

政府組態基準(GCB)實作研習活動 (Windows 8.1)

行政院國家資通安全會報技術服務中心

- 前言
- Windows 8.1 政府組態基準設定分類說明
- Windows 8.1 與 Windows 7 共同項目說明
- Windows 8.1 新增項目說明
- 問題與討論

NCCST

前言(1/2)

- 目的

- 規範資通訊終端設備(如：個人電腦)的一致性安全設定，以降低成為駭客入侵管道，進而引發資安事件之疑慮

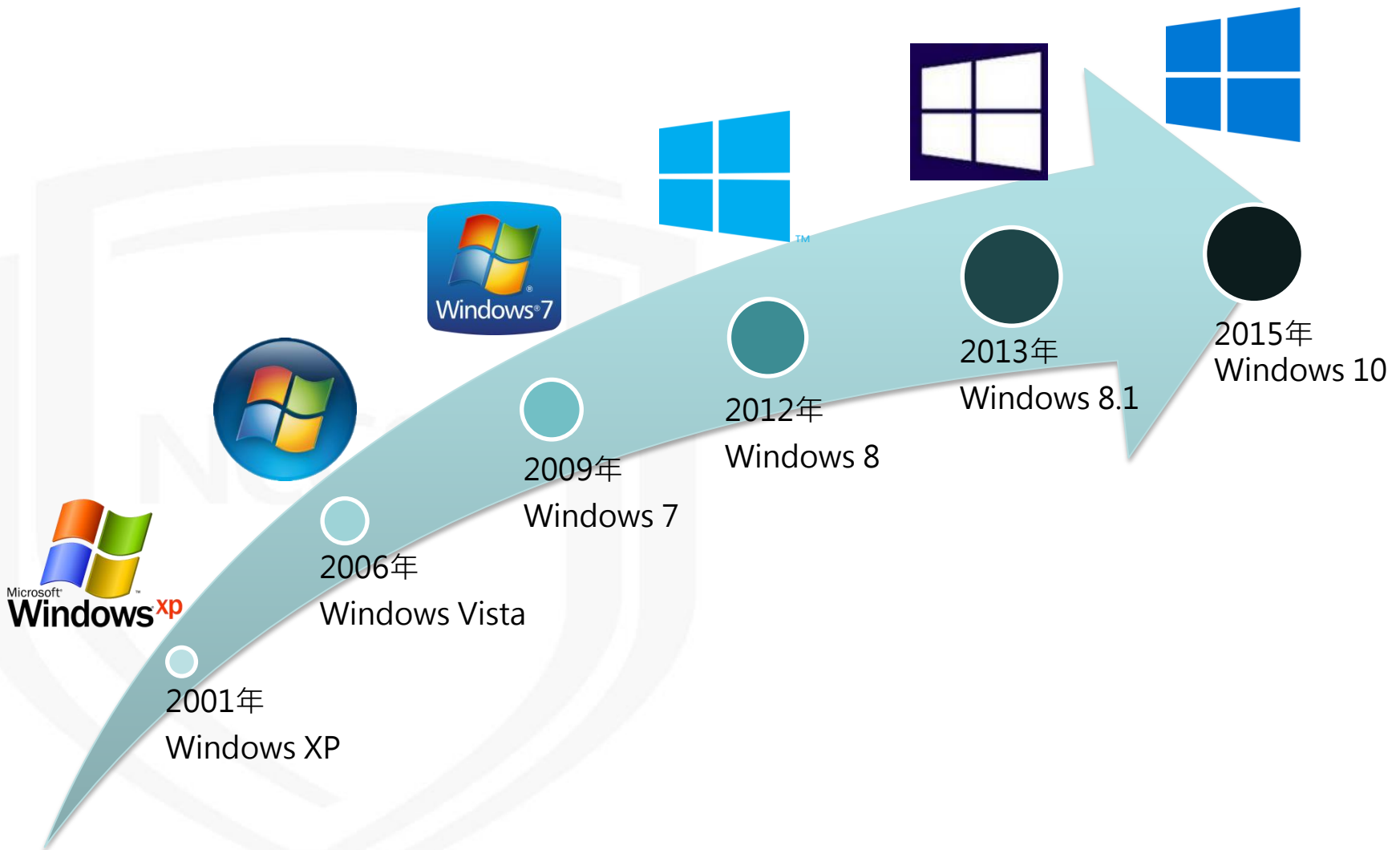
- 政府組態基準項目內容

- Windows 8.1 Account Settings
 - Windows 8.1 Computer Energy Settings
 - Windows 8.1 Computer Settings
 - Windows 8.1 User Settings
 - Windows 8.1 Firewall Settings

前言(2/2)



● Windows 作業系統進展



Windows 8.1

政府組態基準設定項目分類

NCCST

政府組態基準設定分類說明

項次	項目	項數	合計
1	Account Settings	9	340
2	Computer Energy Settings	4	
3	Computer Settings	281	
4	User Settings	13	
5	Firewall Settings	33	



政府組態基準設定分類說明

項次	GPO	項目	項數	合計
1	Computer Settings	網路	14	314
2		進階稽核原則設定	19	
3		具有進階安全性的Windows防火牆	33	
4		控制台\個人化	2	
5		Windows元件	71	
6		安全性選項	90	
7		使用者權限指派	41	
8		系統	27	
9		網際網路通訊管理	15	
10		本機原則\使用者權限指派	2	

政府組態基準設定分類說明

項次	GPO	項目	項數	合計
10	Account Settings	帳戶原則	9	9
11	Computer Energy Settings	電源管理\視訊與顯示設定	4	4
12	User Settings	個人化	5	13
13		附件管理員	3	
14		網際網路通訊設定	1	
15		Windows元件	2	
16		網路共用	1	
17		其他	1	

Windows 8.1 與 Windows 7 共同項目說明

NCCST

群組原則概述

A large, faint watermark of the NCCST logo is visible in the background on the left side of the slide. It features a shield shape with the acronym "NCCST" in the center, rendered in a light gray color.

NCCST

群組原則(Group Policy)

- 根據「Active Directory網域服務」(AD DS)設定網路電腦與使用者設定最簡單的方式
- 群組原則用於「控制組態」與「強化安全性」
- 群組原則部署方式
 - 網路
 - 網域環境下，透過網域控制站(Domain Controller)部署
 - 使用者需擁有編輯網域群組原則之權限
 - 欲管理之電腦與使用者，必須加入網域
 - 單機
 - 使用部署工具，如：LocalGPO

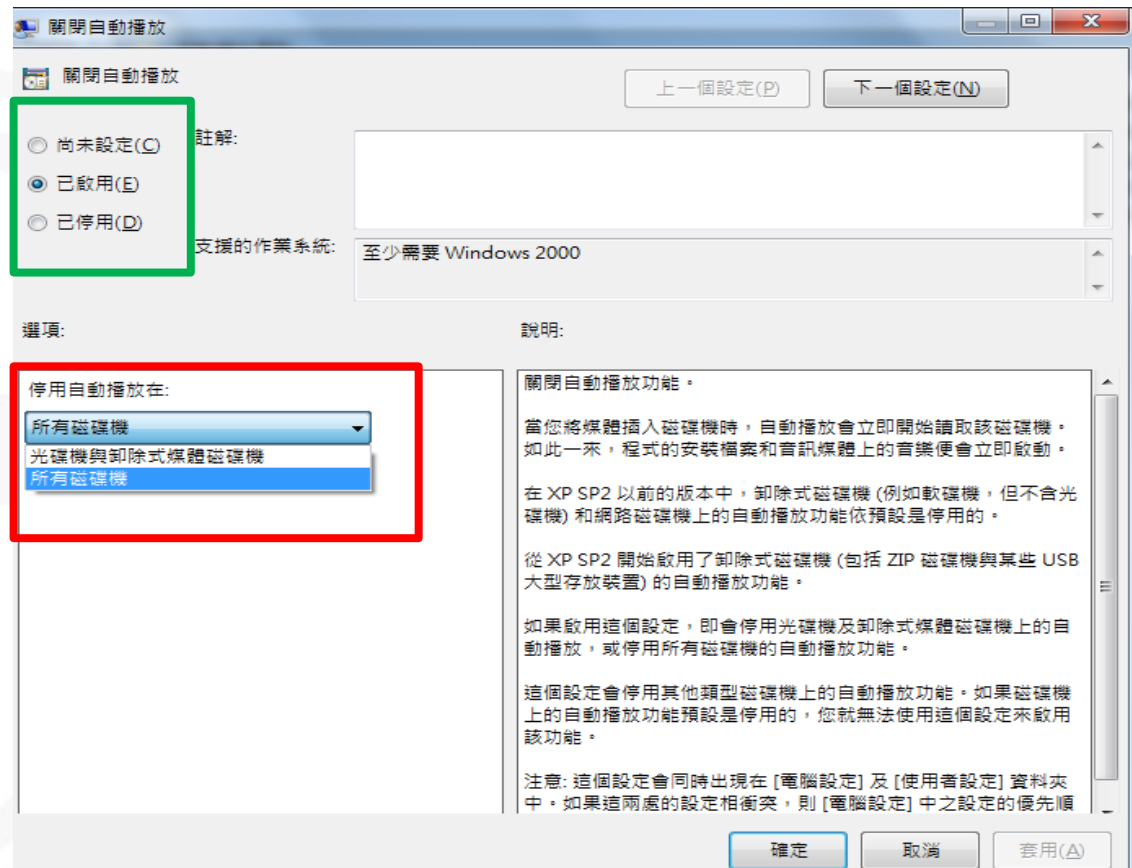
本機群組原則編輯器

- 於「命令提示字元」輸入「gpedit.msc」
 - 需使用「專業版」以上之Windows作業系統

– 設定方式

- 尚未設定
- 啟用
- 停用

◆ 選項設定值



帳戶原則

A large, faint watermark of the NCCST logo is visible in the background on the left side of the slide. It features a shield shape with the letters "NCCST" inside.

帳戶原則\密碼原則

A large, faint watermark of the NCCST logo is visible in the background, centered on the left side of the slide. It features a shield shape with the letters "NCCST" inside.

密碼最長使用期限

- 設定路徑

- 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

- 建議值

- 90(天)以下

- 說明

- 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)

- 數值範圍：1~999 (天)

- 數值 0：代表密碼永遠不會到期

密碼最短使用期限

- 設定路徑

- 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

- 建議值

- 1(天)

- 說明

- 決定在使用者變更密碼之前，密碼必須使用的期限(天數)

- 數值範圍：1~998 (天)

- 數值 0：代表立刻變更密碼

- 限制：密碼最短使用期限不得超過最長使用期限

最小密碼長度

- 設定路徑

- 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

- 建議值

- 8個字元以上

- 說明

- 決定使用者帳戶的密碼可包含的最少字元數

- 數值範圍

- 1~14(字元)

- 數值 0

- 代表不需密碼

密碼必須符合複雜性需求

- 設定路徑

- 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

- 建議值

- 啟用

- 說明

- 決定密碼是否必須符合複雜性需求

- 複雜性需求

- 不包含使用者帳戶名稱全名

- 長度至少為 6 個字元

- 包含「英文大、小寫字元」、「10 進位數字」及「特殊符號」四種字元中的三種

強制執行密碼歷程記錄

- 設定路徑

- 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

- 建議值

- 3次以上

- 說明

- 設定新密碼或密碼更改時，不得與前3次之使用者密碼相同，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
 - 要讓「強制執行密碼歷程記錄」生效，需將「密碼最短使用期限」設為0以上

使用可還原的加密來存放密碼

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\密碼原則\使用可還原的加密來存放密碼

- 建議值

- 停用

- 說明

- 使用可還原的加密來存放密碼，基本上和存放純文字密碼是相同的
 - 支援應用程式使用需要知道使用者密碼來進行驗證的通訊協定，除非應用程式需求比保護密碼資訊重要，否則絕不應該啟用這項原則

帳戶原則\帳戶鎖定原則

A large, faint watermark of the NCCST logo is visible in the background, centered on the left side of the slide. It features the same shield emblem and the acronym "NCCST" in a light gray color.

NCCST

帳戶鎖定閾值

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定閾(閾值)

- 建議值

- 5次不正確的登入嘗試

- 說明

- 決定使用者帳戶被鎖定的嘗試登入失敗次數

- 數值範圍

- 0~999(次)

- 數值 0

- 永不鎖定帳戶

帳戶鎖定期間

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\帳戶鎖定時間

- 建議值

- 15分鐘

- 說明

- 決定在鎖定帳戶自動解除鎖定之前，繼續鎖定的分鐘數

- 數值範圍

- 0~99999(分鐘)

- 限制

- 已設定帳戶鎖定閾值時，此原則設定才有意義

- 已定義帳戶鎖定閾值，帳戶鎖定期間必須大於或等於重設時間

重設帳戶鎖定計數器的時間

- 設定路徑

- 電腦設定\Windows設定\安全性設定\帳戶原則\帳戶鎖定原則\重設帳戶鎖定計數器的時間間隔

- 建議值

- 15分鐘

- 說明

- 決定在登入嘗試失敗之後必須經過幾分鐘，才會將失敗的登入嘗試計數器重設為0次失敗
 - 數值範圍
 - 1~99999(分鐘)
 - 限制
 - 指定帳戶鎖定閾值時，此原則設定才有意義
 - 已定義帳戶鎖定閾值，此重設時間必須小於或等於帳戶鎖定期間

安全性選項

A large, faint watermark of the NCCST logo is visible in the background on the left side of the slide. It features a shield shape with the acronym "NCCST" inside.

安全性選項 (帳戶)

NCCST

帳戶:重新命名系統管理員帳戶



- 設定路徑

- 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

- 建議值

- 機關依實務需求調整建議值(Renamed_Admin)

- 說明

- 重新命名已知的Administrator帳戶會使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和密碼組合

帳戶:重新命名來賓帳戶名稱

- 設定路徑

- 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

- 建議值

- 機關依實務需求調整建議值(Renamed_Guest)

- 說明

- 重新命名已知的 Guest 帳戶會使未經授權的人員較不容易猜出此使用者名稱和密碼組合

帳戶:Administrator 帳戶狀態



- 設定路徑

- 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

- 建議值

- 停用

- 說明

- 停用預設管理者帳戶

- 在停用 Administrator 帳戶後，欲重新啟用此帳戶，需重新輸入密碼。忘記密碼時，須由 Administrators 群組的替代成員，協助重設 Administrator 帳戶密碼

帳戶:Guest 帳戶狀態

- 設定路徑

- 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

- 建議值

- 停用

- 說明

- 停用來賓帳戶

帳戶：限制使用空白密碼的本機帳戶僅能登入到主控台



- 設定路徑

- 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

- 建議值

- 啟用

- 說明

- 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

- 啟用後，未受密碼保護本機帳戶僅能藉由電腦鍵盤登入

安全性選項 (使用者帳戶控制)

NCCST

使用者帳戶控制: 偵測應用程式安裝，並提示提升權限



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 偵測應用程式安裝，並提示提升權限

- 建議值

- 啟用

- 說明

- 當偵測到應用程式安裝封裝需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼
- 輸入有效的認證，操作會以適用的權限繼續

標準使用者帳戶

A large, faint watermark of the NCCST logo is visible in the background on the left side of the slide. It features a shield shape with the acronym "NCCST" in the center.

使用者帳戶控制: 標準使用者之提升權限提示的行為



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 標準使用者之提升權限提示的行為

- 建議值

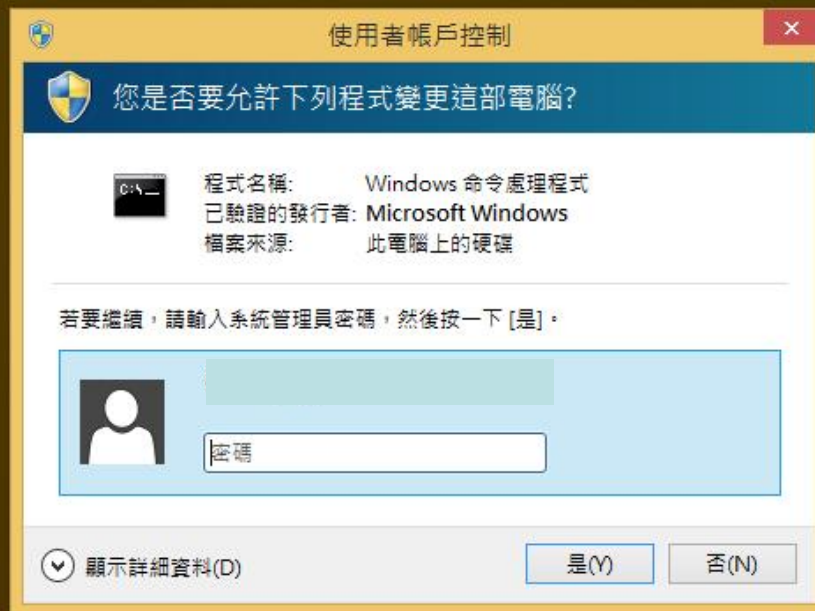
- 提示輸入認證

- 說明

- 當操作需要提升權限時，會提示使用者輸入系統管理使用者名稱與密碼

- 若使用者輸入有效的認證，該操作會以適用的權限繼續執行

管理員核准模式-標準使用者帳戶



系統管理員帳戶

NCCST

使用者帳戶控制:使用內建的 Administrator 帳戶的管理員核准模式



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 使用內建的 Administrator 帳戶的管理員核准模式

- 建議值

- 啟用

- 說明

- 若啟用原則，則使用內建的 Administrator 帳戶使用管理員核准模式

- 根據預設，任何需要提升權限的操作都會提示使用者核准操作

使用者帳戶控制: 所有系統管理員均以管理員核准模式執行



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 所有系統管理員均以管理員核准模式執行

- 建議值

- 啟用

- 說明

- 啟用原則，系統管理員任何需要提升權限的操作都會提示使用者核准操作

使用者帳戶控制:在管理員核准模式，系統管理員之提升權限提示的行為



● 設定路徑

– 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\使用者帳戶控制: 在管理員核准模式，系統管理員之提升權限提示的行為

● 建議值

– 提示要求同意

● 說明

– 當非Microsoft應用程式的操作需要提升權限時，會在安全桌面提示使用者選取「允許」或是「拒絕」

– 選取「允許」，操作會以使用者的最高可用權限繼續

管理員核准模式-系統管理員帳戶



安全性選項 (互動式登入)

NCCST

互動式登入: 在密碼到期前提示使用者變更密碼



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入: 在密碼到期前提示使用者變更密碼

- 建議值

- 14天

- 說明

- 在使用者密碼即將到期時，要提前多久 (天數) 事先提示使用者

互動式登入: 不要求按 CTRL+ALT+DEL 鍵



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入: 不要求按 CTRL+ALT+DEL 鍵

- 建議值

- 停用

- 說明

- 停用原則，則任何使用者都需要按 CTRL+ALT+DEL 才能登入 Windows (除非是使用智慧卡來登入 Windows)

互動式登入: 不要顯示上次登入的使用者名稱



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入:不要顯示上次登入的使用者名稱

- 建議值

- 啟用

- 說明

- 啟用此原則，登入畫面不會顯示上次順利登入的使用者名稱

- 代表每次登入作業系統時，使用者必須輸入 [使用者帳戶名稱] 與 [使用者密碼]

互動式登入: 要求網域控制站驗證以解除鎖定工作站



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入: 要求網域控制站驗證以解除鎖定工作站

- 建議值

- 停用

- 說明

- 必須提供登入資訊才能夠將鎖定的電腦解除鎖定，對於網域帳戶而言，此安全性設定決定是否必須與網域控制站聯絡，才能將電腦解除鎖定
 - 啟用此設定，網域控制站便必須驗證用以解除鎖定電腦的網域帳戶
 - 停用此設定，使用者便可以使用快取的認證來將電腦解除鎖定

互動式登入: 網域控制站無法使用時，要快取的先前登入次數



- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入: 網域控制站無法使用時，要快取的先前登入次數

- 建議值

- 2次

- 說明

- 所有先前使用者的登入資訊存放於本機快取，若網域控制站在後續登入嘗試期間無法使用時，則仍然可以登入
 - 原則設定中，零值會停用登入快取。若值超過50，則只會快取50次登入嘗試

互動式登入: 智慧卡移除操作

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入:智慧卡移除操作

- 建議值

- 鎖定工作站

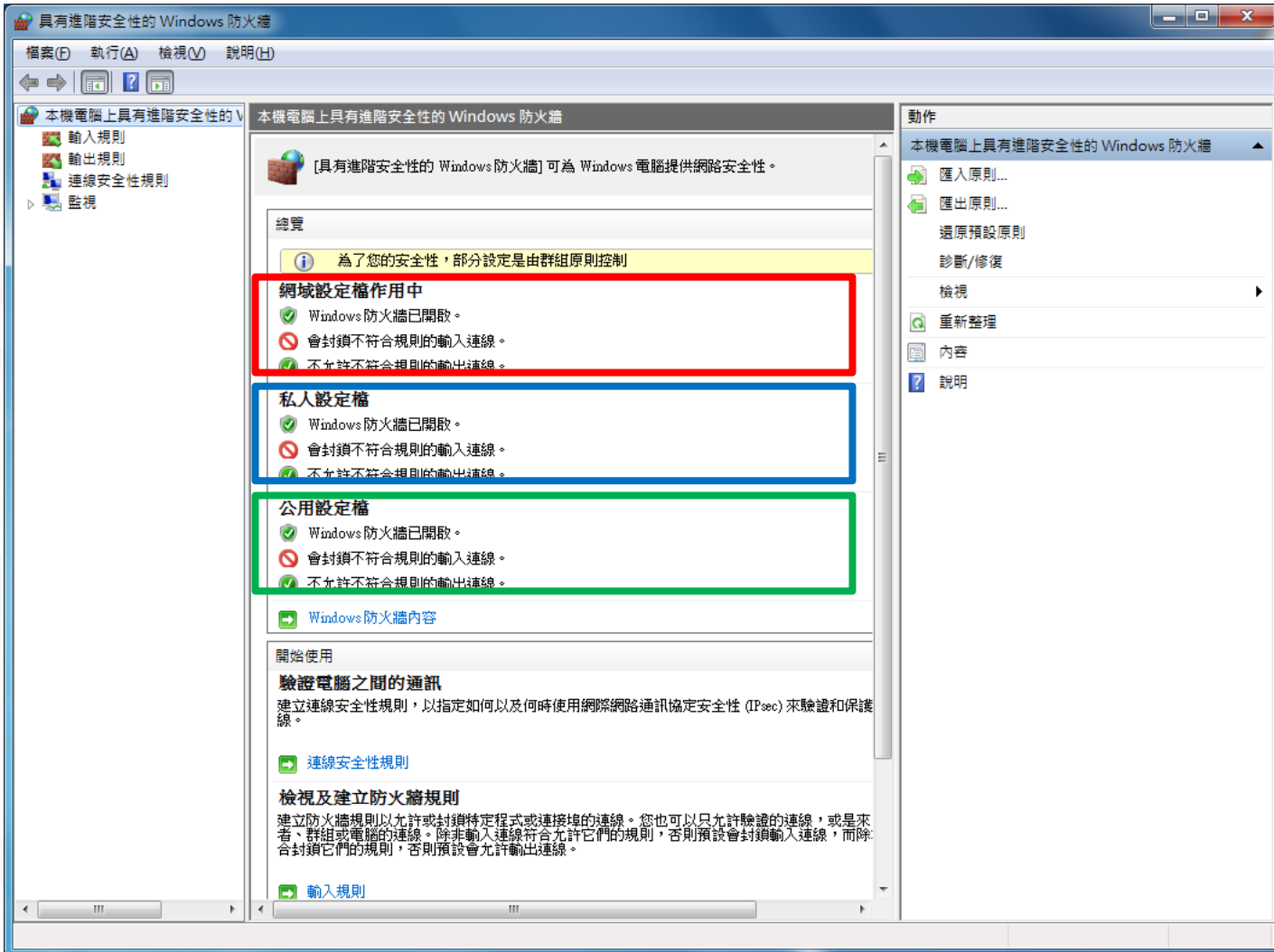
- 說明

- 在智慧卡移除時鎖定工作站，讓使用者帶著智慧卡離開，同時繼續保護工作階段

Windows 防火牆 (網域/私人/公用)

NCCST

Windows 防火牆



防火牆狀態

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\內容\[網域/私人/公用]設定檔\防火牆狀態

- 建議值

- 開啟 (建議選項)

- 說明

- 決定是否開啟Windows防火牆

輸出連線

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\內容\[網域/私人/公用]設定檔\輸出連線

- 建議值

- 允許(預設)

- 說明

- 這項原則設定決定Windows防火牆對於輸出連線的預設行為

輸入連線

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\內容\[網域/私人/公用]設定檔\輸入連線

- 建議值

- 封鎖(預設)

- 說明

- 控制Windows防火牆對於輸入連線的預設行為
- 阻擋防火牆外部對防火牆內部之網路連線

套用本機防火牆規則

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\內容\[網域/私人/公用]設定檔\允許套用本機防火牆規則

- 建議值

- 否

- 說明

- 允許套用本機系統管理員所建立的本機防火牆規則

套用本機連線安全性規則

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\內容\[網域/私人/公用]設定檔\允許套用本機連線安全性規則

- 建議值

- 否

- 說明

- 允許套用本機系統管理員所建立的本機連線安全性規則

Windows防火牆:禁止單點傳送回應到多點傳送或廣播要求



- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\內容\[網域/私人/公用]設定檔\禁止單點傳送回應到多點傳送或廣播要求

- 建議值

- 啟用

- 說明

- 禁止系統針對多點傳送或廣播之要求(Request) 進行回應(Response)

顯示通知

- 設定路徑

- 電腦設定\Windows設定\安全性設定\具有進階安全性的Windows防火牆\具有進階安全性的Windows防火牆\內容\[網域/私人/公用]設定檔\顯示通知

- 建議值

- 是

- 說明

- 當程式接收輸入連線而遭防火牆封鎖時，防火牆即顯示通知告知使用者

Windows 8.1 新增項目說明

NCCST

Windows 7與Windows 8.1比較

作業系統 比較項目		
微軟發布日期	2009年	2013年
GCB發展年份	2013年	2015年
項目	281	340
Windows 8.1 新增功能	<ul style="list-style-type: none"> ● 開始螢幕更新 ● 啟動與導航 ● Win+X選單 ● Windows套用程式商店 ● 雲端整合 	

Windows 元件

NCCST

關閉市集應用程式

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\市集\關閉市集應用程式

- 建議值

- 啟用

- 說明

- 拒絕或允許存取市集應用程式

市集

首頁 App 遊戲



搜尋



熱門免費 App

顯示全部



LINE
★★★★★
免費



KKBOX
★★★★★
免費



Facebook
★★★★★
免費



Messenger
★★★★★
免費



WeChat for Windows 10
★★★★★
免費



RAR Opener
★★★★★
免費



電視連續劇
★★★★★
免費



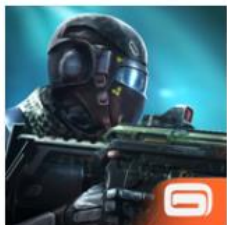
Translator For Microsoft Edge
★★★★★
免費

熱門免費遊戲

顯示全部



狂野飆車8：極速凌雲
★★★★★
免費



現代戰爭5：黑影籠罩
★★★★★
免費



Slither Snake.io
★★★★★
免費



Forza Motorsport 6:
Apex
★★★★★



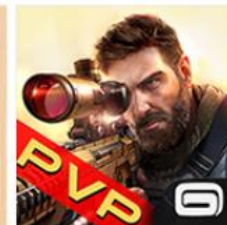
Sonic Dash
★★★★★
免費



神偷奶爸：奔跑小小兵
★★★★★
免費



中國象棋對戰
★★★★★
免費



熾熱狙擊
★★★★★
免費

允許選用 Microsoft 帳戶

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\應用程式執行階段\允許選用 Microsoft 帳戶

- 建議值

- 啟用

- 說明

- 控制需要帳戶登入的Windows市集應用程式是否可以選用Microsoft帳戶

永遠以較高的特殊權限安裝

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows Installer\永遠以較高的特殊權限安裝

- 建議值

- 停用

- 說明

- 指定Windows Installer在安裝任何程式到系統時應使用較高的權限

不要顯示密碼顯示按鈕

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\認證使用者介面\不要顯示密碼顯示按鈕

- 建議值

- 啟用

- 說明

- 可設定當使用者輸入密碼時，是否顯示密碼顯示按鈕

控制記錄檔達到其大小上限時的事件記錄檔行為(應用程式)



- 設定路徑

- 電腦設定\系統管理範本\Windows元件\事件紀錄服務\應用程式\控制記錄檔達到其大小上限時的事件記錄檔行為

- 建議值

- 停用

- 說明

- 如果啟用這個原則設定，且記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失

控制記錄檔達到其大小上限時的事件記錄檔行為(安全性)



- 設定路徑

- 電腦設定\系統管理範本\Windows元件\事件紀錄服務\安全性\控制記錄檔達到其大小上限時的事件記錄檔行為

- 建議值

- 停用

- 說明

- 如果啟用這個原則設定，且記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失

控制記錄檔達到其大小上限時的事件記錄檔行為(系統)



- 設定路徑

- 電腦設定\系統管理範本\Windows元件\事件紀錄服務\系統\控制記錄檔達到其大小上限時的事件記錄檔行為

- 建議值

- 停用

- 說明

- 如果啟用這個原則設定，且記錄檔達到其大小上限時，新事件將不會寫入記錄檔且會遺失

不要連線到任何Windows Update網際網路位置



- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows Update\不要連線到任何Windows Update網際網路位置

- 建議值

- 啟用

- 說明

- 即使Windows Update設定為從內部網路更新服務接收更新，它仍會定期從公用Windows Update服務擷取資訊，以便未來可以連線到Windows Update以及Microsoft Update或Windows市集之類的其他服務

允許未加密的流量(用戶端)

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows 遠端管理(WinRM)\WinRM用戶端\允許未加密的流量

- 建議值

- 停用

- 說明

- 這個原則設定可管理Windows遠端管理(WinRM)用戶端是否透過網路傳送和接收未加密的訊息

允許未加密的流量(服務)

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows 遠端管理(WinRM)\WinRM服務\允許未加密的流量

- 建議值

- 停用

- 說明

- 這個原則設定可管理Windows遠端管理(WinRM)用戶端是否透過網路傳送和接收未加密的訊息

允許基本驗證(用戶端)

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows 遠端管理(WinRM)\WinRM用戶端\允許基本驗證

- 建議值

- 停用

- 說明

- 這個原則設定可管理Windows遠端管理(WinRM)服務是否接受來自遠端用戶端的基本驗證

- 如果停用或未設定這個原則設定，WinRM服務不會接受來自遠端用戶端的基本驗證

允許基本驗證(服務)

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows 遠端管理(WinRM)\WinRM服務\允許基本驗證

- 建議值

- 停用

- 說明

- 這個原則設定可管理Windows遠端管理(WinRM)服務是否接受來自遠端用戶端的基本驗證

不允許摘要式驗證

- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows遠端管理(WinRM)\WinRM用戶端\不允許摘要式驗證

- 建議值

- 啟用

- 說明

- 這個原則設定可管理Windows遠端管理(WinRM)用戶端是否使用摘要式驗證

不允許WinRM儲存RunAs認證



- 設定路徑

- 電腦設定\系統管理範本\Windows元件\Windows遠端管理 (WinRM)\WinRM服務\不允許WinRM儲存RunAs認證

- 建議值

- 啟用

- 說明

- 這個原則設定可管理Windows遠端管理(WinRM)服務是否不允許儲存任何外掛程式的RunAs認證

設定Windows Smart Screen 篩選工具



- 設定路徑

- 電腦設定\系統管理範本\Windows元件\檔案總管\設定 Windows Smart Screen 篩選工具

- 建議值

- 啟用

- 在執行不明軟體下載之前需要系統管理員核准

- 說明

- Windows Smart Screen篩選工具會在從網際網路執行無法辨識的程式下載之前警告使用者，使電腦更加安全。啟用這個功能時，會將檔案以及在電腦上執行之程式的相關資訊傳送給Microsoft

Smart Screen設定方式(1/7)



設定 Windows SmartScreen 篩選工具

上一個設定(P)

下一個設定(N)

- 尚未設定(C) 註解:
- 已啟用(E)
- 已停用(D)

支援的作業系統:

至少需要 Windows Server 2012、Windows 8 或 Windows RT

選項:

說明:

選擇下列其中一個設定

- 在執行不明軟體下載之前需要系統管理員核准
- 在執行不明軟體下載之前需要系統管理員核准
- 在執行不明軟體下載之前對使用者提出警告
- 關閉 SmartScreen 篩選工具

這個原則設定可讓您管理 Windows SmartScreen 篩選工具的行為。Windows SmartScreen 篩選工具會在從網際網路執行無法辨識的程式下載之前警告使用者，使電腦更加安全。啟用這個功能時，會將檔案以及在電腦上執行之程式的相關資訊傳送給 Microsoft。

啟用這個原則設定，可以透過設定下列其中一個選項來控制 Windows SmartScreen 篩選工具的行為：

Smart Screen設定方式(2/7)



→ ↑ 控制台 ▾ ▾ ↻ 搜尋控制台

調整電腦設定

檢視方



系統及安全性

檢閱您的電腦狀態
使用檔案歷程記錄來儲存檔案的備份副本
找出問題並修復



網路和網際網路

檢視網路狀態及工作
選擇家用群組和共用選項



硬體和音效

檢視裝置和印表機
新增裝置



程式集

解除安裝程式



使用者帳戶和家庭安全

變更帳戶類型
 為使用者設定家長監護服務



外觀及個人化

變更佈景主題
變更桌面背景
調整螢幕解析度



時鐘、語言和區域

新增語言
變更輸入法
變更日期、時間或數字格式



輕鬆存取

讓 Windows 建議設定
最佳化視覺顯示

Smart Screen設定方式(3/7)



系統及安全性 ▾



搜尋控制台



重要訊息中心

檢視電腦的狀態和解決問題



變更使用者帳戶控制設定

疑難排解常見電腦問題



Windows 防火牆

檢查防火牆狀態

允許應用程式通過 Windows 防火牆



系統

檢視 RAM 大小及處理器速度



允許遠端存取

啟動遠端協助

查看此電腦的名稱



Windows Update

開啟或關閉自動更新

檢查更新

安裝選用更新

檢視更新記錄



電源選項

喚醒電腦時必須輸入密碼

變更電源按鈕行為

變更電腦睡眠的時間



檔案歷程記錄

使用檔案歷程記錄來儲存檔案的備份副本

使用檔案歷程記錄來還原檔案

Smart Screen設定方式(4/7)

← → ▾ ↑  ▶ 控制台 ▶ 系統及安全性 ▶ 重要訊息中心

控制台首頁

變更重要訊息中心設定

 變更使用者帳戶控制設定

 **變更 Windows SmartScreen
篩選工具設定**


檢視封存的訊息

檢視最近訊息，並

重要訊息中心偵測到一個

安全性(S)

網路防火牆 (重要)

 Windows 防火

關閉有關 網路防火

Smart Screen設定方式(5/7)



Smart Screen設定方式(6/7)



Windows 已保護您的電腦

Windows SmartScreen 篩選工具已防止某個無法辨識的應用程式啟動。執行此應用程式可能會讓您的電腦暴露在風險中。

其他資訊

確定

Smart Screen設定方式(7/7)



Windows 已保護您的電腦

Windows SmartScreen 篩選工具已防止某個無法辨識的應用程式啟動。執行此應用程式可能會讓您的電腦暴露在風險中。

發行者:

應用程式:

仍要執行

不要執行

系統起始的重新啟動系統之後自動登入 最後一個互動式使用者



● 設定路徑

– 電腦設定\系統管理範本\Windows元件\Windows登入
選項\系統起始的重新啟動系統之後自動登入最後一個
互動式使用者

● 建議值

– 停用

● 說明

- 這個原則設定可控制裝置是否在Windows Update重新啟動系統之後自動登入最後一個互動式使用者
- 如果停用這個原則設定，裝置不會儲存Windows Update重新啟動之後自動登入的使用者認證
- 系統重新啟動之後，使用者鎖定畫面的應用程式不會重新啟動

加入Microsoft MAPS



- 設定路徑

- 電腦設定\系統管理範本\Windows元件\ Windows Defender\MAPS\加入Microsoft MAPS

- 建議值

- 停用

- 說明

- MAPS=Microsoft Active Protection Service

- 這個原則設定可加入 Microsoft MAPS。Microsoft MAPS 是協助使用者選擇如何回應潛在威脅的線上社群。這個社群也可協助停止散佈新惡意軟體的感染

安全性選項\帳戶

NCCST

帳戶：封鎖 Microsoft 帳戶

- 設定路徑

- 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

- 建議值

- 使用者無法新增Microsoft 帳戶或以Microsoft 帳戶登入

- 說明

- 此原則設定可防止使用者在此電腦上新增Microsoft 帳戶

安全性選項\稽核

A large, faint watermark of the NCCST logo is visible in the background, centered on the left side of the slide. It features a shield shape with the letters "NCCST" inside.

NCCST

稽核：當無法記錄安全性稽核時，系統立即關機



- 設定路徑

- 電腦設定\Windows設定\安全性設定\本機原則\安全性選項\本機原則\安全性選項\稽核：當無法記錄安全性稽核時，系統立即關機

- 建議值

- 停用

- 說明

- 這項安全性設定決定系統在無法記錄安全性事件時，是否要立即關機

安全性選項\裝置

NCCST

裝置：允許格式化以及退出卸除式媒體

- 設定路徑

- 電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\裝置：允許格式化以及退出卸除式媒體

- 建議值

- Administrators and Interactive Users

- 說明

- 此安全性設定決定允許哪些人格式化和退出卸除式 NTFS 媒體



系統\登入

NCCST

不要顯示網路選取UI

- 設定路徑

- 電腦設定\系統管理範本\系統\登入\不要顯示網路選取UI

- 建議值

- 啟用

- 說明

- 這個原則設定可控制是否讓任何人在登入畫面上與可用的網路UI互動

- 如果啟用這個原則設定，則登入Windows之後才能變更電腦的網路連線狀態

不要列舉加入網域電腦上的連線使用者

- 設定路徑

- 電腦設定\系統管理範本\系統\登入\不要列舉加入網域電腦上的連線使用者

- 建議值

- 啟用

- 說明

- 這個原則設定會禁止列舉加入網域電腦上的連線使用者
 - 如果啟用這個原則設定，登入介面不會列舉加入網域電腦上的連線使用者

列舉加入網域電腦上的本機使用者



- 設定路徑

- 電腦設定\系統管理範本\系統\登入\列舉加入網域電腦上的本機使用者

- 建議值

- 停用

- 說明

- 這個原則設定會允許列舉加入網域電腦上的本機使用者
 - 如果啟用這個原則設定，登入介面將會列舉加入網域電腦上的本機使用者

關閉鎖定畫面上的應用程式通知

- 設定路徑

- 電腦設定\系統管理範本\系統\登入\關閉鎖定畫面上的應用程式通知

- 建議值

- 啟用

- 說明

- 這個原則設定可以讓使用者不要在鎖定畫面上顯示應用程式通知

- 如果啟用該原則設定，則不會在鎖定畫面上顯示應用程式通知

開啟PIN登入

- 設定路徑

- 電腦設定\系統管理範本\系統\登入\開啟PIN登入

- 建議值

- 停用

- 說明

- 這個原則設定可以讓使用者控制是否讓網域使用者使用PIN登入

- 如果啟用這個原則設定，網域使用者可以設定並使用PIN登入

系統\開機初期的反惡意程式碼

NCCST

開機啟動驅動程式初始化原則

- 設定路徑

- 電腦設定\系統管理範本\系統\開機初期的反惡意程式碼
\開機啟動驅動程式初始化原則

- 建議值

- 啟用

- 良好與不明

- 說明

- 這個原則設定允許使用者根據開機初期啟動的反惡意程式碼開機啟動驅動程式所判斷的分類，指定要初始化哪些開機啟動驅動程式

系統

A large, faint watermark of the NCCST logo is positioned on the left side of the slide. It features a shield shape with the acronym "NCCST" in the center, rendered in a light gray color.

指定選用之元件安裝和元件修復的相關設定



- 設定路徑

- 電腦設定\系統管理範本\系統\指定選用之元件安裝和元件修復的相關設定

- 建議值

- 啟用

- 不要從Windows Update 下載裝載

- 說明

- 這個原則設定會指定網路位置，用於修復損毀的作業系統以及啟用已經移除其裝載檔案的選用功能



網路\Windows連線管理員

NCCST

當連線到通過網域驗證的網路時，禁止 連線到非網域網路



- 設定路徑

- 電腦設定\系統管理範本\網路\Windows連線管理員\當連線到通過網域驗證的網路時，禁止連線到非網域網路

- 建議值

- 啟用

- 說明

- 這個原則設定可避免電腦同時連線到網域型網路以及非網域型網路

網際網路通訊管理\網際網路通 訊設定

NCCST

關閉市集的存取權

- 設定路徑

- 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\關閉市集的存取權

- 建議值

- 啟用

- 說明

- 這個原則設定指定是否使用市集服務尋找應用程式來開啟具有未處理檔案類型或通訊協定關聯的檔案

其他

NCCST

在鎖定畫面上關閉快顯通知

- 設定路徑

- 使用者設定\系統管理範本\[開始]功能表與工作列\通知\在鎖定畫面上關閉快顯通知

- 建議值

- 啟用

- 說明

- 這個原則設定可在鎖定畫面上關閉快顯通知

- 如果啟用這個原則設定，應用程式將無法在鎖定畫面上引發快顯通知

進階稽核原則設定

A large, faint watermark of the NCCST logo is centered on the page. It features a shield shape with the acronym "NCCST" written inside in a light gray font.

稽核原則

- 用於檢查及審查可能影響系統安全性之活動，目的是讓系統管理員記錄及檢視指定之安全性相關活動事件的功能和服務
- 「本機原則\稽核原則」
 - 於Windows 2000 開始啟用
 - 9項基本稽核原則設定
- 「進階稽核原則設定」
 - 於Windows Vista與Windows Server 2008開啟啟用
 - 19項進階稽核原則
 - 於Windows 7與Windows Server 2008 R2中與群組原則整合，可透過網域進行群組原則部署作業

成功事件與失敗事件

- 成功稽核事件

- 當已定義之動作成功完成時，就會觸發成功稽核事件

- 失敗稽核事件

- 當已定義之動作未成功完成時，就會觸發失敗稽核事件

- 事件記錄檔中出現失敗稽核事件，不代表系統發生錯誤

- 如：稽核登入事件，失敗事件可能是使用者輸入錯誤密碼，導致登入失敗

稽核原則：帳戶登入

NCCST

稽核原則：帳戶登入：稽核驗證認證

- 設定路徑

- 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

- 建議值

- 成功與失敗

- 說明

- 稽核因使用者帳戶登入認證的驗證測試而產生的事件

稽核原則：帳戶管理

NCCST

稽核原則：帳戶管理：電腦帳戶管理



- 設定路徑

- 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：電腦帳戶管理

- 建議值

- 成功

- 說明

- 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
- 如設定此原則，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，失敗稽核則會記錄失敗嘗試

稽核原則：帳戶管理：使用者帳戶管理



- 設定路徑

- 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：使用者帳戶管理

- 建議值

- 成功與失敗

- 說明

- 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等事件變更

稽核原則：詳細追蹤

A large, faint watermark of the NCCST logo is visible in the background on the left side of the slide. It features a shield shape with the acronym "NCCST" inside.

NCCST

稽核原則：詳細追蹤：建立處理程序

- 設定路徑

- 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：詳細追蹤：建立處理程序

- 建議值

- 成功

- 說明

- 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

稽核原則：登入-登出

NCCST

稽核原則：登入-登出：帳戶鎖定

- 設定路徑

- 電腦設定\Windows設定\安全性設定\進階稽核原則設定\稽核原則\登入/登出\稽核原則：登入-登出：帳戶鎖定

- 建議值

- 成功與失敗

- 說明

- 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

稽核原則：登入-登出：登出

- 設定路徑

- 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：登出

- 建議值

- 成功

- 說明

- 稽核因關閉登入工作階段而產生的事件

稽核原則：登入-登出：登入

- 設定路徑

- 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：登入

- 建議值

- 成功與失敗

- 說明

- 稽核因電腦上的使用者帳戶登入嘗試而產生的事件，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

稽核原則：登入-登出：特殊登入

- 設定路徑

- 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：特殊登入

- 建議值

- 成功

- 說明

- 稽核因特殊登入而產生的事件，例如: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

稽核原則：物件存取

NCCST

稽核原則：物件存取：卸除式存放裝置



- 設定路徑

- 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：卸除式存放裝置

- 建議值

- 成功

- 說明

- 此原則設定可稽核存取卸除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

稽核原則：特殊權限使用

NCCST

稽核原則：特殊權限使用：機密特殊權限使用



- 設定路徑

- 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：機密特殊權限使用

- 建議值

- 成功與失敗

- 說明

- 稽核使用特殊使用者權限時產生的事件，例如：呼叫備份與還原\檔案及目錄、讓電腦及使用者帳戶受信賴，以進行委派、產生安全性稽核、載入及解除載入裝置驅動程式、管理稽核及安全性記錄檔、取得檔案或其他物件的擁有權及修改韌體環境值等特殊權限使用

稽核原則：系統

A large, faint watermark of the NCCST logo is visible in the background, centered on the left side of the slide. It features the same shield emblem and the acronym "NCCST" in a light gray color.

NCCST

稽核原則：系統：安全性狀態變更



- 設定路徑

- 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：安全性狀態變更

- 建議值

- 成功與失敗

- 說明

- 稽核因電腦安全性狀態變更而產生的事件，例如：電腦的啟動及關閉、系統時間的變更...等狀態變更

稽核原則：系統：系統完整性



- 設定路徑

- 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：系統完整性

- 建議值

- 成功與失敗

- 說明

- 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

- 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

報告完畢
敬請指教

NCCST