (16992、16993、16994、16995、623、664)，並透過 Intel® 管理引擎介面驅動程式將流量路由到韌體。

### 其他注意事項

具作業系統管理權限的任何人都將能夠在將 LMS 移除後重新安裝，或停用本服務後重新啟動。因此，務必要小心，避免不慎重新安裝或重新啟用 LMS 的同時在系統上存在的弱點。例如，如果您在未來的某個時間執行 Intel 管理性軟體安裝程式，LMS 可能會重新安裝。

圖 2. INTEL-SA-00075 主控台輸出範例

```
INTEL-SA-00075 探索工具
應用程式版本：<應用程式版本>
掃描日期：<日期和時間>

*** 主機電腦資訊 ***
電腦名稱：<電腦名稱>
製造商：<電腦製造商>
型號：<電腦型號>
處理器：<處理器型號>
Windows 版本：Windows* 版本>

*** ME 資訊 ***
版本：<Intel ME 韌體版本>
SKU：<如有的話，管理性功能>
狀態：<ME 佈建狀態>
已安裝驅動程式：<True/False>
控制模式：<無/ACM/CCM>
CCM 已停用：<True/False/未知>
EHBC 已啟用 <True/False>
LMS 狀態：<執行中/已停止/不存在>
LMS 啟動類型：<開機/系統/自動/手動/已停用/不存在>
MicroLMS 狀態：<執行中/已停止/不存在>
MicroLMS 啟動類型：<開機/系統/自動/手動/已停用/不存在>
是 SPS：<True/False>

*** 風險評估 ***
根據此工具執行的分析，
< 此系統易受攻擊 /
此系統不易受攻擊 /
```

此系統不易受攻擊；非 Intel SKU /  
 此系統不易受攻擊；ME 韌體版本不受影響 /  
 此系統不易受攻擊；ME SKU 不受影響 /  
 此系統不易受攻擊；SMBIOS 指出這是消費者 SKU /  
 此系統不易受攻擊；系統正在執行 SPS 韌體 (伺服器平台服務韌體) /  
 此系統的韌體已經更新，系統在解除佈建的狀態 /  
 此系統的韌體已經更新，系統在已佈建的狀態 /  
 洽詢 OEM /  
 此系統的風險為未知>

如果易受攻擊，請洽詢您的 OEM 以取得支援或此系統的修補。

\*\*\* 如需更多資訊 \*\*\*

請參照 CVE-2017-5689，位於：

<https://nvd.nist.gov/vuln/detail/CVE-2017-5689>

或 Intel 安全性諮詢 Intel-SA-00075，位於：

<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr>

用來判定風險評估的邏輯在表 2 中說明。

表 2. 輸出中風險評估的意義

訊息	意義
易受攻擊	偵測到的管理引擎韌體版本被視為容易受到攻擊的 INTEL-SA-00075。
不易受攻擊	系統符合第 8 頁使用 INTEL-SA-00075 探索工具找出受影響的系統中所述的「不易受攻擊」條件。
此系統的韌體已更新，以及系統處於未佈建狀態	在此系統上偵測到的韌體有 INTEL-SA-00075 的修正。確保 INTEL-SA-00075 工具，用來執行重新佈建之前將系統完整解除佈建。如此將會移除任何未經授權的組態設定。
此系統的韌體已更新，以及系統處於已佈建狀態	在此系統上偵測到的韌體有 INTEL-SA-00075 的修正。如果系統在韌體更新之前已佈建，完整解除佈建且重新佈建系統將會移除任何未經授權的組態設定。
洽詢 OEM 廠商	OEM 的 SMBIOS 中偵測到的資訊會顯示管理性 SKU，但是工具向電腦要求詳細的資料時沒有收到回應。這可能是由於遺失管理引擎介面驅動程式所造成。請洽詢您的 OEM 廠商，以得支您的電腦型號是否也受到影響。
未知的	向電腦要求硬體庫存資料時，工具沒有收到有效的回應。請聯絡您的系統製造商，以協助您判定此系統的弱點。  在沒有安裝 PMX 驅動程式的伺服器平台上可能接收到此訊息。此驅動程式可能無法用於所有的 Windows 作業系統版本。如果未顯示驅動程式，則建議的解決方法是執行隨 SPS 韌體版本提供的 spsInfo 或 spsManuf 應用程式。這兩個應用程式會安裝 PMX 驅動程式。

## 結果

附註：INTEL-SA-00075 探索指令傳回的資料量將取決於 Intel 管理性驅動程式堆疊是否載入系統。如果出現 Intel® 管理引擎介面 (MEI) 驅動程式與管理和安全性應用程式本機管理服務 (LMS)，將會提供更詳細的資料集。有些欄位可能不受製造廠商支援。

## 登錄位置

「結果」表的值可以在下列登錄機碼中找到：

- 32 位元作業系統：HKLM\SOFTWARE\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool
- 64 位元作業系統：HKLM\SOFTWARE\WOW6432Node\Intel\Setup and Configuration Software\INTEL-SA-00075 Discovery Tool

XML

如果您選擇將結果寫入 XML 檔案中，該檔案將會儲存到執行 INTEL SA-00075 console.exe 的目錄中，或指令行選項中指定的路徑中。例如硬體庫存、作業系統、LMS 的存在等資訊已包含在內。如果主動管理技術於預設清單中和將會包含所找到的自訂憑證雜湊。針對儲存主動管理技術中的內容，這份清單可用來稽核預期的雜湊。

主控台傳回碼

表 3. INTEL-SA-00075 主控台的傳回碼

編號	意義
0	NOTVULNERABLE (If Discover command was run)   STATUS_OK
2	MACHINE_STATE_UNCONFIGURED
30	CLIENT_CONFIG_NOT_SUPPORTED
39	DISABLE_CCM_IN_ADMIN_MODE
83	HECI_NOT_INSTALLED
111	HECI_ERROR
500	DISCOVERY_VULNERABLE
501	DISCOVERY_POTENTIALLYVULNERABLE_PROVISIONED
502	DISCOVERY_POTENTIALLYVULNERABLE_UNPROVISIONED
503	DISCOVERY_CHECKWITHOEM
504	DISCOVERY_UNKNOWN_RISK
505	DISCOVERY_UNKNOWN
506	DISCOVERY_UNKNOWN_CPU

表 4. INTEL-SA-00075 主控台輸出值

值	位置	描述
Application Version (應用程式版本)		使用的掃描工具版本
Scan Date (掃描日期)		掃描發生的日期時間
Computer Name (電腦名稱)		所掃描到電腦的名稱
Computer Manufacturer (電腦製造商)	硬體庫存	電腦的製造廠商
Computer Model (電腦型號)		電腦的型號
Processor (處理器)		電腦的處理器型號
ME Version (ME 版本)	ME 韌體資訊	含有完整 ME 韌體版本號碼的字串值格式如下： Major.Minor.Hotfix.Build
ME SKU		若有的話，系統上的管理性功能
ME Provisioning State (ME 佈建狀態)		ME 設定狀態 未偵測到任何 未佈建 佈建程序 已佈建
ME Driver Installed (已安裝的)		電腦上是否有 MEI 驅動程式的 True/False 值

ME 驅動程式)		
EHBC Enabled (啟用 EHBC)		系統是否有嵌入式主機設定佈建方法的 True/False 值
LMS state (LMS 狀態)		LMS 服務是否正在執行、無法執行或不存在的資訊
LMS startup type (LMS 啟動類型)		LMS 啟動類型是否為 NotPresent、Boot、System、Auto、Manuel 或 Disabled 的資訊
MicroLMS state (MicroLMS 狀態)		MicroLMS 服務是否正在執行、無法執行或不存在的資訊
MicroLMS startup type (MicroLMS 啟動類型)		MicroLMS 啟動類型是否為 NotPresent、Boot、System、Auto、Manuel 或 Disabled 的資訊
Control Mode (控制模式)		ME 組態模式 無、ACM 或 CCM
Is CCM Disabled (已停用 CCM)		用戶端控制模式將停用的 True/False/未知狀態
Is SPS (是 SPS)		平台是否為不容易受到攻擊的伺服器平台服務 (SP) 系統？
*** 風險評估 ***	風險評估	請參閱 表 2. 輸出中風險評估的意義

## 使用 INTEL-SA-00075 探索工具找出受影響的系統

受影響的系統是定義為具有受影響的 Intel® 管理引擎 (ME) 韌體版本，以及包含表 5 中所定義的三個管理性功能集的其中一種。

**附註：**伺服器平台服務 (SP) 平台並不容易受到 INTEL-SA-00075 的攻擊。SPS 平台擁有在伺服器平台的管理性引擎 (ME) (PCH 的一部分) 上執行的韌體。此韌體與個人電腦/工作站平台上的 Intel 管理性韌體 (也在 ME 上執行) 不同。

表 5. 判斷系統是否容易受到使用 INTEL-SA-00075 探索工具的 INTEL-SA-00075 攻擊的條件

值的名稱	易受攻擊	不易受攻擊
ME SKU	Intel® 完整主動管理技術管理性 Intel® 標準管理功能 Intel® 小型企業優勢工具 (SBA)	ME SKU 值未列於左邊的易受攻擊清單中 -或- 左邊的 ME SKU 值含有不易受攻擊的韌體版本
ME Version	ME 版本 6.x.x.x – 11.7.x.x 具有小於 3000 的組建值  範例：9.5.22. <b>1760</b>	ME 版本： <ul style="list-style-type: none"> <li>6.x.x.x – 11.7.x.x 含有大於或等於 3000 的組建值  <ul style="list-style-type: none"> <li>範例：11.6.27.<b>3264</b></li> </ul> </li> <li>2.x.x.x – 5.x.x.x</li> <li>11.7.x.x 或更新版本</li> </ul>

**附註：**Intel® 小型企業技術 (SBT) 是 Intel® 小型企業優勢工具 (SBA) 的管理性 SKU。

## 將 Microsoft\* SCCM 硬體庫存延伸為包括 INTEL-SA-00075 主控台工具結果

如果您選擇要從 Windows 登錄中的 Intel-SA-00075 主控台工具儲存結果，您可以利用 Microsoft\* SCCM 硬體庫存延伸性來匯入結果。這可讓您在 SCCM 中建立集合到目標電腦以用於修補方式或韌體更新。若要這麼做，您必須執行下列步驟：

1. 新增硬體庫存類別到 SCCM configuration.mof 檔案。
2. 可讓您在用戶端組態啟用這些新硬體庫存類別。
3. 建立軟體套件來部署和執行 INTEL-SA-00075 主控台工具 (Intel SA-00075 console.exe)。
4. 建立工作順序以執行軟體套件。

## MOF 檔案修改

**附註：**如果您的環境中有中央伺服器，請在其上變更 MOF 檔案。否則，在每一個主伺服器上進行這些變更。

1. 找出您 configuration.mof 檔案。這通常會在 \Program Files\Microsoft Configuration Manager\inboxex\clifiles.src\hin\
2. 進行備份。
3. 編輯 configuration.mof 檔案，把游標放在此檔案上方向下捲動到檔案結尾：

```
//=====
// Added extensions end
//=====
```

4. 將 MOF 檔案的內容變更從本文件的第 13-14 頁貼到步驟三的行上方。
5. 儲存並關閉該檔案。
6. 啟動 configuration.mof 目錄中的系統管理員身份執行命令提示字元。
7. 執行 mofcomp 而不用以修改過的 configuration.mof 檔案為目標的交換器。

## 硬體庫存的變更

**附註：**之後，這些變更將需要時間傳播到您的用戶端，然後這些新項目將會出現在硬體庫存中。這所耗費的時間量會依您環境的設定方式而定。

1. 建立新的檔案，名為 INTEL-SA-00075.mof。
2. 貼上第 155 頁的 INTEL-SA-00075 硬體庫存匯入 內容到新建立的檔案，並儲存。
3. 啟動「組態管理員主控台」。
4. 「管理」>「用戶端設定」>「預設用戶端設定」。
5. 用滑鼠右鍵按一下預設「用戶端設定」>「內容」。
6. 選取「硬體庫存」>「設定類別」。
7. 按一下「匯入」。
8. 瀏覽到 INTEL-SA-00075.mof 檔案>「開啟」。
9. 確認已選取「匯入硬體庫存類別和硬體庫存類別的設定值」選項。
10. 按一下「匯入」。
11. 「確定」>「確定」。
12. SCCM 記錄變更到硬體庫存 dataldr.log 檔案中。

## 建立 SCCM 套件

1. 從第 15 頁建立批次檔案，並將它放含有 INTEL-SA-00075 主控台工具檔案的資料夾中。
2. 啟動「組態管理員主控台」。
3. 「軟體程式庫」>「套件」。
4. 用滑鼠右鍵按一下「套件」>「建立套件」。
5. 名稱：Intel-SA-00075
6. 請檢查此套件是否包含來源檔案。
7. 從步驟一瀏覽至套件資料夾。
8. 「下一步」。

9. 選取「不要建立計劃」。
10. 「下一步」 > 「下一步」 > 「關閉」。
11. 發佈套件到適當的發佈點。

## 建立 SCCM 工作順序

1. 啟動「組態管理員主控台」。
2. 「軟體程式庫」 > 「作業系統」。
3. 用滑鼠右鍵按一下「工作順序」 > 「建立工作順序」。
4. 選取「建立新的自訂工作順序」。
5. 「下一步」。
6. 輸入 Intel-SA-00075 的名稱。
7. 「下一步」 > 「下一步」 > 「關閉」。
8. 用滑鼠右鍵按一下「Intel-SA-00075 工作順序」，並按一下「編輯」。
9. 「新增」 > 「一般」 > 「執行指令行」。
10. 在指令行的欄位中輸入 Intel-SA-00075.bat。
11. 核取「套件」方塊並選取「瀏覽」。

- 12. 選取「先前建立的 Intel-SA-00075 套件」>「確定」。
- 13. 按一下「確定」。

使用 Intel® SCS 系統探索公用程式

什麼是 Intel® SCS 系統探索公用程式？

Intel® SCS 系統探索公用程式是一項 Intel® 安裝及組態軟體 (Intel® SCS) 套件的元件，將會提供支援 Intel® 主動管理技術 (Intel® AMT)、Intel® 標準管理功能 (ISM) 或 Intel® 小型企業技術 (Intel® SBT) 的系統上硬體和軟體的特定詳細資料。執行時，它可將結果儲存到 Microsoft Windows 登錄及/或 XML 檔案。此資訊可用來找出系統為目標的韌體更新或實作安全防護成果。

取得 Intel® SCS 系統探索公用程式

Intel® SCS 系統探索公用程式下載套件位於  
<https://downloadcenter.intel.com/download/26691/Intel-SCS-System-Discovery-Utility>.

使用 Intel® SCS 系統探索公用程式判定系統中的管理性韌體版本

Intel® SCS 系統探索公用程式的輸出可用來判斷系統的韌體版本，以及系統是否為管理性 SKU。輸出的 ManageabilityInfo 區段中提供這項資訊。有關執行此工具的說明，請參閱第 12 頁的執行 Intel® SCS 系統探索公用程式一節。

FWVersion 值包含目前在裝置上的韌體版本。AMTSSKU 值包含支援的管理性 SKU (若有的話)。檢閱 FWVersion 和 AMTSKU 的值，以判斷您系統的弱點，如表 6 中所述。

表 6. 判斷系統是否容易受到使用 Intel® SCS 系統探索工具的 INTEL-SA-00075 攻擊的條件

值的名稱	易受攻擊	不易受攻擊
AMTSKU	Intel(R) 完整主動管理技術管理性 Intel(R) 標準管理性 Intel(R) 小型企業優勢工具 (SBA)  範例輸出 <ManageabilityInfo> <AMTSKU>Intel(R) Full AMT Manageability</AMTSKU> <AMTversion>11.0.0</AMTversion> <FWVersion>11.0.0.1202</FWVersion>	AMTSKU 值不存在輸出中 -或- 左邊的 AMTSKU 值含有不易受攻擊的韌體版本  範例輸出 <ManageabilityInfo> <FWVersion>9.0.13.1402</FWVersion>
FWVersion	Intel® 管理性 SKU 的韌體版本 6.x.x.x – 11.7.x.x 具小於 3000 的組建  範例：9.5.22. <u>1760</u>	Intel® 管理性 SKU 的韌體版本： <ul style="list-style-type: none"><li>6.x.x.x – 11.7.x.x 含有大於或等於 3000 的組建值<ul style="list-style-type: none"><li>範例：11.6.27.<u>3264</u></li></ul></li><li>2.x.x.x – 5.x.x.x</li><li>11.7.x.x 或更新版本</li></ul>

附註：Intel® 小型企業技術 (SBT) 是 Intel® 小型企業優勢工具 (SBA) 的管理性 SKU。

執行 Intel® SCS 系統探索公用程式

### 僅將資料儲存到登錄

以管理權限從指令提示執行下列指令，才能執行 Intel® 系統 SCS 探索公用程式，並將資料寫入登錄：

```
SCSDiscovery.exe SystemDiscovery /nofile
```

### 僅將資料儲存到 XML 檔案

使用下列指令執行 Intel® SCS 系統探索公用程式，並將資料儲存到 XML 檔案：

```
SCSDiscovery.exe SystemDiscovery <filename and path> /nregistry
```

檔案名稱和路徑可以是系統或網路共用的本機位置。如果您選擇使用網路共用，請確定執行 Intel® SCS 系統探索公用程式的帳戶已有寫入到該網路共用的權限。如果您不指定檔案名稱和路徑，系統的 FQDN 會用於 XML 檔的名稱，並將檔案會儲存在包含 Intel® SCS 系統探索公用程式的目錄。

### 將資料儲存到登錄和 XML 檔案

使用下列指令執行 Intel® SCS 系統探索公用程式，以儲存資料到登錄檔與 XML 檔案

```
SCSDiscovery.exe SystemDiscovery <filename and path>
```

如先前範例中，如果您不指定檔案名稱和路徑，系統的 FQDN 會用於 XML 檔的名稱，並將檔案會儲存在包含 Intel(R) SCS 系統探索公用程式的目錄。

## Intel® SCS 系統探索公用程式的結果

Intel® SCS 系統探索公用程式傳回的資料量將取決於 Intel 管理性驅動程式堆疊是否載入系統。如果出現 Intel® 管理引擎介面 (MEI) 驅動程式與管理和安全性應用程式本機管理服務 (LMS)，將會提供更詳細的資料集。以下說明的結果將著重在已知的權限提升問題相關的幾個重要資料欄位。如需其他資料欄位的詳細資訊，請參閱 Intel® SCS 系統探索公用程式文件。有些欄位可能不受製造廠商支援。

### 登錄結果

您可以在下列位置找到儲存結果的登錄：

```
HKLM\Software\Intel\Setup and Configuration Software\SystemDiscovery
```

機碼值：

值的名稱	登錄子機碼	值描述
FWVersion	ManageabilityInfo	Intel® 管理引擎韌體版本
AMTSKU	ManageabilityInfo	支援的管理性功能 (若有的話)

## XML 檔案的結果

Intel® 管理引擎韌體版本是在 xml 檔案中的以下路徑：

```
< SystemDiscovery >
  < ManageabilityInfo >
    <FWVersion> Version Number </FWVersion>
```

系統的受支援管理性功能 (若有的話)，位於 xml 檔案中的以下路徑中：

```
< SystemDiscovery >
  < ManageabilityInfo >
    < AMTSKU > 管理性功能名稱 < / AMTSKU >
```

## 將系統探索資料匯入 SCCM 硬體庫存

收集系統探索資料的程序可以自動化 適用於 Microsoft\* System Center Configuration Manager (SCCM) 的 Intel® SCS 附加元件，。安裝時，這個附加元件就會自動延伸 SCCM 硬體庫存為包括系統探索資料，同時建立可用來對系統集合執行系統探索的工作順序。透過此程序所收集的資訊，則可用來建立 SCCM 集合，以推送韌體更新或補救措施到受影響的系統。

適用於 Microsoft SCCM 下載套件的 Intel® SCS 附加元件位於

<https://downloadcenter.intel.com/download/26506/Intel-SCS-Add-on-for-Microsoft-System-Center-Configuration-Manager>.

## MOF 檔案變更

```
//===== Intel-SA-00075 Start =====

#pragma namespace ("\\\\.\\root\\cimv2")
#pragma deletelclass("INTEL_SA_00075_ME_Information", NOFAIL)
[DYNPROPS]
Class INTEL_SA_00075_ME_Information
{
  [key] string KeyName;
  String MEVersion;
  UInt32 MEVersionMajor;
  UInt32 MEVersionMinor;
  UInt32 MEVersionBuild;
  UInt32 MEVersionRevision;
  String MEDriverInstalled;
  String MESKU;
  String MEProvisioningState;
  String LMSPresent;
  String MicroLMSPresent;
  String IsCCMDisabled;
  String ControlMode;
  String EHBCEEnabled;
};

[DYNPROPS]
```

```
Instance of INTEL_SA_00075_ME_Information
{
  KeyName="INTEL-SA-00075";
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version"),Dynamic,Provider("RegPropProv")] MEVersion;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Major"),Dynamic,Provider("RegPropProv")] MEVersionMajor;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Minor"),Dynamic,Provider("RegPropProv")] MEVersionMinor;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Build"),Dynamic,Provider("RegPropProv")] MEVersionBuild;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Version Revision"),Dynamic,Provider("RegPropProv")] MEVersionRevision;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Driver Installed"),Dynamic,Provider("RegPropProv")] MEDriverInstalled;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME SKU"),Dynamic,Provider("RegPropProv")] MESKU;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|ME Provisioning State"),Dynamic,Provider("RegPropProv")] MEProvisioningState;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|LMS Present"),Dynamic,Provider("RegPropProv")] LMSPresent;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Micro LMS Present"),Dynamic,Provider("RegPropProv")] MicroLMSPresent;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Is CCM Disabled"),Dynamic,Provider("RegPropProv")] IsCCMDisabled;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|Control Mode"),Dynamic,Provider("RegPropProv")] ControlMode;
  [PropertyContext("Local|HKEY_LOCAL_MACHINE\\SOFTWARE\\Intel\\Setup and Configuration Software\\INTEL-SA-00075 Discovery Tool\\ME Information|EHBC Enabled"),Dynamic,Provider("RegPropProv")] EHBCEnabled;
};

//===== Intel-SA-00075 End =====
```

## INTEL-SA-00075 硬體庫存匯入

```
#pragma namespace ("\\\\.\\root\\cimv2\\SMS")
#pragma deleteclass("INTEL_SA_00075_ME_Information", NOFAIL)
[SMS_Report(TRUE),SMS_Group_Name("INTEL_SA_00075_ME_Information"),SMS_Class_ID("INTEL_SA_00075_ME_Information"),
SMS_Context_1("__ProviderArchitecture=32|uint32"),
SMS_Context_2("__RequiredArchitecture=true|boolean")]
Class INTEL_SA_00075_ME_Information: SMS_Class_Template
{
[SMS_Report(TRUE),key] string KeyName;
[SMS_Report(TRUE)] String MEVersion;
[SMS_Report(TRUE)] Uint32 MEVersionMajor;
[SMS_Report(TRUE)] Uint32 MEVersionMinor;
[SMS_Report(TRUE)] Uint32 MEVersionBuild;
[SMS_Report(TRUE)] Uint32 MEVersionRevision;
[SMS_Report(TRUE)] String MEDriverInstalled;
[SMS_Report(TRUE)] String MESKU;
[SMS_Report(TRUE)] String MEProvisioningState;
[SMS_Report(TRUE)] String LMSPresent;
[SMS_Report(TRUE)] String MicroLMSPresent;
[SMS_Report(TRUE)] String IsCCMDisabled;
[SMS_Report(TRUE)] String ControlMode;
[SMS_Report(TRUE)] String EHBCEnabled;
};
```

## INTEL-SA-00075.bat 批次檔案

```
@echo off
.\Intel-SA-00075-console
SET EL=%ERRORLEVEL%
rem Schedule HW inventory
SET HWInventoryGUID="{00000000-0000-0000-0000-000000000001}"
wmic /IMPLEVEL:Impersonate /AUTHLEVEL:Pktprivacy /namespace:\\.\\root\\ccm path sms_client CALL TriggerSchedule
%HWInventoryGUID% /NOINTERACTIVE
echo Exit code: %EL%
exit %EL%
```

## 集合查詢範例

### 已佈建的電腦

```
select * from SMS_R_System inner join SMS_G_System_INTEL_SA_00075_ME_Information on
SMS_G_System_INTEL_SA_00075_ME_Information.ResourceID = SMS_R_System.ResourceID where
SMS_G_System_INTEL_SA_00075_ME_Information.MEProvisioningState = "Provisioned"
```

### LMS 執行

```
select * from SMS_R_System inner join SMS_G_System_INTEL_SA_00075_ME_Information on
SMS_G_System_INTEL_SA_00075_ME_Information.ResourceID = SMS_R_System.ResourceID where
```

```
SMS_G_System_INTEL_SA_00075_ME_Information.LMSPresent = "Running" or  
SMS_G_System_INTEL_SA_00075_ME_Information.MicroLMSPresent = "Running"
```

本文件中的資訊係與 INTEL® 產品相關。禁止授權、明示或暗示，翻供或以其他方式引用本文件的智慧財產權。除了 INTEL 在這類產品的銷售條款與條件中所列的內容外，INTEL 不需負任何其他責任。關於銷售及/或使用 INTEL 產品，INTEL 不提供任何明示或暗示之擔保，包括有關適合特定用途、適售性，或是侵犯任何專利、著作權或其他智慧財產權之責任或擔保。除非得到 INTEL 的書面同意，INTEL 產品的設計或意圖並非是將 INTEL 產品應用在一旦發生故障就可能造成個人傷害或死亡的情況。

Intel 技術的功能與優勢端視系統組態而定，可能需要用到支援該技術的硬體、軟體，或啟用相關服務。實際效能會依系統組態而異。沒有電腦系統能提供絕對的安全性。詳情請洽詢購入系統的製造商或零售商，或是上網參閱 [intel.com](http://intel.com)。

著作權© 2017 Intel 公司。保留一切權利。Intel 和 Intel 圖誌是 Intel 公司在美國及/或其它國家的商標。

\* 其他名稱與品牌可能業經宣告為他人之財產。