|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | |  | |
| **政府組態基準**  **Microsoft Windows 10**  **(V1.3)** | | | | |
|  | |  | |  |
|  | | | | |
| **行政院國家資通安全會報技術服務中心**  中華民國109年11月 | | | | |

**目次**

[壹、 前言 1](#_Toc446493014)

[一、 適用環境 1](#_Toc446493015)

[二、 項數統計 1](#_Toc446493016)

[三、 文件發行 1](#_Toc446493017)

[貳、 Windows 10政府組態基準列表 2](#_Toc446493018)

[參、 參考文獻 36](#_Toc446493019)

# 前言

政府組態基準(Government Configuration Baseline, 以下簡稱GCB)目的在於規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

## 適用環境

本文件適用於微軟公司所發行之Windows 10作業系統。

## 項數統計

政府組態基準針對電腦作業環境提供一致性安全基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。Windows 10組態基準計有345項設定項目，項目統計詳見表1。

1. Windows 10組態基準項目統計

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 項目 | 項數 | 合計 |
| 1 | Windows10 Account Settings | 9 | 345 |
| 2 | Windows10 Computer Settings | 291 |
| 3 | Windows10 User Settings | 12 |
| 4 | Windows10 Firewall Settings | 33 |
| 本中心整理 | | | |

## 文件發行

本文件最新版本公布於本中心網站之「政府組態基準」專區，網址為[https://www.nccst.nat.gov.tw/GCB](http://www.nccst.nat.gov.tw/GCB)。

# Windows 10政府組態基準列表

1. Windows 10政府組態基準列表

| 項次 | GPO | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | GPO設定路徑 | GCB設定值 | 備註 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Windows10 Account Settings | TWGCB-01-005-0001 | 帳戶原則\密碼原則 | 密碼最短使用期限 | * 此項原則設定決定在使用者變更密碼之前，密碼必須使用的期限(天數)。可以設定1與998天之間的值，或設定天數為0，以允許立即變更 * 「密碼最短使用期限」不得超過「密碼最長使用期限」，除非「密碼最長使用期限」設定為0，表示密碼永遠不會到期。如果「密碼最長使用期限」設定為0，則「密碼最短使用期限」可以設定為介於0到998之間的任何數值 * 如果要讓「強制執行密碼歷程記錄」生效，請將「密碼最短使用期限」設為0以上 * 若沒有設定「密碼最短使用期限」，使用者便可重複使用密碼，直到厭倦為止。預設值並未依循此建議，所以系統管理員可為使用者指定密碼，然後在使用者登入時要求變更系統管理員定義的密碼。如果「密碼歷程記錄」設為0，使用者便不需選擇新密碼。因此，根據預設，「強制執行密碼歷程記錄」設定為1 | 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\密碼最短使用期限 | 1 天 | CCE-ID：CCE-41953-1 |
| 2 | Windows10 Account Settings | TWGCB-01-005-0002 | 帳戶原則\密碼原則 | 密碼最長使用期限 | * 此項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在1至999天之後到期；或將天數設為0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於1到999天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為0，則「密碼最短使用期限」可以是介於0到998天之間的任何數值 * 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每30至90天到期。如此一來，攻擊者破解使用者密碼及存取使用者的網路資源的時間便很有限 * 注意：若使用者帳戶啟用「密碼永久有效」設定，將覆蓋此原則設定，導致系統不會要求該使用者變更密碼，即該使用者帳戶之密碼永遠不會到期。 | 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\密碼最長使用期限 | 90天以下 | CCE-ID：CCE-43535-4 |
| 3 | Windows10 Account Settings | TWGCB-01-005-0003 | 帳戶原則\密碼原則 | 最小密碼長度 | * 此項原則設定決定使用者帳戶的密碼可包含的最少字元數。可以設定介於1到14個字元之間的值 * 將字元數設為0，則表示不需要密碼 | 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\最小密碼長度 | 8個字元以上 | CCE-ID：CCE-41679-2 |
| 4 | Windows10 Account Settings | TWGCB-01-005-0004 | 帳戶原則\密碼原則 | 密碼必須符合複雜性需求 | * 此項原則設定決定密碼是否必須符合複雜性需求 * 如果啟用了此原則，則密碼必須符合下列最小需求：   -不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元  -長度至少為6個字元  -包含下列四種字元中的三種：  (1)英文大寫字元(A到Z)  (2)英文小寫字元(a到z)  (3)10進位數字(0到9)  (4)非英文字母字元(例如：!、$、#、%)   * 建立或變更密碼時會強制執行複雜性需求 | 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\密碼必須符合複雜性需求 | 啟用 | CCE-ID：CCE-42872-2 |
| 5 | Windows10 Account Settings | TWGCB-01-005-0005 | 帳戶原則\密碼原則 | 強制執行密碼歷程記錄 | * 此項原則設定決定重複使用舊密碼前，必須與使用者帳戶相關的唯一新密碼數目。此值必須介於0與24個密碼之間 * 此項原則可讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性 | 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\強制執行密碼歷程記錄 | 3以上記憶的密碼 | CCE-ID：CCE-42136-2 |
| 66 | Windows10 Computer Settings | TWGCB-01-005-0066 | 系統\網際網路通訊管理\網際網路通訊設定 | 如果URL連線正在參照Microsoft.com時，關閉網際網路連線精靈 | * 此項原則設定指定網際網路連線精靈是否可以連線到Microsoft下載網際網路服務提供者(ISP)清單 * 如果啟用此項原則設定，網際網路連線精靈中的「選擇網際網路服務提供者清單」路徑將導致精靈結束。這會阻止使用者擷取位於Microsoft伺服器上的ISP清單 * 如果停用或未設定此項原則設定，使用者將可以連線到Microsoft下載其區域的ISP清單 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\如果URL連線正在參照Microsoft.com時，關閉網際網路連線精靈 | 啟用 | CCE-ID：CCE-42453-1 |
| 67 | Windows10 Computer Settings | TWGCB-01-005-0067 | 網際網路通訊管理\網際網路通訊設定 | 關閉Windows錯誤報告 | * 此項原則設定控制是否向Microsoft報告錯誤 * 錯誤報告是用來報告系統或應用程式失敗或停止回應的相關資訊，並用來改進產品的品質 * 如果啟用此項原則設定，使用者將無法報告錯誤 * 如果停用或未設定此項原則設定，可以透過網際網路或機關的檔案共用向Microsoft報告錯誤。此項原則設定會覆寫任何從控制台對報告錯誤所做的使用者設定 * 此外，也可以參閱[電腦設定/系統管理範本/Windows元件/Windows錯誤報告]中的[設定錯誤報告]、[顯示錯誤通知]和[停用Windows錯誤報告]原則設定 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉Windows錯誤報告 | 啟用 | CCE-ID：CCE-41520-8 |
| 68 | Windows10 Computer Settings | TWGCB-01-005-0068 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉網際網路檔案關聯服務 | * 此項原則設定指定是否使用Microsoft網站服務尋找應用程式來開啟具有未處理檔案關聯的檔案 * 當使用者所開啟檔案之副檔名與電腦上任何應用程式都沒有關聯時，使用者可以選擇使用本機應用程式或網站服務來尋找應用程式 * 如果啟用此項原則設定，則會移除使用網站服務來開啟未處理檔案關聯的連結和對話方塊 * 如果停用或未設定此項原則設定，使用者將可以使用網站服務 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉網際網路檔案關聯服務 | 啟用 | CCE-ID：CCE-43045-4 |
| 69 | Windows10 Computer Settings | TWGCB-01-005-0069 | 系統\網際網路通訊管理\網際網路通訊設定 | 關閉Windows Messenger客戶經驗改進計畫 | * 此項原則設定指定Windows Messenger是否收集關於 Windows Messenger軟體和服務使用情形的匿名資訊 * 使用者可以透過客戶經驗改進計畫讓Microsoft收集關於產品使用情形的匿名資訊。這項資訊將用來改善未來上市的產品 * 如果啟用此項原則設定，Windows Messenger將不會收集使用資訊，而且也不會顯示啟用收集使用資訊的使用者設定 * 如果停用此項原則設定，Windows Messenger將收集匿名使用資訊，而且不會顯示該設定 * 如果未設定此項原則設定，使用者將能選擇參加，並允許資料收集 | 電腦設定\系統管理範本\系統\網際網路通訊管理\網際網路通訊設定\關閉Windows Messenger客戶經驗改進計畫 | 啟用 | CCE-ID：CCE-43389-6 |
| 70 | Windows10 Computer Settings | TWGCB-01-005-0070 | 進階稽核原則設定 | 稽核原則：帳戶登入：稽核驗證認證 | * 此項原則設定可讓使用者稽核因使用者帳戶登入認證的驗證測試而產生的事件 * 只有在授權可以使用那些認證的電腦上，才會發生這個子類別中的事件。如果是網域帳戶，則網域控制站具有授權。如果是本機帳戶，則本機電腦具有授權 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\稽核原則：帳戶登入：稽核驗證認證 | 成功與失敗 | CCE-ID：CCE-41615-6 |
| 71 | Windows10 Computer Settings | TWGCB-01-005-0071 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核電腦帳戶管理 | * 此項原則設定可稽核因電腦帳戶變更(如建立、變更或刪除電腦帳戶時)而產生的事件 * 如果設定此項原則，則會在嘗試變更電腦帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則，則不會在電腦帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\稽核原則\帳戶管理\稽核原則：帳戶管理：稽核電腦帳戶管理 | 成功 | CCE-ID：CCE-42031-5 |
| 72 | Windows10 Computer Settings | TWGCB-01-005-0072 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核其他帳戶管理事件 | * 此項原則設定可讓使用者稽核因這個類別未涵蓋的其他使用者帳戶變更而產生的事件，例如：   -已存取使用者帳戶的密碼雜湊。這一般是在Active Directory管理工具密碼移轉期間發生  -已呼叫密碼原則檢查API。在惡意應用程式測試原則以減少密碼字典攻擊期間的嘗試次數時，呼叫這個功能會是一種攻擊   * 下列群組原則路徑下的預設網域群組原則變更：   -電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則  -電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則   * 注意：套用原則設定時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核原則：帳戶管理：稽核其他帳戶管理事件 | 成功與失敗 | CCE-ID：CCE-42317-8 |
| 73 | Windows10 Computer Settings | TWGCB-01-005-0073 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核安全性群組管理 | * 此項原則設定可稽核因安全性群組變更而產生的事件，例如：   -建立、變更或刪除安全性群組  -在安全性群組中新增或移除成員  -變更群組類型   * 如果設定此項原則設定，則會在嘗試變更安全性群組時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在安全性群組變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核原則：帳戶管理：稽核安全性群組管理 | 成功與失敗 | CCE-ID：CCE-43130-4 |
| 74 | Windows10 Computer Settings | TWGCB-01-005-0074 | 進階稽核原則設定 | 稽核原則：帳戶管理：稽核使用者帳戶管理 | * 此項原則設定可稽核使用者帳戶的變更。包含下列事件：   -建立、變更、刪除、重新命名、停用、啟用、鎖定或解除鎖定使用者帳戶  -設定或變更使用者帳戶的密碼  -將安全性識別碼(SID)新增到使用者帳戶的SID歷程記錄  -設定目錄服務還原模式密碼  -變更管理使用者帳戶的權限  -備份或還原認證管理員認證   * 如果設定此項原則設定，則會在嘗試變更使用者帳戶時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在使用者帳戶變更時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\帳戶管理\稽核原則：帳戶管理：稽核使用者帳戶管理 | 成功與失敗 | CCE-ID：CCE-42410-1 |
| 75 | Windows10 Computer Settings | TWGCB-01-005-0075 | 進階稽核原則設定 | 稽核原則：詳細追蹤：稽核建立處理程序 | * 此項原則設定可稽核建立或啟動處理程序時產生的事件，也會稽核建立處理程序的應用程式或使用者名稱 * 如果設定此項原則設定，則會在建立處理程序時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在建立處理程序時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\詳細追蹤\稽核原則：詳細追蹤：稽核建立處理程序 | 成功 | CCE-ID：CCE-43062-9 |
| 76 | Windows10 Computer Settings | TWGCB-01-005-0076 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核帳戶鎖定 | * 此項原則設定可稽核因嘗試登入的帳戶被鎖定而失敗所產生的事件 * 若設定此原則設定，則會在帳戶因鎖定而無法登入電腦時產生稽核事件。成功稽核會記錄成功的嘗試，而失敗稽核則會記錄不成功的嘗試 * 登入事件對於了解使用者活動以及偵測潛在的攻擊是十分重要的 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核帳戶鎖定 | 成功與失敗 | CCE-ID：CCE-42601-5 |
| 77 | Windows10 Computer Settings | TWGCB-01-005-0077 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核登出 | * 此項原則設定可稽核因關閉登入工作階段而產生的事件。這些事件發生於被存取的電腦上。如果是互動式登出，則會在使用者帳戶登入的電腦上產生安全性稽核事件 * 如果設定此項原則設定，則會在關閉登入工作階段時產生稽核事件。成功稽核會記錄成功關閉工作階段嘗試，而失敗稽核則會記錄失敗關閉工作階段嘗試 * 如果未設定此項原則設定，則不會在關閉登入工作階段時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核登出 | 成功 | CCE-ID：CCE-41727-9 |
| 78 | Windows10 Computer Settings | TWGCB-01-005-0078 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核登入 | * 此項原則設定可讓使用者稽核因電腦上的使用者帳戶登入嘗試而產生的事件 * 這個子類別中的事件是與建立登入工作階段有關，而且發生在被存取的電腦上。如果是互動式登入，則會在使用者帳戶登入的電腦上產生安全性稽核事件。如果是網路登入(如存取網路上的共用資料夾)，則會在裝載資源的電腦上產生安全性稽核事件。包含下列事件：   -成功登入嘗試  -失敗登入嘗試   * 使用明確認證的登入嘗試。處理程序嘗試明確指定該帳戶的認證來登入帳戶時，會產生這個事件。這最常發生於批次登入設定(如排定的工作或使用 RUNAS命令時) * 已篩選安全性識別碼(SID)且不允許其登入 * 數量：用戶端電腦上是「低」。網域控制站或網路伺服器上是「中」 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核登入 | 成功與失敗 | CCE-ID：CCE-41786-5 |
| 79 | Windows10 Computer Settings | TWGCB-01-005-0079 | 進階稽核原則設定 | 稽核原則：登入-登出：稽核特殊登入 | * 此項原則設定可稽核因特殊登入而產生的事件，例如：   -使用特殊登入，這是具有管理員同等權限而且可以用來將處理程序提高為較高等級的登入  -特殊群組成員的登入。特殊群組可讓使用者稽核特定群組成員登入網路時產生的事件   * 可在登錄中設定群組安全性識別碼(SID)清單。如果上述任一SID在登入期間被新增至權杖，而且子類別已啟用，則會記錄事件。如需這個功能的詳細資訊，請參閱Microsoft知識庫文章947223(http：//go.microsoft.com/fwlink/?LinkId=121697) | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\登入/登出\稽核原則：登入-登出：稽核特殊登入 | 成功 | CCE-ID：CCE-42066-1 |
| 80 | Windows10 Computer Settings | TWGCB-01-005-0080 | 進階稽核原則設定 | 稽核原則：物件存取：稽核抽取式存放裝置 | * 此項原則設定可稽核存取抽取式存放裝置上之檔案系統物件的使用者嘗試。安全性稽核事件只會針對所有要求之存取類型的所有物件產生 * 如果設定此原則設定，每當有帳戶存取抽取式存放裝置上的檔案系統物件時，就會產生稽核事件。成功稽核會記錄成功的嘗試，失敗稽核會記錄失敗的嘗試 * 如果未設定此原則設定，當有帳戶存取抽取式存放裝置上的檔案系統物件時，就不會產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\物件存取\稽核原則：物件存取：稽核抽取式存放裝置 | 成功 | CCE-ID：CCE-41572-9 |
| 81 | Windows10 Computer Settings | TWGCB-01-005-0081 | 進階稽核原則設定 | 稽核原則：原則變更：稽核「稽核原則變更」 | * 此項原則設定可稽核安全性稽核原則設定變更，例如：   -稽核原則物件上的設定權限及稽核設定  -系統稽核原則的變更  -安全性事件來源的註冊  -解除安全性事件來源的註冊  -每個使用者稽核設定的變更  -CrashOnAuditFail值的變更  -檔案系統或登錄物件上的系統存取控制清單變更  -特殊群組清單的變更   * 注意：物件的SACL變更而且已啟用原則變更類別時，會進行系統存取控制清單(SACL)變更稽核。啟用物件存取稽核且設定物件的SACL以稽核DACL/擁有者變更時，會稽核判別存取控制清單(DACL)及擁有權變更 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核原則：原則變更：稽核「稽核原則變更」 | 成功與失敗 | CCE-ID：CCE-43865-5 |
| 82 | Windows10 Computer Settings | TWGCB-01-005-0082 | 進階稽核原則設定 | 稽核原則：原則變更：稽核驗證原則變更 | * 此項原則設定可稽核因驗證原則變更而產生的事件，例如：   -建立樹系及網域信任  -修改樹系及網域信任  -移除樹系及網域信任   * 變更下列位置下的Kerberos原則：電腦設定\Windows設定\安全性設定\帳戶原則\Kerberos原則 * 將下列任何使用者權限授與使用者或群組：   -從網路存取這台電腦  -允許本機登入  -允許透過終端機服務登入  -以批次工作登入  -以服務方式登入  -命名空間衝突。例如，新信任的名稱與現有命名空間名稱相同時   * 如果設定此項原則設定，則會在嘗試變更驗證原則時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在變更驗證原則時產生稽核事件 * 注意：套用群組原則時，會記錄安全性稽核事件。而修改設定時，則不會發生該事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\原則變更\稽核原則：原則變更：稽核驗證原則變更 | 成功 | CCE-ID：CCE-43416-7 |
| 83 | Windows10 Computer Settings | TWGCB-01-005-0083 | 進階稽核原則設定 | 稽核原則：特殊權限使用：稽核機密特殊權限使用 | * 此項原則設定可稽核使用機密特殊權限(使用者權限)時產生的事件，例如：   (1)呼叫特許服務  (2)呼叫下列其中一種權限： -當成作業系統的一部分  -備份檔案及目錄  -建立權杖物件  -偵錯程式  -讓電腦及使用者帳戶受信賴，以進行委派  -產生安全性稽核  -在驗證後模擬用戶端  -載入及解除載入裝置驅動程式  -管理稽核及安全性記錄檔  -修改韌體環境值  -取代處理程序等級權杖  -還原檔案及目錄  -取得檔案或其他物件的擁有權   * 如果設定此項原則設定，則會在進行機密特殊權限要求時產生稽核事件。成功稽核會記錄成功要求，而失敗稽核則會記錄失敗要求 * 如果未設定此項原則設定，則不會進行機密特殊權限要求時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\特殊權限使用\稽核原則：特殊權限使用：稽核機密特殊權限使用 | 成功與失敗 | CCE-ID：CCE-43224-5 |
| 84 | Windows10 Computer Settings | TWGCB-01-005-0084 | 進階稽核原則設定 | 稽核原則：系統：稽核IPsec驅動程式 | * 此項原則設定可稽核因IPsec篩選器驅動程式而產生的事件，例如： -IPsec服務的啟動及關閉 -因完整性檢查失敗而丟棄的網路封包 -因重新執行檢查失敗而丟棄的網路封包 -因格式為純文字而丟棄的網路封包 -接收到具有不正確安全性參數索引(SPI)的網路封包。這可能表示網路卡未正確運作，或需要更新驅動程式 -無法處理IPsec篩選器 * 如果設定此項原則設定，則會在IPsec篩選器驅動程式操作上產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在IPsec篩選器驅動程式操作上產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核IPsec驅動程式 | 成功與失敗 | CCE-ID：CCE-41593-5 |
| 85 | Windows10 Computer Settings | TWGCB-01-005-0085 | 進階稽核原則設定 | 稽核原則：系統：稽核其他系統事件 | * 此項原則設定可稽核下列任一事件：   -Windows防火牆服務及驅動程式的啟動及關閉  -Windows防火牆服務的安全性原則處理  -加密編譯金鑰檔案及移轉操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\稽核原則: 系統: 稽核其他系統事件 | 失敗 | CCE-ID：CCE-42399-6 |
| 86 | Windows10 Computer Settings | TWGCB-01-005-0086 | 進階稽核原則設定 | 稽核原則：系統：稽核安全性狀態變更 | * 此項原則設定可稽核因電腦安全性狀態變更而產生的事件，例如下列事件：   -電腦的啟動及關閉  -系統時間的變更  -從CrashOnAuditFail復原系統，這是在安全性事件記錄檔已滿且設定CrashOnAuditFail登錄項目時於系統重新啟動之後記錄 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核安全性狀態變更 | 成功與失敗 | CCE-ID：CCE-42615-5 |
| 87 | Windows10 Computer Settings | TWGCB-01-005-0087 | 進階稽核原則設定 | 稽核原則：系統：稽核安全性系統延伸 | * 此項原則設定可稽核與安全性系統延伸或服務相關的事件，例如：   -載入安全性系統延伸(如驗證、通知或安全性封裝)，並向本機安全性授權(LSA)進行註冊。它是用來驗證登入嘗試、提交登入要求，以及任何帳戶或密碼變更，Kerberos及NTLM是安全性系統延伸的範例  -安裝服務，並向服務控制管理員進行註冊。稽核記錄包含服務名稱、二進位、類型、啟動類型及服務帳戶的相關資訊   * 如果設定此項原則設定，則會在嘗試載入安全性系統延伸時產生稽核事件。成功稽核會記錄成功嘗試，而失敗稽核則會記錄失敗嘗試 * 如果未設定此項原則設定，則不會在嘗試載入安全性系統延伸時產生稽核事件 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核安全性系統延伸 | 成功與失敗 | CCE-ID：CCE-43772-3 |
| 88 | Windows10 Computer Settings | TWGCB-01-005-0088 | 進階稽核原則設定 | 稽核原則：系統：稽核系統完整性 | * 此項原則設定可稽核會破壞安全性子系統完整性的事件，例如：   -因稽核系統發生問題而無法寫入事件記錄檔的事件  -使用本機程序呼叫(LPC)連接埠的處理程序，而此連接埠在透過與用戶端位址空間之間的回覆、讀取或寫入來嘗試模擬用戶端的過程中無效  -偵測到危害系統完整性的遠端程序呼叫(RPC)  -偵測到程式碼完整性判斷為無效之可執行檔的雜湊值  -危害系統完整性的加密編譯操作 | 電腦設定\Windows設定\安全性設定\進階稽核原則設定\系統稽核原則\系統\稽核原則：系統：稽核系統完整性 | 成功與失敗 | CCE-ID：CCE-41871-5 |
| 89 | Windows10 Computer Settings | TWGCB-01-005-0089 | 安全性選項\帳戶 | 帳戶：Administrator帳戶狀態 | * 此項原則設定決定要啟用或停用本機Administrator帳戶 * 注意：若在停用Administrator帳戶後嘗試重新啟用此帳戶，而現行Administrator密碼不符合密碼要求時，將無法重新啟用此帳戶。在此情況下，必須由Administrators群組的替代成員重設Administrator帳戶的密碼 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：Administrator 帳戶狀態 | 停用 | CCE-ID：CCE-43470-4 |
| 90 | Windows10 Computer Settings | TWGCB-01-005-0090 | 安全性選項\帳戶 | 帳戶：封鎖Microsoft 帳戶 | * 此原則設定可防止使用者在此電腦上新增Microsoft帳戶 * 若選取[使用者無法新增Microsoft帳戶]選項，使用者將無法在此電腦上建立新的Microsoft帳戶、從本機帳戶切換為Microsoft帳戶，或將網域帳戶關聯到Microsoft帳戶。若使用者必須在機關中限制Microsoft帳戶的使用，此為偏好的選項 * 若選取[使用者無法新增Microsoft帳戶或以Microsoft帳戶登入]選項，現有的Microsoft帳戶使用者將無法登入Windows。選取此選項可能會使此電腦的現有系統管理員無法登入並管理系統 * 若停用或不設定此原則(建議做法)，使用者將可以在Windows使用Microsoft帳戶 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：封鎖Microsoft 帳戶 | 啟用，使用者無法新增Microsoft 帳戶或以Microsoft 帳戶登入 | CCE-ID：CCE-42434-1 |
| 91 | Windows10 Computer Settings | TWGCB-01-005-0091 | 安全性選項\帳戶 | 帳戶：Guest帳戶狀態 | * 此項原則設定決定啟用或停用Guest帳戶 * 注意：如果停用Guest帳戶，而且「網路存取：共用和安全性模式用於本機帳戶」安全性選項是設定為「僅適用於來賓」，則網路登入(例如，由Microsoft網路伺服器(SMB服務)所執行的網路登入)將會失敗 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：Guest帳戶狀態 | 停用 | CCE-ID：CCE-41528-1 |
| 92 | Windows10 Computer Settings | TWGCB-01-005-0092 | 安全性選項\帳戶 | 帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台 | * 此項原則設定決定未受密碼保護的本機帳戶，是否可用來從實體電腦主控台以外的位置登入。如果已啟用，那麼未受密碼保護的本機帳戶將只能藉由電腦鍵盤登入 * 注意：   (1)不是位於實際安全位置的電腦，應一直針對所有本機使用者帳戶強制執行強式密碼原則。否則，每位實際存取電腦的使用者皆可使用沒有密碼的使用者帳戶登入。這對可攜式電腦來說尤其重要  (2)如果將此安全性原則套用到Everyone群組，則任何人都不能透過遠端桌面服務登入  (3)此項設定對於使用網域帳戶的登入沒有影響  (4)應用程式若使用遠端互動式登入，則可以跳過此項設定  (5)遠端桌面服務在舊版的Windows作業系統中稱為「終端機服務」 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台 | 啟用 | CCE-ID：CCE-41787-3 |
| 93 | Windows10 Computer Settings | TWGCB-01-005-0093 | 安全性選項\帳戶 | 帳戶：重新命名系統管理員帳戶 | 此項原則設定將重新命名已知的Administrator帳戶，透過使用不同的帳戶名稱與Administrator帳戶之安全性識別碼(SID)相關聯，使得未經授權的人員較不容易猜出有此特殊權限的使用者名稱與密碼組合 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：重新命名系統管理員帳戶 | Renamed\_Admin | CCE-ID：CCE-42970-4 |
| 94 | Windows10 Computer Settings | TWGCB-01-005-0094 | 安全性選項\帳戶 | 帳戶：重新命名來賓帳戶名稱 | 此項原則設定將重新命名已知的Guest帳戶，透過使用不同的帳戶名稱與Guest帳戶之安全性識別碼(SID)相關聯，使得未經授權的人員較不容易猜出此使用者名稱與密碼組合 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\帳戶：重新命名來賓帳戶名稱 | Renamed\_Guest | CCE-ID：CCE-43078-5 |
| 95 | Windows10 Computer Settings | TWGCB-01-005-0095 | 安全性選項\稽核 | 稽核：稽核通用系統物件的存取 | * 此項原則設定決定是否稽核通用系統物件的存取 * 如果啟用此原則，會導致系統物件(如Mutex(互斥)、事件、信號及DOS裝置在建立時便含有預設的系統存取控制清單(SACL)。只有具名的物件會被指定SACL，SACL不會指定給沒有名稱的物件 * 如果也啟用「稽核物件存取」稽核原則，則會稽核這些系統物件的存取 * 注意：設定此項原則設定時，在重新啟動Windows之後，所做的變更才會生效 | 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\稽核：稽核通用系統物件的存取 | 停用 | CCE-ID：CCE-43276-5 |
| 本中心整理 | | | | | | | | |

# 參考文獻

1. Common Configuration Enumeration(CCE)List. http://cce.mitre.org/lists/cce\_list.html
2. CIS Security Benchmarks. https://benchmarks.cisecurity.org
3. Windows 10 Security Guide, Version 1511. Microsoft Security Compliance Manager. https://technet.microsoft.com/zh-tw/library/cc677002.aspx
4. Windows 10 Security Technical Implementation Guide https://www.stigviewer.com/stig/windows\_10/