# Tenable Identity Exposure SaaS 使用者指南

上次修訂日期：2025 年 6 月 5 日

版權所有 © 2025 Tenable, Inc.保留所有權利。Tenable、Tenable Nessus、Tenable Lumin、Assure 和 Tenable 標誌是 Tenable, Inc. 的註冊商標。或其附屬公司的註冊商標。所有其他產品或服務均為其各自所有者的商標。

# 目錄


**歡迎使用 Tenable Identity Exposure 3.42 內部部署 SaaS 使用者指南 ..... 12**

關於本指南 ..... 12

**開始使用 Tenable Identity Exposure SaaS ..... 13**

查看先決條件 ..... 14

安裝 ..... 14

設定 ..... 15

使用 ..... 15

將 Tenable Identity Exposure 擴充為 Tenable One ..... 15

安全轉送要求 ..... 17

Tenable Identity Exposure 的安全轉送 ..... 23

安全轉送要求 ..... 30

設定轉送 ..... 37

安裝安全轉送 (CLI) ..... 38

安裝安全轉送 (Tenable Agent) ..... 40

解決安全轉送安裝的問題 ..... 42

開始使用 Tenable Identity Exposure ..... 50

**Tenable Identity Exposure 的基本知識 ..... 72**

登入 Tenable Identity Exposure ..... 72

Tenable Identity Exposure 使用者入口網站 ..... 77

Tenable Identity Exposure 深入分析 ..... 80

標題 ..... 81

跨區段瀏覽 ..... 81

選取網域/組織 ..... 82

優先事項與修復區段 ..... 82
群體特徵區段 ..... 83
如要深入瞭解詳細資訊： ..... 85
「研究發現趨勢」區段 ..... 85
建立報告 ..... 86
存取工作區 ..... 89
工作區選單 ..... 90
工作區頁面 ..... 90
使用者喜好設定 ..... 93
通知 ..... 96
儀表板 ..... 98
小工具 ..... 99
曝險中心 ..... 103
先決條件 ..... 103
另請參閱 ..... 104
曝險概覽 ..... 104
標頭資訊 ..... 105
脆弱環節清單 ..... 105
搜尋、篩選、匯出和欄顯示選項 ..... 105
另請參閱 ..... 110
曝險情況 ..... 110
一般資訊 ..... 111
詳細資訊 ..... 111
分析研究發現 ..... 112

研究發現詳細資料 ..... 114
搜尋、篩選和匯出選項 ..... 117
若要篩選脆弱環節清單： ..... 118
另請參閱 ..... 119
曝險情況排除項目 ..... 119
設定資產排除項目，調整您的安全掃描 ..... 119
Identity 360：全面的身分風險管理 ..... 123
身分收集 ..... 126
IDP 租用戶、網域和組織 ..... 126
跨產品資料 (資料來源) ..... 127
主要元素 ..... 128
另請參閱 ..... 129
身分詳細資料 ..... 130
若要存取此頁面： ..... 130
標頭和頂端區段 ..... 130
標頭索引標籤 ..... 132
139
Identity 360 基本資訊 ..... 142
如要套用篩選器： ..... 143
若要匯出資料： ..... 145
若要自訂欄顯示： ..... 146
預設欄 ..... 147
如要重設為預設欄： ..... 147
瞭解租用戶成員資格 ..... 147

將資產連結至租用戶 ..... 148
識別租用戶 ..... 148
範例 ..... 148
特殊案例：瞭解樹系根網域連結 ..... 148
什麼是樹系根網域？ ..... 148
特殊情況產生的方式 ..... 148
範例 ..... 149
範例 ..... 149
為什麼這很重要 ..... 149
Tenable 身分識別總管選擇「租用戶」作為根容器名稱的原因 ..... 150
追蹤流程 ..... 150
追蹤流程表 ..... 151
使用精靈搜尋追蹤流程 ..... 153
手動搜尋追蹤流程 ..... 155
自訂追蹤流程查詢 ..... 156
書籤查詢 ..... 159
查詢歷史記錄 ..... 161
顯示異常事件 ..... 163
事件詳細資料 ..... 164
屬性變更 ..... 167
追蹤流程使用案例 ..... 170
曝險指標 ..... 174
異常情況解決與偵測日期 ..... 176
曝險指標詳細資料 ..... 177

異常物件 ..... 179
搜尋異常物件 ..... 181
略過異常物件或原因 (異常情況) ..... 185
罪證屬性 ..... 188
根據 RSoP 的曝險指標 ..... 190
增強功能 ..... 191
好處 ..... 191
技術層面 ..... 191
修復曝險指標中的異常情況 ..... 192
針對標準使用者設定的 AdminCount 屬性 ..... 192
危險的 Kerberos 委派作業 ..... 195
確保 SDProp 一致性 ..... 200
攻擊指標 ..... 203
攻擊指標詳細資料 ..... 206
攻擊指標資安事端 ..... 208
拓撲 ..... 214
信任關係 ..... 215
危險的信任 ..... 217
攻擊路徑 ..... 219
攻擊關係 ..... 223
新增金鑰憑證 ..... 225
新增成員 ..... 226
允許行動 ..... 227
允許委派 ..... 230

屬於 GPO ..... 232
DCSync ..... 234
授權允許行動 ..... 236
有 SID 歷程記錄 ..... 237
隱含接管 ..... 239
繼承 GPO ..... 241
連結的 GPO ..... 242
成員隸屬於 ..... 244
擁有 ..... 245
重設密碼 ..... 247
RODC 管理 ..... 248
寫入 DACL ..... 250
寫入所有者 ..... 252
識別第 0 層資產 ..... 253
包含攻擊路徑的帳戶 ..... 255
攻擊路徑節點類型 ..... 257
活動記錄 ..... 259
特權實體定義 ..... 261
Active Directory ..... 261
Entra ID ..... 262
**Tenable Identity Exposure 設定和管理 ..... 263**
啟用 Identity 360、曝險中心和 Microsoft Entra ID 支援 ..... 263
Active Directory 設定 ..... 264
存取 AD 物件或容器 ..... 265

特權分析的存取權 ..... 266
攻擊指標的部署 ..... 272
安裝攻擊指標 ..... 275
攻擊指標安裝指令碼 ..... 282
技術變更和潛在影響 ..... 290
攻擊情境 (< v. 3.36) ..... 291
安裝 Microsoft Sysmon ..... 295
解除安裝攻擊指標 ..... 300
從 SYSVOL 手動移除過時的 GPO 資料夾 ..... 301
停用的攻擊指標 ..... 302
第一列圖示狀態 ..... 303
其他列圖示狀態 ..... 303
對攻擊指標進行疑難排解 ..... 305
防毒軟體偵測 ..... 305
進階稽核原則設定優先順序 ..... 306
事件記錄接聽程式驗證 ..... 308
Tenable Identity Exposure 記錄檔 ..... 310
DFS 複製問題緩解措施 ..... 316
Windows 事件記錄保留 ..... 317
攻擊指標警示中的「未知」 ..... 318
操作攻擊指標 ..... 322
攻擊指標偵測延遲 ..... 323
驗證 ..... 324
使用 Tenable One 驗證 ..... 324

使用 Tenable Identity Exposure 帳戶進行驗證 ..... 324
使用 LDAP 驗證 ..... 328
使用 SAML 驗證 ..... 333
使用者帳戶 ..... 336
安全性設定檔 ..... 339
自訂指標 ..... 341
縮小指標自訂範圍 ..... 343
使用者角色 ..... 344
管理角色 ..... 345
設定角色的權限 ..... 346
設定使用者介面實體的權限 (範例) ..... 350
樹系 ..... 352
管理樹系 ..... 352
保護服務帳戶 ..... 353
網域 ..... 354
在網域上強制執行資料重新整理 ..... 357
誘捕帳戶 ..... 358
Kerberos 驗證 ..... 360
警示 ..... 367
SMTP 伺服器設定 ..... 367
部署架構的差異 ..... 367
安全轉送環境的 SMTP 伺服器設定 ..... 368
VPN 環境的 SMTP 伺服器設定 ..... 369
電子郵件警示 ..... 370

Syslog 警示 ..... 374
Syslog 和電子郵件警示詳細資料 ..... 378
Syslog 訊息框架 ..... 381
運作狀況檢查 ..... 384
運作狀況檢查清單 ..... 388
報告中心 ..... 391
Microsoft Entra ID 支援 ..... 392
重新整理 Entra ID 憑證 ..... 400
如要重新整理憑證並恢復同步，請按照下列步驟操作： ..... 401
Tenable Cloud 資料收集 ..... 405
特權分析 ..... 406
活動記錄 ..... 407
Tenable Identity Exposure 公用 API ..... 409
資料管理 ..... 411
部署區域 ..... 412
Tenable Identity Exposure 授權 ..... 413
管理您的授權 ..... 415
防止容器 UUID 不相符 ..... 416
長期支援 (LTS) 版本與一般版本：主要差異和好處 ..... 419
什麼是 LTS? ..... 419
什麼是一般版本? ..... 420
LTS 和一般版本之間的主要差異： ..... 420
為何選擇 LTS? ..... 420
為什麼要選擇一般版本? ..... 420

排解 Tenable Identity Exposure 問題 ..... 420
SYSVOL 強化干擾 Tenable Identity Exposure ..... 421
系統公用程式 (handle.exe) ..... 430

# 歡迎使用 Tenable Identity Exposure 3.42 內部部署 SaaS 使用者指南

**上次更新時間**：年月日

Tenable Identity Exposure 可讓您預測威脅、偵測安全缺口和回應資安事端與攻擊，藉此保障基礎架構的安全。您可以使用直覺易懂的儀表板即時監控 Active Directory，輕鬆找出最關鍵的弱點及相關的修復程序建議。透過 Tenable Identity Exposure 的攻擊指標和曝險指標，您可搜尋影響 Active Directory 的根本問題、識別危險的信任關係，以及分析攻擊的深入詳細資料。

**若要開始，請參閱** 開始使用 Tenable Identity Exposure。

## 關於本指南

此 Tenable Identity Exposure SaaS 使用者指南提供下列資訊：

- 安裝安全轉送
- 啟用安全性監控前要執行的工作。
- Tenable Identity Exposure 的設定和使用

攻擊指標和曝險指標功能是否可用取決於您購買的授權。

**注意：**Tenable Identity Exposure 可單獨使用，也可作為 Tenable One 套件的一部分使用。如需詳細資訊，請參閱 Tenable One。

**提示：**此 *Tenable Identity Exposure 使用者指南*有英文、法文、德文、日文、韓文、簡體中文、西班牙文和繁體中文版本。此 *Tenable Identity Exposure* 使用者介面有英文、法文、德文、日文、韓文、簡體中文、西班牙文和繁體中文版本。若要變更使用者介面語言，請查看使用者喜好設定。

如需有關 Tenable Identity Exposure 的其他資訊，請檢閱下列客戶教育資料：

- Tenable Identity Exposure 自助指南
- Tenable Identity Exposure 簡介 (Tenable University)

## Tenable One 曝險管理平台

Tenable One 是一個曝險管理平台，可幫助組織瞭解現代攻擊破綻，集中精力於防止可能發生的攻擊，並準確傳達網路風險以支援最佳業務績效。

此平台結合了 IT 資產、雲端資源、容器、Web 應用程式和身分識別系統等最廣泛的弱點涵蓋範圍，以 Tenable Research 弱點涵蓋的速度和廣度為基礎，並加入全面的分析來排定行動的優先順序和傳達網路風險。Tenable One 能夠協助組織：

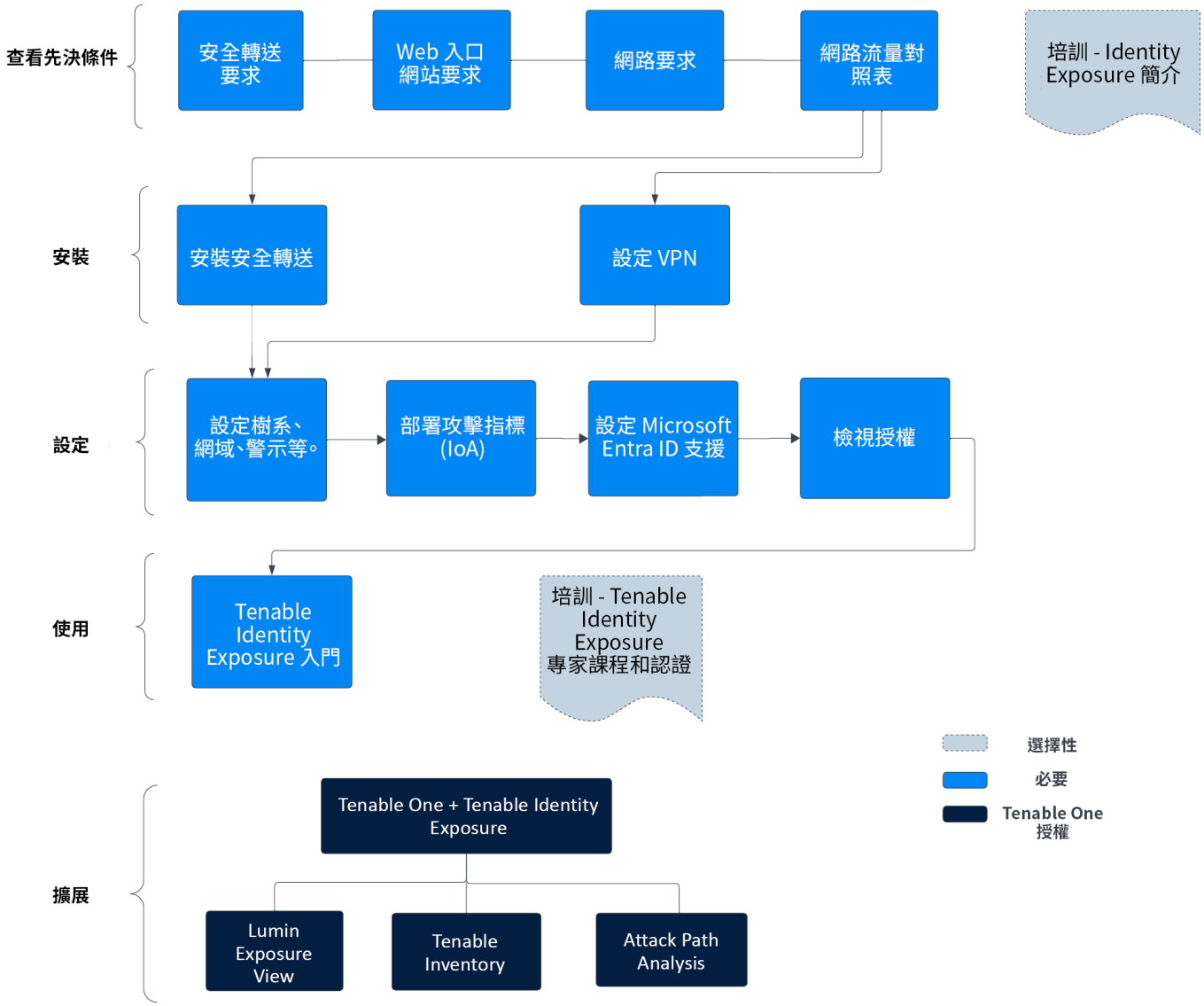
- 全面瞭解現代攻擊破綻
- 預測威脅並確定攻擊防範措施的優先順序
- 傳達網路風險以做出更好的決策

Tenable Identity Exposure 是一款獨立產品，但也可做為 Tenable One 曝險管理平台的一部分購買。

**提示：**如需 Tenable One 產品使用入門的其他資訊，請參閱 Tenable One 部署指南。

## 開始使用 Tenable Identity Exposure SaaS

使用下列工作流程執行 Tenable Identity Exposure 的部署作業。




## 查看先決條件

1. **檢閱**版本資訊。
2. **檢閱並瞭解安全轉送**在 Tenable Identity Exposure 平台中的角色：自 **3.59** 版起，必要的安全轉送功能可讓您設定網域，轉送會從該網域將資料轉送至負責收集 AD 物件的目錄接聽程式元件。參閱安全轉送要求。

## 安裝

1. **安裝** Tenable Identity Exposure 的安全轉送 。

## 設定

1. **檢閱** Tenable Identity Exposure 授權。

## 使用

- 開始使用 Tenable Identity Exposure

# 將 Tenable Identity Exposure 擴充為 Tenable One

**注意**：這需要 Tenable One 授權。如需有關試用 Tenable One 的詳細資訊，請參閱 Tenable One。

將 Tenable Identity Exposure 與 Tenable One 整合，並利用下列功能：

- 在 Lumin Exposure View 中，取得重要業務服務、處理程序和功能的業務一致網路曝險分數，以取得重要的業務背景資訊，並依據 SLA 追蹤交付。追蹤整體身分風險，以瞭解 Web 應用程式對您的整體網路曝險分數所造成的風險影響。
    - 檢閱「**全域**」曝險資訊卡，瞭解您的整體分數。按一下「**每次曝險**」以瞭解決定您獲得分數的因素以及影響程度。
    - 檢閱「**Active Directory**」曝險資訊卡。
    - 設定曝險檢視設定以設定自訂的**卡片目標**，並根據貴公司的原則，設定「**修復 SLA**」和「**SLA 效率**」。
    - 根據業務背景資訊 (例如，「網域」、「網域管理員」、「資產關鍵性」、「重要使用者/重要資產」或「服務帳戶」)，建立自訂曝險資訊卡。
- 在 Tenable Inventory 中，透過存取更深入的資產深入解析 (包括相關攻擊路徑、標籤、曝險資訊卡、使用者、關係等)，增強資產情報。透過可評估身分的總資產風險和資產關鍵性的資產曝險分數，取得更完整的資產曝險檢視，進而提高風險評分。
    - 檢閱您的 AD 資產，瞭解介面的策略性性質。這應該有助於設定您預期在 Tenable Inventory 中使用的功能以及時機。
    - 檢閱您可以使用、編輯和加入書籤的 **Tenable 查詢** 。
    - 熟悉「全域搜尋」查詢產生器及其物件和屬性。將自訂查詢加入書籤，以供日後使用。

**提示：**若要快速檢視可用的屬性：

- 在查詢產生器中，輸入「*has*」。建議的資產屬性清單隨即顯示。
- 透過新增欄自訂清單。可用欄/內容的清單會隨即顯示。

  - 向下切入「資產詳細資料」頁面，以檢視資產屬性和所有相關聯的背景資訊檢視。
  - (選擇性) 建立標籤，其可結合不同的資產類別。

- 在 Attack Path Analysis 中，透過暴露周遊攻擊破綻的高風險攻擊路徑 (包括 Web 應用程式、IT、OT、IoT、身分、ASM)，將風險優先順序最佳化，並防止重大影響。透過識別阻擋點以中斷攻擊路徑，並結合緩解指南來簡化緩解措施，同時透過 AI 深入解析獲得深入的專業知識。

  - 檢視 **Attack Path Analysis 儀表板**，以獲得易受攻擊資產的概覽性檢視，例如通往這些重要資產的攻擊路徑數、開放研究發現數目及其嚴重性、用於檢視來源節點曝險分數不同之路徑和 ACR 目標值組合的矩陣，以及趨勢攻擊路徑清單。

    - 檢閱「**常見攻擊路徑矩陣**」，然後按一下「**常見攻擊路徑**」圖塊，以檢視有關通往 "Crown Jewels" 或網域管理員的路徑的詳細資訊。

    您可以視需要進行調整，以確保您所檢視的是最重要的攻擊路徑資料和研究發現。

  - 在「**研究發現**」頁面上，將您的資料與進階圖形分析和 MITRE ATT&CK® 架構配對以建立「研究發現」，藉此檢視一個或多個攻擊路徑中存在的所有攻擊技術，這些攻擊路徑會通往一個或多個重要資產，讓您瞭解會導致及放大對資產和資訊的威脅影響的未知數，並對其採取行動。

  - 在「**搜尋**」頁面上，產生攻擊路徑查詢，以便將您的資產當作潛在攻擊路徑的一部分檢視：

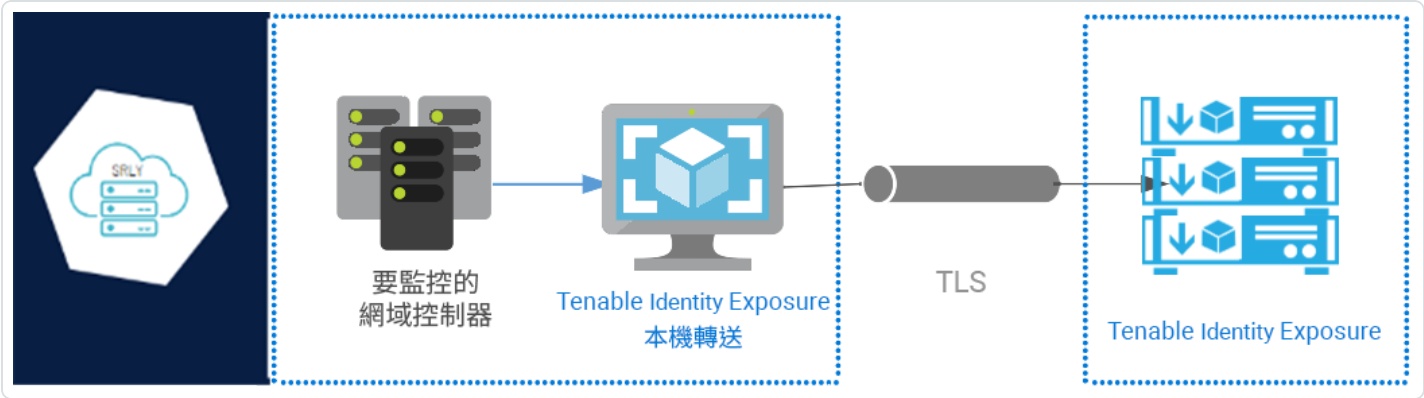
    - 使用內建查詢產生攻擊路徑
    - 使用資產查詢產生器產生資產查詢
    - 使用攻擊路徑查詢產生器產生攻擊路徑查詢

然後，您可以透過查詢結果清單和互動式圖形，檢視攻擊路徑查詢和資產查詢資料並與其互動。

## 安全轉送要求

**安全轉送**是一種使用傳輸層安全性 (TLS) 而不是 VPN 將 Active Directory 資料從您的網路傳輸到 Tenable Identity Exposure 的傳輸模式，如此圖所示。如果您的網路需要 Proxy 伺服器才能連線至網際網路，則安全轉送功能現在也支援需要或不需要驗證的 HTTP Proxy。

Tenable Identity Exposure 可支援多種安全轉送，您可以根據需要將其對應至網域。




### TLS 要求

如要使用 TLS 1.2，自 2024 年 1 月 24 日起，您的轉送伺服器必須至少支援下列其中一項加密套件：

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`

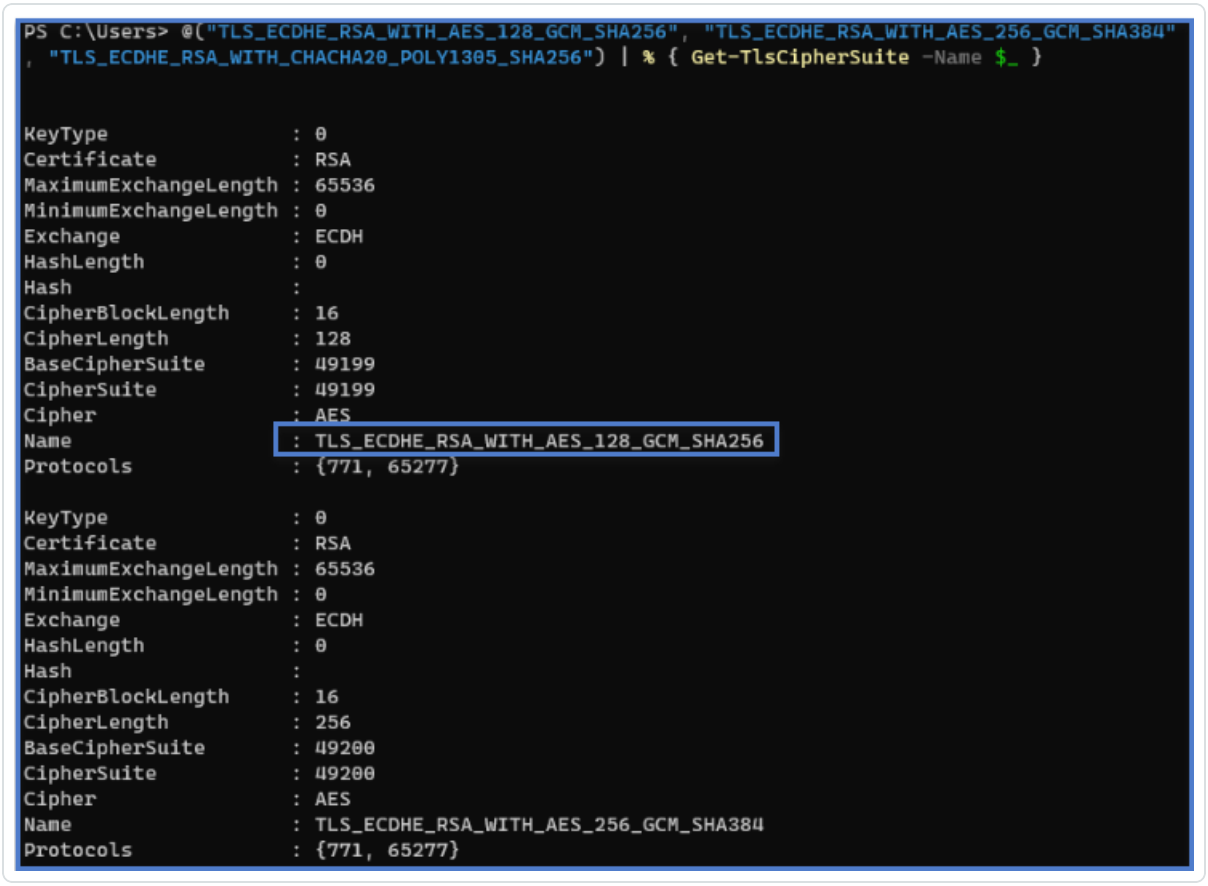
另請確認您的 Windows 設定與指定加密套件相符，以便與轉送功能相容。

### 如要檢查加密套件：

1. 在 PowerShell 中執行下列命令：

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. 檢查輸出：TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256。




3. 空白輸出表示未啟用轉送 TLS 連線正常運作所需的任何加密套件。啟用至少一個加密套件。

4. 驗證來自轉送伺服器的橢圓曲線密碼學 (Elliptic Curve Cryptography，ECC) 曲線。若使用臨時橢圓曲線迪菲-赫爾曼 (Elliptic Curve Diffie-Hellman Ephemeral，ECDHE) 加密套件，必須進行此驗證。在 PowerShell 中執行下列命令：

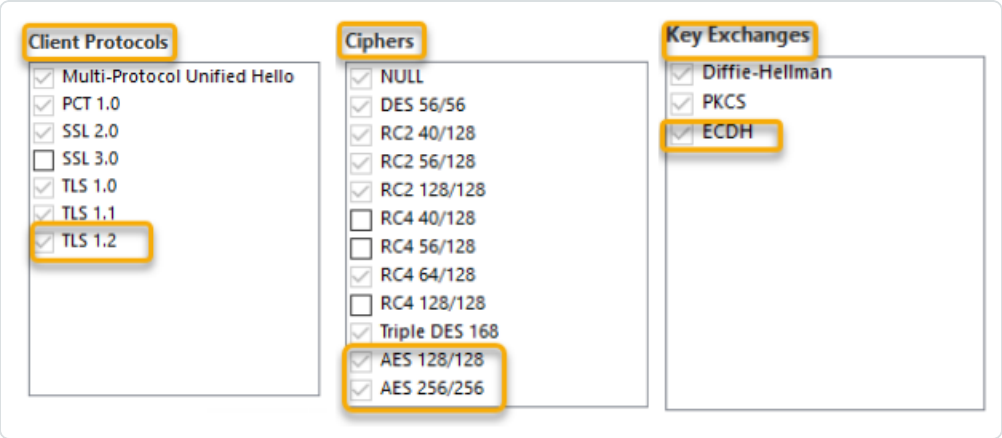
```
Get-TlsEccCurve
```

5. 檢查您是否有曲線 **25519**。若無，請啟用。

```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

### 如要驗證 Windows 密碼編譯設定：

1. 在 IIS Crypto 工具中，檢查您是否已啟用下列選項：
   - 用戶端通訊協定：**TLS 1.2**
   - 密碼：**AES 128/128** 和 **AES 256/256**
   - 金鑰交換：**ECDH**

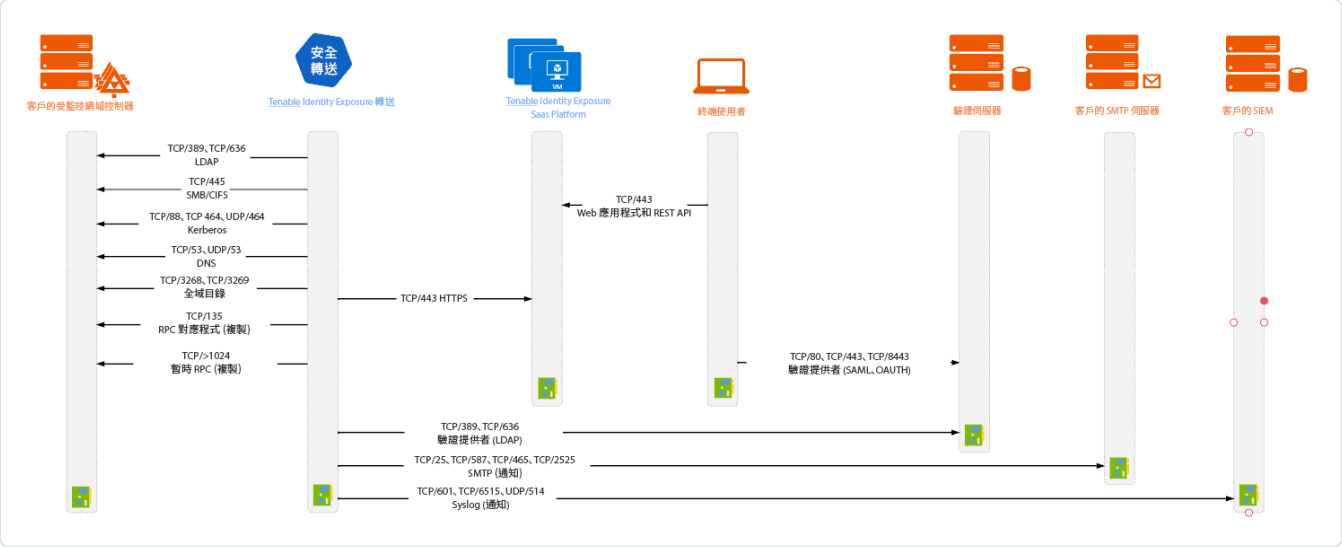



2. 修改密碼編譯設定之後，重新啟動電腦。

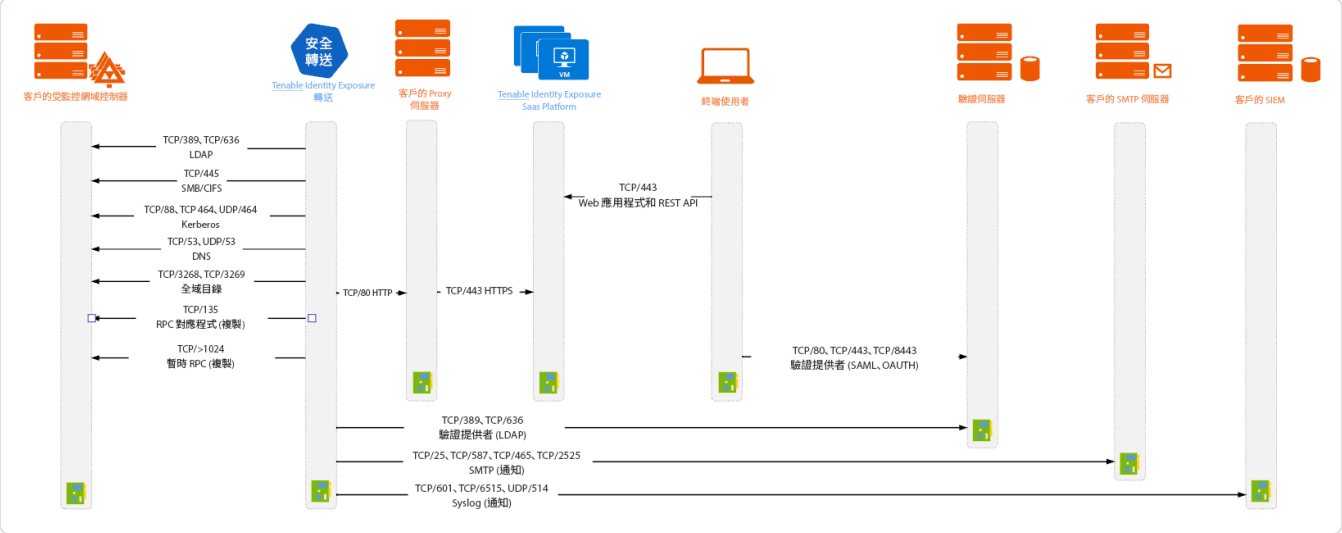
> **注意**：修改 Windows 密碼編譯設定會影響電腦上執行且使用 Windows TLS 程式庫「Schannel」的所有應用程式。因此，請確保您進行的任何調整都不會造成意外副作用。驗證所選設定是否符合組織整體強化目標或合規性授權。

### 所需的連接埠

- 對於**沒有 Proxy 伺服器**的傳統設定，轉送需要下列連接埠：




對於**使用 Proxy 伺服器**的設定，轉送需要下列連接埠：




**注意**：對於內部部署和 SaaS 平台，網路流程的運作方式相同。

## 虛擬機器先決條件

代管安全轉送的虛擬機器 (VM) 需要符合以下要求：

| 客戶規模 | Tenable Identity Exposure 服務 | 需要執行 | 記憶體 (每個執 | vCPU (每個執 | 磁碟拓撲 | 可用磁碟空間 (每個 |
|---|---|---|---|---|---|---|

| | | 個體 | 行個體) | 行個體) | | 執行個體) |
|---|---|---|---|---|---|---|
| 任何大小 | • tenable_Relay<br>• tenable_envoy | 1 | 8 GB RAM | 2 個 vCPU | 與系統分割區分開的記錄分割區 | 30 GB |

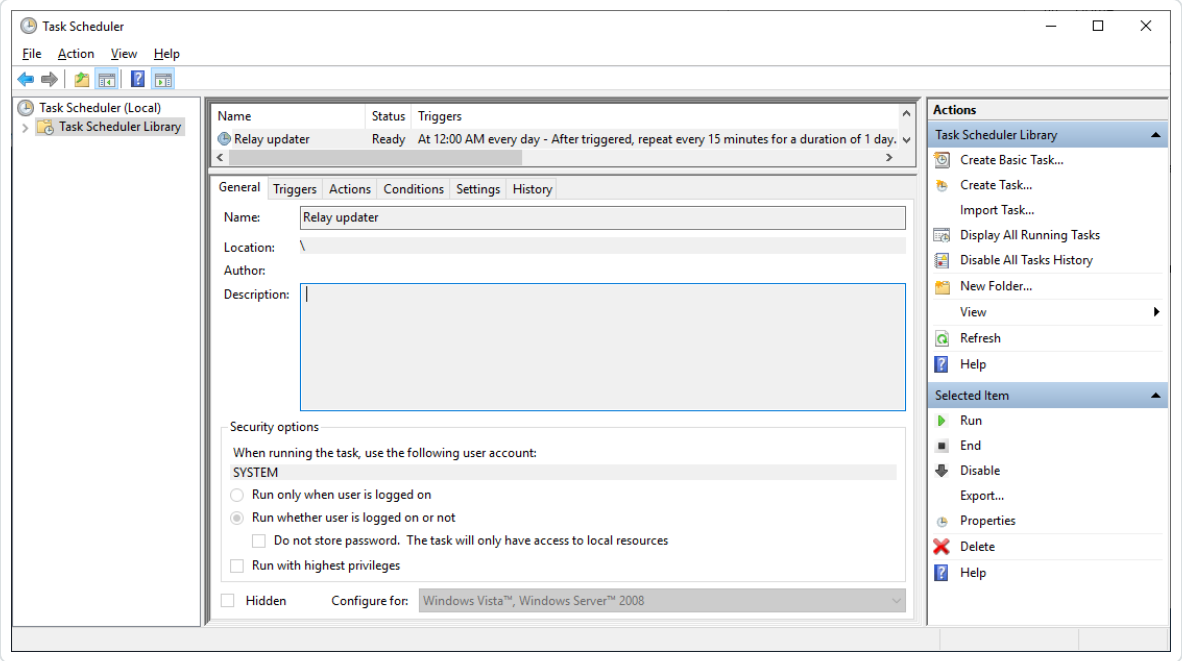
**注意**:如果您在相同的虛擬機器上安裝安全轉送和目錄接聽程式,則必須結合其大小調整要求。請參閱 Resource Sizing。

**提示**:進行初始安裝時,建議讓 VM 保持未加入網域的狀態,以避免繼承可能會干擾安裝處理程序的現有 GPO 原則。安裝完成後,即可將 VM 加入網域。

VM 還必須具備:

- HTTP/HTTPS 流量:移除、停用、繞過或允許將 HTTP/HTTPS 流量導向安全轉送機器的任何用戶端。此動作會封鎖安全轉送安裝,並停止或減緩進入 Tenable 平台的流量。
- Windows Server 2016 以上的作業系統 (不含 Linux)
- 至少針對 `cloud.tenable.com` 和 `*.tenable.ad` 已解析的面向網際網路的 DNS 查詢和網際網路存取 (TLS 1.2)。
- 本機管理員權限
- EDR、防毒和 GPO 設定:
  - VM 上剩餘的 CPU 充足,例如,Windows Defender 即時保護功能會佔用大量 CPU 並可能使電腦飽和。
  - 自動更新:
    - 允許對 `*.tenable.ad` 進行呼叫,以便自動更新功能可下載轉送可執行檔。
    - 檢查並確認沒有封鎖自動更新功能的群組原則物件 (GPO)。

- 不刪除或變更「轉送更新程式」排程工作：




## 獲允許的檔案和處理程序

為使轉送順利運作，請允許第三方安全工具的特定檔案和處理程序，例如防毒和/或 EDR (端點偵測及回應) 和 XDR (延伸偵測及回應)。

> 注意：根據您的轉送安裝磁碟機調整 C:\ 路徑。

| Windows |
| --- |
| 檔案 |
| C:\Tenable* |
| C:\tools* |
| C:\ProgramData\Tenable* |
| 處理程序 |
| nssm.exe --> 路徑：C:\tools\nssm.exe |
| Tenable.Relay.exe --> 路徑：C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe |

| |
|---|
| envoy.exe --> 路徑 : C:\Tenable\Tenable.ad\SecureRelay\envoy.exe |
| updater.exe --> 路徑 : C:\Tenable\Tenable.ad\updater.exe |
| powershell.exe --> 路徑 : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (可能因作業系統版本而有所不同) |
| 排程工作 |
| C:\Windows\System32\Tasks\Relay updater |
| C:\Windows\System32\Tasks\Manual Renew Apikey |
| C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay |
| C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay |
| 登錄機碼 |
| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad 安全轉送 |

## Tenable Identity Exposure 的安全轉送

自 3.59 版開始，**安全轉送**元件將接管 Tenable Identity Exposure 平台中的指定工作：

- 您可以藉此設定網域，從該網域將資料轉送至收集 AD 物件的目錄接聽程式 (DL) 元件。
- 透過自動更新促成大型基礎架構的設定和維護：不再需要必須同時升級的多個 DL。
- 在單一 DL 和多種端點 (例如網域控制器、SMTP 或 SYSLOG 伺服器或用於產品內驗證的 LDAP 伺服器) 之間充當橋接器。
- 連結至一個或數個網域。DL 可管理無限制數量的轉送。
- 需要在 Tenable Identity Exposure 主控台中進行設定，例如命名和對應 (網域、SMTP、SYSLOG、LDAP 驗證)。

**事前準備**

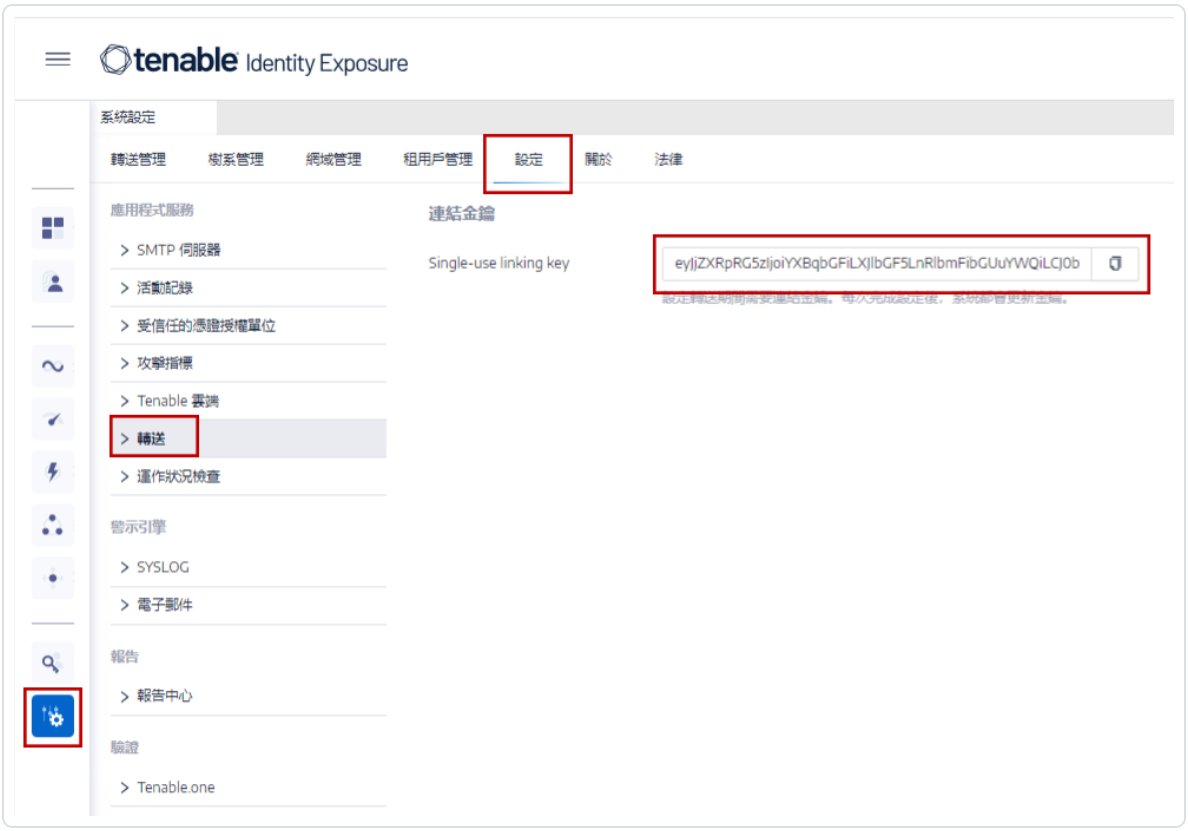
遵照下列準則安裝或升級至具有安全轉送功能的 Tenable Identity Exposure 3.59 版本：

1. 檢閱 安全轉送要求。

2. **網路要求**:
    - 在先前和目前版本中, DL 使用 AMQP(S) 通訊協定直接與 SEN 進行通訊。
    - 在 3.59 版本中, 取代多個 DL 的轉送會透過 HTTPS 與唯一剩餘的 DL 通訊。
    - Envoy 是反向 Proxy。
3. **連結金鑰**:安裝安全轉送功能需要使用包含您的網路位址和身分驗證權杖的一次性連結金鑰。每次成功安裝安全轉送後, Tenable Identity Exposure 都會重新產生新金鑰。

    如要擷取連結金鑰:

    1. 在 Tenable Identity Exposure 主控台中, 按一下左側功能表列上的「**系統**」, 然後選取「**設定**」索引標籤 >「**轉送**」。




    2. 按一下 ⧉ 以複製連結金鑰。

4. **角色權限**：您必須是具有角色型權限的使用者才能設定轉送。所需權限如下：

   - **資料實體**：實體轉送
   - **介面實體**：
     - 管理 > 系統 > 設定 > 應用程式服務 > 轉送
     - 管理 > 系統 > 轉送管理

   詳情請參閱設定角色的權限。

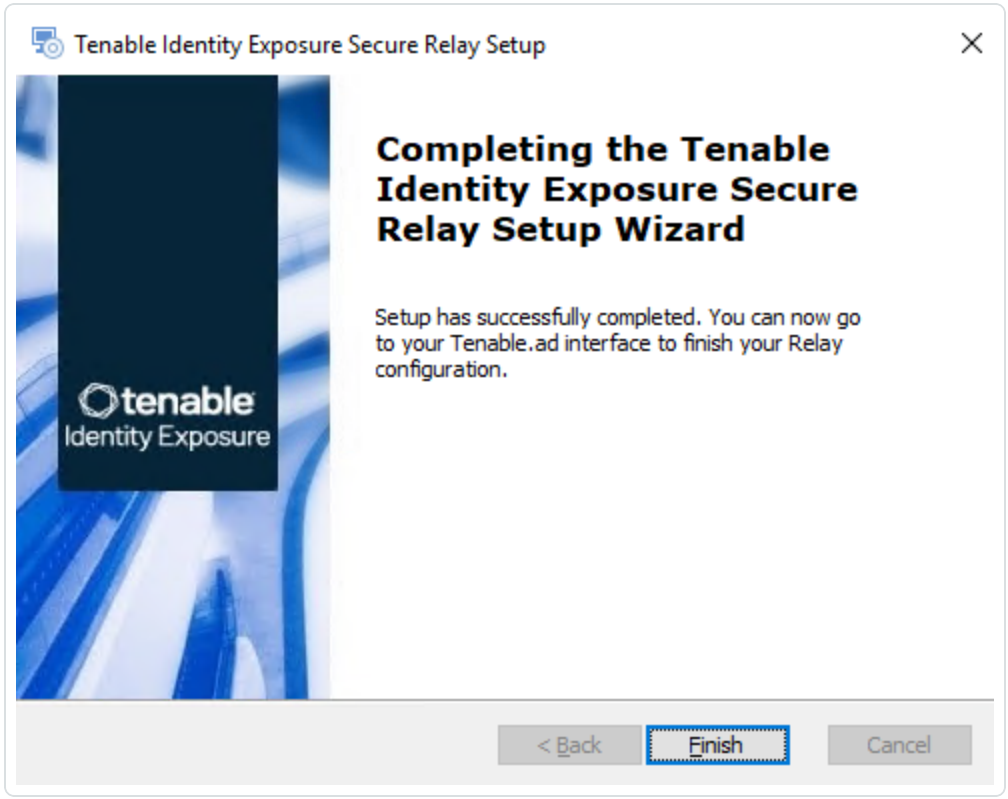
### 安裝程序

**所需使用者角色**：本機電腦上的管理員

如要安裝安全轉送：

1. 從 Tenable 的下載網站下載安全轉送的可執行程式。
2. 按兩下 `tenable.ad_SecureRelay_v3.xx.x` 檔案以啟動安裝精靈。

   「**歡迎**」畫面會隨即顯示。



3. 按一下「**下一步**」。

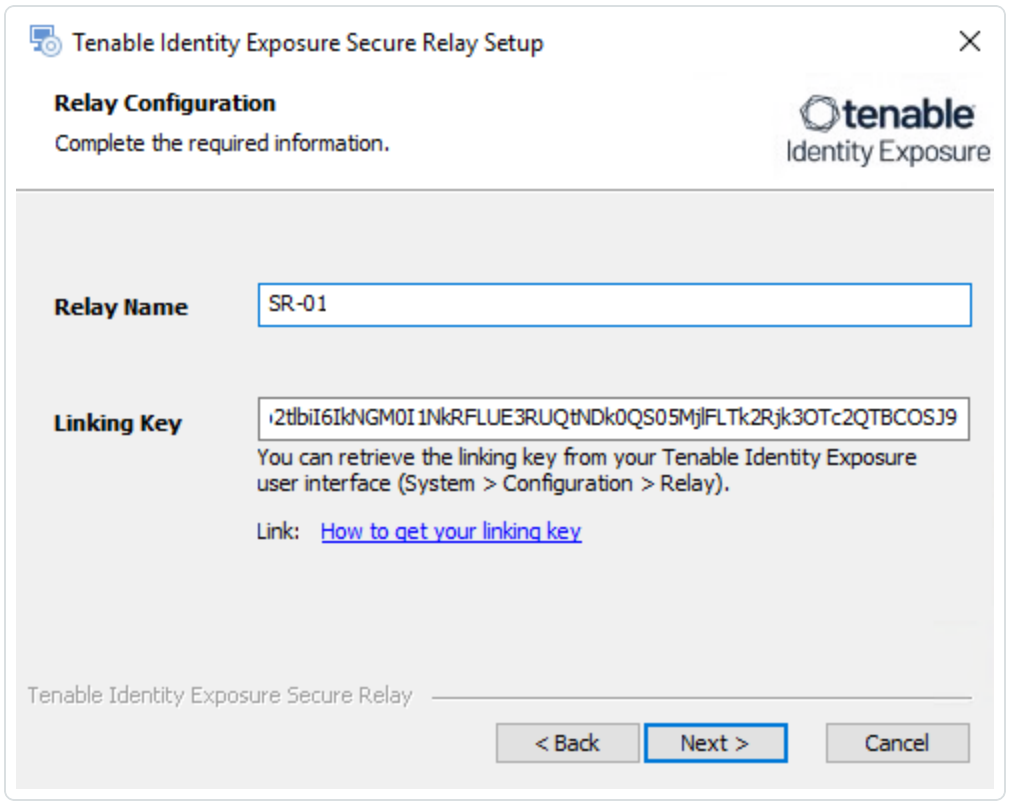
   「**自訂設定**」視窗會隨即顯示。




4. 按一下「**瀏覽**」, 選取您為安全轉送保留的磁碟分割區 (與系統分割區分開)。

5. 按一下「**下一步**」。

   「**轉送設定**」視窗會隨即顯示。




6. 提供以下資訊：

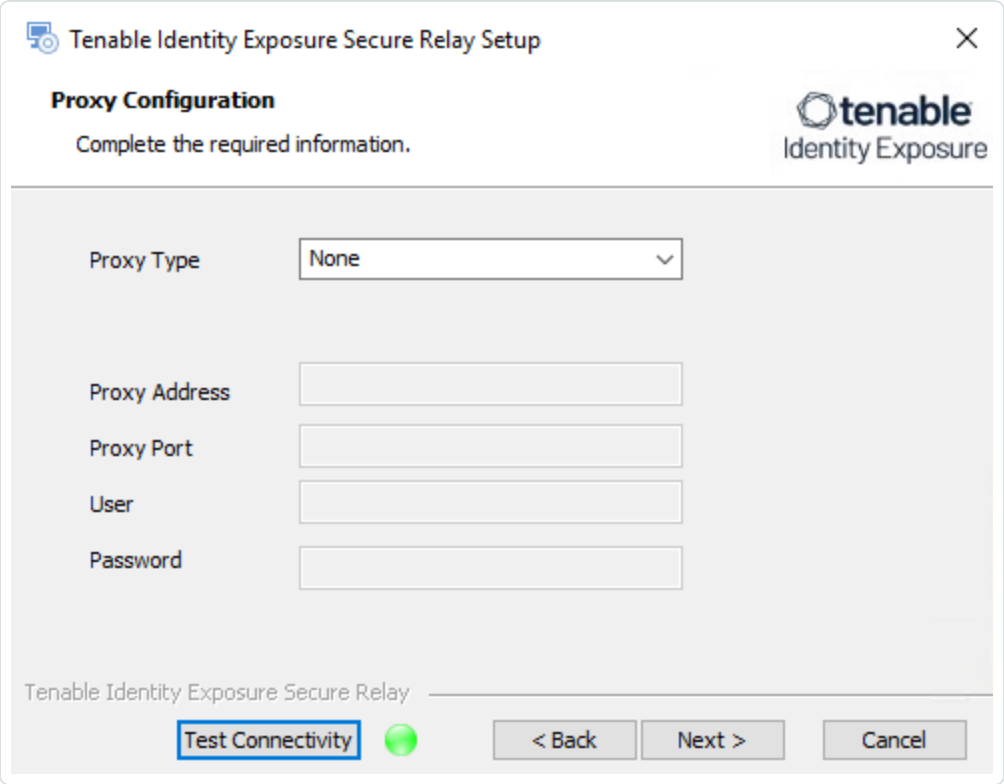
   a. 在「**轉送名稱**」方塊中輸入安全轉送的名稱。

   b. 在「**連結金鑰**」方塊中貼上您從 Tenable Identity Exposure 入口網站擷取的連結金鑰。

   c. 如果您選擇使用 Proxy 伺服器，請選取「**使用 HTTP Proxy 進行轉送呼叫**」選項，並提供 Proxy 位址和連接埠號碼。

7. 按一下「**下一步**」。

   「Proxy 設定」視窗會隨即顯示：




8. 請選取以下選項之一：

   a. **無**：不使用 Proxy 伺服器。

   b. **未經驗證**：輸入 Proxy 伺服器的位址和連接埠。

   c. **基本驗證**：除了位址和連接埠，也請輸入 Proxy 伺服器的使用者名稱和密碼。

   **注意**：若要設定使用「未經驗證」或「基本驗證」的 Proxy，轉送僅支援 IPv4 位址 (例如 `192.168.0.1`) 或不含 `http://` 或 `https://` 的 Proxy URI (例如 `myproxy.mycompany. com`)。轉送不支援 IPv6 位址 (例如 `2001:0db8:85a3:0000:0000:8a2e:0370:7334`)。

9. 按一下**測試連線能力**。可能會發生下列情況：

   - **綠燈**：連線成功。
   - **無效的連結金鑰**：從 Tenable Identity Exposure 入口網站擷取連結金鑰。
   - **無效的轉送名稱**：此方塊不能留空。提供轉送的名稱。
   - **連線失敗**：檢查您的網際網路存取。

10. 按一下「**下一步**」。

「**準備安裝**」視窗會隨即顯示。

11. 按一下「**安裝**」。
12. 安裝完成後，按一下「**完成**」。

## 安裝後檢查

安全轉送安裝完成後，請檢查下列項目：

### Tenable Identity Exposure 中已安裝轉送的清單

如要檢閱已安裝的轉送清單：

- 在 Tenable Identity Exposure 中，按一下左側功能表列上的「**系統**」，然後選取「**轉送管理**」索引標籤。

  此窗格會顯示安全轉送及其連結網域的清單。

### 服務

成功安裝後，系統將執行下列服務：

- `Tenable_Relay`
- `tenable_envoy`

> **注意**：您可以在 Tenable Identity Exposure 中的「**系統**」>「**法律**」>「**Envoy 授權**」中找到 Envoy 授權。

### 環境變數

安裝過程中還新增了 6 個與安全轉送相關的環境變數，其名稱皆以「ALSID_CASSIOPEIA_」開頭。如果您選擇使用 Proxy 伺服器，系統還會額外建立 2 個與 Proxy IP 和連接埠相關的變數。

### 用於疑難排解的記錄

您可以在下列位置找到記錄：

- **安裝記錄**：C:\Users\<your user> \AppData\Local\Temp
- **轉送記錄**：在安裝時指定的資料夾中代管安全轉送的 VM 上。

## 轉送設定

- 設定轉送

### 自動更新

在您安裝安全轉送之後，Tenable Identity Exposure 會定期檢查新版本。此處理程序完全自動化執行，需要對您的網域具有 HTTPS 存取權 (TCP/443)。網路托盤中有一個圖示會指示 Tenable Identity Exposure 將於何時更新安全轉送。此過程完成後，Tenable Identity Exposure 服務將重新啟動並恢復資料收集。

### 解除安裝

如要解除安裝安全轉送：

1. 在 Windows 中，前往**「設定」**>**「應用程式與功能」**>**「Tenable Identity Exposure 安全轉送」**。
2. 按一下**「解除安裝」**。

   解除安裝完成後，Tenable Identity Exposure 安全轉送服務和環境變數不會再出現在您的系統中。
3. 在 Tenable Identity Exposure 中，按一下左側功能表列上的**「系統」**，然後選取**「轉送管理」**索引標籤。
4. 選取您剛剛解除安裝的轉送，然後按一下 即可從可用的轉送清單中刪除它。

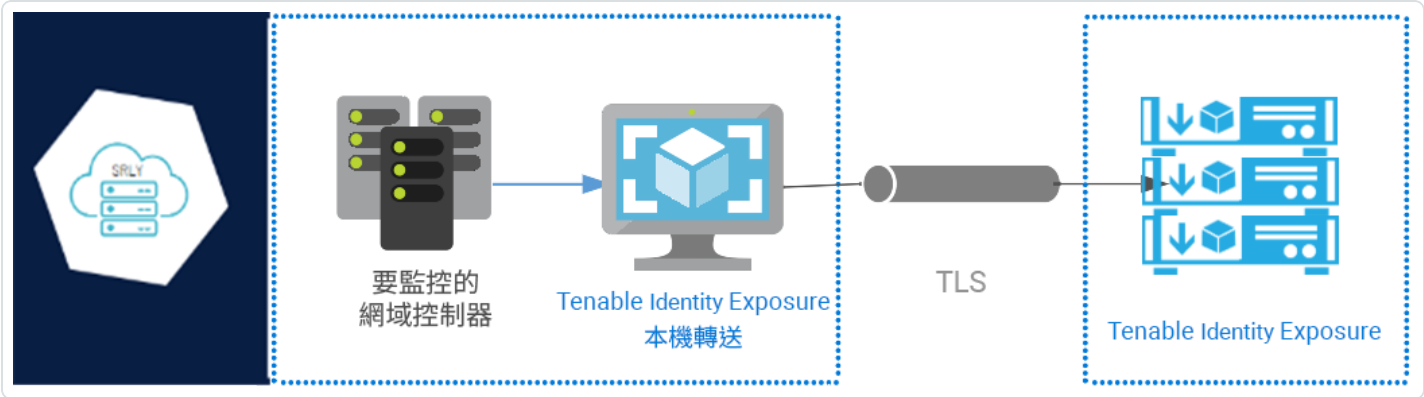
## 另請參閱

- 解決安全轉送安裝的問題

## 安全轉送要求

**安全轉送**是一種使用傳輸層安全性 (TLS) 而不是 VPN 將 Active Directory 資料從您的網路傳輸到 Tenable Identity Exposure 的傳輸模式，如此圖所示。如果您的網路需要 Proxy 伺服器才能連線至網際網路，則安全轉送功能現在也支援需要或不需要驗證的 HTTP Proxy。

Tenable Identity Exposure 可支援多種安全轉送，您可以根據需要將其對應至網域。




### TLS 要求

如要使用 TLS 1.2，自 2024 年 1 月 24 日起，您的轉送伺服器必須至少支援下列其中一項加密套件：

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

另請確認您的 Windows 設定與指定加密套件相符，以便與轉送功能相容。

### 如要檢查加密套件：

1. 在 PowerShell 中執行下列命令：

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_
RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. 檢查輸出：TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256。

```
PS C:\Users> @("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
, "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }


KeyType              : 0
Certificate          : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange             : ECDH
HashLength           : 0
Hash                 :
CipherBlockLength    : 16
CipherLength         : 128
BaseCipherSuite      : 49199
CipherSuite          : 49199
Cipher               : AES
Name                 : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Protocols            : {771, 65277}

KeyType              : 0
Certificate          : RSA
MaximumExchangeLength : 65536
MinimumExchangeLength : 0
Exchange             : ECDH
HashLength           : 0
Hash                 :
CipherBlockLength    : 16
CipherLength         : 256
BaseCipherSuite      : 49200
CipherSuite          : 49200
Cipher               : AES
Name                 : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Protocols            : {771, 65277}
```

3. 空白輸出表示未啟用轉送 TLS 連線正常運作所需的任何加密套件。啟用至少一個加密套件。

4. 驗證來自轉送伺服器的橢圓曲線密碼學 (Elliptic Curve Cryptography, ECC) 曲線。若使用臨時橢圓曲線迪菲-赫爾曼 (Elliptic Curve Diffie-Hellman Ephemeral, ECDHE) 加密套件，必須進行此驗證。在 PowerShell 中執行下列命令：

```
Get-TlsEccCurve
```

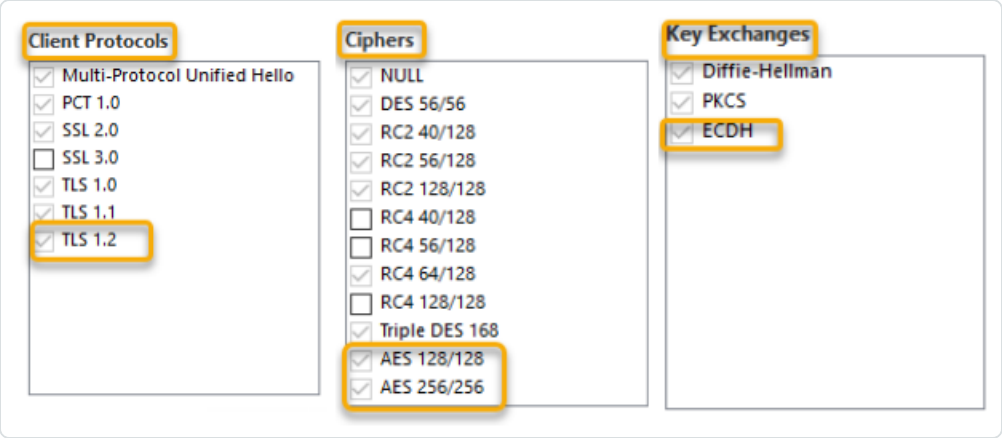
5. 檢查您是否有曲線 **25519**。若無，請啟用。

```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

**如要驗證 Windows 密碼編譯設定：**

1. 在 IIS Crypto 工具中，檢查您是否已啟用下列選項：

   - 用戶端通訊協定：**TLS 1.2**
   - 密碼：**AES 128/128** 和 **AES 256/256**
   - 金鑰交換：**ECDH**

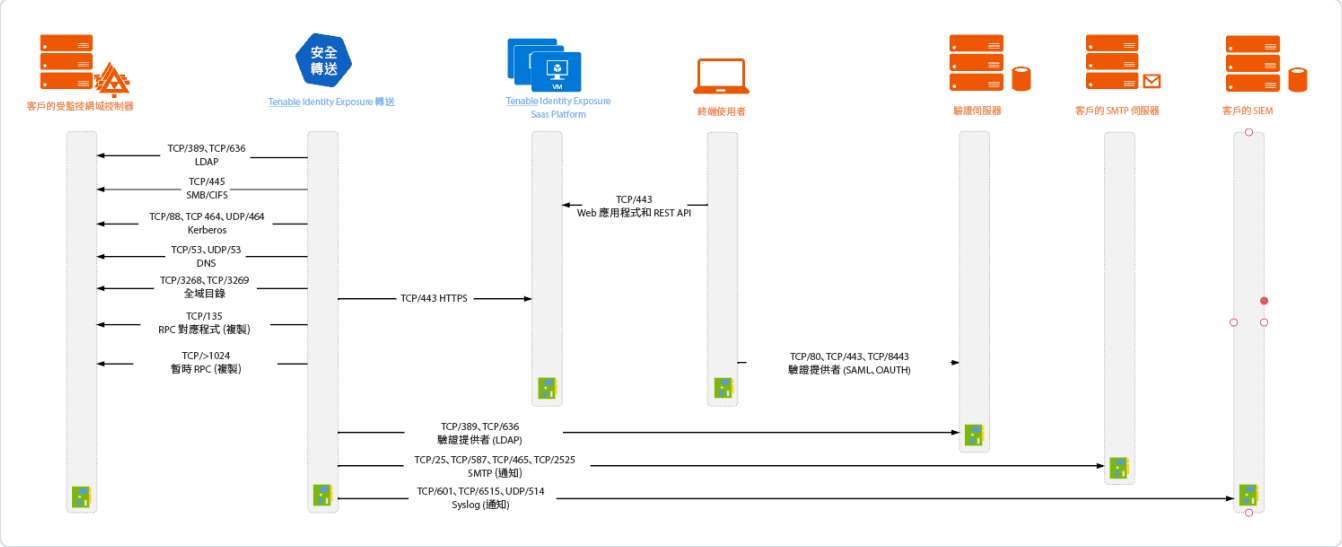



2. 修改密碼編譯設定之後，重新啟動電腦。

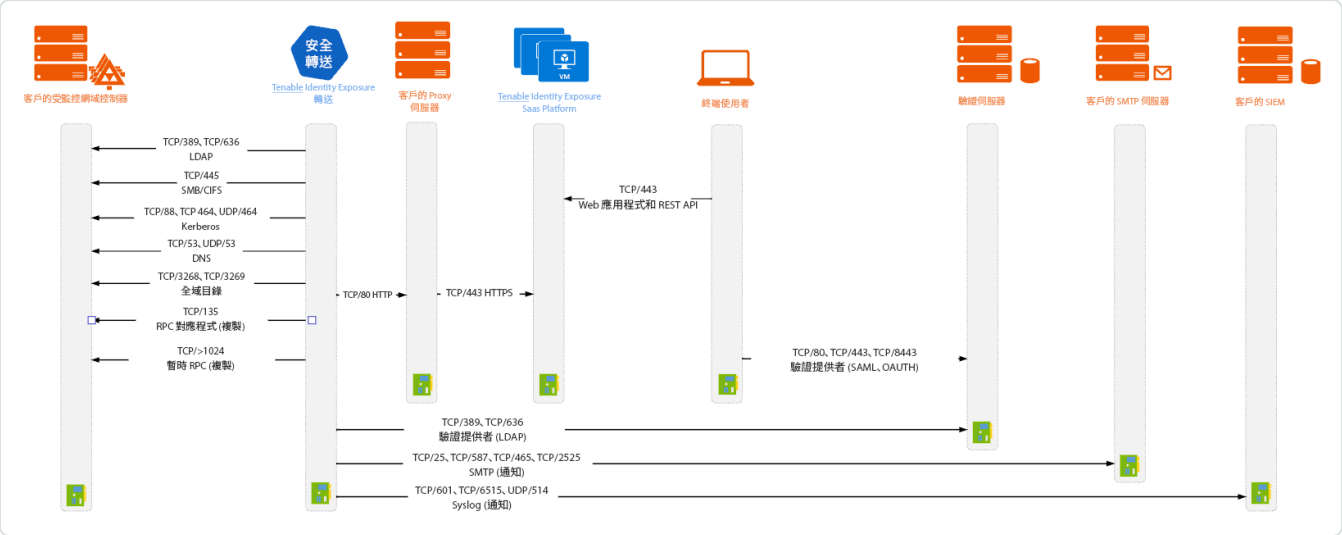
> **注意**：修改 Windows 密碼編譯設定會影響電腦上執行且使用 Windows TLS 程式庫「Schannel」的所有應用程式。因此，請確保您進行的任何調整都不會造成意外副作用。驗證所選設定是否符合組織整體強化目標或合規性授權。

## 所需的連接埠

- 對於**沒有 Proxy 伺服器**的傳統設定，轉送需要下列連接埠：




對於**使用 Proxy 伺服器**的設定，轉送需要下列連接埠：




**注意**：對於內部部署和 SaaS 平台，網路流程的運作方式相同。

## 虛擬機器先決條件

代管安全轉送的虛擬機器 (VM) 需要符合以下要求：

| 客戶規模 | Tenable Identity Exposure 服務 | 需要執行 | 記憶體 (每個執 | vCPU (每個執 | 磁碟拓撲 | 可用磁碟空間 (每個 |
|---|---|---|---|---|---|---|

| | | 個體 | 行個體) | 行個體) | | 執行個體) |
|---|---|---|---|---|---|---|
| 任何大小 | • tenable_Relay<br>• tenable_envoy | 1 | 8 GB RAM | 2 個 vCPU | 與系統分割區分開的記錄分割區 | 30 GB |

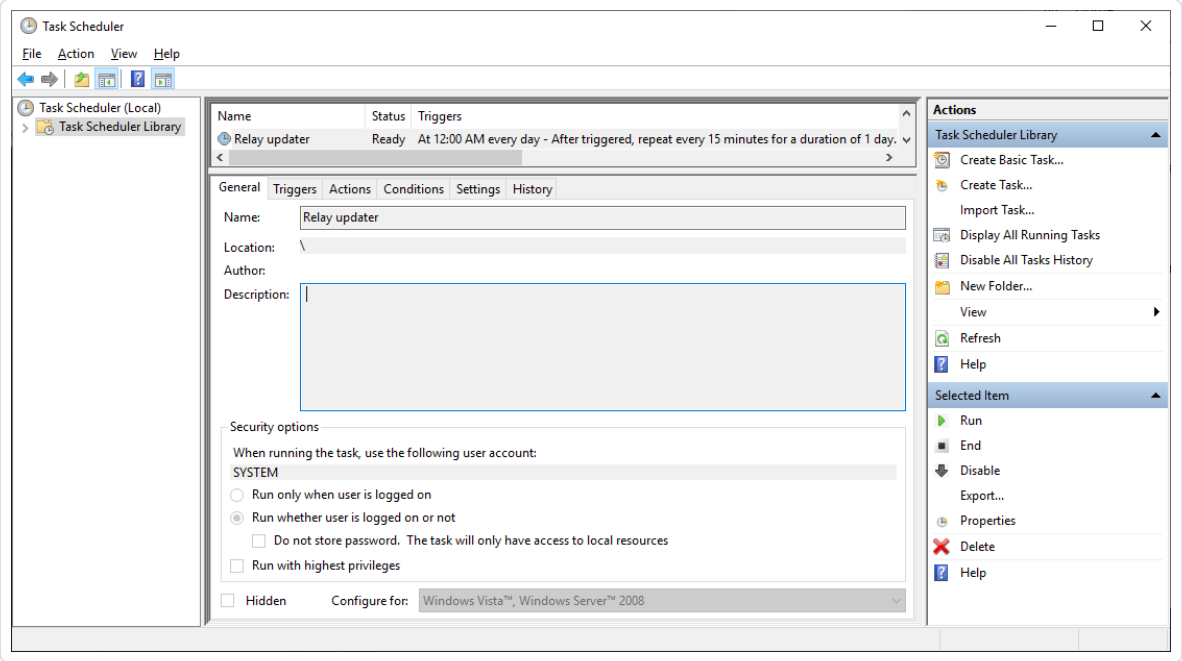
**注意**:如果您在相同的虛擬機器上安裝安全轉送和目錄接聽程式,則必須結合其大小調整要求。請參閱 Resource Sizing。

**提示**:進行初始安裝時,建議讓 VM 保持未加入網域的狀態,以避免繼承可能會干擾安裝處理程序的現有 GPO 原則。安裝完成後,即可將 VM 加入網域。

VM 還必須具備:

- HTTP/HTTPS 流量:移除、停用、繞過或允許將 HTTP/HTTPS 流量導向安全轉送機器的任何用戶端。此動作會封鎖安全轉送安裝,並停止或減緩進入 Tenable 平台的流量。
- Windows Server 2016 以上的作業系統 (不含 Linux)
- 至少針對 `cloud.tenable.com` 和 `*.tenable.ad` 已解析的面向網際網路的 DNS 查詢和網際網路存取 (TLS 1.2)。
- 本機管理員權限
- EDR、防毒和 GPO 設定:
  - VM 上剩餘的 CPU 充足,例如,Windows Defender 即時保護功能會佔用大量 CPU 並可能使電腦飽和。
  - 自動更新:
    - 允許對 `*.tenable.ad` 進行呼叫,以便自動更新功能可下載轉送可執行檔。
    - 檢查並確認沒有封鎖自動更新功能的群組原則物件 (GPO)。

- 不刪除或變更「轉送更新程式」排程工作：




## 獲允許的檔案和處理程序

為使轉送順利運作，請允許第三方安全工具的特定檔案和處理程序，例如防毒和/或 EDR (端點偵測及回應) 和 XDR (延伸偵測及回應)。

> 注意：根據您的轉送安裝磁碟機調整 C:\ 路徑。

| Windows |
| --- |
| 檔案 |
| C:\Tenable* |
| C:\tools* |
| C:\ProgramData\Tenable* |
| 處理程序 |
| nssm.exe --> 路徑：C:\tools\nssm.exe |
| Tenable.Relay.exe --> 路徑：C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe |

| |
|---|
| envoy.exe --> 路徑 : C:\Tenable\Tenable.ad\SecureRelay\envoy.exe |
| updater.exe --> 路徑 : C:\Tenable\Tenable.ad\updater.exe |
| powershell.exe --> 路徑 : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe (可能因作業系統版本而有所不同) |
| 排程工作 |
| C:\Windows\System32\Tasks\Relay updater |
| C:\Windows\System32\Tasks\Manual Renew Apikey |
| C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay |
| C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay |
| 登錄機碼 |
| Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad 安全轉送 |

## 設定轉送

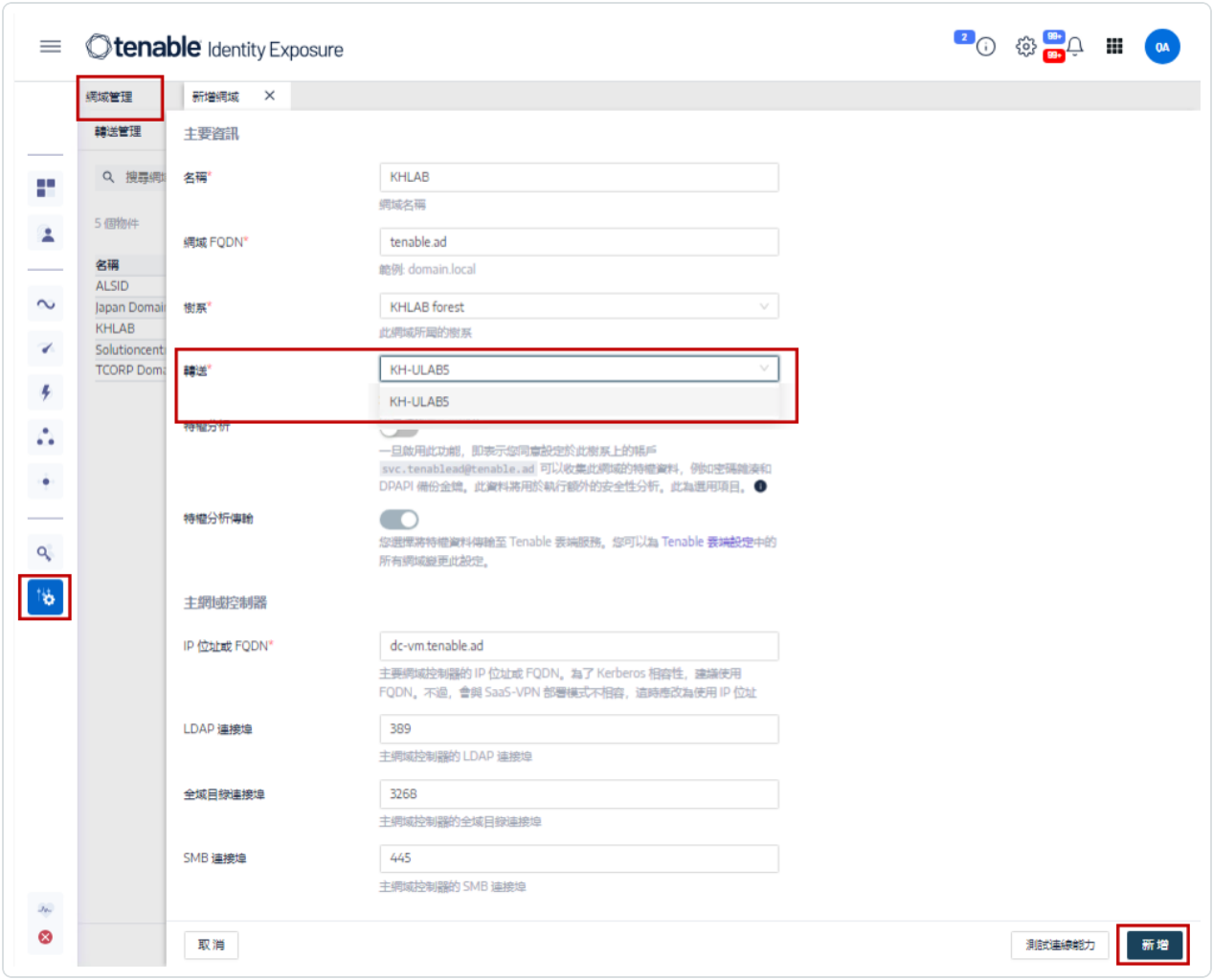
在安裝和安裝後檢查之後，將 Tenable Identity Exposure 中的轉送設定為將其連結至網域並設定警示。

- 網域對應：將多個 DL 應用程式設定或網路環境變數取代為必要的網域設定 (編輯數量可能有所不同)。

  **如要將網域對應至安全轉送：**

  1. 在 Tenable Identity Exposure 中，按一下左側功能表列上的**「系統」**，然後選取**「網域管理」**索引標籤。
  2. 在網域清單中選取要連結的網域，然後按一下行尾的 。

     **「編輯網域」**窗格會隨即開啟。
  3. 在**「轉送」**方塊中按一下箭頭，顯示已安裝轉送的下拉式清單，然後選取要連結至網域的轉送。




按一下「**編輯**」。

系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新網域。SYSVOL 和 LDAP 將執行同步以包含此項修改。追蹤流程開始接收新事件。

- 警示對應：
  - SMTP 設定：對 SMTP 伺服器設定進行必要的編輯。
  - Syslog 警示：設定 Syslog 警示 (編輯數量可能不定)。
- LDAP 對應：建置使用 LDAP 驗證。

## 安裝安全轉送 (CLI)

以下程序使用命令列安裝安全轉送。開始之前，請檢查您是否符合 Tenable Identity Exposure 的安全轉送 中所述的必要先決條件且具備**必要的連結金鑰**。

如要使用 CLI 安裝安全轉送：

1. 從 Tenable Identity Exposure 下載入口網站將安裝程式下載到您的 VM。
2. 在 PowerShell 中輸入下列命令：

安全轉送安裝

```
<PATH>\tenable.ad_SecureRelay_v3.43.0.exe /qn OPTIONS
```

使用下列選項：

- APPDIR=<path> (必要)：轉送安裝資料夾的路徑。請選擇非系統分割的選項，因為轉送會建立大型記錄檔。
- EDIT_LINKINGKEY=<string> (必要)：您從 Tenable Identity Exposure 執行個體擷取的連結金鑰。
- EDIT_INSTANCENAME=<string> (選用)：轉送的名稱。如果不設定名稱，Tenable Identity Exposure 會使用電腦的名稱。在 Tenable Identity Exposure中可以修改名稱。此名稱必須為唯一不重複。
- PROXY_ADDRESS=<IP or DNS> (選用)：如果網路需要 Proxy 伺服器才能連線 Tenable 網域時所使用的 Proxy 位址。如有提供 Proxy 位址，則必須同時提供 Proxy 通訊埠。
- PROXY_PORT=<number> (選用)：如果網路需要 Proxy 伺服器才能連線 Tenable 網域時所使用的 Proxy 通訊埠。如有提供 Proxy 位址，則必須同時提供 Proxy 通訊埠。
- /L* <folder> (選用)：安裝建立的檔案所在的路徑，該檔案僅包含轉送安裝記錄。

使用選項的安全轉送安裝範例

```
.\tenable.ad_SecureRelay_v3.43.0.exe /qn APPDIR=D:\Tenable\Tenable.ad\ EDIT_
LINKINGKEY=eyJjZXRpRG5zIjoicWExc2Fhcy1yZWxheS50ZW5hYmxlLmFkIiwidG9rZW4iOiI4NkYwMzMzQS01Mk
I5LTQ4QTctQjMxMS05RDdGRkM5QjkzNTUifQ== EDIT_INSTANCENAME="US Network Area" /L*
C:\Users\Administrator\Desktop\log.txt
```

**注意**：按下 Enter 鍵後，安裝會開始在背景運作。立即傳回 CLI 提示並不表示安裝已完成。若有選取 /L* 選項，您可查看記錄檔以確認安裝是否成功完成。

## 範例

以下是指示安裝成功或失敗的記錄項目範例：

安裝成功

```
MSI (s) (D8:EC) [17:39:04:383]: Product: Tenable.ad Secure Relay -- Installation completed
successfully.

MSI (s) (D8:EC) [17:39:04:383]: Windows Installer installed the product. Product Name: Tenable.ad
Secure Relay. Product Version: 3.43.0. Product Language: 1033. Manufacturer: Tenable. Installation
success or error status: 0.

=== Logging stopped: 3/15/2023  17:39:04 ===
```

安裝失敗

```
MSI (s) (74:38) [17:18:35:713]: Product: Tenable.ad Secure Relay -- Installation failed.

MSI (s) (74:38) [17:18:35:713]: Windows Installer installed the product. Product Name: Tenable.ad
Secure Relay. Product Version: 3.43.0. Product Language: 1033. Manufacturer: Tenable. Installation
success or error status: 1603.

=== Logging stopped: 3/15/2023  17:18:35 ===
```

# 安裝安全轉送 (Tenable Agent)

以下程序使用 Tenable Agent 安裝安全轉送。

## 事前準備

- 檢查您是否已下載並安裝 Tenable Agent。

  **注意**：Tenable Agent 安裝程式會要求提供代理程式金鑰。安全轉送功能**不需要**此金鑰。

- 符合必要的先決條件，並準備好安全轉送中所述**必要的連結金鑰**。

如要使用 Nessus 安裝安全轉送：

1. 在託管 Tenable Agent 並作為轉送的電腦上，開啟 Tenable Agent 目錄 (`c:\Program Files\Tenable\Nessus Agent`) 中的管理員命令提示視窗，然後輸入下列命令：

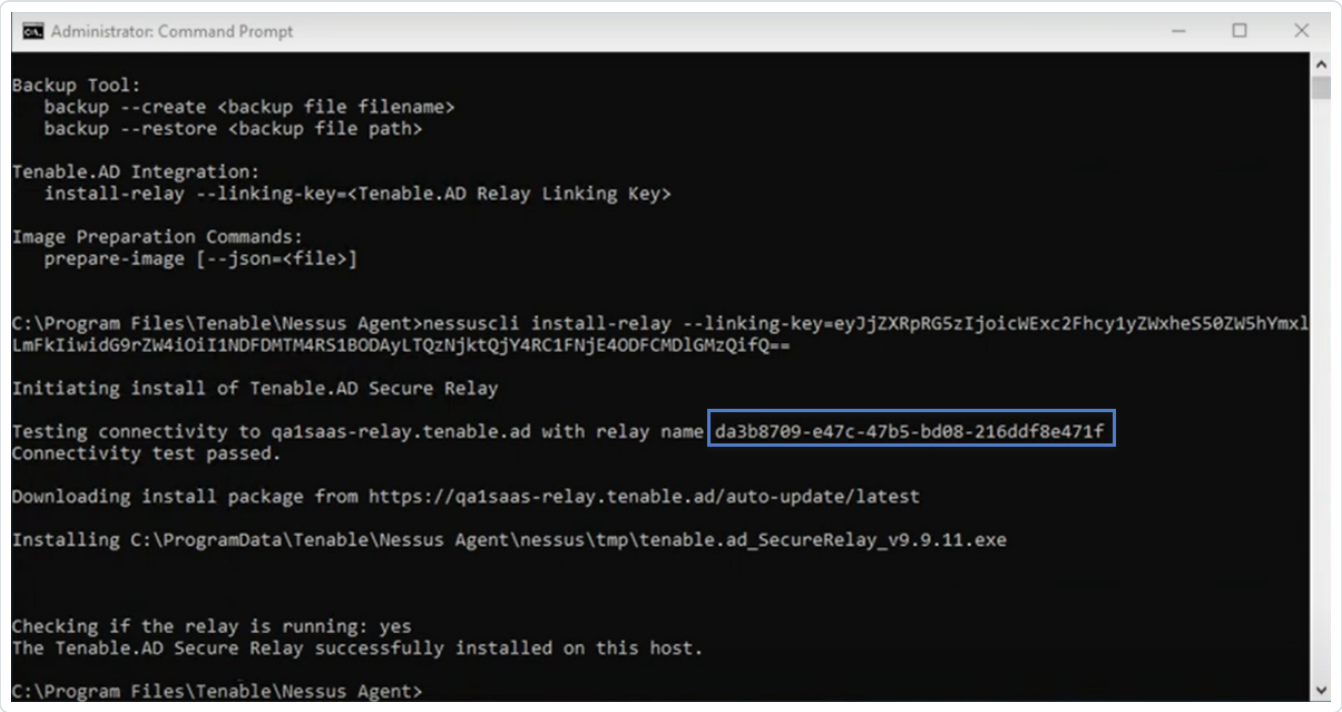
   安全轉送安裝

   ```
   nessuscli install-relay --linking-key=<Relay Linking Key> --proxy-host=<Customer Proxy IP or DNS> --proxy-port=<Customer Proxy Port>
   ```

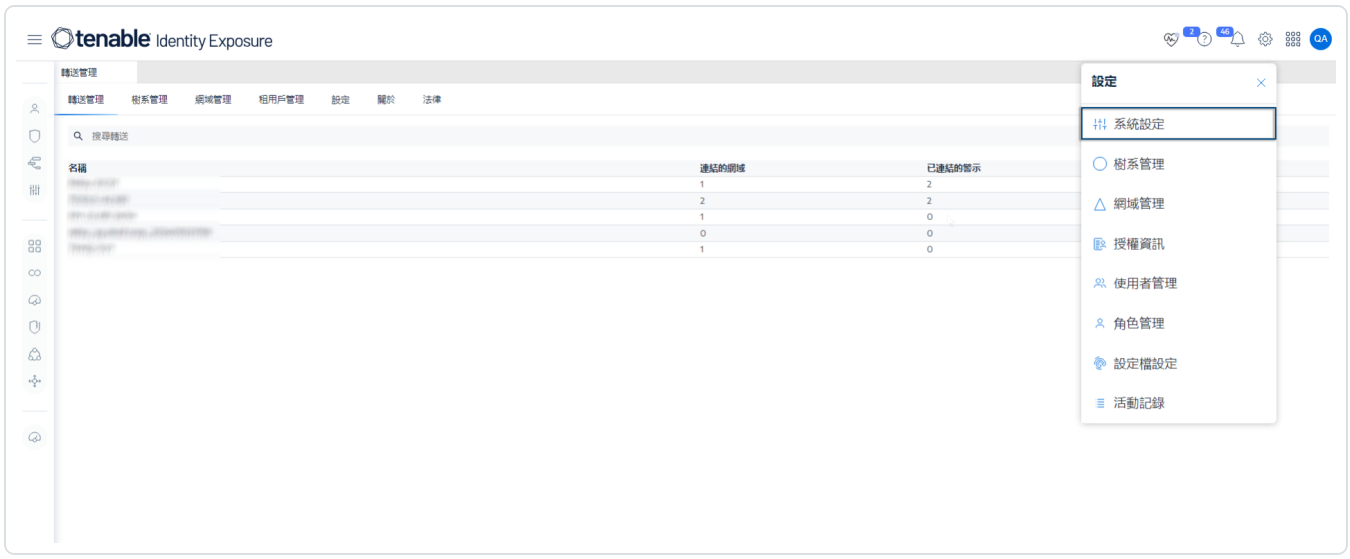
2. 將 <Tenable Identity Exposure Relay Linking Key> 替換為您之前從 Tenable Identity Exposure 執行個體複製的值，如果您使用 Proxy 伺服器，請提供 Proxy 位址和連接埠號碼。

   安裝即會開始。執行連線檢查和安裝處理程序需要幾分鐘的時間。

   安裝成功完成時，系統會顯示一則訊息，提示轉送正在主機上執行。

3. 在 Tenable Identity Exposure 中，按一下**「系統」>「轉送管理」**。轉送清單中會出現新安裝的轉送以及安裝視窗中顯示的識別碼。




# 解決安全轉送安裝的問題

## EDR 或防毒軟體在安裝期間移除設定檔

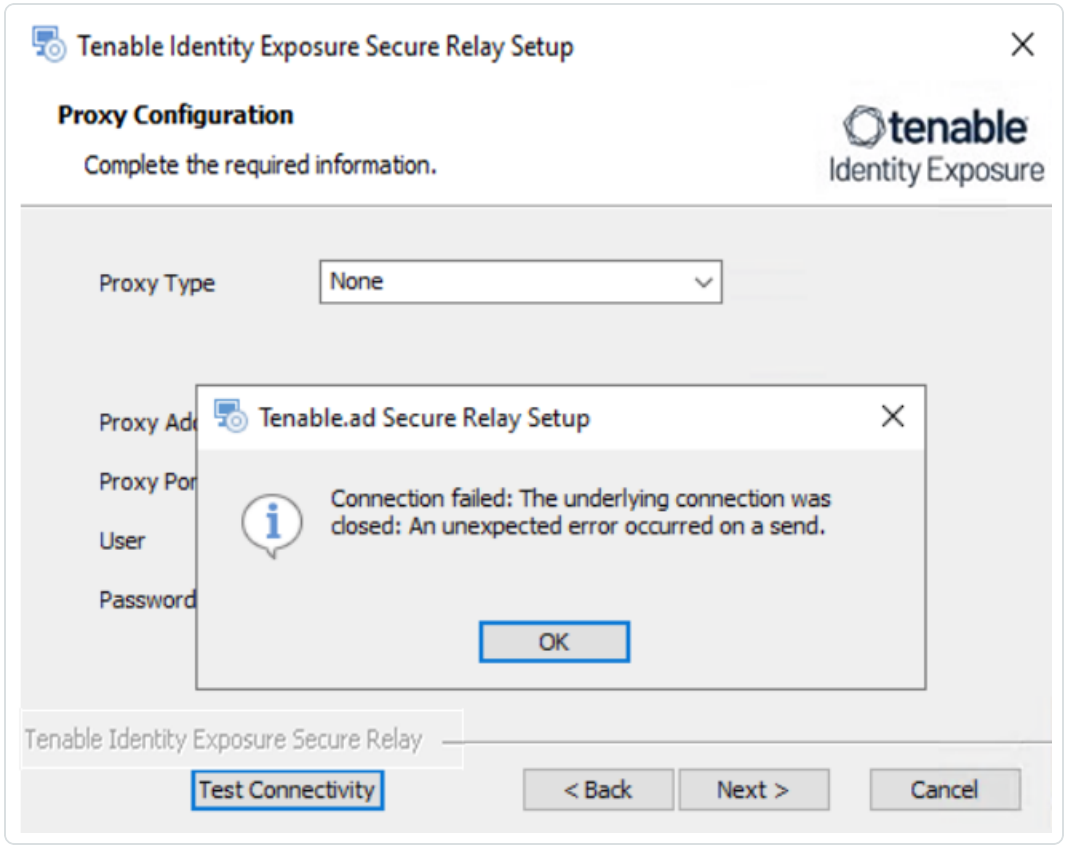
- **原因**：在安裝安全轉送期間，端點偵測與回應 (EDR) 軟體或防毒程式可能會透過自動移除 `envoy.yaml` 設定檔來干擾處理程序。此檔案對於安全轉送正常運作非常重要。如果移除，安裝便會失敗。
- **錯誤訊息**：如果懷疑安裝失敗的原因是 EDR 或防毒軟體移除了 `envoy.yaml` 檔案，您可以檢查 MSI 錯誤記錄來確認。MSI 錯誤記錄是在您系統上的 TEMP 資料夾中產生。尋找下列錯誤訊息：錯誤：缺少 `envoy.yaml` 檔案。

  如果此錯誤出現在您的記錄中，表示 `envoy.yaml` 檔案在安裝處理程序期間遭到移除，很可能是由安全性軟體移除。
- **修復**：若要解決此問題並確保成功安裝，請按照下列步驟操作：

  1. 將安裝資料夾或設定檔列入白名單：
     - 設定您的 EDR 或防毒軟體，避免掃描和移除下列目錄：`[Install_path]\Tenable.ad\SecureRelay\`
     - 或者，如果無法排除整個資料夾，您也可以將 `[Install_path]\Tenable.ad\SecureRelay\envoy.yaml` 檔案列入白名單。
  2. 重新嘗試安裝：新增必要的排除項目後，重新執行安全轉送安裝作業。

### 在獨立伺服器上安裝多個安全轉送和單一安全轉送失敗

- **原因**:在升級期間,安裝程式不會擷取 Ceti 主機 IP 位址的環境變數,而是預設為「127.0.0.1」。
- **錯誤訊息**:因傳輸期間發生意外錯誤而導致連線失敗。



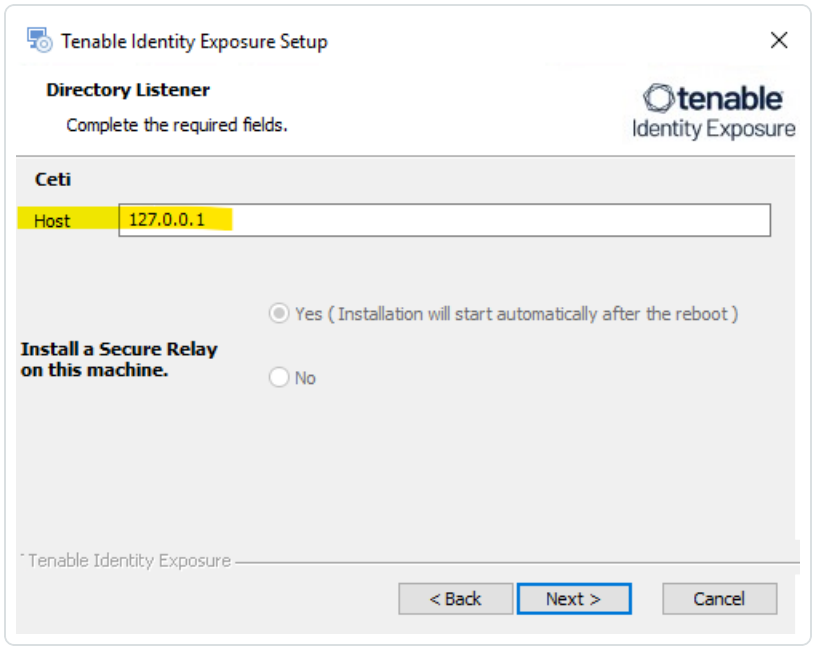

- **修復**:

1. 驗證目錄接聽程式伺服器上的環境變數「TENABLE_CASSIOPEIA_CETI_Service__Broker__Host」。
2. 確保其已**設為安全引擎節點的 IP 位址**。如果變數設為預設的「127.0.0.1」,則會造成安全轉送安裝失敗。
3. 更新環境變數「TENABLE_CASSIOPEIA_CETI_Service__Broker__Host」之後,**重新啟動 Ceti 服務**。

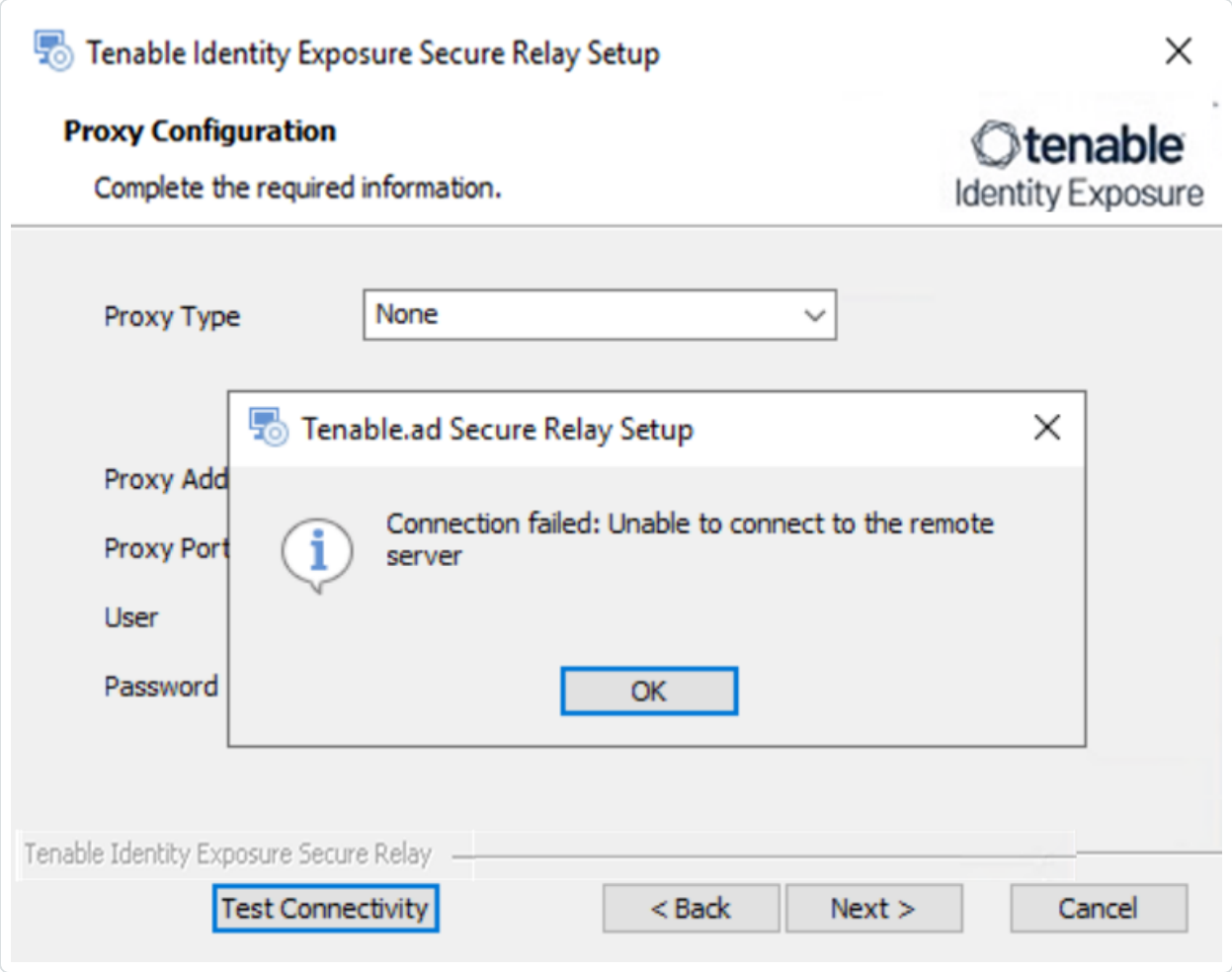
4. **再次開始安全轉送安裝**。否則，它會復原，維持轉送和 Envoy 服務的已安裝狀態，並且封鎖任何後續安裝。

### 無效的 CetiDNS 名稱

- **原因**：升級或安裝安全引擎節點伺服器時，未設定 Ceti 伺服器的 IP 位址。安裝程式預設為「127.0.0.1」：



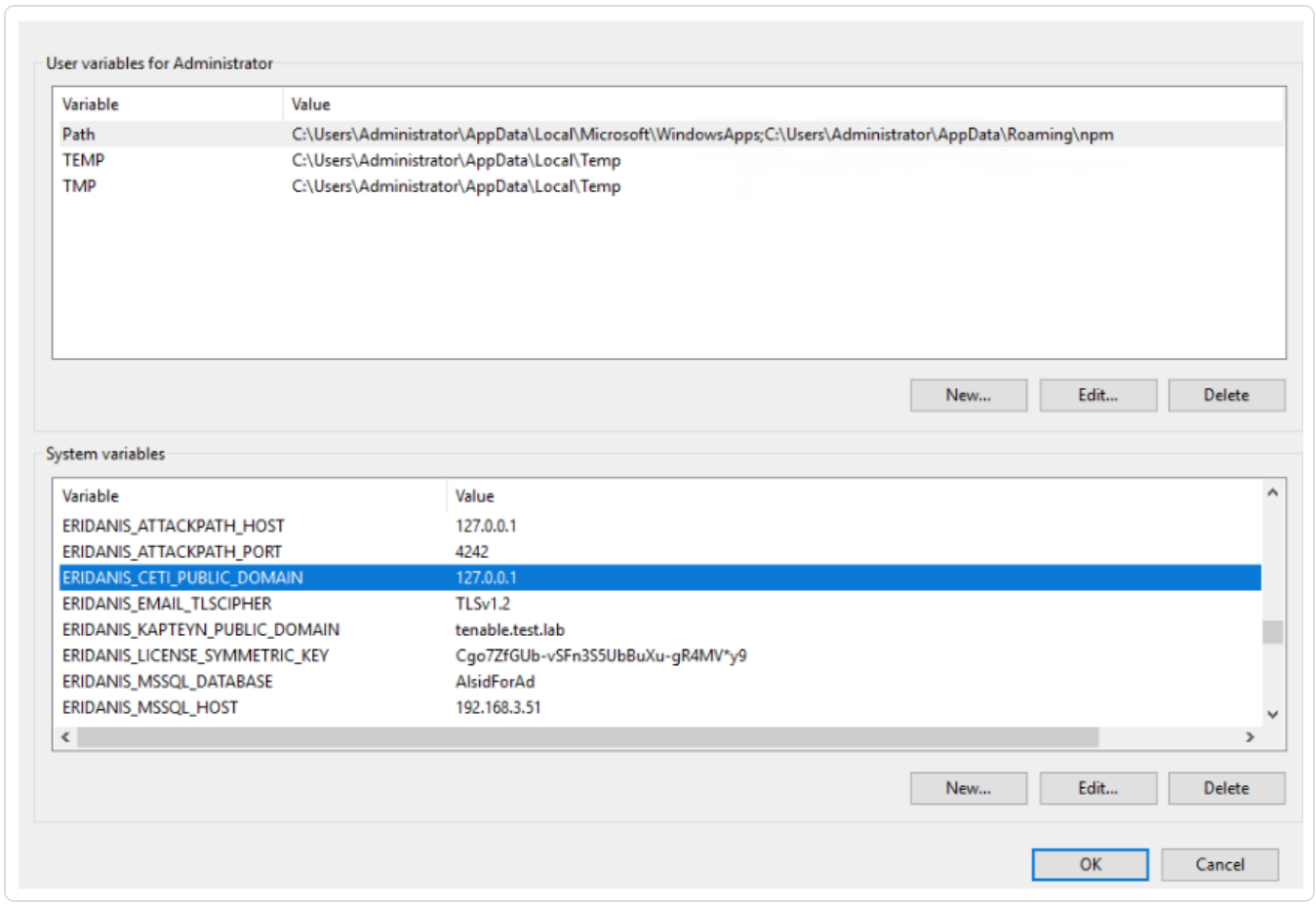

- **錯誤訊息**：連線失敗：無法連線至遠端伺服器。




**針對處於暫停狀態的「tenable_envoy_server」服務**：使用 PowerShell 命令 `netstat -anob | findstr 443` 找出目前佔用連接埠 `0.0.0.0:443` 的應用程式。如果您發現其他應用程式，請將其移除或停止，以解決衝突並讓「tenable_envoy_server」服務正常運作。

**修復**：

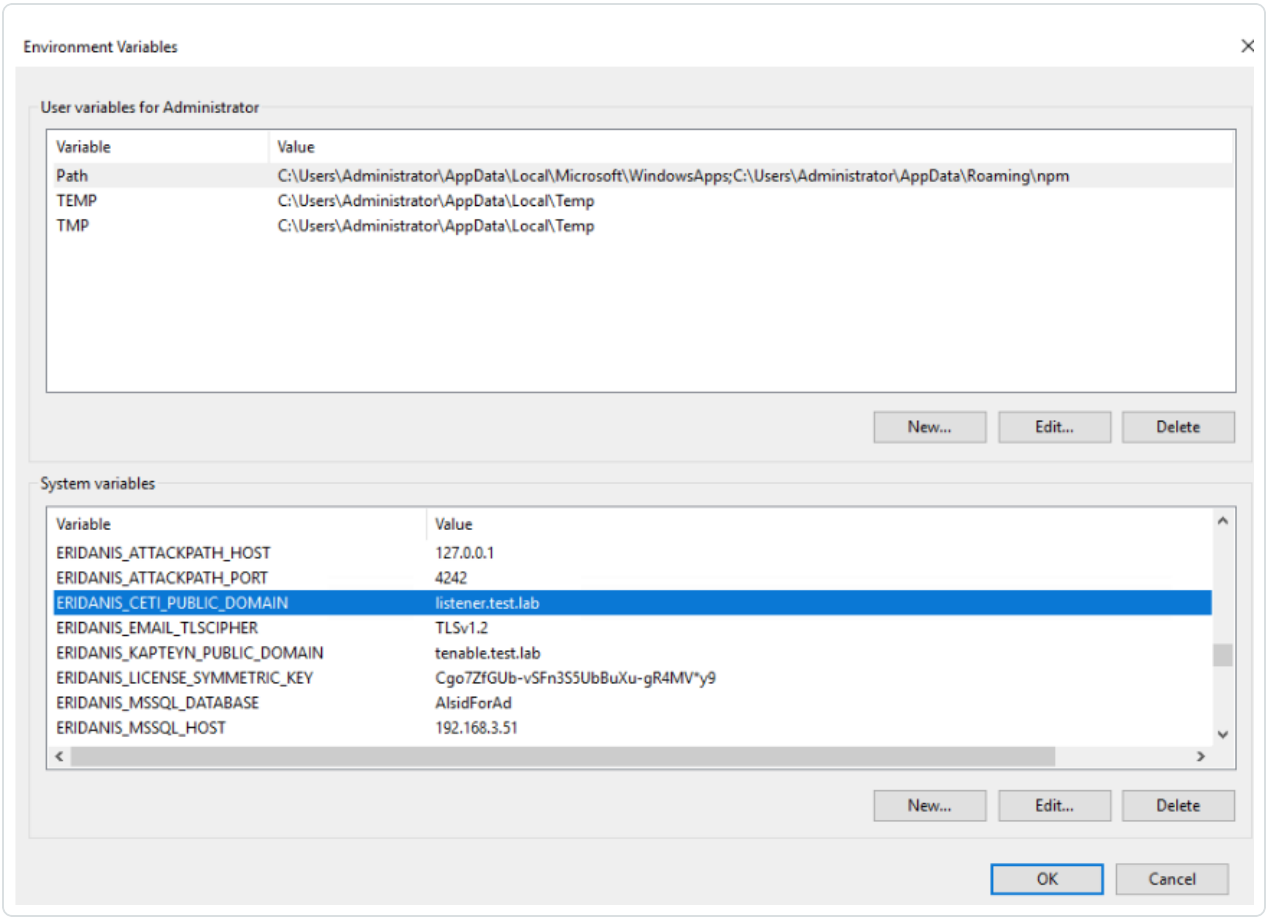
1. 登入安全引擎節點伺服器。
    - 如果您使用分割式安全引擎節點架構，請登入執行 Eridanis 服務的伺服器。
2. 開啟「環境變數」並找到變數名稱 `ERIDANIS_CETI_PUBLIC_DOMAIN`。



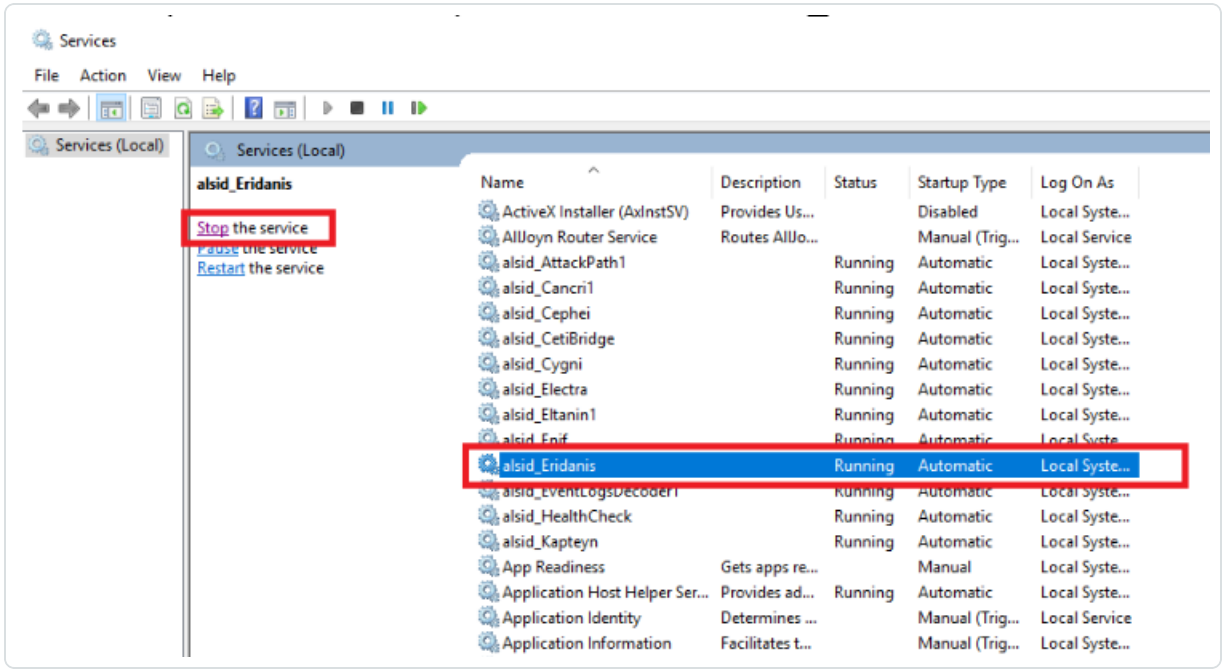

3. 編輯 ERIDANIS_CETI_PUBLIC_DOMAIN 的變數值，插入**目錄接聽程式的 IP 位址或主機名稱**：

    - 更新環境變數 ERIDANIS_CETI_PUBLIC_DOMAIN 以符合目錄接聽程式的 IP 位址或主機名稱。這個同步處理動作有助於部署在不同伺服器上的元件之間進行無縫通訊。
    - 「ERIDANIS_CETI_PUBLIC_DOMAIN」的變數值從 127.0.0.1 變更為目錄接聽程式

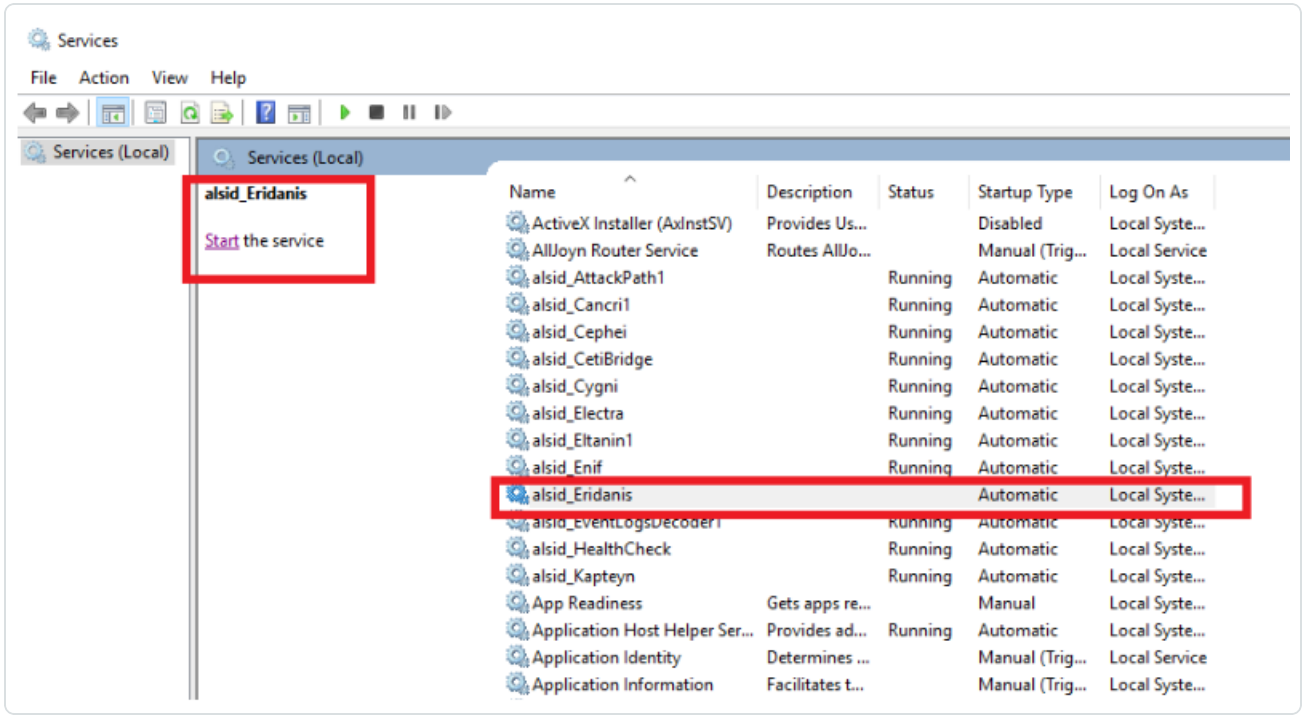
`listener.test.lab` 的 IP 位址或主機名稱。



4. 開啟服務並停止服務 `tenable_Eridanis`。




5. 開始服務 `tenable_Eridanis`。

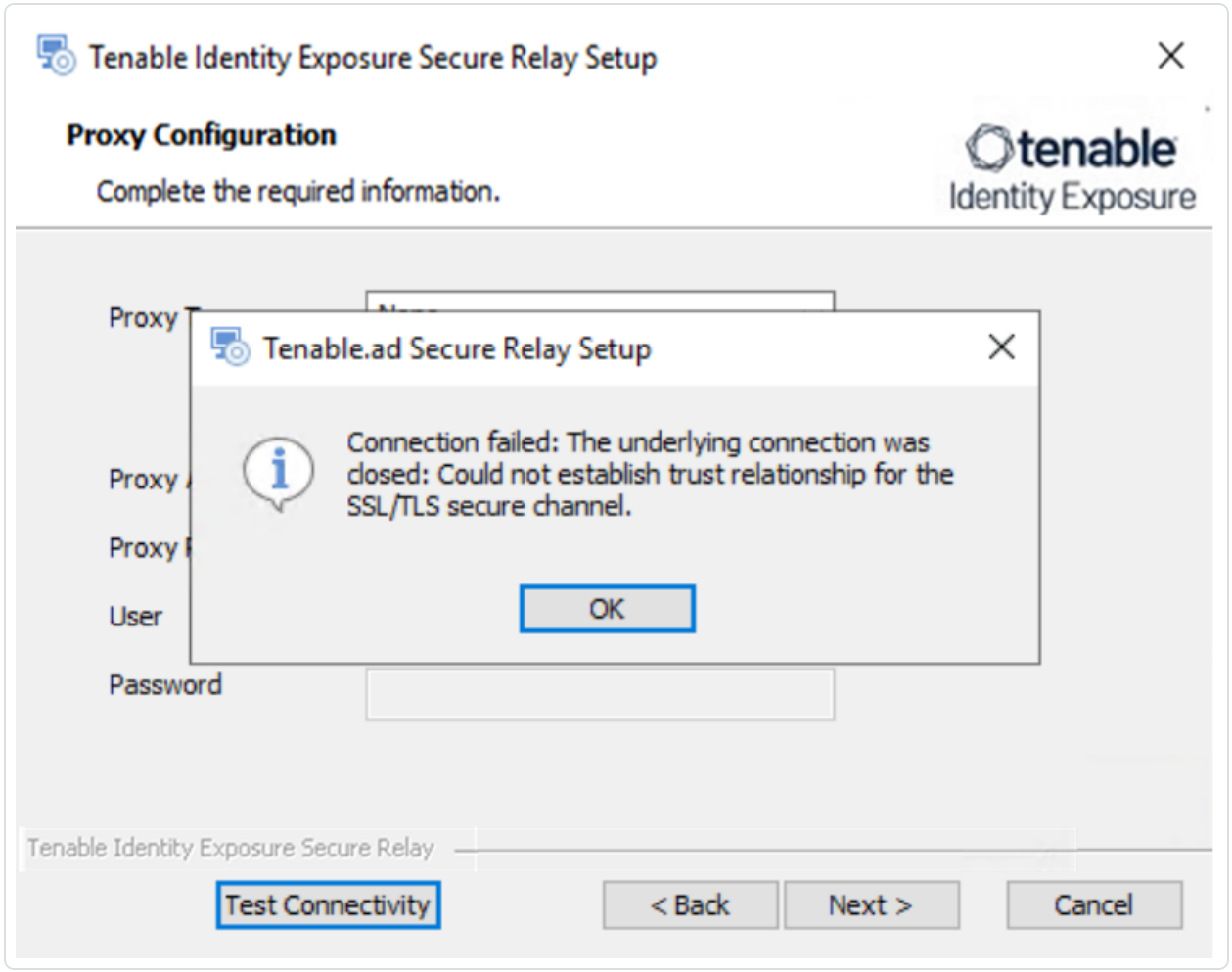


6. 登入安全轉送伺服器。如果安全轉送安裝程式已開啟，請結束該安裝程式，然後再次開始安全轉送安裝。

> **注意**：請務必**結束安裝程式**並開始全新安裝。如果您沒有結束安裝程式而是繼續安裝，則會中斷安裝過程，而且您無法繼續進行 (封鎖程式)。

### SSL/TLS 安全連線沒有「信任關係」

- **原因**：安裝程式在本機伺服器上找不到 CA 憑證。
- **錯誤訊息**：連線失敗：基礎連線已關閉：無法建立 SSL/TLS 安全通道的信任關係。

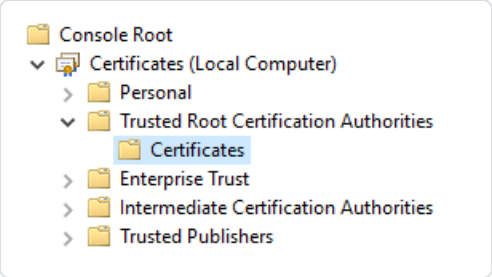



- **修復**：

1. 存取儲存受信任 CA 憑證的來源系統 (目錄接聽程式伺服器) 或存放庫，並找到受信任的 CA 憑證。以下是通常憑證所在的目錄範例：

- 預設自我簽署憑證位置:“installation_drive”:\Tenable\Tenable.ad\DefaultPKI\Certificates\ca
- 自訂憑證位置:“installation_drive”:\Tenable\Tenable.ad\Certificates

2. 將受信任的 CA 憑證檔案從來源系統 (目錄接聽程式伺服器) 複製到本機伺服器 (安全轉送伺服器)。
3. 將憑證匯入安全轉送伺服器的受信任憑證存放區。




4. 成功匯入後,請**結束安全轉送安裝程式,然後重新開始安裝**。

> **注意**:請務必**結束安裝程式**並開始全新安裝。如果您沒有結束安裝程式而是繼續安裝,則會中斷安裝過程,而且您無法繼續進行 (封鎖程式)。

## 開始使用 Tenable Identity Exposure

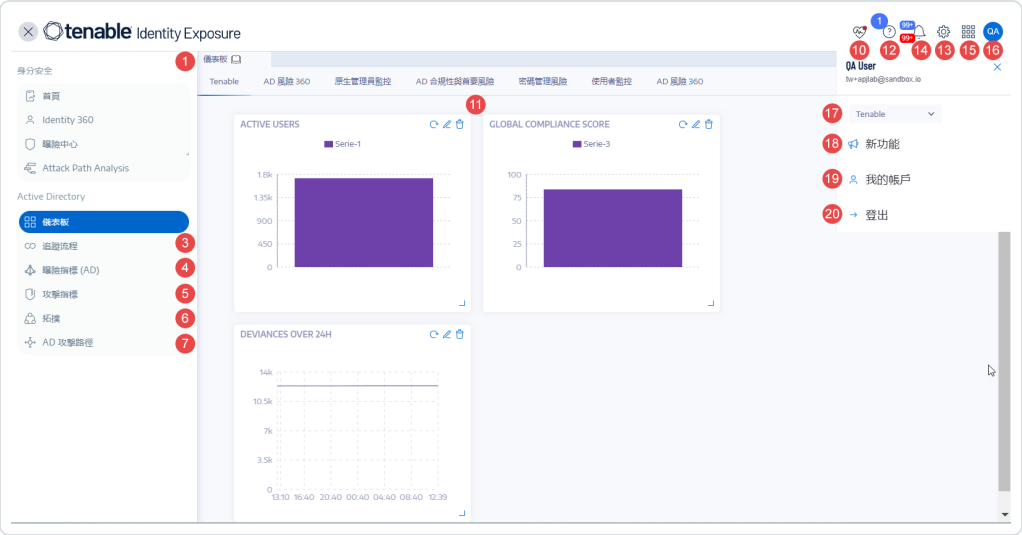
部署 Tenable Identity Exposure 之後,本節將引導您完成開始有效使用 Tenable Identity Exposure 的主要步驟。

各節都有列出連結,提供更詳細的相關工作描述和指示。

1. **登入並前往使用者介面**

   - 登入 Tenable Identity Exposure 入口網站。首頁隨即開啟,如本範例所示。
   - 您的初始登入名稱是 `hello@tenable.ad`,密碼是 `Hello@tenable.ad123!.`
   - 展開或收合側邊導覽列:

- 如要展開：按一下視窗左上角的 ☰ 功能表。
- 如要摺疊：按一下視窗左上角的 ✕。




- 前往 Tenable Identity Exposure 使用者入口網站。

2. **安裝安全轉送**

安全轉送使用 TLS 加密 (而非 VPN 連線)，將 Active Directory 資料從您的網路安全地傳輸至 Tenable Identity Exposure SaaS 平台。根據您的需求，系統可能會使用多個安全轉送。

**先決條件：**

- 對安全轉送虛擬機器 (VM) 的 Windows Server 的管理存取權
- 從 Tenable Identity Exposure 下載入口網站下載的最新安全轉送安裝程式
- Tenable Identity Exposure 入口網站提供的一次性連結金鑰，其中包含網路位址和驗證權杖

> 如需詳細的先決條件資訊，請參閱Tenable Identity Exposure 的安全轉送

**擷取連結金鑰：**

1. 使用系統管理員帳戶連線至 Tenable Identity Exposure web 入口網站。
2. 按一下**「系統」**>**「設定」**>**「轉送」**索引標籤。
3. 按一下連結金鑰旁邊的**「複製到剪貼簿」**圖示。

**安裝安全轉送：**

1. 在 Windows Server VM 上，用滑鼠右鍵按一下安裝程式檔案，然後選取**「以系統管理員身分執行」**。
2. 在安裝精靈中，按一下歡迎畫面中的**「下一步」**。
3. 在**「自訂設定」**視窗中，視需要按一下**「瀏覽」**以變更磁碟分割，然後按一下**「下一步」**。
4. 在**「連結金鑰」**視窗中：
   - 貼上從入口網站複製的連結金鑰。
   - 輸入安全轉送的名稱。
   - 按一下**測試連線能力**。
5. 如果測試成功 (出現綠色圖示)，請按一下**「下一步」**。如果測試失敗，請按一下**「上一步」**以更正錯誤。
6. 在**「準備安裝」**視窗中，按一下**「安裝」**。
7. 安裝完成後，按一下**「完成」**。

   如需瞭解詳細程序，請參閱 Tenable Identity Exposure 的安全轉送 。

**在入口網站中驗證轉送安裝：**

1. 返回 Tenable Identity Exposure 入口網站。
2. 按一下**「系統」**>**「轉送管理」**索引標籤。

   新安裝的轉送會顯示在轉送清單中。

**設定轉送：**

新增要監控的網域時，會出現一個新選項，讓您選取負責該網域的安全轉送。如需瞭解完整程序，請參閱 設定轉送。

**自動更新：**

Tenable Identity Exposure 會定期自動檢查並安裝安全轉送更新 (需要 HTTPS 存取權)。網路狀態區域圖示會標示更新的時間。更新之後，Tenable Identity Exposure 服務會重新啟動，系統也會繼續收集資料。

3. **啟用 Active Directory 網域的曝險指標 (IoE)**

在設定曝險指標之前，您必須擁有或建立具有適當權限的 Active Directory 服務帳戶。雖然 Tenable Identity Exposure 不需要系統管理權限即可進行安全性監控，但某些容器需要手動設定，才能允許服務帳戶使用者的讀取權限。

如需完整資訊，請參閱 存取 AD 物件或容器

1. 使用管理憑證 (例如預設的「hello@tenable.ad」帳戶) 登入 Tenable Identity Exposure web 入口網站。
2. 按一下左上角的功能表圖示以展開導覽面板，然後按一下左側面板中的「**系統**」。

**新增樹系：**

1. 在「**樹系管理**」索引標籤中，按一下「**新增樹系**」。
2. 提供樹系的顯示名稱 (例如 Tenable)。
3. 輸入服務帳戶的登入名稱和密碼，以連線至此樹系中的所有網域。
4. 按一下「**新增**」。

   如需完整詳細資訊，請參閱 樹系。

**新增網域：**

1. 按一下「**新增網域**」。
2. 提供要監控的網域顯示名稱 (例如 HQ)。
3. 輸入符合條件的完整網域名稱 (例如 sky.net)。

4. 從下拉式清單中選取對應的樹系。
5. 如果使用具有安全轉送的 SaaS，請選取要處理此網域的轉送。
6. 如果帳戶具有所需特權，請啟用「特權分析」切換開關。
7. 如果啟用了「**特權分析**」，可選擇針對 Tenable 雲端啟用「**特權分析傳輸**」。
8. 提供具有主要網域控制器模擬器 FSMO 角色的網域控制器的詳細資料：
    - IP 位址或主機名稱
    - 保留 LDAP、全域目錄和 SMB 連接埠預先填入的預設值
9. 按一下底部的「**測試連線能力**」。
10. 如果成功，請按一下「**新增**」。

    在「網域管理」檢視畫面中，LDAP 初始化、SISFul 初始化以及誘捕帳戶設定狀態的欄會持續顯示圓圈載入圖示，直到完成初始檢索作業為止。

    如需完整詳細資訊，請參閱網域。

**監控初始化：**

1. 切換至「**追蹤流程**」檢視畫面。在分析開始之後，資料會在幾分鐘後開始傳入。
2. 返回「**系統**」>「**網域管理**」。
3. 等待綠色圖示出現，這表示 LDAP 和 SYSVOL 初始化已完成。

    您現在已為此網域啟用曝險指標監控。取決於環境大小，web 入口網站會在數分鐘/小時內收到通知。

**查看曝險資料：**

1. 按一下左側功能表中的「**曝險指標**」，以查看針對新增網域觸發的所有指標。
2. 按一下指標，檢視造成違反規則的異常物件詳細資料。
3. 關閉詳細資料並前往「**儀表板**」查看環境指標。

4. **為網域部署攻擊指標 (IoA)**

如要部署攻擊指標 (IoA)，您必須先依照下方說明完成三項設定：

1. 務必針對所有攻擊情境設定攻擊指標 (IoA) 指令碼。
2. 將誘捕帳戶設定為偵測特定攻擊 (例如 Kerberoasting)。
3. 在受監控網域的所有網域控制器上安裝 Sysmon，以偵測作業系統憑證傾印等攻擊。

Tenable Identity Exposure 提供攻擊指標 (IoA) 指令碼、命令列，以及誘捕帳戶設定命令列，但您必須使用適當權限，直接在網域控制器或管理機器上執行這些先決條件。

> 如需完整資訊，請參閱 攻擊指標的部署。

**設定攻擊情境：**

1. 使用管理憑證 (例如 hello@tenable.ad) 登入 Tenable Identity Exposure web 入口網站。
2. 前往**「系統」>「設定」>「攻擊指標」**。
3. 選取要為環境啟用的攻擊情境。
4. 選取網域名稱下方的核取方塊，啟用所有適用的攻擊情境。
5. 按一下右下方的**「儲存」**。
6. 按一下頂端的**「查看程序」**。

   此時會出現一個視窗，顯示部署攻擊指標 (IoA) 引擎的程序。
7. 使用切換開關可啟用或停用自動更新功能。
8. 按一下第一個**「下載」**按鈕可下載 PS1 檔案。
9. 按一下第二個**「下載」**按鈕可下載 JSON 檔案。
10. 記住下載安裝檔案的位置。
11. 找到標記為**「執行下列 PowerShell」**命令的欄位。
12. 複製文字欄位的內容，並貼到文字檔案中。

13. 使用適當權限，將 PS1 和 JSON 檔案複製到網域控制器或管理伺服器。
14. 以系統管理員身分啟動 Windows PowerShell 的 Active Directory 模組，並找到儲存檔案的資料夾。
15. 貼上從 Tenable Identity Exposure web 入口網站複製的命令，然後按下 Enter 鍵。
16. 開啟「群組原則管理」主控台，找到連結至網域控制器 OU 且名為「Tenable.ad」的 GPO。

如需瞭解詳細程序，請參閱 安裝攻擊指標。

**設定誘捕帳戶：**

1. 返回 Tenable Identity Exposure web 入口網站。
2. 前往「**系統**」>「**網域管理**」索引標籤。
3. 按一下網域右側「**誘捕帳戶設定狀態**」下方的「**+**」圖示 (當另外兩個狀態顯示綠色時可用)。
4. 在「**名稱**」搜尋方塊中，輸入要做為誘捕系統使用的帳戶名稱。
5. 從下拉式清單中選取物件的可辨別名稱。
6. 複製命令列文字欄位的內容，並貼到文字檔案中。
7. 返回您執行攻擊指標 (IoA) 指令碼的伺服器。
8. 以系統管理員身分開啟或啟動 PowerShell 命令列。
9. 貼上從 Tenable Identity Exposure web 入口網站複製的命令，然後按下 Enter 鍵。
10. 確認命令列是否正確執行。
11. 返回 Tenable Identity Exposure Web 入口網站，然後按一下底部的「**新增**」按鈕。

    誘捕帳戶設定狀態應會在數秒後顯示一個綠點。

如需瞭解詳細程序，請參閱 誘捕帳戶。

### 安裝 Sysmon：

Tenable Identity Exposure web 入口網站未提供自動部署 Sysmon 的選項。請參閱 安裝 Microsoft Sysmon 以瞭解所需的 Sysmon 設定檔。您可以依照說明文件手動安裝 Sysmon，也可以透過 GPO 安裝。

> 如需瞭解詳細程序，請參閱 安裝 Microsoft Sysmon。

5. ### 設定 Tenable Identity Exposure 的 Microsoft Entra ID：

Tenable Identity Exposure 也支援 Microsoft Entra ID 和具有 Entra ID 身分識別專用曝險指標 (IoE) 的 Active Directory。

> 如需完整資訊，請參閱 Microsoft Entra ID 支援。

### 建立 Entra ID 應用程式：

1. 使用適當的憑證在 portal.azure.com 上登入 Azure 管理員入口網站。
2. 按一下「**Azure Active Directory**」圖塊，然後按一下左側功能表中的「**應用程式註冊**」。
3. 按一下「**新註冊**」並提供應用程式名稱 (例如「Identity Exposure App」)。
4. 按一下底部的「**註冊**」。
5. 在應用程式的「概覽」頁面上，記下「應用程式 (用戶端) ID」和「目錄 (租用戶) ID」。
6. 按一下左側功能表中的「**憑證與密碼**」。
7. 按一下「**新用戶端密碼**」，提供說明並根據原則設定到期日。
8. 按一下「**新增**」，然後安全地儲存顯示的密碼值。
9. 按一下「**API 權限**」和「**新增權限**」。
10. 選取「**Microsoft Graph**」，然後選取「**應用程式權限**」。
11. 新增下列權限：`Audit Log.Read.All`、`Directory.Read.All`、`IdentityProvider.Read.All`、`Policy.Read.All`、lReports.Read.All、

RoleManagement.Read.All、UserAuthenticationMethod.Read.All。

12. 按一下**「新增權限」**和**「授予管理員同意」**。

**設定 Tenable Vulnerability Management：**

1. 使用適當的帳戶連線至 Tenable Vulnerability Management web 入口網站。
2. 按一下**「功能表」**>**「設定」**>**「憑證」**。
3. 按一下**「建立憑證」**並選取**「Microsoft Azure」**類型。
4. 提供名稱、描述，並貼上租用戶 ID、應用程式 ID 和用戶端密碼。
5. 按一下**「建立」**。
6. 按一下**「功能表」**>**「設定」**>**「我的帳戶」**>**「API 金鑰」**。
7. 按一下**「產生」**並查看警告，然後按一下**「繼續」**。
8. 複製存取金鑰和私密金鑰值。

**設定 Tenable Identity Exposure：**

1. 使用全域管理員帳戶連線。
2. 按一下**「功能表」**>**「系統」**>**「設定」**>**「Tenable 雲端」**。
3. 切換**「啟動 Microsoft Entra ID 支援」**以便將其啟用。
4. 輸入先前產生的存取金鑰和私密金鑰。
5. 按一下核取記號即可成功提交 API 金鑰。
6. 按一下**「租用戶管理」**索引標籤，然後按一下**「新增租用戶」**。
7. 提供 Azure AD 租用戶的名稱。
8. 選取先前建立的 Azure 憑證。
9. 按一下**「新增」**。

**追蹤和查看結果：**

1. Tenable Identity Exposure 可掃描租用戶。如要查看下次掃描時間，請將游標停留在「**掃描狀態**」上。
2. 第一次掃描結束時，「**掃描狀態**」欄會出現一個綠色圖示。
3. 按一下左側功能表中的「**曝險指標**」。
4. 使用索引標籤在 AD 和 Azure AD 指標之間篩選。
5. 切換「**顯示所有指標**」以查看所有可用的指標。
6. 三個索引標籤會提供**指標詳細資料**、**租用戶研究發現**和**建議**。
7. 檢閱潛在的曝露風險和修復指南。

6. **在您的環境中設定和使用曝險指標 (IoE)**

Tenable Identity Exposure 會使用曝險指標衡量 Active Directory 的安全成熟度，並向其監控和分析的事件流程指派嚴重性等級。

> 如需有關曝險指標 (IoE) 的完整資訊，請參閱 曝險指標。

**存取曝險指標 (IoE)：**

1. 登入 Tenable Identity Exposure。
2. 按一下左上角的圖示以展開面板。
3. 按一下左側的「**曝險指標**」以查看曝險指標 (IoE)。

   預設檢視會顯示您環境中可能存在有弱點的設定項目，並依嚴重性評等為：「嚴重」、「高度」、「中度」和「低度」。

**檢視所有曝險指標 (IoE)：**

- 按一下「**顯示所有指標**」右側的切換開關。
  - 您可以查看 Tenable Identity Exposure 執行個體中所有可用的曝險指標 (IoE)。任何未顯示網域的項目都是您沒有存在該風險的項目。

- 您可以在「**顯示所有指標**」的右側看到「**網域**」。如果您的環境中有多個網域，請在上面按一下並選取要檢視的網域。

**搜尋曝險指標 (IoE)：**

- 按一下「**搜尋指標**」並輸入關鍵字，例如「密碼」。

  系統會顯示所有與密碼相關的曝險指標 (IoE)。

**檢閱曝險指標 (IoE) 詳細資料：**

- 若要查看有關指標的其他資訊，請按一下該指標。
  - 詳細檢視首先會顯示特定曝險的執行摘要，
  - 接下來會列出與其相關的文件，以及可洩漏此特定項目的已知攻擊者工具。
- 您可以在右邊看見「**受影響的網域**」。
  - 按一下「**弱點詳細資料**」索引標籤，閱讀有關針對此曝險指標 (IoE) 所完成檢查的其他資訊。
  - 按一下「**異常物件**」索引標籤，查看物件清單和觸發曝險的原因。
  - 如果您在清單中展開物件，可以瞭解有關異常情況成因的更多詳細資訊。

**建立查詢：**

1. 若要建立查詢，請按一下「**輸入運算式**」，然後輸入項目的布林查詢。您也可以按一下左側的篩選器圖示以建立查詢。
2. 可以設定開始和結束日期、選擇網域，以及按一下「**略過**」切換開關，搜尋略過的項目。

> 如需完整程序的資訊，請參閱 搜尋異常物件。

**略過/匯出異常物件：**

- 您可以透過略過物件將清單中的物件加以隱藏。
    - 選取一個或多個物件，然後按一下頁面底部的**「選取動作」**。
    - 選取**「略過所選物件」**，然後按一下**「確定」**。
    - 選擇要停止略過所選物件的日期。
    - 您可以使用**「停止略過所選物件」**選項，以相同方式停止略過物件。
- 若要將此指標的所有異常物件清單匯出為 CSV 檔案，請按一下**「全部匯出」**按鈕。

> 如需完整程序的資訊，請參閱 異常物件。

**修復建議：**

- 按一下**「建議」**索引標籤，查看有關如何修復此指標的建議。

> 另請參閱 修復曝險指標中的異常情況 瞭解修復使用案例。

7. **使用追蹤流程追蹤 AD 中的設定變更**

追蹤流程可顯示對於影響 AD 基礎架構之事件的即時監控和分析。您可以用它來識別嚴重弱點，並瞭解建議的修復方法。

> 如需完整資訊，請參閱 追蹤流程 和 追蹤流程使用案例。

**存取追蹤流程：**

1. 登入 Tenable Identity Exposure。
2. 按一下左上角的圖示以展開導覽列。
3. 按一下**「追蹤流程」**。

**瀏覽「追蹤流程」頁面：**

系統隨即會開啟包含事件清單的追蹤流程頁面，內容包括來源類型、物件路徑、網域和日期。

1. 按一下右上角的日期方塊，指出您要搜尋的日期。
2. 按一下**「網域」**以變更 Active Directory 伺服器或樹系。
3. 按一下右上角的暫停按鈕，可暫停或重新啟動追蹤流程擷取。

**建立查詢：**

有兩種方法可針對您的搜尋建立查詢：手動或使用精靈。

- 若要手動篩選事件，請在搜尋方塊中輸入運算式，即可使用布林運算子精簡結果。

  如需完整資訊，請參閱手動搜尋追蹤流程。

- 若要使用搜尋精靈：

  1. 按一下左側的魔杖圖示。
  2. 遵照提示建立並合併查詢運算式。

  如需完整資訊，請參閱使用精靈搜尋追蹤流程 和 自訂追蹤流程查詢

**檢閱事件詳細資料：**

一旦您發現重要事件：

1. 按一下該事件，系統會在該物件上顯示變更的屬性。
2. 將游標停留在左側的藍點圖示上，可比較事件發生前和事件發生時的值。
3. 將游標停留在項目上可查看其他資訊。
4. 按一下**「查看完整值」**，然後按一下按鈕，將此資訊複製到剪貼簿。

**識別設定變更：**

Active Directory 伺服器網路安全的一大挑戰是有大量設定變更並不會影響網路曝險。若要識別設定變更：

1. 按一下魔杖圖示。
2. 啟用**「僅限異常」**。
3. 按一下**「驗證」**。

**檢視網路曝險項目：**

請注意，事件旁邊會顯示一個紅色菱形符號。按一下事件以查看有關設定變更的資訊。可以使用標有「異常情況」的其他索引標籤。按一下即可查看已建立或已解決的特定網路曝險項目。

8. **使用攻擊指標 (IoA) 識別針對 AD 的潛在攻擊**

Tenable Identity Exposure 的攻擊指標 (IoA) 能夠協助您偵測 Active Directory (AD) 上發生的攻擊。

> 如需完整資訊，請參閱 攻擊指標。

**存取攻擊指標 (IoA)：**

1. 登入 Tenable Identity Exposure。
2. 按一下左上角的圖示以展開導覽列。
3. 按一下**「攻擊指標」**。

**篩選時間軸：**

根據預設，您會看到今天的攻擊偵測時間軸。若要變更篩選器：

- 按一下**「日」**、「月」或**「年」**。
- 若要變更時間範圍，請按一下行事曆圖示，然後選取適當的時間範圍。

**篩選檢視：**

您可以使用入口網站右側的選取器篩選特定網域或攻擊指標 (IoA) 的檢視。

1. 按一下**「網域」**以檢視選項並進行選取。
2. 按一下 **X** 即可關閉。
3. 按一下**「指標」**以檢視選項並進行選取。
4. 按一下 **X** 即可關閉。

下面我們以 2022 年的情況為例來說明：

1. 按一下**「年」**按鈕，然後選取**「2022」**。
2. 按一下時間軸中的紅色和黃色列。
3. 您現在會看見新檢視，其中包含當月偵測到的前三個嚴重攻擊和前三個中度攻擊。
4. 按一下黑色方塊外部即可關閉檢視。

**檢視偵測到攻擊的詳細資訊：**

在時間軸下方，您會看見一張卡片，當中有偵測到攻擊的受監控網域。

- 按一下**「排序依據」**下拉式清單。
- 您可以按照網域、指標嚴重性或樹系對卡片進行排序。
- 若要搜尋特定網域或攻擊，請使用搜尋方塊。
- 根據預設，您只會看見受攻擊網域的卡片。將**「僅顯示受到攻擊的網域」**從**「是」**切換為**「否」**，可切換檢視以查看每個網域。

**自訂圖表：**

卡片包含兩種資訊類型：圖表和前三個攻擊。

1. 若要變更圖表類型，請按一下卡片右上方的鉛筆圖示。
2. 選取**「攻擊分布」**或**「事件數」**。
3. 按一下**「儲存」**。

**檢視資安事端詳細資料：**

若要查看有關偵測到攻擊的更多詳細資訊：

- 按一下卡片以查看與網域相關的資安事端。
- 若要進行篩選，請使用搜尋方塊、選取開始或結束日期、特定指標，或切換**「否/是」**方塊以顯示或隱藏已關閉的資安事端。
- 若要關閉資安事端，請選取一個警示，按一下底部的**「選取動作」**功能表，選取**「關閉所選資安事端」**，然後按一下**「確定」**。
- 若要重新開啟資安事端，請選取一個警示，按一下底部的**「選取動作」**功能表，選取**「重新開啟所選資安事端」**，然後按一下**「確定」**。

**檢視攻擊詳細資料和 Yara 偵測規則：**

- 按一下攻擊以開啟詳細資料檢視。描述面板中會有攻擊的資安事端描述、MITRE ATT&CK 架構資訊，以及含有外部網站連結的其他資源。
- 按一下 Yara 偵測規則面板以查看可在偵測工具中執行惡意軟體研究的規則範例。
- 按一下**「全部匯出」**，以便匯出資安事端清單。CSV 是唯一可用的格式。

**通知和警示：**

Tenable Identity Exposure 偵測到攻擊時，右上角的鈴鐺圖示會顯示通知。這些攻擊會顯示在「攻擊警示」索引標籤中。

9. **設定及使用警示**

Tenable Identity Exposure 警示系統可協助您識別受監控的 Active Directory 上的安全狀態惡化或攻擊。系統會透過電子郵件或 Syslog 通知，即時推送有關弱點和攻擊的分析資料。

> 如需完整程序的資訊，請參閱警示。

**設定 SMTP 伺服器：**

1. 連線至 Tenable Identity Exposure。
2. 按一下**「系統」**>**「設定」**。
3. 在此功能表中設定 SMTP 伺服器。

**建立電子郵件警示：**

1. 按一下**「警示引擎」**底下的**「電子郵件」**。
2. 按一下**「新增電子郵件警示」**按鈕。
3. 在**「電子郵件地址」**方塊中輸入收件者的電子郵件地址。
4. 在**「描述」**方塊中輸入有關地址的描述。
5. 從**「觸發警示」**下拉式清單中，選取**「變更時」**、**「每次有異常情況時」**或**「每次攻擊時」**。
6. 在**「設定檔」**下拉式清單中，選取要用於此電子郵件警示的設定檔。
7. 勾選**「有異常情況時傳送警示」**方塊，可在系統重新開機觸發警示時傳送電子郵件通知。
8. 從**「嚴重性臨界值」**下拉式清單中，選取 Tenable Identity Exposure 將會傳送警示的臨界值。
9. 選取要傳送警示的指標。
10. 選取警示網域：
    a. 按一下**「網域」**以便選取 Tenable Identity Exposure 要傳送警示的網域。
    b. 選取樹系或網域，然後按一下**「篩選選取項目」**按鈕。
11. 按一下**「測試設定」**按鈕。

    系統會顯示一則訊息，確認 Tenable Identity Exposure 已傳送電子郵件警示至伺服器。

12. 按一下「**新增**」按鈕。

    系統將顯示一則訊息，確認 Tenable Identity Exposure 已建立電子郵件警示。

**建立 Syslog 警示：**

1. 按一下「**Syslog**」，然後按一下「**新增 Syslog 警示**」按鈕。
2. 在「收集器 **IP 位址或主機名稱**」方塊中，輸入接收通知的伺服器 IP 或伺服器主機名稱。
3. 在「**連接埠**」方塊中輸入收集器的連接埠號碼。
4. 從「**通訊協定**」下拉式清單中，選取 UDP 或 TCP。
5. 如果您選擇 TCP，想要啟用 TLS 安全性通訊協定，請選取「**TLS**」選項核取方塊。
6. 在「**描述**」方塊中輸入有關收集器的簡要描述。
7. 從下列三個選項中選擇一個觸發警示：「**變更時**」、「**每次有異常情況時**」或**或「每次攻擊時」**。
8. 在「**設定檔**」下拉式清單中，選取要用於此 Syslog 警示的設定檔。
9. 如果想要在系統重新開機或升級後傳送警示，請勾選「**在初始分析階段偵測到異常情況時傳送警示**」。
10. 如果您將警示設定為在變更時觸發，請輸入觸發事件通知的運算式。
11. 按一下「**測試設定**」按鈕。

    系統會顯示一則訊息，確認 Tenable Identity Exposure 已傳送 Syslog 警示至伺服器。

12. 按一下「**新增**」。

    系統將顯示一則訊息，確認 Tenable Identity Exposure 已建立 Syslog 警示。

## 10. 在 Tenable Identity Exposure 入口網站中設定儀表板

透過儀表板，您可以將影響 Active Directory 安全的資料和趨勢視覺化。您可以使用小工具自訂儀表板，根據您的要求顯示圖表和計數器。

如需完整資訊，請參閱儀表板。

**存取儀表板：**

1. 登入 Tenable Identity Exposure。
2. 按一下左上角的圖示以展開導覽列。

**建立自訂儀表板：**

1. 前往「**儀表板**」，然後按一下「**新增**」。
2. 按一下「**新增儀表板**」。
3. 為儀表板命名，然後按一下「**確定**」。

**新增小工具至儀表板：**

1. 按一下右上角的「**新增**」。
2. 選取「**在此儀表板上新增小工具**」或按一下螢幕中間的按鈕。
3. 選取小工具的類型 (長條圖、折線圖或計數器)。

**設定折線圖小工具：**

1. 按一下「**折線圖**」。
2. 為小工具命名，例如「過去 30 天內的異常情況」。
3. 選擇資料類型 (使用者計數、異常情況計數或合規分數)。
4. 選取「**異常情況**」並將其設為一個月。
5. 按一下「**無指標**」，然後選取要使用的指標。
6. 為資料集命名，例如「嚴重」。
7. 視需要新增其他資料集 (例如，命名為「中度」和「低度」)。
8. 按一下「**新增**」。

**新增長條圖小工具：**

1. 按一下「**長條圖**」。
2. 將其命名為「**合規**」，並選擇合規分數資料類型。
3. 選取所有指標。
4. 為資料集命名，例如「IoE」。
5. 按一下「**新增**」。

**新增計數器小工具：**

1. 按一下「**計數器**」。
2. 將小工具命名為「使用者」，並將資料類型設定為「**使用者計數**」。
3. 選取狀態「**全部**」，然後選取網域。
4. 為資料集命名，然後按一下「**新增**」。

11. **檢視攻擊路徑**

Tenable Identity Exposure 提供數種方式，可以透過圖形表示法將企業資產的潛在弱點視覺化。

> 如需完整資訊，請參閱 攻擊路徑。

**存取攻擊路徑功能：**

1. 登入 Tenable Identity Exposure。
2. 按一下左上角的功能表圖示以展開導覽列。
3. 在「**安全性分析**」區段中，按一下「**攻擊路徑**」。攻擊路徑功能具有三種模式：
    - 攻擊路徑
    - 影響範圍
    - 資產曝險

**使用影響範圍 (Blast Radius) 模式：**

1. 在搜尋方塊中，輸入帳戶的名稱 (例如「John Doe」)。
2. 從清單中選取帳戶，然後按一下放大鏡圖示。
3. 從選取的遭入侵帳戶中探索影響範圍。
4. 視需要篩選與檢視節點。
5. 將游標停留在端點上可檢視攻擊路徑。
6. 切換選項以顯示所有節點工具提示。
7. 使用縮放列調整檢視。
8. 若要變更搜尋物件，請按一下帳戶名稱旁邊的 **X**，然後執行新的搜尋。

**使用「資產曝險」模式：**

1. 在搜尋方塊中輸入敏感伺服器的名稱 (例如「srv-fin」)。
2. 從清單中選取物件，然後按一下放大鏡圖示。
3. 探索所選敏感伺服器的資產曝險程度。
4. 使用與「影響範圍」模式中類似的選項。
5. 將游標停留在路徑上可檢視詳細資料。
6. 切換選項以顯示所有節點工具提示。
7. 使用底部列調整檢視。

**使用「攻擊路徑」模式：**

1. 在起點搜尋方塊中，輸入遭入侵帳戶的名稱 (例如「John Doe」)。
2. 按一下帳戶名稱。
3. 在到達點搜尋方塊中輸入敏感資產的名稱 (例如「s or v-fin」)。
4. 按一下資產名稱。

5. 按一下放大鏡圖示。
6. 探索遭入侵帳戶和敏感資產之間的可用攻擊路徑。
7. 使用與「影響範圍」模式和「資產曝險」模式中類似的選項。

**其他功能：**

- **誰可以控制我的特權資產**：顯示具有以特權資產為目標的攻擊路徑的所有使用者和電腦帳戶。
- **我的特權資產內容是什麼**：會列出第 0 層資產和帳戶，以及通往這些資產的潛在攻擊路徑。
- 在索引標籤之間切換以檢視清單。
- 按一下項目旁邊的放大鏡圖示可切換檢視。
- 按一下藍色箭頭和點圖示可開啟已篩選為僅顯示此資產的資產曝險檢視。

**解譯結果：**

1. 使用「攻擊路徑」功能確認假設，並且視覺化實體之間的危險攻擊路徑。
2. 採取修復動作關閉已識別的攻擊路徑。

**提示：**如需有關 Tenable Identity Exposure 的其他資訊，請檢閱下列客戶教育資料：

- Tenable Identity Exposure 自助指南
- Tenable Identity Exposure 簡介 (Tenable University)

# Tenable Identity Exposure 的基本知識

本節介紹大多數使用者開始使用並充分利用 Tenable Identity Exposure 所需要瞭解的基本日常任務。

無論是第一次使用本產品，還是只是需要複習基礎知識，您都可以在此處找到常見操作的逐步說明，例如驗證、導覽工作區、設定喜好設定和通知、使用儀表板和小工具、使用曝險中心探索身分、使用追蹤流程將資料追蹤視覺化，以及瞭解曝險指標和攻擊指標。

如需與特定工作相關的資訊，請按一下畫面左側功能表窗格中的相關主題。

## 登入 Tenable Identity Exposure

您可以透過用戶端 URL 存取 Tenable Identity Exposure 的 Web 應用程式。

如要登入 Tenable Identity Exposure，請選取其中一個以下選項：

- 使用 Tenable Identity Exposure 帳戶
- 使用 LDAP 帳戶
- 使用 SAML

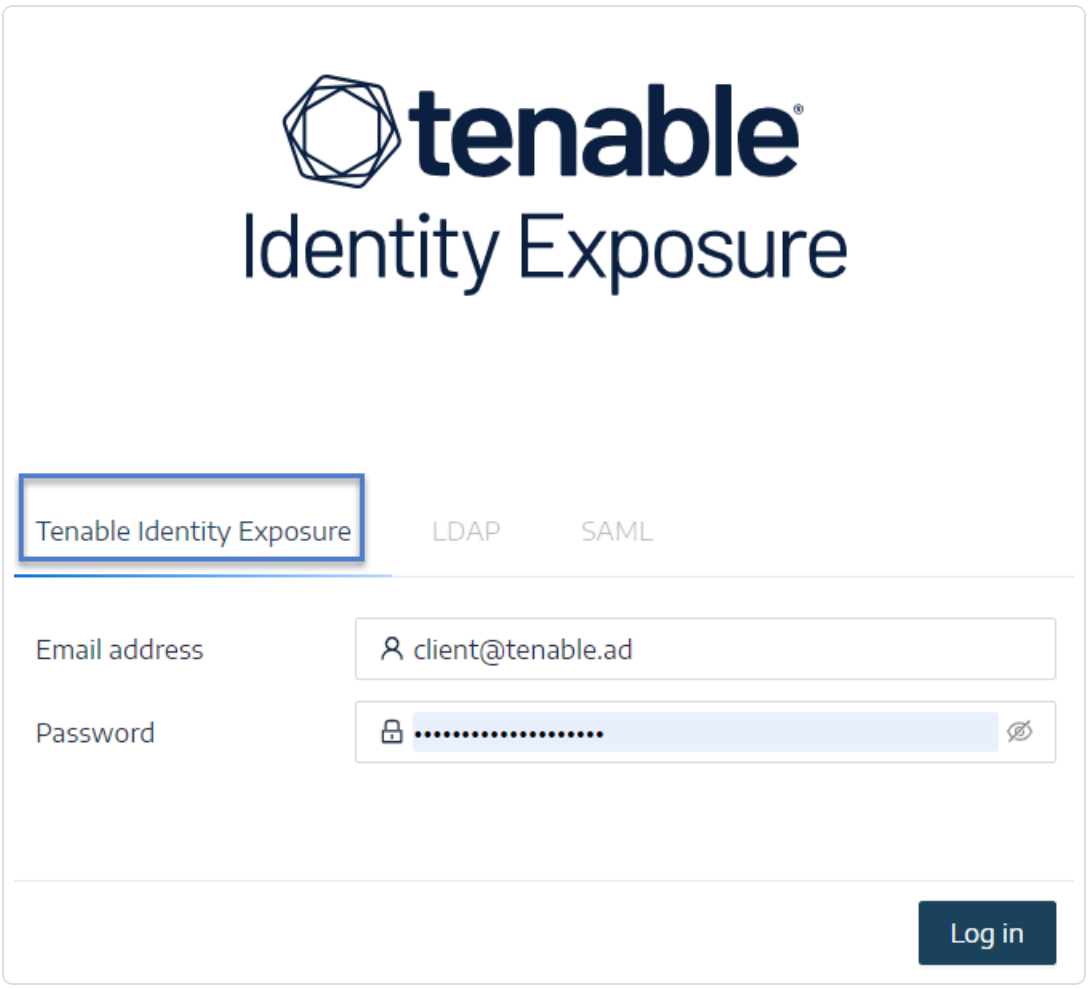
**注意**：您初始憑證的使用者名稱為 `hello@tenable.ad`，密碼為 `Hello@tenable.ad123!.`

### 使用 Tenable Identity Exposure 帳戶

如要使用您的 Tenable Identity Exposure 帳戶登入：

1. 在任意瀏覽器的網址列中輸入您的用戶端 URL (例如：client.tenable.ad)。

   **登入**視窗會隨即顯示。




2. 按一下「**Tenable Identity Exposure**」索引標籤。
3. 輸入您的電子郵件地址。
4. 輸入您的密碼。
5. 按一下「**登入**」。

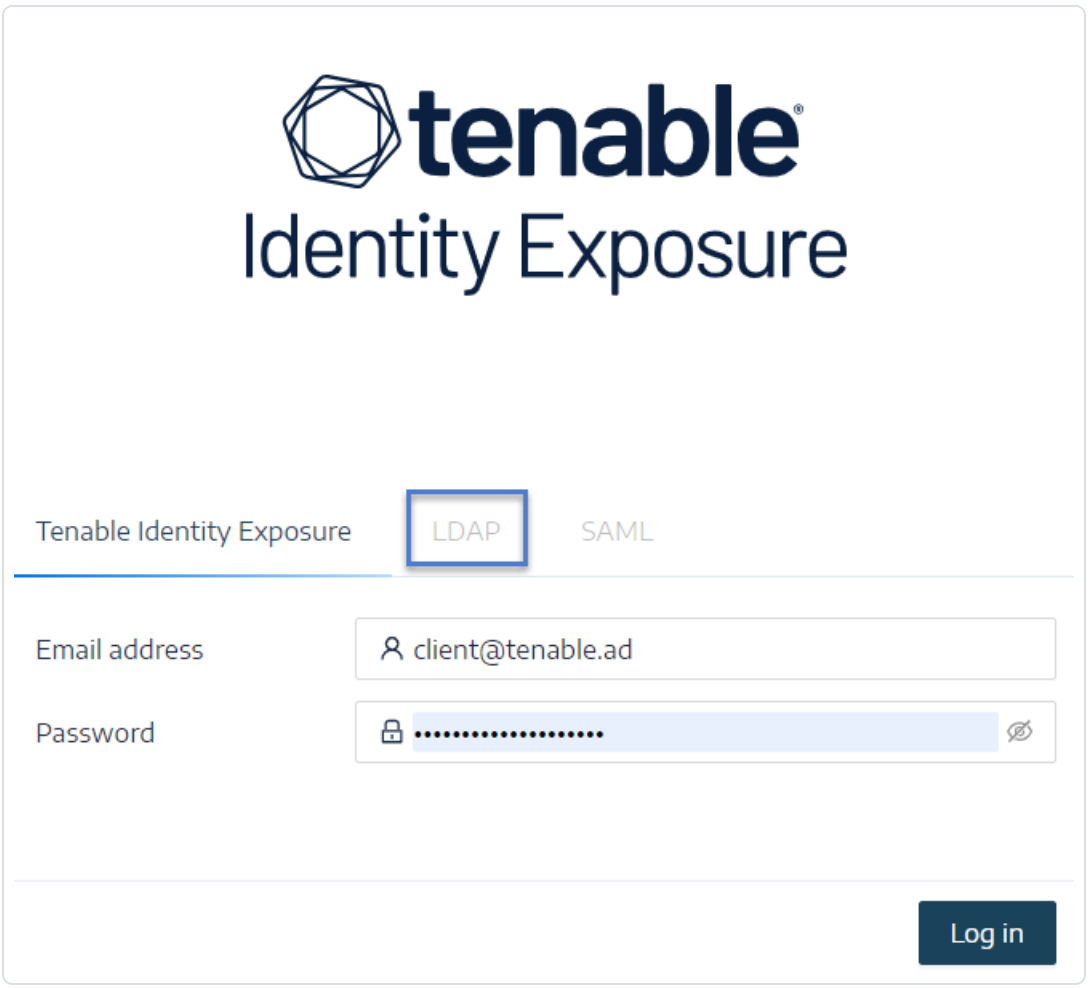
   Tenable Identity Exposure 頁面會隨即開啟。

### 使用 LDAP 帳戶

如要使用 LDAP 登入：

1. 在任意瀏覽器的網址列中輸入您的用戶端 URL (例如：client.tenable.ad)。

   **登入**視窗會隨即顯示。




2. 按一下「**LDAP**」索引標籤。
3. 輸入您的 LDAP 帳戶名稱。
4. 輸入您的 LDAP 密碼。
5. 按一下「**登入**」。

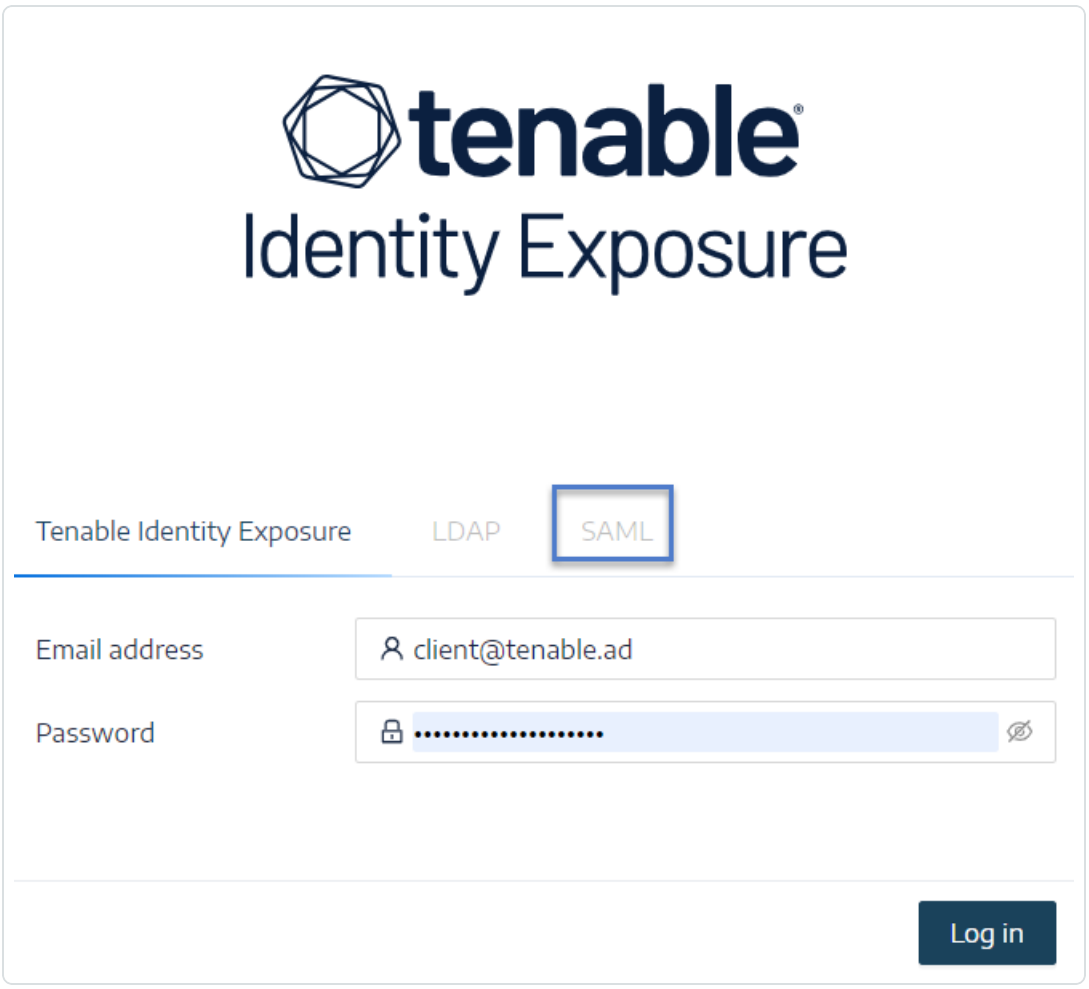
   Tenable Identity Exposure 頁面會隨即開啟。

### 使用 SAML

如要使用 SAML 登入：

1. 在任意瀏覽器的網址列中輸入您的用戶端 URL (例如：client.tenable.ad)。

   **登入**視窗會隨即顯示。




2. 按一下「**SAML**」索引標籤。
3. 按一下通往您的身分識別提供者 (IDP) 的連結。

   Tenable Identity Exposure 會將您重新導向至您的 SAML 伺服器進行身分驗證。
4. 在 IDP 上輸入您的公司憑證。

   您將以已登入的使用者身分重新導向至 Tenable Identity Exposure。

**注意**：如果您多次登入失敗，Tenable Identity Exposure 將鎖定您的帳戶。請聯絡您的管理員。

**如要在第一次登入後重設密碼：**

首次以 `hello@tenable.ad` 帳戶登入時，Tenable Identity Exposure 會提示您重設預設密碼。

**注意**：如果您擁有 Tenable One 授權，則無法使用密碼資訊，在這種情況下是由 Tenable Vulnerability Management 管理您的所有身分驗證設定。如需詳細資訊，請參閱《Tenable Vulnerability Management 使用者指南》中的「存取控制」章節。

1. 在 Tenable Identity Exposure 中，按一下右上角的使用者設定檔圖示。

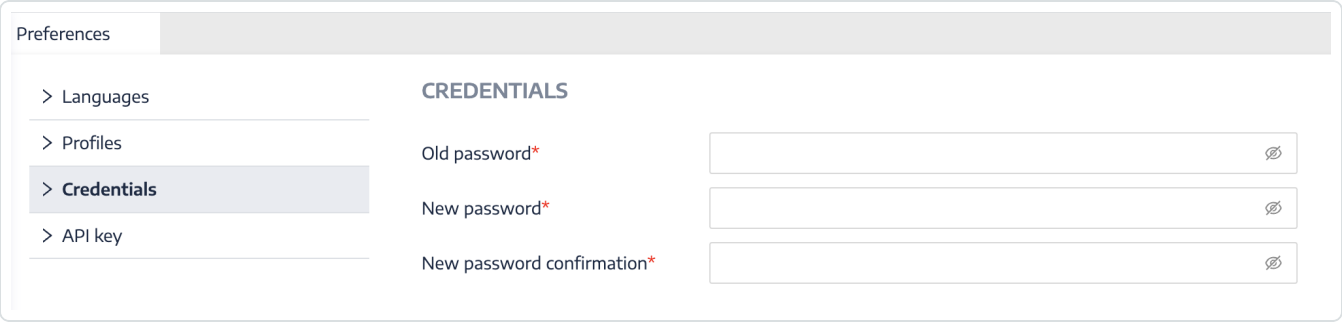
   子功能表會隨即顯示。




2. 選取「**我的帳戶**」。

   「**喜好設定**」頁面會隨即顯示。

3. 在「**喜好設定**」下方，按一下「**憑證**」。




4. 在「**舊密碼**」中輸入舊密碼。

5. 在「**新密碼**」中輸入新密碼。遵守下列密碼複雜性規則，這些規則與 Tenable One 帳戶所需的規則一致：

- 長度必須至少為 12 個字元。
- 必須包含以下字元，且每項至少一個：
  - 大寫字母 (A-Z)
  - 小寫字母 (a-z)
  - 數字 (0-9)
  - 特殊字元 (例如 !、@、#、$)
- 不能包含字串 `verysecure`，以防止重複使用先前的預設密碼 `verySecure1!`。

6. 在「**新密碼確認**」方塊中，重新輸入新密碼。
7. 按一下「**儲存**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已變更您的密碼。

**如要登出 Tenable Identity Exposure：**

1. 在 Tenable Identity Exposure 中。按一下您的使用者圖示。

   子功能表會隨即顯示。

2. 按一下「**登出**」。

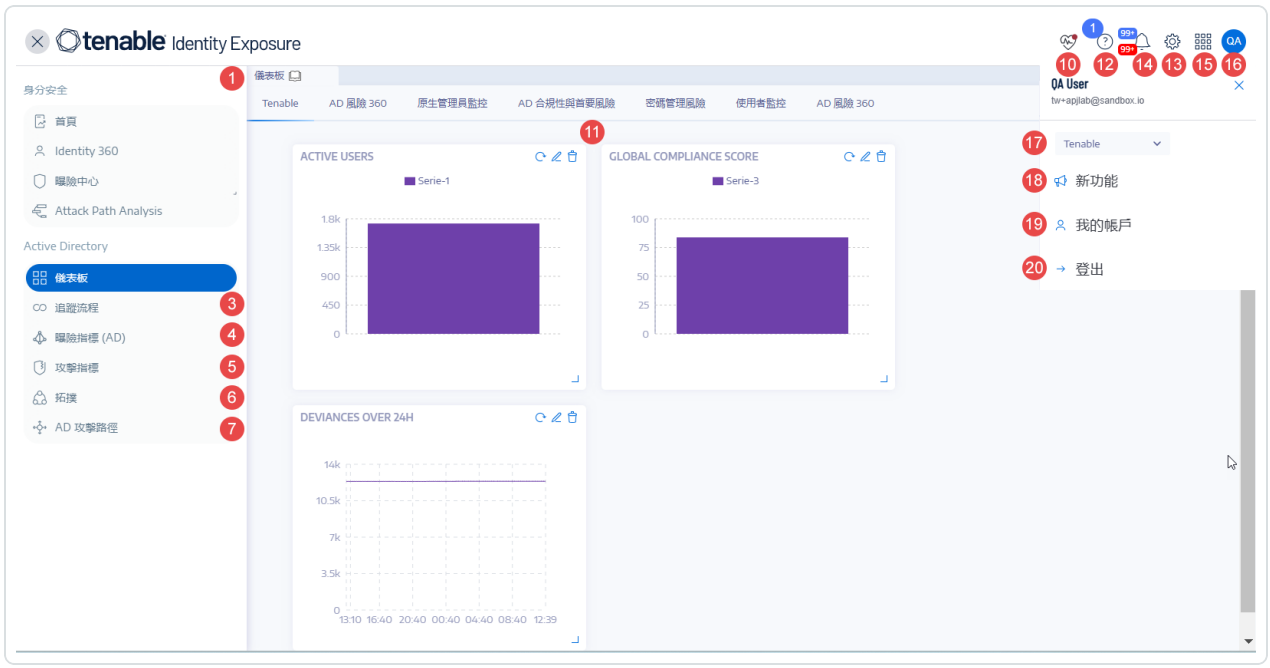
   Tenable Identity Exposure 將返回登入頁面。

## Tenable Identity Exposure 使用者入口網站

登入 Tenable Identity Exposure 後，首頁將開啟，如本範例所示。

如要展開或摺疊側邊導覽列：

- 如要展開：按一下視窗左上角的 ☰ 功能表。
- 如要摺疊：按一下視窗左上角的 ✕。




| # | 名稱 | 用途 |
|---|---|---|
| 1 | 儀表板 | 儀表板能讓您以視覺化的方式有效率地管理和監控 Active Directory 基礎架構的安全性。 |
| 2 | - | - |
| 3 | 追蹤流程 | 追蹤流程顯示對於影響 Active Directory 之事件的即時監控和分析。 |
| 4 | 曝險指標 | Tenable Identity Exposure 會使用曝險指標 (IoE) 衡量您 Active Directory 的安全成熟度，並向其監控和分析的事件流程指派嚴重性等級 (嚴重、高度、中度或低度)。 |
| 5 | 攻擊指標 | Tenable Identity Exposure 可以透過攻擊指標即時偵測攻擊。 |
| 6 | 拓撲 | 「拓撲」頁面提供 Active Directory 的互動式圖形視覺化，其中顯示樹系、網域以及它們之間存在的信任 |

| | | |
|---|---|---|
| | | 關係。 |
| 7 | 攻擊路徑 | 攻擊路徑頁面提供 Active Directory 關係的圖形表示：<br>• 影響範圍：評估 AD 中可能遭入侵資產的橫向移動。<br>• 攻擊路徑：預期特權提升技倆從特定進入點到達資產。<br>• 資產曝險：透過資產曝險視覺化來衡量資產的弱點並解決所有升級路徑。 |
| 8、9 | 管理<br>**所需的使用者角色**：具有適當權限的組織使用者。 | 您可以在此部分設定以下內容：<br>• 帳戶：使用者帳戶、角色和安全性設定檔。<br>• 系統：樹系和網域、應用程式服務、警示和身分驗證。<br>如需詳細資訊，請參閱 Tenable Identity Exposure 設定和管理。 |
| 10 | 運作狀況檢查 | 運作狀況檢查可讓您在單一整合檢視畫面中即時查看網域和服務帳戶的設定，以深入了解更多詳細資訊。 |
| 11 | 小工具 | 小工具是儀表板上可自訂的資料集，其中可以包含橫條圖、折線圖和計數器。 |
| 12 | 產品更新 | 有關最新產品功能的資訊。 |
| 13 | 設定 | 存取系統設定、樹系和網域管理、授權、使用者和角色管理、設定檔和活動記錄的權限。 |

| | | |
|---|---|---|
| 14 | 通知 (鈴鐺) | 鈴鐺圖示和徽章計數通知您有等待確認的攻擊警示和/或曝險警示。 |
| 15 | 存取工作區 | 按一下此圖示可在 Tenable 工作區的應用程式之間切換。 |
| 16、19 | 使用者設定檔圖示 (使用者喜好設定) | 按一下此圖示可存取安全性設定檔、版本資訊、活動記錄、喜好設定或登出的子功能表。 |
| 17 | 安全性設定檔 | 安全性設定檔允許不同類型的使用者從不同的報告角度來檢閱安全性分析。 |
| 18 | 新功能 | 按一下即可開啟最新版 Tenable Identity Exposure 的版本資訊。 |
| 20 | 登出 | 按一下即可登出 Tenable Identity Exposure。 |

## Tenable Identity Exposure 深入分析

「Tenable Identity Exposure **深入分析**」頁面提供以使用者為中心的全面介面，專門設計來滿足組織在控管身分安全方面的關鍵需求，這包括評估身分風險環境的不穩定性、重點呈現組織所面臨最重大的身分風險，並提供「高成效，低投入」的修復步驟指引，幫助在現今日趨複雜的安全環境中面臨嚴峻限制條件的團隊確定優先事務。

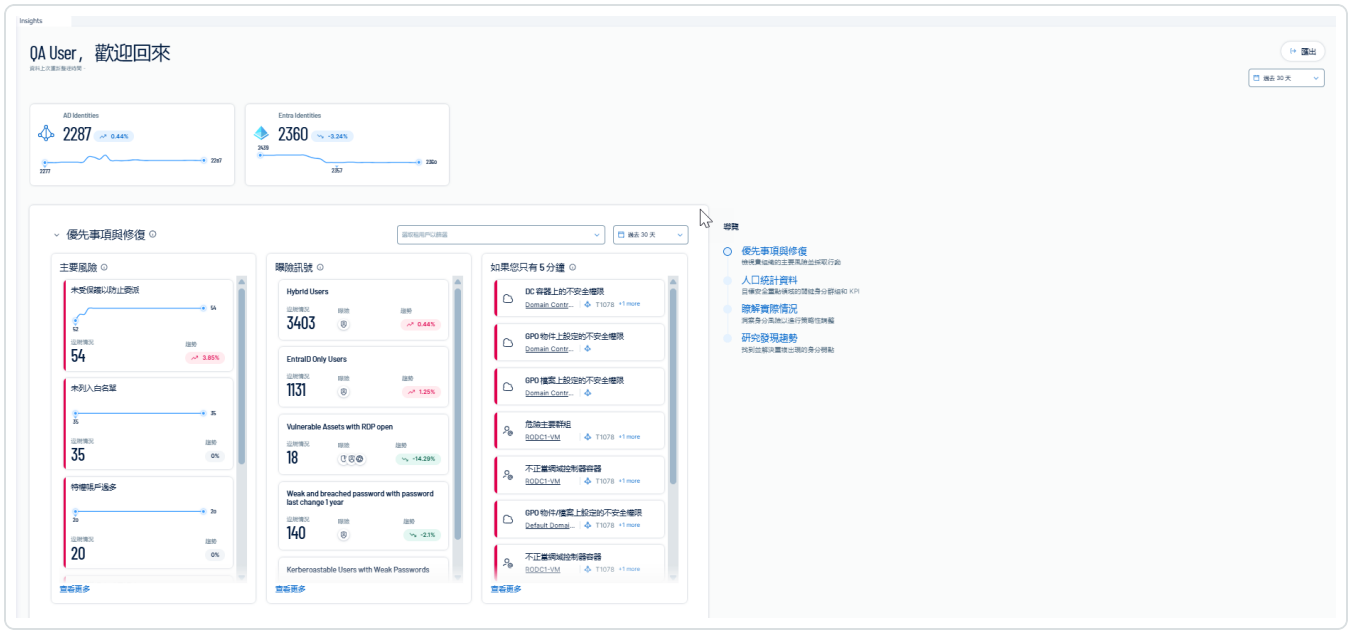
此儀表板專為提供沉浸式登錄頁面體驗而設計，將重要的身分安全指標和深入分析整合到單一互動檢視畫面 (即「單一虛擬管理平台」) 中。透過簡化的身分安全追蹤方法，Tenable Identity Exposure 可讓您快速評估安全狀態、識別高風險弱點和確定優先順序，並採取可行的步驟來減輕潛在威脅。

「**深入分析**」頁面讓您可以全面深入探討、依據身分篩選，還能透過豐富的報告服務，順暢分享關鍵資料和深入分析。此頁面經過設計，專門供各種身分安全相關人員使用。

> **注意**：「**深入分析**」頁面目前僅顯示與「Tenable」安全設定檔相關的資料，忽略其他所有安全設定檔。

若要存取「Tenable Identity Exposure **深入分析**」頁面：

- 在 Tenable Identity Exposure 中，按一下左側導覽列中的  。




## 標題

標題功能匯總了新風險和已解決的風險，讓您無需深入研究詳細報告，即可快速瞭解目前的安全狀態，有助於加快決策制定和回應速度。

- 歡迎訊息：此訊息會顯示使用者名稱，歡迎回訪的使用者。
- Active Directory、Entra ID 等不同供應商的身分指標：透過視覺化資料幫助您察覺不同身分供應商之間是否有不尋常的變化，反映可能有潛在安全問題，或者呈現身分成長趨勢。
    - AD 身分、Entra 身分等項目的圖塊會顯示各個供應商目前的身分數量，以及透過小型折線圖呈現的趨勢百分比。按一下任何圖塊，即可深入瞭解特定身分平台的更多詳細資訊。
    - 按一下 **>**，即可檢視所有未顯示在頁面上的身分平台。
- 時間範圍選取器：用來選取一段時間 (例如「過去 90 天」) 的下拉式選單，可用於自訂顯示的資料，方便瞭解不同時間範圍的趨勢。此功能為分析帶來靈活性，既能滿足短期風險追蹤的需求，也符合長期策略規劃需要。

## 跨區段瀏覽

使用以下任一方式，即可瀏覽「**深入分析**」頁面的各個區段：

- 身分指標圖塊下方的索引標籤：



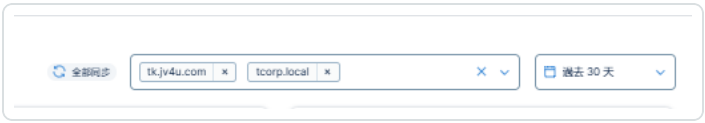

- 右側的垂直導覽選單，可用於在「**深入分析**」頁面的不同區段之間移動。按一下任何區段，即可瀏覽該頁面。




> **提示**：將頁面的縮放比例調低，導覽列便會顯示在右側。

## 選取網域/組織

使用篩選方塊，即可選取一或多個網域，重點關注特定網域或業務單位。



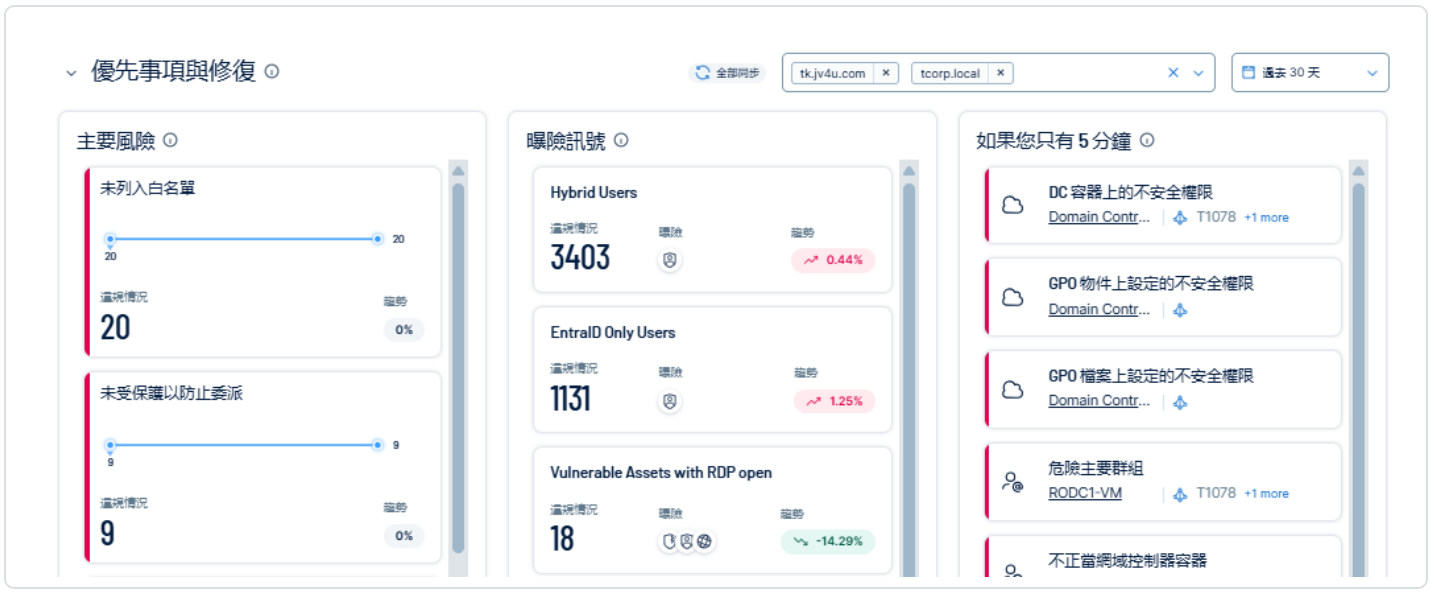

如要選取網域或組織：

1. 按一下篩選方塊中的箭頭以顯示網域或組織，然後選取要篩選的網域或組織。
2. 按一下時間範圍選取器中的箭頭，即可調整資料分析的時間範圍，或追蹤特定時間內的趨勢。
3. 按一下「全部同步」，套用篩選器。系統將顯示一則訊息，確認 Tenable Identity Exposure 已成功套用篩選器。

此篩選方塊適用於「**深入分析**」頁面上的所有區段。

## 優先事項與修復區段

此區段基本上就像是安全控制中心，有助於管理員清楚掌握最具影響力的安全性弱點，並有效排定修復工作的優先順序。




### 主要風險

此面板會顯示所選網域和時間範圍內最需要優先處理的風險，並依嚴重程度排序，當中會呈現環境中目前的違規數量，並透過折線圖反映趨勢，指出問題是惡化還是有所改善。

- 按一下圖塊，即可瞭解目前應針對哪些風險優先採取修復措施。

### 曝險訊號

「曝險訊號」中呈現可能會變成攻擊路徑或帶來危害的多個風險的組合，提供的深入分析會依嚴重性排序，而且都會列出違規數量和引發潛在問題的風險類型 (以圖示呈現)。另外也會提供趨勢指標，以百分比形式呈現變化情形。

- 按一下圖塊，即可深入瞭解有關「曝險訊號」的詳細資訊。

### 如果時間不多

此面板重點呈現高優先順序的風險，有助於快速採取行動解決迫切問題。

- 按一下圖塊，即可深入瞭解更多有關修復風險的詳細資訊。

## 群體特徵區段

「**群體特徵**」區段提供關鍵深入分析，讓安全團隊可以掌握需要重點留意的重要身分同類群組 (具有共同特徵的身分或使用者群體)，有助於您更清楚瞭解組織內的風險分布，據此做出更明智的決策。




這些圓形圖代表「群體特徵」區段中的主要身分同類群組，分別呈現需要密切留意的特定帳戶類別或安全指標。

- **中央數字**：每張圖中心的數字代表特定弱點或身分同類群組目前的數量或值，不但有助於快速瞭解與特定類別相關的總執行個體數量，例如休眠帳戶、低強度密碼或特權帳戶等項目的數量，還提供直觀的視覺指標，方便掌握組織內潛在安全問題或身分相關風險的規模。請結合趨勢指標和顏色編碼解讀此數字，全面瞭解風險的重大程度。
- **趨勢指標**：這會呈現特定指標相較於先前報告期的百分比變化，反映一段時間內的情況是改善、惡化還是保持穩定。
    - 綠色百分比的向下箭頭 (↓)：表示減少，與安全風險相關時通常是正面的象徵 (例如，低強度密碼減少)。
    - 紅色百分比的向上箭頭 (↑)：表示增加，根據具體指標，可能代表問題日益嚴峻。

- **顏色指標**:每個指標周圍的彩色圓環代表與特定弱點相關的風險等級分布,範圍從嚴重(紅色)到低(黃色)。
- **說明文字**:每個彩色圓環下方的文字提供特定弱點的簡要說明,有助於您瞭解指標所追蹤事項對安全的影響,例如低強度密碼和休眠帳戶等。

如要深入瞭解詳細資訊:

- 如需瞭解特定弱點影響的資產詳細資訊,請按一下圓環中央前往 Tenable Inventory。
- 如需瞭解特定弱點的風險分布詳細資訊,請按一下圓環的彩色部分,前往「Exposure View」。如需詳細資訊,請參閱曝險中心。

**注意**:「機器帳戶」已暫時從 Tenable Inventory 移除,所以目前無法深入瞭解這些帳戶的資訊。也是因為如此,Tenable Inventory 不會顯示「機器帳戶」,導致 Tenable Identity Exposure 和 Tenable Inventory 顯示的數量有所差異。

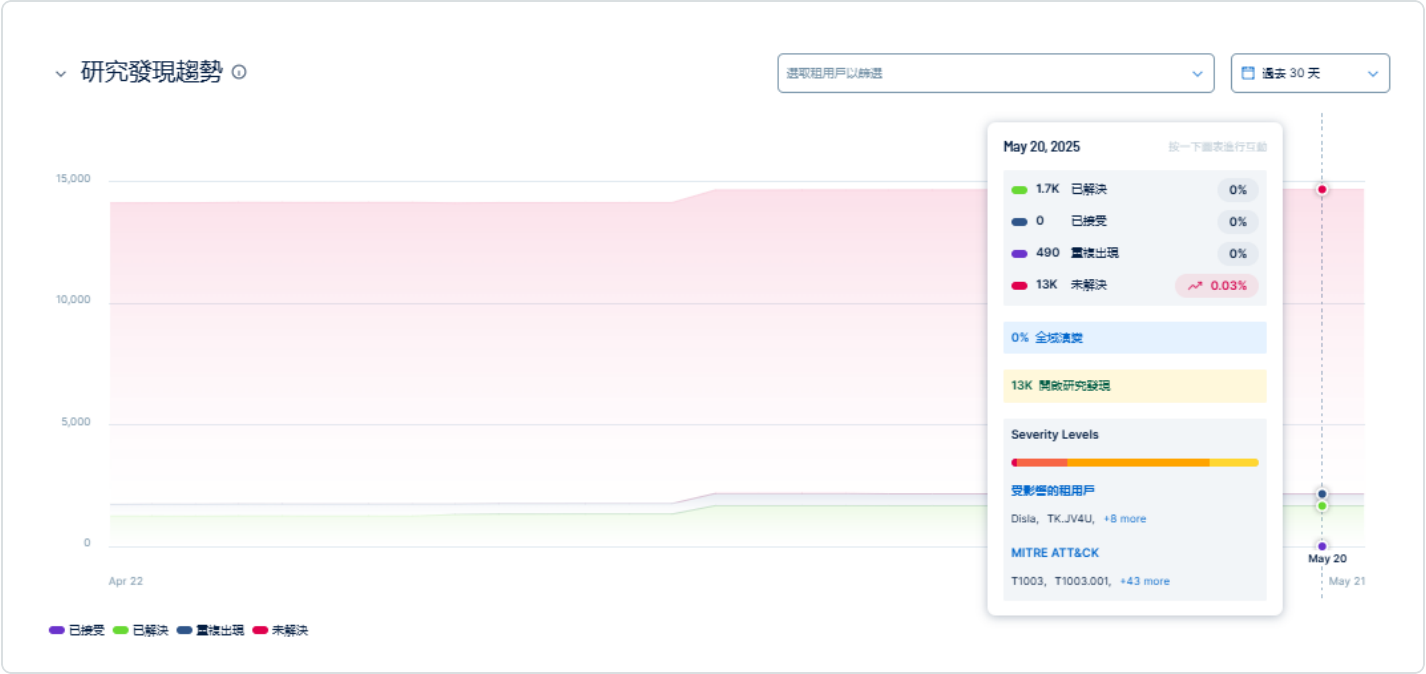
**注意**:曝險概覽功能目前會根據**預設的 Tenable 設定檔**顯示弱點相關資料,不會自動反映**您在其他設定檔中列入白名單的 AD 物件的異常情況狀態**。

因此:

- 如果您已將特定曝險指標(例如「原生系統管理群組成員」)的 **AD 物件列入白名單**,**當預設設定檔將其識別為異常時,曝險概覽仍會將其標記為安全性弱點**。
- 即使物件已在不同的設定檔下列入白名單,這仍可能會造成問題尚未解決的印象。
- 如果根據曝險概覽顯示採取修復動作(例如移除群組成員資格),則物件將從檢視畫面中消失,但若該物件已在其他地方列入白名單,可能沒有必要採取修復動作。

## 「研究發現趨勢」區段

**「研究發現趨勢」**區段呈現組織歷來安全資料的持續性分析,反映身分相關弱點和漏洞的模式。透過此歷來資料分析,安全團隊可以掌握反覆發生的問題和不斷變化的風險模式,先行採取措施應對潛在威脅。




「**研究發現趨勢**」區段以堆疊面積圖呈現時間線，可用於追蹤不同類別的安全研究發現結果。視覺化資料將研究發現分為四個主要狀態：

- 已解決的研究發現結果 (標為綠色)
- 接受的研究發現結果 (標為藍色)
- 重新出現的研究發現結果 (標為紫色)
- 未解決的研究發現結果 (標為粉色/紅色)

如要篩選出上述任何狀態，請按一下圖表底部的狀態名稱。

其他功能包括：

- 整體演變指標
- 總研究發現結果計數器
- 嚴重程度指標

如需詳細瞭解這些資料，請點選以下連結：

- MITRE ATT&CK
- 受影響的租用戶

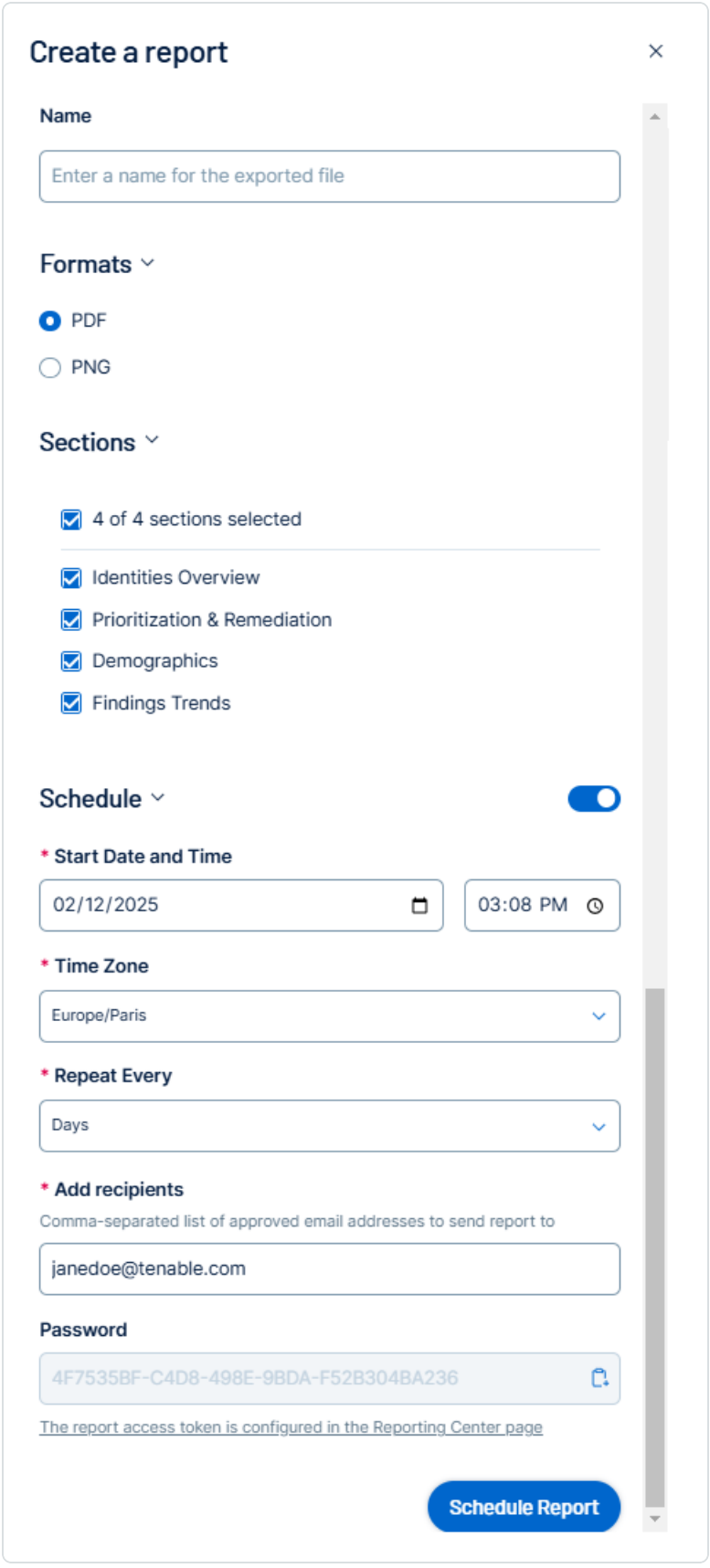
## 建立報告

使用**「深入分析」**頁面上的匯出功能時，系統會開啟一個建立報告的視窗，可用於根據需要自訂並產生詳細的報告。

如要建立報告：

1. 按一下**「深入分析」**頁面右上角的**「匯出」**。

   **「建立報告」**視窗便會顯示。


Create a report
Name
Enter a name for the exported file
Formats
PDF
PNG
Sections
4 of 4 sections selected
Identities Overview
Prioritization & Remediation
Demographics
Findings Trends
Schedule
* Start Date and Time
02/12/2025
03:08 PM
* Time Zone
Europe/Paris
* Repeat Every
Days
* Add recipients
Comma-separated list of approved email addresses to send report to
janedoe@tenable.com
Password
4F7535BF-C4D8-498E-9BDA-F52B304BA236
The report access token is configured in the Reporting Center page
Schedule Report

2. 在「**名稱**」方塊中輸入報告的名稱，讓您和其他人可以知道報告內容為何，例如將報告命名為「每週安全深入分析」或「每月身分趨勢」。
3. 在「**格式**」下方，選擇報告的檔案格式，提供的選項包括 **PDF** (適用於標準文件格式) 或 **PNG** (適用於個別快照或視覺元素)。
4. 選擇要納入報告中的**區段**：
   - **身分概覽**：列出來自不同身分識別提供者 (Identity 360) 的身分清單。
   - **優先順序與修復**：總結重大風險和建議的行動。
   - **群體特徵**：有助於深入瞭解主要身分同類群組。
   - **研究發現趨勢**：呈現持續性分析，反映身分相關弱點和漏洞的模式。
5. 如要設定在指定時間產生報告，請將「**排程**」按鈕啟用，然後完成下列步驟：
   - **開始日期和時間**：設定第一份報告的開始日期和時間。
   - **時區**：選取適當時區，確保排定的時間準確無誤。
   - **重複**：選擇產生報告的頻率 (例如，每週和每月)。舉例來說，如要接收每週報告，請選取「每週」。
   - **新增接收者**：輸入應接收報告的人員的電子郵件地址。若有多個電子郵件地址，請以逗號分隔。
   - **密碼**：在報告中心中設定的唯讀權杖僅供參考。
6. 按一下「**排程報告**」，儲存您的設定並根據指定的時間產生報告。

   報告接收者會收到電子郵件通知，信中提供報告下載網址。

## 存取工作區

登入 Tenable 時，預設會顯示工作區頁面。在**工作區**頁面中，您可以在 Tenable 應用程式之間切換，或將預設的應用程式設定為日後略過**工作區**頁面。

您也可以前往頂端導覽列中的工作區選單，即可從任何頁面在 Tenable 應用程式之間快速切換。

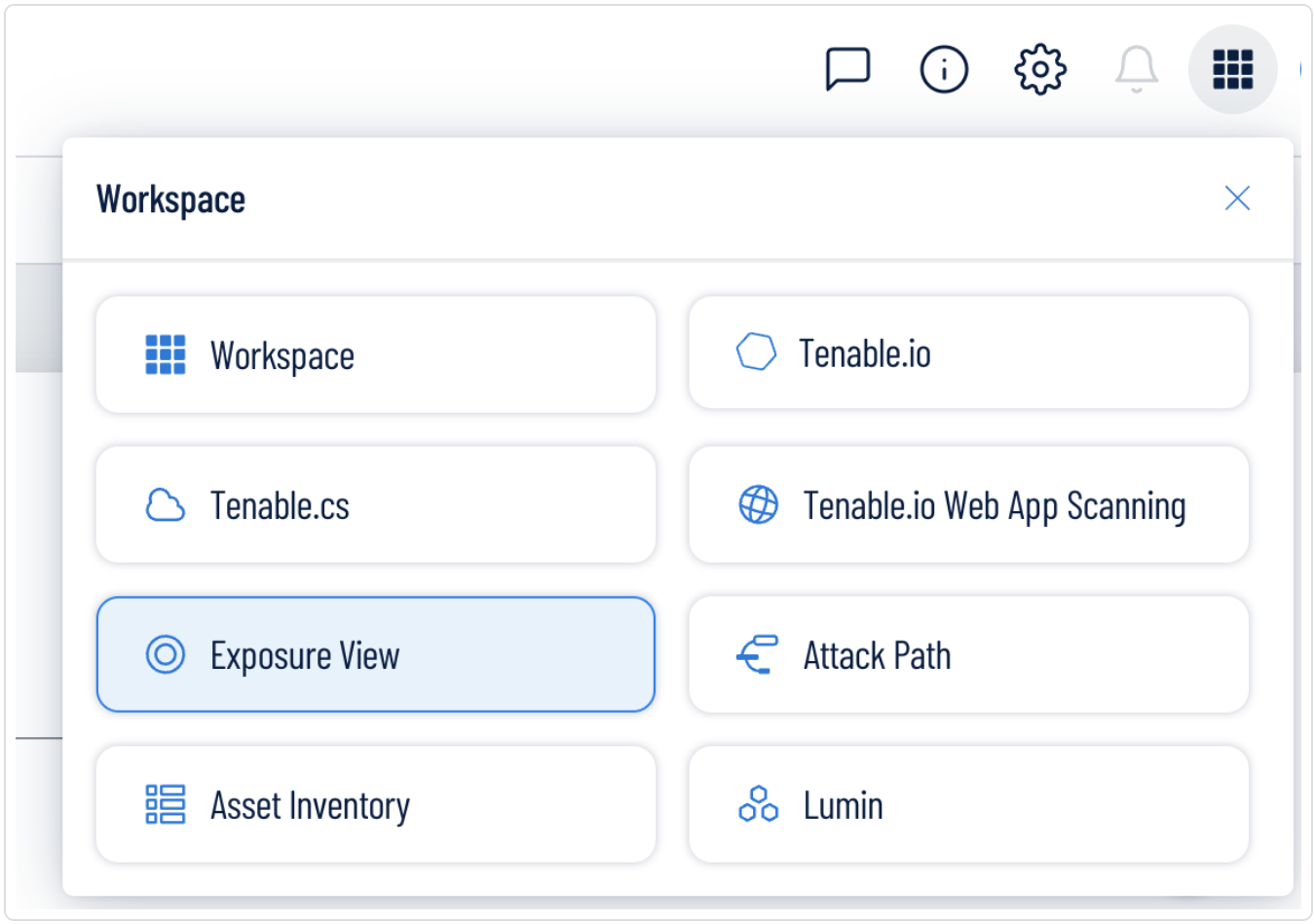
**重要事項：**Tenable 停用過期應用程式的應用程式圖塊。Tenable 會在應用程式到期的 30 天後，從「**工作區**」頁面和功能表移除應用程式圖塊。

## 工作區選單

開啟**工作區**選單的步驟如下：

1. 開啟任何 Tenable 應用程式，並在右上角按一下 按鈕。

   **工作區**選單隨即會顯示。




2. 按一下應用程式圖塊以開啟。

## 工作區頁面

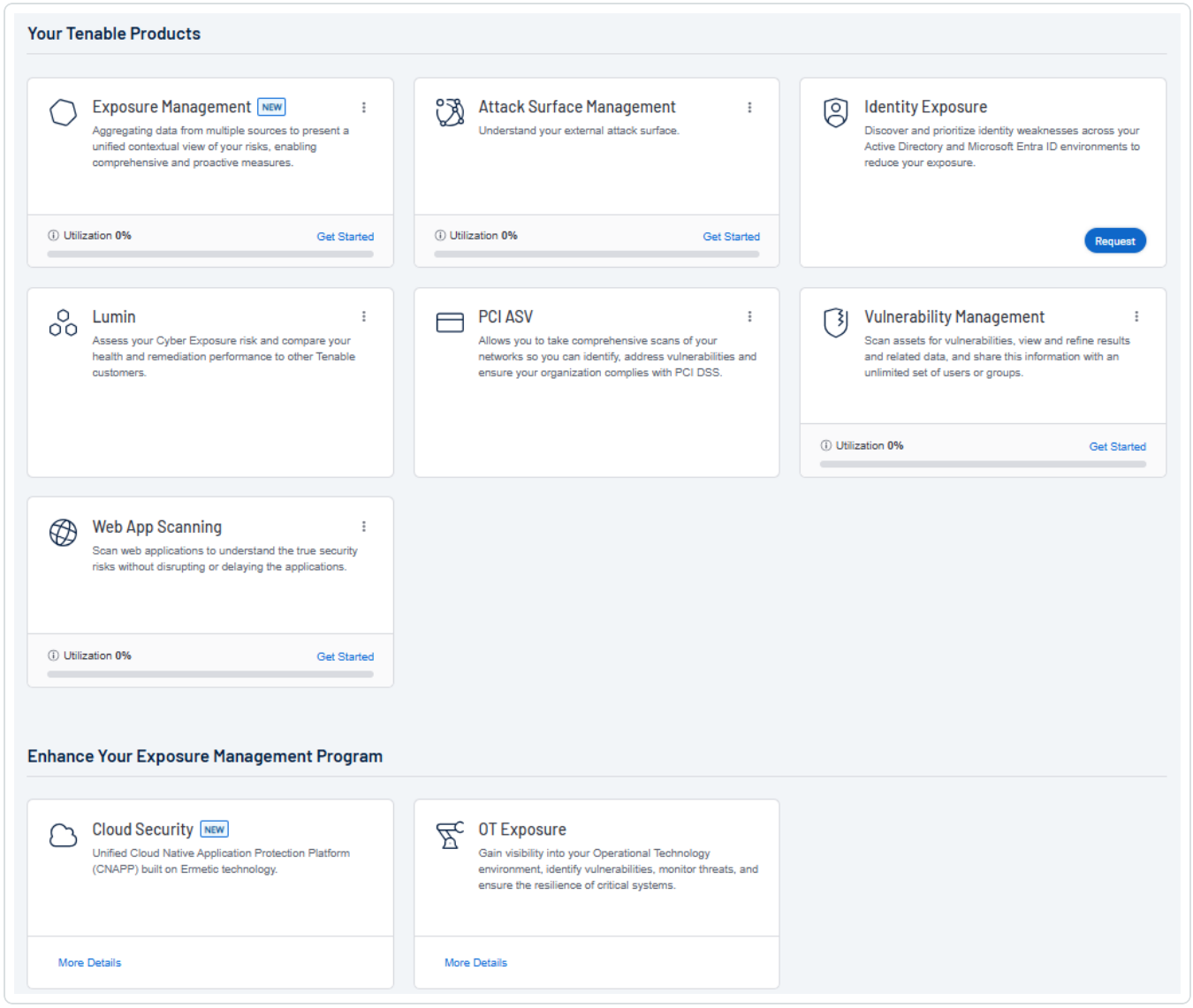
檢視工作區頁面的步驟如下：

1. 開啟任何 Tenable 應用程式，並在右上角按一下 按鈕。

   **工作區**選單隨即會顯示。

2. 在**工作區**選單中，按一下「**工作區**」。

**工作區**頁面隨即會顯示。




在「**工作區**」頁面上，您可以執行下列動作：

- 如果適用，請在圖塊底部檢視應用程式的授權使用率。按一下「**查看更多**」直接前往所選應用程式的「**授權資訊**」頁面。

  **提示：**如需有關 Tenable 授權運作方式，以及各產品中資產或資源授權規則的詳細資訊，請參閱「Tenable 產品授權指南」。

- **設定預設應用程式：**

當您登入 Tenable 時，預設會顯示**工作區**頁面。不過，您可以將預設的應用程式設定為日後略過**工作區**頁面。

> 根據預設，具有**管理員**、**掃描管理員**、**掃描操作員**、**標準**和**基本**角色的使用者可以設定預設的應用程式。如果您擁有其他角色，請聯絡您的管理員，並在**「我的帳戶」**部分要求**管理**權限。如需更多資訊，請參閱自訂角色。

設定預設登入應用程式的步驟如下：

1. 在右上角要選取的應用程式中，按一下⋮按鈕。

   功能表隨即會顯示。

2. 在功能表中，按一下**「設定為預設登入頁面」**。

   此應用程式現在會在您登入時顯示。

- **移除預設應用程式：**

移除預設登入應用程式的步驟如下：

1. 在要移除的應用程式的右上角，按一下⋮按鈕。

   功能表隨即會顯示。

2. 按一下**「移除預設登入頁面」**。

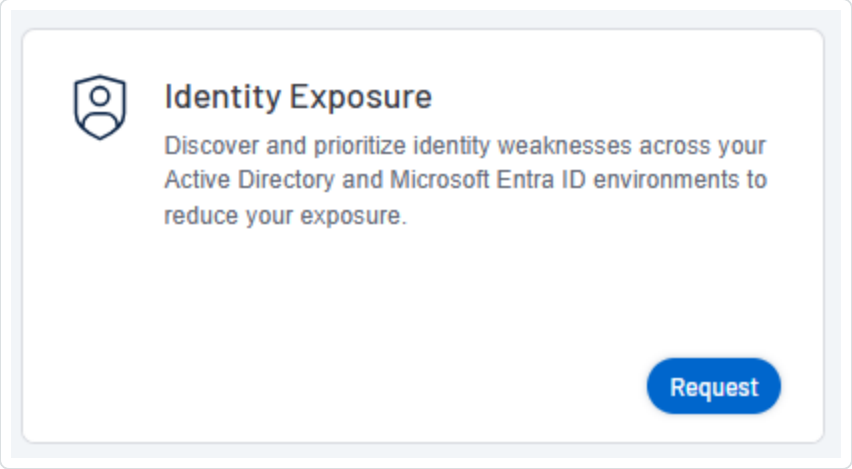
   **「工作區」**頁面現在會在您登入時顯示。

- **要求存取 Tenable 應用程式：**

某些應用程式 (例如 Tenable Identity Exposure) 會要求您請求存取應用程式。您可以透過**「工作區」**頁面直接執行此操作。

如何請求存取 Tenable 應用程式：

1. 在圖塊的右下角，按一下**「請求」**。




您可以直接前往所選應用程式的請求頁面。

## 使用者喜好設定

您可以在 Tenable Identity Exposure 中設定使用者喜好設定。

- 如要選取您的語言：
- 如要選取您的設定檔：
- 如要變更您的密碼：
- 如要選取您的設定檔：

如要設定您的喜好設定：

1. 在 Tenable Identity Exposure 中，按一下右上角的使用者設定檔圖示。

   子功能表會隨即顯示。




2. 選取「**我的帳戶**」。

   「**喜好設定**」頁面會隨即顯示。

**如要選取您的語言：**

a. 在「**語言**」中，按一下下拉式清單的箭頭以選取您喜好的語言。

b. 按一下「**儲存**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新您的喜好設定。使用者介面將顯示您選取的語言。

**如要選取您的設定檔：**

在不同安全性設定檔之間切換，會改變 Tenable Identity Exposure 在儀表板、小工具和追蹤流程上顯示指標設定和資料表示的方式。

a. 在「**喜好設定**」下方，按一下「**設定檔**」。

b. 在「**慣用設定檔**」中，按一下下拉箭頭以選取連接到 Tenable Identity Exposure 後的預設設定檔。

c. 按一下「**儲存**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新您的喜好設定。

如需詳細資訊，請參閱 安全性設定檔。

**如要變更您的密碼：**

**注意**：如果您擁有 Tenable One 授權，則無法使用密碼資訊，在這種情況下是由 Tenable Vulnerability Management 管理您的所有身分驗證設定。如需詳細資訊，請參閱《Tenable Vulnerability Management 使用者指南》中的「存取控制」章節。

a. 在「**喜好設定**」下方，按一下「**憑證**」。

b. 在「**舊密碼**」中輸入舊密碼。

c. 在「**新密碼**」中輸入新密碼。遵守下列密碼複雜性規則，這些規則與 Tenable One 帳戶所需的規則一致：

- 長度必須至少為 12 個字元。
- 必須包含以下字元，且每項至少一個：
  - 大寫字母 (A-Z)
  - 小寫字母 (a-z)
  - 數字 (0-9)
  - 特殊字元 (例如 !、@、#、$)
- 不能包含字串 `verysecure`，以防止重複使用先前的預設密碼 `verySecure1!`。

d. 在「**新密碼確認**」方塊中，重新輸入新密碼。

e. 按一下「**儲存**」。

系統會顯示一則訊息，確認 Tenable Identity Exposure 已變更您的密碼。

**注意**：您無法變更透過 Tenable Identity Exposure 中 LDAP 或 SAML 等外部提供者連線之帳戶的密碼。

**如要管理您的 API 金鑰：**

a. 在「**喜好設定**」下方，按一下「**API 金鑰**」。

「**目前 API 金鑰**」方塊中將顯示您的存取權杖。

b. 您可以執行以下動作：

c. 按一下 圖示，將 API 金鑰複製到剪貼簿以根據需要使用。

d. 按一下**「重新整理 API 金鑰」**，以產生新的存取權杖。

系統會顯示一則訊息，要求您確認。

> **注意**：重新整理 API 金鑰會導致 Tenable Identity Exposure 停用目前的權杖。

如需詳細資訊，請參閱使用公用 API。

## 通知

在 Tenable Identity Exposure 首頁的右上方，鈴鐺圖示和徽章計數通知您有等待確認的攻擊警示和/或曝險警示。當收到新警示時，Tenable Identity Exposure 會增加通知徽章計數。

| | | |
|---|---|---|
|  | **藍色** | 曝險警示 |
| | **紅色** | 攻擊警示 |

如要顯示警示：

1. 在 Tenable Identity Exposure 中，按一下鈴鐺圖示。

**「警示」**窗格會隨即開啟。

2. 執行下面的其中一項動作：

- 按一下**「曝險警示」**索引標籤以顯示曝險警示。
- 按一下**「攻擊警示」**索引標籤以顯示攻擊警示。

相關警示清單會隨即顯示。

如要檢視與警示關聯的事件：

1. 從清單中選取一個警示，然後按一下**「動作」>「查看異常情況」**。

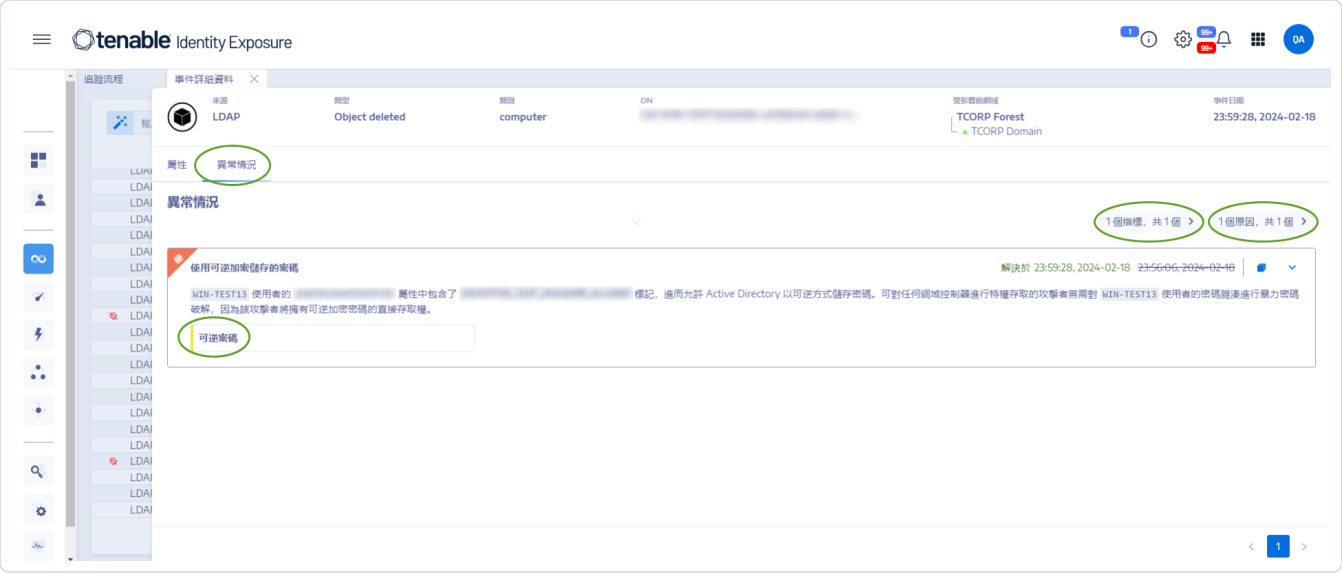
事件詳細資料窗格會隨即開啟，其中包含以下資訊：

- 來源 (事件收集器)
- 物件類型

- 檔案
- 路徑
- 受影響的網域
- 日期
- 具有事件發生時的值和目前值的屬性清單

2. 按一下**「異常情況」**索引標籤。

   **「異常情況」**窗格會隨即開啟，其中包含與事件關聯的異常情況清單。




3. 按一下**「n/n 指標」**以顯示觸發警示的曝險指標窗格。
4. 按一下**「n/n 原因」**以顯示警示的原因。
5. 按一下箭頭以展開或摺疊警示資訊。
6. 按一下指標名稱以顯示指標詳細資料頁面。

如要封存警示：

檢視警示後，可將其封存。

1. 在**「警示」**窗格的警示清單中選取要封存警示的核取方塊。
   - 或者，您可以按一下窗格底部**所選 n/n 個物件**的核取方塊，以大量選取所有警示。

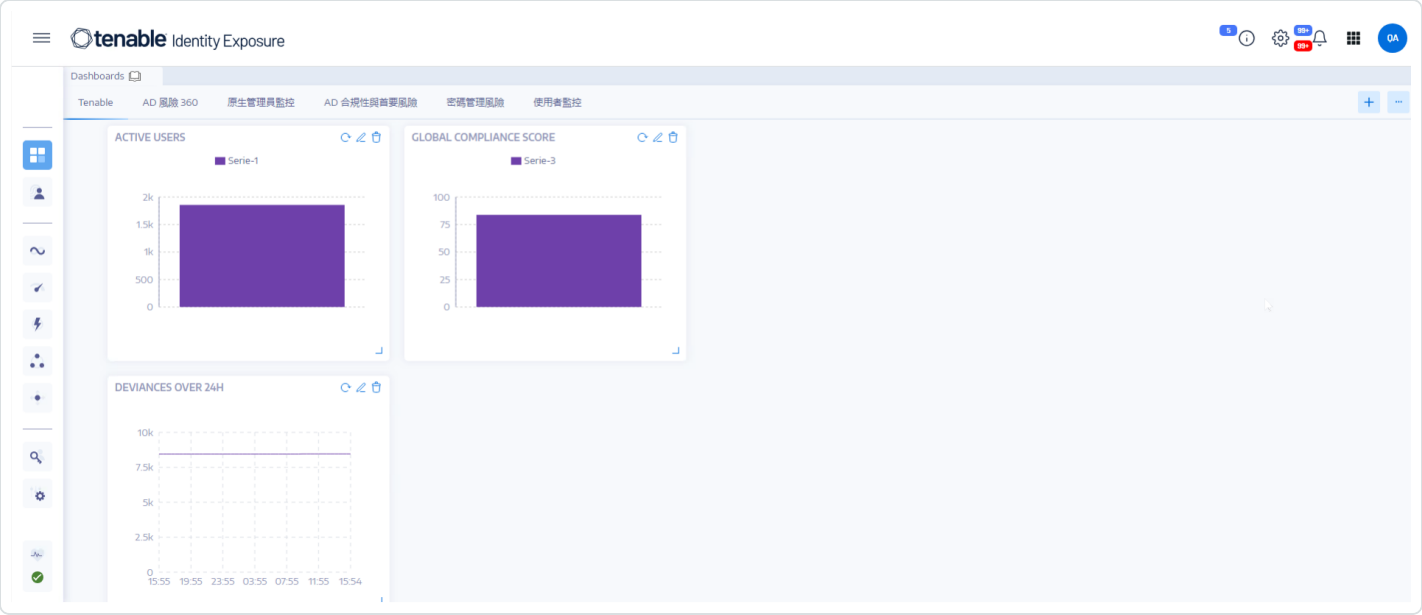
2. 在窗格底部，按一下「**選取動作**」>「**封存**」。

3. 按一下「**確定**」。

## 儀表板

透過儀表板，您可以將影響 Active Directory 安全的資料和趨勢視覺化。您可以使用小工具自訂儀表板，根據您的要求顯示圖表和計數器。

Tenable Identity Exposure 儀表板可作為貴組織 Active Directory (AD) 安全性的即時指揮中心，提供身分狀況的全面概覽 (例如即時集中式檢視畫面)，並會重點顯示嚴重弱點、精確指出潛在的攻擊媒介，以及啟用主動風險緩解措施。




## 儀表板主要功能

- **一目了然的概覽**：您可快速查看安全性狀態，且系統會醒目顯示合規性評分、主要風險和使用者活動趨勢等關鍵指標。
- **資料詳盡**：互動式小工具會按嚴重性、使用者類別和其他相關條件細分風險因素，可供您深入探究特定領域。
- **可自訂的焦點**：使用預先建立的範本或製作自己的版面配置，根據您的優先順序設計個人化儀表板。舉例來說，可以針對經常出現的曝險指標 (IoE) 建立常見錯誤設定儀表板：

    - 確保 SDProp 一致性
    - 不正當使用者管理的網域控制器
    - 危險的 Kerberos 委派作業
- **即時監控**:透過持續更新和警示,隨時掌握新興威脅以及可疑活動。
- **可據以行動的見解**:取得實用的修復建議,並根據嚴重性和潛在影響排定優先順序。

## 小工具

儀表板中的小工具可用來以橫條圖、折線圖和計數器的形式視覺化您的 Active Directory 資料。您可以自訂小工具以顯示特定資訊,並透過拖曳重新確定其在儀表板上的位置。

您可以將小工具新增到新建立的儀表板或現有儀表板。

**如要將小工具新增到儀表板:**

1. 在 Tenable Identity Exposure 中,按一下 或「**儀表板**」(此頁面在 Tenable Identity Exposure 中也會預設開啟)。
2. 在「儀表板」窗格中,選取「儀表板」索引標籤。
3. 您可以執行下列任一動作:
    - 如果儀表板為空,請按一下「**新增小工具**」。
    - 如果儀表板已包含小工具,請依序按一下 > 右上角的「**新增小工具至目前儀表板**」。

      「**新增小工具**」窗格會隨即開啟。
4. 按一下圖塊以選取下方的任一選項:
    - 長條圖
    - 折線圖
    - 計數器

5. 在「**小工具的名稱**」方塊中輸入小工具的名稱
6. 在「**小工具設定**」下的「**資料類型**」方塊中，按一下下拉式清單中的箭頭以選擇下面的一個選項：
    - 使用者計數：網域的使用中使用者數量。
    - 異常情況計數：偵測到的異常情況或安全缺口的數量。
    - 合規性分數：Tenable Identity Exposure 以偵測到的異常情況數量及其嚴重性等級作為考量，所計算得出的分數 (介於 0-100 之間)。
    - (折線圖) 持續時間：按一下下拉式清單上的箭頭，選取要顯示的持續時間。

7. 在「**資料集設定**」下方：

| 資料集設定 | |
|---|---|
| **狀態** (使用者計數) | 選擇「使用中」、「非使用中」或「全部」。 |
| **指標** | a. 按一下「**指標**」以選取一個或多個指標。<br>「**曝險指標**」窗格會隨即開啟。<br>b. 從清單中選取一個或多個指標。或者，您還可以：<br>■ 在搜尋方塊中輸入指標名稱。<br>■ 選取所有指標。<br>■ 選取特定嚴重性層級 (嚴重、高度、中度或低度) 的所有指標。<br>c. 按一下「**篩選選取的項目**」。 |
| **網域** | a. 按一下「**網域**」以選取一個或多個網域。<br>「**樹系和網域**」窗格會隨即開啟。<br>b. 從清單中選取一個網域。或者，您還可以：<br>■ 在搜尋方塊中輸入網域名稱。<br>■ 選取所有網域。<br>c. 按一下「**篩選選取的項目**」。 |

8. 在「**資料集名稱**」中輸入資料集的名稱。
9. 選取小工具的網域。

   或者，您還可以在搜尋方塊中輸入網域名稱。
10. 按一下「**篩選選取的項目**」。
11. 或者，您可以按一下「**新增資料集**」，為小工具新增另一個具有不同選項的資料集。
12. 按一下「**新增**」。

    系統將顯示一則訊息，確認 Tenable Identity Exposure 已新增小工具。

**如要修改小工具：**

1. 在 Tenable Identity Exposure 中，按一下「**儀表板**」。
2. 選取包含待修改小工具的儀表板。
3. 選取此小工具。
4. 按一下小工具右上角的 圖示。

   「**修改小工具**」窗格會隨即開啟。
5. 視需要進行修改。
6. 按一下「**編輯**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新小工具。

**如要重新整理小工具：**

1. 選取此小工具。
2. 按一下小工具右上角的 圖示。

   小工具會重新整理。

**如要刪除小工具：**

1. 在 Tenable Identity Exposure 中，按一下「**儀表板**」。
2. 選取包含待刪除小工具的儀表板。
3. 選取此小工具。
4. 按一下 圖示。

   「移除小工具」窗格會隨即開啟。系統會顯示一則訊息，要求您確認刪除。
5. 按一下「**確定**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已從儀表板中刪除此小工具。

## 另請參閱

- 儀表板

## 曝險中心

**曝險中心**是 Tenable Identity Exposure 的一項功能，可增強貴組織的身分安全狀態。此功能可識別整個身分風險破綻的脆弱環節和錯誤設定，涵蓋基礎身分系統 (例如 Entra ID) 以及這些系統內的身分。

此功能的使用者體驗圍繞三個相互關聯的概念展開：**曝險概覽**、**曝險情況**和**研究發現**。Tenable Research 透過**新的安全引擎**和專門開發的曝險指標 (IoE) 來支援這些概念，以驅動其功能。

- **曝險概覽**與 Tenable Identity Exposure 中的曝險指標 (IoE) 檢視類似，代表攻擊者可惡意利用的潛在脆弱環節或錯誤設定。這些是安全風險的一般描述，例如「非使用中的使用者帳戶」或「設定錯誤的存取權限」。曝險指標 (IoE) 會主動醒目提示曝險的區域，讓組織對於其安全狀態有全面的瞭解。
- **曝險情況**指的是產生這些一般脆弱環節的特定情形。例如，一般脆弱環節「非使用中的使用者帳戶」可能有特定的情況，例如「在市場行銷部門中有使用者帳戶超過 30 天沒有活動」。
- **研究發現**是針對各種身分資料來源中的實際資料分析曝險情況的結果。研究發現呈現受影響資產上的安全問題，由使用者、群組和角色等屬性唯一識別。舉例來說，如果使用者帳戶在曝險情況中的閒置時間超過指定臨界值，則系統會將其標記為研究發現。

處理程序以脆弱環節程式庫開始，透過掃描持續套用至您的身分識別提供者。

Tenable Research 會提供預設脆弱環節，並持續更新這些脆弱環節，以符合威脅版圖。這些針對您在曝險情況中的特定需求量身定做的脆弱環節會產生研究發現，然後連同嚴重性評等和修復準則一起呈現。藉由利用此功能，Tenable Identity Exposure 可協助組織主動緩解安全性風險。

> **注意**：曝險中心僅包含新安全引擎支援的脆弱環節。從舊版安全引擎產生的曝險指標 (IoE) 不會在此處顯示。不過，目前的 Active Directory (AD) 曝險指標 (IoE) 仍可在 Tenable Identity Exposure 中的「曝險指標」頁面上查看。

## 先決條件

- 若要使用**曝險中心**，您必須在 Tenable Identity Exposure 設定中啟用該功能。
- 如需指示，請參閱啟用 Identity 360、曝險中心和 Microsoft Entra ID 支援。

## 另請參閱

- 曝險概覽
- 曝險情況

## 曝險概覽

Tenable Identity Exposure 有助於您全面瞭解多種身分識別提供者的脆弱環節和錯誤設定，包括 Active Directory (AD) 和 Entra ID。

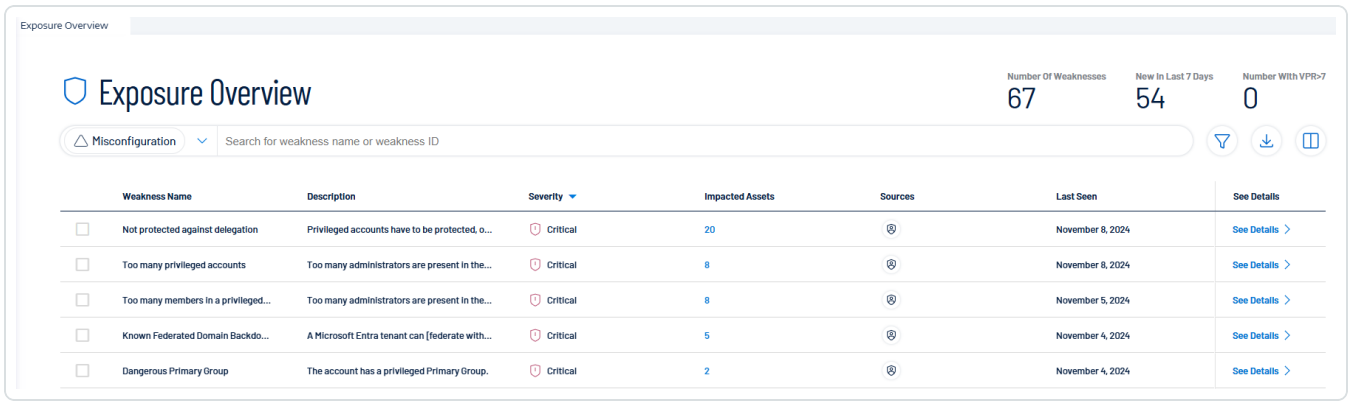
藉由持續掃描並識別特權帳戶、密碼原則、委派設定等項目中的重大脆弱環節，Tenable Identity Exposure 讓組織能夠主動解決安全缺口。

此概覽可讓您根據嚴重性、受影響的資產和最近偵測到的問題排列問題的優先順序，確保透過集中且有效的方式進行身分安全管理。

若要存取**曝險概覽**頁面：

1. 在 Tenable Identity Exposure 的左側導覽窗格中，按一下曝險中心圖示 。
2. 在子功能表中，按一下**曝險概覽**。

   **曝險概覽**頁面隨即顯示。



## 標頭資訊

- **脆弱環節數目**：顯示偵測到的脆弱環節總數。
- **過去 7 天的新增脆弱環節**：醒目提示在過去一週內偵測到的新脆弱環節。

## 脆弱環節清單

脆弱環節清單中會顯示以下各欄：

- **脆弱環節名稱**：列出偵測到的特定脆弱環節或錯誤設定。範例：「未防範委派工作」、「特權帳戶太多」等。
- **描述**：提供問題的簡短說明。範例：「必須保護特權帳戶...」、「系統管理員過多...」。
- **嚴重性**：顯示每個脆弱環節的關鍵性 (嚴重、高、中、低)。
- **受影響的資產**：顯示受每個脆弱環節影響的資產數量。
- **來源**：偵測到資料的系統或平台。此資料可能來自多個產品。
- **上次查看時間**：顯示上次偵測或報告每個脆弱環節的時間。範例：「2024 年 9 月 10 日」、「2024 年 9 月 29 日」。
- **查看詳細資料**：可讓您檢視每個脆弱環節的詳細資訊。

> **提示**：「查看詳細資料」箭頭會將您帶至 Tenable Inventory。如需有關特定脆弱環節的詳細資訊，請參閱 Tenable Inventory 中的脆弱環節。

> **注意**：曝險概覽功能目前會根據**預設的 Tenable 設定檔**顯示弱點相關資料，不會自動反映**您在其他設定檔中列入白名單的 AD 物件的異常情況狀態**。
>
> 因此：
>
> - 如果您已將特定曝險指標 (例如「原生系統管理群組成員」) 的 **AD 物件列入白名單，當預設設定檔將其識別為異常時，曝險概覽仍會將其標記為安全性弱點**。
> - 即使物件已在不同的設定檔下列入白名單，這仍可能會造成問題尚未解決的印象。
> - 如果根據曝險概覽顯示採取修復動作 (例如移除群組成員資格)，則物件將從檢視畫面中消失，但若該物件已在其他地方列入白名單，可能沒有必要採取修復動作。

## 搜尋、篩選、匯出和欄顯示選項

## 篩選器

**曝險概覽**中的篩選器函式可透過套用特定準則的方式，縮小或調整顯示的資料範圍。

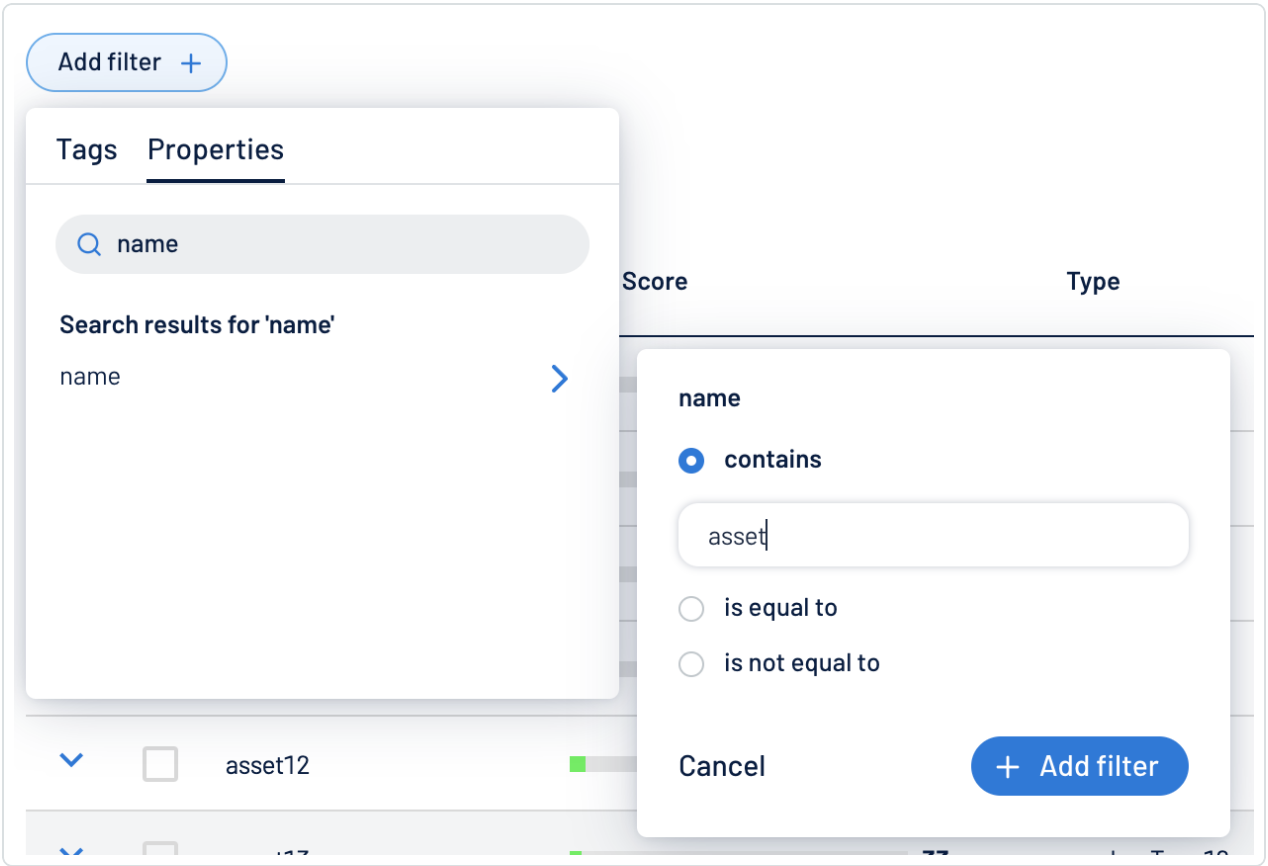
若要將篩選器套用至脆弱環節清單：

1. 在**曝險概覽**頁面的標頭中，按一下 圖示。

   「新增篩選器」按鈕會隨即顯示。

2. 按一下**「新增篩選器 +」**。

   功能表隨即會顯示。




3. 執行下面的其中一項動作：

- 如要依標籤搜尋脆弱環節清單，請按一下**「標籤」**(僅適用於 Tenable One 授權，且在 Tenable Inventory 中進行管理。)
- 如要依屬性搜尋脆弱環節清單，請按一下**「屬性」**。

4. 在搜尋方塊中輸入想要使用的搜尋準則。

   Tenable Inventory 會根據您的準則填入選項清單。

5. 按一下您要用來篩選脆弱環節清單的標籤或屬性。

   功能表隨即會顯示。

6. 選取如何套用篩選器。例如，如果您要搜尋名稱為「Weakness14」的脆弱環節，請選取「包含」單選按鈕，並且在文字方塊中輸入「Weakness14」。

7. 按一下**「新增篩選器」**。

   篩選器會顯示在脆弱環節清單上方。

8. 在要套用的每個其他篩選器中重複上述步驟。

9. 按一下**「套用篩選器」**。

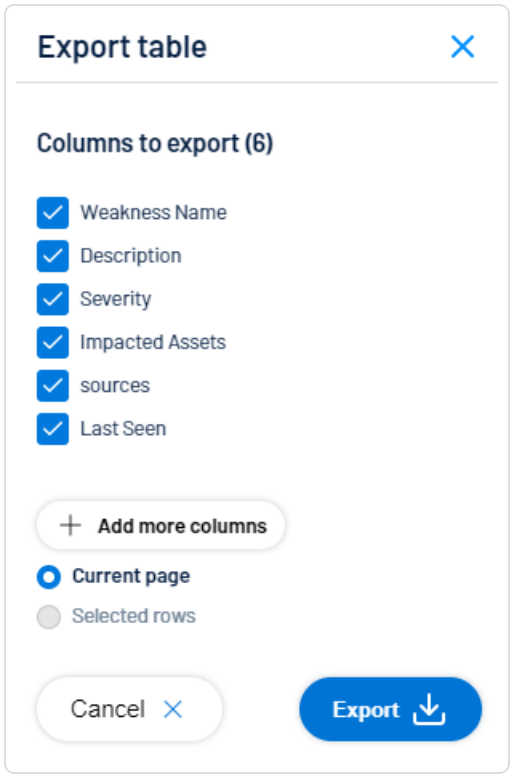
   頁面會依指定的準則篩選身分清單。

### 匯出

您可以將表格中顯示的資料匯出至 Excel 檔案。

若要匯出資料：

1. 在**曝險概覽**頁面的標頭中，按一下 圖示。
2. 在「匯出表格」視窗中選取要匯出的欄。您可以選擇匯出目前頁面或所選取的列。




3. 按一下「**匯出**」。

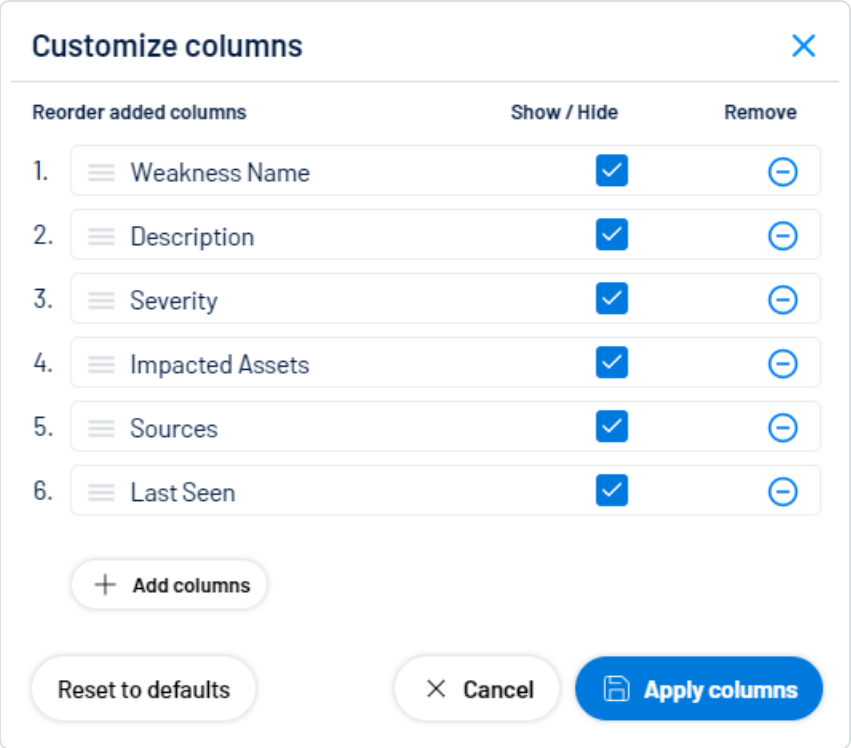
### 自訂欄

您可以新增、移除欄或重新排列欄，根據自己的喜好調整檢視。如果您想要還原任何變更，可以隨時重設為預設設定。

若要自訂欄顯示：

1. 在**曝險概覽**頁面的標頭中，按一下 。

   「自訂欄」視窗會隨即顯示。




2. 選擇性：

   - 在「**重新排列新增欄**」區段中，按一下並拖曳任何欄名稱，即可重新排列欄。
   - 在「**顯示/隱藏**」區段中選取/取消選取核取方塊，即可顯示或隱藏表格中的欄。
   - 在「**移除**」區段中，按一下 (-) 將某欄從表格中永久移除。
   - 若要將欄新增至表格，請按一下「**新增欄**」。

     「**新增欄至表格**」視窗會隨即顯示。

     - (選擇性) 使用搜尋列搜尋欄屬性。

       欄屬性清單會根據您的搜尋查詢進行更新。

     - 選取要新增至表格的任何一欄或多欄旁邊的核取方塊。
     - 按一下「**新增**」。

       欄會出現在「自訂欄」視窗中。

3. 按一下「**套用欄**」。

   Tenable 會將您的變更儲存在表格的欄中。

## 預設欄

欄的預設配置可確保金鑰資料易於存取，同時又能提供自訂彈性。

- **脆弱環節名稱**
- **說明**
- **嚴重性**
- **受影響的資產**
- **來源**
- **上次出現時間**

如要重設為預設欄：

- 按一下**「重設為預設值」**，將所有欄重設為其預設值。

## 另請參閱

- 曝險情況

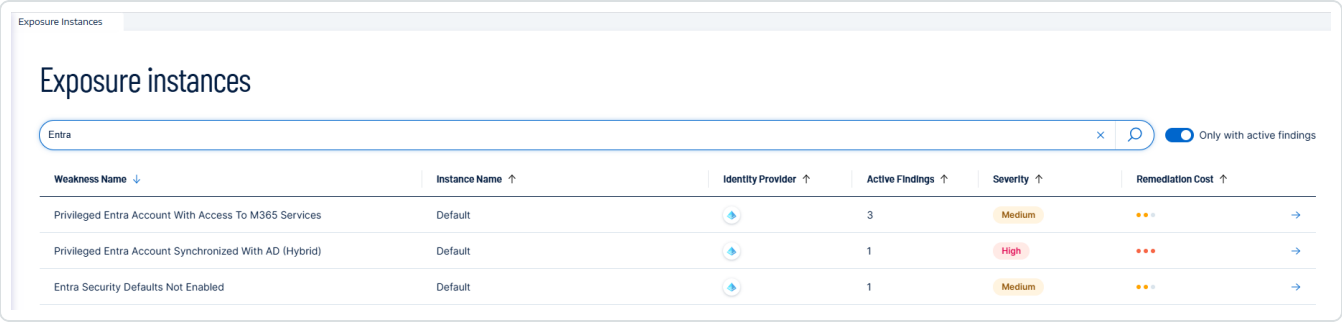
# 曝險情況

**曝險情況**頁面會顯示已識別脆弱環節的特定執行個體清單。

如要存取**曝險情況**頁面：

1. 在 Tenable Identity Exposure 的左側導覽窗格中，按一下曝險中心圖示 。
2. 在子功能表中，按一下**「曝險情況」**。

   **「曝險情況」**頁面隨即顯示。



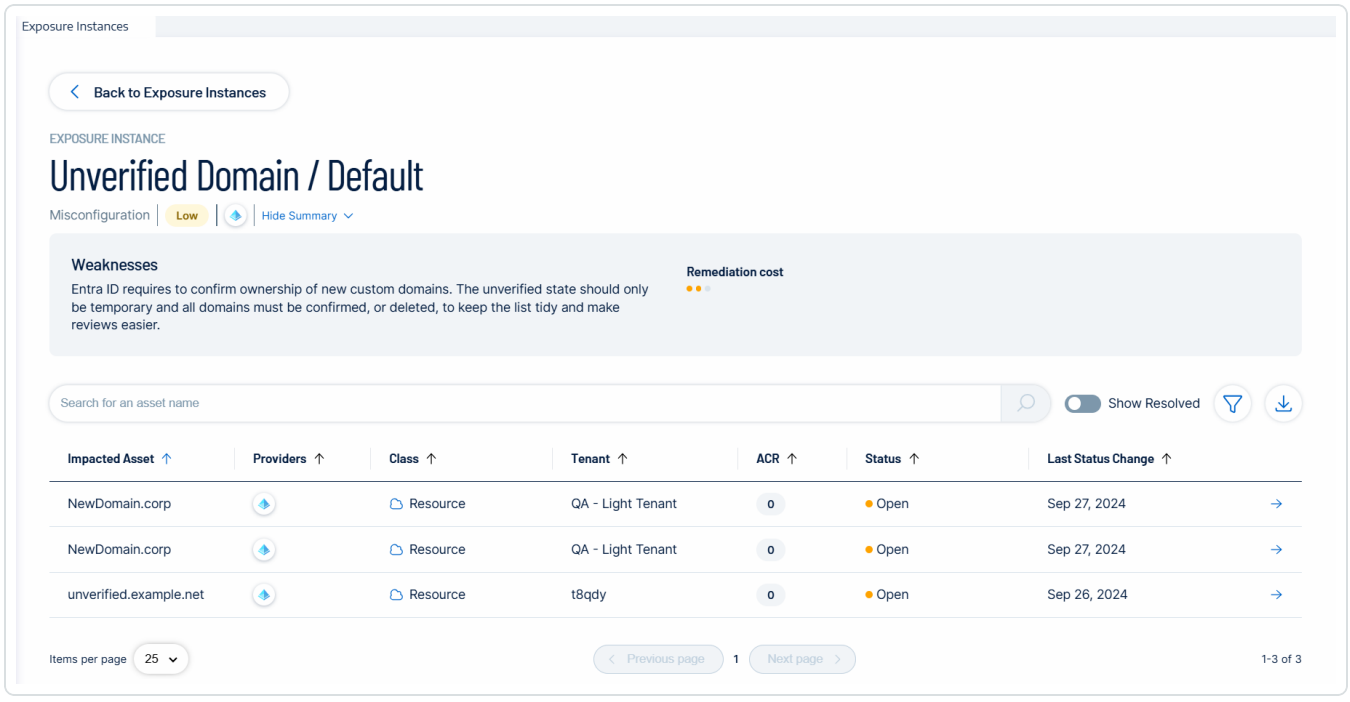
## 一般資訊

此頁面會顯示一個表格，其中列出了所有曝險情況及其對應資訊：

- **脆弱環節名稱**：脆弱環節的一般名稱
- **執行個體名稱**：此執行個體的特定名稱
- **身分識別提供者**：於其中產生資料的身分識別提供者名稱
- **作用中研究發現數目**
- **嚴重性**：指出此脆弱環節的關鍵性
- **修復成本**：指出解決此脆弱環節 (低、中、高) 所需執行的工作

## 詳細資訊

- 若要深入瞭解每個曝險情況的詳細資料，請按一下此行結尾的箭頭。這樣會開啟另一個頁面，其中包含每個曝險情況的下列資訊：




### 標題資訊

標頭會顯示下列資訊：

- 脆弱環節類型，例如錯誤設定和執行個體名稱 (預設)
- 嚴重性：脆弱環節的嚴重性 (低、中、高)
- 脆弱環節描述：脆弱環節的詳細說明及其造成安全性風險的原因。
- 預估修復成本

**受影響的資產**

受影響的資產是指受到曝險情況影響的資產及其對應的詳細資料：

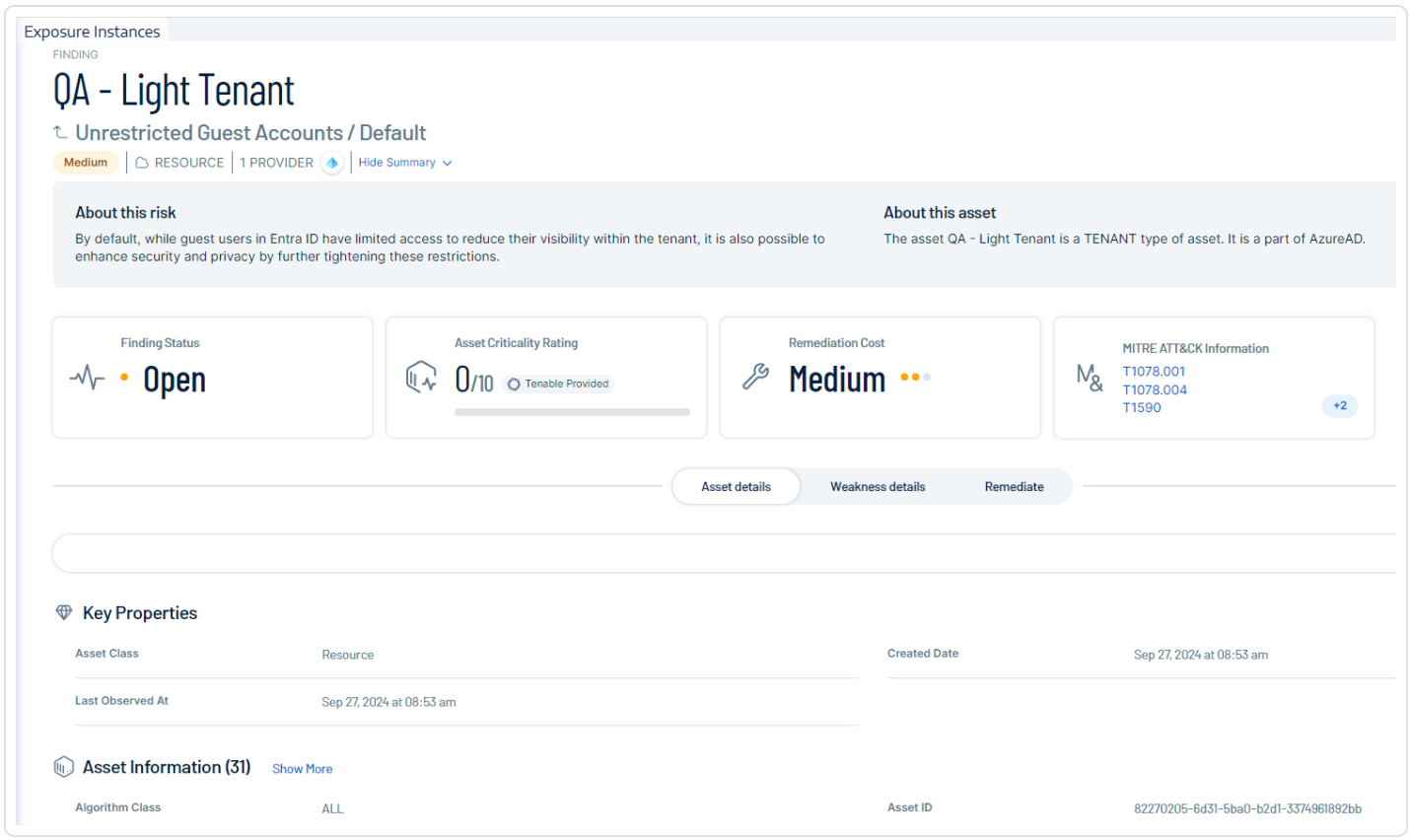
- 提供者
- 資產類型
- 租用戶：「租用戶」一詞泛指身分識別提供者 (IDP) 租用戶，即使每個 IDP 對此概念可能有其特定名稱 (例如 Entra ID 租用戶、AD 網域等)。
- ACR 分數 (Asset Criticality Rating)
- 狀態：未解決 (Open)、已解決 (Resolved) 或重新出現 (Resurfaced)
- 上次狀態變更日期

**排除項目**

如需完整詳細資訊，請參閱「曝險情況排除項目」。

## 分析研究發現

如要檢視與受影響資產相關的研究發現，請按一下此行結尾的箭頭。如此會開啟另一個頁面，其中包含此研究發現相關資訊：




## 標頭資訊

**研究發現**頁面中的標頭會顯示下列資訊：

- **租用戶名稱**
- **脆弱環節名稱**和相關的曝險情況名稱
- **嚴重性**：脆弱環節的嚴重性 (低、中、高)
- **資產類別**：資產所屬的類別。如需詳細資訊，請參閱資產類別。
- **提供者**：身分識別提供者
- 曝險情況**摘要**
  - 「關於此風險」提供此脆弱環節的簡短描述
  - 「關於此資產」指出資產類型 (例如「租用戶」) 和身分識別提供者

## 研究發現狀態

研究發現可顯示下列狀態：

**注意**:根據預設,此頁面僅顯示未解決和重新出現的研究發現。

- **未解決**:表示需要注意的作用中安全問題。已偵測到此脆弱環節,但尚未解決。
- **已解決**:此狀態表示先前發現的脆弱環節已成功解決。安全問題不再存在。

  **提示**:啟用「顯示已解決的弱點」切換開關顯示已解決的研究發現。

- **再次出現**:再次偵測到先前已解決的問題時,會出現此狀態。這可能表示此解決方案是暫時的,或問題再次發生。
- **已排除**:當您套用篩選器以顯示已套用排除項目的受影響資產時,系統將顯示此狀態。

### Asset Criticality Rating (ACR)

Tenable 會給您身分識別提供者上的每項資產指派一個 ACR,以 1 到 10 的整數表示資產的相對關鍵性。ACR 越高表示重要程度較高。如需詳細資訊,請參閱 ACR。

### 修復成本

修復成本是指解決特定脆弱環節所需的預估工作量,並綜合考慮勞動力、複雜性和潛在的財務費用。

它以三個層級表示:

- 低:相對容易修復,需要最少的時間和資源。
- 中:需要執行中等程度的工作才能解決的問題。
- 高:可能需要耗費大量時間、資源或變更才能解決的複雜問題。

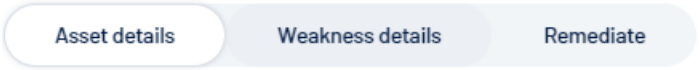
此分類有助於根據問題的嚴重性和修復問題所需的工作量,按優先順序排定要先解決的問題。

### MITRE ATT&CK 資訊

來自 MITRE ATT&CK 架構的相關技術。

## 研究發現詳細資料

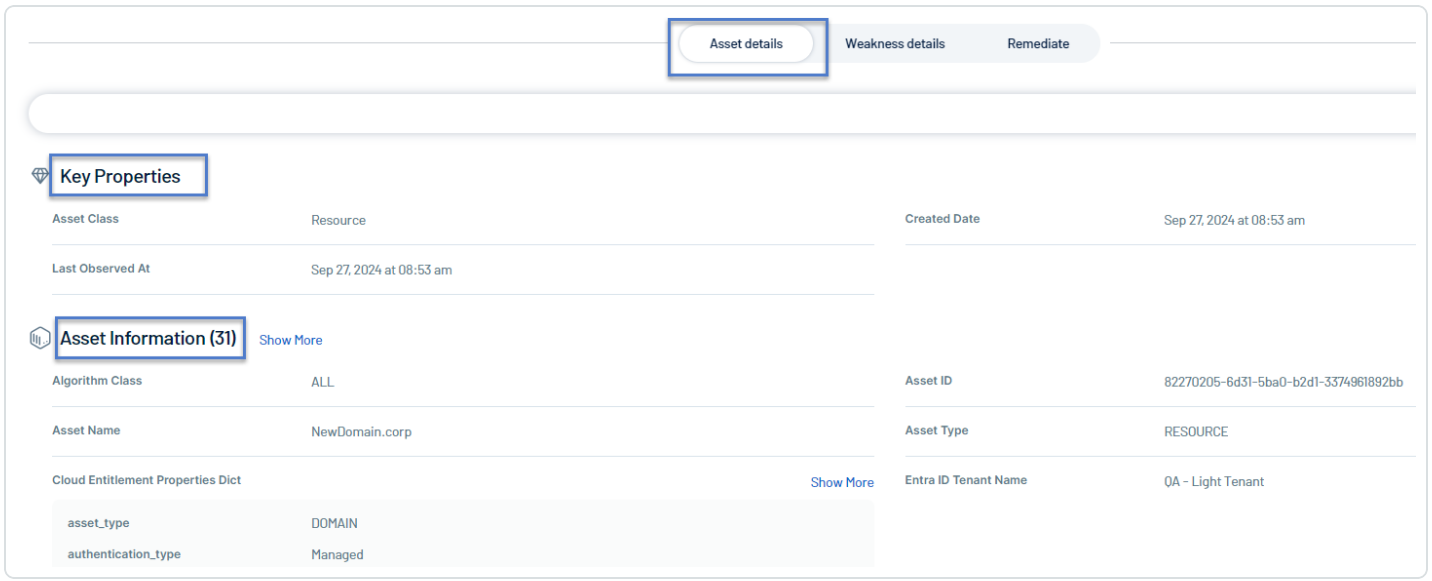
在標頭下方,「研究發現」頁面會顯示三個索引標籤,醒目提示下列資訊:




- 按一下其中任何一個索引標籤以展開詳細資料。

## 資產詳細資料

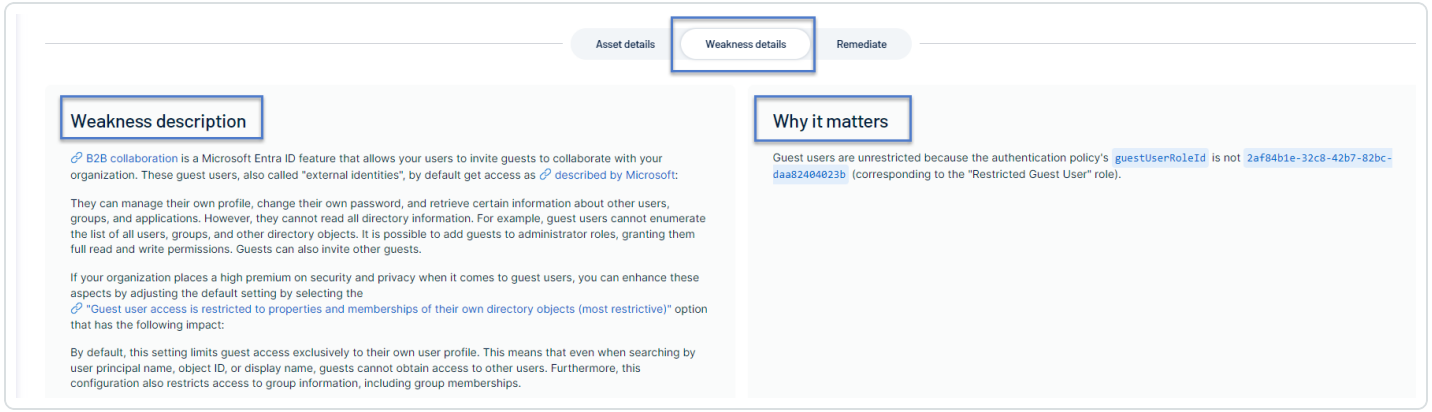
「資產詳細資料」是「研究發現」頁面中預設開啟的索引標籤。




這部分提供下列資訊：

- **主要屬性**：此區段提供有關資產的高階詳細資訊，例如資產類別。同時也會顯示資產建立日期和上次觀察的時間。
- **資產資訊**：此區段包含與身分識別提供者提供之資訊相關的更詳細的資產屬性。

## 弱點詳細資料

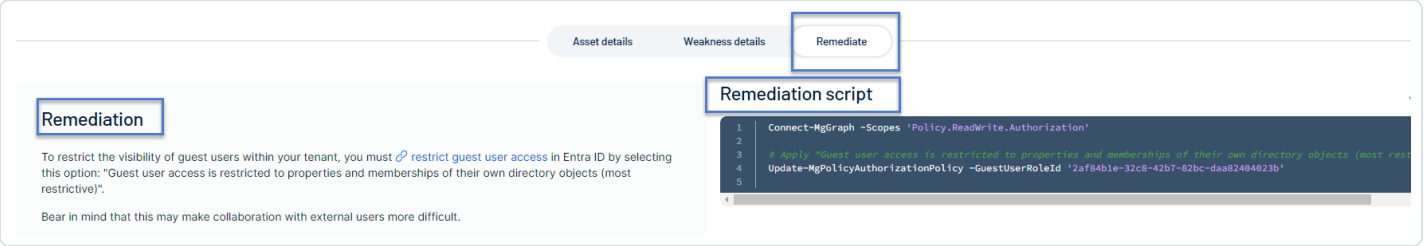


這部分提供下列資訊：

**脆弱環節描述**：此區段會簡單扼要地說明脆弱環節會造成安全性風險的原因，以協助您瞭解和解決脆弱環節。

**重要意義**：此區段會指出出現此脆弱環節的特定情況，以便您集中精力修復此脆弱環節。

## 修復




此區段將指導您完成修復脆弱環節的過程。

**修復準則**：文字準則提供有關如何解決已識別脆弱環節的逐步指示。這些準則通常包括：

- 有關如何更正脆弱環節的詳細指示。
- 防範未來發生類似問題的最佳做法。
- 相關說明文件或其他資源的連結。

**修復指令碼**：針對某些研究發現，可能會提供自動化修復指令碼。

> **注意**：由於產品無法自動化修復，或者可能涉及實作組織變更，而不是簡單的技術修正，因此可能無法使用指令碼。在這種情況下，您會看到一則訊息，指出只能手動修復此研究發現，此時您應該遵循文字準則。

執行指令碼之前：

- 檢閱其內容以瞭解將進行哪些變更。
- 視需要針對您的環境進行調整。
- 如果可能，請在非生產環境中測試指令碼。
- 確保您具有執行指令碼所需的權限。

> **提示**：儘管修復指令碼可節省時間，但是請務必謹慎行事，並確保瞭解對環境進行任何自動化變更的影響。

若要執行修復指令碼：

您可以開啟 PowerShell 主控台，貼上修復指令碼並直接執行，或者如果您願意，也可以將其下載為 .ps1 檔案後執行。

1. 在「修復」索引標籤中尋找「下載指令碼」按鈕。
2. 按一下此按鈕可下載修復指令碼。
3. 像執行任何 PowerShell 指令碼一樣執行檔案。

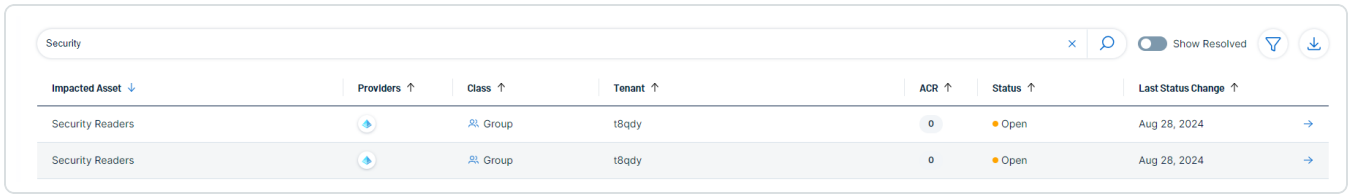
## 搜尋、篩選和匯出選項

### 搜尋

- 您可以按照**脆弱環節名稱**、**執行個體名稱**或**嚴重性**，在曝險情況清單中搜尋特定執行個體。
  - 在「搜尋」方塊中，輸入搜尋字詞 (例如「Entra」)。清單會顯示符合搜尋準則的所有執行個體。




- 您可以搜尋特定受影響資產的曝險情況。
  - 在「搜尋」方塊中，輸入**資產名稱** (例如「安全性」)。清單會顯示符合搜尋準則的所有執行個體。




### 篩選器

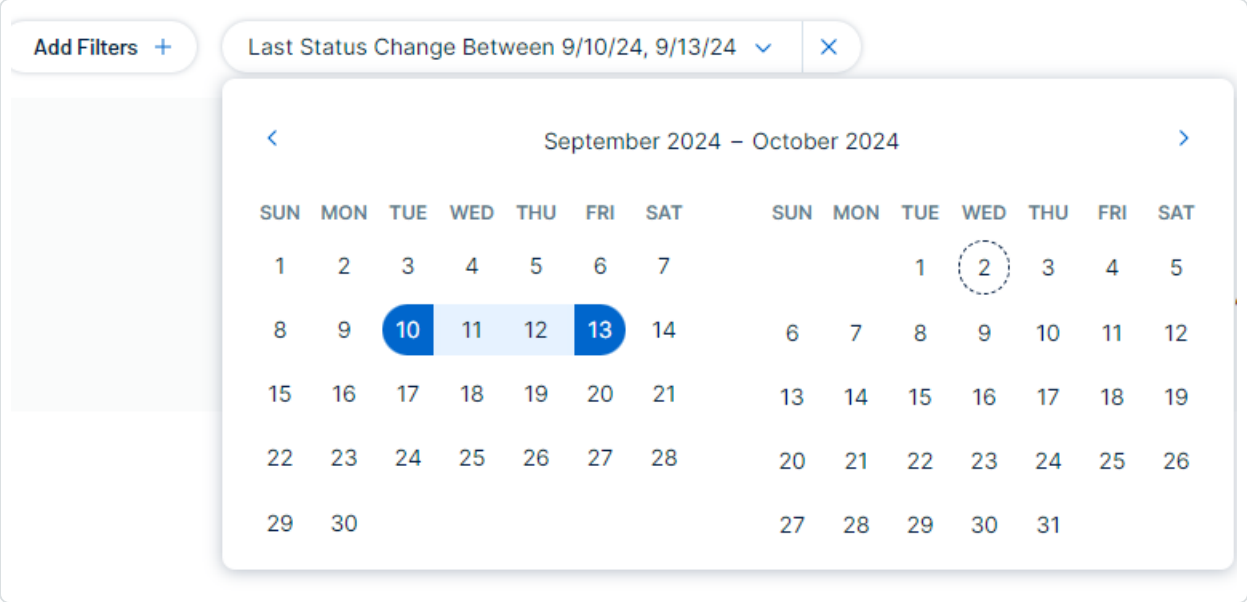
若要篩選脆弱環節清單：

1. 按一下 圖示。

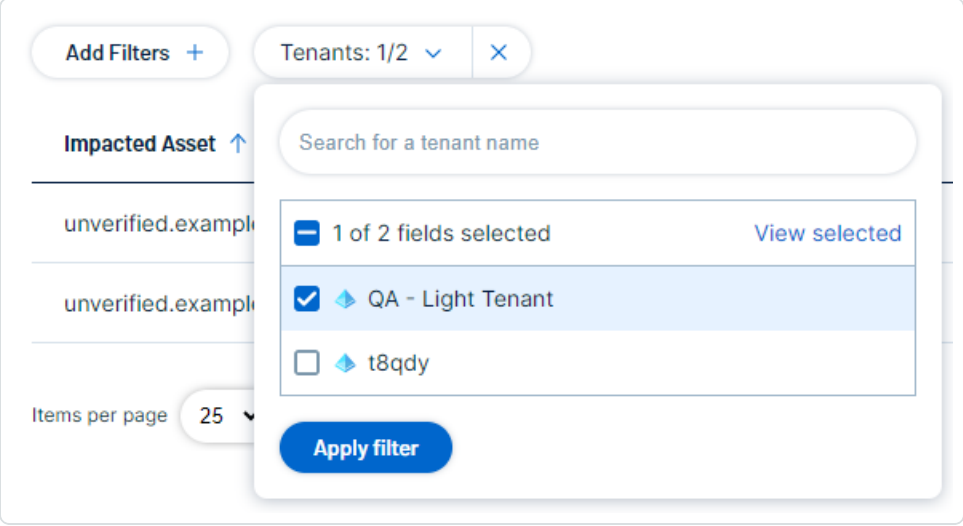
   「新增篩選器」按鈕會隨即顯示。

2. 按一下「新增篩選器」。篩選選項如下：

   - 依「上次狀態變更時間」：從日期選擇器中選取一個日期。




   - 依「租用戶」：選取租用戶名稱。您也可以在「搜尋」方塊中搜尋特定租用戶，然後按一下「**檢視所選**」。



3. 按一下「**套用篩選器**」。

**匯出**

您可以將曝險情況的受影響資產清單匯出為 Excel 檔案。

如要匯出：

- 在曝險情況頁面上，按一下 圖示。

## 另請參閱

- 曝險概覽

# 曝險情況排除項目

## 設定資產排除項目，調整您的安全掃描

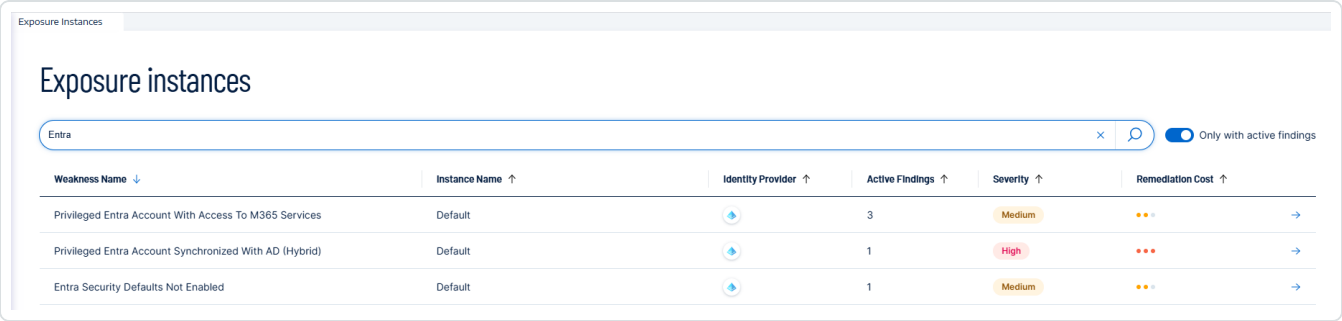
並非所有安全警示都需要處理，也不是每一個受標記的資產都實際存在風險。在某些情況下，即使沒有真正的威脅，系統設定的方式也可能會觸發警示。這可能導致安全報告中出現不必要的干擾，讓人忽略真正重要的問題。

為了協助您將注意力集中在重要事項上，**排除項目**功能可讓您將特定資產排除 (或加入允許清單)，使其不再顯示為影響特定弱點的來源。只要排除安全資產，您就能有效掌握掃描結果，報告也會更加清晰、相關且方便執行。

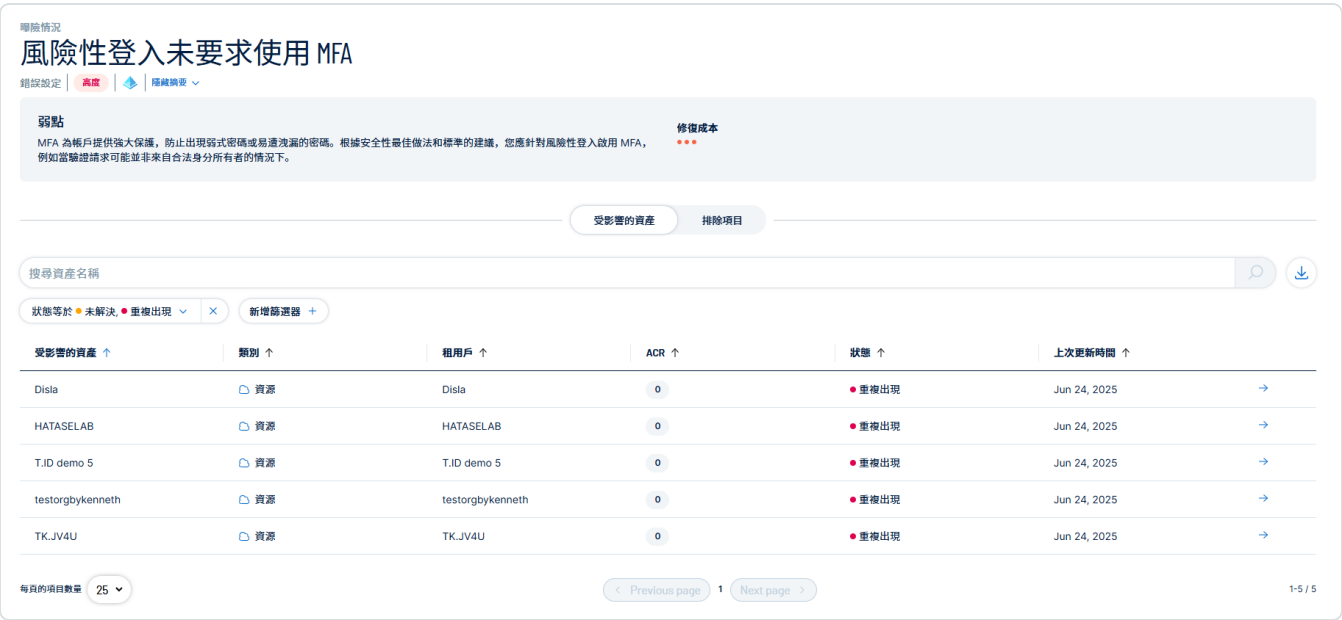
**如何存取「排除項目」頁面：**

1. 在 Tenable Identity Exposure 的左側導覽窗格中，按一下曝險中心圖示 。
2. 在子功能表中，按一下「**曝險情況**」。

   「**曝險情況**」頁面隨即顯示。




3. 若要深入瞭解每個曝險情況的詳細資料，請按一下此行結尾的箭頭。這樣會開啟另一個頁面，其中包含每個曝險情況的下列資訊：




4. 按一下「**排除項目**」索引標籤。

   系統將開啟一個頁面，顯示該曝險情況的所有排除項目 (若有)。

## 如何建立排除項目：

1. 按一下「建立**排除項目**」。

   「**建立排除項目**」視窗隨即開啟。

2. 提供以下資訊：

| | |
|---|---|
| **名稱** | 為排除項目輸入一個直觀的名稱 |

<table>
<tr><td>租用戶</td><td colspan="2">按一下「可用租用戶」下拉式清單的箭頭，並選取一個租用戶。</td></tr>
<tr><td>條件</td><td colspan="2">根據弱點的類型，會顯示不同的相關資訊與條件。</td></tr>
<tr><td></td><td colspan="2">◦ 在「資產類型」下拉式清單中，選取要排除的資產類型：<br>◦ 按一下屬性名稱旁的「+」圖示並指派值，以識別要排除的資產。Tenable Identity Exposure 會根據您選取的受影響資產，提供建議的值。<br>◦ 按一下「選取」。</td></tr>
<tr><td></td><td>資產類型</td><td>屬性</td></tr>
<tr><td></td><td>租用戶</td><td>資產名稱、外部識別碼</td></tr>
<tr><td></td><td>特權角色</td><td>資產名稱、外部識別碼、角色具有特權</td></tr>
<tr><td></td><td>帳戶</td><td rowspan="2">帳戶登入、帳戶狀態、ACR、資產名稱、Entra ID 安全識別碼、外部識別碼、MFA 標記、使用者類型</td></tr>
<tr><td></td><td>使用者</td></tr>
<tr><td>業務理由</td><td colspan="2">輸入此排除項目的說明，為其提供背景資訊。</td></tr>
</table>

按一下「**儲存**」以建立排除項目。




系統會顯示一則訊息，指出 Tenable Identity Exposure 建立了該排除項目，並且下次安全分析會將其納入考量。

**注意**：新的排除項目不會立即生效，因此受影響資產的狀態要等到下一次掃描後才會更新。

### 如何檢視排除項目：

**排除項目**清單依最近更新時間排序，最新建立的排除項目會顯示在最上方。




| 名稱 | 說明 |
|---|---|
| **名稱** | 顯示排除項目的指定名稱。 |
| **租用戶** | 與排除項目中受影響資產相關聯的租用戶。 |

| | |
|---|---|
| **業務理由** | 排除原因 |
| **條件** | 系統會以膠囊式標籤列出排除項目的條件與屬性，這些標籤會依據欄寬自動調整大小。<br><br>若未完整顯示所有屬性，請按一下**「更多」**以開啟右側面板，檢視完整排除項目詳細資料，每個膠囊代表一項條件或屬性。在此面板中按一下膠囊，即可展開可搜尋的值清單，以便查看因空間不足而被隱藏的內容。 |
| **上次更新時間** | 排除項目最近一次建立或更新的日期。 |
| **最後一位編寫者** | 建立或更新此排除項目的人員名稱。 |
| ⋮ | 可點選的功能選單，供您編輯或刪除排除項目。 |

**如何編輯排除項目：**

1. 在清單中選取排除項目，然後按一下該行尾端的選單符號⋮。
2. 選取**「刪除」**。

   **「編輯排除項目」**視窗隨即開啟。
3. 編輯必要的資訊。請參閱建立排除項目的程序。
4. 按一下**「儲存」**。

   系統會顯示一則訊息，指出排除項已成功更新，並將於下次掃描時套用。

**如何刪除排除項目：**

1. 在清單中選取排除項目，然後按一下該行尾端的選單符號⋮。

   系統會顯示一則訊息，要求您確認刪除。此操作無法復原。
2. 按一下**「刪除排除項目」**。

   系統會顯示一則訊息，指出排除項已成功刪除，並將於下次掃描時套用。

## Identity 360：全面的身分風險管理

**Identity 360** 為 Tenable Identity Exposure 中以身分為核心的新功能，可針對整個組織身分風險途徑的每個身分，提供豐富而詳盡的清單。

此功能可統合 Active Directory 和 Entra ID 中的身分，並依據風險進行排序，因此您可以將組織內的身分從風險最高排到最低。

此外，**Identity 360** 讓使用者可透過與特定身分相關聯的帳戶、脆弱環節和裝置等各種情境類別，深入瞭解並全面掌握每個身分。

### 主要功能

- **統一身分檢視**：Identity 360 會從多個身分識別提供者處 (從 Active Directory 和 Entra ID 開始) 彙總身分。
- **風險型排名**：您可以使用 Identity 360 的進階分析功能，依照風險從高到低的順序對組織內的身分進行排名。此優先順序可讓安全團隊將精力專注在最重要的項目上，進而最佳化資源配置並改善整體安全狀態。
- **情境身分見解**：透過多種情境視角，深入瞭解每個身分：
  - 關聯的帳戶
  - 發現的脆弱環節
  - 已連接的裝置
  - 存取特權
  - 活動模式

  透過這種多層面的方法，您可以全面瞭解每個身分的狀況，進而實現更準確的風險評估，採取有針對性的安全措施。
- **可執行的情報**：藉由整合不同來源的身分資訊，Identity 360 能夠提供可執行的見解，讓安全團隊能夠：
  - 識別並修復與高風險身分相關的弱點
  - 實作更有效的存取控制原則
  - 更快速地偵測並回應可能由內部人員造成的威脅
  - 簡化合規性報告和稽核

透過集中化身分風險管理並提供組織身分環境的整體檢視，**Identity 360** 可協助縮小攻擊破綻、改善作業效率，並且強化您的整體安全狀態。

## 什麼是身分？

**身分**是人類 (或非人類) 的數位表示。

- 他們是誰 (姓名、職稱、部門等)
- 他們可以存取的內容 (檔案、系統、資料)
- 他們如何與您組織的數位環境互動

另一方面，**帳戶**只是身分的一部分。這就像讓使用者登入特定係統或服務的金鑰。例如，某人可能有一個公司的電子郵件帳戶、一個客戶資料庫帳戶和一個專案管理工具帳戶，所有這些帳戶都是其整體數位身分的不同部分。

Identity 360 會檢視整個身分而非個別帳戶，幫助您更完整地瞭解每個人的數位存在狀況和潛在風險。

## Identity 360 資料

**Identity 360** 會利用來自 Tenable Platform 的資料，為 Tenable Identity Exposure 提供前所未見的資料存取權，以評估貴組織的安全狀態。

在 Tenable 生態體系中，實體稱為「資產」。Tenable Identity Exposure 會持續醒目提示與這些資產相關的弱點，同時透過詳細資產頁面揭露其關係。

**注意**：檢視資產屬性時，您會發現某些欄位與其在身分識別提供者 (IDP) 中的原始格式相比，可能會顯示錯誤的大小寫 (例如小寫)。

**注意**：曝險概覽功能目前會根據**預設的 Tenable 設定檔**顯示弱點相關資料，不會自動反映**您在其他設定檔中列入白名單的 AD 物件的異常情況狀態**。

因此：

- 如果您已將特定曝險指標 (例如「原生系統管理群組成員」) 的 **AD 物件列入白名單**，**當預設設定檔將其識別為異常時，曝險概覽仍會將其標記為安全性弱點**。
- 即使物件已在不同的設定檔下列入白名單，這仍可能會造成問題尚未解決的印象。

- 如果根據曝險概覽顯示採取修復動作 (例如移除群組成員資格)，則物件將從檢視畫面中消失，但若該物件已在其他地方列入白名單，可能沒有必要採取修復動作。

## 身分收集

**Identity 360** 會將 IDP 帳戶整合到統一的 Person 實體之下。為判斷其是否應該與帳戶關聯，**Identity 360** 會比較數個屬性，例如帳戶的電子郵件地址和使用者主體名稱 (UPN)。

Tenable 會排列高品質比對的優先順序以防止錯誤關聯，即使這偶爾會遺漏在人類觀察者看來似乎很明顯的比對。例如，Tenable 會從比對中排除名字和姓氏，因為大型組織中存在同音異義詞的可能性較大，而這會顯著增加誤判的風險。

**注意：**當 IDP 移除與人員相關聯的最後一個帳戶時，Tenable Identity Exposure 使用者介面可能需要長達 12 小時才能移除對應的人員資產。**Identity 360** 也可能顯示人員及其相關帳戶之間的重複關係。

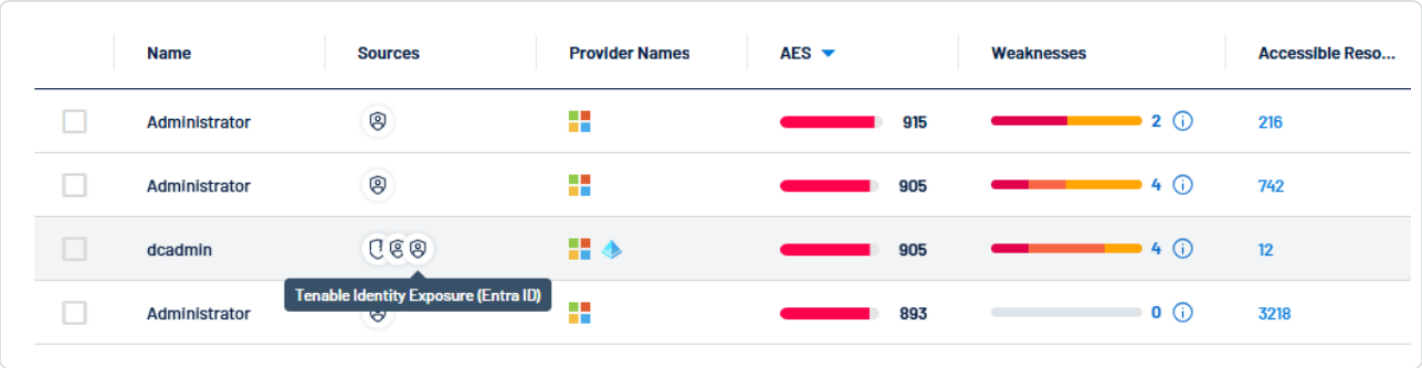
## IDP 租用戶、網域和組織

Tenable 使用術語「租用戶」來涵蓋各種 IDP 概念，包括「租用戶」(例如在 Microsoft Entra ID 中)、「組織」(例如在 Okta 中) 和「網域」(例如在 Microsoft Active Directory 中)。

如需有關 Tenable 如何識別 IDP 物件之租用戶的詳細資訊，請參閱 瞭解租用戶成員資格。

### 跨產品資產和資料來源

Identity 360 讓使用者可以全面掌握 Tenable 生態體系內所有身分相關資料，這包括 Tenable Identity Exposure 資料、雲端安全性資料，甚至 Nessus 掃描結果。收集每個資料集的特定 Tenable 產品稱為其「來源」。

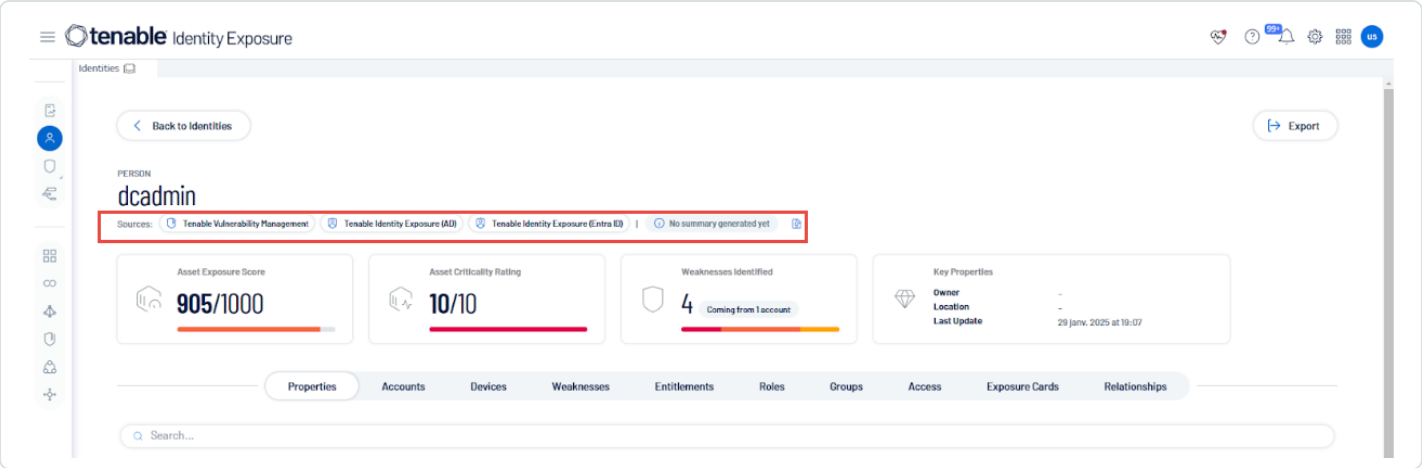



另一個關鍵詳細資料是可用的資料類型，例如 Active Directory、Entra ID 和 AWS 等 IDP 名稱。

此資訊會顯示在「提供者名稱」欄中。「來源」和「提供者名稱」欄位均支援篩選和排序，每個欄位皆可包含多個值。

### 跨產品資料 (資料來源)

Identity 360 會顯示 Tenable 生態體系中所有可用的身分導向資料。指定資產可有一或多個來源，表示可能會有一或多個 Tenable 產品監測該資產。Tenable Identity Exposure 顯示從 Tenable Identity Exposure 本身以及從補充來源收集的資料。




**可能的來源包括：**

| 需要的授權 | 設定先決條件 | 資產來源 | 值 |
|---|---|---|---|
| Tenable Identity Exposure 或 Tenable One | • Tenable Identity Exposure 中的 Active Directory (AD) 網域<br>• 資料傳送至 Tenable 的雲端平台 | Tenable Identity Exposure (AD) | 完整的 AD 資料 |
| Tenable Identity Exposure 或 Tenable One | • Tenable Identity Exposure 中的 Microsoft Entra ID (MEID) 租用戶 | Tenable Identity Exposure MEID | 完整的 MEID 資料 |
| Tenable One | • Tenable Cloud Security 中 Tenable 的身分識別提供者 | Tenable Cloud Security | ID360 中的其他 IDP 資料：AWS、Okta、GCI、OneLogin 和 |

| | | | |
|---|---|---|---|
| | | | PingIdentity。<br>資料將限於在 IDP 中填入電子郵件地址的 IDP 帳戶。 |
| Tenable One | • Nessus 掃描使用外掛程式 171956「Windows 列舉帳戶」。如需有關掃描的詳細資訊，請參閱 Tenable Vulnerability Management 使用者指南中的掃描概覽。 | Tenable Vulnerability Management | Active Directory (AD) 和 Entra ID 帳戶之間的對應，以及使用這些帳戶的裝置。 |

## 先決條件

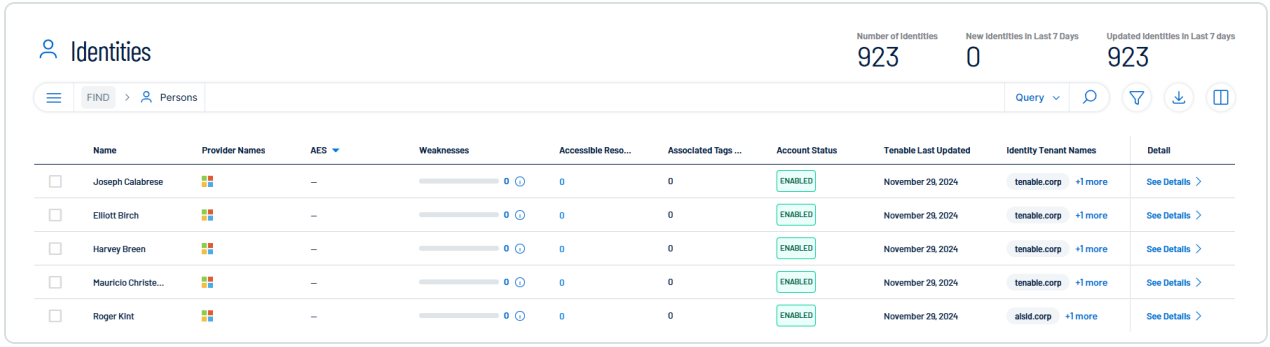
- 若要使用 **Identity 360**，您必須在 Tenable Identity Exposure 設定中啟用 Identity 360 支援。
- 如需指示，請參閱啟用 Identity 360、曝險中心和 Microsoft Entra ID 支援。

## 存取身分概覽

若要開啟**身分概覽**頁面：

- 在 Tenable Identity Exposure 中，按一下左側導覽列中的 。

  「**身分概覽**」頁面會隨即開啟，其中的儀表板可用來管理和監控組織系統內的身分。




主要元素

此儀表板可讓您檢視、搜尋和管理身分資訊，並且將重點放在脆弱環節和攻擊曝險等安全性指標上。它會以表格格式提供個別身分的高層級概觀 (在標頭中) 以及詳細資訊。

- **關鍵指標**
    - 身分數目
    - 過去 7 天內的新身分
    - 過去 7 天內更新的身分
- **導覽與搜尋**
    - 用於查詢身分的搜尋列
    - 查詢、篩選、匯出和欄自訂的選項

      如需有關如何使用搜尋功能的完整資訊，請參閱 《全域搜尋快速參照指南》。
- 身分識別提供者 (IDP) 中所有身分資產的**資料表**。此檢視特別關注身分類型的資產，這點與會顯示所有資產類型的 Tenable One 不同。每一列都代表一個具有此資訊的唯一身分：(預設欄顯示)
    - 名稱、提供者、AES (Asset Exposure Score)、脆弱環節、可存取的資源、相關標籤、帳戶狀態、上次更新時間、身分租用戶名稱和詳細資料
- **資料視覺化**
    - AES 和脆弱環節欄中的長條圖或指標，可提供資料的視覺呈現
- **狀態指標**
    - 「帳戶狀態」欄內的「ENABLED/DISABLED」標籤

### 與 Tenable 曝險管理 Inventory 的比較

**Identity 360** 介面在外觀和功能上與 Tenable 曝險管理 中的「**清單**」頁面類似，只是針對身分管理進行特定調整。如果您已使用過 Tenable 曝險管理，則對於 Identity 360 的版面配置和許多功能會很熟悉。

如需詳細資訊，請參閱 《Tenable One 曝險管理平台部署指南》。

另請參閱

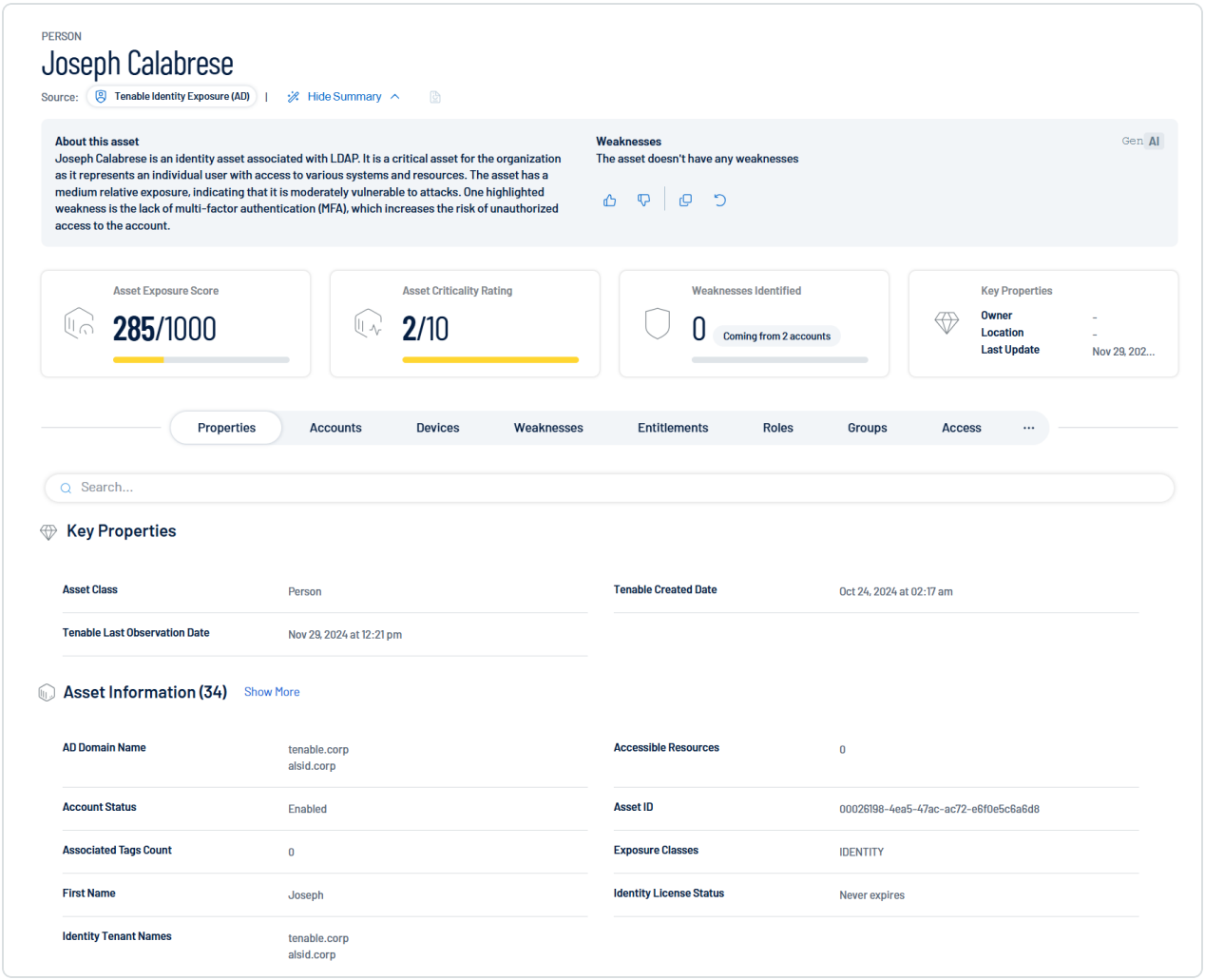
- 瞭解租用戶成員資格

## 身分詳細資料

**身分詳細資料**頁面著重在個別身分，並提供身分的數位足跡、存取權限、潛在弱點，以及組織 IT 生態體系內部的整體安全性狀態的全面檢視。

若要存取此頁面：

- 在「**身分概觀**」頁面中，按一下位於表格中人員姓名所在列尾的「**查看詳細資料**」。




## 標頭和頂端區段

- **身分名稱**：顯示身分的名稱。
- **人物圖示**和**來源**：顯示身分與特定來源的關聯。將游標懸停在來源圖示上方，即可看到身分識別提供者的名稱。
- **摘要**：針對此身分偵測到的身分和脆弱環節的詳細摘要。

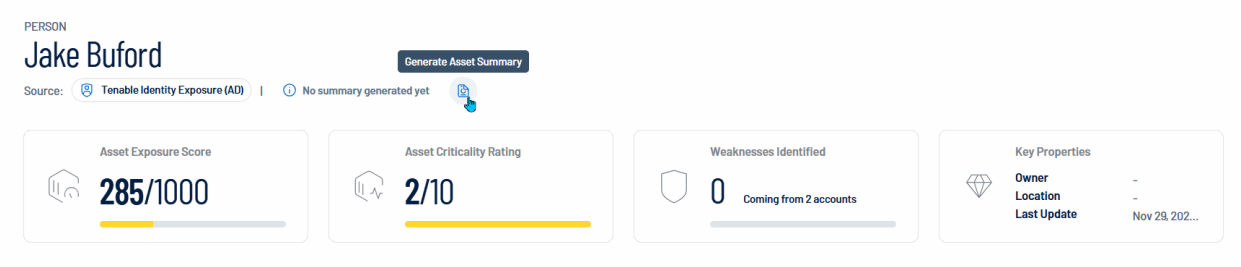
**產生並檢視資產的 AI 摘要：**

Tenable Identity Exposure 可讓您產生使用 AI 的身分摘要。摘要是在容器層級產生，並且僅適用於您容器內的授權身分。

**注意：**Tenable Identity Exposure 將可產生的摘要數限制為每小時 100 個，每天最多產生 1000 個摘要。

執行下面的其中一項動作：

- 若要首次產生資產的 AI 摘要，請在「**尚未產生摘要**」旁邊按一下 按鈕。




Tenable Identity Exposure 會使用 AI 產生資產摘要，包括一般詳細資料和資產脆弱環節的細節。

- 若要重新產生資產的現有 AI 摘要，請按一下「**顯示摘要**」，然後在摘要面板底部按一下 按鈕。

Tenable Identity Exposure 會重新產生身分的 AI 摘要。

**提示：**按一下 按鈕可將摘要直接複製到剪貼簿。您也可以在日後按一下 或 來評價摘要的實用性，以協助改善 Tenable Identity Exposure 內 AI 產生內容的品質。

- **Asset Exposure Score**：量化身分的安全性曝險，最高分數為 1000，代表最高的曝險等級。

- **Asset Criticality Rating**：反映身分在組織內的重要性，以 1 到 10 的等級評等，其中 10 代表最高的重要性。
- **已識別的脆弱環節**：顯示針對此特定身分發現的安全性弱點或脆弱環節的數量。
- **主要屬性**：列出主要資訊，包括所有者、位置，以及此身分上次更新的日期。

標頭索引標籤

在標頭下方，特定索引標籤可提供其類別特定的詳細資訊。請參閱以下區段中每個索引標籤的詳細描述。

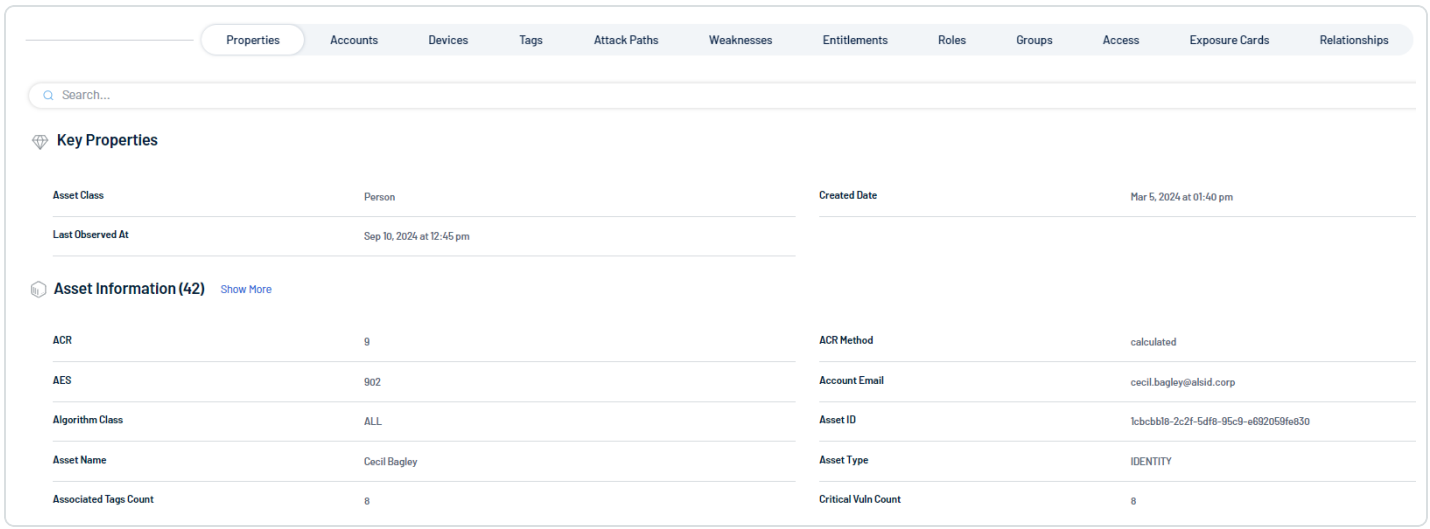



- **屬性**：身分的基本資訊和屬性。
- **帳戶**：身分的相關帳戶和網路設定檔。
- **裝置**：與身分相關的電子裝置。
- **脆弱環節**：特定的安全性弱點或風險。
- **權限**：授予組織 IT 系統內某個身分的特定權限或存取權。
- **角色**：根據工作職能、責任或組織職務組合的一系列權限。
- **群組**：身分所屬的組織單位或團隊。
- **存取權**：有關此身分可存取哪些資源或系統的概觀。
- **曝險資訊卡**：風險曝險等級摘要。
- **關係**：與其他身分或實體的關聯。

在適用的情況下，按一下「查看詳細資料」即可在 Tenable Inventory 中查看更詳細的資訊。

### 屬性

預設檢視會顯示「屬性」索引標籤。




## 主要屬性

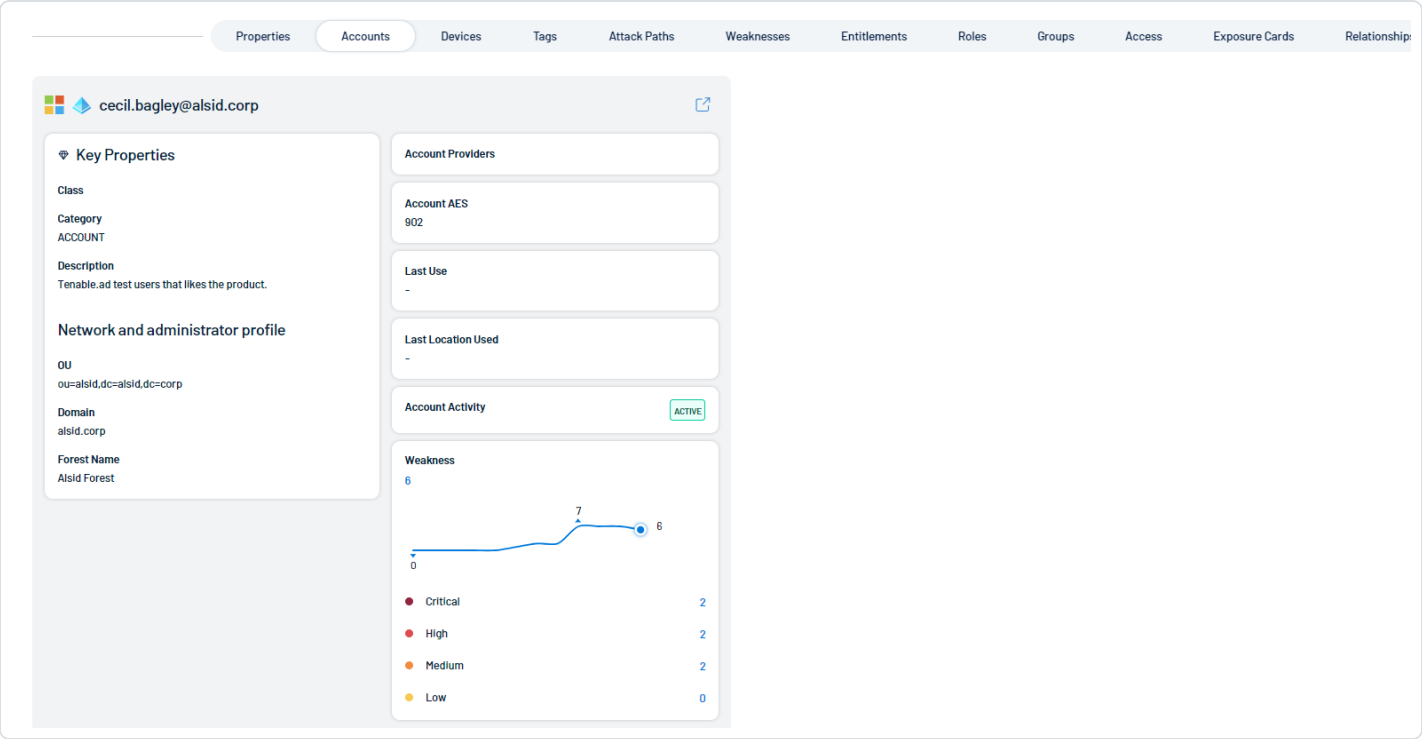
與資產或身分相關的最基本屬性摘要。摘要內容通常包含資產類別、上次觀察時間等高階詳細資料，以及可提供實體狀態快速概觀的其他核心資訊。

## 資產資訊

與資產或身分相關聯的特定屬性的詳細清單，其中可能包括 ACR、AES、資產名稱、電子郵件、建立日期等技術識別碼。它提供與實體相關的特性和中繼資料的全面檢視。

## 帳戶

「帳戶」區段提供有關身分相關聯帳戶和網路設定檔的詳細資訊。




### 主要屬性

包括重要詳細資料，例如帳戶類別 (資產類型)、類別 (例如 ACCOUNT)，以及帳戶用途或角色的描述。「網路和管理員設定檔」區段會醒目提示技術詳細資訊，例如組織單位 (OU)、網域以及樹系名稱。

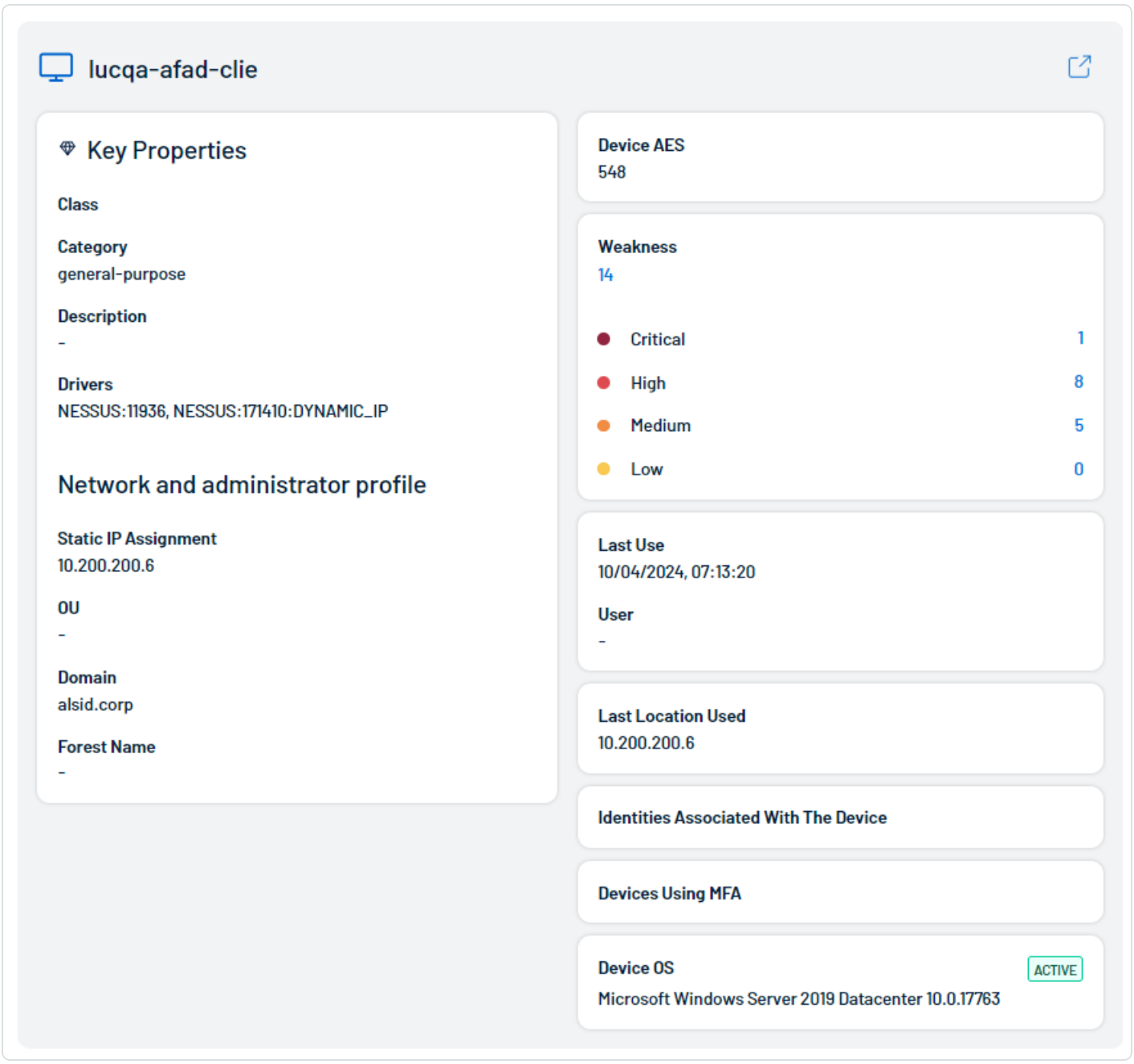
### 弱點

以圖形方式顯示所找到的脆弱環節數量，並且按嚴重性 (重大、高、中和低) 分類。圖形會提供趨勢線，指示脆弱環節在經過一段時間之後的進展情況。

## 裝置

裝置通常是可連線至網路、與其他裝置通訊，以及執行與身分相關聯之特定功能或任務的實體或虛擬元件。

若要開始查看此人員的裝置，請使用 Tenable Vulnerability Management 掃描所登入的裝置。




您可以在每個圖塊中檢視下列裝置資訊：

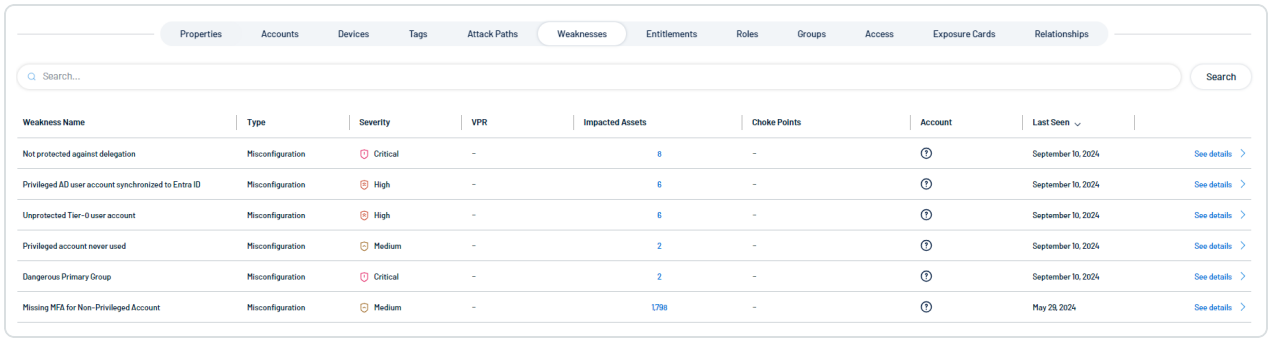
- **主要屬性**：
  - **類別**：與裝置相關的資產類別。
  - **類別**：與裝置相關的類別，例如**一般用途**。

- **描述**：裝置的描述 (若可用)。
- **驅動程式**：裝置上安裝的驅動程式清單。

- **網路和管理員設定檔**：
  - **靜態 IP 分配**：與裝置相關聯的靜態 IP 位址。
  - **OU**：與裝置相關聯的組織單位 (OU)。
  - **網域**：與裝置相關聯的網域。如需詳細資訊，請參閱《*Tenable Identity Exposure 使用者指南*》中的 <網域> 一節
  - **樹系名稱**：與裝置相關聯的樹系名稱。如需詳細資訊，請參閱《*Tenable Identity Exposure 使用者指南*》中的 <樹系> 一節。
- **裝置 AES**：與裝置相關的整體 AES。如需詳細資訊，請參閱 Tenable Inventory Metrics。
- **脆弱環節**：裝置中脆弱環節的圖形表示法。此區段包含每個脆弱環節及其關鍵性的折線圖和個別計數。

## 脆弱環節

- **脆弱環節**係指表明與此身分或其帳戶相關弱點或安全缺口的情形。
- **弱點**係指產品或資訊系統中的技術脆弱環節，此脆弱環節可能遭到惡意利用，進而造成經濟和社交活動中斷或受損。
- **曝險指標** (IoE) 是一種偵測特徵，可識別您環境中與身分相關的潛在安全性曝險。
- **風險評分**是一個全面性指標，用於評估整個組織的身分風險。評估時會考慮脆弱環節、權限以及其他安全性相關指標等多種元素，以針對潛在威脅進行整體評估。



**提示**：若要深入探究有關脆弱環節的更詳細資料，請按一下「查看詳細資料」，前往 Inventory「脆弱環節詳細資料」頁面。

**注意**：此頁面目前僅供 Tenable One 授權使用者使用。

此圖塊包含以下資訊：

- **名稱**：已識別的特定弱點或脆弱環節
- **類型**：弱點的類別或分類，例如「錯誤設定」
- **嚴重性**：用於衡量脆弱環節的關鍵性 (等級從低到重大)，進而判斷遭惡意利用時的潛在影響。
- **VPR**：(弱點優先順序評分)：以分數或排名的形式，根據脆弱環節的可利用性和潛在危害指出解決脆弱環節的緊迫性。請參閱弱點優先順序評分。
- **受影響的資產**：列出脆弱環節遭到惡意利用時可能會受影響的系統、應用程式或資料。
- **阻擋點**：系統中的潛在領域，您可以在這些領域集中努力緩解攻擊，以限制攻擊的損害或擴散程度。
- **帳戶**：與所識別的脆弱環節或弱點相關聯的帳戶。
- **上次查看時間**：上次偵測到弱點的日期或時間。

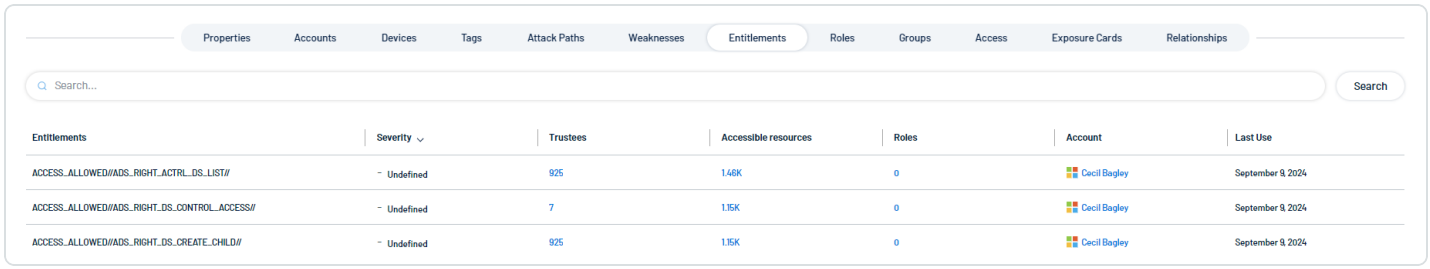
**注意**：Identity 360 功能目前會根據**預設的 Tenable 設定檔**顯示弱點相關資料，不會自動反映**您在其他設定檔中列入白名單的 AD 物件的異常情況狀態**。

因此：

- 如果您已將特定曝險指標 (例如「原生系統管理群組成員」) 的 **AD 物件列入白名單，當預設設定檔將其識別為異常時，Identity 360 仍會將其標記為安全性弱點**。
- 即使物件已在不同的設定檔下列入白名單，這仍可能會造成問題尚未解決的印象。
- 如果根據 Identity 360 顯示的內容採取修復動作 (例如移除群組成員資格)，則物件將從檢視畫面中消失，但若該物件已在其他地方列入白名單，可能沒有必要採取修復動作。

**權限**

**權限**指的是授予組織 IT 系統內某個身分的特定權限或存取權。它代表存取控制的精細程度，可準確定義某個身分能夠在特定資源上執行的動作。



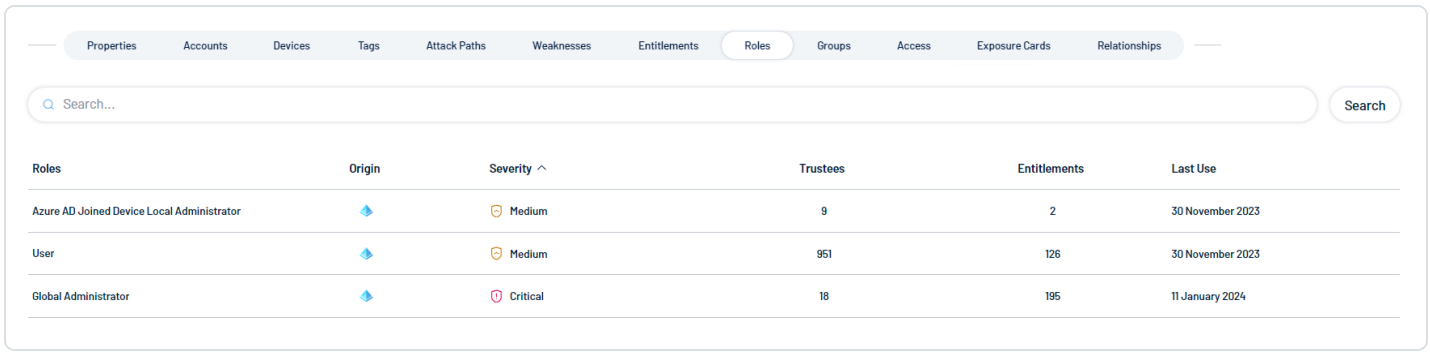

此圖塊包含以下資訊：

- **權限**：列出授予帳戶的特定權限或存取權，例如具有詳細權限的「ACCESS_ALLOWED」。這些可能代表系統 (如 Active Directory) 中的權限。
- **嚴重性**：顯示與每項權限相關的關鍵性或風險層級。在此情況下，系統會將其標記為「未定義」，表示未套用任何特定的風險分類。
- **信任者**：指示被授予這些權利或權限的使用者或帳戶 (信任者) 的數目。
- **可存取的資源**：顯示可透過指定權限存取的資源 (例如檔案、資料夾、系統等) 數量。
- **角色**：顯示與此特定權限相關聯的角色數量。
- **帳戶**：指定與這些權限相關聯的使用者或帳戶。例如，「Cecil Bagley」列為所顯示權限的帳戶擁有者。
- **上次使用時間**：提供上次使用這些權限的日期，指出帳戶上次使用特定權限存取資源的時間。

### 角色

**角色**是根據工作職能、責任或組織職務組合的一系列權限。角色可將一組預定義的權利分配給共用類似工作職能的多個使用者，進而更有效地管理存取權限。

**角色**圖塊會顯示指派給身分的所有角色。例如，如果此身分具有 Microsoft Entra ID 中指派的角色，其詳細資料會顯示在此處。

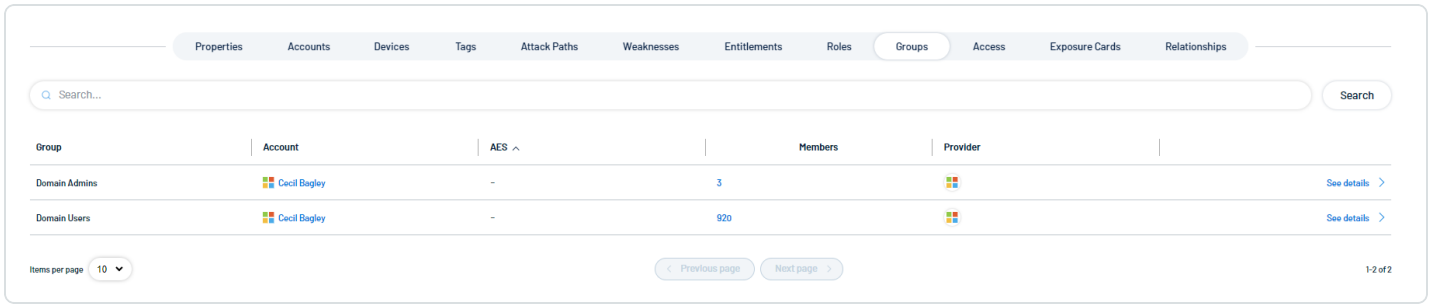



此圖塊包含以下資訊：

- **角色**：指派給身分的角色名稱。
- **來源**：指示帳戶來源提供者的圖示。
- **嚴重性**：資產的整體嚴重性，例如**關鍵**。
- **信任者**：與身分角色相關的信任者數量。
- **權限**：角色可存取的權限數目。
- **上次使用時間**：最近在資產上使用角色的日期。

## 群組

群組指的是此身分在組織內所屬的集合單位或團隊。



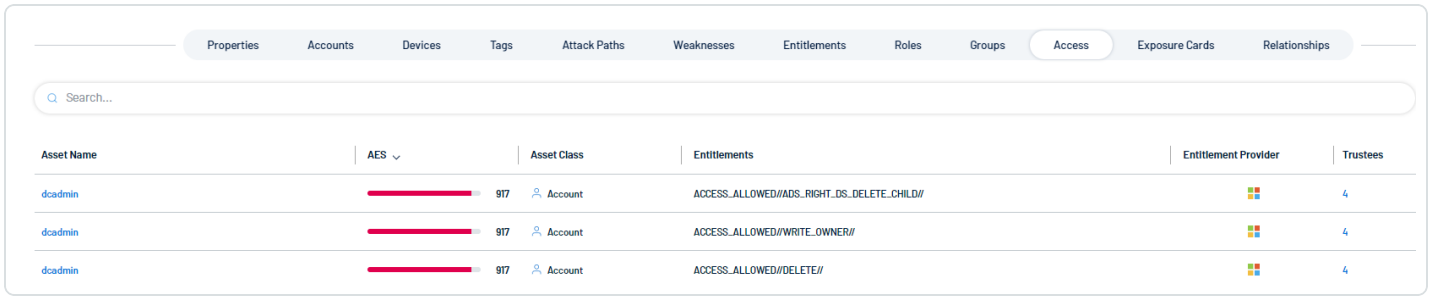

此圖塊包含以下資訊：

- **群組**：使用者或帳戶所屬群組的名稱 (例如，「網域管理員」或「網域使用者」)。
- **帳戶**：與特定使用者或實體 (在本例中為「Cecil Bagley」) 有所關聯的帳戶。這可以是管理群組的系統管理員或使用者。

- **AES**：Asset Exposure Score。Tenable 會針對您網路上的每項資產計算一個動態 AES，以 0 到 1000 之間的整數表示資產的相對曝險程度。較高的 AES 表示較高的曝險程度。如需詳細資訊，請參閱 Tenable Inventory Metrics。
- **成員**：每個群組中的成員數目 (例如，「網域管理員」中有 3 個成員，而「網域使用者」中有 920 個成員)。
- **提供者**：帳戶或群組資訊的身分識別提供者來源。

### 存取權

此索引標籤可概括提供此身分可以存取哪些資源或系統。



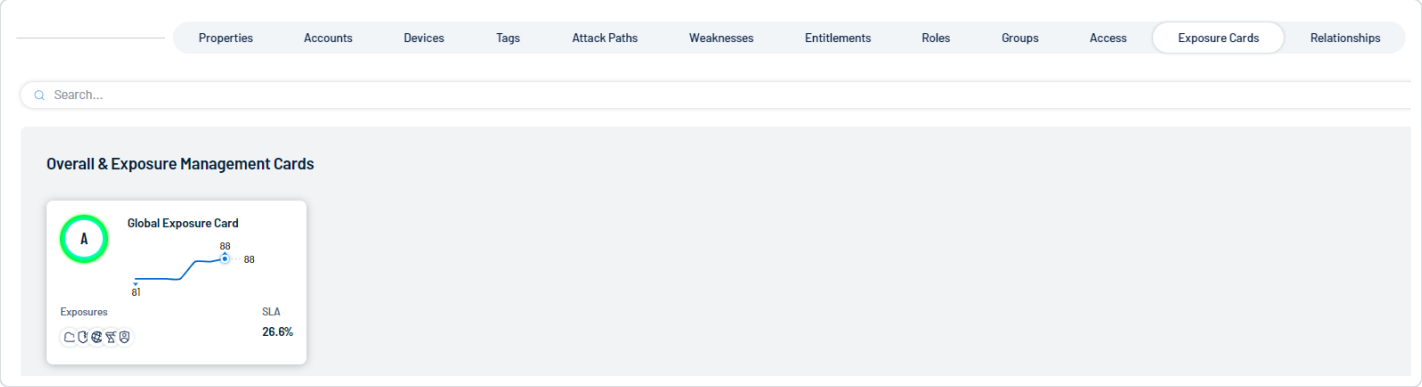

此圖塊包含以下資訊：

- **資產名稱**：列出與身分相關聯的受管理資產或帳戶的名稱 (例如「dcadmin」)。
- **AES**：Asset Exposure Score。Tenable 會針對您網路上的每項資產計算一個動態 AES，以 0 到 1000 之間的整數表示資產的相對曝險程度。較高的 AES 表示較高的曝險程度。它有一個數值，此處顯示的是 917，其中的圖形條代表安全性或存取權的相關度量。如需詳細資訊，請參閱 Tenable Inventory Metrics。
- **資產類別**：指示資產類型，在此情況下標記為「帳戶」。所列資產為使用者或系統帳戶。
- **權限**：描述授予資產的權限或權利。例如，ACCESS_ALLOWED//ADS_RIGHT_DS_DELETE_CHILD//、WRITE_OWNER// 和 DELETE// 等權限會定義與每項資產相關聯的特定權限。
- **權限提供者**：指定提供這些權限的來源或服務。
- **信任者**：顯示與資產相關聯的信任者數量，代表可控制或負責資產的個人或群組 (顯示為每列 4 個信任者)。

### 曝險資訊卡

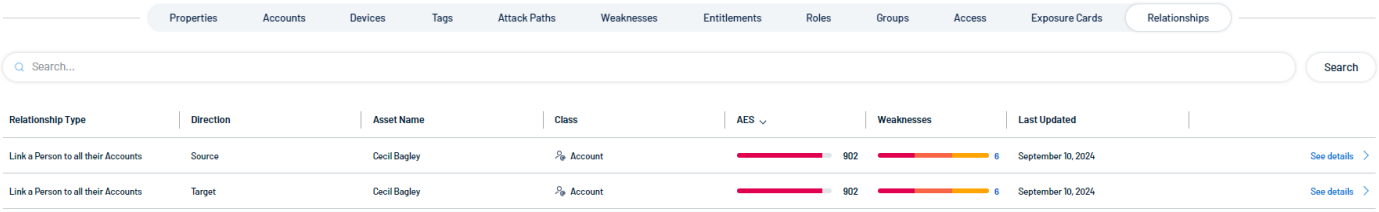
曝險資訊卡代表從您設定的標籤和資料來源傳入的資料。它會彙總資料並將其標準化，以提供 Cyber Exposure Score (CES) 和其他指標的視覺效果。使用者可以建立自訂卡片，或使用 Tenable 提供的卡片，獲得有關最需要關注哪些領域的見解與指導。

- 按一下任何卡片可直接瀏覽 Lumin Exposure View，且系統會根據預設顯示所選的卡片資料。




## 關係

**關係**區段會顯示與您正在檢視詳細資料的目前身分具有已知關係的所有資產清單。




此圖塊包含以下資訊：

- **關係類型**：兩個身分之間的關係類型。
- **方向**：指出相關身分是關係的來源還是目標。
- **資產名稱**：相關身分的資產識別碼。
- **資產類別**：指示資產類型，在此情況下標記為「帳戶」。
- **AES**：Asset Exposure Score。Tenable 會針對您網路上的每項資產計算一個動態 AES，以 0 到 1000 之間的整數表示資產的相對曝險程度。如需詳細資訊，請參閱 Tenable Inventory Metrics。

- **脆弱環節**：與資產相關的脆弱環節。
- **上次更新時間**：最近一次掃描識別資產的日期。

## Identity 360 基本資訊

**Identity 360** 提供健全的工具可用於管理和分析貴組織的身分資料，讓您可以在知情的情況下做出安全性決策。

### 搜尋

**Identity 360** 提供三個功能強大的搜尋選項，可協助您找到所需的確切資訊：

- **全域搜尋查詢建立器**
  - 啟用使用特定內容和相關查詢進行複雜、精確的搜尋
  - 非常適合超級使用者使用以及進行詳細分析
  - 範例：尋找屬於「具有屬於特定群組之帳戶的身分」或「具有在過去 30 天內存取過之高風險權限的身分」成員的所有帳戶。
  - 優點：可讓您建構精確的多層式搜尋，以便準確地找到您需要的資料。

  如需有關如何使用此查詢建立器的完整資訊，請參閱 《全域搜尋快速參照指南》。
- **自然語言處理 (NLP) 搜尋**
  - 只需以簡單英文輸入您的要求即可
  - 系統會以智慧方式解譯您的意圖，並將其轉換為結構化查詢
  - 範例：「顯示行銷部門中所有非活躍使用者的帳戶」
  - 優點：易於使用，不需要任何查詢語法知識，非常適合快速臨時搜尋
- **簡易搜尋**
  - 針對即時結果進行快速、直接的文字型搜尋
  - 非常適合尋找特定身分或簡單檢索

- 範例：輸入例如姓名「John Smith」或員工 ID
- 優點：即時執行，非常適合日常作業和快速檢索

每種搜尋類型都能滿足不同的使用者需求和情境，從複雜的資料分析到快速的身分檢索皆可完成。您可以根據目前的工作、技術專長以及您所尋找資訊的複雜性，選擇最適當的搜尋方法。

### 篩選器

**Identity 360** 中的篩選器函式可透過套用特定準則的方式，縮小或調整顯示的資料範圍。

如要套用篩選器：

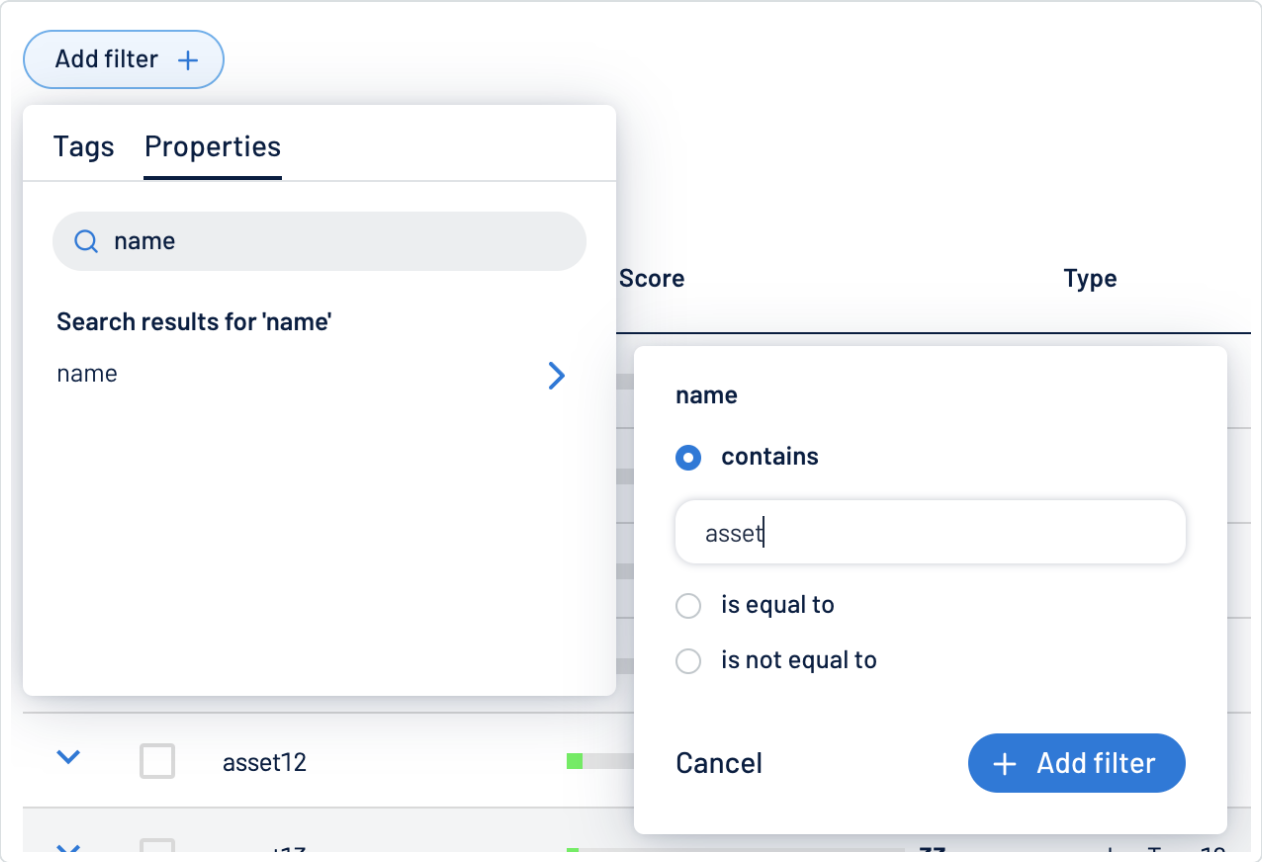
1. 在「身分」頁面的標頭中，按一下「

」。

   「新增篩選器」按鈕會隨即顯示。

2. 按一下「**新增篩選器 +**」。

   功能表隨即會顯示。




3. 執行下面的其中一項動作：

   - 如要依標籤搜尋資產清單，請按一下「**標籤**」(僅適用於 Tenable One 授權，且在 Tenable Inventory 中進行管理。)
   - 如要依資產屬性搜尋資產清單，請按一下「**屬性**」。

4. 在搜尋方塊中輸入想要用來搜尋資產清單的準則。

   Tenable Inventory 會根據您的準則填入選項清單。

5. 按一下您要用來篩選資產清單的標籤或屬性。

   功能表隨即會顯示。

6. 選取如何套用篩選器。例如，如果您要搜尋名稱為 Asset14 的資產，請選取「包含」單選按鈕，並且在文字方塊中輸入 Asset14。

7. 按一下「**新增篩選器**」。

   篩選器會顯示在資產清單上方。

8. 在要套用的每個其他篩選器中重複上述步驟。
9. 按一下「**套用篩選器**」。

   頁面會依指定的準則篩選身分清單。

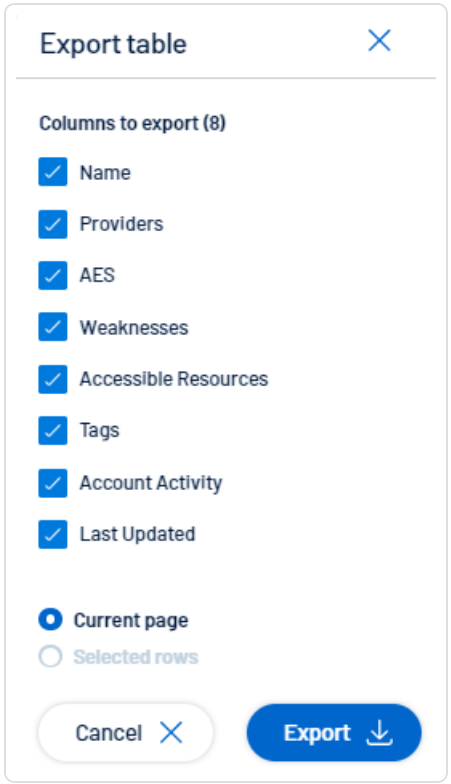
### 匯出

您可以將表格中顯示的資料匯出至 Excel 檔案。

> **注意**：詳細身分檢視中的每個索引標籤都會提供自己的匯出選項，讓您可以擷取更多的目標資料集。

若要匯出資料：

1. 在「身分」頁面的標頭中，按一下 圖示。
2. 在「匯出表格」視窗中選取要匯出的欄。您可以選擇匯出目前頁面或所選取的列。




3. 按一下「**匯出**」。

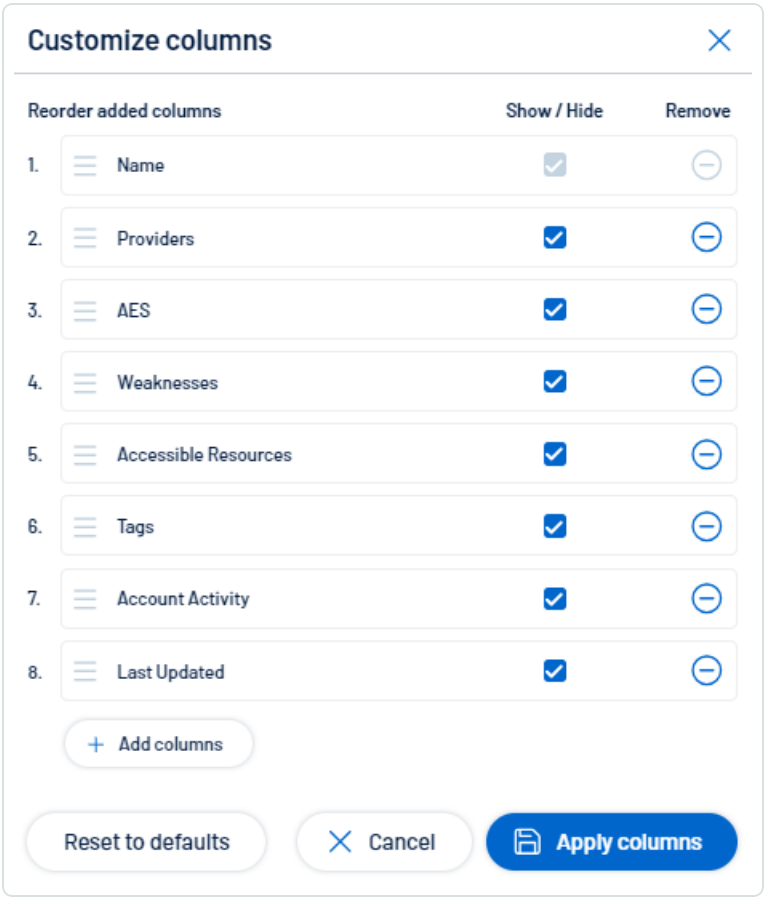
### 自訂欄

您可以新增、移除欄或重新排列欄，根據自己的喜好調整檢視。如果您想要還原任何變更，可以隨時重設為預設設定。

若要自訂欄顯示：

1. 在「身分」頁面的標頭中，按一下「」。

   「自訂欄」視窗會隨即顯示。




2. 選擇性：

   - 在「**重新排列新增欄**」區段中，按一下並拖曳任何欄名稱，即可重新排列欄。
   - 在「**顯示/隱藏**」區段中選取/取消選取核取方塊，即可顯示或隱藏資料表中的欄。
   - 在「**移除**」區段中，按一下按鈕將某欄從表格中永久移除。
   - 若要將欄新增至資料表，請按一下「**新增欄**」。

     「**新增欄至表格**」視窗會隨即顯示。

- (選擇性) 使用搜尋列搜尋欄屬性。

  欄屬性清單會根據您的搜尋查詢進行更新。

- 選取要新增至表格的任何一欄或多欄旁邊的核取方塊。
- 按一下「新增」。

  欄會出現在「自訂欄」視窗中。

3. 按一下**「套用欄」**。

   Tenable 會將您的變更儲存在表格的欄中。

預設欄

欄的預設配置可確保金鑰資料易於存取，同時又能提供自訂彈性。

- **名稱** - 無法隱藏或移除的必填欄位，因為它可以作為每個項目的主要識別碼。
- **提供者** - 顯示連結至項目的相關服務或平台。
- **AES** - 顯示 Asset Exposure Score。
- **脆弱環節** - 醒目提示針對所列項目偵測到的所有弱點或問題。
- **可存取的資源** - 顯示可由帳戶或實體存取的資源。
- **標籤** - 與每個項目相關聯的標籤或中繼資料，有助於分類。
- **帳戶活動** - 與帳戶活動相關的記錄或指標。
- **上次更新** - 顯示項目的最近更新日期。

如要重設為預設欄：

- 按一下**「重設為預設值」**，將所有欄重設為其預設值。

## 瞭解租用戶成員資格

**租用戶成員資格**代表身分識別提供者生態體系內兩種資產之間的單向連結：

1. **身分識別提供者的資產** - 例如使用者帳戶、群組或資源。
2. **「租用戶」資產** - 代表包含此資產的更廣泛實體或網域。「租用戶」的本質取決於特定的身分識別提供者。

此租用戶成員資格有助於您識別資產及其租用戶之間的關係，進而深入瞭解資產組織和階層。

## 將資產連結至租用戶

對於 Active Directory (AD)，資產是使用資產的**可辨別名稱 (DN)** 連結至其租用戶 (AD 網域)。DN 提供目錄結構中資產位置的相關階層資訊，可用於判斷租用戶。

### 識別租用戶

當資產符合 AD 物件 (例如，使用者或群組) 時，其租用戶識別如下：

- 擷取資產的**可辨別名稱**。
- 從 DN 中的**網域元件 (DC)** 項目識別租用戶。

### 範例

- 資產 DN：`CN=UserA,CN=Users,DC=tenable,DC=corp`
- 租用戶：`DC=tenable,DC=corp` (代表 AD 網域)。

## 特殊案例：瞭解樹系根網域連結

在某些情況下，Active Directory (AD) 資產及其租用戶 (網域) 之間的關係可能因 AD 處理特定物件的方式而未能遵循預期的結構。為了清楚起見，本節將更詳細地說明這些「特殊情況」。

### 什麼是樹系根網域？

Active Directory 樹系是由一或多個依階層組織的網域所組成。**樹系根網域**是此階層中最頂層的網域，包含樹系中的所有其他網域。AD 中的某些物件會在其可辨別名稱中參照樹系根網域，即使這些物件屬於不同網域。此行為會影響識別租用戶的方式。

### 特殊情況產生的方式

從資產的可辨別名稱 (DN) 識別租用戶時，網域元件 (DC=...) 通常會指出資產的網域。然而也有例外狀況：

1. **全樹系設定物件**
    - 某些 AD 物件與適用於整個樹系而非特定網域的組態或設定相關聯。
    - 這些物件的可辨別名稱結尾為：
        - `CN=Configuration,DC=...`
    - 此類物件會連結至**樹系根網域**，而非其「真正的」網域。

    範例

    - DN：`CN=Configuration,DC=forestRoot,DC=com`
    - 租用戶：**樹系根網域** (`DC=forestRoot,DC=com`)。
2. **樹系 DNS 區域**
    - 某些物件會管理在整個樹系中共用的 DNS 區域。其可辨別名稱結尾為：
        - `DC=ForestDnsZones,DC=...`
    - 這些物件與**樹系根網域** (而非其特定網域) 相關聯。

    範例

    - DN：`DC=ForestDnsZones,DC=forestRoot,DC=com`
    - 租用戶：**樹系根網域** (`DC=forestRoot,DC=com`)。

## 為什麼這很重要

瞭解這些特殊情況對於準確解譯**租用戶成員資格**至關重要。主要影響包括：

1. **租用戶識別可能與預期不同**
    - 看似屬於特定網域的物件可能反而會連結至樹系根網域。
    - 「**Configuration**」或「**ForestDnsZones**」命名內容中的物件連結至**樹系根網域**，這是因為其作用範圍為全樹系。
2. **階層和範圍說明**

- 與樹系根網域相關的物件通常具有更廣泛的適用性，因為它們管理或代表樹系層級的設定。

3. **用於疑難排解和稽核**

   - 對這些案例的錯誤解譯可能導致在稽核網域結構或解決身分相關問題時發生錯誤。

瞭解這些細微差別後，您就可以放心地解譯研究發現，並在稽核和疑難排解工作中保持準確性。

## Tenable 身分識別總管選擇「租用戶」作為根容器名稱的原因

這是每個身分識別提供者 (IdP) 的根容器的通用、非 IdP 專屬名稱，可確保其能夠跨不同系統 (例如「Entra 租用戶」和「AD 網域」) 運作。

之所以選擇「**租用戶**」這個術語，是因為它在身分管理中廣為人知、跨平台中立，且與 Microsoft Entra 等現有標準保持一致。如此可確保管理不同 IdP 實作的清晰度、一致性和彈性。

# 追蹤流程

Tenable Identity Exposure 的追蹤流程顯示對於影響 AD 基礎架構事件的即時監控和分析。您可以用它來識別嚴重弱點及其建議的修復方法。

使用**追蹤流程**頁面，您可以回到過去載入以前的事件或搜尋特定事件。您還可以使用頁面頂端的搜尋方塊來搜尋威脅和偵測惡意模式。

追蹤流程會追蹤下列事件：

- **使用者和群組變更**：包括建立、刪除及修改帳戶和群組。
- **權限變更**：包括修改檔案、資料夾和印表機等物件的存取控制。
- **系統設定調整**：包括變更群組原則物件 (GPO) 和其他重要設定。
- **可疑活動**：包括未經授權的嘗試、特權提升和其他會觸發紅色標記的事件。

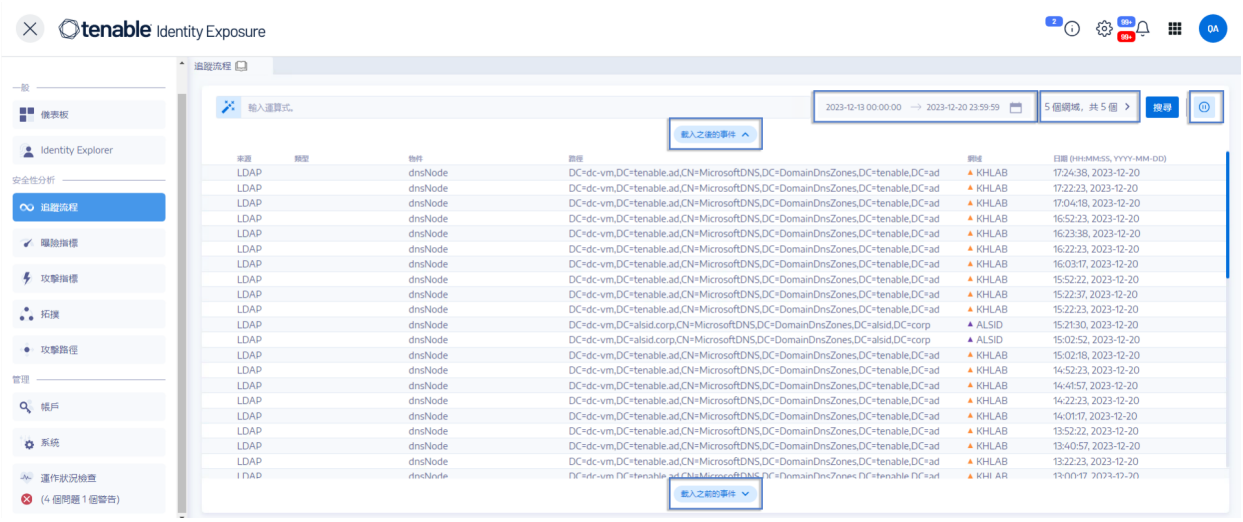
Tenable Identity Exposure 提供以下功能，可用於有效運用追蹤流程資料：

- **可供搜尋和篩選**：使用關鍵字或特定條件輕鬆瀏覽事件串流，有助於專注於相關活動上，盡可能減少無關資訊的干擾。
- **詳細的事件資訊**：每個事件項目都有詳盡的資訊，包括受影響的物件、負責變更的使用者、使用的通訊協定，以及相關聯的曝險指標 (IoE)。
- **視覺化關係**：可呈現事件之間的關係，說明看似不相關的活動如何引發更廣泛的攻擊活動。

**如要存取追蹤流程：**

- 在 Tenable Identity Exposure 中，按一下左側導覽列中的「**追蹤流程**」。

  追蹤流程頁面會隨即開啟，其中包含事件清單。如需詳細資訊，請參閱 追蹤流程表。




**如要選取時間範圍：**

**如要選取網域：**

**如要檢視事件：**

**如要暫停和重新啟動追蹤流程：**

**如要載入之後或之前的事件：**

## 追蹤流程表

Tenable Identity Exposure 會在事件發生時在追蹤流程表中持續列出您 Active Directory 中的事件。其中包括以下資訊：

| 資訊 | 說明 |
| --- | --- |
| 來源 | 指示 AD 基礎架構中任何安全性相關變更的來源。<br><br>可能有兩個來源：<br><br>• 用於與您的 AD 基礎架構通訊的輕量型目錄存取通訊協定 (LDAP)。<br><br>• 用於共用檔案、印表機等的伺服器訊息區 (SMB) 通訊協定。<br><br>**Tenable Identity Exposure** 會全面分析網路上的 LDAP 和 SMB 流量，以偵測異常情況和潛在威脅。<br><br>**注意**：Active Directory (AD) 允許管理員建立群組原則來控制部署在使用者和電腦帳戶上的設定。群組原則物件 (GPO) 儲存這些控制設定。SYSVOL 資料夾儲存網域控制器上的 GPO 檔案。每個網域成員都可以使用較高等級權限套用或執行 GPO，所以監控 GPO 的內容對於 AD 的安全非常重要。 |
| 類型 | 顯示事件的特徵元素，例如：<br><br>• ACL 已變更<br><br>• SPN 已變更<br><br>• 成員已移除<br><br>• 新成員<br><br>• 新信任<br><br>• 已新增未知的檔案類型<br><br>• 新物件<br><br>• 物件已刪除<br><br>• 密碼已變更<br><br>• UAC 已變更<br><br>• 已連結新的 GPO<br><br>• GPO 連結已刪除 |

| | |
|---|---|
| | • 所有者變更<br>• 已重新命名檔案<br>• 已建立 SPN<br>• 驗證重設失敗<br>• 驗證失敗 |
| 物件 | 指示與 AD 物件關聯的類或副檔名。您可以搜尋目錄物件 (使用者、電腦等) 或具有特定副檔名 (ini、XML、csv) 的檔案。 |
| 路徑 | 指示 AD 物件的完整路徑，以標識此物件在 AD 中的唯一位置。 |
| 目錄 | 指示 AD 基礎架構中變更的來源目錄。 |
| 日期 | 指示事件發生的時間。 |

## 使用精靈搜尋追蹤流程

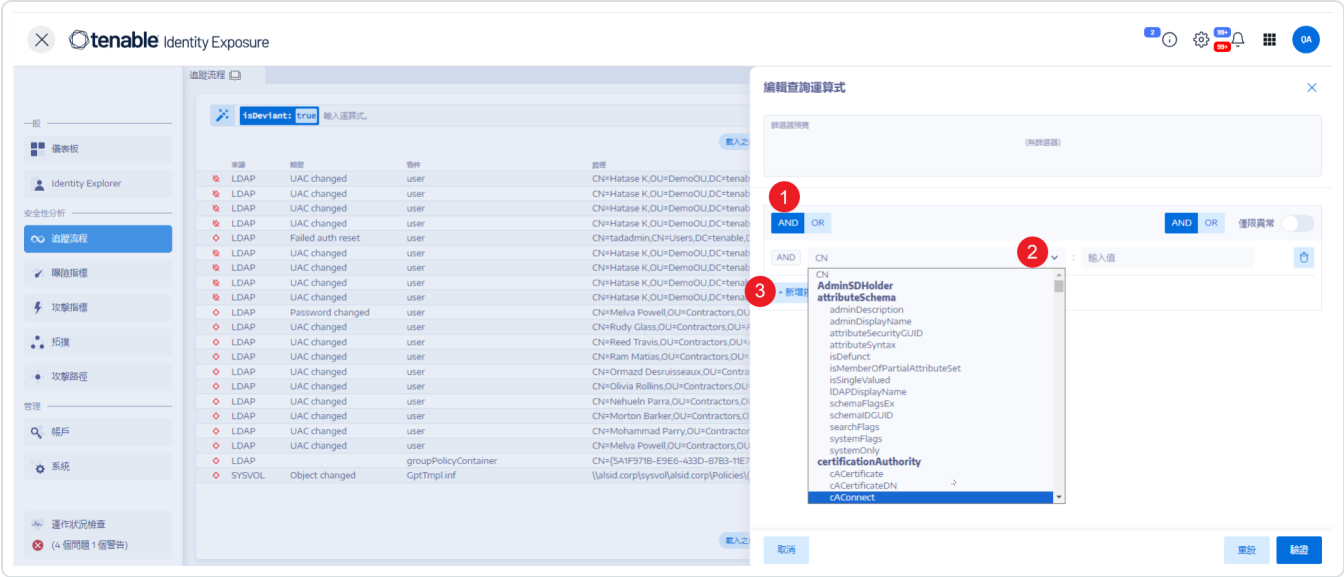
搜尋精靈允許您建立和組合查詢運算式。

- 在搜尋方塊中使用常用運算式時，您可以將它們新增到書籤清單中以供日後使用。
- 當您在搜尋方塊中輸入運算式時，Tenable Identity Exposure 會將此運算式儲存在「歷史記錄」窗格中以供您重複使用。

如要使用精靈搜尋：

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 按一下 圖示。

   **「編輯查詢運算式」**窗格會隨即開啟。如需詳細資訊，請參閱 自訂追蹤流程查詢。




3. 如要在面板中定義查詢運算式，請按一下「**AND**」或「**OR**」運算子按鈕 (1) 以套用到第一個條件。
4. 從下拉式功能表中選取一個屬性並輸入其值 (2)。
5. 執行下列任一動作：
   - 如要新增屬性，請按一下「**+ 新增規則**」(3)。
   - 如要新增另一個條件，請按一下「**新增條件**」「**+AND**」或「**+OR**」運算子。從下拉式功能表中選取一個屬性並輸入其值。
   - 如要將搜尋限制為異常物件，請按一下「**僅限異常**」切換為允許。選取「**+AND**」或「**+OR**」運算子將條件新增到查詢。
   - 如要刪除條件或規則，請按一下 圖示。
6. 按一下「**驗證**」以執行搜尋，或按一下「**重設**」以修改您的查詢運算式。

## 另請參閱

- 手動搜尋追蹤流程
- 使用精靈搜尋追蹤流程
- 自訂追蹤流程查詢

- 書籤查詢
- 查詢歷史記錄

## 手動搜尋追蹤流程

如要篩選符合特定字元字串或模式的事件，您可以在搜尋方塊中輸入運算式，以使用布林運算子 *、AND 和 OR 改善結果。您可以用括號封裝 OR 陳述式來修改搜尋優先順序。搜尋功能會在 Active Directory 屬性中尋找任何特定值。

如要手動搜尋追蹤流程：

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 在搜尋方塊中輸入查詢運算式。
3. 您可以按如下方式篩選搜尋結果：
    - 按一下**「日曆」**方塊以選取開始日期和結束日期。
    - 按一下**「n/n 網域」**以選取樹系和網域。
4. 按一下**「搜尋」**。

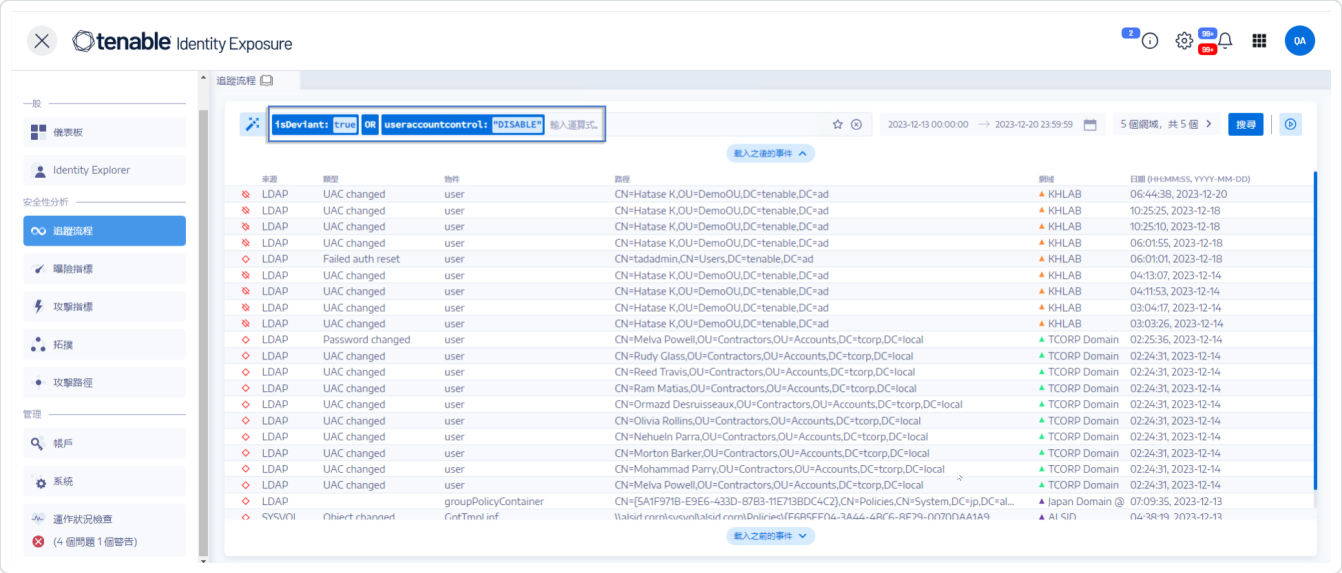
    Tenable Identity Exposure 將使用符合搜尋條件的結果更新清單。

**提示**：如要使用其他準則搜尋，您可以 使用精靈搜尋追蹤流程

範例：

以下範例搜尋：

- 已停用的可能危及受監控的 AD 基礎架構的使用者帳戶。
- 可疑活動和異常帳戶使用。

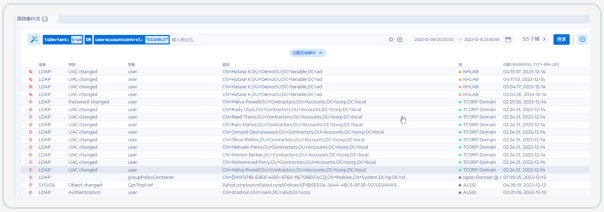
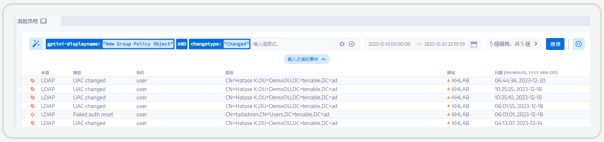


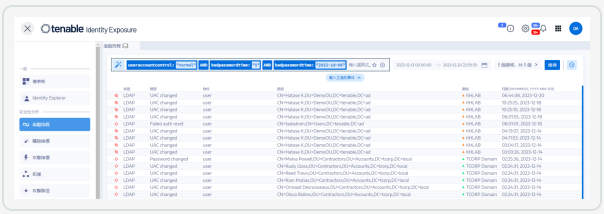
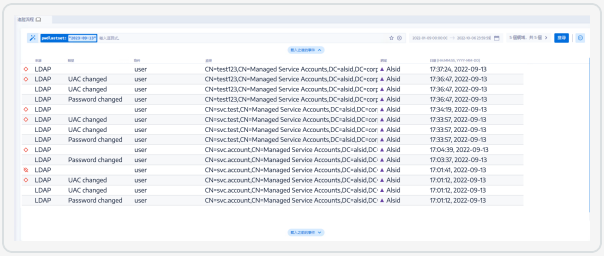
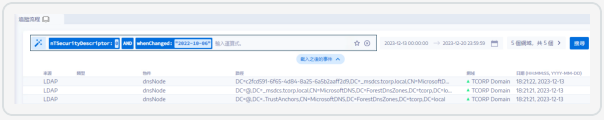

## 自訂追蹤流程查詢

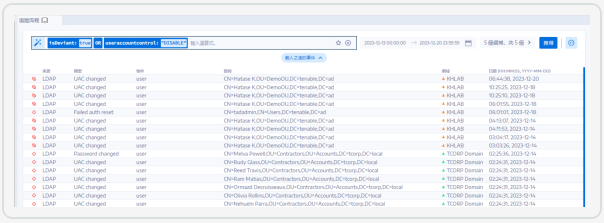
追蹤流程允許您擴展 Tenable Identity Exposure 的功能，而不限於預設的攻擊指標和曝險指標監控。您可以建立自訂查詢以快速擷取資料，也可以將查詢用作 Tenable Identity Exposure 可向您的安全資訊和事件管理 (SIEM) 系統傳送的自訂警示。

以下範例顯示 Tenable Identity Exposure 中實用的自訂查詢。

| 使用案例 | 說明 |
| --- | --- |
| **GPO 啟動和關閉二進位檔與全域 SYSVOL 路徑監控** | 監控開啟啟動路徑和/或全域 SYSVOL 複製路徑中的指令碼。攻擊者經常使用這些指令碼來濫用本機 AD 服務，從而在整個環境中快速傳播勒索軟體。<br>• **啟動路徑中的指令碼查詢：**<br>`globalpath: "sysvol" AND types: "Scriptsini"`<br>**注意**：此處的 `types` 是指物件屬性，而不是欄標題。<br>• **SYSVOL 監控查詢**： |

| | |
|---|---|
| | globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")<br> |
| **GPO 設定修改** | 監控對於 GPO 設定的修改。攻擊者經常使用這種方法來降低安全設定，以幫助長期潛伏和/或帳戶接管。<br>• **GPO 監控查詢：**<br>gptini-displayname:"New Group Policy Object" AND changetype:"Changed"<br> |
| **驗證失敗和密碼重設** | 監控多次失敗導致鎖定的身分驗證嘗試，這可以作為暴力密碼破解嘗試的早期警告標誌。<br>**注意**：您必須設定鎖定原則和日期/時間變數。如需詳細資訊，請參閱 使用 Tenable Identity Exposure 帳戶進行驗證。<br>• **驗證失敗查詢：**<br>useraccountcontrol:"Normal" AND badpwdcount:"<ACCOUNT_LOCKOUT_THRESHOLD>" AND badpasswordtime:"<DATE_TIME_STAMP>" |

| | |
|---|---|
| | <br><br>• **密碼重設查詢：**<br>`pwdlastset:"<DATE_TIME_STAMP"`<br> |
| **新增、刪除或變更物件權限** | 監控對於 ACL 權限和相關物件權限集合未經授權的修改。攻擊者可濫用此方法來提升權限。<br>**注意**：您必須提供日期/時間變數。<br>• **物件權限查詢：**<br>`ntsecuritydescriptor:0 AND whenchanged:"DATE_TIME_STAMP"`<br> |
| **導致異常情況的管理員變更** | 內建管理群組和自訂群組是敏感群組，需要密切監控可能引入風險的異常情況或設定變更。此查詢使您可以快速檢閱最近可能對管理員群組中的安全性設定產生不利影響的變更。<br>• **管理員變更查詢：** |

| | |
|---|---|
| | `isDeviant:true AND cn:"admins"`<br> |

## 另請參閱

- 手動搜尋追蹤流程
- 使用精靈搜尋追蹤流程
- 書籤查詢
- 查詢歷史記錄
- 追蹤流程使用案例

## 書籤查詢

您可以將使用頻繁的查詢運算式新增到自訂書籤清單中以供再次使用。

**如要為查詢運算式加上書籤：**

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 按一下搜尋方塊旁邊的 圖示。

   **「編輯查詢運算式」**窗格會隨即開啟。
3. 在搜尋方塊中輸入查詢運算式。
4. 按一下搜尋方塊右側的 圖示。

   **「新增到您的書籤」**方塊隨即出現。
5. 在**「選擇資料夾」**方塊中，按一下下拉箭頭以從清單中選取資料夾。

6. (可選) 按一下**「建立新資料夾」**切換為**「是」**。在**「資料夾名稱」**方塊中輸入書籤資料夾的名稱。
7. 在**「書籤名稱」**方塊中輸入書籤的名稱。
8. 按一下**「新增」**。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已將書籤新增至清單。

**如要使用加入書籤的查詢運算式：**

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 在搜尋方塊內按一下。

   搜尋方塊下方會顯示**「歷史記錄」**和**「書籤」**索引標籤。
3. 按一下**「書籤」**索引標籤。

   書籤清單會隨即顯示。
4. 按一下書籤以將其選取。

   Tenable Identity Exposure 將載入查詢運算式並執行搜尋。

**如要管理書籤：**

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 在搜尋方塊內按一下。

   搜尋方塊下方會顯示**「歷史記錄」**和**「書籤」**索引標籤。
3. 按一下**「書籤」**索引標籤。

   書籤清單會隨即顯示。
4. 按一下**「管理您的書籤」**。

   **「書籤」**窗格會隨即開啟。
5. 執行下列任一動作：

- 搜尋書籤：
  a. 在搜尋方塊中輸入書籤名稱。
  b. 從下拉式清單中選取一個資料夾。
- 編輯書籤或書籤資料夾的名稱：
  a. 按一下書籤或書籤資料夾的 圖示。
  b. 在**「書籤名稱」**或**「資料夾名稱」**方塊中，輸入新的書籤名稱或書籤資料夾的名稱。
  c. 按一下**「編輯」**。

     系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新書籤或書籤資料夾的名稱。
- 刪除書籤或書籤資料夾：
  - 按一下書籤或書籤資料夾的 圖示。

## 另請參閱

- 手動搜尋追蹤流程
- 使用精靈搜尋追蹤流程
- 自訂追蹤流程查詢
- 查詢歷史記錄
- 追蹤流程使用案例

## 查詢歷史記錄

當您在搜尋方塊中輸入運算式時，Tenable Identity Exposure 會將此運算式儲存在**「歷史記錄」**窗格中以供您重複使用。

**如要在歷史記錄中使用查詢運算式：**

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 在搜尋方塊內按一下。

搜尋方塊下方會顯示「**歷史記錄**」和「**書籤**」索引標籤。

3. 按一下「**歷史記錄**」索引標籤。

   查詢運算式清單會隨即顯示。

4. 按一下以選取要使用的查詢運算式。

   Tenable Identity Exposure 將載入查詢運算式並執行搜尋。




**如要管理您的查詢運算式歷史記錄：**

1. 在 Tenable Identity Exposure 中，按一下「**追蹤流程**」以開啟追蹤流程頁面。
2. 在搜尋方塊內按一下。

   搜尋方塊下方會顯示「**歷史記錄**」和「**書籤**」索引標籤。

3. 按一下「**歷史記錄**」索引標籤。

   查詢運算式清單會隨即顯示。

4. 按一下「**管理您的歷史記錄**」。

   「**歷史記錄**」窗格會隨即開啟。

5. 執行下列任一動作：

- 搜尋查詢運算式：

  a. 在搜尋方塊中輸入查詢運算式。

  b. 按一下「日曆」方塊以選取開始日期和結束日期。

  c. 按一下**「搜尋」**。

- 如要從歷史記錄中刪除查詢運算式：

  - 按一下 圖示。

- 如要從歷史記錄中清除全部查詢運算式：

  a. 按一下**「清除選取的項目」**。

  系統會顯示一則訊息，要求您確認刪除。

  b. 按一下**「確認」**。

## 另請參閱

- 手動搜尋追蹤流程
- 使用精靈搜尋追蹤流程
- 自訂追蹤流程查詢
- 書籤查詢
- 追蹤流程使用案例

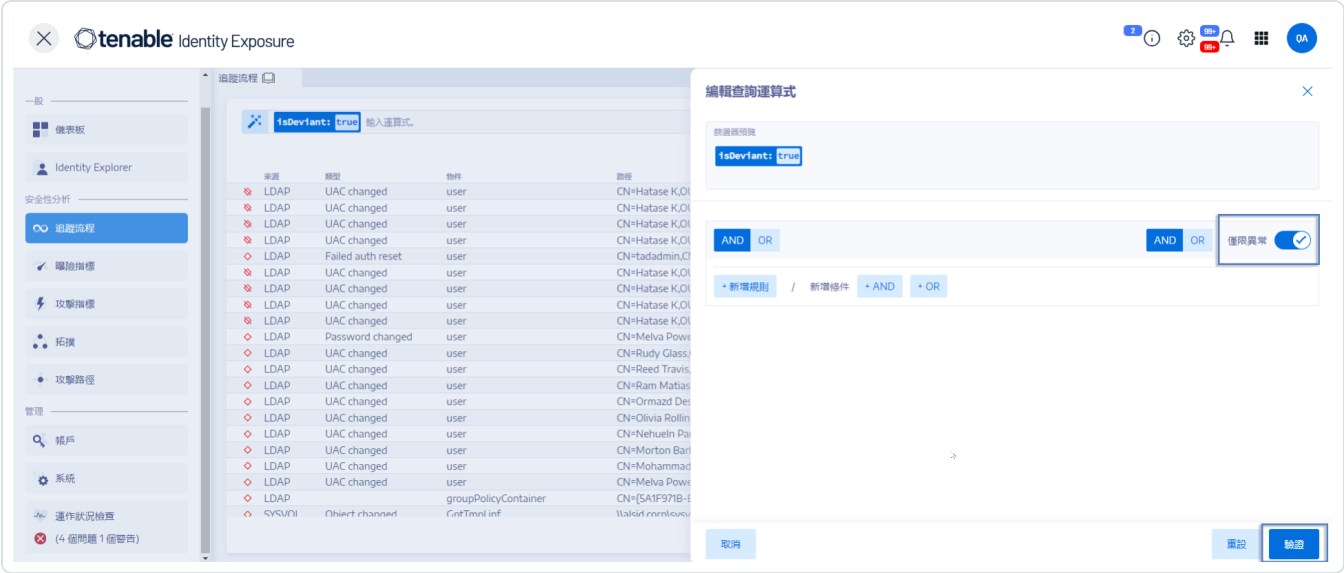
## 顯示異常事件

您可以直接將追蹤流程表中的異常事件歸零。

如要僅顯示異常事件：

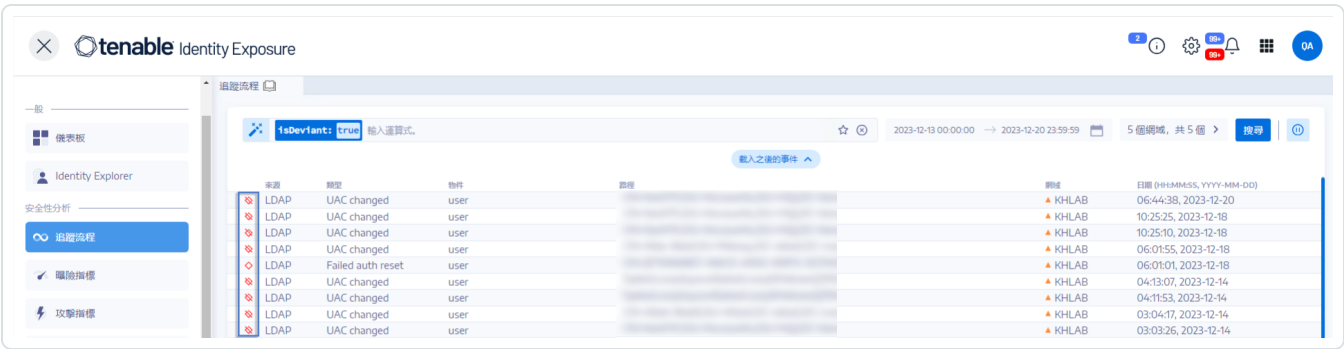
1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 按一下搜尋方塊旁邊的 圖示。

   **「編輯查詢運算式」**窗格會隨即開啟。




3. 按一下「**僅限異常**」切換為「允許」。
4. 按一下「**驗證**」。

   Tenable Identity Exposure 會使用來源旁邊帶有紅色菱形符號的事件清單更新追蹤流程表。




其中：

- ◇追蹤流程偵測到 Tenable Identity Exposure 安全性設定檔中存在異常情況。
- ◆追蹤流程偵測到其他安全性設定檔中存在異常情況。
- 顯示已透過變更解決異常情況。

## 事件詳細資料

Tenable Identity Exposure 中的追蹤流程提供有關影響您的 Active Directory (AD) 的每個事件的詳細資料。有關特定事件的詳細資料，您可以檢閱技術資訊，並依據曝險指標 (IoE) 的嚴重程度採取必要的補救措施。

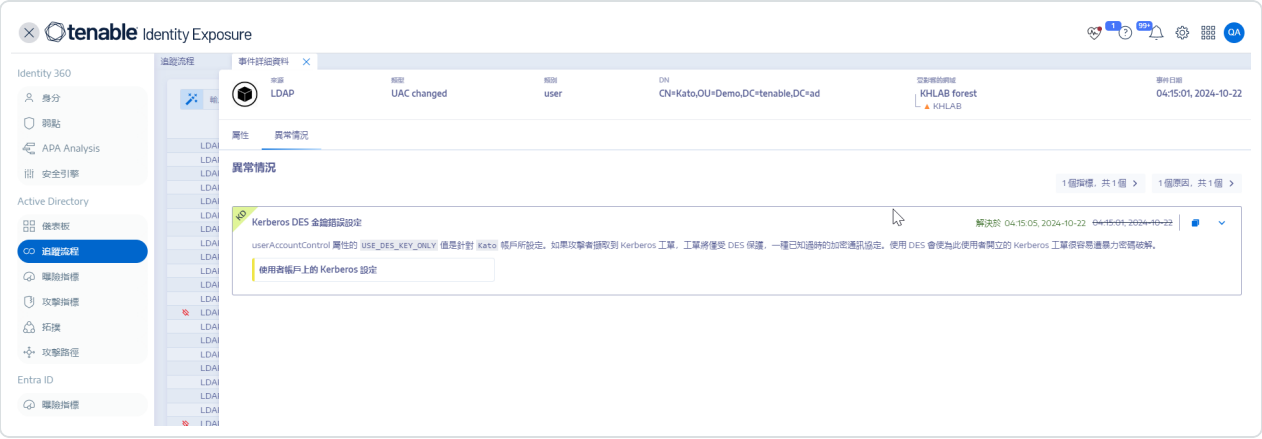
**如要檢閱事件詳細資料：**

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 按一下以選取追蹤流程表中的項目。

   **「事件詳細資料」**窗格會隨即開啟。

## 曝險指標 (IoE)、事件和異常物件

- **曝險指標** (IoE) 描述影響 AD 的威脅。Tenable Identity Exposure 的曝險指標 (IoE) 是在即時接收事件後評估安全性等級。曝險指標 (IoE) 可能包含多個技術弱點。曝險指標 (IoE) 提供有關偵測到的弱點、相關異常物件和補救措施建議的資訊。
- **事件**表示 AD 中可能出現的與安全性相關的變更，它可以是變更密碼、建立使用者、新建或修改 GPO 或新委派的權限等。事件可能會使曝險指標 (IoE) 的合規狀態從合規變成不合規。
- **異常物件**是一種技術元素 (可單獨存在或與另一個異常物件相關聯)，可讓曝險指標 (IoE) 的攻擊媒介發揮作用。如需詳細資訊，請參閱 曝險指標。




## 屬性表

屬性表包括以下欄：

| 欄 | 說明 |
| --- | --- |
| 屬性 | 指示與您在追蹤流程表中所選事件關聯的 AD 物件的屬性。屬性描述物件的特徵。多個屬性可以描述單一 AD 物件。 |
| 事件發生時的值 | 指示事件發生時的屬性值。 |
| 目前的值 | 指示您檢視時 AD 中屬性的值。 |

**提示**:如要顯示事件發生前的屬性值,請將游標移動至左側的藍點 (如果有) 上。

**如要搜尋屬性:**

- 在「**事件詳細資料**」窗格的「搜尋」方塊中輸入字串。

  Tenable Identity Exposure 會將清單縮小為與搜尋字串對應的屬性。

如需詳細資訊,請參閱 屬性變更。

## 異常情況

如果追蹤流程中的事件包含異常情況,則「事件詳細資料」窗格也會顯示這些異常,以便您深入瞭解問題的根源。

Tenable Identity Exposure 會將異常情況繫結至根物件,而且可以將其連結至多個罪證屬性。當您解決其中一個屬性時,Tenable Identity Exposure 就可以解決根物件的異常情況。接著,它會為根物件建立新的異常情況,並保留相同原因,但僅包含未解決的屬性。

例如,由於連接到多個相關物件 (**B**、**C** 和 **D**) 的單一原因,Tenable Identity Exposure 將異常情況繫結至物件 **A**。當您解決物件 **C** 的罪證屬性時,Tenable Identity Exposure 就可以解決物件 **A** 的異常情況。然後,它會為物件 **A** 建立新的異常情況,並將其連結至相同原因,但僅包含物件 **B** 和 **D**。

在此過程中,Tenable Identity Exposure 可以產生追蹤流程事件,將多個異常情況顯示為已解決,並以相同的時間戳記重新開啟。

**如要顯示異常情況:**

1. 在 Tenable Identity Exposure 中,按一下「**追蹤流程**」以開啟追蹤流程頁面。
2. 按一下以選取追蹤流程表中的項目。

「**事件詳細資料**」窗格會隨即開啟。

3. 選取「**異常情況**」索引標籤。

   Tenable Identity Exposure 會顯示異常情況清單和觸發異常情況的曝險指標 (IoE)。




**如要向下切入曝險指標 (IoE) 詳細資料：**

1. 在**異常情況**索引標籤中，按一下異常情況原因下方的曝險指標 (IoE) 圖塊。

   **指標詳細資料** 窗格會隨即開啟，其中包含異常物件清單和以下資訊：

   - 曝險指標 (IoE) 的名稱
   - 曝險指標 (IoE) 的嚴重性 (嚴重、高度、中度、低度)
   - 曝險指標 (IoE) 的狀態
   - 最近一次偵測的時間戳記

2. 按一下以下任一索引標籤：

   - **資訊**：包括曝險指標 (IoE) 的內部和外部資源。
   - **弱點詳細資料**：針對在您的 AD 中偵測到的弱點提供的解釋。
   - **異常物件**：包括技術詳細資料和用於篩選物件的搜尋方塊。
   - **建議**：包括有關如何解決問題的提示。

## 屬性變更

當屬性的值發生變化時，追蹤流程會在**屬性**欄前顯示一個藍點。

**如要顯示屬性變更：**

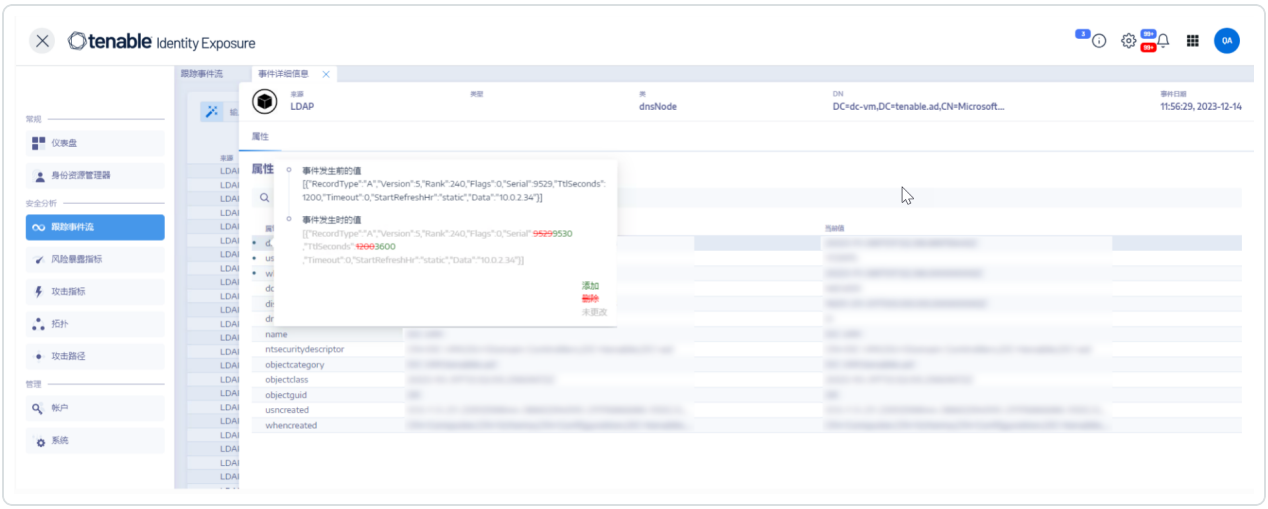
1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的**「追蹤流程」**。

   **追蹤流程**頁面會隨即開啟，其中包含事件清單

2. 將游標移動至事件行前面的藍點上即可顯示變更。

   **「事件當時的值」**標籤的顏色取決於套用至屬性的變更：

   - 綠色：**新增**
   - 紅色：**刪除**
   - 灰色：**不變**




## 「ntsecuritydescriptor」屬性

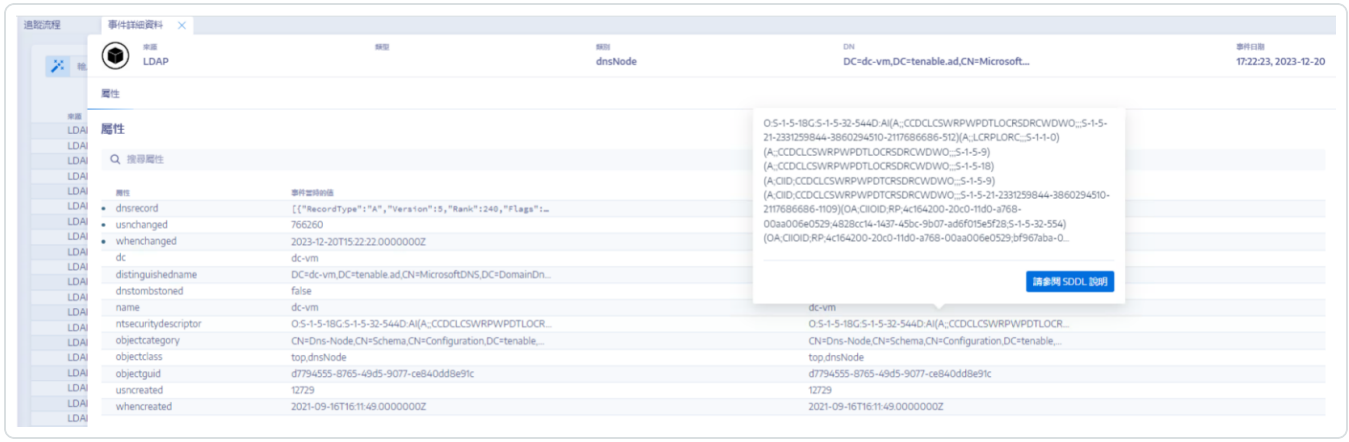
安全性描述元是一種資料結構，其中包含有關 AD 物件的安全資訊，例如其擁有權和權限。如需詳細資訊，請參閱 Microsoft 的線上說明文件。

**如要顯示物件安全性描述元的詳細資料：**

1. 在 Tenable Identity Exposure 中，按一下**「追蹤流程」**以開啟追蹤流程頁面。
2. 按一下以選取追蹤流程表中的項目。

   **「事件詳細資料」**窗格會隨即開啟。

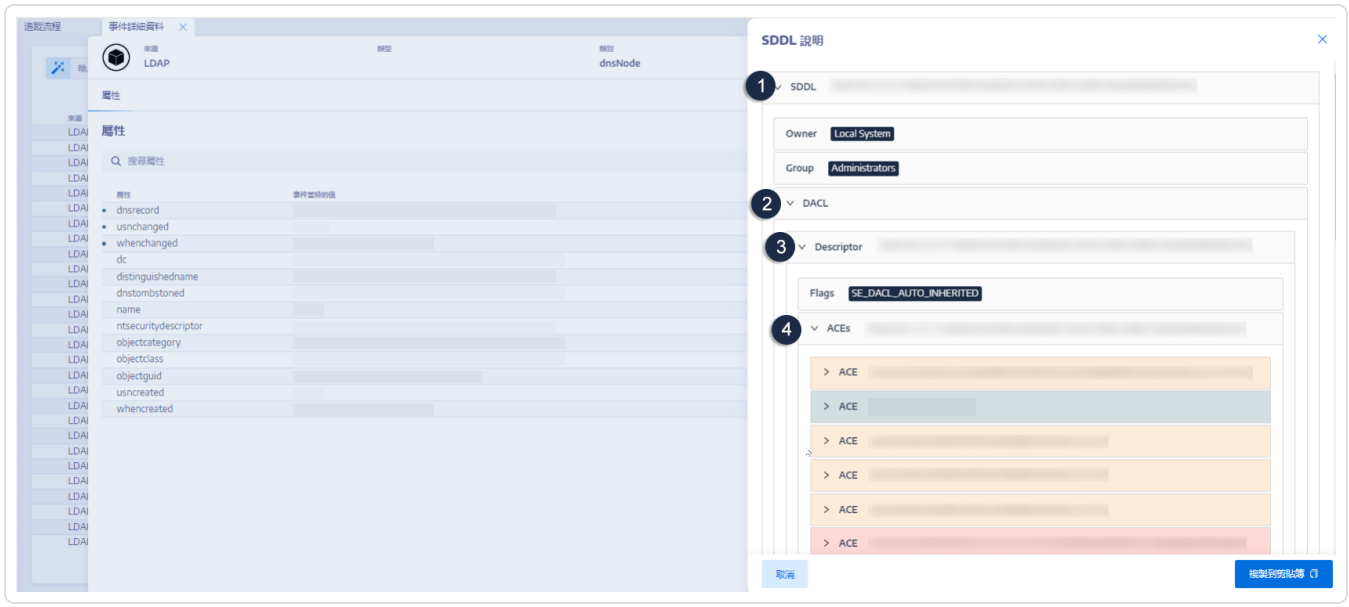
3. 將游標移動至 ntsecuritydescriptor 屬性項目 (事件發生時的值或目前值欄) 上方**。



4. 按一下「**檢閱 SDDL 描述**」。

   「**nSDDL 描述**」窗格開啟。

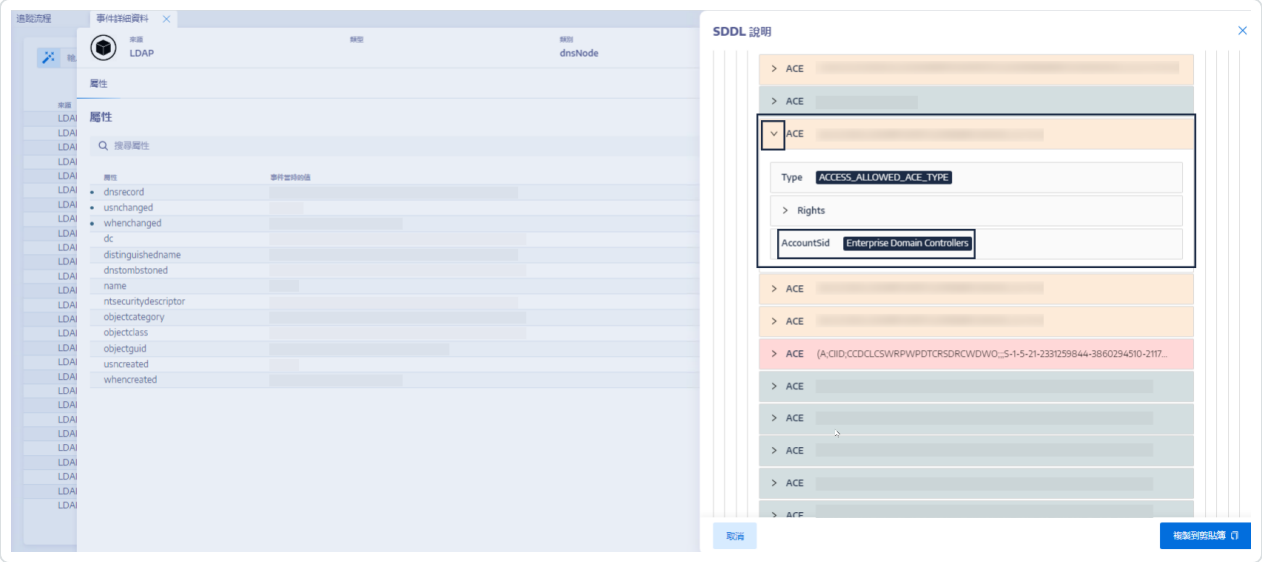
5. 按一下 SDDL (1)、DACL (2) 和描述元 (3) 左邊的箭頭展開描述：




6. 瀏覽到以顏色醒目提示的存取控制項目 (ACE) (4)，以顯示物件的存取權限。顏色代碼表示：

   - **紅色**：使用者被指派危險權限，但他們不應擁有對於此物件的存取權。
   - **橙色**：特權使用者被指派危險權限，但他們通常擁有此類權限 (例如：網域管理員)。

- **綠色**:沒有危險權限。




7. 如要複製 SDDL 描述,請按一下「**複製到剪貼簿**」。

## 追蹤流程使用案例

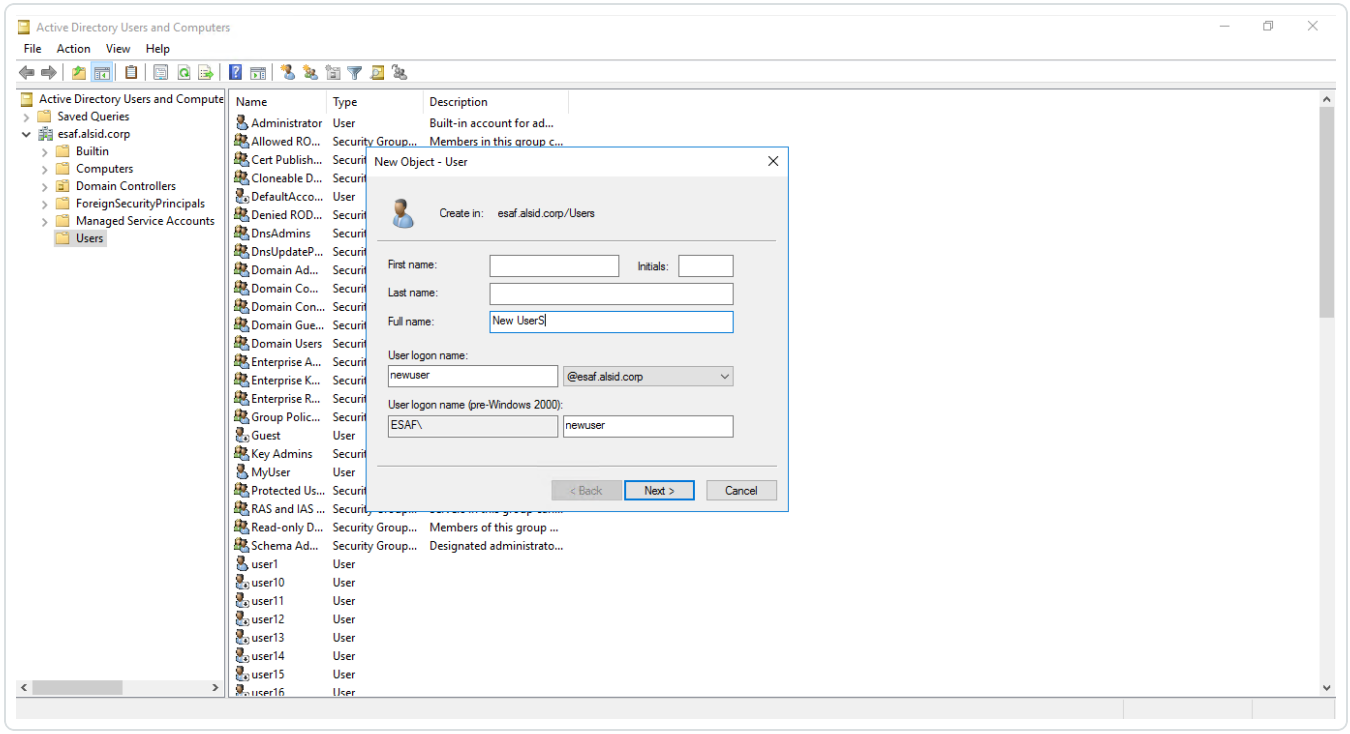
為幫助瞭解追蹤流程的行為,下面透過兩個範例說明您在 Active Directory (AD) 介面中執行的作業如何反映在追蹤流程頁面中。

每個範例都會將管理員端 (在 AD 介面中) 的資料與最終使用者端 (在 Tenable Identity Exposure中) 的資料進行比較。無論您是使用應用程式、API 還是服務在 AD 中執行作業,追蹤流程上的結果都是相同的。

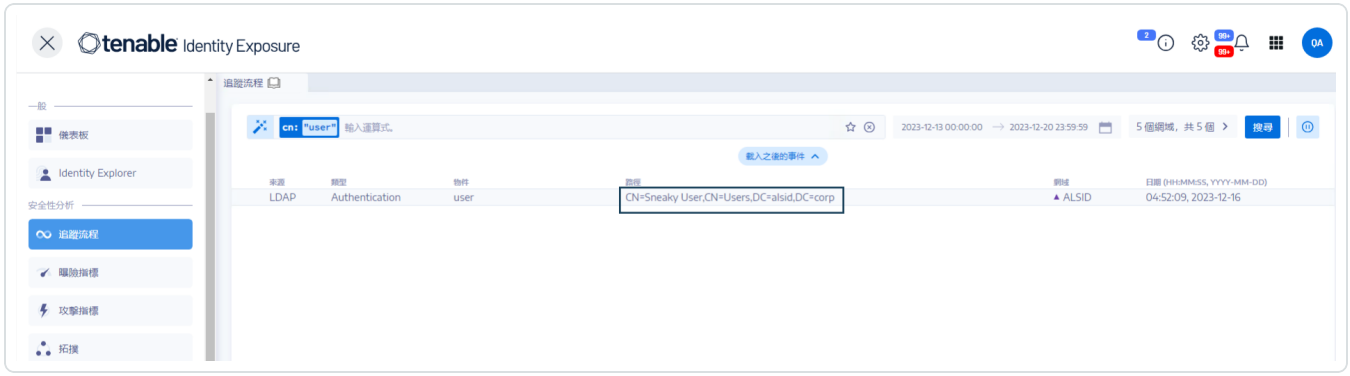
**注意**:這些範例並不詳盡,無法涵蓋所有可能的情況。

### 當您建立新的 AD 使用者帳戶時,追蹤流程會發生什麼?

- 在管理員端，您輸入有關新使用者帳戶的各種資訊。

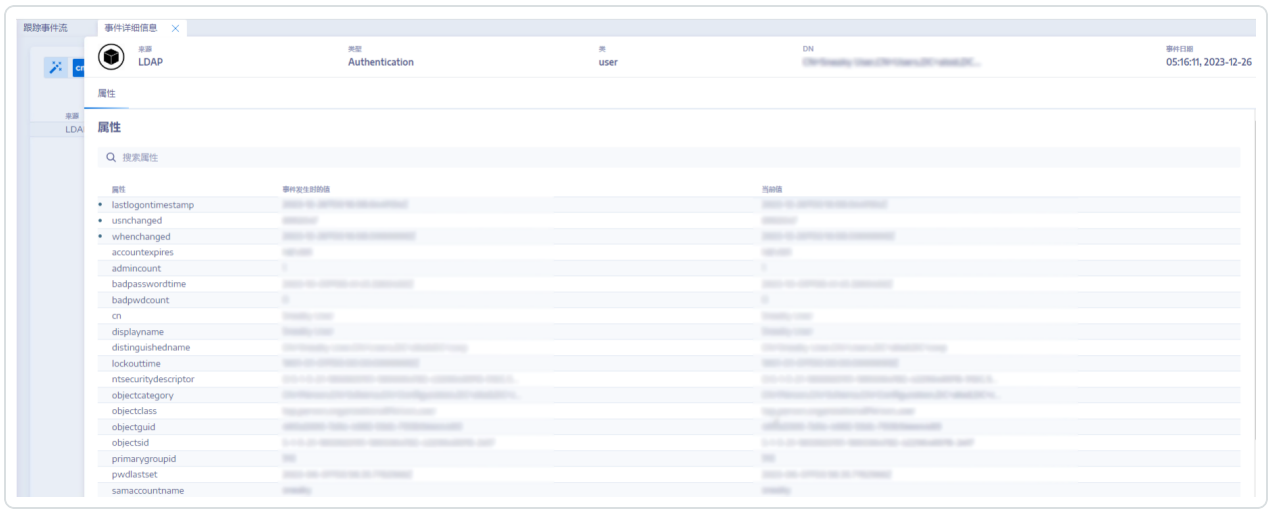



- 在最終使用者端，Tenable Identity Exposure 會更新**追蹤流程**頁面。請參閱指示*新物件*的**類型**欄。



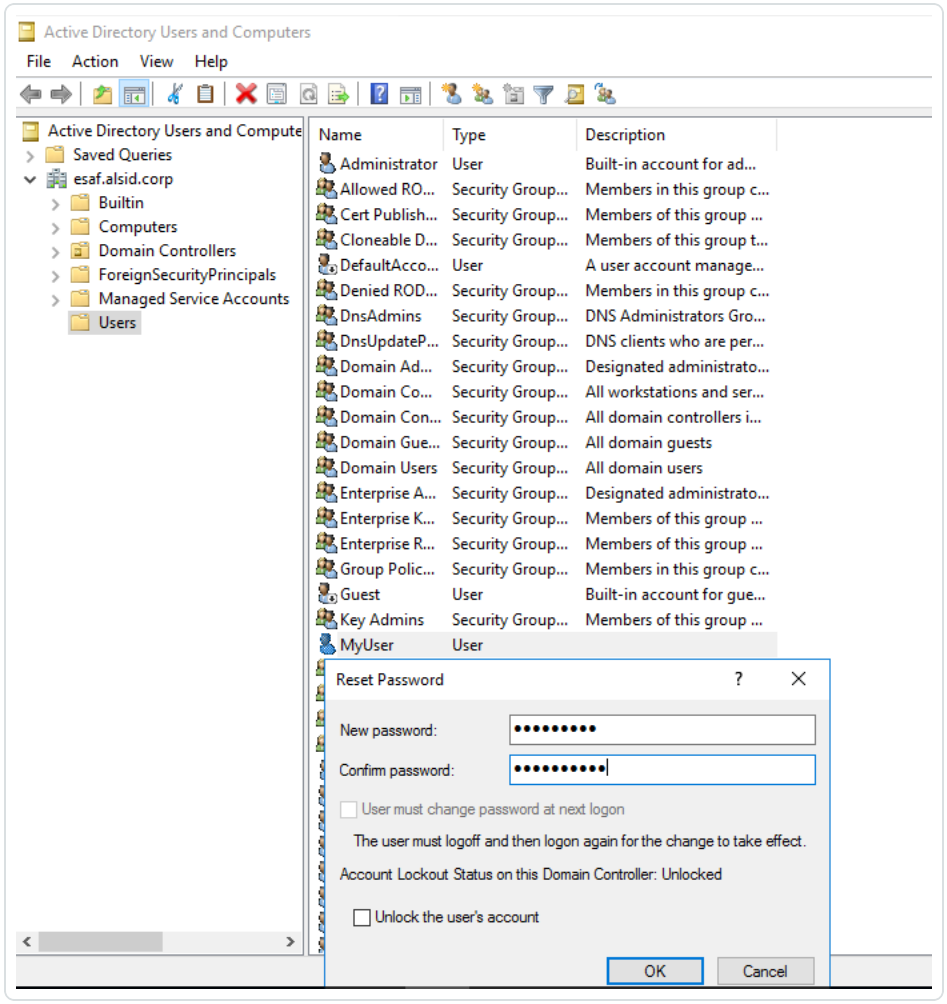

- **事件詳細資料**頁面也會反映這一變化。屬性名稱左側的藍點表示發生了更新。

  如需有關屬性的詳細資訊，請參閱檢視事件詳細資料。




## 當您變更 AD 使用者的密碼時，追蹤流程會發生什麼？

- 在管理員端，您輸入重設使用者密碼所需要的各種資訊。

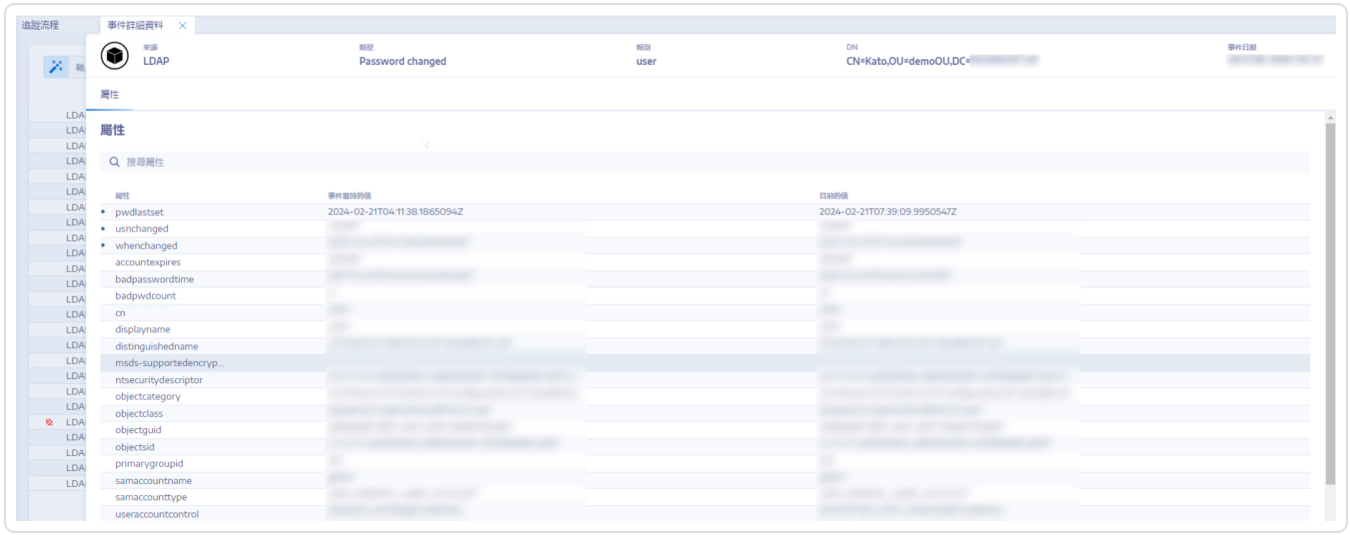



- 在最終使用者端，Tenable Identity Exposure 會更新**追蹤流程**頁面。請參閱指示「密碼已變更」的**類型**欄。



- **事件詳細資料**頁面還透過 whenchanged 屬性左側的藍點反映這一變化。

  如需有關屬性的詳細資訊，請參閱事件詳細資料。




## 另請參閱

- 手動搜尋追蹤流程
- 使用精靈搜尋追蹤流程
- 自訂追蹤流程查詢
- 書籤查詢
- 查詢歷史記錄

## 曝險指標

Tenable Identity Exposure 會透過曝險指標 (IoE) 衡量您 AD 基礎架構的安全成熟度，並向其監控和分析的事件流程指派嚴重性等級。Tenable Identity Exposure 在偵測到安全性降低時會觸發警示。

**如要顯示曝險指標 (IoE)：**

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的**「曝險指標」**。

   **「曝險指標」**窗格會隨即開啟。根據預設，Tenable Identity Exposure 僅顯示包含異常情況的曝險指標 (IoE)。

2. (選用) 如要顯示所有曝險指標，請按一下**「顯示全部指標」**切換為**「是」**。

Tenable Identity Exposure 曝險指標 (IoE) 具有一系列功能，可提升您的調查能力：

- 可供搜尋和篩選：套用樹系和網域的篩選器，輕鬆探索曝險指標 (IoE)。
- 匯出功能：異常情況物件讓您可匯出 CSV 格式的曝險指標 (IoE)。
- 對曝險指標 (IoE) 事件採取的措施：將暴露風險從白名單中移除/重新啟用。

曝險指標 (IoE) 的資料包括：

- 資訊部分：此部分提供每個曝險指標 (IoE) 的執行摘要，內容包括已知的攻擊工具、受影響的網域和相關說明文件。
- 弱點詳細資料：此部分提供更多關於 Active Directory 中錯誤設定的深入資訊。
- 異常物件：此部分著重於 Active Directory 中可能造成更廣泛攻擊破綻的錯誤設定。
- 建議：此部分引導您制定有效的設定策略，以盡可能減少攻擊破綻。

**如要搜尋曝險指標 (IoE)：**

1. 在**「曝險指標」**頁面頂端的「搜尋」方塊中輸入字串。可以是與曝險指標 (IoE) 相關的任何字詞，例如密碼、使用者、登入等等。
2. 按 Enter 鍵。

   曝險指標 (IoE) 頁面更新為與您的搜尋詞相關的指標。

**如要篩選特定樹系或網域的曝險指標 (IoE)：**

1. 按一下**「n/n 網域」**。

   **「樹系和網域」**窗格會隨即開啟。
2. 選取樹系或網域。
3. 按一下**「篩選選取的項目」**。

## 嚴重性等級

嚴重性等級可協助您評估偵測到的弱點的嚴重性，並決定修復動作的優先順序。

**「曝險指標」**窗格會按照以下方式顯示曝險指標 (IoE)：

- 按不同顏色的嚴重性等級。
- 垂直方向:嚴重性由高到低 (紅色代表優先順序最高,藍色代表優先順序最低)。
- 水平方向:複雜度由高到低。Tenable Identity Exposure 會以動態方式計算複雜度指標,指出修復異常曝險指標 (IoE) 的難度。

| 嚴重性 | 說明 |
|---|---|
| 嚴重:紅色 | 顯示如何防止某些無特權的使用者攻擊和入侵 Active Directory。 |
| 高度:橙色 | 表示導致憑證遭竊取或迴避安全機制的後滲透攻擊技術,或需要鏈結才具有危險性的滲透攻擊技術。 |
| 中度:黃色 | 指出對 Active Directory 基礎架構的有限風險。 |
| 低度:藍色 | 代表良好的安全做法。某些業務環境可能允許存在影響較小的異常情況,該類異常情況不一定會影響 AD 的安全性。只有在管理員犯了啟動非作用中帳戶等錯誤時,這些異常情況才會對 AD 造成影響。 |

## 異常情況解決與偵測日期

Tenable Identity Exposure 有時會使用與實際事件日期不同的解決日期或偵測日期。這是因為 Tenable Identity Exposure 儲存了在快取處理程序期間影響每個 Active Directory (AD) 物件的最近事件日期。

當 Tenable Identity Exposure 偵測到並解決影響 AD 物件的異常情況時,它會指派該物件最近的事件日期作為解決日期。

例如,當使用者的群組成員資格變更時,Tenable Identity Exposure 就會記錄群組的事件日期,而不是使用者。如果影響使用者的異常情況已透過群組成員資格變更解決,則 Tenable Identity Exposure 將使用使用者上次記錄的事件日期,而非群組成員資格變更的日期。

## 另請參閱

- 曝險指標詳細資料
- 異常物件
- 搜尋異常物件

- 略過異常物件或原因 (異常情況)
- 罪證屬性

## 曝險指標詳細資料

您可以查看特定曝險指標的詳細資料，瞭解與偵測到的弱點、相關異常物件以及修復建議有關的技術資訊。

如要顯示曝險指標詳細資料：

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的**「曝險指標」**。

   **「曝險指標」**窗格會隨即開啟。根據預設，Tenable Identity Exposure 僅顯示包含異常情況的曝險指標 (IoE)。

2. (選用) 如要顯示所有曝險指標，請按一下**「顯示全部指標」**切換為**「是」**。

3. 按一下頁面上的任何**「曝險指標」**圖塊。

   **「指標詳細資料」**窗格會隨即開啟。

   在畫面頂端，**「指標詳細資料」**窗格彙總了追蹤流程表中已提供的資訊：

   - 曝險指標 (IoE) 的**名稱**
   - 其**嚴重性**等級 (嚴重、高度、中度或低度)。
   - 曝險指標 (IoE) 合規性**狀態**，根據 Tenable Identity Exposure 上次執行的分析結果。
   - **上次偵測時間**，指出 Tenable Identity Exposure 上次執行分析的時間。

4. 按一下下面的任一索引標籤，可提供有關曝險指標 (IoE) 的更多詳細資料：

| 索引標籤 | 說明 |
| --- | --- |
| 資訊 | 包括有關曝險指標 (IoE) 的內部和外部資源，例如：<br>• 執行摘要：問題概覽，有助於您做出適當決策。<br>• 文件：曝險指標 (IoE) 上外部資源的連結。<br>• 攻擊者已知工具：入侵攻擊工具的名稱。<br>• 受影響網域的樹狀結構。 |
| 弱點詳細資料 | 說明在您的 AD 中偵測到的弱點，以及如果不採取修復動作，這些弱點會對您的 Active Directory (AD) 造成哪些風險。 |
| 異常物件 | 異常物件揭露了 AD 中存在的弱點或可能的危險行為。您可以將篩選器套用至異常物件以準確顯示嚴重問題。<br>當曝險指標 (IoE) 的狀態為合規並且包含異常物件時，您可以採取修復動作來更正 Tenable Identity Exposure 偵測到的安全性缺陷。如需詳細資訊，請參閱 異常物件。 |
| 建議 | 有關如何重新符合安全要求以及改進 AD 安全的提示：<br>• 執行摘要提供 Tenable Identity Exposure 建議的解決方案概覽。<br>• 「詳細資料」子區段提供有關如何執行行動計畫的建議，並且可以協助管理員對 AD 基礎架構作出必要變更。<br>• 「文件」子區段提供建議的解決方案或威脅的外部資源連結。 |

## 另請參閱

- 曝險指標
- 異常物件
- 搜尋異常物件

- 略過異常物件或原因 (異常情況)
- 罪證屬性

## 異常物件

Tenable Identity Exposure 的曝險指標 (IoE) 可以標記異常物件，這些異常物件揭示 Active Directory (AD) 中的弱點或潛在危險行為。關注這些異常物件可以幫助您查明關鍵問題並進行補救。您可以執行下列任一動作：

- 搜尋異常物件。
- 在一段時間內略過異常物件。
- 選取樹系和網域以搜尋異常物件。
- 取得影響曝險指標 (IoE) 之罪證屬性的相關說明。
- 下載顯示所有異常物件的報告。

如要顯示異常物件：

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的**「曝險指標」**。

   **「曝險指標」**頁面會隨即開啟。根據預設，Tenable Identity Exposure 僅顯示包含異常情況的曝險指標 (IoE)。

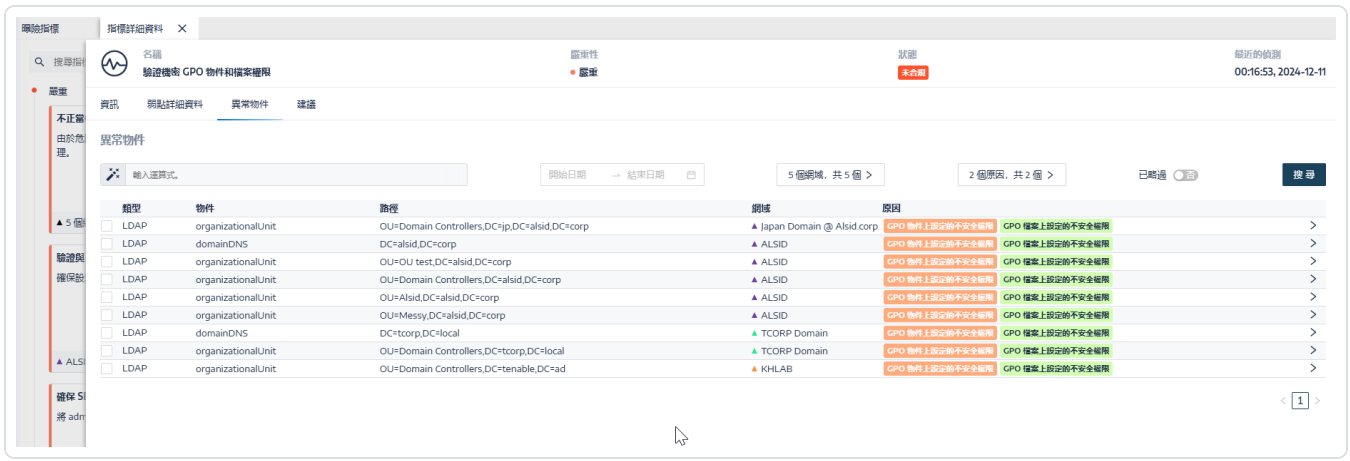
2. 按一下頁面上的任何**「曝險指標」**圖塊。

   **「指標詳細資料」**窗格會隨即開啟。




3. 按一下**「異常物件」**索引標籤。

   與曝險指標 (IoE) 相關的異常物件清單會隨即顯示。




異常物件表包含下列資訊：

- **類型**：指出 AD 中任何安全性相關變更的來源 (LDAP 或 SMB 通訊協定)。
- **物件**：指出與 AD 物件關聯的類別或副檔名。
- **路徑**：指出 AD 物件的完整路徑，您可以藉此識別物件在 AD 中的唯一位置。
- **網域**：指出 AD 中變更的來源網域。
- **原因**：列出影響異常物件的罪證屬性。

如要匯出異常物件報告：

1. 在「**異常物件**」頁面底部，按一下「**全部匯出**」。

   「**匯出異常物件**」窗格會隨即開啟。

2. 在「**匯出格式**」方塊中，按一下下拉箭頭以選取格式。
3. 按一下「**全部匯出**」。

   Tenable Identity Exposure 會將異常物件報告下載至您的電腦。

## 另請參閱

- 曝險指標
- 曝險指標詳細資料
- 搜尋異常物件

- 略過異常物件或原因 (異常情況)
- 罪證屬性

## 搜尋異常物件

您可以手動搜尋異常物件，也可以使用精靈搜尋。

**精靈搜尋**

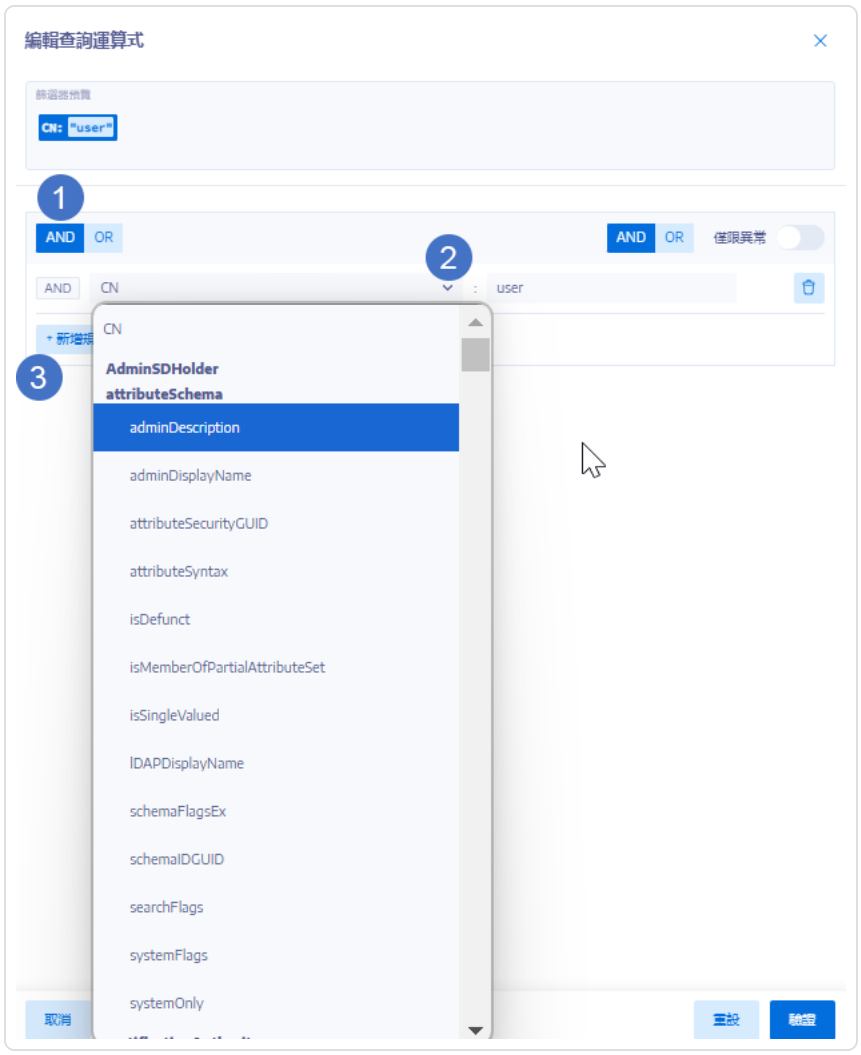
搜尋精靈可以協助您建立查詢運算式。

- 在搜尋方塊中使用常用運算式時，您可以將它們新增到書籤清單中以供日後使用。
- 當您在搜尋方塊中輸入運算式時，Tenable Identity Exposure 會將此運算式儲存在「歷史記錄」窗格中以供您重複使用。

如要使用精靈搜尋異常物件：

1. 顯示 異常物件 清單。
2. 按一下 圖示。

   **「編輯查詢運算式」**窗格會隨即開啟。




3. 如要在面板中定義查詢運算式，請按一下「**AND**」或「**OR**」運算子按鈕 (1) 以套用到第一個條件。
4. 從下拉式功能表中選取一個屬性並輸入其值 (2)。
5. 執行下列任一動作：
   - 如要新增屬性，請按一下「**+ 新增規則**」(3)。
   - 如要新增另一個條件，請按一下「**新增條件**」「**+AND**」或「**+OR**」運算子。從下拉式功能表中選取一個屬性並輸入其值。
   - 如要將搜尋限制為異常物件，請按一下「**僅限異常**」切換為允許。選取「**+AND**」或

「+OR」運算子將條件新增到查詢。

- 如要刪除條件或規則，請按一下 圖示。

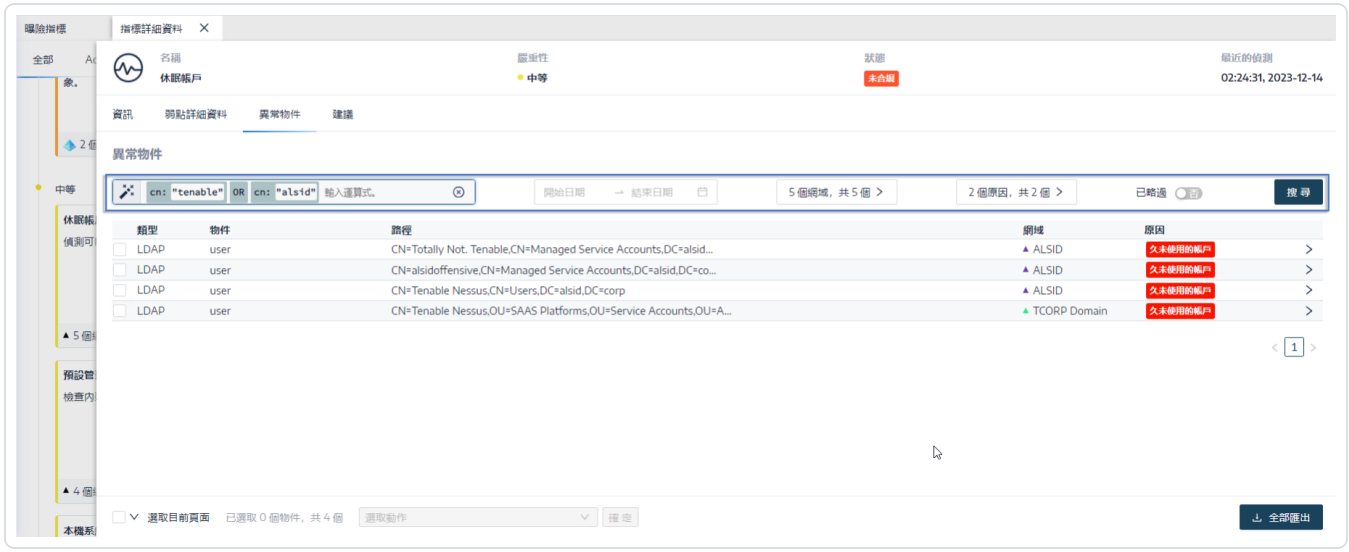
6. 按一下「**驗證**」以執行搜尋，或按一下「**重設**」以修改您的查詢運算式。

## 手動搜尋

如要篩選符合特定字元字串或模式的異常物件，您可以在搜尋方塊中輸入運算式，以使用布林運算子 *、AND 和 OR 縮小搜尋結果範圍。您可以用括號封裝 OR 陳述式來修改搜尋優先順序。搜尋功能會在 Active Directory 屬性中尋找任何特定值。如要手動搜尋追蹤流程：

如要手動搜尋異常物件：

1. 顯示 異常物件 清單。




2. 在搜尋方塊中輸入查詢運算式。
3. 您可以按如下方式篩選搜尋結果：
   - 按一下「**日曆**」方塊以選取開始日期和結束日期。
   - 按一下「**n/n 網域**」以選取樹系和網域。
4. 按一下「**搜尋**」。

   Tenable Identity Exposure 將使用符合搜尋條件的結果更新清單。

## 文法和語法

手動查詢運算式使用以下文法和語法：

- 文法：`EXPRESSION [OPERATOR EXPRESSION]*`
- 語法：`__KEY__ __SELECTOR__ __VALUE__`

  其中：

  - `__KEY__` 指的是要搜尋的 AD 物件屬性 (如 `CN`、`userAccountControl`、`members` 等)
  - `__SELECTOR__` 指的是運算子：`:`、`>`、`<`、`>=`、`<=`。
  - `__VALUE__` 指的是要搜尋的值。

    您可以使用更多索引鍵來尋找特定內容：

  - `isDeviant` 可尋找造成異常情況的事件。

您可以使用 **AND** 和 **OR** 運算子組合多個追蹤流程查詢運算式。

範例：

- 尋找通用名稱屬性中包含 `alice` 字串的所有物件：`cn:"alice"`
- 尋找通用名稱屬性中包含 `alice` 字串並且建立了特定異常情況的所有物件：`isDeviant:"true" and cn:"alice"`
- 尋找名為「預設網域原則」的 GPO：`objectClass:"groupPolicyContainer" and displayname:"Default Domain Policy"`
- 尋找 SID 中含有 S-1-5-21 的所有已停用帳戶：`userAccountControl:"DISABLE" and objectSid:"S-1-5-21"`
- 尋找 SYSVOL 中所有的 `script.ini` 檔案：`globalpath:"sysvol" and types:"SCRIPTSini"`

  > **注意**：此處的 `type` 是指物件屬性，而非欄標頭。

## 另請參閱

- 曝險指標
- 曝險指標詳細資料
- 異常物件
- 略過異常物件或原因 (異常情況)
- 罪證屬性

## 略過異常物件或原因 (異常情況)

在 Tenable Identity Exposure 中，**異常物件** 是指 Active Directory (AD) 中呈現異常或危險行為的任何物件，例如不當的設定或權限，進而可能暴露安全性弱點。這些物件是透過 Tenable 的曝險指標 (IoE) 識別的，曝險指標可識別與最佳做法和安全性規範的偏差。

**原因** (又稱為「**異常情況**」) 是指造成物件異常的特定屬性或因素。曝險指標 (IoE) 之所以會將物件標記為異常，可能有多個原因。例如，物件會因不正確的檔案權限、錯誤設定或有風險的委派而被標記為異常，其中每一個都代表一個不同的「原因」。

總結來說：

- **異常物件**：因有風險或異常行為而遭到標記的 AD 物件。
- **原因/異常情況**：造成曝險指標 (IoE) 標記物件的特定屬性或因素。

這些原因對於了解與每個異常物件相關的基礎安全性弱點至關重要。

**略過異常物件**

當您選擇略過異常物件時，也會略過所有相關聯的原因或異常情況。

當某些標記的物件並非需立即關注的問題時，這麼做對於減少介面的雜亂感非常有用。

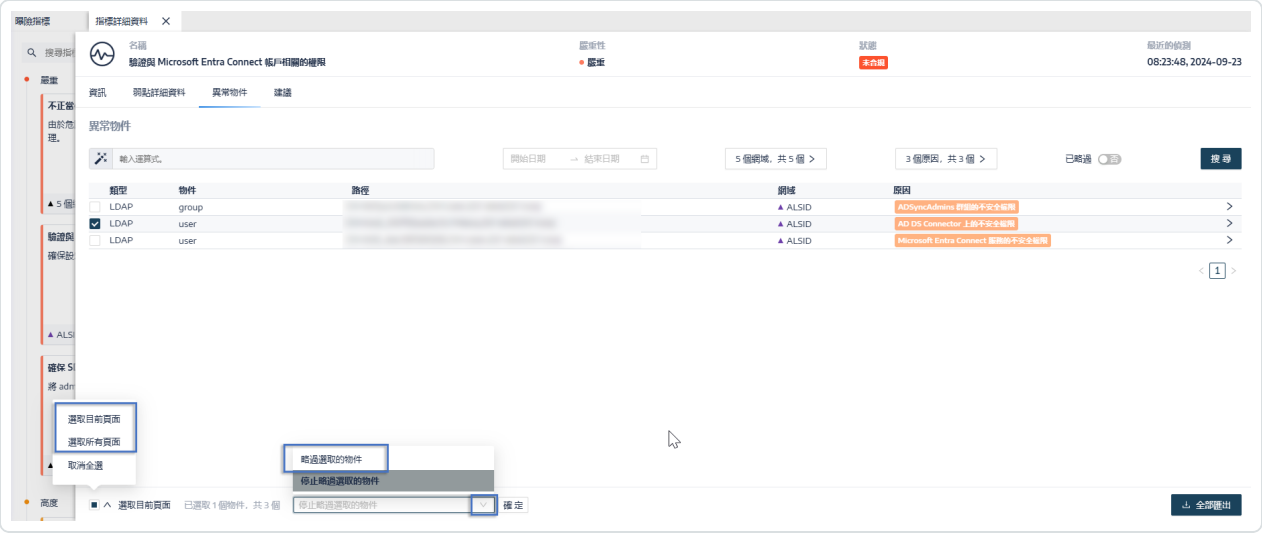
但是，略過這些物件並不能解決根本問題；只會防止這些物件在指定的時間範圍內出現在報告或調查畫面中。

如要略過異常物件：

1. 在 Tenable Identity Exposure 中顯示 異常物件 清單
2. 針對要略過的異常物件，選取前方的核取方塊。
3. 或者，您也可以篩選要略過的異常物件：

- 按一下「**日曆**」方塊以選取開始日期和結束日期。
- 按一下「**n/n 網域**」以選取樹系和網域。

**提示**：如要加快選取速度，您可以勾選頁面底部的「**選取所有頁面**」或「**選取目前頁面**」方塊。




4. 從頁面底部的下拉式清單中選取「**略過選取的物件**」。
5. 按一下「**確定**」。

   「**略過選取的物件**」窗格會隨即顯示。
6. 按一下「**略過截止日期**」方塊以顯示日曆，然後選擇一個日期，Tenable Identity Exposure 必須在此日期之前略過此異常物件。
7. 按一下「**確定**」。

   Tenable Identity Exposure 會顯示確認訊息並更新剩餘異常物件清單。

如要顯示略過的異常物件：

1. 按一下「**已略過**」切換為「**是**」。
2. 在頁面底部，按一下「**選取所有頁面**」。
3. 從下拉式清單中選取「**停止略過選取的物件**」。
4. 按一下「**確定**」。

確認窗格會隨即顯示。

5. 按一下「**確定**」以驗證您的更改。

   Tenable Identity Exposure 會顯示已略過的異常物件。

## 略過原因或「異常情況」

當您選擇略過 Tenable Identity Exposure 中的特定原因 (或「異常情況」) 時，曝險指標 (IoE) 會停止向您顯示有關該特定問題的警示，但不會解決問題本身。

作用中的監控儀表板中不會再出現已略過的異常情況，有效地對因該特定原因而觸發的警示進行靜音處理。

不過，除非您一併個別略過，否則同一物件相關的其他異常情況仍會繼續觸發警示。

如要略過原因 (「異常情況」):

1. 在 Tenable Identity Exposure 中顯示 異常物件 清單

   異常物件清單會隨即顯示。

2. 識別異常物件並按一下行末的箭頭 (>)。

   檢視會展開，以顯示原因的詳細資料。

3. 按一下行末的核取方塊。如果有多個原因，請選取要略過的原因，或按一下「**全選**」以略過所有相關的原因。




4. 按一下「**確定**」。

「**略過所選異常情況**」窗格會隨即顯示。

5. 按一下「**略過截止日期**」方塊以顯示日曆，然後選擇一個日期，Tenable Identity Exposure 必須在此日期之前略過此異常情況。
6. 按一下「**確定**」。

   Tenable Identity Exposure 會顯示確認訊息並更新剩餘異常情況的清單。

若要顯示已略過的異常情況：

1. 按一下「**已略過**」，切換為「**是**」。

   異常物件清單隨即更新，以顯示包含所有原因的展開檢視。略過的原因顯示  圖示。
2. 選取已略過的原因，然後從下拉式清單中按一下「停止略過所選的異常情況」。
3. 按一下「**確定**」。

   「停止略過所選異常情況」窗格隨即顯示。
4. 按一下「**確定**」。

   Tenable Identity Exposure 會顯示確認訊息並更新剩餘異常情況的清單。

## 另請參閱

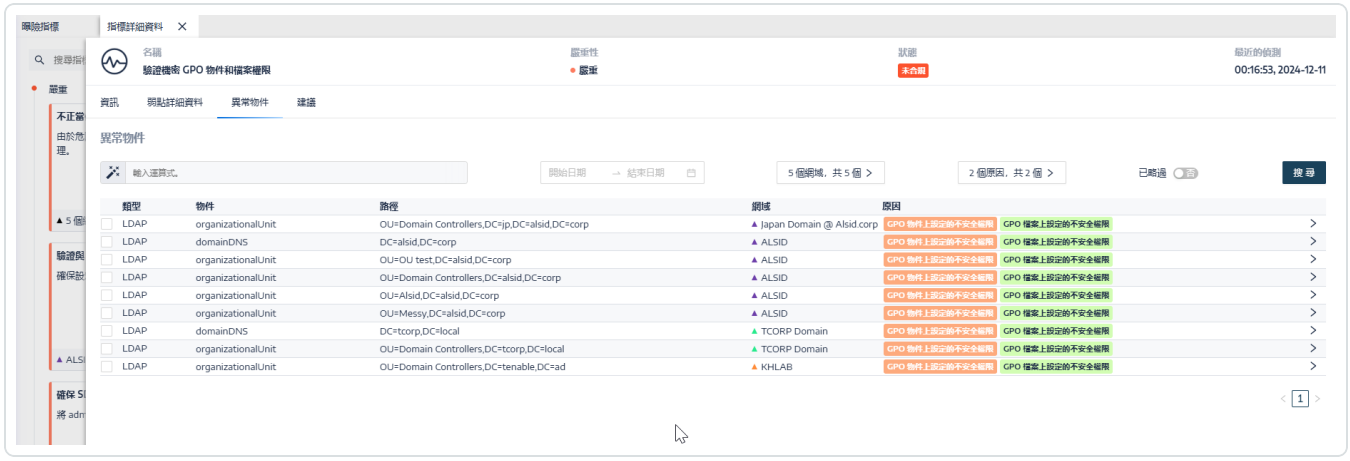
- 曝險指標
- 曝險指標詳細資料
- 異常物件
- 搜尋異常物件
- 罪證屬性

## 罪證屬性

Tenable Identity Exposure 會顯示觸發曝險指標 (IoE) 中異常物件的罪證屬性，並提供理由，以協助您瞭解異常狀況並加以修復。

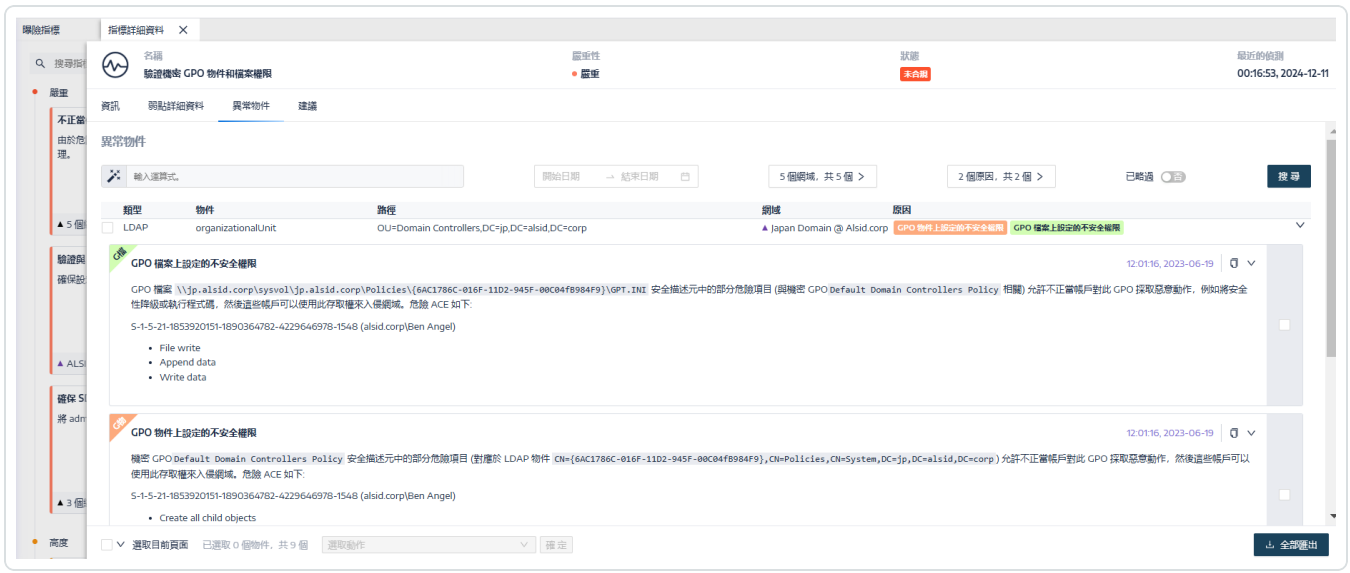
如要檢視罪證屬性：

1. 顯示 異常物件 清單。




2. 按一下異常物件清單中的項目。

   Tenable Identity Exposure 會顯示此異常物件的罪證屬性清單：




此清單包含以下資訊：

- **不同顏色的標籤**：當有數個不同原因時，可用於區分。
- 值：
  - ?：表示異常行為的遺漏 (空) 屬性值。
  - 沒有適用於此異常狀況的說明：偵測日期回溯至 2.6 版，Tenable Identity Exposure 不再管理此屬性。

如要複製罪證屬性：

- 選取屬性並按一下  圖示。

## 另請參閱

- 曝險指標
- 曝險指標詳細資料
- 異常物件
- 搜尋異常物件
- 略過異常物件或原因 (異常情況)

## 根據 RSoP 的曝險指標

Tenable Identity Exposure 使用一組以 RSoP (原則結果集) 為根據的曝險指標 (IoE) 來評估和確保各個方面安全無虞、遵循法規。本節提供有關特定 RSoP 曝險指標 (IoE) 目前行為的見解，以及 Tenable Identity Exposure 如何解決與其運算相關的效能問題。

下列根據 RSoP 的曝險指標 (IoE) 在 Tenable Identity Exposure 的安全架構中發揮作用：

- 特權使用者的登入限制
- 危險機密特權
- 針對使用者套用脆弱密碼原則
- 針對勒索軟體的強化措施不足
- 不安全的 Netlogon 通訊協定設定

這些曝險指標 (IoE) 依賴在需要時初始化的 RSoP 運算結果快取，這些運算值會依要求新增，而非依賴先前存在的值。先前，對 `AdObjects` 的變更會觸發快取無效判定程序，造成在曝險指標 (IoE) 的 RSoP 執行期間頻繁重新運算。

Tenable Identity Exposure 解決了與 RSoP 運算相關的效能影響，具體情況如下：

1. **包含可能過時資料的即時曝險指標 (IoE) 分析**：即使用於處理的資料可能不是最新版本，根據 RSoP 的曝險指標 (IoE) 運算也會在發生輸入/輸出事件時即時進行。可能會讓 RSoP 快取失效的緩衝事件在符合特定條件前維持儲存狀態，等到符合條件後再開始預

定的運算作業。

2. **排定的 RSoP 無效判定程序**:符合重新運算的條件後,系統會讓 RSoP 快取失效,並在無效判定程序期間將緩衝事件納入考量。
3. **使用最新的快取重新執行曝險指標 (IoE)**:在快取失效之後,曝險指標 (IoE) 會使用快取中最新版本的 `AdObject` 重新執行,對象也包含緩衝事件。Tenable Identity Exposure 會逐一執行每項緩衝事件的曝險指標 (IoE) 運算作業。

基於這些原因,加快根據 RSoP 的曝險指標 (IoE) 運算時間會導致與 RSoP 相關的異常情況運算變慢。

## 增強功能

Tenable Identity Exposure 針對處理 RSoP 工作的曝險指標實施變更,以改善其整體效能和回應能力。

- **更智慧的安全檢查**:重新設計我們執行特定安全性檢查 (稱為 RSoP 檢查) 的方式,以減少系統減速的情況。
- **適應性排程**:系統會根據目前的工作負載,自動選擇執行這些檢查的最佳時間。
- **過載保護**:我們已實施新的措施來防止系統在忙碌期間過載。
- **GPO 檔案安全性分析**:分析 GPO 檔案安全性的曝險指標現在每 30 分鐘處理一次,不像其他曝險指標 (IoE) 那樣即時處理。

## 好處

- **更快速的回應時間**:透過最佳化安全性檢查程序,您應該會發現系統回應速度更快,特別是在使用高峰期。
- **改善可靠性**:新的適應性排程有助於確保重要的安全性檢查不會干擾您的工作。
- **更順暢的體驗**:透過更完善的過載保護,即使在使用量大的情況下,系統也應能維持一致的效能。
- **增強平台穩定性**:這些變更特別有利於 AD 活動頻繁的用戶端,可確保更一致的效能。

## 技術層面

- RSoP 檢查和 GPO 檔案安全性分析會定期執行，而非即時執行。
- 平台每 30 分鐘會評估一次其工作負載。如果判斷為可處理分析則繼續，否則會等到負載減少為止。
- 實施可偵測系統過載的演算法，以考量訊息佇列長度和處理趨勢等因素。
- 在過載期間延遲非重要檢查，以維持系統回應能力。

## 修復曝險指標中的異常情況

曝險指標 (IoE) 遇到需要修復的異常物件時，Tenable Identity Exposure 會觸發警示。

下列範例說明如何針對三個特定曝險指標 (IoE) 執行修復程序。

- 針對標準使用者設定的 AdminCount 屬性
- 危險的 Kerberos 委派作業
- 確保 SDProp 一致性

如需曝險指標 (IoE) 的完整資訊，請參閱 Tenable Identity Exposure 使用者介面中提供的說明文件。

### 針對標準使用者設定的 AdminCount 屬性

使用者帳戶上的 `adminCount` 屬性表示系統管理群組中的過去成員資格，其在帳戶離開群組時不會重設。因此，即使舊的系統管理帳戶已有此屬性，其仍會封鎖 Active Directory 權限的繼承。此屬性原用途雖為保護管理員，但卻可能會產生難以處理的權限問題。

此中等曝險指標 (IoE) 只會報告具有此屬性的作用中使用者帳戶和群組，並排除具有正當成員且 `adminCount` 屬性設為 `1` 的特權群組。

如要修復**標準使用者上設定的 AdminCount 屬性**曝險指標 (IoE) 中的異常物件：

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的**「曝險指標」**以開啟。

   根據預設，Tenable Identity Exposure 僅會顯示包含異常物件的曝險指標 (IoE)。

2. 按一下**標準使用者上設定的 AdminCount 屬性**曝險指標 (IoE) 的圖塊。



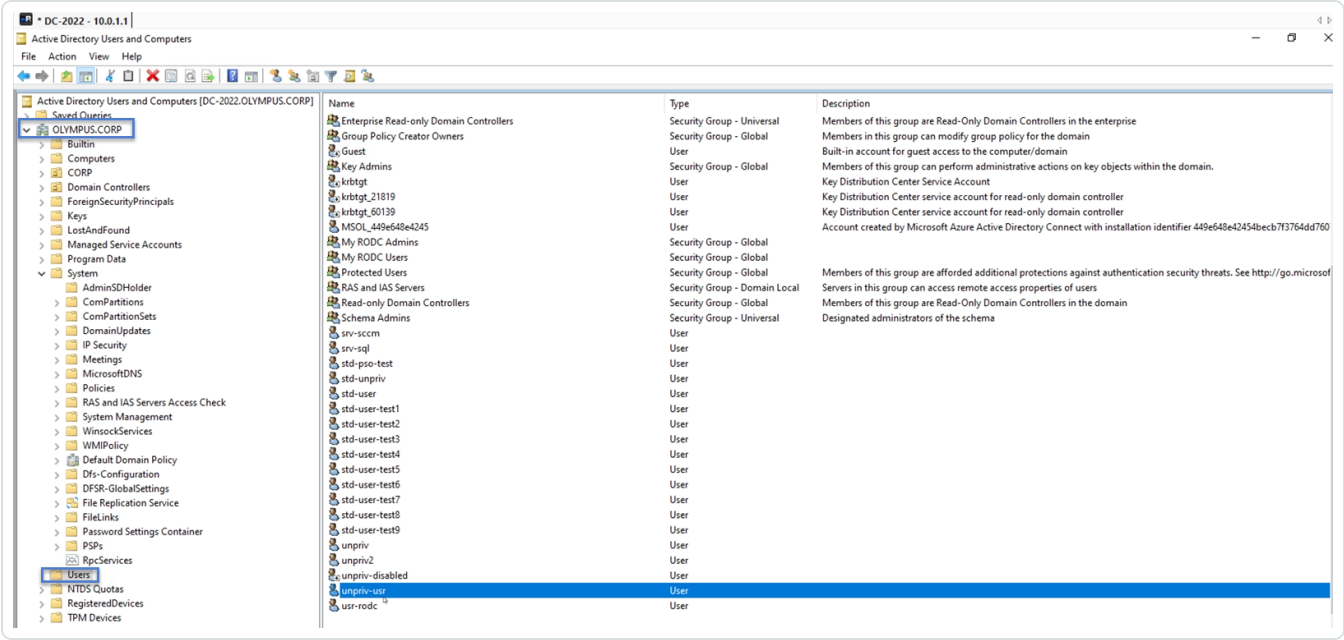

「**指標詳細資料**」窗格會隨即開啟。

3. 將游標停留在異常物件上並按一下即可顯示詳細資料，記下網域名稱和帳戶(在此範例中：網域為 `OLYMPUS.CORP`，標準帳戶為 `unpriv-usr`)。



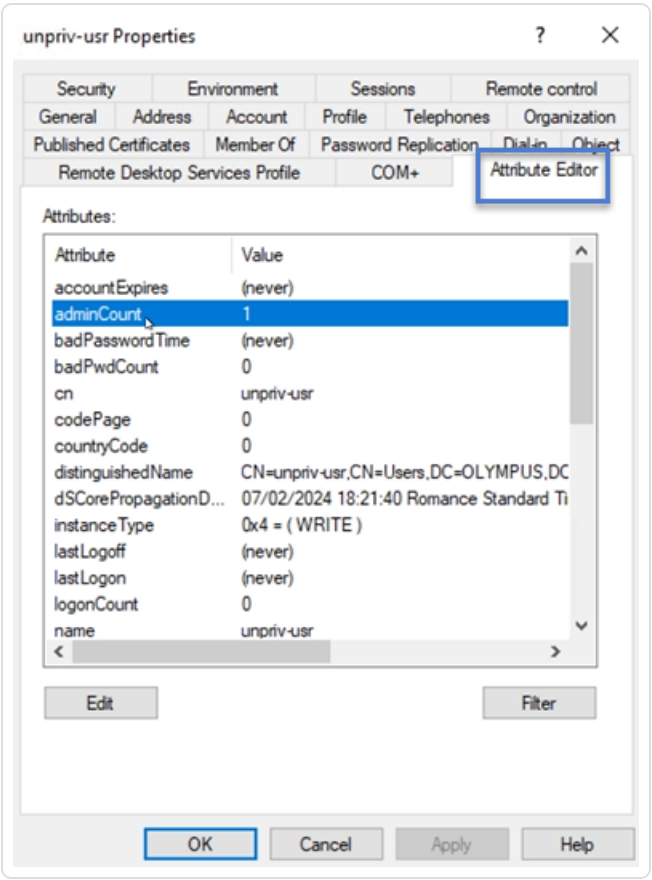

4. 在 Remote Desktop Manager (或類似工具) 中，找到網域名稱並導覽至 Tenable Identity Exposure 標記的**使用者**和帳戶。

> **必要權限**：您必須擁有網域的管理員帳戶才能執行程序。

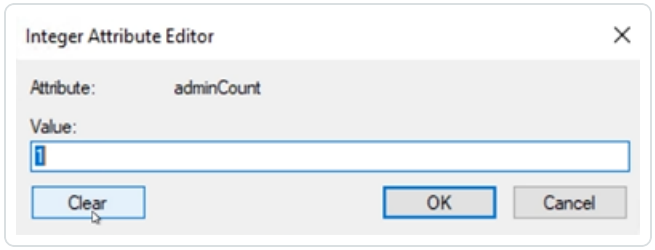



5. 按一下帳戶名稱以開啟「**內容**」對話方塊，然後選取「**屬性編輯器**」索引標籤。

6. 在屬性清單中按一下 `adminCount` 以開啟「**整數屬性編輯器**」對話方塊。



7. 在對話方塊中按一下「**清除**」和「**確定**」。




8. 在 Tenable Identity Exposure 中，返回「指標詳細資料」窗格並重新整理頁面。

   清單中不會再出現異常物件。

## 危險的 Kerberos 委派作業

Kerberos 通訊協定為 Active Directory 安全的核心，其允許選定伺服器重複使用使用者憑證。若攻擊者入侵其中一個伺服器，則可竊取其憑證並用來在其他資源上進行驗證。

此嚴重曝險指標 (IoE) 會報告具有委派屬性的所有帳戶，並排除已停用的帳戶。特權使用者不應具有委派屬性。如要保護這些使用者帳戶，請將帳戶新增至「受保護的使用者」群組，或將其標示為「帳戶為機密帳戶，不可委派」。

**如要將帳戶新增至「受保護的群組」：**

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的「**曝險指標**」以開啟。

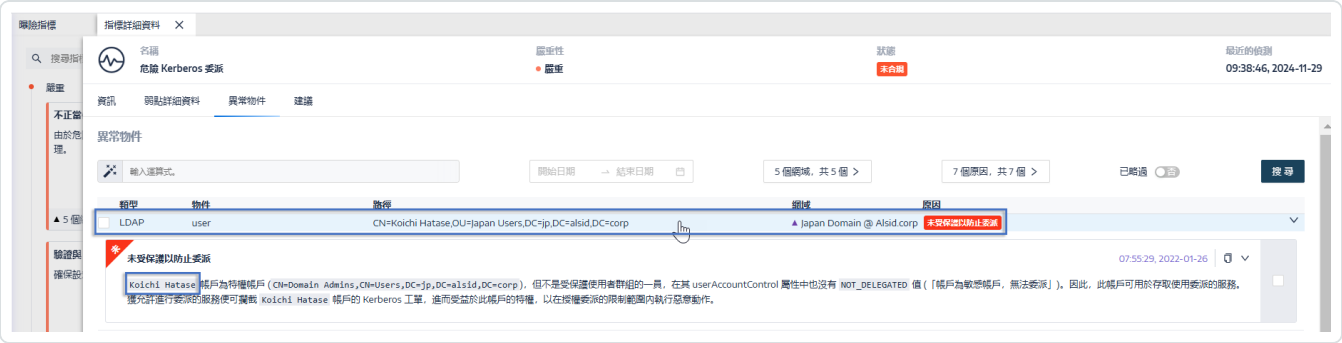
   根據預設，Tenable Identity Exposure 僅會顯示包含異常物件的曝險指標 (IoE)。

2. 按一下**危險 Kerberos 委派**曝險指標 (IoE) 的圖塊。



「**指標詳細資料**」窗格會隨即開啟。

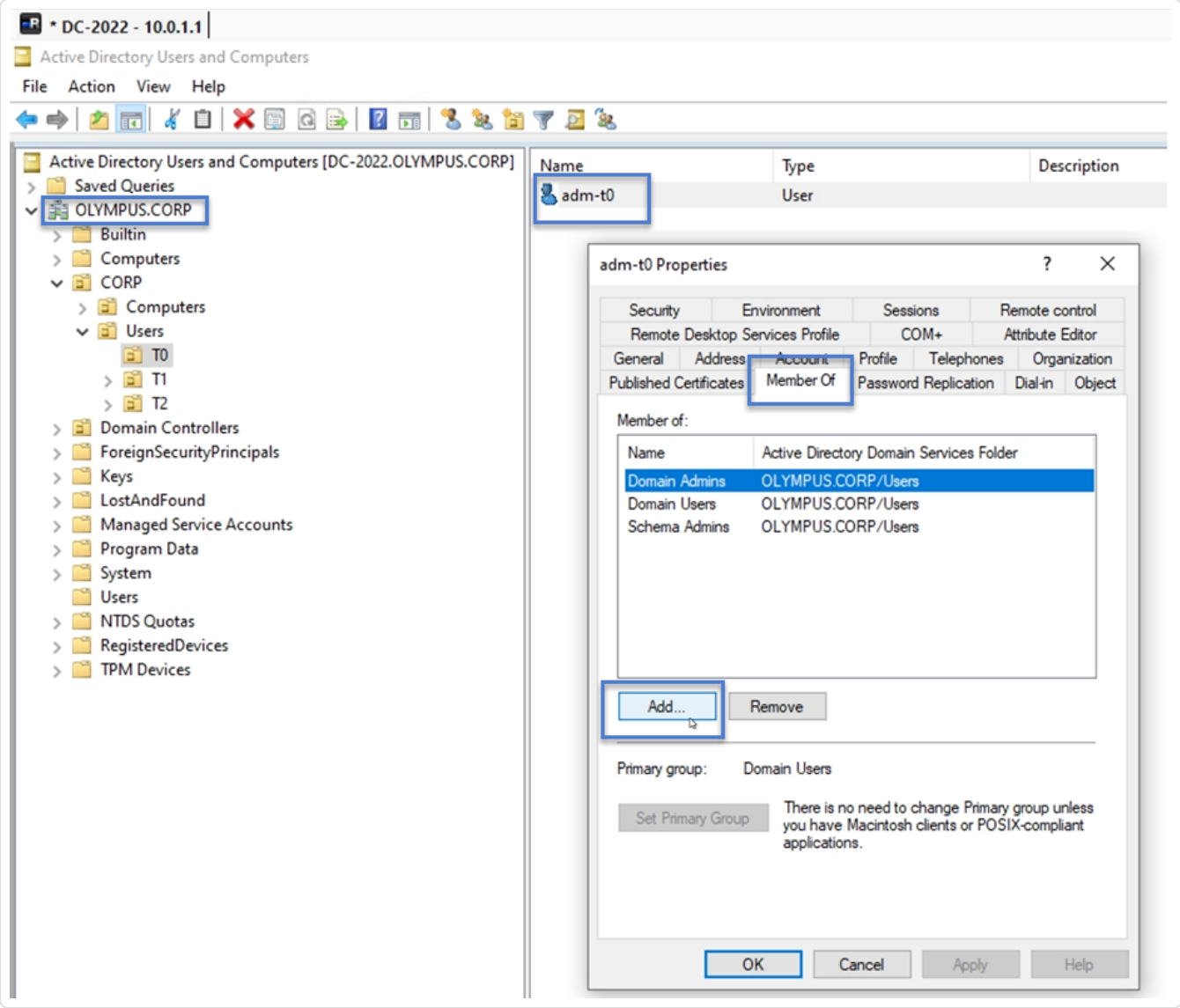
3. 將游標停留在異常物件上並按一下即可顯示詳細資料，記下網域名稱和帳戶(在此範例中：網域為 OLYMPUS.CORP，帳戶 = `adm-t0`)。




4. 在 Remote Desktop Manager (或類似工具) 中，找到網域名稱並導覽至 Tenable Identity Exposure 標記的網域和帳戶。

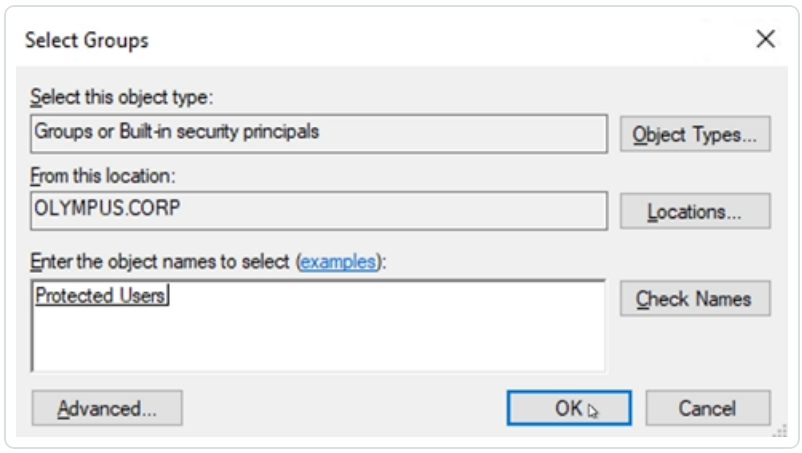
> **必要權限**：您必須擁有網域的管理員帳戶才能執行程序。

5. 按一下帳戶名稱以開啟「**內容**」對話方塊，然後選取「**成員隸屬**」索引標籤。
6. 在成員清單中按一下「**新增**」。



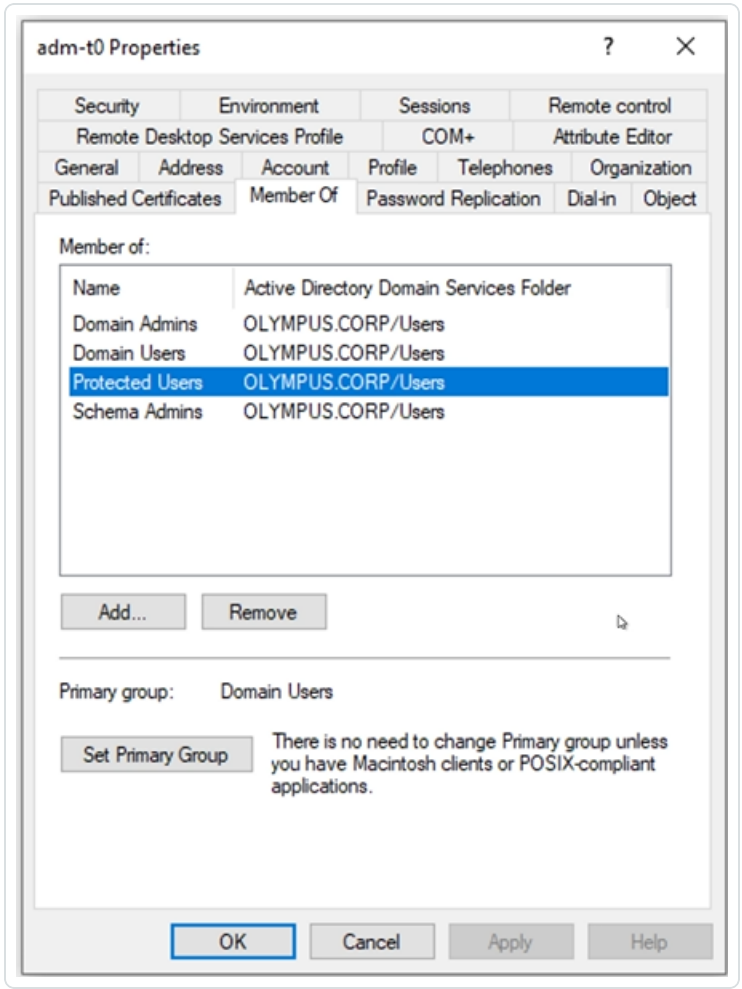

「**選取群組**」對話方塊會隨即顯示。

7. 輸入物件名稱「受保護的使用者」，然後按一下「**檢查名稱**」。




8. 按一下**「確定」**關閉對話方塊。
9. 在**「內容」**對話方塊中按一下**「套用」**。

   新群組會隨即顯示在成員清單上。



10. 按一下「**確定**」關閉對話方塊。
11. 在 Tenable Identity Exposure 中，返回「指標詳細資料」窗格並重新整理頁面。

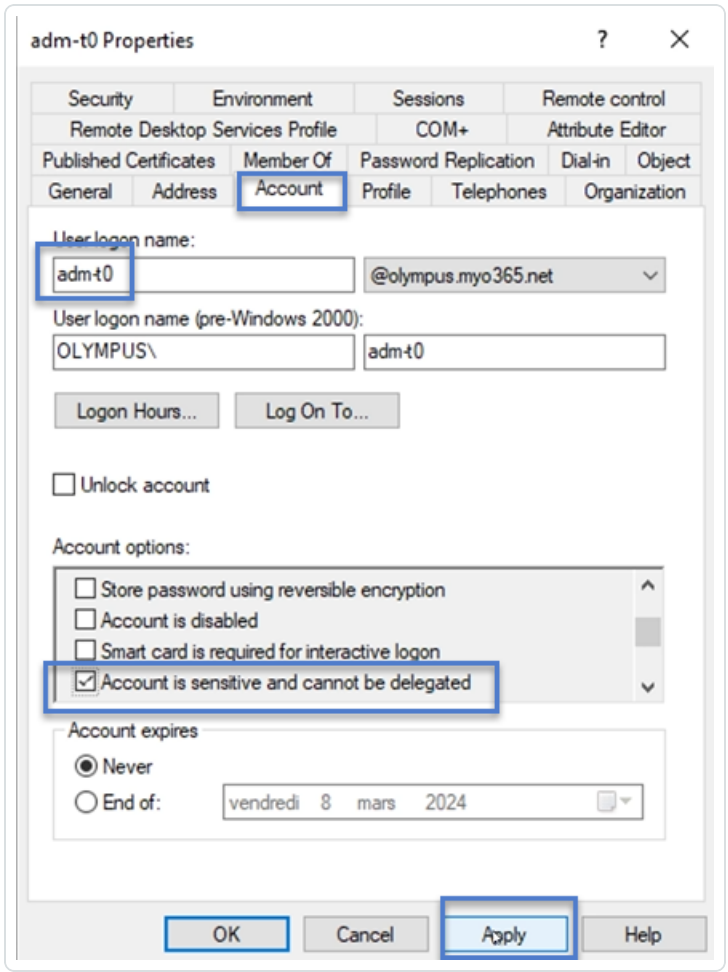
    清單中不會再出現異常物件。

**如要將帳戶設為「不可委派」：**

1. 在 Remote Desktop Manager 中，找到網域名稱並導覽至 Tenable Identity Exposure 標記的網域和帳戶。

   **必要權限**：您必須擁有網域的管理員帳戶才能執行程序。

2. 按一下帳戶名稱以開啟「**內容**」對話方塊，然後選取「**帳戶**」索引標籤。
3. 從帳戶選項清單中選取「帳戶為機密帳戶，不可委派」，然後按一下「**套用**」。




4. 按一下「**確定**」關閉對話方塊。

5. 在 Tenable Identity Exposure 中，返回「指標詳細資料」窗格並重新整理頁面。

   清單中不會再出現異常物件。

## 確保 SDProp 一致性

入侵 Active Directory 網域的攻擊者通常會變更 `adminSDHolder` 物件的 ACL，而且他們新增至 ACL 的任何權限都會複製給特權使用者，因此可以輕鬆設定後門程式。

此嚴重曝險指標 (IoE) 會檢查 `adminSDHolder` 物件上設定的權限是否只允許對管理帳戶進行特權存取。

如要修復**確保 SDProp 一致性**曝險指標 (IoE) 中的異常物件：

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的「**曝險指標**」以開啟。

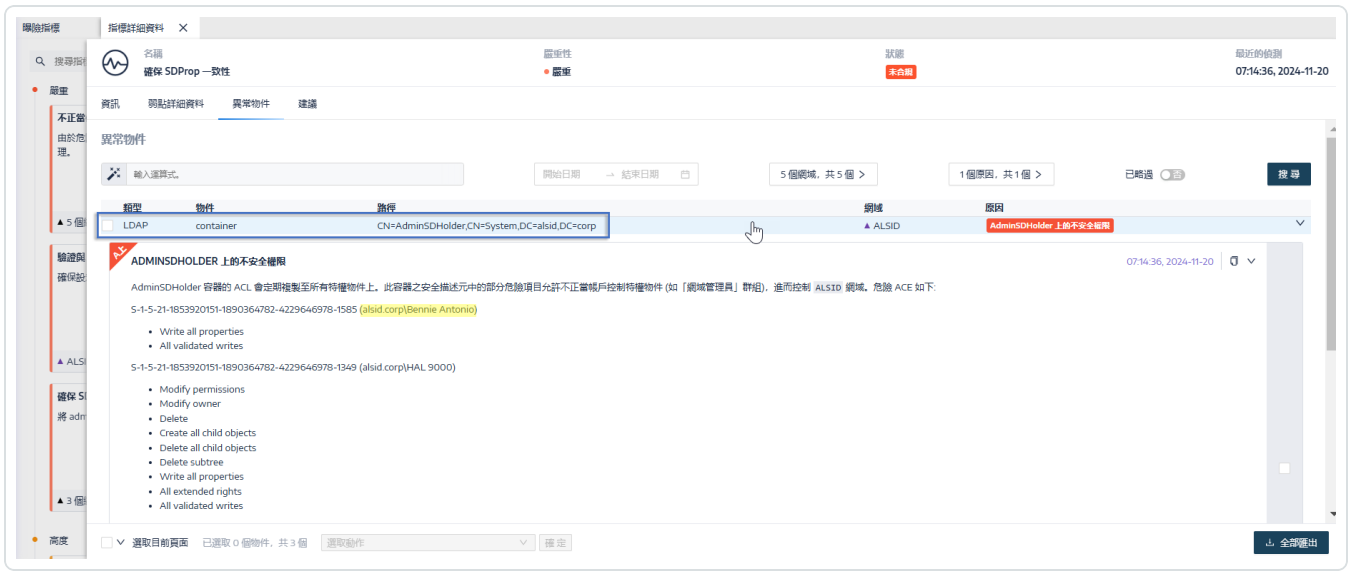
   根據預設，Tenable Identity Exposure 僅會顯示包含異常物件的曝險指標 (IoE)。

2. 按一下**確保 SDProp 一致性**曝險指標 (IoE) 的圖塊。




   「**指標詳細資料**」窗格會隨即開啟。

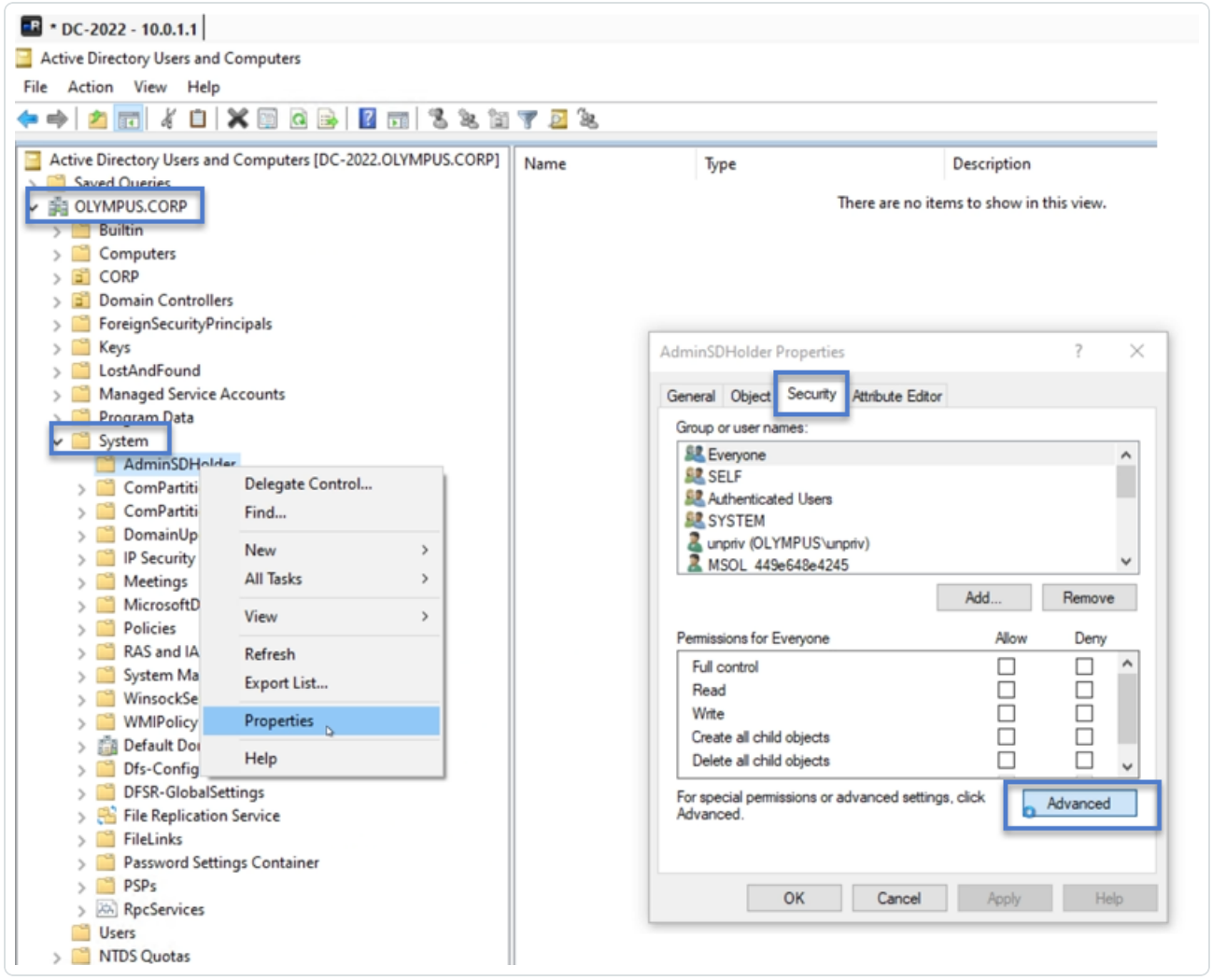
3. 將游標停留在異常物件上並按一下即可顯示詳細資料，記下 Tenable Identity Exposure 標記的網域名稱和相關權限(在此範例中：`OLYMPUS.CORP .\unpriv`)。



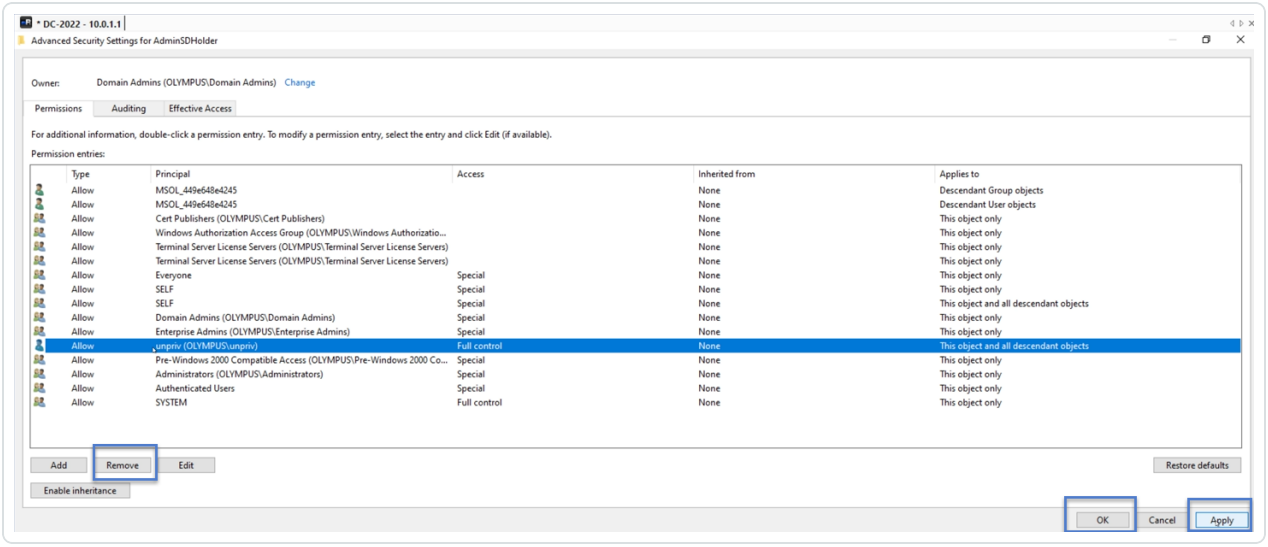

4. 在 Remote Desktop Manager (或類似工具) 中，找到網域名稱並導覽至「**系統**」> 「**AdminSDHolder**」。

> **必要權限**：您必須擁有網域的管理員帳戶才能執行程序。

5. 用右鍵按一下「**AdminSDHolder**」，然後從內容功能表中選取「**內容**」。




6. 在「**內容**」對話方塊中選取「**安全性**」索引標籤，然後按一下「**進階**」。
7. 在「**進階安全性設定**」視窗和「**權限**」索引標籤中，從權限項目清單選取引發警示的權限。
8. 按一下「**移除**」。
9. 按一下「**套用**」和「**確定**」關閉設定視窗。
10. 按一下「**確定**」關閉「**內容**」視窗。




11. 在 Tenable Identity Exposure 中，返回「指標詳細資料」窗格並重新整理頁面。

    清單中不會再出現異常物件。

## 攻擊指標

> **需要的授權**：攻擊指標

Tenable Identity Exposure 的**攻擊指標** (IoA) 能夠協助您偵測 Active Directory (AD) 上發生的攻擊。

攻擊指標的合併檢視會在單一窗格中即時顯示時間軸、影響 AD 的前 3 個資安事端和攻擊分布情況。您可以執行以下動作：

- 視覺化顯示準確攻擊時間軸上的每個威脅。
- 深入分析有關 AD 攻擊的詳細資料。
- 直接從偵測到的資安事端中探索 MITRE ATT&CK 描述。

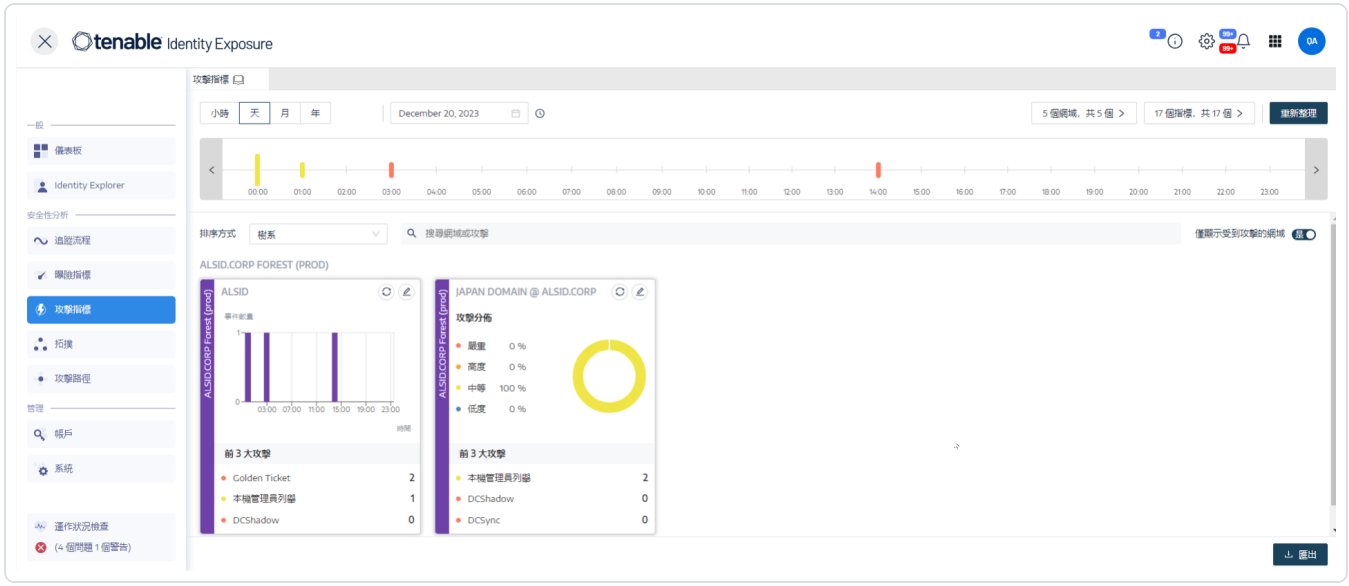
如需有關特定攻擊指標 (IoA) 的詳細資訊，請參閱攻擊指標參考指南 (需要登入 Tenable 下載網站登入)。

> **注意**：如果您發現大量偵測到的攻擊，請確認您的系統管理員是否已針對各種攻擊指標 (IoA) 選項套用建議的值，以正確校正這些攻擊指標。如需詳細資訊，請參閱「校正攻擊指標 (IoA)」。

如要顯示攻擊指標：

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的**「攻擊指標」**。

   **「攻擊指標」**窗格會隨即開啟。




2. 根據預設，Tenable Identity Exposure 會顯示您的所有 AD 樹系和網域。如要調整此檢視，請執行下列任一動作：

   - 選取要顯示的時間段：按一下**「小時」**、**「日」**(預設)、**「月」**或**「年」**。
   - 沿時間軸移動：按一下向左或向右箭頭可在時間軸上前進或後退。
   - 選取特定的時間：按一下日期選擇器以選擇小時、日、月或年。
   - 返回至目前日期和時間：按一下日期選擇器旁邊的 圖示。
   - 選取網域：按一下**「n/n 網域」**。

     a. 在**「樹系和網域」**窗格中選取網域。

     b. 按一下**「篩選選取的項目」**。

     Tenable Identity Exposure 將更新檢視。

   - 選取攻擊指標 (IoA)：按一下**「n/n 指標」**。

a. 在「攻擊指標」窗格中選取攻擊指標 (IoA)。

b. 按一下「**篩選選取的項目**」。

Tenable Identity Exposure 將更新檢視。

- 對攻擊指標 (IoA) 圖塊進行排序：在「**排序依據**」方塊中，按一下箭頭以顯示選項的下拉式清單：「**網域**」、「**關鍵性**」或「**樹系**」。
- 搜尋網域或攻擊：在「**搜尋**」方塊中輸入網域名稱或攻擊。
- 僅顯示受到攻擊的域：按一下「**僅顯示受到攻擊的域**」切換為「**是**」。
- 匯出攻擊報告：按一下「**匯出**」。

「**匯出卡片**」窗格會隨即顯示。

a. 在「**匯出格式**」方塊中，按一下下拉式清單箭頭以選取一種格式：**PDF**、**CSV** 或 **PPTX**。

b. 按一下「**匯出**」。

Tenable Identity Exposure 將報告下載到本地電腦。

## 嚴重性等級

Tenable Identity Exposure 會偵測攻擊並指派嚴重性等級：

| 等級 | 說明 |
|---|---|
| **嚴重**：紅色 | 偵測到經驗證的後滲透攻擊，此類攻擊需要以網域支配權作為先決條件。 |
| **高度**：橙色 | 偵測到允許攻擊者取得網域支配權的重大攻擊。 |
| **中度**：黃色 | 與此攻擊相關的攻擊指標 (IoA) 可導致危險的特權提升，或允許攻擊者存取敏感資源。 |
| **低度**：藍色 | 與偵察動作或低影響資安事端相關的可疑行為警示。 |

## 另請參閱

- 攻擊指標詳細資料
- 攻擊指標資安事端

## 攻擊指標詳細資料

Tenable Identity Exposure 的「攻擊指標」窗格會顯示與 Active Directory 中所發生的攻擊相關資訊。

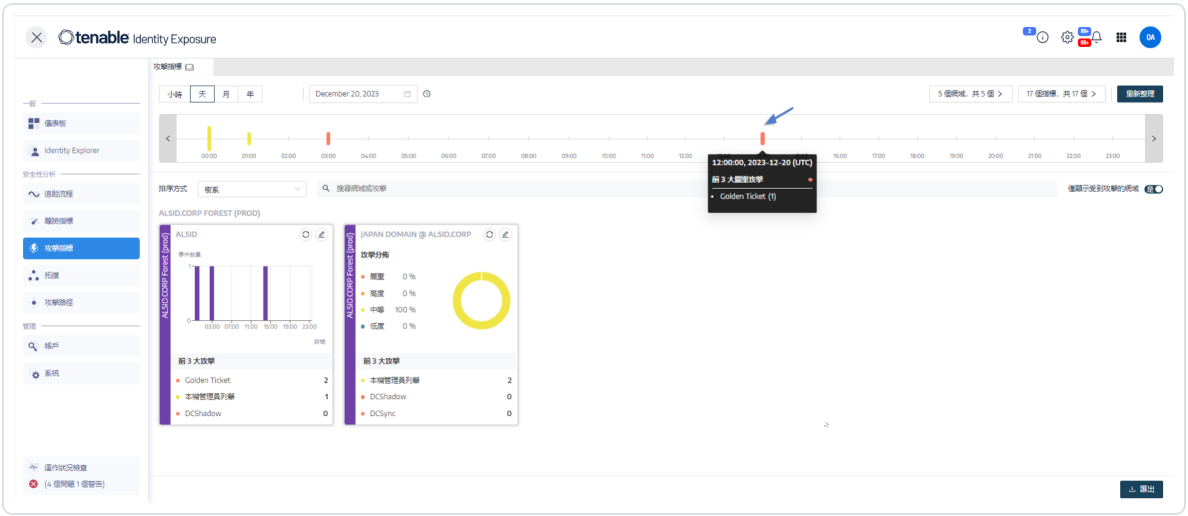
如要檢視攻擊指標：

- 在 Tenable Identity Exposure 中，按一下導覽窗格中的**「攻擊指標」**。

  **「攻擊指標」**窗格會隨即開啟。

如要在時間軸上顯示攻擊資訊：

- 按一下時間軸上的任何事件以顯示：
  - 資安事端偵測日期和時間。
  - 前 3 大攻擊的嚴重性等級。
  - 在此日期和時間偵測到的攻擊總數。



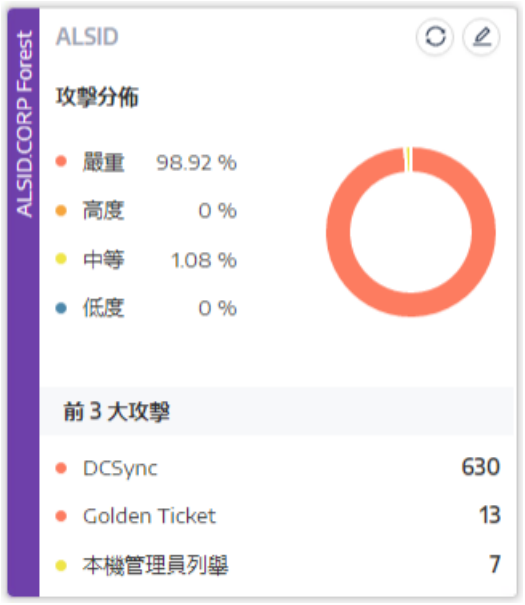

如要變更圖表類型：

1. 按一下 圖示以編輯網域圖塊。

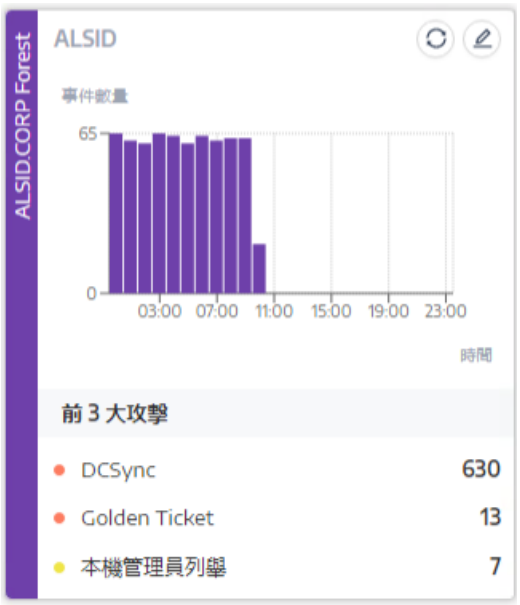
   「**編輯卡片資訊**」窗格會隨即顯示。

2. 選取圖表類型：

   - **攻擊分布**：顯示攻擊嚴重性的分布狀況。




   - **事件數量**：顯示前 3 大攻擊及攻擊發生次數。




3. 按一下「**儲存**」。

Tenable Identity Exposure 會更新圖表。

## 另請參閱

- 攻擊指標
- 攻擊指標資安事端

## 攻擊指標資安事端

攻擊指標 (IoA) 資安事端清單提供有關 Active Directory (AD) 上特定攻擊的詳細資訊。這有助於您根據攻擊指標 (IoA) 的嚴重性等級採取必要的動作。

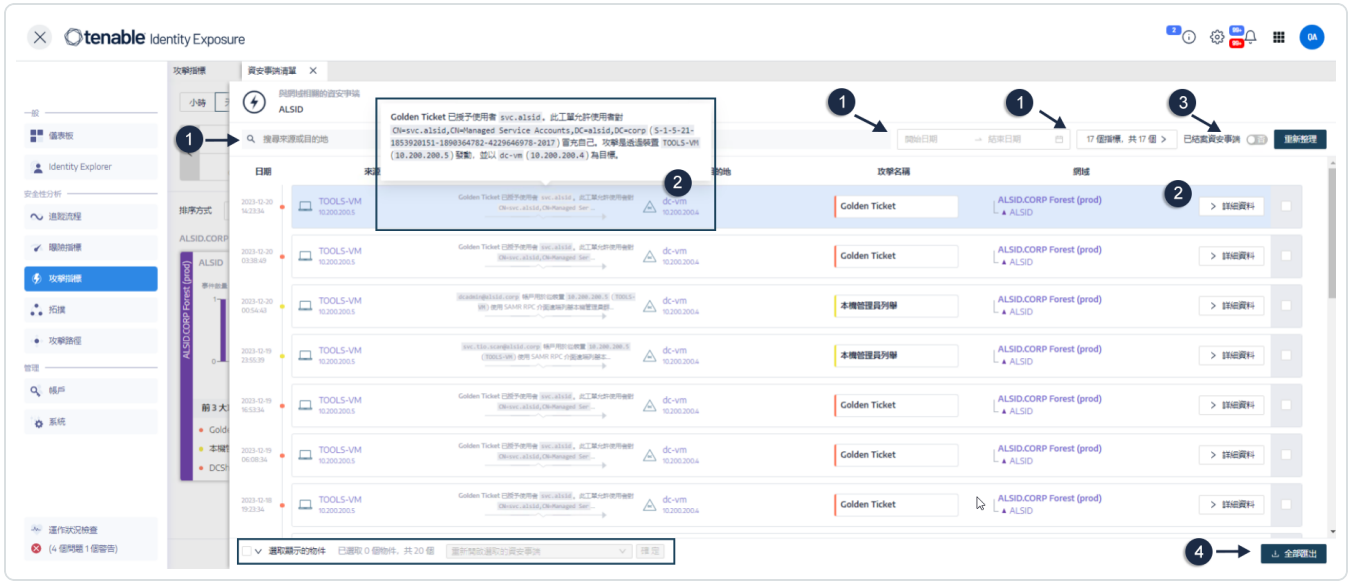
**如要檢視攻擊資安事端：**

1. 在 Tenable Identity Exposure 中，按一下導覽窗格中的**「攻擊指標」**。

   **「攻擊指標」**窗格會隨即開啟。

2. 按一下任何網域圖塊。

   **「資安事端清單」**窗格會隨即顯示，列出網域上發生的資安事端。




3. 您可以在此清單中執行下列任一動作：

- 定義搜尋條件以搜尋特定的資安事端 (**1**)。
- 存取與影響 AD 的攻擊相關的詳細說明 (**2**)。
- 關閉或重新開啟資安事端 (**3**)。
- 下載顯示所有資安事端的報告 (**4**)。

**如要搜尋資安事端：**

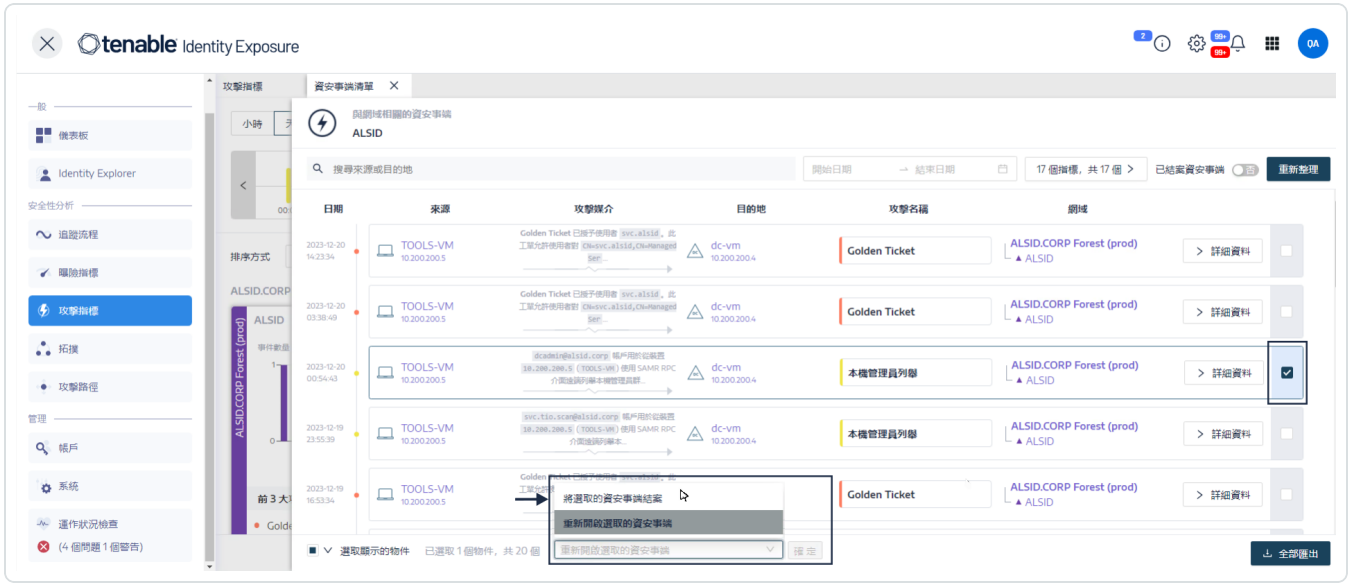
1. 在「**搜尋**」方塊中輸入來源或目的地的名稱。
2. 按一下日期選擇器，選取資安事端的開始日期和結束日期。
3. 按一下「**n/n 指標**」以選取相關指標。
4. 按一下「**已關閉的資安事端**」切換為「**是**」，將搜尋範圍限定為已關閉的資安事端。
5. 按一下「**重新整理**」。

   Tenable Identity Exposure 會使用符合的資安事端更新清單。




**如要關閉資安事端：**

1. 從資安事端清單中選取要關閉或重新開啟的資安事端。




2. 在窗格底部按一下下拉式功能表，並選取**「關閉選取的資安事端」**。
3. 按一下**「確定」**。

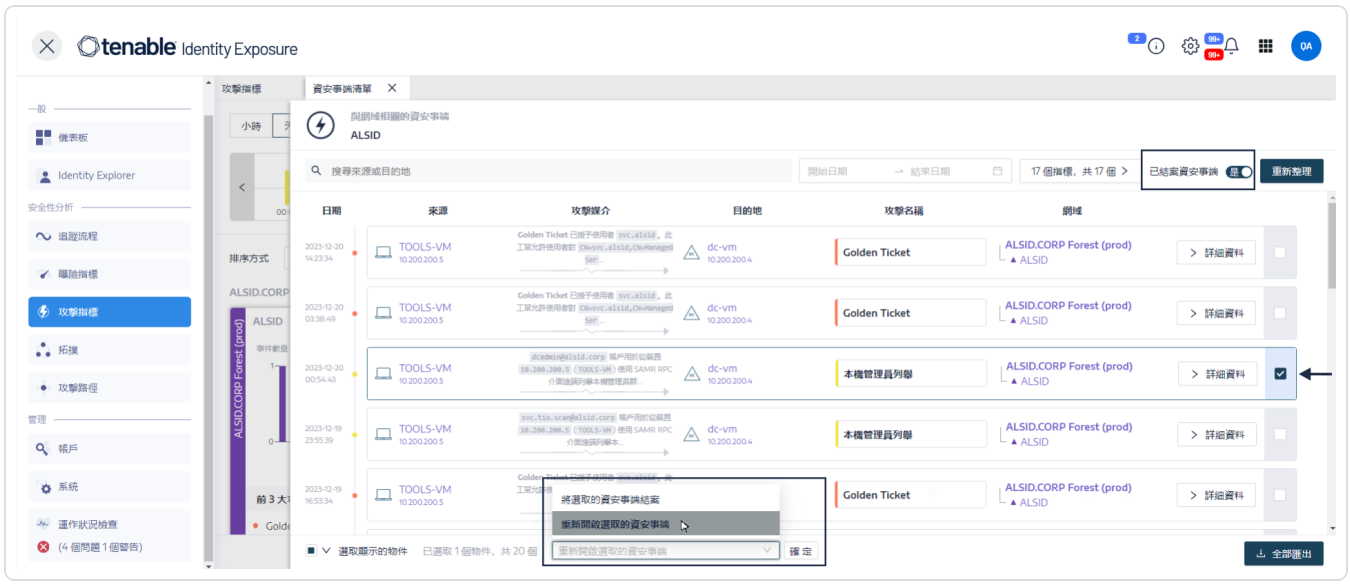
   系統會顯示一則訊息，要求您確認關閉。
4. 按一下**「確認」**。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已關閉資安事端，並且不再顯示。

**如要重新開啟資安事端：**

1. 在**「資安事端清單」**窗格中，按一下**「已關閉的資安事端」**切換為**「是」**。

   Tenable Identity Exposure 會使用已關閉的資安事端更新清單。
2. 選取要重新開啟的資安事端。




3. 在窗格底部按一下下拉式功能表，並選取「**重新開啟選取的資安事端**」。
4. 按一下「**確定**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已重新開啟此資安事端。

**提示**：您可以大量關閉或重新開啟資安事端。在窗格底部按一下「**選取顯示的物件**」。

### 若要匯出資安事端

1. 在「**資安事端清單**」窗格中，按一下底部的「**全部匯出**」按鈕。

   「**匯出資安事端**」側面板隨即開啟。
2. 從「**分隔符號**」下拉式清單方塊中，選取所匯出資料的分隔符號：**逗號**或**分號**。

   Tenable Identity Exposure 會以 CSV 格式匯出資料以供下載。




## 資安事端詳細資料

資安事端清單中的每個項目都會顯示下列資訊：

- **日期**：觸發攻擊指標 (IoA) 的資安事端發生的日期。Tenable Identity Exposure 在時間軸的頂端顯示最近的項目。
- **來源**：攻擊的來源及其 IP 位址。
- **攻擊媒介**：說明攻擊期間發生的情況。

  **提示**：將游標停留在攻擊媒介上可檢閱有關攻擊指標 (IoA) 的更多資訊。
- **目的地**：攻擊的目標及其 IP 位址。
- **攻擊名稱**：攻擊的技術名稱。
- **網域**：攻擊影響的網域。

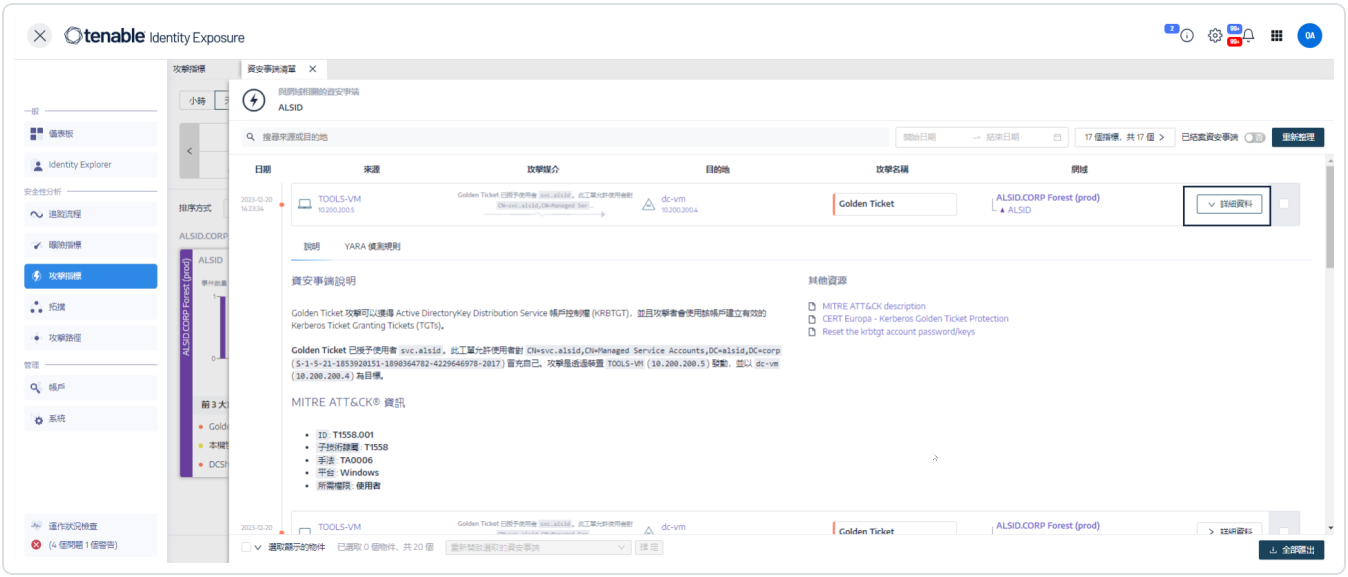
  **提示**：若按一下**資安事端清單**中的多個互動元素 (連結、動作按鈕等)，Tenable Identity Exposure 最多可以顯示五個窗格。如要同時關閉所有窗格，請按一下頁面上的任意位置。

## 攻擊詳細資料

您可以從資安事端清單向下切入特定攻擊，並採取必要的修復措施。

如要顯示攻擊詳細資料：

1. 從資安事端清單中選取要向下切入詳細資料的資安事端。
2. 按一下「**詳細資料**」。




Tenable Identity Exposure 會顯示與此攻擊相關的詳細資料：

## 說明

**說明索引標籤**包含下列區段：

- **資安事端說明**：提供有關攻擊的簡短描述。
- **MITRE ATT&CK 資訊：**提供從 Mitre Att&ck (對抗性戰術、技術和通用知識) 知識庫擷取的技術資訊。Mitre Att&ck 是一個對惡意攻擊進行分類並描述攻擊者在入侵網路後所採取行動的框架。它會為安全弱點提供標準標識符，以確保網路安全社群達成共識。
- **其他資源**：提供通往網站、文章和白皮書的連結，協助您取得更深入的攻擊資訊。

## YARA 偵測規則

**YARA 偵測規則**索引標籤描述 Tenable Identity Exposure 用於在網路層級偵測 AD 攻擊以加強 Tenable Identity Exposure 偵測鏈的 YARA 規則。

**注意**:YARA 是一個主要用於惡意軟體研究和偵測的工具。它提供一種基於規則的方法,用來根據文字或二進位模式建立有關惡意軟體系列的描述。描述本質上是一個 YARA 規則名稱,這些規則由字串集和布林運算式組成 (來源:wikipedia.org。)

### 另請參閱

- 攻擊指標
- 攻擊指標詳細資料

## 拓撲

「拓撲」頁面提供 Active Directory 的互動式圖形視覺化,**拓撲圖**顯示樹系、網域以及它們之間存在的信任關係。




如要開啟拓撲頁面:

- 在 Tenable Identity Exposure 中,按一下左側導覽功能表中的「**拓撲**」。

  「拓撲」窗格會隨即開啟,其中包含您的 AD 的圖形表示。

如要搜尋網域:

- 在「**拓撲**」窗格的「**搜尋**」方塊中輸入網域名稱。

  Tenable Identity Exposure 將醒目提示此網域。

如要放大圖表：

- 在「**拓撲**」窗格中，按一下「**縮放**」滑桿以調整圖形大小。

如要顯示兩個網域之間的連結：

- 在「**拓撲**」窗格中，按一下「**顯示內部關係**」切換為「**是**」。

如要顯示有關網域的詳細資料：

- 在「**拓撲**」窗格中，按一下網域名稱的 ▲。

  「**網域詳細資料**」窗格會隨即開啟，其中顯示偵測到的曝險指標 (IoE) 和網域的合規性分數。您可以按一下曝險指標 (IoE) 圖塊以深入瞭解更多資訊。

## 另請參閱

- 信任關係
- 危險的信任

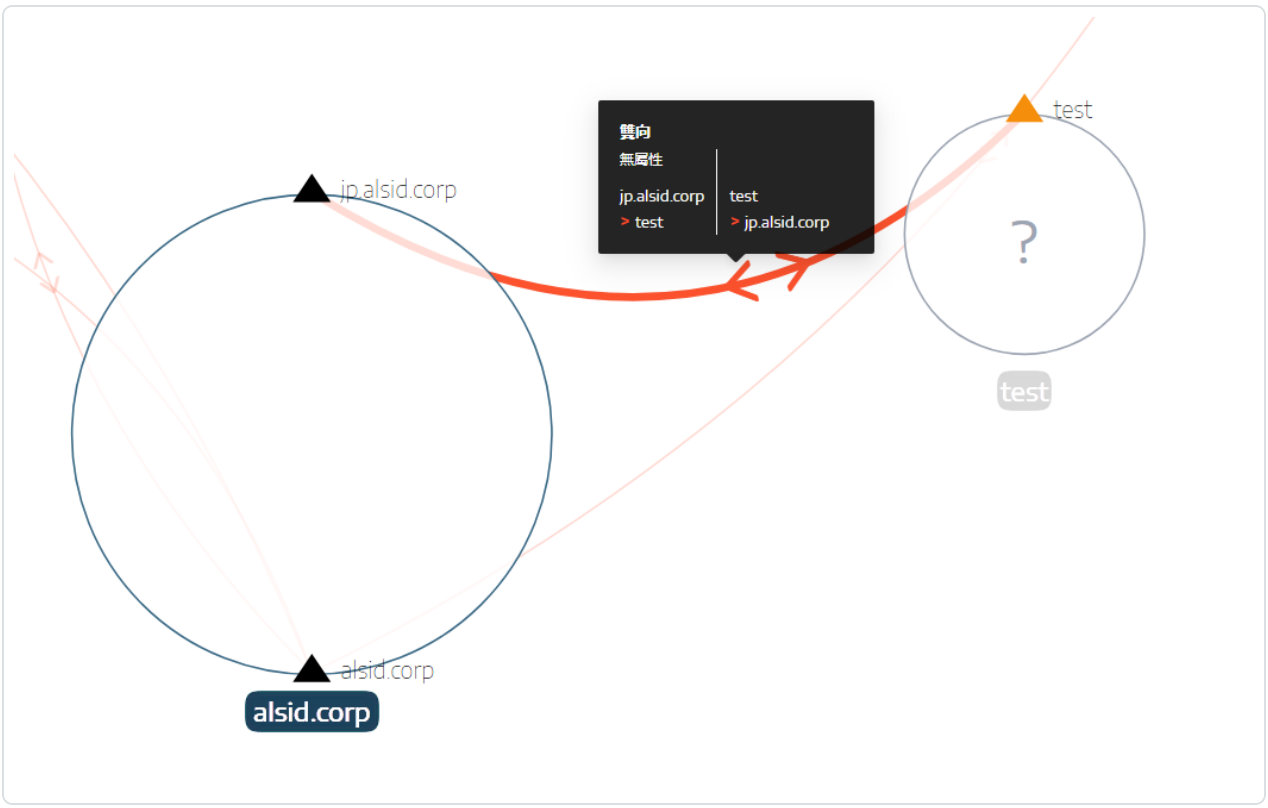
## 信任關係

拓撲圖上網域之間的曲線箭頭表示信任關係。

如要顯示信任關係：

- 在拓撲圖上，將游標移到曲線箭頭上方。

  Tenable Identity Exposure 將顯示信任關係顯示兩個實體之間的特定屬性。




信任關係的顏色取決於其威脅程度：

- **紅色**表示危險信任
- **橙色**表示普通信任
- **藍色**表示未知信任

如需詳細資訊，請參閱 危險的信任。

信任屬性資訊將信任方向指示為**單向**或**雙向** (傳入/傳出)，並顯示以下值之一：

| 值 | 說明 |
|---|---|
| **不可轉移** | 預設情況下，樹系內的信任是可轉移的信任。Tenable Identity Exposure 使用此標誌將它們轉換為不可轉移的信任。另一方面，樹系間的信任預設為不可轉移，因此存在樹系可轉移標誌。如果存在樹系內網域間的信任，則 Tenable Identity Exposure 會顯示此值。此信任不授予存取權，也不向樹系以外的互連網域委派任何授權。 |
| **樹系轉移** | 表示兩個樹系之間存在可轉移的信任。授予另一個網域的信任可以傳遞給受信任的樹系。 |

| | |
|---|---|
| **樹系內** | 表示在同一個樹系中存在網域間信任。如果同時存在 `WITHIN_FOREST` 和 `QUARANTINED_DOMAIN`，則此信任稱為 **QuarantinedWithinForest**。 |
| **僅限上層** | 表示僅執行 Windows 2000 作業系統和更高版本的用戶才能使用此信任。 |
| **視為外部** | (僅當適用 `FOREST_TRANSITIVE` 時) 表示外部信任類型。Tenable Identity Exposure 會修改此信任的安全性識別碼 (SID) 篩選，並授權相對識別碼 (RID) 大於或等於 1000 的 SID 通過樹系。 |
| **已隔離** | 表示 Tenable Identity Exposure 為信任啟用了篩選 RID 大於或等於 1000 的 SID 選項。預設情況下，Tenable Identity Exposure 只為外部信任啟用此選項，但也可以套用至父/子信任或樹系信任。 |
| **跨組織驗證** | 表示 Tenable Identity Exposure 啟用了選擇性驗證並且可以跨網域或樹系信任使用。 |
| **選擇性驗證** | 請參閱跨組織驗證。 |
| **跨組織 (無 TGT 委派)** | 顯示是否已完全停用受信任網域上的委派 (絕不在已發出的服務工單中設定 ok-as-delegate 選項)。 |
| **RC4 加密：** | 表示此信任支援用於 Kerberos 交換的 RC4 加密金鑰。僅當 `trustType` 套用至 `TRUST_TYPE_MIT` 時，才會出現此標誌。 |
| **AES 金鑰** | 表示此信任支援用於 Kerberos 交換的 AES 加密金鑰。 |
| **PIM 信任** | 如果 `FOREST_TRANSITIVE` 和 `TREAT_AS_EXTERNAL` 標誌適用並且 `QUARANTINED_DOMAIN` 標誌未開啟，則 PIM 信任標誌表示受信任的樹系管理與 SID 篩選有關的特殊權限身分識別 (Privileged Identity Management) (本機 SID 可以通過此信任)。PIM 信任的作用是建置堡壘樹系。 |
| **無屬性** | 表示外部信任沒有特定屬性。 |

## 危險的信任

信任關係的顏色取決於其威脅程度：

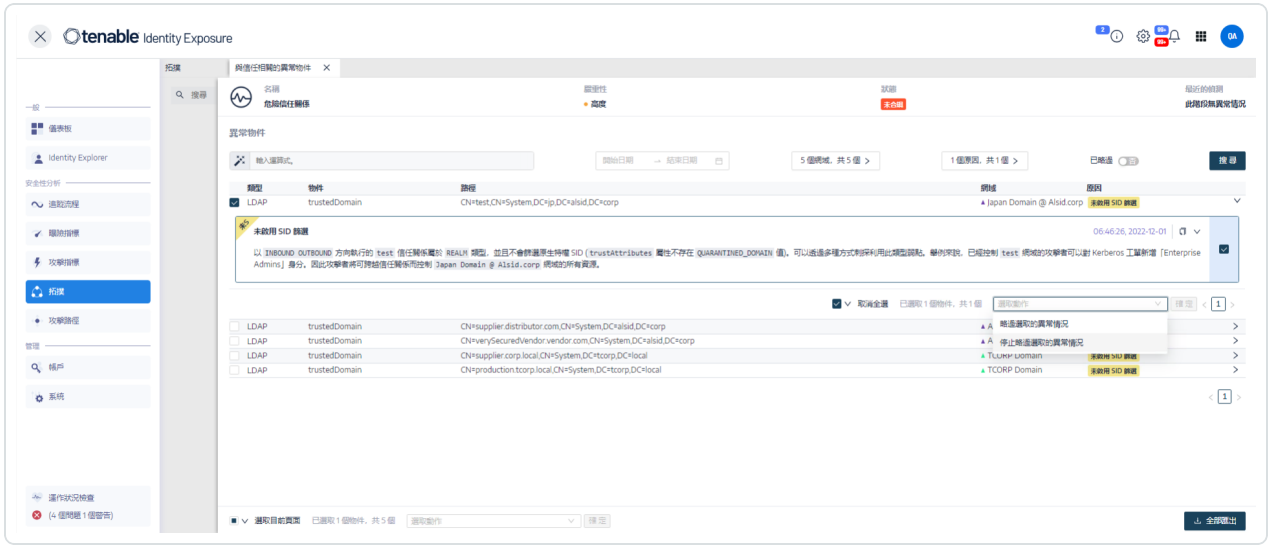
- **紅色**表示危險信任
- **橙色**表示普通信任
- **藍色**表示未知的信任

如要調查危險的信任：

1. 在拓撲圖上，按一下曲線箭頭。

   **「與信任相關的異常物件」**窗格會隨即開啟。

   > **提示**：此危險信任關係窗格中顯示的事件詳細資料全部連結至**危險信任關係**曝險指標，您也可以從**曝險指標**導覽功能表存取。




2. 將游標移到清單中的異常物件上面並按一下以顯示詳細資料。

如要匯出異常物件：

1. 在拓撲圖上，按一下曲線箭頭。

   **「與信任相關的異常物件」**窗格會隨即開啟。

2. 按一下**「全部匯出」**。

   **「匯出異常物件」**窗格會隨即開啟。

3. 在**「匯出格式」**方塊中，按一下下拉箭頭以選取一種格式。

4. 按一下「**全部匯出**」。

   Tenable Identity Exposure 會以所選格式將檔案下載到您的電腦。

5. 按一下 **X** 關閉窗格。

## 攻擊路徑

Tenable Identity Exposure 提供數種方式，可以透過圖形表示法將企業資產的潛在弱點視覺化。

- **攻擊路徑**：顯示攻擊者可從進入點入侵資產的可能路徑。
- **影響範圍**：顯示從任何資產進入 Active Directory 時可能的橫向移動。
- **資產曝險**：顯示可能控制資產的所有路徑。

瞭解攻擊路徑就能以必要的緩解措施對應，以避免攻擊者惡意利用弱點，這類措施可能包括修補系統、強化設定、採用更強大的存取控制，或提高使用者的意識。

在 Tenable Identify Exposure 中使用「攻擊路徑」的好處如下：

- **主動保障安全**：有助於提前預測和處理潛在攻擊媒介，避免遭到惡意利用。
- **確立優先順序**：有助於在實施安全相關工作時，著重在最需留意的弱點和攻擊路徑上。
- **視覺化**：用清楚好懂的方式呈現 AD 中複雜的安全關係。
- **溝通**：提供潛在攻擊情境的視覺化證據，方便針對安全風險與利害相關人溝通。

**如要顯示攻擊路徑：**

您可以指定起始點，像是 AD 中的任何資產 (例如，使用者帳戶、電腦、群組)。您可以定義到達點，代表攻擊者最終企圖入侵的資產 (例如，網域控制器、敏感資料伺服器)。

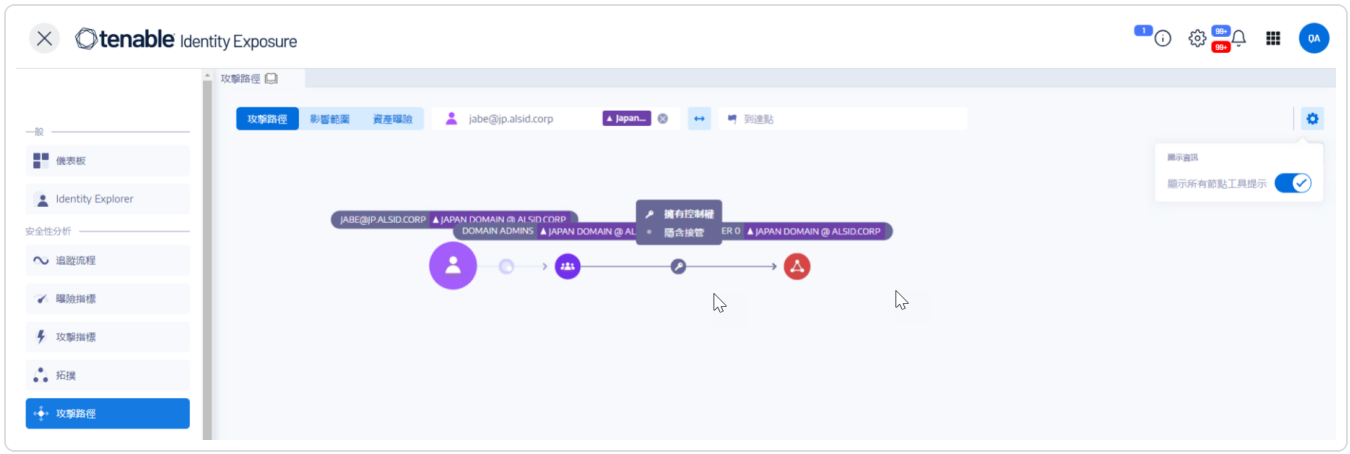
1. 在 Tenable Identity Exposure 中，按一下側邊欄功能表上的「**攻擊路徑**」。

   「**攻擊路徑**」窗格會隨即顯示。




2. 在橫幅中，按一下**「攻擊路徑」**。
3. 在**「起始點」**方塊中輸入進入點的資產。
4. 在**「到達點」**方塊中輸入路徑末端的資產。
5. 按一下 圖示。

   Tenable Identity Exposure 將顯示兩個資產之間的攻擊路徑。




6. 或者，您可以按一下 圖示來執行以下動作：
   - 按一下**「縮放」**滑桿以調整圖形的放大倍數。
   - 按一下**「顯示所有節點工具提示」**開關以顯示有關資產的信息。

**如要顯示影響範圍：**

Tenable Identity Exposure 會以圖形方式呈現潛在攻擊路徑，並著重於資產之間的關係。每個關係都代表一個潛在的弱點或錯誤設定，讓攻擊者可惡意利用，在您的 AD 中橫向移動。您可以放大和縮小，深入瞭解路徑的詳細資料。

1. 在 Tenable Identity Exposure 中，按一下側邊欄功能表上的**「攻擊路徑」**。

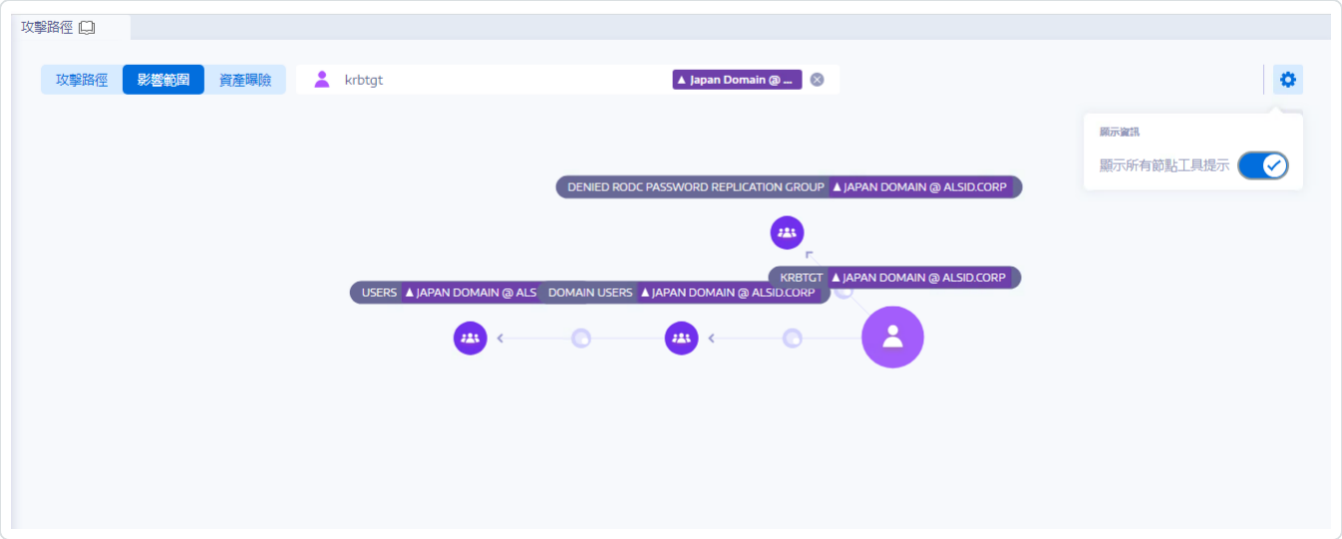
   **「攻擊路徑」**窗格會隨即顯示。

2. 在橫幅中，按一下**「影響範圍」**。

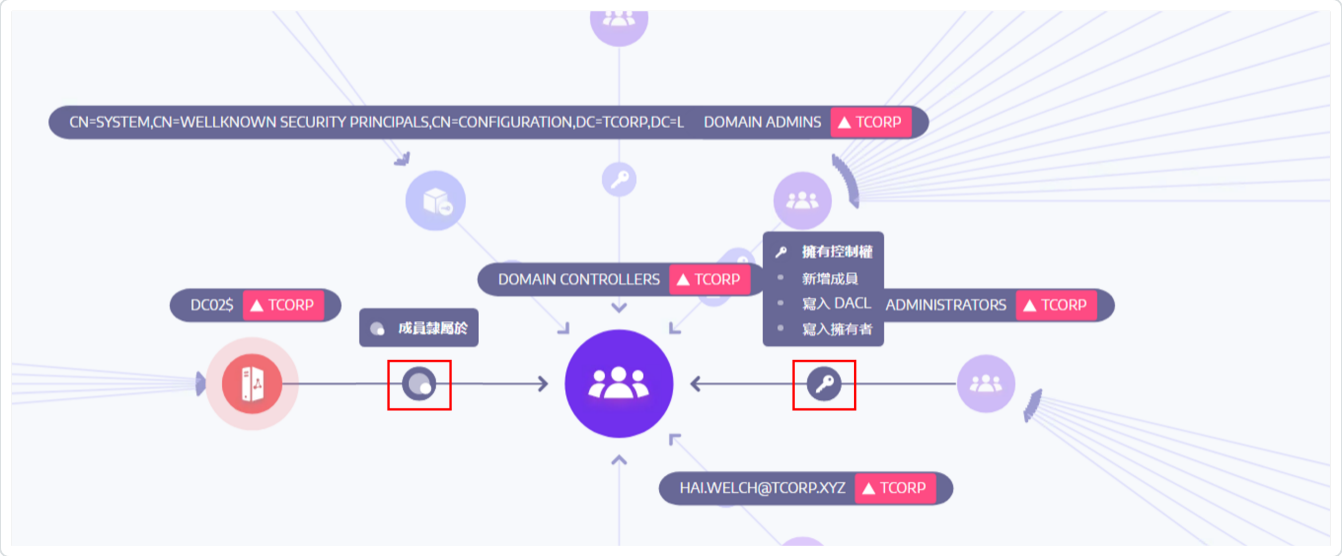
3. 在**「搜尋物件」**方塊中輸入資產的名稱。

4. 按一下 圖示。

   Tenable Identity Exposure 會顯示從此資產輻射的橫向連接：



5. 按一下資產之間箭頭上的圖示以顯示它們之間的關係。




**如要顯示資產曝險：**

攻擊路徑中的每個步驟都對應一個風險評分，反映弱點的嚴重性，有助於您確定哪個路徑帶來的威脅最大，需要立即處理。您也可以按一下個別關係點，進一步瞭解特定弱點或相關錯誤設定。

1. 在 Tenable Identity Exposure 中，按一下側邊欄功能表上的**「攻擊路徑」**。

   **「攻擊路徑」**窗格會隨即顯示。

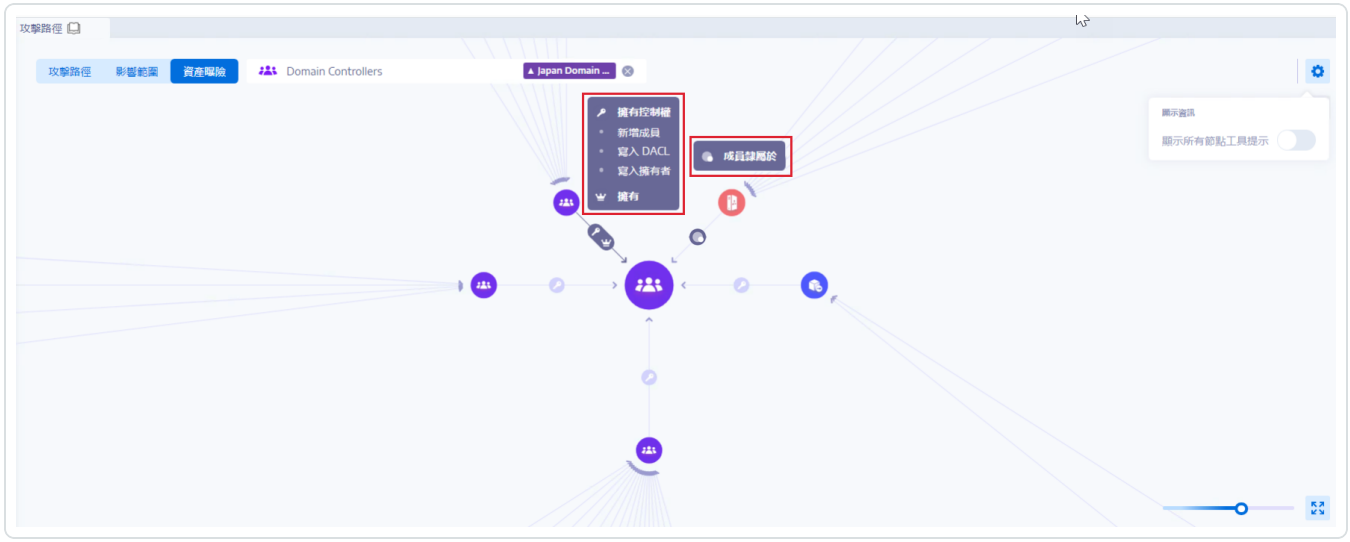
2. 在橫幅中，按一下**「資產曝險」**。

3. 在**「搜尋物件」**方塊中輸入資產的名稱。

4. 按一下 圖示。

   Tenable Identity Exposure 會顯示通往資產的路徑以及資產之間的關係。

5. 按一下資產之間箭頭上的圖示以顯示它們之間的關係。



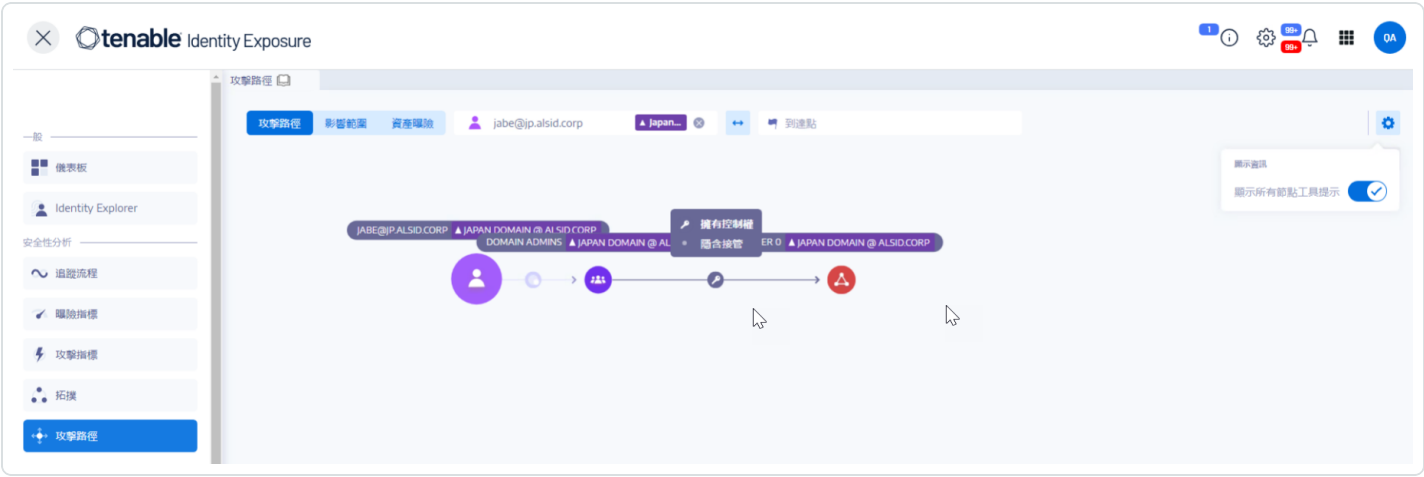

**如要釘選攻擊路徑：**

## 另請參閱

- 攻擊關係
- 識別第 0 層資產
- 包含攻擊路徑的帳戶
- 攻擊路徑節點類型

## 攻擊關係

從來源節點到目標節點的攻擊關係是單向關係。由於關係可以傳遞，所以攻擊者可以將它們鏈結在一起，建立「攻擊路徑」：




Tenable Identity Exposure 具有下列攻擊關係：

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理

- 寫入 DACL
- 寫入所有者

新增金鑰憑證

## 說明

來源安全主體可以透過利用金鑰信任帳戶對應來模擬目標，這也稱為金鑰憑證或「影子憑證」。

因為來源具有編輯目標的 `msDS-KeyCredentialLink` 屬性的權限，所以可以做到這點。

Windows Hello 企業版 (WHfB) 通常會使用此功能，但即使未使用，攻擊者仍可以利用它。

## 利用

破壞來源安全主體的攻擊者必須使用專門的駭客工具 (如 Whisker 或 DSInternals) 來編輯目標電腦的 `msDS-KeyCredentialLink` 屬性。

攻擊者的目標是向此目標的屬性新增憑證，他們擁有此憑證的私密金鑰。然後，他們可以使用 Kerberos PKINIT 通訊協定，以已知的私密金鑰驗證為目標，以取得 TGT。此通訊協定還允許攻擊者取得目標的 NTLM 哈希。

## 修復

依照預設，數個具有本機權限的安全主體擁有此權限，即帳戶管理員、管理員、網域管理員、企業管理員、企業金鑰管理員、金鑰管理員和系統。這些合法的安全主體不需要修復。

對於沒有修改此屬性的合法需要的來源安全主體，您必須移除此權限。搜尋「寫入所有屬性」、「寫入 msDS-AllowedToActOnBehalfOfOtherIdentity」、「完全控制」等權限。

## 另請參閱

- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO

- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

新增成員

## 說明

來源安全主體可以將自己 (已驗證的寫入權限) 或任何人 (寫入屬性權限) 新增至目標群組的成員中，並使用已授予此群組的存取權限。

執行此作業的惡意安全主體會建立「成員隸屬於」攻擊關係。

## 利用

入侵來源安全主體的攻擊者只需透過本機 Windows 命令 (如「net group /domain」)、PowerShell (如「Add-ADGroupMember」)、管理工具 (如「Active Directory 使用者和電腦」) 或專用的駭客工具 (如 PowerSploit) 編輯目標群組的「成員」屬性。

## 修復

如果來源安全主體不需要擁有將成員新增到目標群組的權限，則您必須移除此權限。

如要修改目標群組的安全性描述元：

1. 在「Active Directory 使用者和電腦」中，右鍵按一下「**屬性**」>「**安全性**」。
2. 移除權限，例如「寫入成員」、「寫入所有屬性」、「完整控制權」、「所有已驗證的寫入」、「將自己新增為成員/移除成員」等。

**注意**：群組可從 Active Directory 樹系中較高層級的物件繼承權限。

## 另請參閱

- 新增金鑰憑證
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

## 允許行動

## 說明

來源安全主體可以在目標電腦上執行 Kerberos 資源型限制委派。換言之，當使用 Kerberos 對目標電腦上執行的任何服務進行身分驗證時，它可以模擬任何使用者。

因此，它通常會導致目標電腦完全受損。

此攻擊也稱為資源型限制委派 (RBCD)、Kerberos 資源型限制委派 (KRBCD)、資源型 Kerberos 限制委派 (RBKCD) 和「允許代表其他身分執行」。

## 利用

入侵來源安全主體的攻擊者可使用專用的駭客工具 (如 Rubeus) 利用合法的 Kerberos 通訊協定延伸模組 (S4U2self 和 S4U2proxy)，以偽造 Kerberos 服務工單並模擬目標使用者。攻擊者可能會選擇模擬特權使用者來取得特殊權限存取權。

一旦攻擊者偽造服務工單，他們就可以使用與 Kerberos 相容的任何原生管理工具或專門的駭客工具，從遠端執行任意命令。

成功的攻擊行為必須符合下列限制條件：

- 來源和目標安全主體必須具有 ServicePrincipalName。如果沒有此條件，Tenable Identity Exposure 不會建立此攻擊關係。
- 偽造的目標帳戶不得標記為「敏感且無法委派」(UserAccountControl 中的 `ADS_UF_NOT_DELEGATED`)，也不能是「受保護使用者」群組的成員，這是因為 Active Directory 可保護此類帳戶不受委派攻擊。

## 修復

如果來源安全主體不需要在目標電腦上執行 Kerberos 資源型限制委派 (RBCD) 的權限，則您必須將其移除。您必須修改目標端，而不是「允許委派」委派攻擊關係。

您不能使用現有的圖形管理工具 (例如「Active Directory 使用者和電腦」) 來管理 RBCD。您必須改用 PowerShell 來修改 `msDS-AllowedToActOnBehalfOfOtherIdentity` 屬性的內容。

使用下列命令列出允許在目標電腦上執行動作的來源安全主體 (在「Access:」區段中)：

```
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -
ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

如果您不想要任何列出的安全主體，可以使用此命令清除所有這些主體：

```
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

如果您只需要從清單中移除一個安全主體，那很遺憾，Microsoft 沒有提供直接命令。您必須使用同一個清單減去要移除的主體，以覆寫此屬性。例如，如果「sourceA」、「sourceB」和「sourceC」都是允許的主體，而您只想移除「sourceB」，請執行：

```
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

最後，作為一般建議，為了限制敏感的特權帳戶遭受此類委派攻擊，Tenable Identity Exposure 建議您在仔細驗證相關的作業影響之後，將其標記為「敏感且無法委派」(ADS_UF_NOT_DELEGATED)，或是將其新增至「受保護的使用者」群組。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理

- 寫入 DACL
- 寫入所有者

允許委派

## 說明

來源安全主體可以透過轉換通訊協定在目標電腦上執行 Kerberos 資源型限制委派 (KCD)。換言之，當使用 Kerberos 對目標電腦上執行的任何服務進行身分驗證時，它可以模擬任何使用者。

因此，它通常會導致目標電腦完全受損。

## 利用

入侵來源安全主體的攻擊者可使用專用的駭客工具 (如 Rubeus) 利用合法的 Kerberos 通訊協定延伸模組 (S4U2self 和 S4U2proxy)，以偽造 Kerberos 服務工單並模擬目標使用者。攻擊者可能會選擇模擬特權使用者來取得特殊權限存取權。

一旦攻擊者偽造服務工單，他們就可以使用與 Kerberos 相容的任何原生管理工具或專門的駭客工具，從遠端執行任意命令。

成功的攻擊行為必須符合下列限制條件：

- 必須針對通訊協定轉換啟用來源安全主體 (UserAccountControl 中的 `ADS_UF_TRUSTED_FOR_DELEGATION`/委派 GUI 中的「使用任何驗證通訊協定」)。更確切地說，攻擊可以在沒有轉換通訊協定的情況下運作 (委派 GUI 中的「僅使用 Kerberos」)，但攻擊者必須先將 Kerberos 驗證從目標使用者強制轉換為來源安全主體，這會使攻擊更加困難。因此，在此情況下，Tenable Identity Exposure 不會建立攻擊關係。
- 來源和目標安全主體必須具有 ServicePrincipalName。如果沒有此條件，Tenable Identity Exposure 不會建立此攻擊關係。
- 偽造的目標帳戶不得標記為「敏感且無法委派」(UserAccountControl 中的 `ADS_UF_NOT_DELEGATED`)，也不能是「受保護使用者」群組的成員，這是因為 Active Directory 可保護此類帳戶不受委派攻擊。

相反，允許委派的目標電腦由服務主體名稱 (SPN) 指定，因此包含特定的服務，例如帶有「cifs/host.example.net」的 SMB、帶有「http/host.example.net」的 HTTP 等。但是，攻擊者實際上

可以使用「sname 替代攻擊」，將相同「目標」帳戶下執行的任何其他 SPN 和服務作為攻擊目標，因此這不是限制。

## 修復

如果來源安全主體不需要在目標電腦上執行 Kerberos 限制委派 (KCD) 的權限，則您必須將其移除。您必須修改來源端，而不是「允許執行」委派攻擊關係。

如要移除來源安全主體：

1. 在「Active Directory 使用者和電腦」管理 GUI 中，轉到來源物件的「**屬性**」>「**委派**」索引標籤。
2. 移除與目標對應的服務主體名稱。
3. 如果您不想要來自此來源的任何委派，請移除所有 SPN 並選取「不信任此電腦的委派」。

或者，您可以使用 PowerShell 修改來源的「msDS-AllowedToDelegateTo」屬性內容。

- 例如，在 Powershell 中執行此命令以取代所有值：

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @{ "msDS-
AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }
```

- 如果您不想要來自此來源的任何委派，請執行以下命令以清除此屬性：

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-
AllowedToDelegateTo"
```

也可以透過停用通訊協定轉換，在不完全關閉此攻擊路徑的情況下降低風險。這會要求所有安全主體僅使用 Kerberos 而非 NTLM 連線至來源。

如要停用通訊協定轉換：

1. 在「Active Directory 使用者和電腦」管理 GUI 中，前往來源物件的「**屬性**」>「**委派**」索引標籤。
2. 選取「僅使用 Kerberos」，而非「使用任何驗證通訊協定」。

或者，您可以在 PowerShell 中執行下列命令以停用通訊協定轉換：

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation
$false
```

最後，作為一般建議，為了限制敏感的特權帳戶遭受此類委派攻擊，Tenable Identity Exposure 建議您在仔細驗證相關的作業影響之後，將其標記為「敏感且無法委派」(ADS_UF_NOT_DELEGATED)，或是將其新增至「受保護的使用者」群組。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

## 屬於 GPO

## 說明

SYSVOL 共用中的來源 GPO 檔案或資料夾屬於目標 GPC (GPO)，這表示它定義了 GPO 套用的設定或程式/指令碼。

## 利用

這不是攻擊者孤立使用的攻擊關係。但是，舉例而言，它可以顯示完整的攻擊路徑，攻擊者若能控制屬於 GPO 的 GPO 檔案/資料夾，就可以在攻擊路徑末端的使用者/電腦上強制執行任意設定或啟動指令碼。

## 修復

此關係顯示在 SYSVOL 中找到的 GPO 檔案和資料夾如何與對應的 GPC (GPO) 物件相關聯。這是正常現象，屬於原有設計。

因此不需要修復。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼

- RODC 管理
- 寫入 DACL
- 寫入所有者

## DCSync

### 說明

DCSync 是 Active Directory 的一項合法功能，網域控制器僅將其用於複製變更，但非法的安全主體也可以使用它。

來源安全主體可使用 DCSync 功能從目標網域要求敏感密碼 (密碼雜湊、Kerberos 金鑰等)，最終導致網域遭到完全入侵。

如要擷取密碼，需要兩個安全性權限：「複製目錄變更」(DS-Replication-Get-Changes) 和「複製全部目錄變更」(DS-Replication-Get-Changes-All)。只有當您直接或透過巢狀群組成員資格將這兩個權限都提供給來源時，才會發生此關係。

### 利用

入侵來源安全主體的攻擊者可使用專用的駭客工具 (如 *mimikatz* 或 *impacket*) 擷取密碼。

- **Golden ticket**：取得「krbtgt」帳戶的密碼雜湊後的結果，這讓攻擊者可以偽造 Kerberos TGT，並在任何電腦/服務上冒充任何人。特別是，這會賦予攻擊者對網域中任何電腦的管理權限。
- **Silver ticket**：取得電腦/服務帳戶的密碼雜湊後的結果，這讓攻擊者可以偽造 Kerberos 服務工單，並在任何電腦/服務上冒充任何人。

### 修復

預設允許利用 DCSync 的合法安全主體為：

- 管理員
- 網域管理員
- 企業管理員
- 系統

此外，Microsoft Entra ID Connect 設定允許其密碼雜湊同步處理服務帳戶 (MSOL_...) 使用 DCSync。

最後，可以發現特定安全性工具的服務帳戶，特別是密碼稽核解決方案。向負責人驗證其合法性。

對於沒有執行 DCSync 的合法需要的來源安全主體，您必須移除此權限。

如要修改目標網域的安全性描述元：

1. 在「Active Directory 使用者和電腦」中，右鍵按一下網域名稱，然後選取「屬性」>「安全性」。
2. 移除非法安全主體的「複製目錄變更」和「複製全部目錄變更」權限。

**注意**：可以透過巢狀群組成員資格的權限產生 DCSync 關係。因此，您必須視具體情況決定移除群組本身或僅移除部分群組成員。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有

- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

### 授權允許行動

## 說明

允許來源安全主體授予自己或其他人與目標電腦的 允許行動 關係。這經常引致攻擊者可透過 Kerberos RBCD 委派攻擊完全入侵目標電腦。

因為來源具有編輯目標的「msDS-AllowedToActOnBehalfOfOtherIdentity」屬性的權限，所以可以做到這點。

執行此作業的惡意安全主體可建立「Allowed To Act」攻擊關係。

## 利用

入侵來源安全主體的攻擊者必須使用 PowerShell 編輯目標電腦的 `msDS-AllowedToActOnBehalfOfOtherIdentity` 屬性 (例如「Set-ADComputer <target> -PrincipalsAllowedToDelegateToAccount ...」)。

## 修復

依照預設，數個具有本機權限的安全主體擁有此權限，即帳戶操作員、管理員、網域管理員、企業管理員和系統。這些合法的安全主體不需要修復。

Kerberos RBCD 的設計讓電腦管理員可以向任何需要者授予在電腦上執行委派的權利。這與需要網域管理員層級權限的其他 Kerberos 委派模式不同。這允許較低層級的管理員自行管理這些安全性設定，這也稱為委派原則。在這種情況下，這種關係是合法的。

但是，如果來源安全主體不是目標電腦的合法管理員，則此關係不合法，您必須移除此權限。

### 如要修改目標電腦的安全性描述元：

1. 在「Active Directory 使用者和電腦」中，右鍵按一下「**屬性**」>「**安全性**」。
2. 移除授予來源安全主體的權限。搜尋「寫入 msDS-AllowedToActOnBehalfOfOtherIdentity」、「寫入所有屬性」、「寫入帳戶限制」、「完全控制」等權限。

**注意**：來源安全主體可從 Active Directory 樹系中較高層級的物件繼承權限。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

## 有 SID 歷程記錄

## 說明

來源安全主體的 SIDHistory 屬性中具有目標安全主體的 SID，這表示來源具有與目標相同的權限。

SID 歷程記錄是在網域之間移轉安全主體時使用的合法機制，用於保留參照其先前 SID 功能的所有授權。

但是，這也是攻擊者使用的潛伏機制，因為它允許隱密的後門程式帳戶擁有與所需目標 (例如管理員帳戶) 相同的權限。

## 利用

因為目標的 SID 被透通地新增至 Active Directory 驗證機制產生的權杖 (NTLM 和 Kerberos)，所以入侵來源安全主體的攻擊者可直接以目標安全主體的身分進行驗證。

## 修復

如果來源安全主體和目標安全主體與核准的網域移轉相關，您可以認為此關係合法，不用執行任何動作。系統在提醒潛在的攻擊路徑時仍會顯示此關係。

如果原始網域在移轉後遭到刪除，或 Tenable Identity Exposure 中未設定原始網域，則目標安全主體會被標記為「未解決」。由於風險存在於目標安全主體，而此目標安全主體並不存在，因此沒有風險，也不需要修復。

相反，Active Directory 會阻止建立本機權限使用者或群組的 SID 歷程記錄關係，所以這些關係很可能是惡意的。這表示它們可能是使用「DCShadow」攻擊等駭客技術建立。您也可以在與「SID 歷程記錄」相關的曝險指標 (IoE) 中找到這些案例。

如果是這種情況，Tenable Identity Exposure 建議對整個 Active Directory 樹系進行鑑識檢查。這是因為攻擊者必須取得提高的特權 (網域管理員或同等權限)，才能惡意編輯來源的 SID 歷程記錄。鑑識檢查可協助您使用對應的修復指南來分析攻擊，找出潛在的後門程式並將其要移除。

最後，Microsoft 建議您修改所有服務 (SMB 共用、Exchange 等) 中所有的存取權限，然後使用新的 SID，並在此移轉完成後移除不必要的 SIDHistory 值。這是清理的最佳做法，全面識別並修復所有 ACL 會非常困難。

有權編輯來源物件中 SIDHistory 屬性的使用者可移除 SIDHistory 值。與建立作業不同，此作業不需要網域管理員權限。

您只能使用 PowerShell 執行此作業時，Active Directory 使用者和電腦等圖形工具會失效。範例：

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

**注意**：雖然移除 SIDHistory 值很容易，但還原此作業卻非常複雜。這是因為您必須重新建立 SIDHistory 值，而這需要有其他可能已淘汰的網域。因此，Microsoft 也建議您準備快照或備份。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

## 隱含接管

## 說明

來源是第 0 層安全主體。第 0 層是網域中具有最高特權的一組 Active Directory 物件，例如網域管理員或網域控制器群組的成員。即使沒有其他明確的關係，所有第 0 層資產也都可以暗中入侵網域中的任何其他物件。

此關係可用於對 Active Directory 內建的隱含權限建立模型。這些是專門設計並記錄在案的權限，因此可以被攻擊者知悉。但是，Tenable Identity Exposure 無法透過標準方式收集這些權限。此外，此關係可簡化攻擊路徑圖。攻擊者一旦入侵第 0 層節點，就可以直接攻擊任何其他物件，而無需經過其他明確的關係。

總而言之，來源的第 0 層資產可被視為與圖形中的任何目標節點都有「隱含接管」關係。

## 利用

確切的利用方法取決於所針對的來源第 0 層資產的類型，但攻擊者可以有效地掌握這些詳細記錄的技術。

## 修復

這是專門設計的關係，您無法修復它。一旦攻擊者到達第 0 層資產，幾乎無法阻止其進一步發動攻擊。

修復工作必須集中於攻擊路徑中的上游關係。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動

- 有 SID 歷程記錄
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

繼承 GPO

## 說明

來源可連結容器 (例如組織單位 (OU) 或網域) 而非網站的 LDAP 樹系中包含目標 OU、使用者、裝置、DC 或唯讀網域控制器 (RODC)。這是因為可連結容器的子物件繼承了建立連結時所在的 GPO (請參閱「連結的 GPO」關係)。

每當 OU 封鎖繼承時，Tenable Identity Exposure 都會將其納入考量。

## 刺探利用

只要攻擊者成功入侵攻擊路徑中的 GPO 上游，就無需利用此關係。按照設計，此關係適用於可連結的容器及其下面的物件，如「繼承 GPO」關係所示。

## 修復

在大多數情況下，GPO 從其父項容器套用至可連結的子容器是正常且合法動作。但是，此連結會使其他攻擊路徑面臨風險。

因此，為了降低風險，您應該盡可能將 GPO 連結到組織單位階層中的最低層級。

此外，還需要保護 GPO 免遭攻擊者未經授權的修改，以免其暴露於其他攻擊關係。

最後，OU 可以透過其「禁止繼承」選項禁用從高層級繼承 GPO。但是，此選項只能作為最後的手段使用，因為它會禁止所有 GPO，包括在最高網域層級定義的潛在安全性強化 GPO。這也會使關於所套用 GPO 的推理變得更加困難。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

## 連結的 GPO

## 說明

來源 GPO 連結至目標可連結容器，例如網域或組織單位 (OU)。這表示來源 GPO 可指派設定，並在目標中包含的裝置和使用者環境中執行程式。來源 GPO 也透過「繼承 GPO」關係套用至其下層容器中的物件。

最終，GPO 可能危害套用它的裝置和使用者。

## 利用

攻擊者必須先透過另一個攻擊關係入侵來源 GPO。

然後，他們可以採用數種技術，對目標及其下層所包含的裝置和使用者執行惡意動作。例如：

- 濫用合法的「直接排程任務」在裝置上執行任意指令碼。
- 在所有裝置上新增具有管理權限的本機使用者
- 安裝 MSI 程式
- 停用防火牆或防毒程式
- 授予進一步權限
- 等等

攻擊者可使用管理工具 (例如「群組原則管理」) 或專用的駭客工具 (例如 PowerSploit)，透過手動編輯 GPO 的內容來修改 GPO。

## 修復

在大多數情況下，將 GPO 連結至可連結的容器是正常且合法的動作。但是，此連結會增加所在位置及其下方容器中的攻擊破綻。

因此，為了降低風險，您應該盡可能將 GPO 連結到組織單位階層中的最低層級。

此外，還需要保護 GPO 免遭攻擊者未經授權的修改，以免其暴露於其他攻擊關係。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動

- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

成員隸屬於

## 說明

來源安全主體是目標群組的成員。因此，它可以使用此群組擁有的所有存取權限，例如存取文件共用、承擔業務應用程序中的角色等。

## 利用

攻擊者無需採取任何措施即可利用此攻擊關係。他們只需作為來源安全主體進行身分驗證，即可取得其本機或遠端安全性權杖或 Kerberos 工單中的目標群組。

## 修復

如果來源安全主體是目標群組的非法成員，則必須將其移除。

您可以使用任何標準 Active Directory 管理工具 (例如「Active Directory 使用者和電腦」) 或 PowerShell (例如 Remove-ADGroupMember)。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

## 擁有

## 說明

來源安全主體可能建立了目標物件，因此它是宣告的目標物件所有者。所有者擁有隱含的權限，即「讀取控制」和「寫入 DACL」，所以他們可以為自己或其他人取得額外的權限，並最終入侵目標物件。

## 利用

入侵來源安全主體的攻擊者只需使用本機 Windows 命令 (例如「dsacls」)、PowerShell (例如「Set-ACL」)、管理工具 (例如「Active Directory 使用者和電腦」) 或專用的駭客工具 (例如 PowerSploit) 編輯目標物件的安全性描述元。

建立物件時，如果是低權限使用者 (例如，標準服務台技術人員) 建立並擁有物件，然後將此物件提升到更高的權限 (例如，管理員)，則存在特權提升風險。原來的所有者仍然存在，並且現在可以入侵具有新權限的物件，以利用它的權限。

## 修復

如果來源安全主體不是目標物件的合法所有者，則必須予以變更。

如要變更目標物件的所有者：

1. 在「Active Directory 使用者和電腦」中，右鍵按一下「**屬性**」>「**安全性**」>「**進階**」。
2. 在頂端的「**所有者**」行中，按一下「**更改**」。

大多數敏感 Active Directory 物件預設使用的安全目標物件所有者為：

- 網域分割區中的物件：「管理員」或「網域管理員」
- 設定分割區中的物件：「企業管理員」
- 架構分割區中的物件：「架構管理員」

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄

- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 重設密碼
- RODC 管理
- 寫入 DACL
- 寫入所有者

重設密碼

## 說明

來源安全主體可重設目標的密碼，進而使用新的密碼屬性以目標的身分進行驗證，並取得目標的權限。

重設密碼與變更密碼不同，知道目前密碼的任何人皆可變更密碼。當密碼到期時，通常會發生密碼變更。

## 利用

入侵來源安全主體的攻擊者可使用本機 Windows 命令 (如「net user /domain」)、PowerShell (如「Set-ADAccountPassword -Reset」)、管理工具 (如「Active Directory 使用者和電腦」) 或專用的駭客工具 (如 PowerSploit) 重設目標的密碼。

然後，攻擊者只需要使用合法的驗證方法 (加上其新選擇的密碼) 通過 Active Directory 或目標資源的驗證，即可完全模擬目標。

但是，攻擊者通常不知道先前的密碼，無法在攻擊之後還原。因此，目標背後的合法人員常常可以看到攻擊，而此攻擊甚至可造成拒絕服務，特別是對於服務帳戶而言。

## 修復

IT 管理員和服務台工作人員可以合法重設密碼。但是，您必須建立適當的委派，讓他們只在允許的範圍內執行此動作。

此外，根據階層處理模型，您必須確保較低層級的員工 (例如普通使用者的服務人員) 不能重設較高層級帳戶 (例如網域管理員) 的密碼，因為這是特權提升的機會。

如要修改目標的安全性描述元並移除非法權限：

1. 在「Active Directory 使用者和電腦」中，右鍵按一下「屬性」>「安全性」。
2. 移除授予來源安全主體的「重設密碼」權限。

> **注意**：請勿將此權限與「變更密碼」權限混淆。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- RODC 管理
- 寫入 DACL
- 寫入所有者

## RODC 管理

## 說明

來源安全主體位於目標唯讀網域控制器 (RODC) 的「ManagedBy」屬性中。這表示來源對目標 RODC 具有管理權限。

> **注意**：其他 Active Directory 物件類型僅出於告知目的使用相同的「ManagedBy」屬性，不會向宣告的管理員提供任何管理權限。因此，只有 RODC 類型的目標節點存在此關係。

RODC 的敏感度低於較常見的可寫入網域控制器，所以對攻擊者而言它們仍然是極具價值的目標，因為攻擊者可以在竊取 RODC 的憑證後進一步對其他系統進行樞紐攻擊。這取決於 RODC 設定中的強化等級，例如可同步化的包含密碼的物件數量。

## 刺探利用

刺探利用方法與「AdminTo」關係相同。

入侵來源安全主體的攻擊者可刺探利用其身分從遠端連線，並以系統管理權限在目標 RODC 上執行命令。他們可以刺探利用可用的原生通訊協定，例如具有管理共用的伺服器訊息區 (SMB)、遠端桌面通訊協定 (RDP)、Windows Management Instrumentation (WMI)、遠端程序呼叫 (RPC)、Windows 遠端管理 (WinRM) 等。

攻擊者可使用本機遠端管理工具 (例如 PsExec、服務、排程任務、Invoke-Command 等)，或使用專門的駭客工具 (例如 wmiexec、smbexec、Invoke-DCOM、SharpRDP 等)。

攻擊的最終目標可以是入侵目標 RODC，也可以是使用憑證傾印工具 (例如 mimikatz) 來取得更多憑證和密碼，以便對其他電腦進行樞紐攻擊。

## 修復

如果來源安全主體不是目標唯讀網域控制器 (RODC) 的合法管理員，您必須將其替換為適當的管理員。

請注意，網域管理員通常不管理 RODC，因此是專用的「管理者」設定。這是因為 RODC 的信任等級較低，並且具有高特權的網域管理員不應透過驗證而洩漏其憑證。

因此，您必須根據 Active Directory RODC 規則，為 RODC 選擇適當的「中層」管理員，例如屬於組織當地分部的 IT 管理員。

如要變更「ManagedBy」屬性：

1. 在「Active Directory 使用者和電腦」中，選取「RODC」>「**屬性**」>「**ManagedBy**」索引標籤。
2. 按一下「**更改**」。

您也可以在 PowerShell 中執行下列命令：

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- 寫入 DACL
- 寫入所有者

## 寫入 DACL

## 說明

來源安全主體擁有變更判別存取控制清單 (DACL) 中目標物件權限的權限。來源可以為自己取得或授予其他人額外的權限，並最終危害目標物件。

## 刺探利用

入侵來源安全主體的攻擊者只需使用本機 Windows 命令 (例如「dsacls」)、PowerShell (例如「Set-ACL」)、管理工具 (例如「Active Directory 使用者和電腦」) 或專用的駭客工具 (例如 PowerSploit) 編輯目標物件的安全性描述元。

## 修復

如果來源安全主體不具備變更目標物件權限的合法權限，您必須移除此權限。

如要修改目標物件的安全性描述元：

1. 在「Active Directory 使用者和電腦」中，用右鍵按一下此物件，然後按一下「**屬性**」>「**安全性**」>「**進階**」。
2. 移除來源安全主體的「修改權限」權限。

> **注意**：物件可從 Active Directory 樹系中較高層級的物件繼承此權限。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管

- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入所有者

寫入所有者

## 說明

來源安全主體擁有變更目標物件所有者的權限，包括將自己指派為所有者的權限。所有者擁有隱含的權限，即「讀取控制」和「寫入 DACL」，所以他們可以為自己或其他人取得額外的權限，並最終入侵目標物件。

如需詳細資訊，請參閱 擁有 關係。

## 刺探利用

入侵來源安全主體的攻擊者可使用本機 Windows 命令 (例如「dsacls /takeownership」)、PowerShell (例如「Set-ACL」)、管理工具 (例如「Active Directory 使用者和電腦」) 或專用的駭客工具 (如 PowerSploit) 將自己指派為目標所有者。

然後，他們可以使用類似的方法編輯目標物件的安全性描述元。

## 修復

如果來源安全主體不具備變更目標物件所有者的合法權限，則您必須移除此權限。

如要修改目標物件的安全性描述元：

1. 在「Active Directory 使用者和電腦」中，用右鍵按一下此物件，然後選取「**屬性**」>「**安全性**」>「**進階**」。
2. 移除來源安全主體的「修改所有者」權限。

**注意**：物件可從 Active Directory 樹系中較高層級的物件繼承這一權限。

## 另請參閱

- 新增金鑰憑證
- 新增成員
- 允許行動
- 允許委派
- 屬於 GPO
- DCSync
- 授權允許行動
- 有 SID 歷程記錄
- 隱含接管
- 繼承 GPO
- 連結的 GPO
- 成員隸屬於
- 擁有
- 重設密碼
- RODC 管理
- 寫入 DACL

## 識別第 0 層資產

第 0 層資產包括對 Active Directory 樹系和網域具有直接或間接管理控制權的帳戶、群組和其他資產。

Tenable Identity Exposure 會列出您的第 0 層資產和帳戶，以及通往此資產的潛在攻擊路徑。

如要列出第 0 層資產：

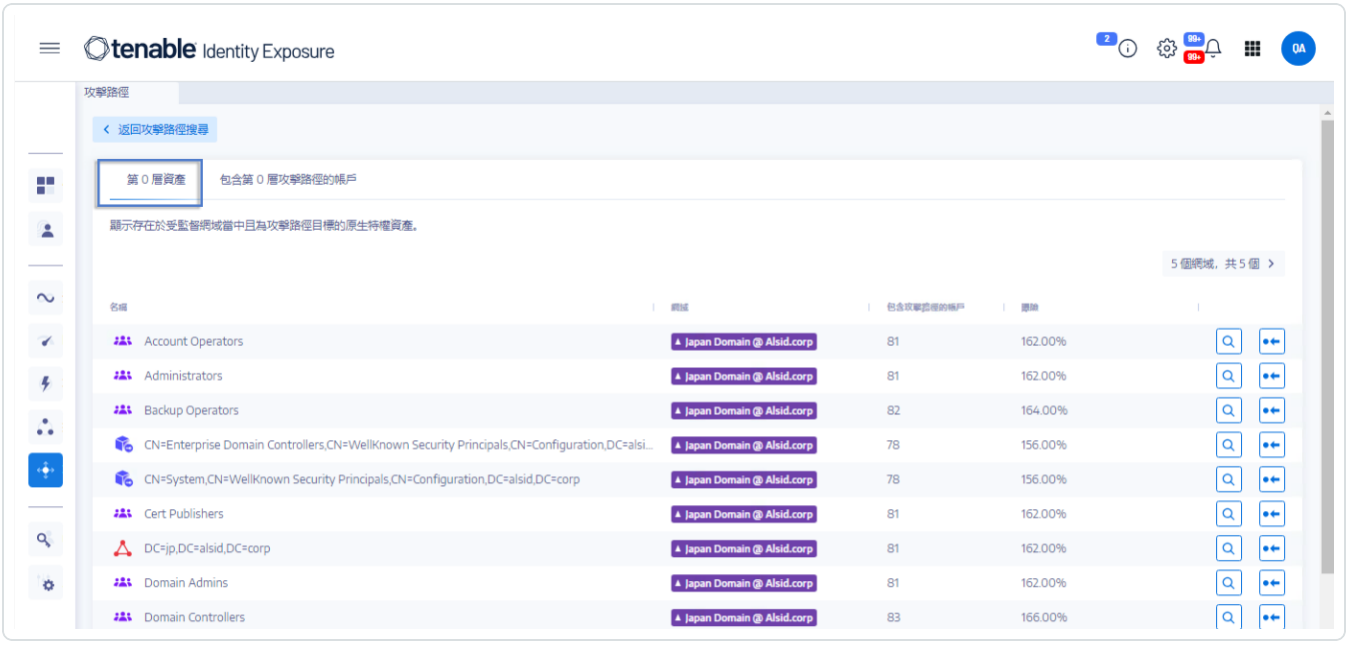
1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的攻擊路徑圖示 。

   「**攻擊路徑**」窗格會隨即開啟。

2. 按一下「**哪些是我的特權資產?**」。




   Tenable Identity Exposure 會顯示 AD 中的第 0 層資產清單。




   每一行都會提供**資產名稱**、**網域**和下列資訊：

   - **包含攻擊路徑的帳戶**：包含通往第 0 層資產的攻擊路徑的資產數量。
   - **曝險程度**：包含通往第 0 層資產的攻擊路徑的帳戶佔網域內帳戶總數的百分比。

如要篩選任何特定網域的資產：

1. 按一下「**n/n**」按鈕。

   「**樹系和網域**」窗格會隨即開啟。您可以執行下列任一動作：

- 在「**搜尋**」方塊中輸入樹系或網域的名稱。
- 選取「**全部展開**」方塊，然後選取所需的樹系或網域。

2. 按一下「**篩選選取的項目**」。

   Tenable Identity Exposure 將更新資產清單。

如要列出包含通往第 0 層資產的攻擊路徑的帳戶：

- 在第 0 層資產名稱行的末尾按一下 圖示。

  Tenable Identity Exposure 會顯示包含通往第 0 層資產的攻擊路徑的帳戶清單。

如要檢閱第 0 層資產的資產曝險程度：

- 在第 0 層資產名稱行的末尾按一下 圖示。

  Tenable Identity Exposure 會開啟此第 0 層資產的資產曝險頁面。如需詳細資訊，請參閱 攻擊關係

## 包含攻擊路徑的帳戶

因為使用者和電腦帳戶可以通過各種攻擊關係取得特權，所以 Tenable Identity Exposure 會顯示包含通往第 0 層資產的攻擊路徑的帳戶，協助您全面瞭解潛在的安全威脅。

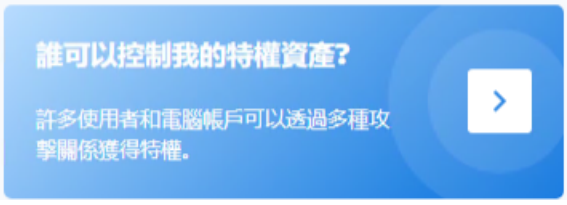
如需詳細資訊，請參閱 識別第 0 層資產。

如要顯示包含攻擊路徑的資產：

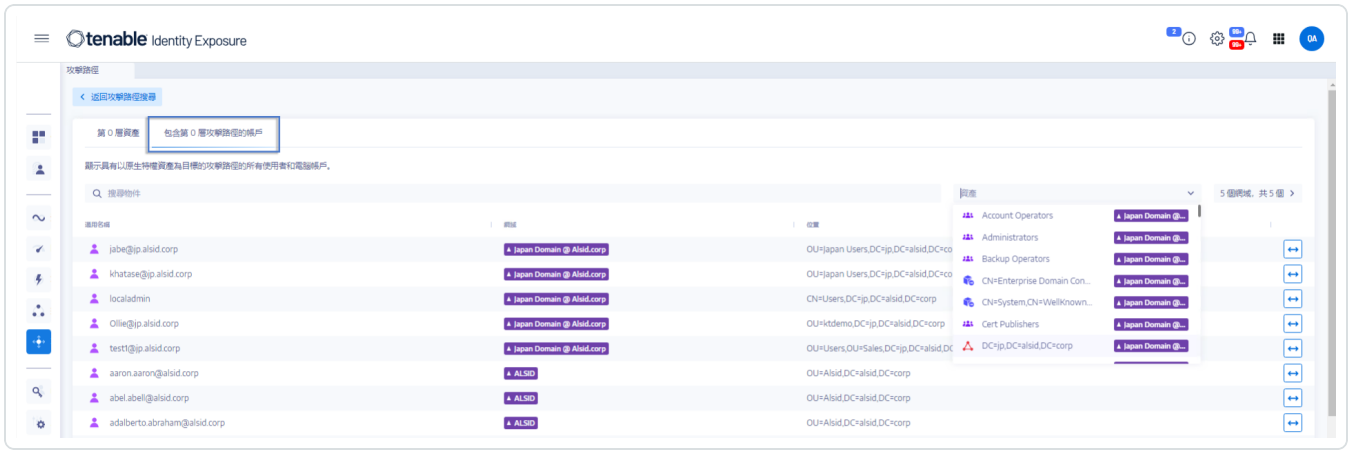
1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的攻擊路徑圖示 。

   「**攻擊路徑**」窗格會隨即開啟。

2. 按一下「**誰可以控制我的特權資產?**」圖塊。



Tenable Identity Exposure 會顯示包含通往第 0 層資產的攻擊路徑的所有使用者和電腦帳戶。




**如要搜尋特定資產：**

1. 在「**搜尋**」方塊中輸入資產的名稱。
2. 在「**資產**」方塊中，按一下箭頭 **>** 以顯示第 0 層資產的下拉式清單，從中選擇一個。

   Tenable Identity Exposure 會使用符合的結果更新清單。

**如要篩選任何特定網域的資產：**

1. 按一下「**n/n**」按鈕。

   「**樹系和網域**」窗格會隨即開啟。您可以執行下列任一動作：

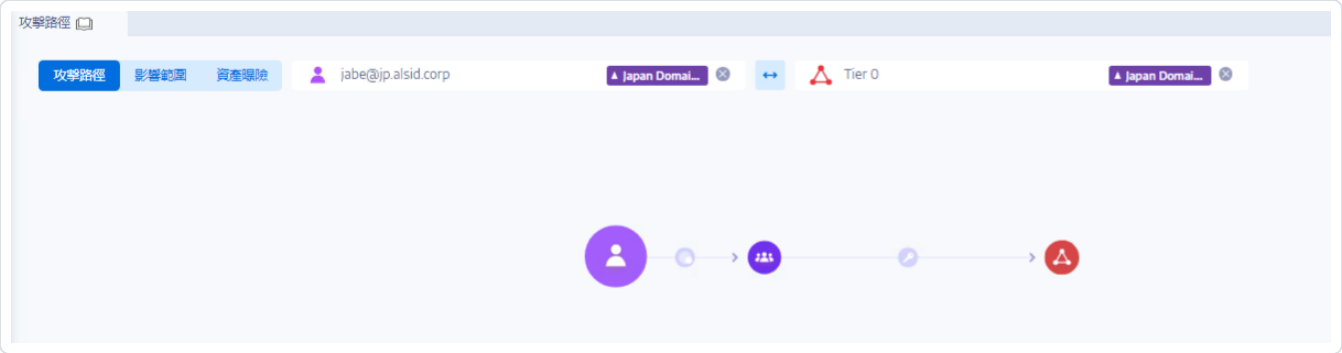
   - 在「**搜尋**」方塊中輸入樹系或網域的名稱。
   - 選取「**全部展開**」方塊，然後選取所需的樹系或網域。
2. 按一下「**篩選選取的項目**」。

   Tenable Identity Exposure 將更新資產清單。

**如要探索攻擊路徑：**

- 在資產名稱行的末尾按一下 ↔ 圖示。

  Tenable Identity Exposure 會開啟從此資產到所有第 0 層資產的攻擊路徑頁面。如需詳細資訊，請參閱 攻擊路徑 和 攻擊關係




## 攻擊路徑節點類型

Tenable Identity Exposure 中的攻擊路徑功能會顯示一張圖表，以視覺化方式呈現您的 Active Directory 環境中攻擊者可利用的攻擊路徑。該圖表分成展示攻擊關係的**邊**和顯示 Active Directory (LDAP/SYSVOL) 物件的**節點**。

下列清單描述了您可能會在攻擊路徑圖表中看到的所有節點類型。

| 節點類型 | 位置 | 圖示 | 說明 |
|---|---|---|---|
| 使用者 | LDAP |  | `objectClass` 屬性包含 `user` 類別但不包含 `computer` 類別的 LDAP 物件。 |
| 群組 | LDAP |  | `objectClass` 屬性包含 `group` 類別的 LDAP 物件。 |
| 裝置 | LDAP |  | `objectClass` 屬性包含 `computer` 類別但不包含 `msDS-GroupManagedServiceAccount` 類別的 LDAP 物件。<br>`primaryGroupID` 屬性不等於 516 (DC) 或 521 (RODC)。<br>**注意**：為了與 Tenable 產品加以區分，我們將此類別稱為「裝置」，而不是涵蓋範圍更廣的「電腦」。 |
| 組織單位 (OU) | LDAP |  | `objectClass` 屬性包含 `organizationalUnit` 類別的 LDAP 物件。任何 Active Directory (AD) 物件都可以作為 |

| | | | |
|---|---|---|---|
| | | | 容器使用，以便容納其他物件。請不要將這類物件與 `container` 類別的物件弄混了。 |
| 網域 | LDAP |  | `objectClass` 屬性包含 `domainDNS` 類別和特定屬性的 LDAP 物件。 |
| 網域控制器 (DC) | LDAP |  | `objectClass` 屬性包含 `computer` 類別，而且 `primaryGroupID` 屬性等於 516 (因此不是 RODC) 的 LDAP 物件。 |
| 唯讀網域控制器 (RODC) | LDAP |  | `objectClass` 屬性包含 `computer` 類別，而且 `primaryGroupID` 屬性等於 521 (因此不是正常 DC) 的 LDAP 物件。 |
| 群組原則 (GPC) | LDAP |  | `objectClass` 屬性包含 `groupPolicyContainer` 類別的 LDAP 物件。 |
| GPO 檔案 | SYSVOL |  | 可在特定 GPO 的 SYSVOL 共用資料夾中找到的檔案 (例如 「`\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml`」) |
| GPO 資料夾 | SYSVOL |  | 可在特定 GPO 的 SYSVOL 共用資料夾中找到的資料夾。每個 GPO 都有一個這類資料夾 (例如 「`\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup`」) |
| 群組管理服務帳戶 (gMSA) | LDAP |  | `objectClass` 屬性包含 `msDS-GroupManagedServiceAccount` 類別的 LDAP 物件。 |
| Enterprise NtAuth | LDAP |  | `objectClass` 屬性包含 `certificationAuthority` 類別的 LDAP 物件。 |

| | | | |
|---|---|---|---|
| 儲存區 | | | |
| PKI 憑證範本 | LDAP |  | `objectClass` 屬性包含 `pKICertificateTemplate` 類別的 LDAP 物件。 |
| 未解析的安全性主體 | LDAP |  | 在建立關係期間的某個時間點，LDAP 物件使用了 `objectSid` 或 `DistinguishedName` 屬性，但對應的 LDAP 安全性主體物件卻不明 (「未解析 SID」的常見案例)。<br><br>另外，也缺少與其相關的特定安全性主體類型 (使用者、電腦、群組等) 的相關資訊；只有 SID/DN 已知。 |
| 特殊身分 | LDAP |  | Windows 和 Active Directory 在內部使用已知身分，這些身分的運作方式與群組類似，但 AD 並未如此宣告。如需更多資訊，請參閱特殊身分群組。 |
| 其他 | |  | 目前不屬於上述類別的所有 AD/SYSVOL 物件。 |

## 活動記錄

Tenable Identity Exposure 中的活動記錄可用來檢視 Tenable Identity Exposure 平台上發生的所有活動痕跡，這些活動與特定 IP 位址、使用者或動作有關。

**注意**：由於技術限制，目前看不到有關特定檢視 (例如「租用戶管理」) 的活動記錄 (包括新增、編輯或移除)。

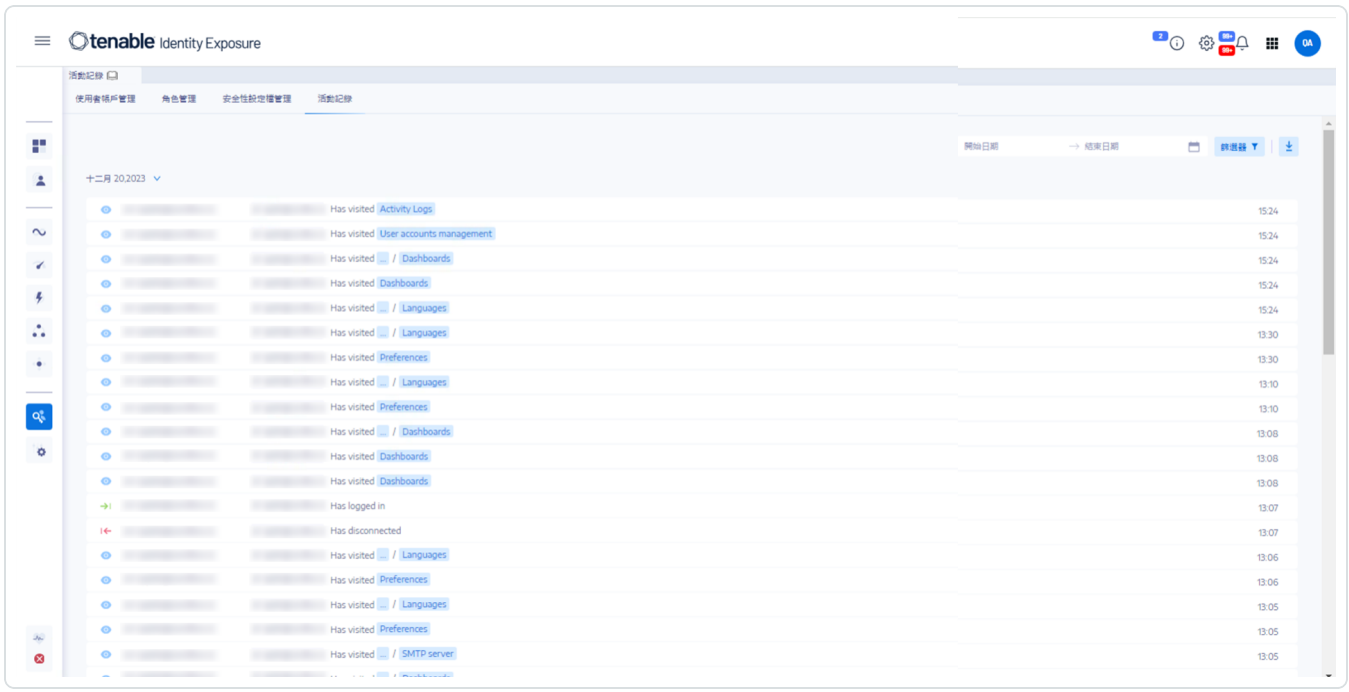
**如要檢視活動記錄：**

1. 在 Tenable Identity Exposure 中，按一下左側導覽功能表中的**帳戶**  圖示。

   「**使用者帳戶管理**」窗格會隨即開啟。

2. 選取「**活動記錄**」索引標籤。

   「活動記錄」窗格會隨即開啟。




**如要顯示特定時間範圍的活動記錄：**

1. 在活動記錄窗格頂端，按一下日期選擇器。
2. 選取所需期間的開始日期和結束日期。
3. (選用) 使用捲軸選取時間 (預設值：目前時間)。
4. 按一下「**確定**」。

   Tenable Identity Exposure 會顯示此時間段的活動記錄。

**如要篩選活動記錄：**

1. 在活動記錄窗格頂端，按一下 Filters 按鈕。

   「**篩選器**」窗格會隨即顯示。
2. 按一下下面方塊中的「>」：
   - IP 位址
   - 使用者
   - 動作

3. 按一下「**驗證**」。

   Tenable Identity Exposure 會顯示您定義的篩選器的活動記錄。

**如要清除篩選器：**

- 在「**篩選器**」窗格的底部，按一下「**清除篩選器**」。

  Tenable Identity Exposure 會顯示未篩選的活動記錄。

**如要匯出活動記錄：**

- 在活動記錄窗格頂端，按一下  圖示。

  Tenable Identity Exposure 會將 CSV 格式的活動記錄下載到您的電腦。

## 特權實體定義

Tenable Identity Exposure 在各種曝險指標、攻擊指標和其他功能中使用「**特權**」實體的概念。對於特權實體，Active Directory 和 Entra ID 有不同的定義：

### Active Directory

特權實體可能包含**特權使用者**、**特權電腦帳戶**、**特權服務帳戶**、**特權群組**、**特權安全主體**等。特權實體包括 (本機) 系統和 KRBTGT (Kerberos 工單授予工單) 使用者，以及下列原生特權群組的所有直接或間接 (轉移) 成員。無論名稱為何，內部都會根據其廣為所有系統所知的 RID/SID 識別。

- 帳戶運算子
- 管理員
- 備份運算子
- 憑證發行者
- 網域管理員
- 網域控制器
- 企業管理員

- 企業網域控制器
- 企業金鑰管理員
- 企業唯讀網域控制器
- 群組原則建立工具所有者
- 金鑰管理員
- 列印運算子
- 唯讀網域控制器
- 複製器
- 架構管理員
- 伺服器操作員

### Entra ID

- **特權權限**或**權限**是由 Microsoft 識別的權利或權限。
- **特權角色**是指含有至少一個 Microsoft 所定義之特權權限的 Entra 角色。
- **特權實體** (使用者、群組或服務主體) 是指直接或間接 (透過角色可指派的群組轉移) 指派給任何特權 Entra 角色的實體。

# Tenable Identity Exposure 設定和管理

本節所述的選項和功能適用於為想要自訂、最佳化和維護 Tenable Identity Exposure 安裝或部署的系統管理員以及進階使用者。

這裡也有提供管理 Active Directory、設定攻擊指標部署、驗證設定、使用者帳戶、安全性設定檔、角色、樹系、網域和警示等主題的專用指示。本節還有介紹執行運作狀況檢查、使用報告中心、與 Microsoft Entra ID (前稱 Azure AD) 整合、授權及疑難排解。

如需與特定工作相關的資訊，請按一下畫面左側功能表窗格中的相關主題。

**權限**：這些工作需要管理存取權限。

## 啟用 Identity 360、曝險中心和 Microsoft Entra ID 支援

啟用 **Identity 360、曝險中心**和 **Microsoft Entra ID** 支援：

**注意**：如要成功啟用這些功能，已建立存取權和秘密金鑰的 Tenable 雲端使用者必須在 Tenable Identity Exposure 授權所引用的 Tenable 雲端容器中擁有管理特權。如需詳細資訊，請參閱 Tenable Identity Exposure 授權。

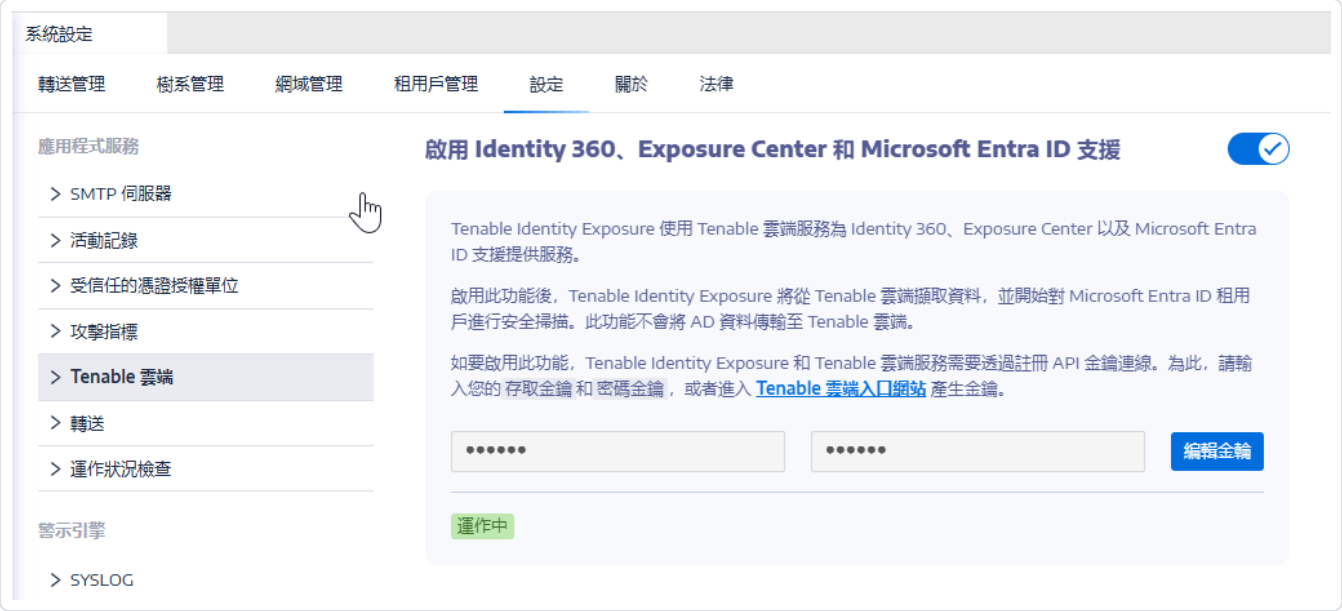
1. 在 Tenable Identity Exposure 中，按一下左側導覽選單中的**系統**圖示 。
2. 按一下「**設定**」索引標籤。

   「**設定**」頁面會隨即開啟。
3. 在「應用程式服務」下方，按一下「**Tenable Cloud**」。
4. 在**啟用 Identity 360、曝險中心和 Microsoft Entra ID 支援**中，點選切換鈕以啟用。
5. 如果您之前未曾登入 Tenable Cloud，請按一下連結前往登入頁面：
   a. 按一下「**忘記密碼?**」以要求重設密碼。
   b. 輸入與 Tenable Identity Exposure 授權相關聯的電子郵件地址，然後按一下「**要求重設密碼**」。

      Tenable 會向此地址傳送包含重設密碼連結的電子郵件。

**注意**：如果您的電子郵件地址與 Tenable Identity Exposure 授權相關聯的電子郵件地址不同，請聯絡您的客戶支援團隊以取得協助。

6. 登入 Tenable Vulnerability Management。
7. 若要在 Tenable Vulnerability Management 中產生 API 金鑰，請前往「Tenable Vulnerability Management」>「**設定**」>「**我的帳戶**」>「**API 金鑰**」。
8. 輸入 Tenable Vulnerability Management「管理員」使用者存取金鑰和密碼金鑰，在 Tenable Identity Exposure 與 Tenable Cloud Service 之間設定連線。
9. 按一下「**編輯金鑰**」以提交 API 金鑰。




Tenable Identity Exposure 會顯示一則訊息，確認其已更新 API 金鑰。

**注意**：若要使用此功能，您**不得**在 Tenable Vulnerability Management 中套用 IP 位址篩選以便允許 API 存取 Tenable Identity Exposure。如需詳細資訊，請參閱 API 存取安全性。

## Active Directory 設定

Tenable Identity Exposure 需要在受監控的 Active Directory 上進行某些設定，才能讓特定功能正常運作：

- 存取 AD 物件或容器
- 特權分析的存取權
- 攻擊指標的部署

## 存取 AD 物件或容器

**注意**：本節僅適用於曝險指標模組的 Tenable Identity Exposure 授權。

Tenable Identity Exposure 不需要系統管理權限即可實現安全性監控。

此方法依賴 Tenable Identity Exposure 用來讀取網域中儲存的所有 Active Directory 物件的使用者帳戶的功能 (包括使用者帳戶、組織單位、群組等)。

根據預設，大多數物件對於 Tenable Identity Exposure 服務帳戶使用的網域使用者群組具有讀取權限。但是，您必須手動設定某些容器，以允許 Tenable Identity Exposure 使用者帳戶的讀取權限。

下表詳述了需要在 Tenable Identity Exposure 監控的每個網域上手動設定讀取權限的 Active Directory 物件和容器。

| 容器的位置 | 說明 |
| --- | --- |
| `CN=Deleted Objects,DC=<DOMAIN>,DC=<TLD>` | 主控已刪除物件的容器。 |
| `CN=Password Settings Container,CN=System,DC=<DOMAIN>,DC=<TLD>` | (選用) 主控密碼設定物件的容器。 |

如要授予 AD 物件和容器的存取權：

- 在網域控制器的 PowerShell 主控台中執行下列命令，即可授予 Active Directory 物件或容器的存取權：

  **注意**：您必須在 Tenable Identity Exposure 監控的每個網域上執行這些命令。

  ```
  #Set Service Account $serviceAccount = "<SERVICE_ACCOUNT>" #Don't Edit after here $domain =
  ```

```
Get-ADDomain @($domain.DeletedObjectsContainer, "CN=Password Settings
Container,$($domain.SystemsContainer)") | ForEach-Object { & dsacls $_ /takeownership & dsacls
$_ /g "$($serviceAccount):LCRP" /I:T }
```

<__SERVICE_ACCOUNT__> 指的是 Tenable Identity Exposure 使用的服務帳戶。

或者，如果無法使用 PowerShell，您也可以針對每個容器執行下列命令：

```
dsacls "<__CONTAINER__>" /takeownership
dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
```

其中：

- <__CONTAINER__> 是指需要存取權的容器。
- <__SERVICE_ACCOUNT__> 指的是 Tenable Identity Exposure 使用的服務帳戶。

## 特權分析的存取權

選用的「特權分析」功能需要系統管理權限。您必須為 Tenable Identity Exposure 使用的服務帳戶指派權限。

如需詳細資訊，請參閱特權分析。

**注意**：您必須在啟用「特權分析」的每個網域上指派權限。

**如要使用命令列指派權限：**

**要求**：如要指派權限，您需要具有網域管理員權限或同等權限的帳戶。

- 在網域控制器的命令列介面中執行下列命令，以新增兩項權限：

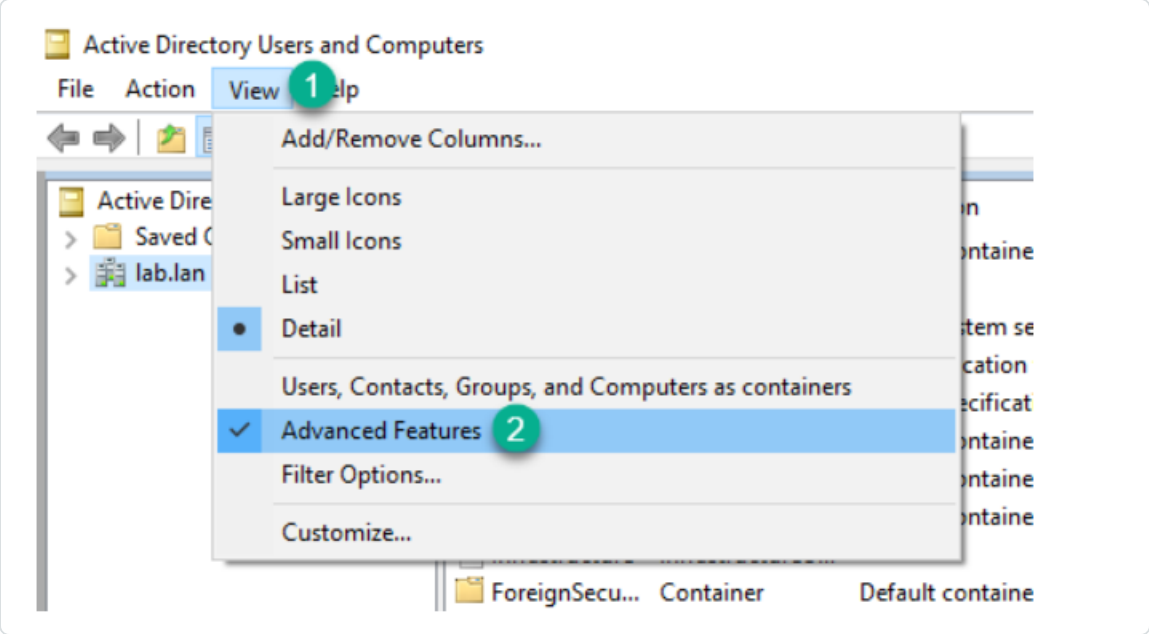
```
dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
```

其中：

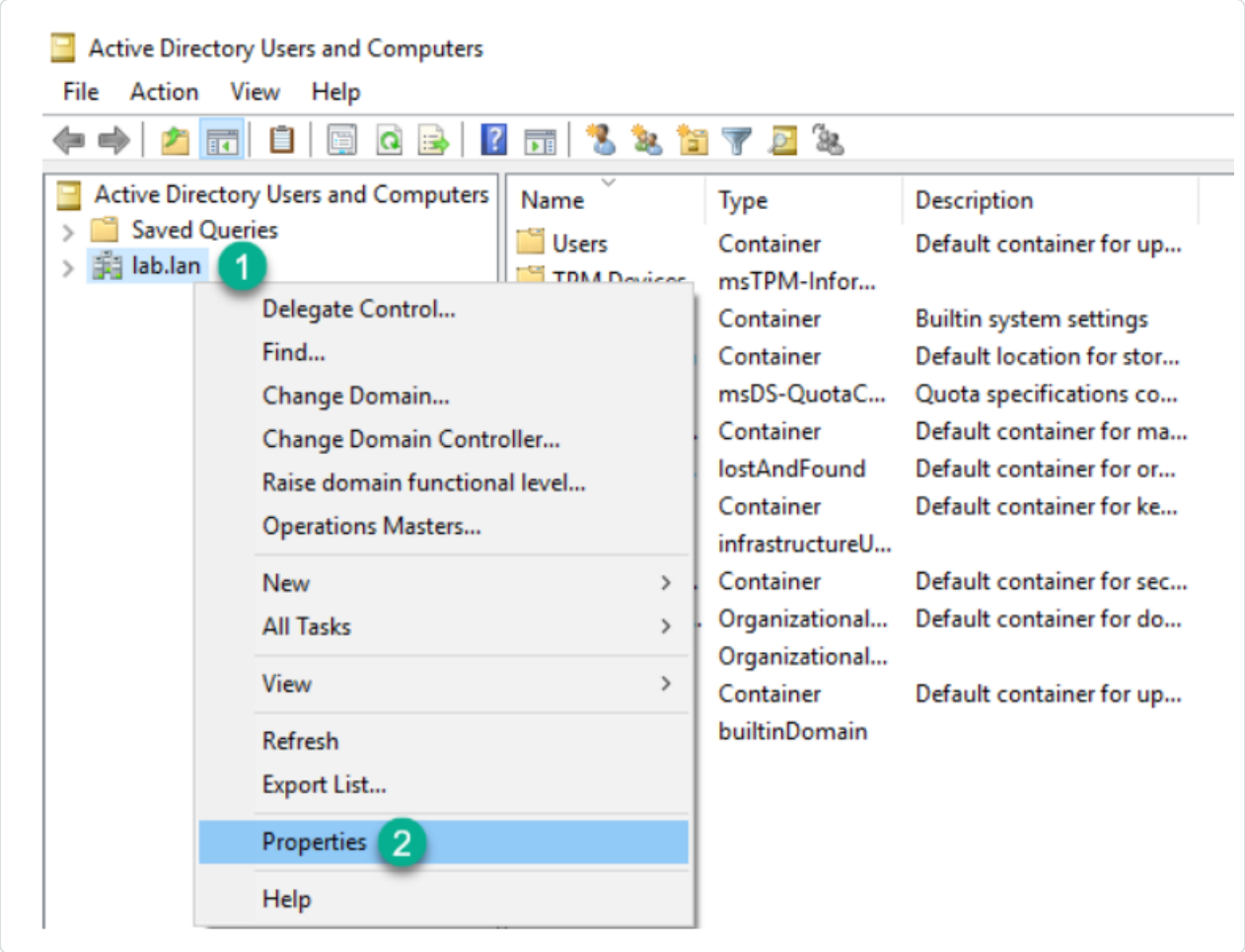
- `<__DOMAIN_ROOT__>` 指的是網域 root 的辨別名稱。範例：`DC=<DOMAIN>,DC=<TLD>`
- `<__SERVICE_ACCOUNT__>` 指的是 Tenable Identity Exposure 使用的服務帳戶。範例：`DOMAIN\tenablead`。

**如要使用圖形化使用者介面指派權限：**

1. 從 Windows 的「**開始**」功能表中開啟「**Active Directory 使用者和電腦**」。
2. 從「**檢視**」功能表中選取「**進階功能**」。

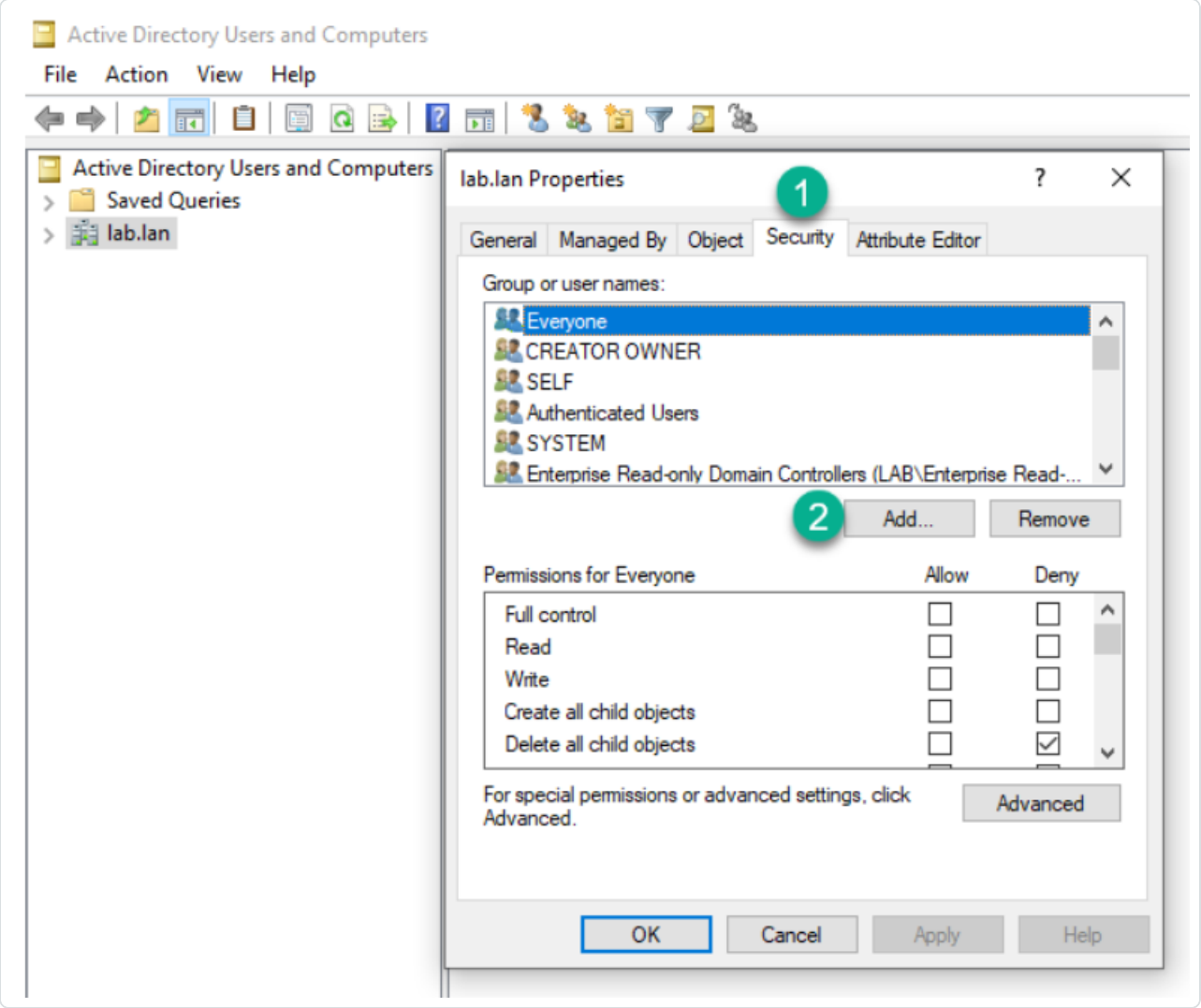



3. 右鍵按一下網域 root 並選取「**屬性**」。



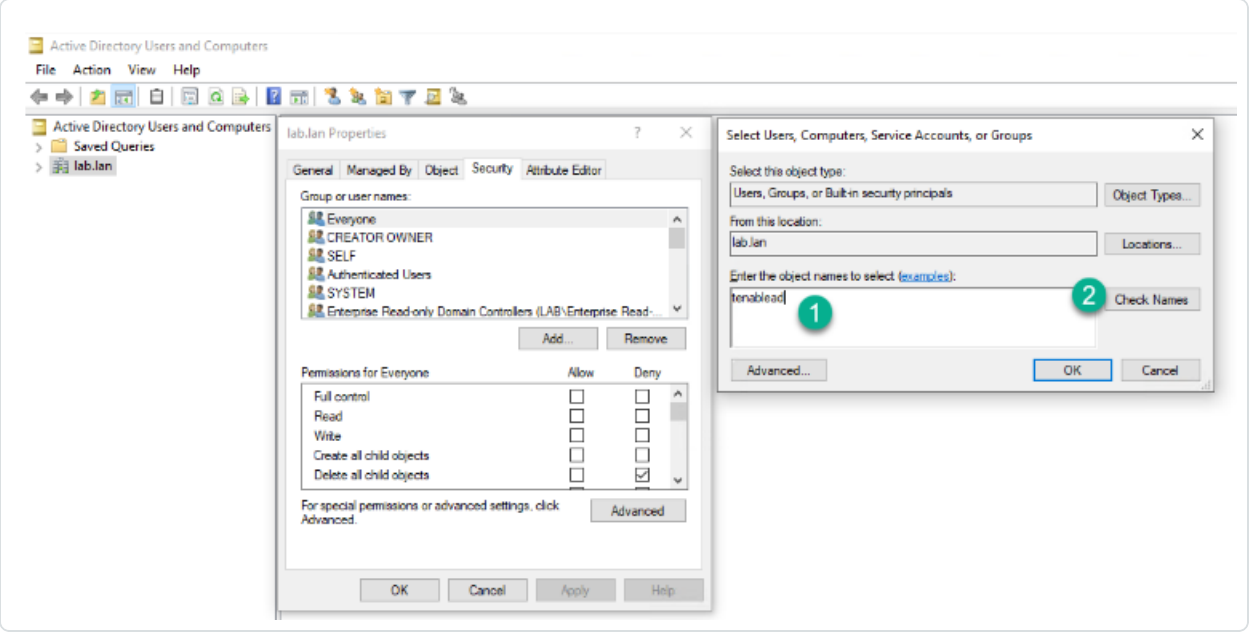

網域 root 的屬性窗格會隨即開啟。

4. 按一下「**安全性**」索引標籤，然後按一下「**新增**」。



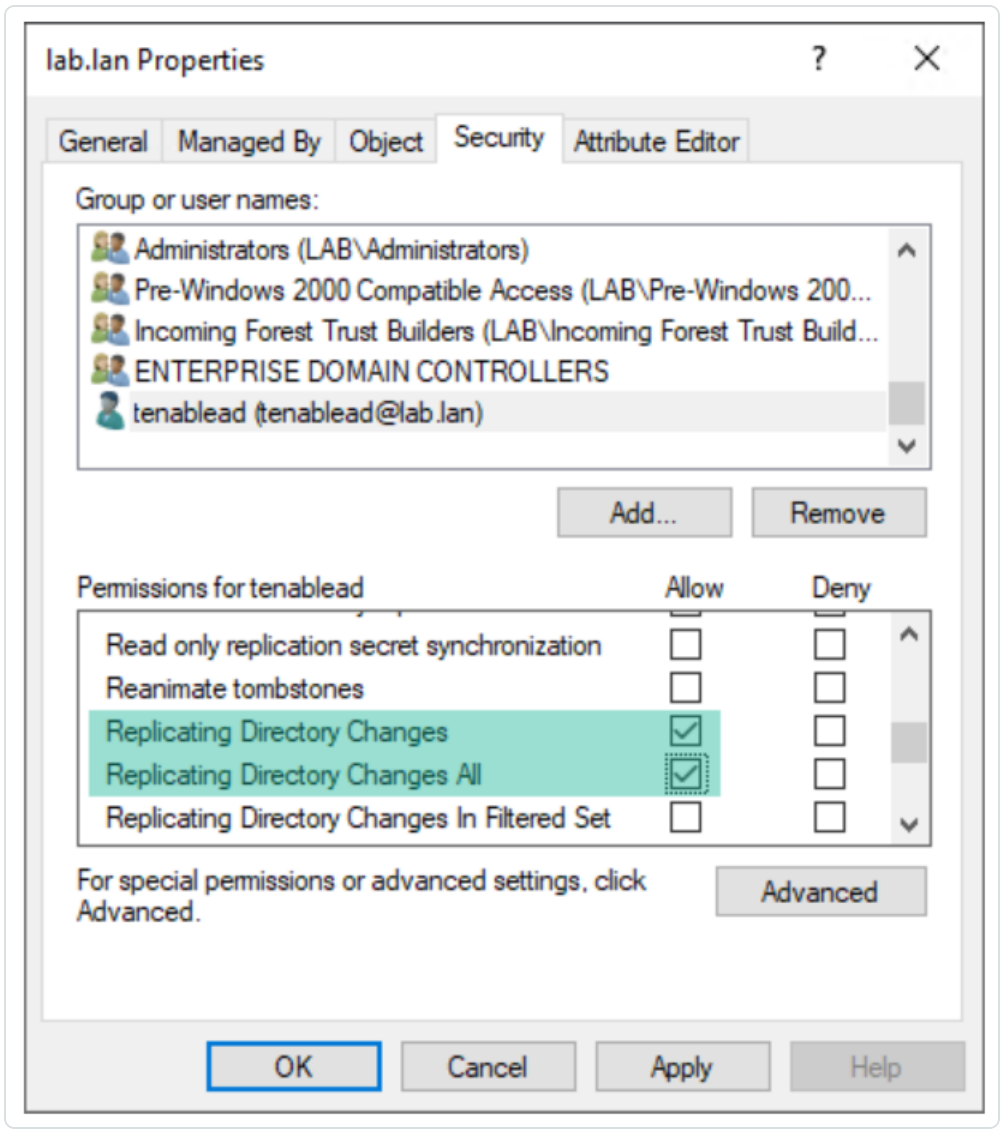

5. 尋找 Tenable Identity Exposure 服務帳戶：

> **注意**：在具有多個網域環境的樹系中，服務帳戶可能位於不同的 Active Directory 網域中。




6. 向下捲動清單並取消選取預設的所有權限。

7. 在「**允許**」欄中，選取「*複製目錄變更*」和「*複製全部目錄*」的權限。




8. 按一下**「確定」**。

## 重要注意事項

Tenable Identity Exposure 中每個樹系只需要一個服務帳戶，因此當您在一個網域中指派權限時，可能需要**從另一個網域搜尋服務帳戶**。

您必須**在網域 root 層級**指派額外的權限。Active Directory 不支援指派給組織單位或特定使用者的權限 (例如將「特權分析」限制為 OU 或使用者)，因此這不會產生任何影響。

這些權限授予 Tenable Identity Exposure 服務帳戶遠高於 Active Directory 網域的權限。您必須將其視為**特權帳戶 (第 0 層)**，並給予與網域管理員帳戶相似的保護。如需完整的程序，請參閱保護服務帳戶。

# 攻擊指標的部署

**注意**:此資訊僅適用於可使用攻擊指標模組的授權。

Tenable Identity Exposure 的**攻擊指標** (IoA) 能夠協助您偵測 Active Directory (AD) 上發生的攻擊。每個攻擊指標 (IoA) 都需要安裝指令碼自動啟用的特定稽核原則。如需 Tenable Identity Exposure IoA 及其實作的完整清單,請參閱 Tenable 下載入口網站中的《Tenable Identity Exposure 攻擊指標參考指南》。

## 攻擊指標和 Active Directory

Tenable Identity Exposure 作為一種非侵入式解決方案,無需部署代理程式即可監控 Active Directory 基礎架構,而且只需在您的環境中進行最少的設定更改。

Tenable Identity Exposure 會使用沒有管理權限的一般使用者帳戶連線至標準 API,以實現安全性監控功能。

Tenable Identity Exposure 會利用 Active Directory 複製機制擷取相關資訊,這只會在每個網域的 PDC 和 Tenable Identity Exposure 的目錄接聽程式之間產生有限的頻寬成本。

為了使用攻擊指標有效率地偵測安全性資安事端,Tenable Identity Exposure 會使用 Windows 事件追蹤 (ETW) 資訊和每個網域控制器上可用的複製機制。如要收集這組資訊,請使用 Tenable Identity Exposure 中的指令碼部署專用的群組原則物件 (GPO),如 安裝攻擊指標 中所述。

此 GPO 會在所有網域控制器上啟動寫入系統磁碟區 (SYSVOL) 的使用 Windows EvtSubscribe API 的事件記錄接聽程式,以便從 AD 複製引擎和 Tenable Identity Exposure 偵聽 SYSVOL 事件的功能中獲益。GPO 會在 SYSVOL 中為每個網域控制器建立一個檔案,並定期清除其內容。

如要啟動安全性監控,Tenable Identity Exposure 必須聯絡 Microsoft 的標準目錄 API。




## 網域控制器

Tenable Identity Exposure 只需要使用網路流量對照表中描述的網路通訊協定與主要網域控制器模擬器 (PDCe) 通訊。

如果有多個受監控的網域或樹系，Tenable Identity Exposure 必須聯絡每個網域的 PDCe。為了達到最佳效能，Tenable 建議您將 Tenable Identity Exposure 託管在靠近 PDCe 的物理網路上進行監控。

## 使用者帳戶

Tenable Identity Exposure 使用非管理員使用者帳戶對受監控的基礎架構進行驗證，以存取複製流程。

單一 Tenable Identity Exposure 使用者可存取所有收集的資料。Tenable Identity Exposure 不會存取秘密屬性，例如憑證、密碼雜湊或 Kerberos 金鑰。

Tenable 建議您建立屬於「網域使用者」群組的服務帳戶，如下所示：

- 服務帳戶位於主要的受監控網域上。
- 服務帳戶位於任何組織單位 (OU) 中，最好是在您建立其他安全性服務帳戶的位置。
- 服務帳戶具有標準使用者群組成員資格 (例如，網域使用者 AD 預設群組的成員)。

**開始之前**

- 檢閱安裝攻擊指標 (IoA) 的限制和潛在影響，如 技術變更和潛在影響 中所述。
- 檢查 DC 是否已安裝適用於 Active Directory 和 GroupPolicy 的 PowerShell 模組並且可用。

  若要執行此操作，請在您計劃部署攻擊指標 (IoA) 模組的目標機器 (DC) 上執行下列 PowerShell 命令：

  ```
  if (-not (Get-Module -ListAvailable -Name GroupPolicy)) {
      Write-Error "The GroupPolicy module is not installed or not available on this machine. This is a requirement for this script and the IOAs to run, please install it and run this script again."
  }
  ```

  主控台中出現的任何錯誤皆表示此要求並未在您目前的環境中經過驗證。
- 檢查 DC 是否啟用了分散式檔案系統工具功能 RSAT-DFS-Mgmt-Con，以便部署指令碼可以檢查複製狀態，因為其無法在 DC 複製時建立 GPO。
- Tenable Identity Exposure 建議您在非高峰時間安裝/升級攻擊指標 (IoA)，以限制您的平台中斷。
- 檢查權限：如要安裝攻擊指標 (IoA)，您必須擁有具有下列權限的使用者角色：
  - 在**資料實體**中，以下項目的「讀取」存取權：
    - 所有攻擊指標
    - 所有網域
  - 在**介面實體**中，以下項目的存取權：
    - 管理 > 系統 > 設定
    - 管理 > 系統 > 設定 > 應用程式服務 > 攻擊指標
    - 管理 > 系統 > 設定 > 應用程式服務 > 攻擊指標 > 下載安裝檔案

  如需有關角色型權限的詳細資訊，請參閱 設定角色的權限。

## 另請參閱

- 安裝攻擊指標
- 攻擊指標安裝指令碼

- 技術變更和潛在影響
- 安裝 Microsoft Sysmon 是 Tenable Identity Exposure 的某些攻擊指標取得相關系統資料時需要用到的 Windows 系統工具。
- 對攻擊指標進行疑難排解

## 安裝攻擊指標

**所需的使用者角色**：具有在 Tenable Identity Exposure 中修改攻擊指標設定權限的組織使用者。如需詳細資訊，請參閱 設定角色的權限。

Tenable Identity Exposure 的攻擊指標 (IoA) 模組要求您使用系統管理帳戶執行 PowerShell 安裝指令碼，此帳戶要能夠建立新的群組原則物件 (GPO) 並將其連結至組織單位 (OU)。您可以從任何已加入您的 Active Directory 網域的電腦執行此指令碼，此網域應是 Tenable Identity Exposure 監控的網域並且可以透過網路連線至網域控制器。

**注意**：Tenable Identity Exposure 每次發行新的主要版本之後，您都必須重新部署攻擊指標 (IoA) 安裝指令碼。

**注意**：建議的 PowerShell 版本為 5.1。

所建立的 GPO 會自動將事件接聽程式部署至所有現有和新的網域控制器 (DC)，因此您只需針對每個 AD 網域執行此安裝指令碼一次。

此外，啟用「自動更新」選項可避免重新執行安裝指令碼，即使您變更攻擊指標 (IoA) 設定也是如此。

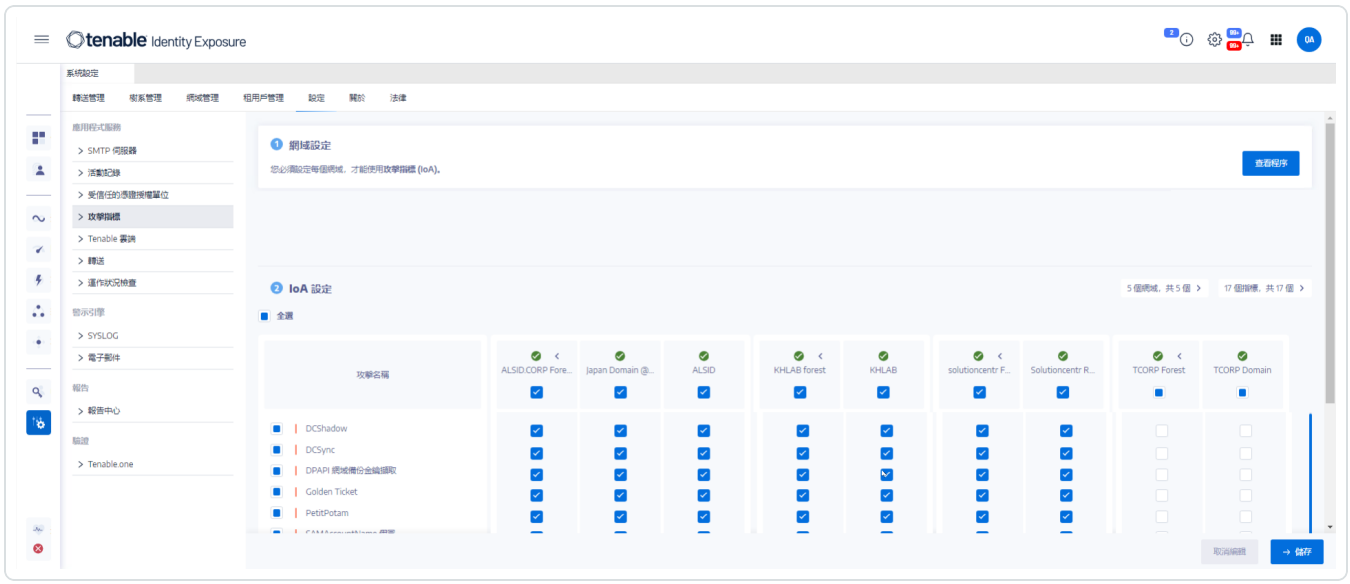
**如要設定攻擊指標 (IoA) 的網域：**

1. 在 Tenable Identity Exposure 中，按一下左側功能表列上的「**系統**」，然後按一下「**設定**」索引標籤 。

   「**設定**」窗格會隨即顯示。

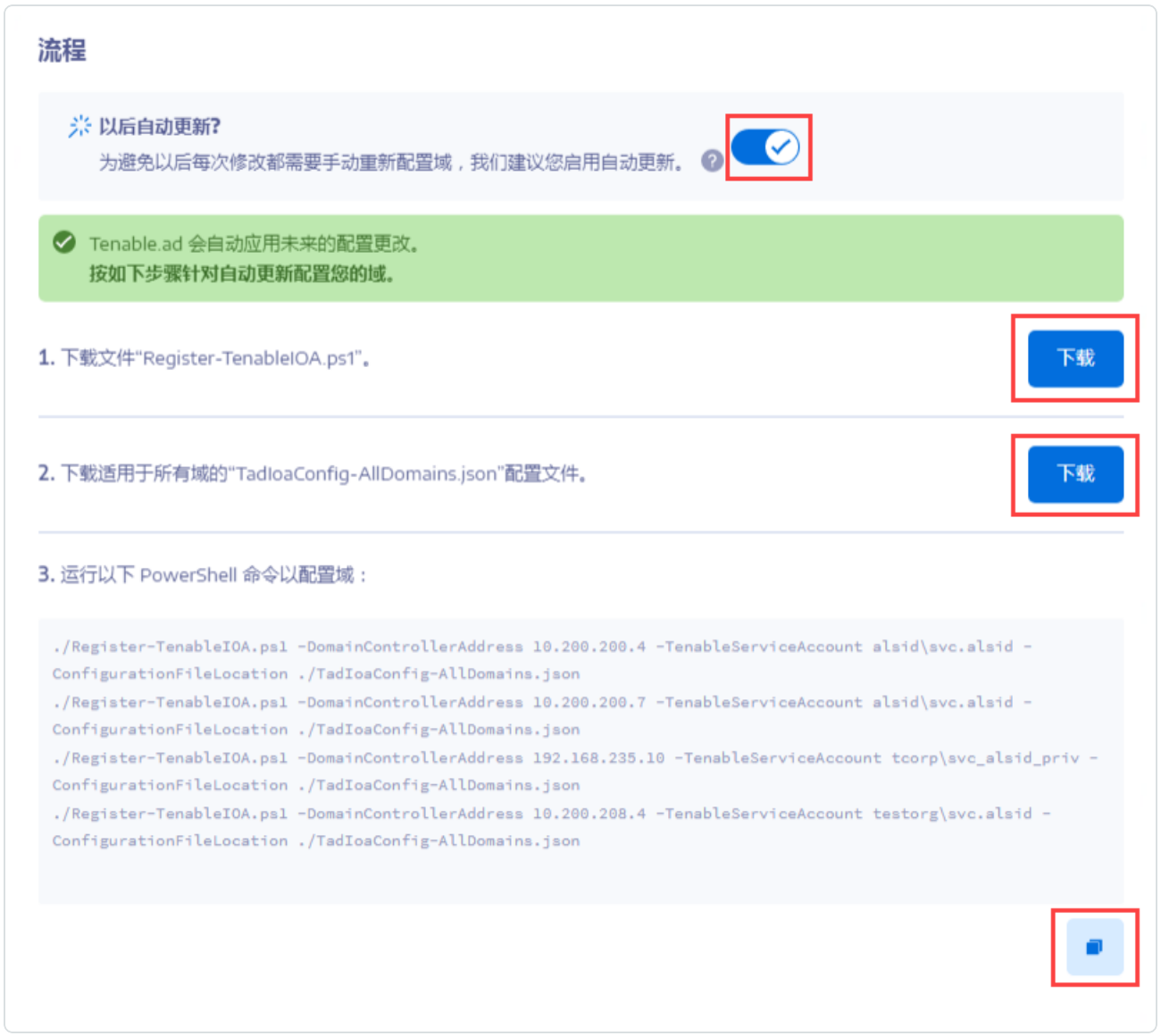
2. 按一下「**攻擊指標**」。

   攻擊指標設定窗格會隨即顯示。




3. 在「**(1) 網域設定**」中，按一下「**查看程序**」。

   程序視窗會隨即開啟。




4. 在「**未來是否自動更新?**」下方：
   - 預設選項「**啟用**」允許 Tenable Identity Exposure 在您日後在 Tenable Identity Exposure 中修改時自動更新您的攻擊指標 (IoA) 設定。這也可確保持續的安全性分析。
   - 如果您關閉此選項，系統會顯示一則訊息，要求您將其開啟以取得未來自動更新。按一下「**查看程序**」並切換為「**啟用**」。
5. 按一下「**下載**」以下載要為每個網域執行的指令碼 (`Register-TenableIOA.ps1`)。
6. 按一下「**下載**」以下載網域的設定檔 (`TadIoaConfig-AllDomains.json`)。

7. 按一下 以複製 Powershell 命令，設定您的網域。

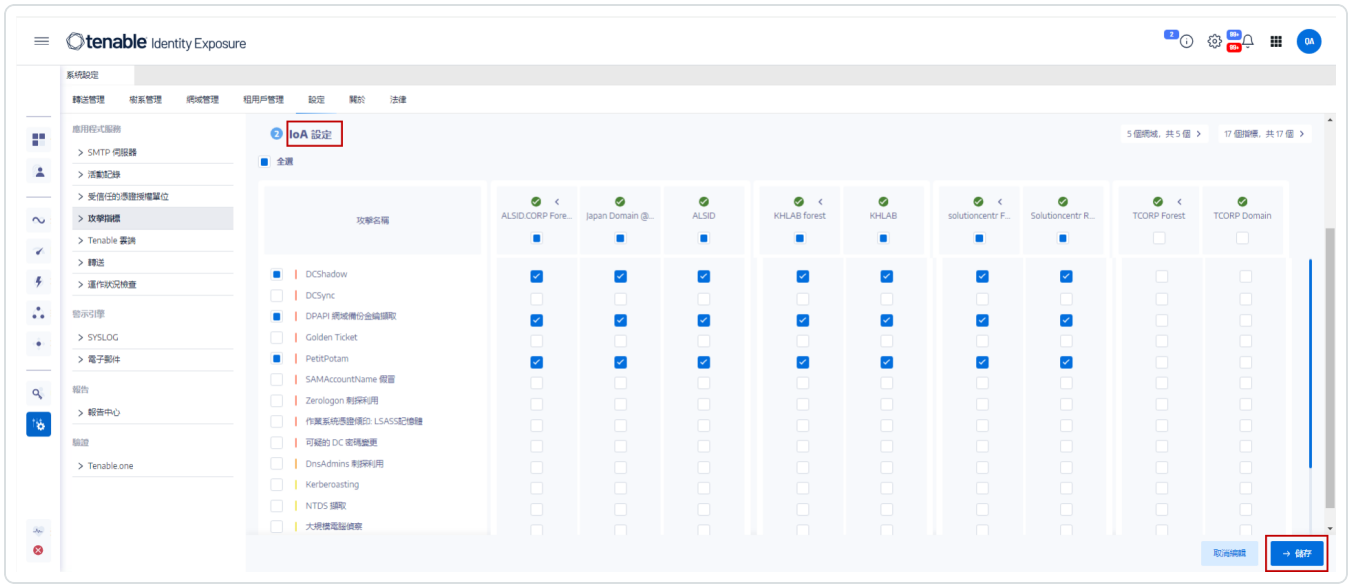
8. 在程序窗口外按一下將其關閉。

9. 以系統管理權限開啟 PowerShell 終端機，然後執行命令，為攻擊指標 (IoA) 設定網域控制器。

> **注意**：您在安裝攻擊指標 (IoA) 和查詢網域時使用的服務帳戶必須在 Tenable Identity Exposure (前稱 Tenable.ad) GPO 資料夾中擁有寫入權限。安裝指令碼會自動新增此權限。如果您移除此權限，Tenable Identity Exposure 會顯示錯誤訊息，並且自動更新將不再運作。如需詳細資訊，請參閱 攻擊指標安裝指令碼。

**如要設定攻擊指標 (IoA)：**

1. 在攻擊指標 (IoA) 設定窗格中，在「**IoA 設定**」下選取您要在設定中使用的攻擊指標。



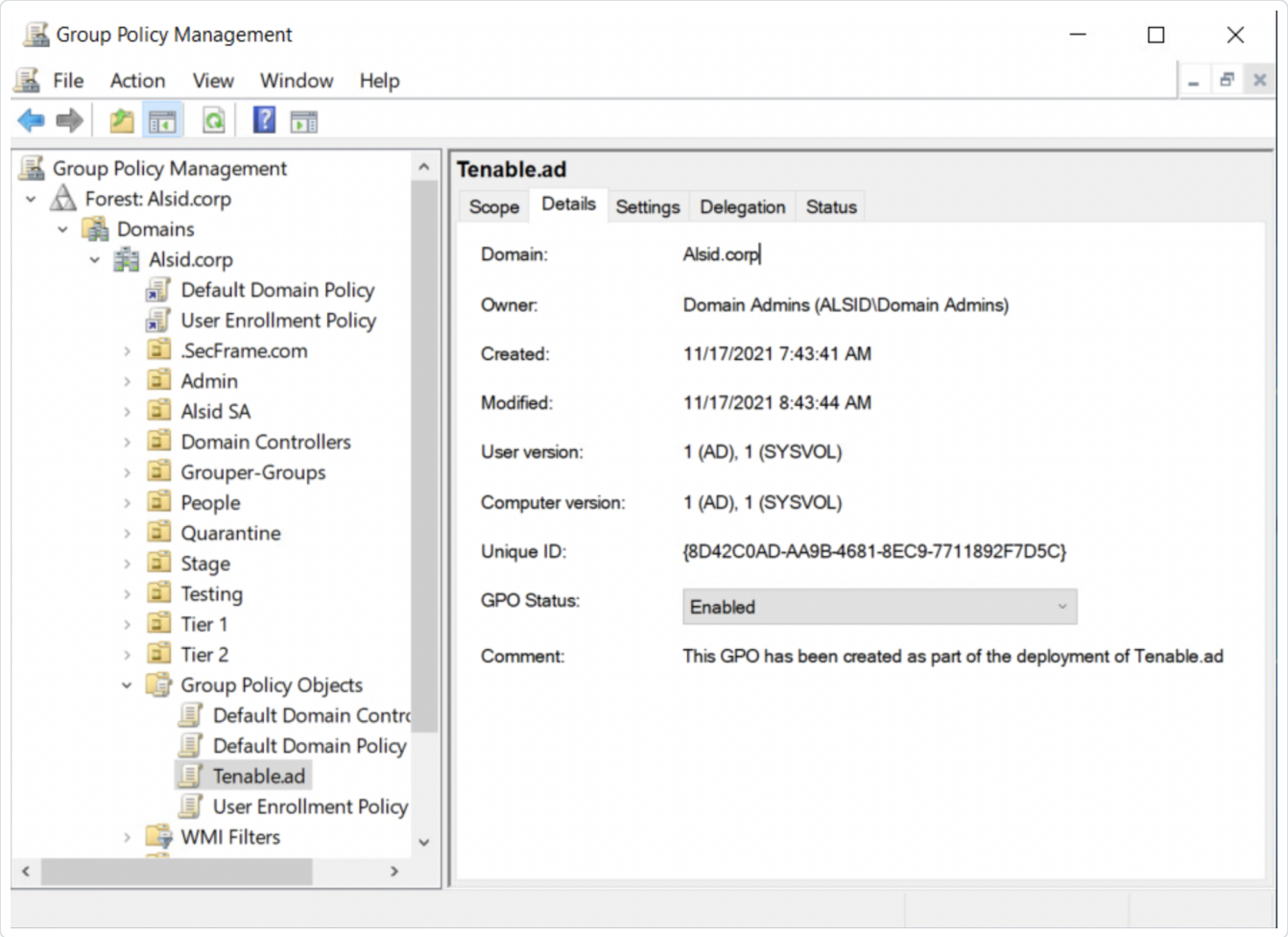

> **提示**：**Zerologon 攻擊程式**的攻擊指標 (IoA) 從 2020 年開始引入。如果您所有網域控制器 (DC) 在過去三年內收到更新，便會受到保護，不用擔心此弱點遭到攻擊者利用。若要確定需要哪些修補程式來保護您的 DC 免於此弱點的影響，請參閱 Microsoft 的 Netlogon 特權提升弱點 (Netlogon Elevation of Privilege Vulnerability) 中的資訊。確認 DC 的安全性之後，您可以安全地停用此攻擊指標 (IoA) 以避免收到不必要的警示。

2. 按一下「**儲存**」。

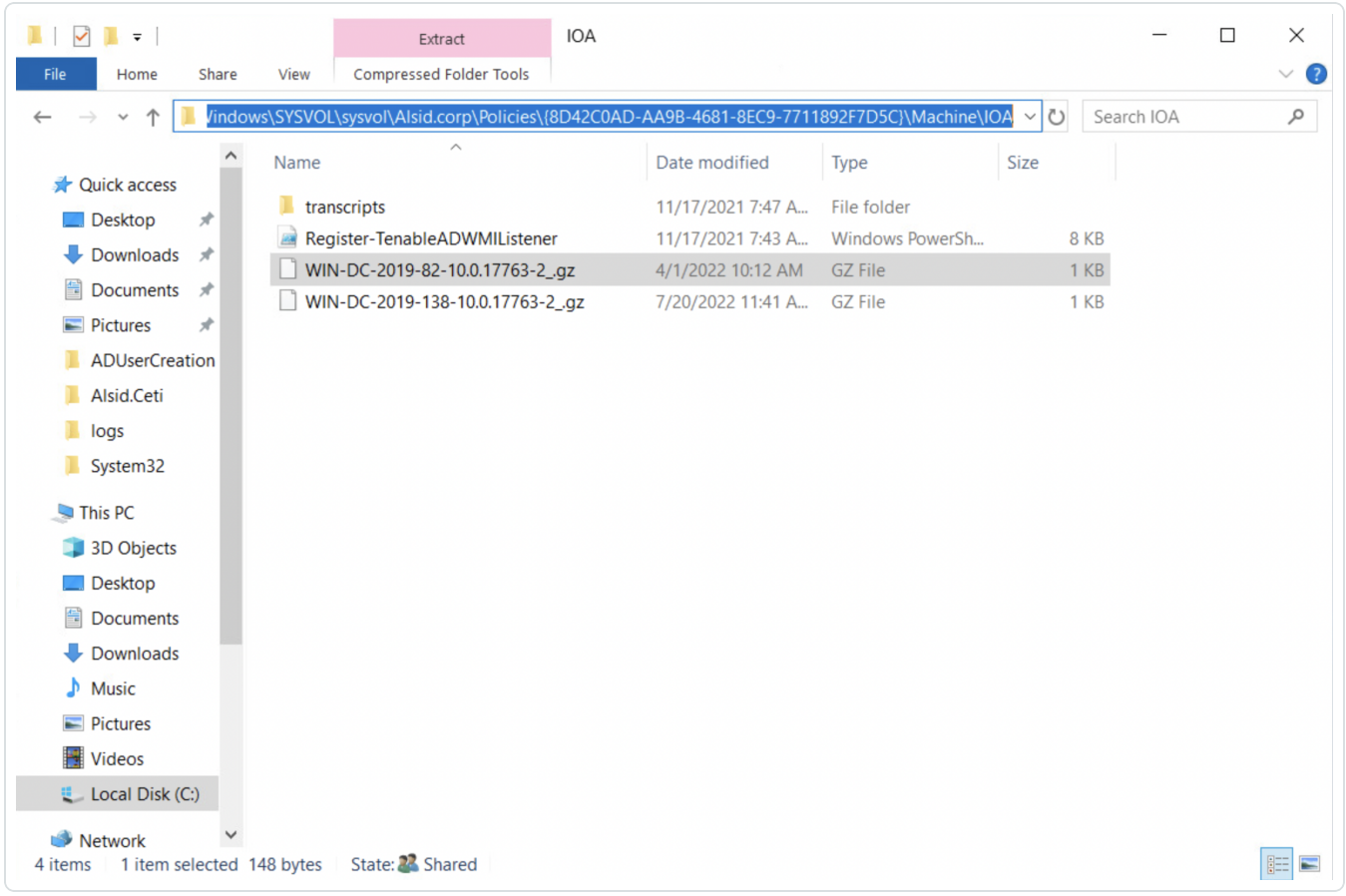
- 如果您已啟用「**未來自動更新**」，Tenable Identity Exposure 會儲存並自動更新您的新設定。等待幾分鐘後，此更新才會生效。
- 如果您未啟用「**未來自動更新**」，系統會顯示程序視窗，指引您 如要設定攻擊指標 (IoA) 的網域：

**如要檢查攻擊指標 (IoA) 安裝：**

1. 在「群組策略管理」中檢查是否存在新的 Tenable Identity Exposure GPO，以及它是否連結至網域控制器 OU：



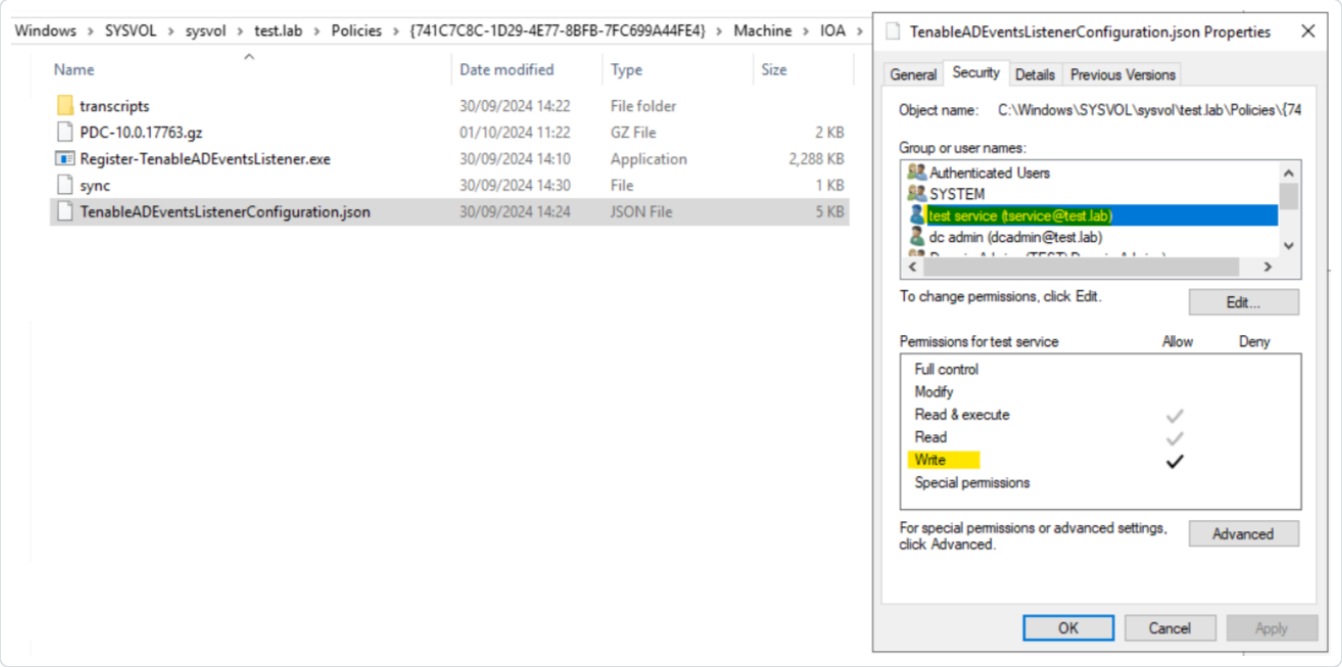

2. 測試攻擊指標 (IoA) 之前，請前往路徑 `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA`，並檢查**所有網域控制器**的 `.gz` 檔案是否存在：




**如要檢查 Tenable Identity Exposure 服務帳戶的「寫入」權限：**

1. 在檔案管理員中，前往 `\\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\Machine\`。
2. 右鍵按一下 `TenableADEventsListenerConfiguration.json` 檔案，然後選取「**屬性**」。
3. 選取「**安全性**」索引標籤，然後按一下「**進階**」。
4. 按一下「**有效存取權**」索引標籤。
5. 按一下「**選取使用者**」。
6. 類型 `<TENABLE-SERVICE-ACCOUNT-NAME>`，然後按一下「**確定**」。
7. 按一下「**檢視有效存取權**」。

8. 檢查 Tenable 服務帳戶的「寫入」權限是否已啟用。




或者，您可以使用 PowerShell：

- 執行下列命令：

```
Install-Module -Name NTFSSecurity -RequiredVersion 4.2.3
```

```
Get-NTFSEffectiveAccess -Path \\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\IOA\ -
Account <TENABLE-SERVICE-ACCOUNT-NAME>
```

### 若要校正攻擊指標 (IoA)：

為避免誤報攻擊或缺少合法攻擊偵測，您必須根據環境來校正攻擊指標，方法是調整攻擊指標以使其適應 Active Directory 的大小，或是將已知工具列入白名單等。

1. 如需瞭解選項相關資訊和要選取的建議值，請參閱《Tenable Identity Exposure 攻擊指標參考指南》。
2. 在安全性設定檔中，將選項和值套用至每個攻擊指標 (如 自訂指標 中所述)。

### 疑難排解

部署期間可能會出現下列錯誤訊息：

| 訊息 | 修復 |
| --- | --- |
| 「Tenable Identity Exposure無法寫入設定檔，因為目標資料夾 <targetFolder> 不存在。這表示攻擊指標 (IoA) 模組部署可能已失敗。」 | 解除安裝指令碼，然後按一下「查看程序」以獲取重新安裝指令碼的說明。 |
| 「Tenable Identity Exposure無法寫入位於 <targetFile> 的設定檔以執行更新。這可能是因為另一個處理程序鎖定了檔案或權限有變更。」 | • 請確認除攻擊指標 (IoA) 模組外沒有其他處理程序在使用此設定檔。<br>• 檢查服務帳戶是否具有修改檔案內容的權限。<br>• 如果您不想向服務帳戶授予權限，請停用「自動更新」開關，並按一下「查看程序」以取得有關在每次修改攻擊指標 (IoA) 設定時如何進行手動更新的說明。 |
| 「目標資料夾 <targetFolder> 包含無法執行自動更新的 Tenable Identity Exposure 版本。」 | 目前安裝的指令碼是使用 WMI 的舊版本。解除安裝目前版本，然後下載新的安裝指令碼，並執行此指令碼。 |
| 「設定檔部署遇到意外錯誤。」 | 解除安裝指令碼，然後按一下「查看程序」以獲取重新安裝指令碼的說明。如果這行不通，請聯絡您的客戶支援代表。 |

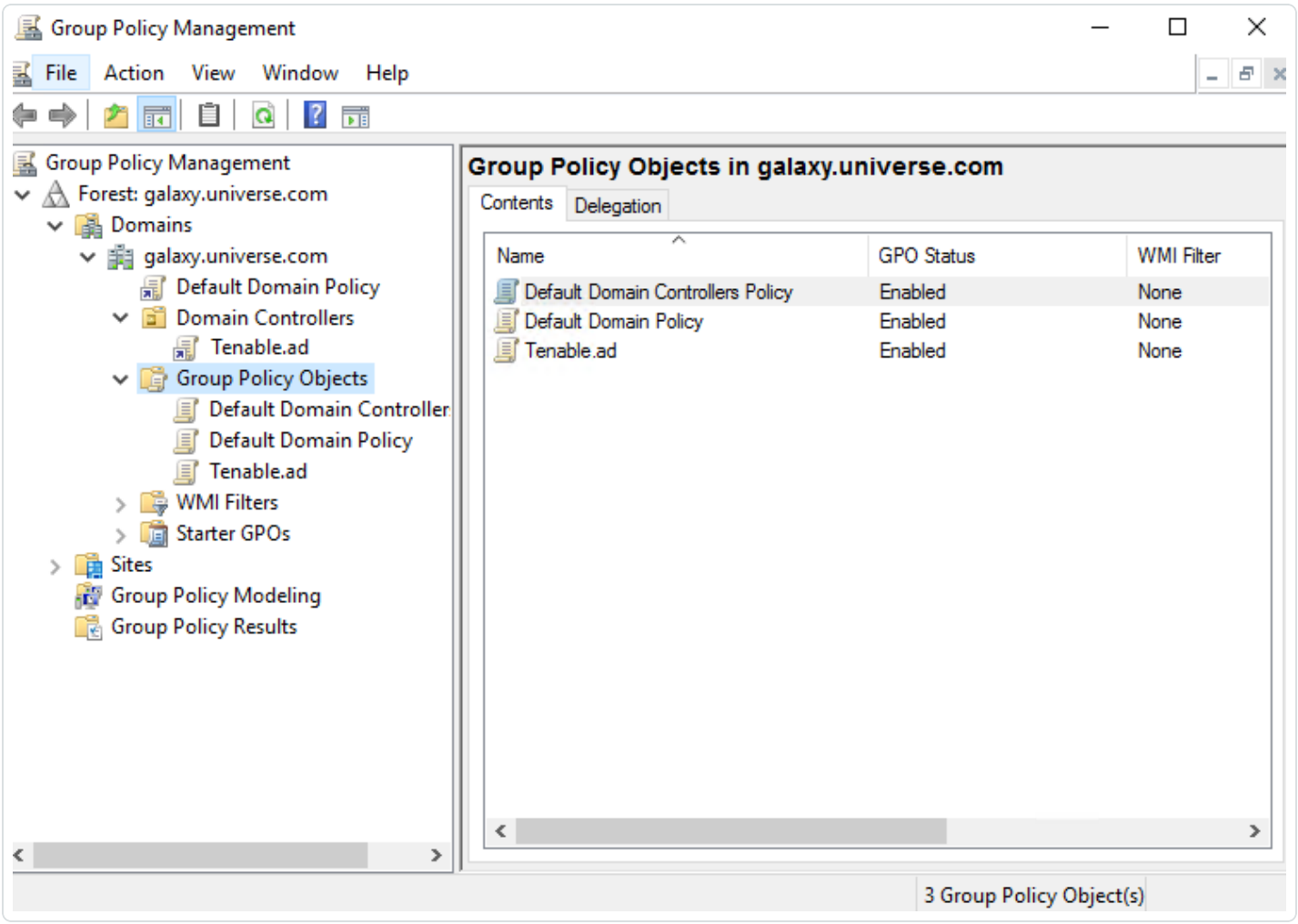
如需詳細資訊，請參閱：

- 攻擊指標安裝指令碼
- 技術變更和潛在影響
- 防毒軟體偵測
- 進階稽核原則設定優先順序

## 攻擊指標安裝指令碼

在您下載並執行攻擊指標 (IoA) 安裝檔案之後，IoA 指令碼會在 Active Directory (AD) 資料庫中建立一個預設命名為 `Tenable.ad` 的新群組原則物件 (GPO)。系統僅會將 Tenable Identity

Exposure GPO 連結至包含所有網域控制器 (DC) 的網域控制器組織單位 (OU)。新原則會使用 GPO 機制在所有 DC 之間自動複製。




### 安裝指令碼 (Tenable Identity Exposure v. 3.29 及更新版本)

GPO 包含所有 DC 為收集相關資料而在本機執行的 PowerShell 指令碼，如下所示：

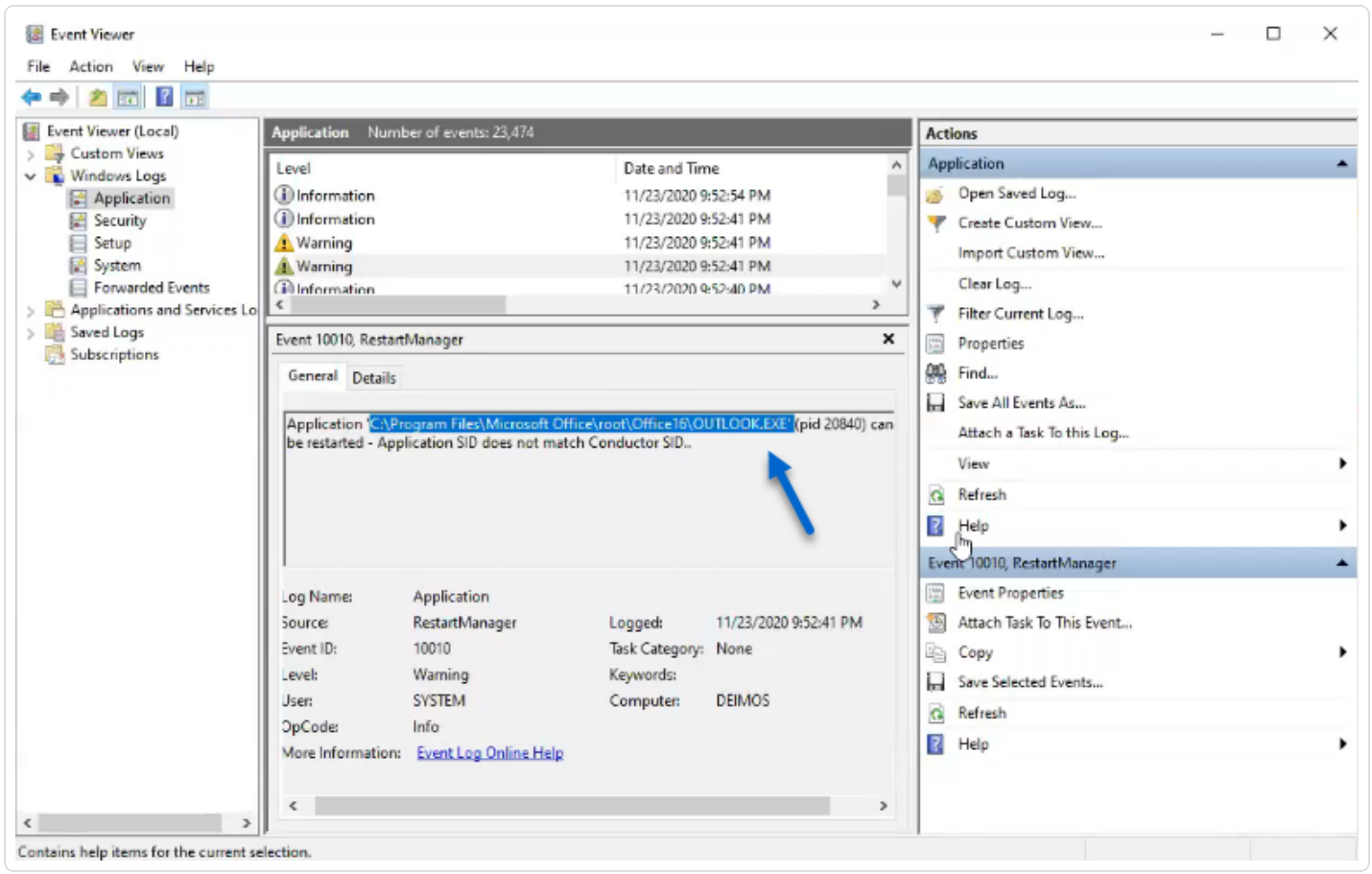
- 此指令碼使用 Windows EvtSubscribe API 在每個網域控制器上設定事件記錄接聽程式。如 `TenableADEventsListenerConfiguration.json` 設定檔中所指定，此指令碼透過為每個符合的事件記錄提交請求和由 EvtSubscribe 觸發的回呼來訂閱每個必要的事件記錄通道。
- 事件接聽程式會接收事件記錄並進行緩衝，然後定期將它們排清到儲存在 SYSVOL 網路共用的一個檔案中。每個 DC 的內容都會被清除至一個儲存所收集事件的 SYSVOL 檔案中，然後複製到其他網域控制器。

- 此指令碼還會建立一個 WMI 消費者，通過在 DC 重新啟動時重新註冊事件訂閱者來確保此機制的持久性。每次 DC 重新啟動時，WMI 都會通知消費者，以便消費者再次註冊事件接聽程式。
- 此時，分散式檔案系統 (DFS) 會複製，並在網域控制器之間自動同步檔案。Tenable Identity Exposure 的平台會接聽傳入的 DFS 複製流量，並使用此資料收集事件、執行安全性分析，然後產生攻擊指標 (IoA) 警示。

## 本機資料擷取

Windows 事件記錄會記錄作業系統及其應用程式中發生的所有事件。事件記錄依賴 Windows 中整合的元件架構。

Tenable Identity Exposure 攻擊指標 (IoA) 事件記錄接聽程式只會使用 EvtSubscribe API，以插入字串形式收集其從事件記錄中擷取的有用事件記錄資料區段。Tenable Identity Exposure 會將這些插入字串寫入儲存在 SYSVOL 資料夾中的檔案，並透過 DFS 引擎複製這些字串。這樣，Tenable Identity Exposure 就可從事件記錄中收集正確數量的安全性資料，以執行安全性分析並偵測攻擊。




## 攻擊指標 (IoA) 指令碼摘要

下表提供 Tenable Identity Exposure 指令碼部署的概覽。

| 步驟 | 說明 | 涉及的元件 | 技術動作 |
|---|---|---|---|
| 1 | 註冊 Tenable Identity Exposure 的 IoA 部署 | GPO 管理 | 建立 `Tenable.ad` (預設名稱) GPO 並將其連結至網域控制器 OU。 |
| 2 | 在 DC | DC 本 | 每個 DC 都會偵測要套用的新 GPO，具體取決於 AD 複製和 |

| | | | |
|---|---|---|---|
| | 上啟動 Tenable Identity Exposure 的 IoA 部署 | 機系統 | 群組原則重新整理間隔。 |
| 3 | 控制進階記錄原則狀態 | DC 本機系統 | 系統透過設定登錄機碼 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy` 來啟動進階記錄原則。 |
| 4 | 更新本機記錄原則 | DC 本機系統 | 根據要偵測的攻擊指標 (IoA), Tenable Identity Exposure 會動態產生並啟動特定的稽核原則。此原則不會停用任何現有的記錄原則, 而只會在必要時加以擴充。如果偵測到衝突, GPO 安裝指令碼會停止並顯示訊息「Tenable Identity Exposure 需要稽核原則 '...', 但目前的 AD 設定禁止使用。」 |
| 5 | 註冊事件接聽程式和 WMI 生產者 | DC 本機系統 | 系統會註冊並執行 GPO 中包含的指令碼。此指令碼會執行 PowerShell 處理程序, 以使用 EvtSubscribe API 訂閱事件記錄, 並建立 `ActiveScriptEventConsumer` 的執行個體以供持續使用。Tenable Identity Exposure 會使用這些物件接收和儲存事件記錄內容。 |
| 6 | 收集事件記錄訊息 | DC 本機系統 | Tenable Identity Exposure 會擷取相關的事件記錄訊息, 然後定期緩衝, 並將其儲存在與 Tenable Identity Exposure GPO (`...{GPO_GUID}\Machine\IOA<DC_name>`) 相關聯的 SYSVOL 資料夾中儲存的檔案 (每個 DC 一個檔案) 中。 |
| 7 | 將檔案複製到宣告的 DC SYSVOL 資料 | Active Directory | AD 可使用 DFS 跨網域複製檔案, 特別是在宣告的 DC 中。Tenable Identity Exposure 平台會取得每個檔案的通知並讀取其內容。 |

| | | | |
|---|---|---|---|
| | 夾 | | |
| 8 | 覆寫這些檔案 | Active Directory | 每個 DC 都會自動且持續地將定期緩衝的事件寫入相同的檔案中。 |

**安裝指令碼 (Tenable Identity Exposure v. 3.19.11 和更早版本)**

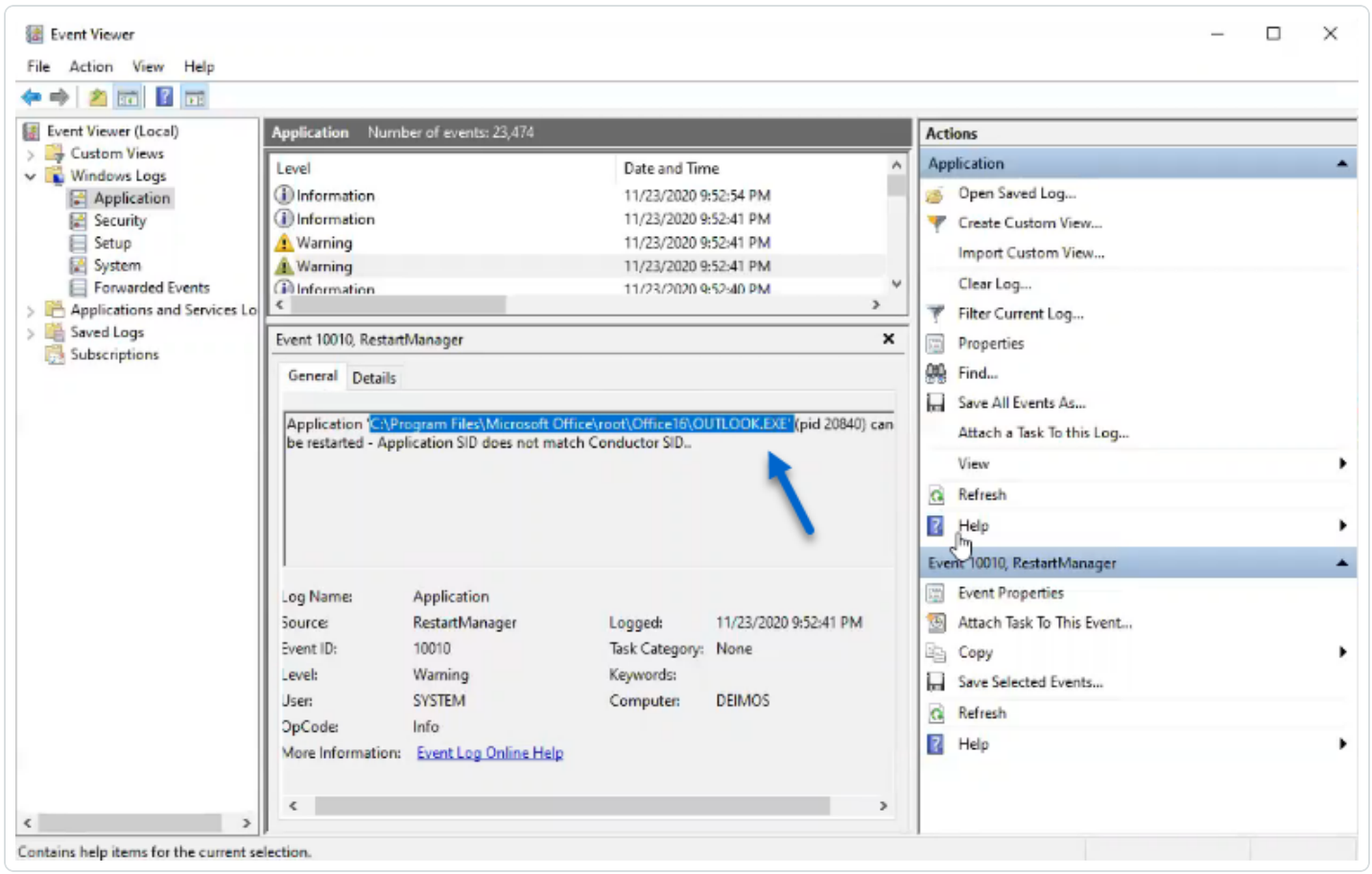
GPO 包含所有 DC 為收集相關資料而在本機執行的 PowerShell 指令碼，如下所示：

- 這些指令碼可在電腦的記憶體中設定事件監控程式和 Windows Management Instrumentation (WMI) 生產者/消費者。WMI 是一個 Windows 元件，可為您提供有關本機或遠端電腦系統狀態的資訊。
- 事件監控程式會接收事件記錄並定期進行緩衝，然後將它們排清到 SYSVOL 網路共用中儲存的一個檔案中。每個 DC 的內容都會被清除至一個儲存所收集事件的 SYSVOL 檔案中，然後複製到其他網域控制器。
- 當 DC 重新啟動時，WMI 消費者會再次註冊事件監控程式，從而使此機制持續存在。每次 DC 重新啟動時，生產者都會喚醒並通知消費者。因此，消費者會再次註冊事件監控程式。
- 此時，分散式檔案系統 (DFS) 會複製，並在網域控制器之間自動同步檔案。Tenable Identity Exposure 的平台會接聽傳入的 DFS 複製流量，並使用此資料收集事件、執行安全性分析，然後產生攻擊指標 (IoA) 警示。

## 本機資料擷取

Windows 事件記錄會記錄作業系統及其應用程式中發生的所有事件。名為 Windows 事件追蹤 (ETW) 的事件記錄服務依賴 Windows 中整合的元件架構。ETW 位於核心中，產生的資料儲存在 DC 上，不會由 AD 通訊協定複製。

Tenable Identity Exposure 只會使用 WMI API，以插入字串形式收集其從事件記錄中擷取的有用的 ETW 資料區段。Tenable Identity Exposure 會將這些插入字串寫入儲存在 SYSVOL 資料夾中的檔案，並透過 DFS 引擎複製這些字串。這樣，Tenable Identity Exposure 就可從 ETW 收集正確數量的安全性資料，以執行安全性分析並偵測攻擊。




## 攻擊指標 (IoA) 指令碼摘要

下表提供 Tenable Identity Exposure 指令碼部署的概覽。

| 步驟 | 說明 | 涉及的元件 | 技術動作 |
|---|---|---|---|
| 1 | 註冊 Tenable Identity Exposure 的 IoA 部署 | GPO 管理 | 建立 `Tenable.ad` (預設名稱) GPO 並將其連結至網域控制器 OU。 |
| 2 | 在 DC | DC 本 | 每個 DC 都會偵測要套用的新 GPO，具體取決於 AD 複製和 |

| | | | |
|---|---|---|---|
| | 上啟動 Tenable Identity Exposure 的 IoA 部署 | 機系統 | 群組原則重新整理間隔。 |
| 3 | 註冊事件監控程式和 WMI 生產者 | DC 本機系統 | 系統註冊並執行立即工作。此工作會執行 PowerShell 處理程序，以建立下列類別的執行個體：`ManagementEventWatcher` 和 `ActiveScriptEventConsumer`。Tenable Identity Exposure 會使用這些物件接收和儲存 ETW 訊息。 |
| 4 | 控制進階記錄原則狀態 | DC 本機系統 | 系統透過設定登錄機碼 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy` 來啟動進階記錄原則。 |
| 5 | 更新本機記錄原則 | DC 本機系統 | 根據要偵測的攻擊指標 (IoA)，Tenable Identity Exposure 會動態產生並啟動特定的記錄原則。此原則不會停用任何現有的記錄原則，而只會在必要時加以擴充。如果偵測到衝突，GPO 安裝指令碼會停止並顯示訊息「Tenable Identity Exposure 需要稽核原則 '...'，但目前的 AD 設定禁止使用。」 |
| 6 | 收集 ETW 訊息 | DC 本機系統 | Tenable Identity Exposure 會擷取相關的 ETW 訊息，然後定期緩衝，並將其儲存在與 Tenable Identity Exposure GPO (`...{GPO_GUID}\Machine\IOA<DC_name>`) 相關聯的 SYSVOL 資料夾中儲存的檔案 (每個 DC 一個檔案) 中。 |
| 7 | 將檔案複製到 Tenable Identity Exposure 平台 | Active Directory | AD 可使用 DFS 跨網域複製檔案。Tenable Identity Exposure 平台也會接收檔案。 |

| | | | |
|---|---|---|---|
| 8 | 覆寫這些檔案 | Active Directory | 每個 DC 都會自動且持續地將定期緩衝的事件寫入相同的檔案中。 |

## 另請參閱

- 安裝攻擊指標
- 技術變更和潛在影響

### 技術變更和潛在影響

攻擊指標 (IoA) 模組的安裝指令碼會建立一個 GPO，其可在受監控的 DC 上透通地套用下列變更：

- 預設名為「Tenable.ad」的新 GPO 預設連結至網域控制器的組織單位 (OU)。
- 修改登錄機碼以啟用 Microsoft 進階記錄原則。
- 啟用新的事件記錄原則，以強制網域控制器產生攻擊指標 (IoA) 所需的 ETW 資訊。

  > **注意**：事件記錄原則為強制執行，如此 ETW 引擎才能產生 Tenable Identity Exposure 所需的插入字串。此原則不會停用任何現有的記錄原則，而是會新增其中。如果發生衝突，部署指令碼會停止，並顯示錯誤訊息。

- 新增 Tenable Identity Exposure 服務帳戶的寫入權限，允許 GPO 資料夾中儲存的攻擊指標 (IoA) 設定「自動更新」。

## 限制和潛在影響

**攻擊指標** (IoA) 模組可造成下列限制：

- 攻擊指標 (IoA) 模組依賴 ETW 資料，並在 Microsoft 定義的限制內運作。
- 安裝的 GPO 必須在整個網域中複製，並且 GPO 重新整理間隔必須過去才能完成安裝過程。在此複製期間，可能會發生誤報和漏報，儘管 Tenable Identity Exposure 會透過不立即在攻擊指標引擎中啟動檢查來最大限度地減少這種影響。

- Tenable 使用 SYSVOL 檔案共用來從網域控制器擷取 ETW 資訊。SYSVOL 會複製到網域中的每個網域控制器，因此在 Active Directory 活動的高峰期間會出現複製活動顯著增加。
- 在網域控制器和 Tenable Identity Exposure 之間複製檔案也會消耗一些頻寬。Tenable Identity Exposure 會透過自動移除所收集的檔案來控制這些影響，並且會限制這些檔案的大小 (預設為最大 500 MB)。
- 分散式檔案系統 (DFS) 複製緩慢或損毀問題。如需詳細資訊，請參閱 DFS 複製問題緩解措施。

## 另請參閱

- Indicators of Attack and the Active Directory
- 安裝攻擊指標
- 攻擊指標安裝指令碼
- 對攻擊指標進行疑難排解

## 攻擊情境 (< v. 3.36)

**注意**：此攻擊指標設定更新功能不再適用於 Tenable Identity Exposure 3.36 以上版本。

**所需的使用者角色**：具有修改攻擊指標設定權限的組織使用者。

定義攻擊情境時，您可以選取 Tenable Identity Exposure 要在特定網域上監控的攻擊類型。

### 開始之前

如要修改攻擊情境，您必須擁有具有下列權限的使用者角色：

- 在**資料實體**中，以下項目的「讀取」存取權：
  - 所有攻擊指標
  - 所有網域

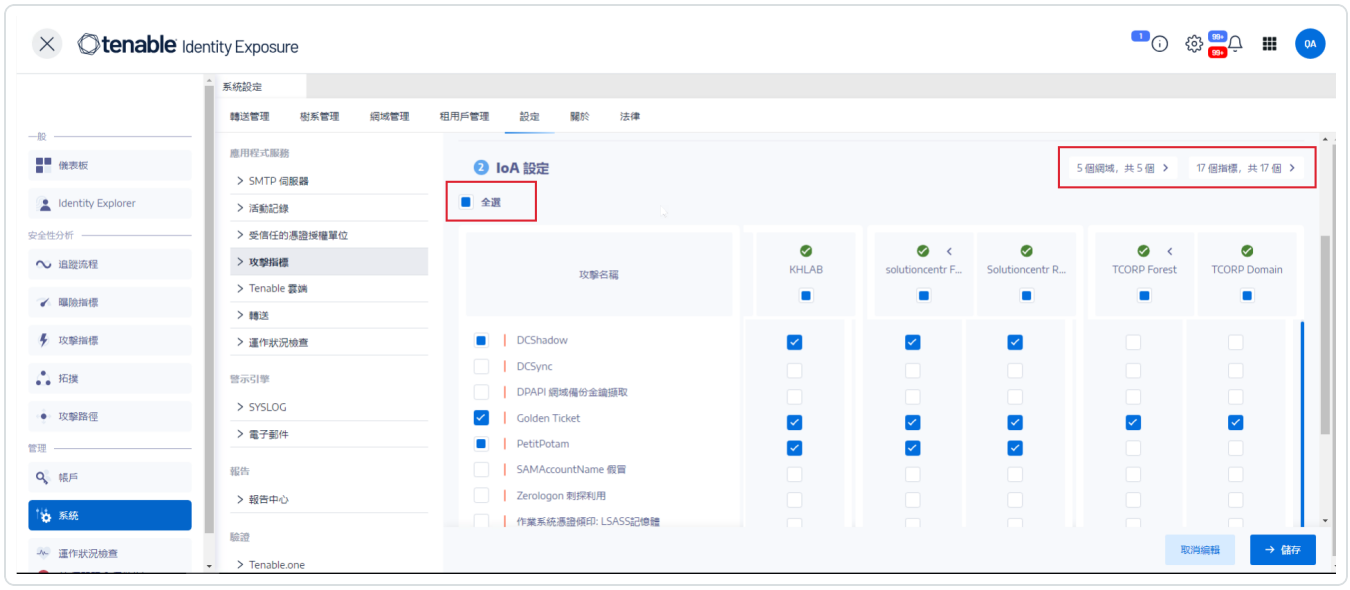
- 在**介面實體**中，以下項目的存取權：
  - 管理 > 系統 > 設定
  - 管理 > 系統 > 設定 > 應用程式服務 > 攻擊指標
  - 管理 > 系統 > 設定 > 應用程式服務 > 攻擊指標 > 下載安裝檔案

如需有關角色型權限的詳細資訊，請參閱 設定角色的權限。

**如要定義攻擊情境：**

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「設定」**>**「攻擊指標」**。

   **「攻擊情境的定義」**窗格會隨即開啟。




2. 在**「攻擊名稱」**下面選取要監控的攻擊。
3. 選取要監控所選攻擊的網域。
4. 或者，您可以執行下列任一項動作：
   - 按一下**「全選」**以監控所有網域的所有攻擊。
   - 按一下**「n/n 網域」**或**「n/n 指標」**，以篩選要監控特定攻擊的特定網域。

5. 按一下「**儲存**」。

   系統會顯示確認訊息，通知您 Tenable Identity Exposure 會在您儲存設定後清除每次攻擊的活動狀態。

6. 按一下「**確認**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新「攻擊指標」設定。

7. 按一下「**下載安裝檔案**」。

8. 如要使新的攻擊設定生效，請執行安裝檔案：

   a. 將下載的安裝檔案複製並貼到受監控網域中的 DC。

   b. 使用系統管理權限開啟 PowerShell 終端。

   c. 在 Tenable Identity Exposure 中，複製視窗底部攻擊指標區段下的命令。




   d. 在 PowerShell 視窗中，貼上命令以執行指令碼。

## 工作負載配額

**注意事項**：只有工作負載配額功能不再適用於 Tenable Identity Exposure 3.36 以上版本。

**所需的使用者角色**：具有工作負載配額編輯權限的組織使用者。

Tenable Identity Exposure 中的每個攻擊指標都有一個關聯的工作負載配額，此配額會考慮分析攻擊資料所需的資源。

Tenable Identity Exposure 會計算工作負載配額以限制同時執行的攻擊指標 (IoA) 數量，這會影響網域控制器上產生事件時的頻寬和 CPU 使用率。

修改工作負載配額限制後，請執行下列動作：

- 增加：在增加之後監控統計資料，以確保有適當的餘量。
- 減少：停用部分攻擊指標以維持在此配額之下，這會降低針對攻擊的安全範圍。

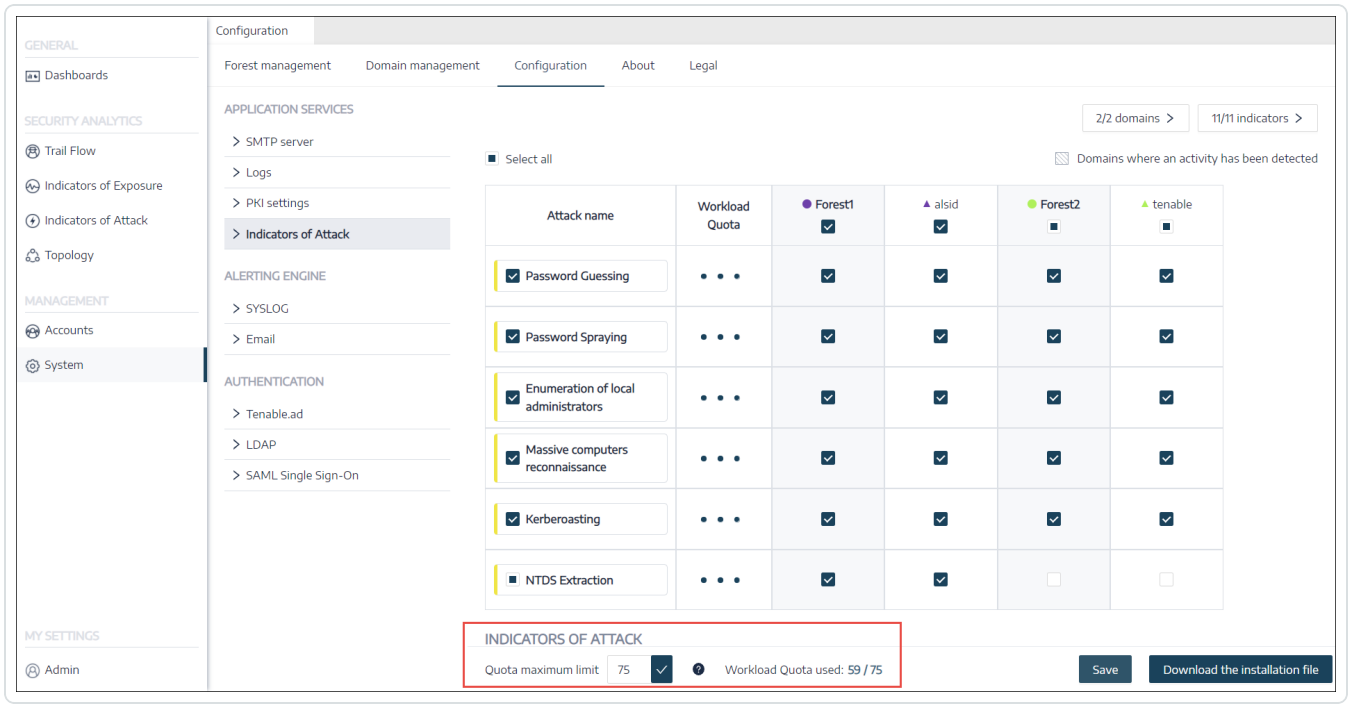
**如要修改工作負載配額限制：**

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」>「**攻擊指標**」。

   「**攻擊指標設定**」窗格會隨即開啟。

2. 為設定選取所需的攻擊指標。

3. 在「**攻擊指標**」下面的「**配額上限**」方塊中，輸入工作負載配額限制的值。




4. 按一下您輸入的值旁邊的核取記號。

   系統會顯示一則訊息，告知您此修改對 Tenable Identity Exposure 的影響。

   **注意**：如果您輸入的配額上限小於目前攻擊設定要求的值，則必須調整作用中攻擊指標的數量或提高限制。

5. 按一下「**確認**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新警示配額上限。

6. 按一下「**儲存**」。

   系統會顯示確認訊息，通知您 Tenable Identity Exposure 會在您儲存設定後清除每次攻擊的活動狀態。

7. 按一下「**確認**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新「攻擊指標」設定。

8. 按一下「**下載安裝檔案**」。

9. 如要使新的攻擊設定生效，請執行安裝檔案：

   a. 將下載的安裝檔案複製並貼到受監控網域中的 DC。

   b. 使用系統管理權限開啟 PowerShell 終端。

   c. 在 Tenable Identity Exposure 中，複製視窗底部攻擊指標區段下的命令。




   d. 在 PowerShell 視窗中，貼上命令以執行指令碼。

## 安裝 Microsoft Sysmon

有些 Tenable Identity Exposure 攻擊指標 (IoA) 需要 Microsoft 系統監視器 (Sysmon) 服務才能啟動。

Sysmon 會監視系統活動並將其記錄到 Windows 事件記錄中，以便在 Windows 事件追蹤 (ETW) 基礎架構中提供更多面向安全性的資訊。

因為安裝額外的 Windows 服務和驅動程式可能會影響代管 Active Directory 基礎架構的網域控制器的效能。Tenable 未自動部署 Microsoft Sysmon。您必須手動安裝或使用專用的 GPO。

下列攻擊指標 (IoA) 需要 Microsoft Sysmon。

| 名稱 | 原因 |
| --- | --- |
| OS 憑證傾印：LSASS 記憶體 | 偵測處理程序插入 |

**注意**：如果您選擇安裝 Sysmon，則必須在所有網域控制器上安裝，而不僅僅是在 PDC 上安裝，如此才能收集所有必要的事件。

**注意**：在完整部署 Tenable Identity Exposure 之前，請先測試您的 Sysmon 安裝是否有相容性問題。

**提示**：請務必在安裝後定期更新 Sysmon，以利用可解決潛在弱點的任何修補程式。與 Tenable Identity Exposure 相容的最舊版本是 Sysmon 12.0。

**如要安裝 Sysmon：**

1. 從 Microsoft 網站下載 Sysmon。
2. 在命令列介面中，執行以下命令以在本機電腦上安裝 Microsoft Sysmon：

   ```
   .\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
   ```

   **注意**：如需設定說明，請參閱註解的 Sysmon 設定檔。

3. 執行下列命令以新增登錄機碼，向 WMI 篩選器指示已安裝 Sysmon：

   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
   ```

**如要解除安裝 Sysmon：**

1. 開啟 PowerShell 終端機。
2. 瀏覽至包含 `Sysmon64.exe` 的資料夾。
3. 輸入下列命令：

```
PS C:\> .\Sysmon64.exe -u
```

如要刪除登錄機碼：

- 在命令列介面中，在所有執行 Sysmon 的電腦上輸入以下命令：

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

## Sysmon 設定檔

**注意：**
- 使用 Sysmon 設定檔之前，先將其複製並儲存為 XML 檔案。若發生錯誤，您也可以在此處直接下載設定檔。
- 執行前在檔案內容中取消封鎖此檔案。

```
<Sysmon schemaversion="4.40">
  <EventFiltering>

    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM
[FileCreateTime]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>
```

```
    <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessTerminate>
    </RuleGroup>

    <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DriverLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </ImageLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
    <RuleGroup name="" groupRelation="or">
      <CreateRemoteThread onmatch="include">
        <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      </CreateRemoteThread>
    </RuleGroup>

    <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RawAccessRead>
    </RuleGroup>

    <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <RuleGroup name="" groupRelation="or">
        <ProcessAccess onmatch="include">
          <!-- Detect Access to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1FFFFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1F1FFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1010</GrantedAccess>
          </Rule>
```

```
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x143A</GrantedAccess>
          </Rule>

          <!-- Detect process hollowing to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0800</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x800</GrantedAccess>
          </Rule>

          <!-- Detect process process injection to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0820</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x820</GrantedAccess>
          </Rule>
        </ProcessAccess>
    </RuleGroup>

    <!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
    <RuleGroup name="" groupRelation="or">
      <RegistryEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RegistryEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreateStreamHash onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateStreamHash>
    </RuleGroup>

    <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
    <RuleGroup name="" groupRelation="or">
```

```
      <PipeEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </PipeEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
    <RuleGroup name="" groupRelation="or">
      <WmiEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </WmiEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
    <RuleGroup name="" groupRelation="or">
      <DnsQuery onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DnsQuery>
    </RuleGroup>

    <!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileDelete>
    </RuleGroup>

  </EventFiltering>
</Sysmon>
```

## 解除安裝攻擊指標

**所需角色**：本機電腦上的管理員。

如要解除安裝攻擊指標 (IoA) 模組，請執行命令建立名為「Tenable Identity Exposure cleaning」的新群組原則物件 (GPO)。

根據預設，解除安裝處理程序會使用此新 GPO 清除先前安裝的 GPO 及其 SYSVOL 檔案、登錄設定、進階記錄原則和 WMI 篩選器。

**注意**：如果您變更了初始 GPO 的名稱，則必須將其傳遞給解除安裝程式，以便其知道要解除安裝哪個 GPO。如要傳遞新的 GPO 名稱，請使用參數 `-GpoDisplayName`。

**如要解除安裝攻擊指標 (IoA) 模組：**

1. 在命令列介面中，執行下列命令以解除安裝攻擊指標 (IoA) 模組：

```
Register-TenableIOA.ps1 -Uninstall
```

2. 在整個網域中複製這個新的 GPO。此指令碼會強制執行 4 小時的延遲以完成複製。
3. 執行下列命令刪除清理 GPO：

```
Remove-GPO -Guid <GUID> -Domain "<DOMAIN>"
```

4. 可選：執行下列命令以驗證此 GPO 是否已不存在：

```
(Get-ADDomainController -Filter *).Name | Foreach-Object {Get-GPO -Name "Tenable.ad cleaning"}
| Select Displayname| measure
```

您現在已經完全解除安裝攻擊指標 (IoA)。但是，如果其他 GPO 未定義其登錄項目，其可能會持續存在。以下是大規模電腦偵察攻擊指標 (IoA) 使用的登錄項目 (視您的特定攻擊指標 (IoA) 設定而定)：

- HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\AuditRecomingNTLMTraffic (值：2)
- HKLM\MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\RestrictSendingNTLMTraffic (value: 1)
- HKLM\MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\AuditNTLMInDomain (值：7)

若要移除這些登錄項目，請在您的所有網域控制器上執行下列 PowerShell 指令碼：

```
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name
"AuditReceivingNTLMTraffic"
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" -Name
"RestrictSendingNTLMTraffic"
Remove-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\Netlogon\Parameters" -Name
"AuditNTLMInDomain"
```

## 從 SYSVOL 手動移除過時的 GPO 資料夾

在某些情況下，重新安裝 IoA GPO 時，由於 Microsoft 功能的緣故，較舊的資料夾可能會保留在 SYSVOL 目錄中。如果目錄接聽程式將這些過時的資料夾識別為攻擊指標 (IoA) 資料夾，可能會導致偵測失敗。

執行下列程序，確保徹底移除過時的 IoA GPO 資料夾，避免在重新安裝期間發生偵測問題。

**若要移除過時的 IoA GPO 資料夾：**

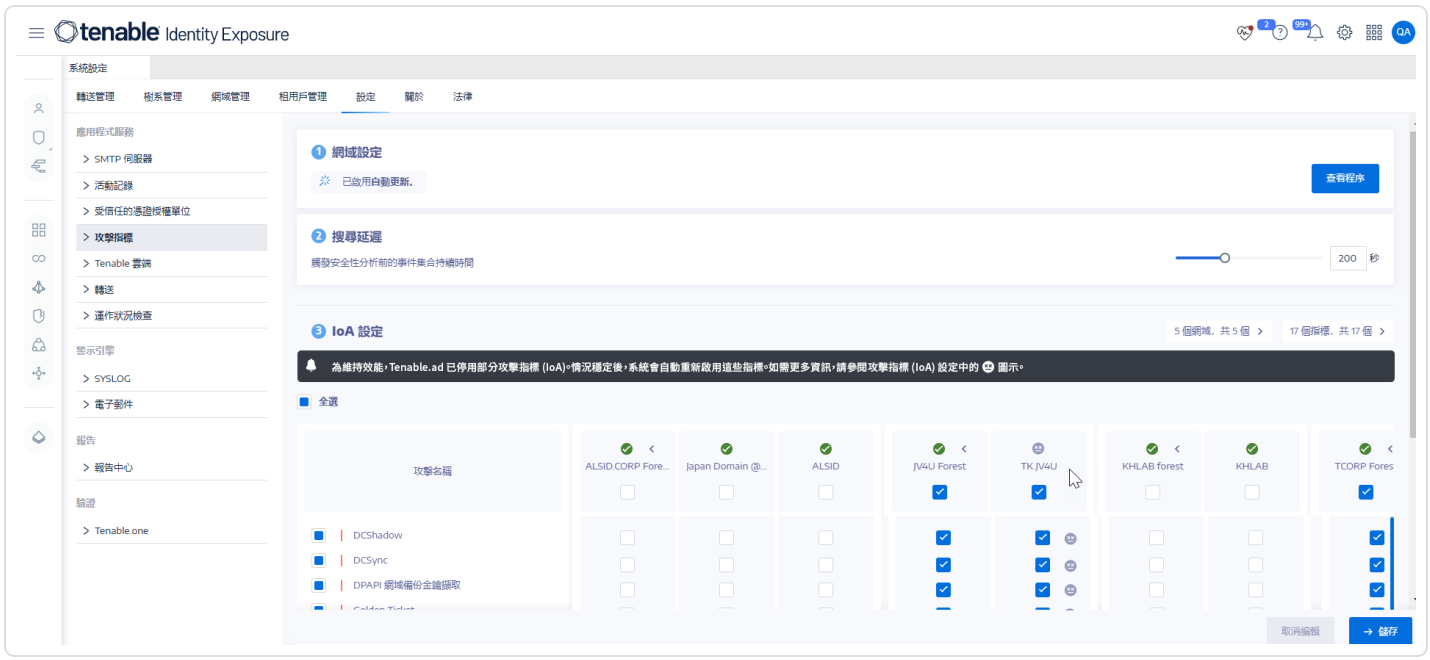
從 SYSVOL 目錄手動刪除任何與最新攻擊指標 (IoA) GPO GUID 不對應的過時攻擊指標 (IoA) 資料夾。確保僅保留最新的群組原則物件 (GPO)，可維持一致性並防止潛在的原則衝突。

如果您需要進一步的指導或遇到任何問題，請向支援團隊尋求協助。

## 停用的攻擊指標

偶爾，Tenable Identity Exposure 可能會暫時停用部分攻擊指標 (IoA) 以維持最佳效能。

停用時，攻擊指標 (IoA) 旁邊會顯示  圖示。




## 攻擊指標 (IoA) 狀態圖示

第一列圖示狀態

- 灰色圖示 :表示至少有一個攻擊指標 (IoA) 暫時遭到停用。
- 綠色勾號圖示 :表示所有已設定的攻擊指標 (IoA) 都已啟用。

其他列圖示狀態

- 灰色圖示 :顯示在停用攻擊指標 (IoA) 所在的特定網域旁邊。

## 工具提示資訊

將游標停留在狀態圖示上時，您會看到下列工具提示：

- 灰色圖示 :「一個或多個攻擊指標 (IoA) 暫時遭到停用」
- 綠色勾號圖示 :「所有已設定的攻擊指標 (IoA) 都已啟用」

- 其他列中的灰色圖示 :「攻擊指標 (IoA) 暫時遭到停用 (自 yyyy-mm-dd hh:mm 起) 以維持效能。」

### 警示訊息

當 Tenable Identity Exposure 停用攻擊指標 (IoA) 時，攻擊指標 (IoA) 表格上方會顯示一個警示訊息：

「為維持效能，Tenable Identity Exposure 已停用部分攻擊指標 (IoA)。一旦情況穩定下來，就會自動重新啟用這些攻擊指標 (IoA)。如需詳細資訊，請參閱攻擊指標 (IoA) 設定中的圖示。」

### 能見度規則

網域和樹系層級皆可看到已停用狀態。

- 如果您取消勾選具有停用圖示的網域，且沒有其他任何網域具有此圖示，則連結網域的圖示會消失。
- 如果連結到某個樹系的所有網域都不再有停用圖示，則連結樹系的圖示會消失。

### 自動重新啟用

一旦系統效能穩定後，Tenable Identity Exposure 會自動重新啟用已停用的攻擊指標 (IoA)。不需要任何手動介入。

攻擊指標 (IoA) 的暫時停用是一項內建功能，專為維持系統效能而設計。Tenable Identity Exposure 會動態調整作用中的攻擊指標 (IoA)，以確保最佳運作而不影響安全性監控功能。

### 回應灰色的「已停用」圖示

當您看到灰色的「已停用」圖示時：

1. 等待情況解決：在大多數情況下，您只需要等待即可。一旦系統效能穩定後，Tenable Identity Exposure 會自動重新啟用攻擊指標 (IoA)。
2. 針對內部部署：

- 如果您發現此情況頻繁發生，即使遵循資源對照表的建議，仍可能需要將更多資源新增至託管 Cygni 服務的電腦。
- 請考慮視需要升級 CPU、RAM 或磁碟空間，以提升整體系統效能。

3. 監控頻率：追蹤您看到此圖示的頻率。如果此圖示定期出現，可能表示您目前的資源一直處於過載狀態。
4. 請檢閱您的攻擊指標 (IoA) 設定：等待重新啟用時，您可能需要檢閱目前的攻擊指標 (IoA) 設定，以確保其符合您的安全需求和可用資源。

## 對攻擊指標進行疑難排解

- 進階稽核原則設定優先順序
- 防毒軟體偵測
- Tenable Identity Exposure 記錄檔
- 事件記錄接聽程式驗證
- DFS 複製問題緩解措施
- Windows 事件記錄保留
- 攻擊指標警示中的「未知」
- 操作攻擊指標
- 攻擊指標偵測延遲

### 防毒軟體偵測

Tenable 和 Microsoft 不建議在網域控制器上安裝防毒軟體、端點保護平台 (EPP) 或端點偵測及回應 (EDR) 軟體 (或任何其他具有中央管理主控台的工具)。如果您選擇這麼做，您的防毒軟體/EPP/EDR 可能會偵測甚至封鎖或刪除網域控制器上收集攻擊指標 (IoA) 事件所需的項目。

Tenable Identity Exposure 的攻擊指標部署指令碼不包含惡意程式碼，甚至沒有經過模糊處理。但是，鑑於其使用 PowerShell 和 WMI，再加上這種實作的無代理程式特性，偶爾偵測到是正常情況。

如果您遇到下列問題：

- 安裝期間的錯誤訊息
- 偵測中的誤報或漏報

如要對安裝指令碼防毒偵測進行疑難排解：

1. 檢閱您的防毒軟體/EPP/EDR 的安全性記錄，以檢查是否有任何 Tenable Identity Exposure 元件遭偵測、封鎖或刪除。防毒軟體/EPP/EDR 可影響下列元件：
    - 套用至網域控制器的 Tenable Identity Exposure GPO 中的 `ScheduledTasks.xml` 檔案。
    - 網域控制器上啟動 PowerShell.exe 的 Tenable Identity Exposure 排程任務。
    - 網域控制器上啟動的 Tenable Identity Exposure`Register-TenableADEventsListener.exe` 處理程序。
2. 在您的工具中為受影響的元件新增安全性例外狀況。
    - 具體而言，Symantec Endpoint Protection 可能在攻擊指標 (IoA) 安裝期間引發 `CL.Downloader!gen27` 偵測。您可以將此特定的已知風險新增至例外狀況原則。
    - 設定工作排程器後，執行 PowerShell 以啟動 `Register-TenableADEventsListener.exe` 處理程序。防毒軟體/EPP/EDR 軟體可能會阻礙此 PowerShell 指令碼，導致攻擊指標無法正確執行。密切追蹤此處理程序，並確保該程序只在所有受監控的網域控制器中執行一次。

    防毒軟體/EPP/EDR 的檔案路徑排除範例：

```
Register-TenableADEventsListener.exe process
 "\\"domain"\sysvol\"domain"\Policies\{"GUID_Tenable.ad}\Machine\IOA\Register-
TenableADEventsListener.exe"
```

```
ScheduledTasks.xml file
    C:\Users\<User Name>\AppData\Local\Temp\4\Tenable.ad\
{GUID}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    C:\Windows\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    \\[DOMAIN.FQDN]\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
```

進階稽核原則設定優先順序

Tenable Identity Exposure 為啟用必要的事件記錄而建立的群組原則物件 (GPO) 連結至已啟用「強制執行」模式的組織單位 (OU) 網域控制器。

這為 GPO 提供了高優先順序，但在更高層級 (例如網域或據點) 設定的強制 GPO 優先於它。

如果定義「進階稽核原則設定」設定的高優先等級 GPO 與 Tenable Identity Exposure 的需求相衝突，將以該 GPO 為準，並且 Tenable Identity Exposure 會遺漏攻擊偵測所需的事件。

由於 Windows 會合併 GPO 定義的「進階稽核原則設定」設定，因此不同的 GPO 可定義不同的設定。

但是，在每個設定層級，它僅使用優先順序較高的 GPO 定義值。例如，Tenable Identity Exposure 需要「稽核憑證驗證」設定的「成功」與「失敗」值。但是，如果高優先等級 GPO 僅為「稽核憑證驗證」定義了「成功」，則 Windows 將只收集「成功」事件，而 Tenable Identity Exposure 會遺漏所需的「失敗」事件。

**如要檢查 GPO 優先順序**

1. 在命令列介面中，在網域控制器上執行下列命令。

   它會在考量所有 GPO 和優先順序後，輸出有效的「進階稽核原則設定」。

   ```
   auditpol.exe /get /category:*
   ```

2. 比較輸出結果與 Tenable Identity Exposure 進階稽核原則要求。針對 Tenable Identity Exposure 要求的每個設定，檢查有效的原則是否也涵蓋此設定。

   - 如果有效原則更詳盡，例如 Tenable Identity Exposure 需要「成功」或「失敗」，而設定為「成功與失敗」，則這不是問題。
   - 如果有效原則不足，則表示優先順序較高的 GPO 定義了有衝突的設定。

**如要修復 GPO 優先順序：**

1. 在定義「進階稽核原則設定」的「強制」模式下，搜尋連結至更高層級 (網域或據點) 的 GPO。
2. 在命令列介面中，在網域控制器上執行下列命令，以準確顯示優先的 GPO：

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. 修改 GPO 中對應的「進階稽核原則設定」設定，以符合 Tenable Identity Exposure 的最低要求。例如：

    - 如果 Tenable Identity Exposure 要求「成功」，而優先順序較高的 GPO 定義了「失敗」，則將設定修改為「成功與失敗」。
    - 如果 Tenable Identity Exposure 要求「成功與失敗」，而優先順序較高的 GPO 定義了「成功」，則將設定修改為「成功與失敗」。

4. 修改設定後，您可以等待套用更新後的 GPO，也可以使用 `gpupdate` 命令強制執行。
5. 重複程序「如要檢查 GPO 優先順序」以檢查新的有效原則。

### 事件記錄接聽程式驗證

攻擊指標安裝指令碼可在電腦的記憶體中設定事件觀察程式和 Windows Management Instrumentation (WMI) 生產者/消費者。WMI 是一個 Windows 元件，可為您提供有關本機或遠端電腦系統狀態的資訊。

如要檢查 WMI 註冊是否正確：

- 在 PowerShell 中執行下列命令：

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter
= ""__EventFilter.name='AlsidForAD-Launcher'"""
```

- 如果至少有一個消費者，您會獲得以下類型的輸出：

```
> Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter
"Filter = ""__EventFilter.name='AlsidForAD-Launcher'"""


__GENUS                 : 2
__CLASS                 : __FilterToConsumerBinding
__SUPERCLASS            : __IndicationRelated
__DYNASTY               : __SystemClass
__RELPATH               : __
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name=\"AlsidForAD-Launcher\"",F
                          ilter="__EventFilter.Name=\"AlsidForAD-Launcher\""
__PROPERTY_COUNT        : 7
__DERIVATION            : {__IndicationRelated, __SystemClass}
__SERVER                : DC-999
__NAMESPACE             : ROOT\subscription
__PATH                  : \\DC-999\ROOT\subscription:__
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name
                          =\"AlsidForAD-Launcher\"",Filter="__EventFilter.Name=\"AlsidForAD-
```

```
Launcher\""
Consumer                : ActiveScriptEventConsumer.Name="AlsidForAD-Launcher"
CreatorSID              : {1, 1, 0, 0...}
DeliverSynchronously    : False
DeliveryQoS             :
Filter                  : __EventFilter.Name="AlsidForAD-Launcher"
MaintainSecurityContext : False
SlowDownProviders       : False
PSComputerName          : DC-999
```

- 如果沒有已註冊的 WMI 消費者，則此命令不返回任何內容。
- 這是在 WMI 的 DC 上執行處理程序的先決條件。

**如要擷取事件記錄接聽程式 (適用於 3.29 (含) 以上版本):**

- 在 PowerShell 中執行下列命令：

```
gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}
```

- 有效結果範例：

```
PS C:\IOAInstall> gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}

ProcessId Name                                HandleCount WorkingSetSize VirtualSize

5748      Register-TenableADEventsListener.exe 152         4096000        4384534528
```

**如要擷取 WMI 處理程序 (適用於 3.19 (含) 以下版本):**

- 在 PowerShell 中執行下列命令：

```
gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

- 有效結果範例：

```
> gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

```
ProcessId Name           HandleCount WorkingSetSize VirtualSize
--------- ----           ----------- -------------- -----------
952       powershell.exe 502         26513408       2199678185472
```

## Tenable Identity Exposure 記錄檔

如果您在驗證 GPO 和 WMI 消費者後仍未看到「攻擊指標」警示，可以檢閱 Tenable Identity Exposure 的內部記錄檔。

### Ceti 記錄

- 檢查 CETI 記錄中是否有下列錯誤訊息：

```
[2022-02-22 22:23:27:570 UTC WARNING] Some domain controllers are not generating IOA
events: 'CORP-DC'. {SourceContext="DirectoryEventToCetiAdObjectMessageMapper",
DirectoryId=2, Dns="corp.bank.com", Host="10.10.20.10", Source=SYSVOL, Version="3.11.5"}
```

- 如果您看到此訊息，請驗證 GPO 設定和 WMI 消費者是否在上述錯誤訊息中所列的網域控制器 (DC) 上執行。

### 稽核設定

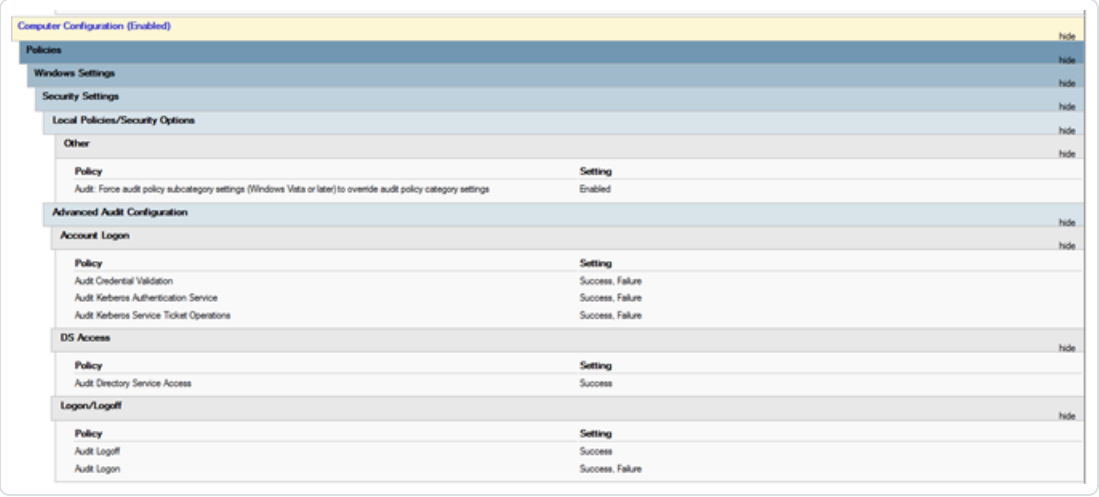
- 如果您看到與下列類似的錯誤：「Tenable Identity Exposure 需要稽核原則...」，請檢查您現有的 GPO，確保您沒有將所需的稽核原則設定為「無稽核」。

```
2022-02-10 16:54:21 [2022-02-10 21:54:21:845 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                    _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
2022-02-10 16:54:07 [2022-02-10 21:54:07:849 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                    _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
2022-02-10 16:54:07 [2022-02-10 21:54:07:773 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                    _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
2022-02-10 16:54:07 this could prevent IOA engine from working. {SourceContext="FileProcessor", DirectoryId=
2022-02-10 16:54:07 Tenable.ad requires the audit policy Audit Detailed'
2022-02-10 16:54:07 [2022-02-10 21:54:07:662 UTC ERROR] Detected transcript '\\alsid.corp\sysvol\alsid.corp\
                    _ce599bf8-57cc-4dd9-9fb9-f06a263c3b6a.log' with errors: 'Tenable.ad requires the audit p
```

- 如果您收到指出「RSOP...」的錯誤：




- 檢查稽核原則並檢視 SYSVOL 資料夾中的記錄檔，瞭解您在安裝期間是否遇到過任何問題。




## Cygni 記錄

Cygni 會記錄攻擊，並列出 Tenable Identity Exposure 為產生警示而呼叫的特定 .gz 檔案。

## I-DCSync

```
2022-03-15 11:39:31
[2022-03-15 15:39:30:759 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCSync' and Event '110052' {SourceContext="AttackEngine", CodeName="I-DCSync", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

## I-GoldenTicket

```
2022-03-15 11:40:31
[2022-03-15 15:40:31:490 UTC INFORMATION] Anomaly 'Logon' has been raised for Indicator 'I-
GoldenTicket' and Event '110061' {SourceContext="AttackEngine", CodeName="I-GoldenTicket",
ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

## I-ProcessInjectionLsass

```
022-03-15 12:47:09
[2022-03-15 16:47:09:811 UTC INFORMATION] Anomaly 'ProcessAccess' has been raised for Indicator 'I-
ProcessInjectionLsass' and Event '115948' {SourceContext="AttackEngine", CodeName="I-
ProcessInjectionLsass", ProfileId=1, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

## I-DCShadow

```
2022-03-15 11:30:30
[2022-03-15 15:30:30:657 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCShadow' and Event '109948' {SourceContext="AttackEngine", CodeName="I-DCShadow", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

## I-BruteForce

```
2022-03-15 08:02:11
[2022-03-15 12:02:11:231 UTC INFORMATION] Anomaly 'An account failed to log on' has been raised for
Indicator 'I-BruteForce' and Event '109082' {SourceContext="AttackEngine", CodeName="I-BruteForce",
ProfileId=6, AdObjectId="3:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{765297AD-3BAF-4820-B7F5-
AD90DEEE941E}\\Machine\\IOA\\dc-vm-10.0.17763-8_.gz", Event.Id=0, Version="3.16.0"}
```

## I-PasswordSpraying

```
2022-03-15 12:39:43
[2022-03-15 16:39:43:793 UTC INFORMATION] Anomaly 'An account failed to log on.' has been raised for
Indicator 'I-PasswordSpraying' and Event '115067' {SourceContext="AttackEngine", CodeName="I-
PasswordSpraying", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

## I-PetitPotam

```
2022-03-15 12:43:02
[2022-03-15 16:43:02:737 UTC INFORMATION] Anomaly 'PetitPotamEFSError' has been raised for Indicator
'I-PetitPotam' and Event '115844' {SourceContext="AttackEngine", CodeName="I-PetitPotam",
ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

### I-ReconAdminsEnum

```
022-03-15 12:55:31
[2022-03-15 16:55:31:638 UTC INFORMATION] Anomaly 'LocalAdmin enumeration (BloodHound/SharpHound).
Version 2016+' has been raised for Indicator 'I-ReconAdminsEnum' and Event '116085'
{SourceContext="AttackEngine", CodeName="I-ReconAdminsEnum", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

### I-Kerberoasting

```
022-03-15 12:51:30
[2022-03-15 16:51:30:236 UTC INFORMATION] Anomaly 'Kerberos TGS requested on honey account' has been
raised for Indicator 'I-Kerberoasting' and Event '116013' {SourceContext="AttackEngine", CodeName="I-
Kerberoasting", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-
7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

### I-NtdsExtraction

```
2022-03-15 12:03:51
[2022-03-15 16:03:50:949 UTC INFORMATION] Anomaly 'Shadow copy created on 2012 and above' has been
raised for Indicator 'I-NtdsExtraction' and Event '111168' {SourceContext="AttackEngine",
CodeName="I-NtdsExtraction", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

### Cephei 記錄

下列記錄項目驗證 Cephei 是否正在寫入攻擊。金鑰值是指定攻擊類型的 **attackTypeID**，可用來與 Cygni 項目相關聯：

### I-DCSync attackTypeID:1

```
2022-03-15 11:39:52
2022-03-15T15:39:52.037023041Z stdout F [2022-03-15 15:39:52:035 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 32.16 ms : Request Body=
```

```
{"timestamp":"1647358722449","directoryId":5,"profileId":4,"attackTypeId":1,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

## I-GoldenTicket attackTypeID:2

```
2022-03-15 11:40:52
2022-03-15T15:40:52.084931986Z stdout F [2022-03-15 15:40:52:084 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.6607 ms : Request Body=
{"timestamp":"1647358773608","directoryId":5,"profileId":4,"attackTypeId":2,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

## I-ProcessInjectionLsass attackTypeID:3

```
2022-03-15 12:47:52
2022-03-15T16:47:52.29927328Z stdout F [2022-03-15 16:47:52:298 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 35.7532 ms : Request Body=
{"timestamp":"1647362812784","directoryId":5,"profileId":1,"attackTypeId":3,"count":2}
{SourceContext="Equuleus", Version="3.16.0"}
```

## I-DCShadow attackTypeID:4

```
2022-03-15 11:30:52
2022-03-15T15:30:51.949399295Z stdout F [2022-03-15 15:30:51:944 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.2605 ms : Request Body=
{"timestamp":"1647358182800","directoryId":5,"profileId":3,"attackTypeId":4,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

## I-BruteForce attackTypeID:5

```
2022-03-15 08:02:54
2022-03-15T12:02:54.698814039Z stdout F [2022-03-15 12:02:54:698 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 30.7623 ms : Request Body=
{"timestamp":"1647345728023","directoryId":3,"profileId":6,"attackTypeId":5,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

## I-PasswordSpraying attackTypeID:6

```
2022-03-15 12:39:52
2022-03-15T16:39:52.187309945Z stdout F [2022-03-15 16:39:52:186 UTC INFORMATION] [Equuleus] POST
```

```
http://equuleus:3004/attacks/write responded 204 in 21.9422 ms : Request Body=
{"timestamp":"1647362356837","directoryId":5,"profileId":4,"attackTypeId":6,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

### I-PetitPotam attackTypeID:7

```
022-03-15 12:43:52
2022-03-15T16:43:52.226125918Z stdout F [2022-03-15 16:43:52:223 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 15.8402 ms : Request Body=
{"timestamp":"1647362570534","directoryId":5,"profileId":1,"attackTypeId":7,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

### I-ReconAdminsEnum attackTypeID:8

```
2022-03-15 12:55:52
2022-03-15T16:55:52.399889635Z stdout F [2022-03-15 16:55:52:399 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 40.6632 ms : Request Body=
{"timestamp":"1647363305295","directoryId":5,"profileId":4,"attackTypeId":8,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

### I-Kerberoasting attackTypeID:10

```
2022-03-15 12:51:52
2022-03-15T16:51:52.352432644Z stdout F [2022-03-15 16:51:52:351 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.0547 ms : Request Body=
{"timestamp":"1647363026345","directoryId":5,"profileId":4,"attackTypeId":10,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

### I-NtdsExtraction attackTypeID:11

```
022-03-15 12:03:52
2022-03-15T16:03:52.137547488Z stdout F [2022-03-15 16:03:52:137 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 13.0304 ms : Request Body=
{"timestamp":"1647360224606","directoryId":5,"profileId":4,"attackTypeId":11,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

### Electra 記錄

您應該看到以下項目：

[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-alert (namespace=electra)

```
[2022-03-15T14:04:39.151Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-
alert (namespace=electra)
[2022-03-15T14:04:39.168Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Sending ws message to listeners.
alertIoA (namespace=electra)
```

**Eridanis 記錄**

您應該看到以下項目：

```
022-03-15T14:04:39.150Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2010 200
122 - 7ms (namespace=hapi)
[2022-03-15T14:04:39.165Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: notifyAttackAndAttackAlertCreation
success { attackId: 2011 } (namespace=eridanis)
[2022-03-15T14:04:39.170Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2011 200
122 - 6ms (namespace=hapi)
```

## DFS 複製問題緩解措施

攻擊指標部署指令碼中新增的參數 `-EventLogsFileWriteFrequency X` 可協助解決您可能會遇到的分散式檔案系統 (DFS) 複製緩慢或損毀問題。

此參數為選用，Tenable 建議您僅在遇到 DFS 複製問題或在部署攻擊指標 (IoA) 指令碼後發現這些問題時使用。在正常情況下，此參數會維持其預設值，您不需要在執行指令碼時將其包含在命令列中。

### 何時修改參數

`-EventLogsFileWriteFrequency X` 參數的值 [X] 是 Tenable Identity Exposure 接聽程式在非 PDCe 網域控制器 (DC) 上產生事件記錄檔的頻率。Tenable Identity Exposure 接聽程式所使用的預設建議值為 15 秒。不過，自訂值不適用於 PDCe DC，且會維持其預設的 15 秒間隔，以確保攻擊偵測功能可完全運作。Tenable 建議您僅在基礎架構面臨或容易受到 DFS 複製問題影響時，才使用此參數，並將其值從預設的 15 秒增加到 300 秒 (5 分鐘)。

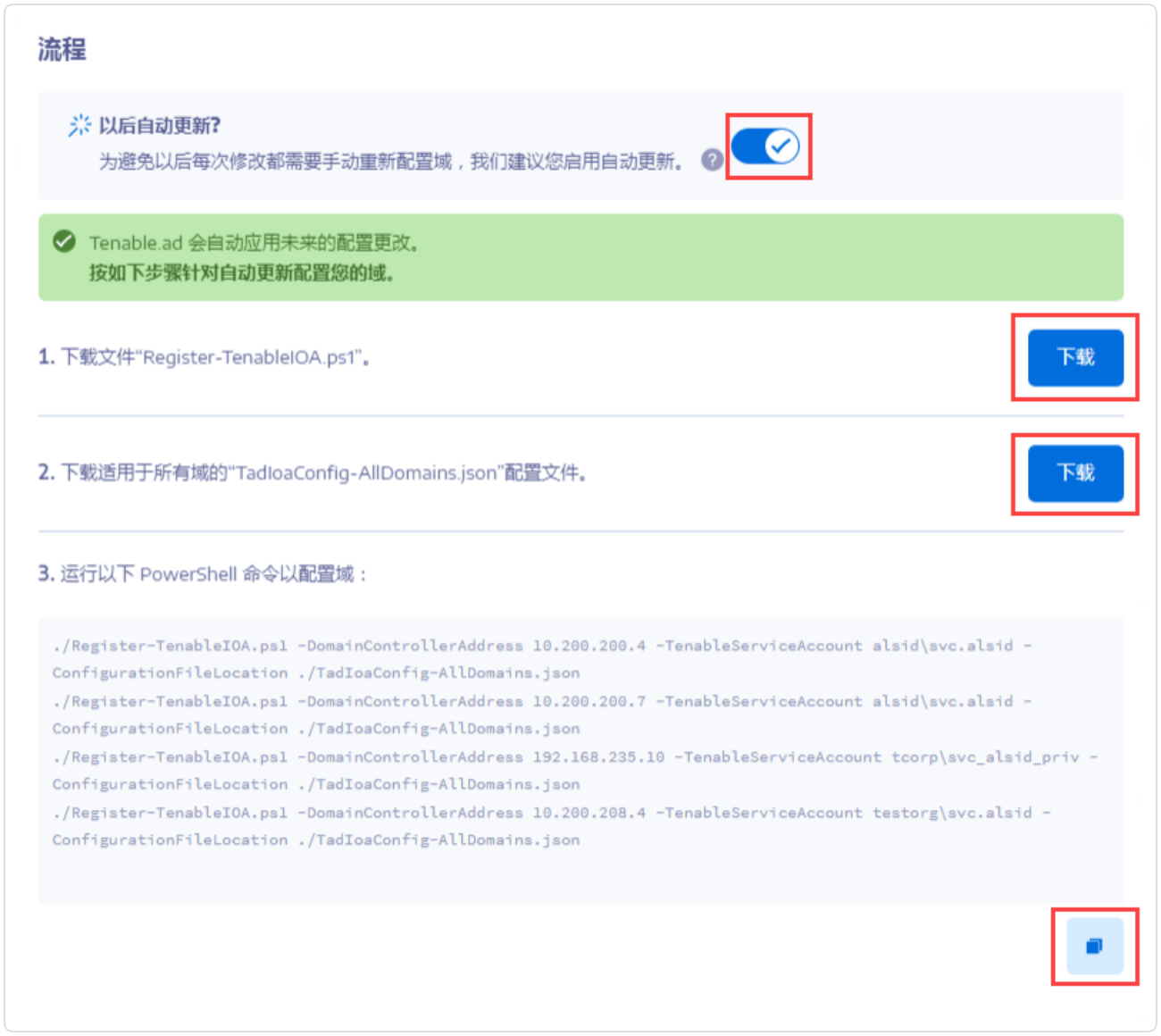
### 建議

請注意，增加事件記錄檔寫入頻率會降低檔案產生頻率，進而增加攻擊偵測的延遲時間 (例如，如果每 30 秒產生一次檔案，而不是非 PDCe DC 上預設的 15 秒)。此外，增加延遲時間可

將產生的事件記錄檔大小擴大到 技術變更和潛在影響 中定義的設定限制內。因此，請僅將此參數作為緩解策略使用，而非適當調查 DFS 複製問題的替代方法。

如要套用參數：

1. 依照程序中所述，針對攻擊指標 (IoA) 設定網域。如需詳細資訊，請參閱 安裝攻擊指標。




2. 使用系統管理權限開啟 PowerShell 終端。
3. 執行指令碼，以針對攻擊指標 (IoA) 設定您的網域控制器，並附加 `-EventLogsFileWriteFrequency X` 參數，其中 [X] 是您要針對事件記錄檔頻率設定的頻率。

## Windows 事件記錄保留

雖然 Tenable Identity Exposure 會盡力處理 Windows 事件記錄，以支援攻擊指標功能中的安全性分析，但仍有技術限制，例如服務執行機器上的可用記憶體。

**預設全域保留期** 為 5 分鐘。不過特定 Windows 事件記錄會延長保留期，以減輕安全性引擎可能遇到的相關性問題：

- `SYSMON 5722` 和 `5723`：保留 6 小時。
- `Microsoft-Windows-Security-Auditing/4624`：此記錄的保留期是動態的，因為此記錄在攻擊指標中大量用於偵測和關聯。系統會根據記憶體使用情形調整保留，以平衡事件處理與系統資源：
  - **第一個小時**：安全性分析服務會套用 5 分鐘的預設保留期。
  - **在第一個小時後**，系統會評估剩餘記憶體並調整保留期，如下所示：
    - 如果可用記憶體**超過 50%**：1 天。
    - 若可用記憶體為 **35%-50%**：6 小時。
    - 若可用記憶體為 **20%-35%**：1 小時。
    - 若可用記憶體為 **10%-20%**：10 分鐘。
    - 若可用記憶體**低於 10%**：預設 5 分鐘。

此動態方法可確保系統可有效管理傳入事件，同時維持足夠的記憶體進行安全性分析。

## 攻擊指標警示中的「未知」

在某些情況下，您可能會在攻擊指標 (IoA) 警示中遇到「未知」項目，如下圖所示：




這些項目通常是因為下列主要情境所引起：

1. **Active Directory (AD) 之外的外部 DNS**

   如果您的組織使用 Active Directory (AD) 網域之外的 DNS 伺服器，請務必注意該產品不支援非 AD DNS 環境。這表示透過不屬於 AD 的外部 DNS 伺服器路由特定 DNS 查詢或要求時，Tenable Identity Exposure 無法識別它們，進而導致攻擊指標 (IoA) 警示清單中出現「未知」項目。

   在這些情況下預期會出現這類「未知」，並不表示 Tenable Identity Exposure 內有任何功能失常或錯誤。這是因為與 Active Directory 整合的本質所導致，其需要在 AD 環境中管理 DNS 記錄，才能完整掌握並追蹤。

   **解決方案**

   - 若要將這些「未知」項目減到最少，請確認您的 DNS 基礎架構已針對身分識別曝險監控至關重要的網域和資源完全整合到 AD 中。
   - 如果 DNS 查詢必須在 AD 之外執行，請瞭解這些「未知」項目將會繼續出現，因為 Tenable Identity Exposure 無法解決這些問題。

2. **Tenable Identity Exposure 帳戶的權限不足**

攻擊指標 (IoA) 警示中出現「未知」項目的另一個原因可能是 Tenable Identity Exposure 使用的帳戶缺少讀取 DNS 項目的足夠權限。Tenable Identity Exposure 服務需要讀取權限，才能正確存取和分析 Active Directory 中的 DNS 記錄。

### 解決方案

若要解決此問題，請確認 Tenable Identity Exposure 使用的帳戶對 AD 內必要的 DNS 項目具有讀取存取權。具體而言，此帳戶必須具有查詢 DNS 伺服器和存取其執行識別身分曝險分析所需記錄的權限。

如果 Tenable Identity Exposure 帳戶沒有適當的讀取權限，您可以使用下列程序授予這些權限。

> 提示：在指令碼中，您只需要變更 Tenable Identity Exposure 使用的帳戶的名稱即可。讀取權限包含在下列屬性中：
>
> - `distinguishedName`
> - `dnsRecord (包含 IP)`
> - `name`
> - `ntSecurityDescriptor`
> - `objectCategory`
> - `objectClass`
> - `objectGUID`

您有以下**兩個**使用 PowerShell 指令碼的選項：

a. 在 Active Directory 管理員中，對容器 (dnsZone) 設定讀取權限，並將其傳播到所有子 dnsNode (建議的解決方案，若適用)：

```
Import-Module ActiveDirectory

$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }

# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-
00c04fb96050')

$dnsZones = Get-ADObject -LDAPFilter "(objectClass=dnsZone)" -SearchBase
$dnsZonePartition

ForEach ($dnsZone in $dnsZones) {
    $acl = Get-Acl -Path "AD:\$dnsZone"

    ForEach ($guid in $guids) {
      $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [guid]$guid,
        [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
        [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
        )

      $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [System.DirectoryServices.ActiveDirectorySecurityInheritance]::All,
        [guid]'e0fa1e8c-9b45-11d0-afdd-00c04fd930c9' # dnsZone GUID
        )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsZone" -AclObject $acl
}
```

b. 對所有現有 dnsNode 物件設定讀取權限 (在影響所有子 dnsNode 的 dnsZone 上)：

```
Import-Module ActiveDirectory

$identity = New-Object System.Security.Principal.NTAccount('EXAMPLE\user2') # Service
account used by TIE for collect/listening
```

```
$dnsZonePartition = (Get-ADRootDSE).namingContexts | Where-Object { $_ -match
"DomainDnsZones" }

# dnsRecord attribute GUID
# and Public-Information property set GUID
$guids = @('e0fa1e69-9b45-11d0-afdd-00c04fd930c9', 'e48d0154-bcf8-11d1-8702-
00c04fb96050')

$dnsNodes = Get-ADObject -LDAPFilter "(objectClass=dnsNode)" -SearchBase
$dnsZonePartition

ForEach ($dnsNode in $dnsNodes) {
    $acl = Get-Acl -Path "AD:\$dnsNode"

    ForEach ($guid in $guids) {
      $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadProperty,
        [System.Security.AccessControl.AccessControlType]::Allow,
        [guid]$guid
        )

      $acl.AddAccessRule($ace)
    }

    # ntSecurityDescriptor
    $ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule(
        $identity,
        [System.DirectoryServices.ActiveDirectoryRights]::ReadControl,
        [System.Security.AccessControl.AccessControlType]::Allow
        )

    $acl.AddAccessRule($ace)
    Set-Acl -Path "AD:\$dnsNode" -AclObject $acl
}
```

3. **支援的 DNS 磁碟分割**

   Tenable Identity Exposure 不會執行主動式 DNS 解析。而是依賴從 `ForestDnsZones` 和 `DomainDnsZones` 磁碟分割擷取的 DNS 項目。如果您使用自訂 DNS 磁碟分割，Tenable Identity Exposure 將不會對其進行抓取或儲存其 DNS 項目。

## 操作攻擊指標

確保攻擊指標處理程序正常運作對於準確偵測和回應而言至關重要。本節提供的逐步指示可以幫助您驗證攻擊指標 (IoA) 元件是否可正常運作、故障排除常見問題，以及有效率地解決問題。請按照下列步驟確認所有情況是否如預期般運作。

- 確保攻擊指標 (IoA) 監控可在您的網域控制器上正常運作。
  - 檢查網域連線：透過驗證設定來確保網域連線運作正常。如需詳細資訊，請參閱網域。
- 驗證 SYSVOL 中的 IoA GPO 資料夾：
  - 檢查 SYSVOL 目錄中的 IoA GPO 資料夾，確認每個網域控制器都產生最新的 `.gz` 檔案。
  - 如果任何網域控制器未產生此 `.gz` 檔案，請繼續執行後續步驟。
- 確認攻擊指標 (IoA) 事件接聽程式處理程序正在執行：
  - 驗證 `Register-TenableADEventsListener.exe` 處理程序是否正在執行。
  - 在最新版本中，除了 `Register-TenableADEventsListener.exe` 以外，此處理程序在工作管理員中也列為「Tenable - 攻擊指標 (IoA) 事件接聽程式」。

    如需詳細資訊，請參閱事件記錄接聽程式驗證。
- 如果處理程序未執行：
  - 確保網域控制器上的任何 EDR/防毒軟體未封鎖 `Register-TenableADEventsListener.exe` 處理程序。

    如需詳細資訊，請參閱防毒軟體偵測。
- 手動啟動處理程序：
  - 編輯工作排程器中的相關工作 (`TenableADTask_*`)，然後按一下「**確定**」以重新啟動處理程序。
- 如果問題仍然存在，則向上呈報：如果上述步驟未能解決問題，請向 Tenable 提出支援個案。可能有基本問題使得 `Register-TenableADEventsListener.exe` 處理程序無法執行。

## 攻擊指標偵測延遲

Tenable Identity Exposure 偵測到遺失或延遲事件 (例如因 GZ 檔案複製時間過長或產生大量資料而造成的事件) 時，會自動調整分析視窗。

雖然其通常會在 5 分鐘的時間範圍中分析資料，但可將時間範圍延長至一小時，以將延遲到達的事件納入考量。此調整可將攻擊偵測延遲至攻擊發生後一小時內。

## 驗證

有數種方法可驗證 Tenable Identity Exposure 使用者：

- 使用 Tenable Identity Exposure 帳戶進行驗證
- 使用 LDAP 驗證
- 使用 SAML 驗證

## 使用 Tenable One 驗證

**所需的授權**：Tenable One

**注意**：使用 Tenable One 授權，您可以管理 Tenable Vulnerability Management 中的所有驗證設定。如需詳細資訊，請參閱*《Tenable Vulnerability Management 使用者指南》*中的「存取控制」章節。

如要使用 Tenable One 設定驗證：

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」。

   「設定」窗格會隨即顯示。

2. 在「**驗證**」區段下，按一下「**Tenable One**」。
3. 在「**預設設定檔**」下拉式方塊中，選取使用者的設定檔。
4. 在「**預設角色**」方塊中，選取使用者的角色。

   **提示**：Tenable One 中經驗證的使用者如果之前未曾連線至 Tenable Identity Exposure，則登入 Tenable Identity Exposure 時會自動擁有一個帳戶。預設設定檔和預設角色會依預設套用至此使用者。**例外狀況**：在 Tenable Vulnerability Management 中具有「管理員」角色的使用者在 Tenable Identity Exposure 中也具有「全域管理員」角色。

5. 按一下「**儲存**」。

## 使用 Tenable Identity Exposure 帳戶進行驗證

最簡單的驗證方法是使用 Tenable Identity Exposure 帳戶，此帳戶需要使用者名稱和密碼。

此驗證方法提供預設鎖定原則，這是一種安全性控制機制，用於緩解針對驗證機制的暴力密碼破解攻擊。如果登入嘗試失敗次數過多，它會鎖定使用者的帳戶。帳戶被鎖定後，使用者無權存取 Tenable Identity Exposure API。

如要使用 Tenable Identity Exposure 帳戶設定驗證：

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」。

   「設定」窗格會隨即顯示。

2. 在「**驗證**」區段下，按一下「**Tenable Identity Exposure**」。

3. 在「**預設設定檔**」下拉式方塊中，選取使用者的設定檔。

4. 在「**預設角色**」方塊中，選取使用者的角色。

5. 設定鎖定原則設定：

| 設定 | 說明 | 預設值 |
| --- | --- | --- |
| **啟用** | • **啟用**：Tenable Identity Exposure 會在登入嘗試失敗達到設定的次數後阻止此帳戶。<br>• **停用**：Tenable Identity Exposure不會在登入嘗試失敗後阻止此帳戶。 | 啟用 |
| **鎖定持續時間** | Tenable Identity Exposure 鎖定帳戶阻止任何登入嘗試的持續時間。在這段時間過後，Tenable Identity Exposure 會自動解除鎖定帳戶，允許使用者再次嘗試登入。<br>如要設定鎖定持續時間：<br>1. 按一下滑桿以設定鎖定持續時間。<br>2. 如果您不想在設定的持續時間之後自動解除鎖定帳戶，請選取「**無限**」。<br>**注意**：如果「全域管理員」群組內的所有帳戶都被鎖定，Tenable Identity Exposure 會在 10 秒後解除鎖定預設系統管理帳戶。 | 300 秒 |
| **鎖定前的嘗試次數** | Tenable Identity Exposure 鎖定帳戶前的登入嘗試失敗次數。 | 3 |
| **挽回期** | Tenable Identity Exposure 計算登入嘗試失敗次數的時間間隔。在登入嘗試失敗達指定次數後，Tenable Identity Exposure 會鎖定此帳戶。<br>如要設定挽回期：<br>1. 按一下滑桿以設定時間間隔。<br>2. 如果您不想設定一個時間間隔，用來計算 Tenable Identity Exposure 鎖定帳戶之前的登入嘗試失敗次數，請選取「無限」。 | 900 秒 |

6. 按一下「**儲存**」。

**如要停用鎖定原則：**

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」。

   「設定」窗格會隨即顯示。

2. 按一下「**啟用**」切換開關以關閉鎖定原則。

**注意**：如果停用鎖定原則，則鎖定的使用者帳戶可嘗試重新連線。

**如要檢視鎖定帳戶清單：**

- 在 Tenable Identity Exposure 中，前往「**帳戶**」>「**使用者帳戶管理**」。

  在使用者清單中，Tenable Identity Exposure 會顯示帶有紅色掛鎖圖示的鎖定帳戶。Tenable Identity Exposure 會向帳戶遭鎖定的使用者顯示下列訊息：「因驗證嘗試失敗次數過多，您的帳戶已被鎖定。您必須聯絡管理員。」

**如要解除鎖定帳戶：**

您必須擁有編輯使用者的權限，才能解除鎖定帳戶。

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**使用者帳戶管理**」。

   「使用者帳戶管理」窗格會隨即開啟。

2. 在使用者清單中，找到被鎖定的帳戶。

3. 按一下鉛筆圖示以編輯鎖定的使用者帳戶。

   使用者資訊窗格會隨即顯示。

4. 按一下「**移除鎖定**」按鈕。

**如要向使用者角色授予鎖定原則設定權限：**

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**角色管理**」。

   「**角色管理**」窗格會隨即顯示。

2. 按一下角色名稱旁邊的鉛筆圖示以編輯角色。

   「**編輯角色**」窗格會隨即顯示。

3. 按一下「**系統設定實體**」索引標籤。

4. 在「**權限管理**」區段下，選取「**帳戶鎖定原則**」核取方塊。

5. 按一下切換到「**未授權**」或「**已授權**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新使用者權限。

   > **注意**：對於僅具有讀取權限的使用者，Tenable Identity Exposure 會在此窗格中停用鎖定原則設定。

## 使用 LDAP 驗證

Tenable Identity Exposure 允許您使用輕量型目錄存取通訊協定 (LDAP) 驗證使用者。

如要啟用 LDAP 驗證，您必須具備下列條件：

- 預先設定的服務帳戶，其中包含存取 Active Directory 的使用者和密碼。
- 預先設定的 Active Directory 群組。

設定 LDAP 驗證之後，登入頁面的索引標籤中會出現 LDAP 選項。

**如要設定 LDAP 驗證：**

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」。

   「設定」窗格會隨即顯示。

2. 在「**驗證**」區段下，按一下「**LDAP**」。

3. 按一下「**啟用 LDAP 驗證** 切換為「啟用」。

   LDAP 資訊表會隨即顯示。

4. 提供以下資訊：

   - 在「**LDAP 伺服器位址**」方塊中，輸入以 `ldap://` 開頭並以網域名稱和連接埠號碼結尾的 LDAP 伺服器的 IP 位址。

**注意**：如果您使用 LDAPS 伺服器，請輸入以 `ldaps://` 開頭並以網域名稱和連接埠號碼結尾的伺服器位址。利用此程序以完成 LDAPS 的設定。

- 在**「用於查詢 LDAP 伺服器的服務帳戶」**方塊中，輸入您用來存取 LDAP 伺服器的辨別名稱 (DN)、SamAccountName 或 UserPrincipalName。
- 在**「服務帳戶密碼」**方塊中，輸入此服務帳戶的密碼。
- 在**「LDAP 搜尋基礎」**方塊中，輸入 Tenable Identity Exposure 在搜尋嘗試連線的使用者時使用的 LDAP 目錄，以 `DC=` 或 `OU=` 開頭。這可以是 root 目錄或特定的組織單位。
- 在**「LDAP 搜尋篩選器」**方塊中，輸入 Tenable Identity Exposure 用於篩選用戶的屬性。Active Directory 中的標準驗證屬性為 `sAMAccountname={{login}}`，其中 `login` 的值是使用者在驗證期間提供的值。

5. 針對**「啟用 SASL 繫結」**，請執行下列其中一項動作：
   - 如果您使用 `SamAccountName` 作為服務帳戶，請按一下**「啟用 SASL 繫結」**切換為**啟用**。
   - 如果您為服務帳戶使用可辨別名稱或 `UserPrincipalName`，請將**「啟用 SASL 繫結」**保持**停用**狀態。

     **Windows Server 2025 的重要注意事項**：

     **Windows Server 2025 中設有限制，只有在啟用 LDAPS 時，停用 SASL 繫結的 LDAP 設定才會有效。**

     如要確保功能正常運作：

     - 如果為 Tenable 服務帳戶使用 **UPN** 或 **DN**，您可以在 LDAP 設定中**啟用 SASL 繫結**，該功能會正常運作。
     - 如果想**讓 SASL 繫結保持停用狀態**，必須**啟用 LDAPS**，LDAP 才能正常運作。

6. 在**「預設設定檔和角色」**區段下，按一下**「新增 LDAP 群組」**以指定允許進行驗證的群組。

   LDAP 群組資訊表會隨即顯示。

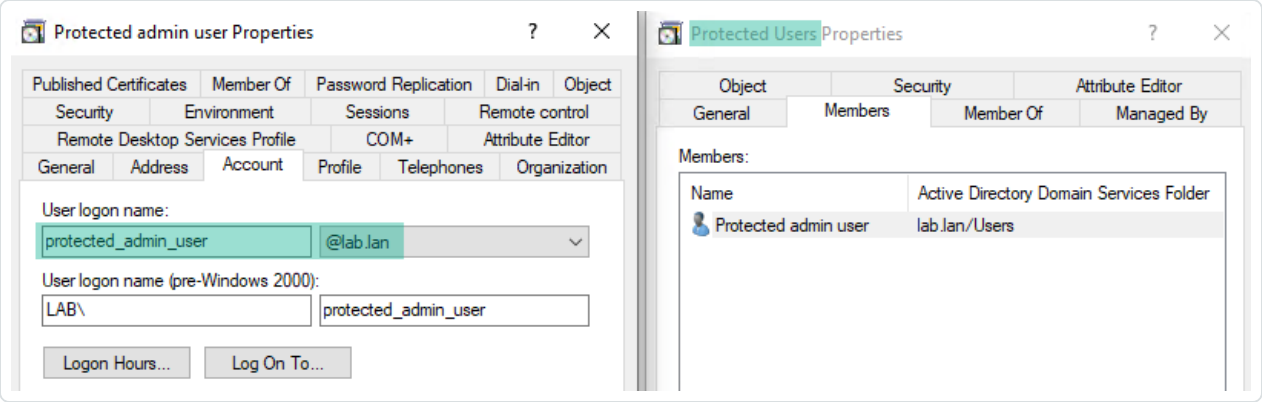
- 在「**LDAP 群組名稱**」方塊中，輸入群組的辨別名稱 (例如：`CN=TAD_User,OU=Groups,DC=Tenable,DC=ad`)
- 在「**預設設定檔**」下拉式方塊中，選取允許群組的設定檔。
- 在「**預設角色**」方塊中，選取允許群組的角色。

7. 如有必要，按一下 **+** 以便加入允許的新群組。
8. 按一下「**儲存**」。

**如要在 AD 中以「受保護的使用者」群組成員身分使用 LDAP：**

由於受保護使用者群組成員無法使用 NTLM，因此您必須確保將 LDAP 驗證正確設定為使用 Kerberos。

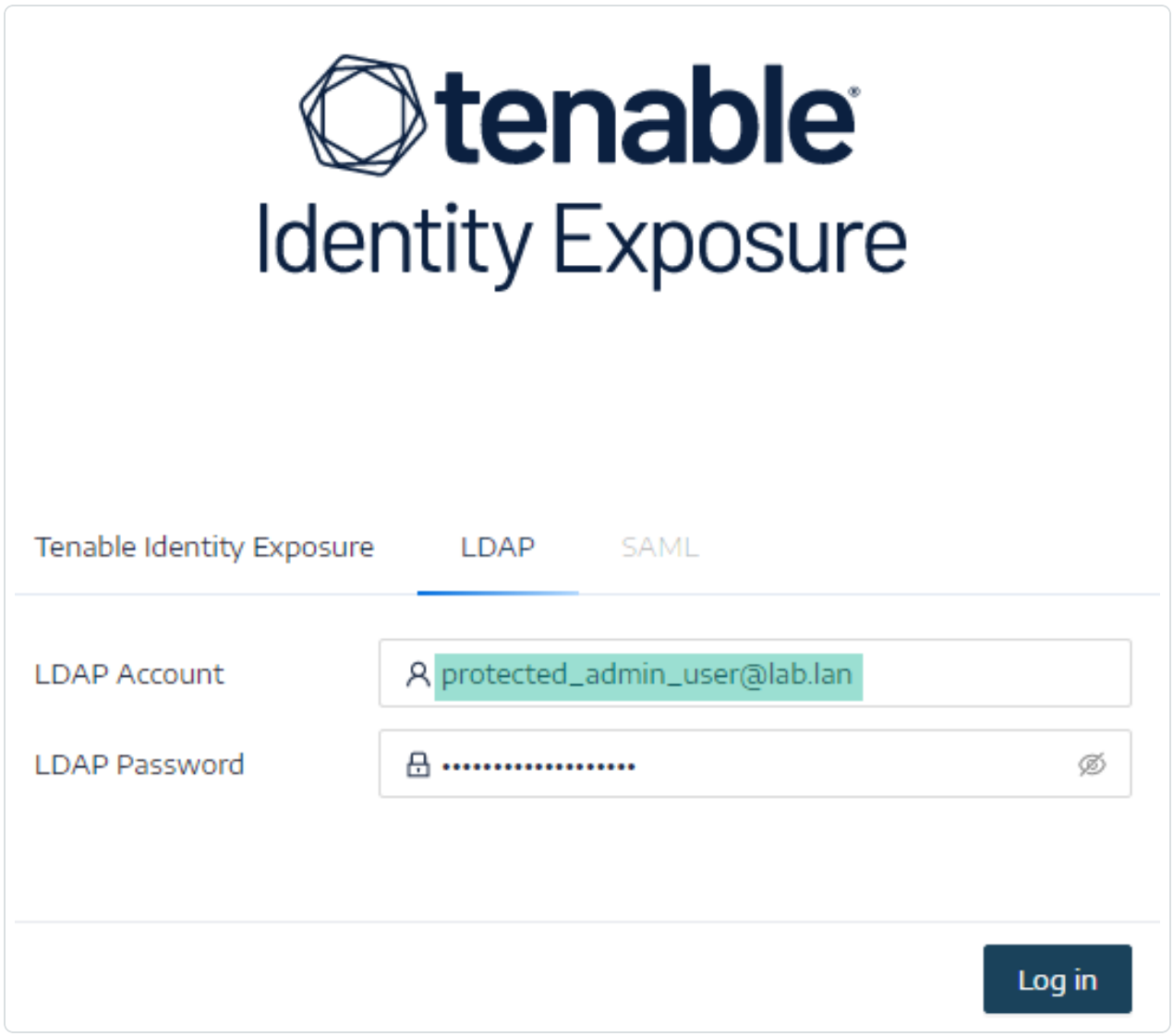
1. **先決條件**：您必須已在 Microsoft Active Directory 中設定使用者主體名稱 (UPN)，這是與電子郵件地址類似的使用者名稱格式。它通常採用 username@domain.com 的格式，其中「username」是使用者的帳戶名稱，「domain.com」則是帳戶所在的網域。




2. 使用您的憑證登入 Tenable Identity Exposure。
3. 設定下列 LDAP 選項：
   - 針對 LDAP 伺服器位址使用 FQDN (以確保安全轉送可解析位址)。
   - 使用 UPN 格式的服務帳戶 (例如 login@domain.com)。
   - 將 LDAP 搜尋篩選器設為「`(userprincipalname={{login}})`」
   - 將 SASL 繫結設為「開啟」。




4. 請使用 LDAP 憑證，並以採用使用者主體名稱語法的「受保護的使用者」群組的成員身分登入 Tenable Identity Exposure。




### 如要為 LDAPS 新增自訂的受信任憑證授權單位 (CA) 憑證：

1. 在 Tenable Identity Exposure 中，按一下「**系統**」。
2. 按一下「**設定**」索引標籤以顯示設定窗格。
3. 在「**應用程式服務**」區段下，按一下「**受信任的憑證授權單位**」。
4. 在「**其他 CA 憑證**」方塊中，貼上貴公司 PEM 編碼的受信任 CA 憑證，以便 Tenable Identity Exposure 使用。
5. 按一下「**儲存**」。

### LDAP 驗證問題

完成並儲存設定之後，登入頁面上應會顯示 LDAP 選項。若要確認設定有效，您必須能夠使用 LDAP 帳戶登入。

### 錯誤訊息

此時可能會出現兩個錯誤訊息：

- 驗證過程中發生錯誤。請再試一次。
    - 在此情況下，設定發生問題。
    - 仔細檢查完整的設定。
    - 檢查主控 Tenable Identity Exposure 的伺服器是否能夠連絡 LDAP 伺服器。
    - 檢查用於搜尋的帳戶是否可在 LDAP 伺服器上進行連結。
    - 如需更多詳細資訊，請檢查應用程式記錄。
- 您的登入帳號或密碼錯誤。
    - 確認 CAPS LOCK 未開啟，然後重新輸入您測試過的登入名稱和密碼。
    - 這可能是群組篩選器、搜尋篩選器或搜尋基準欄位的問題所導致。
    - 嘗試暫時移除任何群組篩選。如需更多詳細資訊，請檢查應用程式記錄。

如需有關安全性設定檔和角色的詳細資訊，請參閱：

- 安全性設定檔
- 使用者角色

## 使用 SAML 驗證

您可以設定 SAML 驗證，以便 Tenable Identity Exposure 使用者在登入 Tenable Identity Exposure 時可以使用身分識別提供者啟動的單一登入 (SSO)。

### 開始之前

- 請參閱 Tenable SAML 設定快速參考指南，取得設定 SAML 以搭配使用 Tenable Identity Exposure 的逐步指南。
- 檢查您的身分識別提供者 (IDP) 是否符合下列條件：

- 僅限 SAML v2。
- 已啟用「宣告加密」。
- Tenable Identity Exposure 用來在 Tenable Identity Exposure 入口網站中授予存取權的 IDP 群組。
- SAML 伺服器的 URL。
- 由受信任的憑證授權單位 (CA) 簽署的 PEM 編碼格式 SAML 伺服器憑證以 `-----BEGIN CERTIFICATE -----` 開頭，以 `-----END CERTIFICATE -----` 結尾。

如要設定 SAML 驗證：

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」。

   「設定」窗格會隨即顯示。

2. 在「**驗證**」區段下，按一下「**SAML 單一登入**」。
3. 按一下「**啟用 SAML 驗證**」切換開關。

   SAML 資訊表會隨即顯示。




4. 提供以下資訊：

   - 在「**SAML 伺服器的 URL**」方塊中，輸入 Tenable Identity Exposure 必須連線的 IDP SAML 伺服器完整 URL。
   - 在「**受信任的憑證授權單位**」方塊中，貼上簽署 SAML 伺服器憑證的 CA。

5. 在「**Tenable Identity Exposure 憑證**」方塊中，按一下「**產生並下載**」。這會產生新的自行簽署憑證、更新資料庫中的 SAML 設定，並傳回新憑證以供下載。

   **注意**：當您按一下此按鈕時，它會中斷您的 SAML 設定，這是因為 Tenable Identity Exposure 要求 IDP 立即使用最近產生的憑證進行驗證，而此時 IDP 仍在使用先前的憑證 (如果存在)。產生新的 Tenable Identity Exposure 憑證後，您必須將 IDP 重新設定為使用新憑證。

6. 按一下「**自動啟用新使用者帳戶**」切換開關，以便在首次 SAML 登入後啟用新使用者帳戶。
7. 在「**Tenable Identity Exposure 端點**」下方提供以下資訊：
   - Tenable Identity Exposure 服務提供者的 URL
   - 宣告 Tenable Identity Exposure 服務提供者的端點
8. 在「**預設設定檔和角色**」區段下，按一下「**新增 SAML 群組**」以指定允許進行驗證的群組。

   SAML 群組資訊表會隨即顯示。
9. 提供以下資訊：
   - 在「**SAML 群組名稱**」方塊中，輸入 SAML 伺服器中顯示的允許群組名稱。
   - 在「**預設設定檔**」下拉式方塊中，選取允許群組的設定檔。
   - 在「**預設角色**」方塊中，選取允許群組的角色。
10. 如有必要，按一下 **+** 以便加入允許的新群組。
11. 按一下「**儲存**」。

    設定 SAML 驗證之後，登入頁面的索引標籤中會出現 SAML 選項。

如需有關安全性設定檔和角色的詳細資訊，請參閱：

- 安全性設定檔
- 使用者角色

## 使用者帳戶

**使用者帳戶管理**頁面提供新增、編輯、刪除或檢視 Tenable Identity Exposure 使用者帳戶詳細資料的功能。

使用者屬於兩個類別：

- 全域管理員:包含所有特權的管理員角色。
- 使用者:僅擁有商業資料唯讀權限的簡單使用者角色

**注意事項**

如果您擁有**獨立的 Tenable Identity Exposure 授權**,則可選擇透過您設定將資料傳送至 Tenable Platform。選擇這麼做會啟用 Tenable Identity Exposure 的 Identity 360 和 Security Engine 功能。

為促進與 Tenable 平台的通訊並追蹤使用者動作,Tenable Identity Exposure 會在 Tenable 平台中自動建立下列物件,這些物件會顯示在 Tenable Vulnerability Management 容器設定中:

- 以「TIE - 自動產生的使用者 - {random_string}」模式命名的群組
- 名為「TIE - 自動產生 - 可檢視所有資產 - {random_string}」的權限套用至群組「TIE - 自動產生的使用者 - {random_string}」。其允許使用者查看 Tenable Identity Exposure 匯出至 Tenable 平台的資產。
- 針對每個 Tenable Identity Exposure 使用者,屬於群組「TIE - 自動產生的使用者 - {random_string}」的使用者會依循模式「tie-{username}-{random_string}」命名。此使用者擁有強式隨機密碼,您**不**應在 Tenable Vulnerability Management 容器中使用該密碼進行驗證。它在 Tenable Vulnerability Management 容器中具有基本唯讀權限。

系統管理員可檢視這些物件,但**不得加以變更**,因為變更可中斷 Indentity 360 和 Security Engine 功能。

**如要建立使用者:**

1. 在 Tenable Identity Exposure 中,按一下**「帳戶」**>**「使用者帳戶管理」**。

   **「使用者帳戶管理」**窗格會隨即開啟。

2. 按一下右側的**「建立使用者」**按鈕。

   **「建立使用者」**窗格會隨即顯示。

3. 在**「主要資訊」**區段下面輸入下列使用者資訊:
   - 名字
   - 姓氏
   - 電子郵件地址

- 密碼：需要至少 12 個字元，密碼中至少有 1 個小寫字母、1 個大寫字母、1 個數字和 1 個特殊字元
- 密碼確認
- 部門
- 簡介

4. 按一下切換開關**「允許驗證」**以啟用使用者。
5. 在**「角色管理」**區段下，選取要套用至使用者的角色。
6. 按一下**「建立」**。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已建立具有所選角色的使用者。

**如要編輯使用者：**

1. 在 Tenable Identity Exposure 中，按一下**「帳戶」**>**「使用者帳戶管理」**。

   **「使用者帳戶管理」**窗格會隨即開啟。

2. 在使用者清單中，將游標停留在顯示使用者名稱的行上，然後按一下此行末尾的 圖示。

   **「編輯使用者」**窗格會隨即顯示。

3. 在**「主要資訊」**區段下，視需要輸入下列使用者資訊：
   - 名字
   - 姓氏
   - 電子郵件地址
   - 密碼：至少需要 8 個字元
   - 密碼確認
   - 部門
   - 簡介

4. 在「**角色管理**」區段下，視需要修改使用者的角色。
5. 按一下「**編輯**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新具有所選角色的使用者。

**如要停用使用者：**

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**使用者帳戶管理**」。

   「**使用者帳戶管理**」窗格會隨即開啟。
2. 在使用者清單中，將游標停留在顯示使用者名稱的行上，然後按一下此行末尾的 圖示。

   「**編輯使用者**」窗格會隨即顯示。
3. 按一下切換開關「**允許驗證**」以停用使用者。
4. 按一下「**編輯**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新使用者。

**如要刪除使用者：**

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**使用者帳戶管理**」。

   「**使用者帳戶管理**」窗格會隨即開啟。
2. 在使用者清單中，將游標停留在顯示待刪除使用者名稱的行上，然後按一下此行末尾的 圖示。

   系統會顯示一則訊息，要求您確認刪除。
3. 按一下「**刪除**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已刪除使用者。

## 安全性設定檔

**所需的使用者角色**：具有適當權限的管理員或組織使用者。

設定檔允許您建立和自訂影響 Active Directory 的風險檢視。

每個設定檔顯示為具有此設定檔的使用者設定的曝險和攻擊場景。例如，IT 管理員的資料分析一般檢視可能與安全團隊的檢視不同，後者顯示 AD 基礎架構所面臨的所有風險的全面檢視。

套用安全性設定檔允許不同類型的使用者從不同的報告角度審查資料分析，正如此安全性設定檔的指標所定義的那樣。

「安全性設定檔管理」窗格允許不同類型的使用者從不同的報告角度來檢閱安全性分析。您可以透過安全性設定檔自訂曝險指標和攻擊指標的行為表現。

**注意：**Tenable Identity Exposure 提供名稱為「Tenable」的預設安全性設定檔。**您無法修改或刪除 Tenable 設定檔**，但可以將它作為範本使用，以根據需要透過調整的設定建立其他安全性設定檔。

**如要建立新的安全性設定檔：**

1. 在 Tenable Identity Exposure 中，按一下**「帳戶」**>**「安全性設定檔管理」**。

   **「安全性設定檔管理」**窗格會隨即顯示。

2. 按一下右側的**「建立設定檔」**按鈕。

   **「建立設定檔」**窗格會隨即顯示。

3. 從「動作」下拉式方塊中，您可以執行以下任一項動作：

   - **建立新的設定檔**。
   - **複製**現有的安全性設定檔，就能以此為基礎建立新的設定檔 (例如「Tenable」設定檔)。

4. 在**「新設定檔的名稱」**方塊中輸入新設定檔的名稱。

   **注意：**Tenable Identity Exposure 僅接受英數字元和底線。

5. 按一下右下角的**「建立」**按鈕。

   系統會顯示一則訊息，指出 Tenable Identity Exposure 已建立設定檔。**「設定檔設定」**窗格會隨即顯示。

**如要刪除安全性設定檔：**

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**安全性設定檔管理**」。

   「**安全性設定檔管理**」窗格會隨即顯示。

2. 在安全性設定檔清單中，將游標停留在您要刪除的安全性設定檔上，然後按一下此行末尾的 圖示。

   系統會顯示一則訊息，要求您確認刪除。

3. 按一下「**刪除**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已刪除設定檔。

## 下一步做什麼

如要完成設定檔的建立，請參閱 自訂指標 瞭解詳細資訊。

如需詳細資訊，請參閱：

- 自訂指標
- 縮小指標自訂範圍

## 自訂指標

**所需的使用者角色**：具有適當權限的管理員或組織使用者。

您可以針對安全性設定檔自訂曝險指標和攻擊指標。

每個安全性設定檔都會獨立運作，確保設定檔之間不會互相影響。您應該僅將「Tenable」設定檔當作參考，因為您無法自訂該設定檔或使用它將異常情況列入白名單。您必須建立自己的自訂設定檔，以便符合特定要求。

指標自訂窗格中的「全域自訂」一詞**涉及所有網域**，而不是所有設定檔。因此，當您在安全性設定檔的任何設定中套用「全域自訂」時，「Tenable」設定檔或其他設定檔都不會受到影響。

**提示**：如要檢視「Tenable」安全性設定檔的設定，請按一下該行末尾的 圖示。

如要自訂指標：

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**安全性設定檔管理**」。

   「**安全性設定檔管理**」窗格會隨即顯示。

2. 在安全性設定檔清單中，將游標停留在包含待自訂指標的安全性設定檔上。按一下顯示安全性設定檔名稱的行末尾的 圖示。

   「**設定檔設定**」窗格會隨即顯示。

3. 選取「**曝險指標**」或「**攻擊指標**」索引標籤。

4. (可選) 在「**搜尋指標**」方塊中輸入指標名稱。

5. 按一下待自訂指標的名稱。

   「**指標自訂**」窗格會隨即顯示。

6. 從「選項」表格中選取選項。

   > **提示**：如要針對攻擊指標啟用**積極模式**，請按一下「積極模式」選項的切換按鈕並將其變更為「是」。

   > **提示**：某些指標選項需要使用規則運算式 (regex)。正則運算式是「包含」比對，而不是「等於」比對。
   > - 如要取得完全相符的項目，您必須使用正則運算式特殊字元 (「`^...$`」) 語法。
   > - 使用正則運算式時，您還必須使用反斜杠逸出特殊字元。範例：如要聲明「`domain\user`」和「`CN=Vincent C (Test),DC=tenable,DC=corp`」，您需要輸入「`domain\\user`」和「`CN=Vincent C. \(Test\),DC=tenable,DC=corp`」。

7. 按一下「**儲存為草稿**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已儲存自訂選項。

**如要套用自訂選項：**

1. 您可以執行下面任一項動作：

   - 在「**設定檔設定**」窗格中，按一下右下角的「**套用待定自訂**」；或者
   - 在「**安全性設定檔管理**」窗格中，按一下顯示安全性設定檔名稱的行末尾的 ✓ 圖示。

系統會顯示一則訊息，警告您套用自訂選項會清除其所有資料，並需要對受監控的 Active Directory 進行完整分析，這可能需要一些時間。

2. 按一下**「確定」**。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已套用自訂選項。在**「安全性設定檔管理」**表格的*「安全性分析」*欄中，**「等候」**表示根據您的安全性設定檔進行的分析正在等待執行。

**如要捨棄自訂：**

- 您可以執行下面任一項動作：
  - 在**「設定檔設定」**窗格中，按一下左下角的**「還原待定自訂」**；或者
  - 在**「安全性設定檔管理」**窗格中，按一下顯示安全性設定檔名稱的行末尾的 ↺ 圖示。

  系統會顯示一則訊息，確認 Tenable Identity Exposure 已取消自訂選項。

## 另請參閱

- 縮小指標自訂範圍

## 縮小指標自訂範圍

**所需的使用者角色**：具有適當權限的管理員或組織使用者。

針對安全性設定檔的指標進行額外自訂，有助於您為特定網域選取指標選項。依預設，全域自訂會套用至所有網域。

**如要精簡指標自訂：**

1. 在 Tenable Identity Exposure 中，按一下**「帳戶」**>**「安全性設定檔管理」**。

   **「安全性設定檔管理」**窗格會隨即顯示。

2. 在安全性設定檔清單中，將游標停留在包含待自訂指標的安全性設定檔上。按一下顯示安全性設定檔名稱的行末尾的 ✎ 圖示。

**「設定檔設定」**窗格會隨即顯示。

3. 選取**「曝險指標」**或**「攻擊指標」**索引標籤。
4. (可選) 在**「搜尋指標」**方塊中輸入指標名稱。
5. 按一下待自訂指標的名稱。

   **「指標自訂」**窗格會隨即顯示。
6. 在**「全局自訂」**索引標籤旁邊，按一下 **+** 圖示。

   **自訂號碼」**索引標籤會隨即顯示。
7. 按一下**「套用於」**方塊。

   **「樹系和網域 」**窗格會隨即顯示。
8. (可選) 在「搜尋」方塊中輸入樹系或網域的名稱。
9. 選取網域。
10. 按一下**「篩選選取的項目」**。
11. 根據需要對所選網域的指標進行進一步自訂。
12. 按一下**「儲存為草稿」**。

**如要捨棄精簡後的自訂：**

1. 按一下選項卡進行自訂。
2. 按一下窗格底部的**「移除此設定」**。

## 另請參閱

- 自訂指標

# 使用者角色

Tenable Identity Exposure 使用角色型存取控制 (RBAC) 來保護組織內的資料與職能存取安全。根據使用者的角色不同，角色決定使用者可從其帳戶存取的資訊類型。

根據角色不同，具有適當權限的使用者可向其他使用者指派權限，以執行下列動作：

- 讀取內容和功能表、系統和曝險指標設定。
- 編輯內容和功能表、系統和攻擊指標設定。
- 建立帳戶、安全性設定檔和角色。

## 另請參閱

- 管理角色
- 設定角色的權限
- 設定使用者介面實體的權限 (範例)

## 管理角色

如要建立新角色：

1. 在 Tenable Identity Exposure 中，前往「**帳戶**」>「**角色管理**」。
2. 按一下右上角的「**建立角色**」按鈕。

   「**建立角色**」窗格會隨即顯示。
3. 在「名稱」方塊中輸入角色的名稱。
4. 在「描述」方塊中輸入有關角色的一些資訊。
5. 按一下右上角的「**新增**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已建立角色。出現「**編輯角色**」窗格隨即會出現，供您設定此角色的權限。

**注意**：您無法修改 Tenable Identity Exposure 管理員角色 (稱為全域管理員)。按一下 圖示以顯示 Tenable Identity Exposure 角色設定。

如要刪除角色：

1. 在 Tenable Identity Exposure 中，前往「**帳戶**」>「**角色管理**」。
2. 在角色清單中，將游標停留在要刪除的角色上，按一下右側的 圖示。

   系統會顯示一則訊息，要求您確認刪除。

3. 按一下「刪除」。

   系統會顯示一則訊息，要求您確認刪除此角色。

## 另請參閱

- 設定角色的權限

## 設定角色的權限

**所需的使用者角色**：具有適當權限的管理員或組織使用者。

Tenable Identity Exposure 使用角色型存取控制 (RBAC) 來保護資料存取安全。角色會決定使用者可存取的資訊類型，這取決於使用者在組織中的職能角色。當您在 Tenable Identity Exposure 中建立新使用者時，就會為此使用者指派一個特定的角色及角色相關權限。

如要設定角色的權限：

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**角色管理**」。
2. 將游標停留在需要設定權限的角色上，按一下右側的 圖示。

   「**編輯角色**」窗格會隨即顯示。
3. 在「**權限管理**」下面選取一個實體類型：
   - 資料實體
   - 使用者實體
   - 系統設定實體
   - 介面實體
4. 在實體名稱清單中，選取要設定權限的實體。
5. 在「**讀取**」、「**編輯**」或「**建立**」欄下面，按一下切換為「已授予」或「未授權」。
6. 您可以執行下面任一項動作：

- 按一下「套用」以套用權限，並使「**編輯角色**」窗格保持在開啟狀態，以進行進一步修改。
- 按一下「套用並關閉」，套用權限並關閉「**編輯角色**」窗格。

系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新角色。

如要大量設定角色的權限：

1. 在 Tenable Identity Exposure 中，按一下「**帳戶**」>「**角色管理**」。
2. 將游標停留在需要設定權限的角色上，按一下右側的 圖示。

   「**編輯角色**」窗格會隨即顯示。
3. 在「**權限管理**」下面選取一個實體類型。
4. 選取要設定權限的實體或實體區段 (例如，曝險指標)。
5. 在頁面底部，按一下下拉方塊上的箭頭以顯示權限清單。
6. 選取角色的權限。
7. 按一下「**確定**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已設定實體權限。




## 權限類型

| 權限 | 說明 |
| --- | --- |
| 讀取 | 檢視物件或設定的權限。 |
| 編輯 | 修改物件或設定的權限。需要擁有「讀取」權限才能套用修改。 |
| 建立 | 建立物件或設定的權限。「**建立**」權限需要擁有「**讀取**」和「**編輯**」權限，才能對允許的資源執行允許的動作。 |

## 實體類型

Tenable Identity Exposure 中有四種類型的實體需要存取權限，您可以針對組織中的每個使用者角色進行調整：

| 實體類型 | 包含 | 權限 |
| --- | --- | --- |
| 資料實體 | | |
| 此實體控制在 Tenable Identity Exposure 中設定受監控的 Active Directory 和設定資料分析的權限。 | • 攻擊指標<br>• 曝險指標<br>• 樹系<br>• 網域<br>• 設定檔<br>• 使用者<br>• 電子郵件警示<br>• Syslog 警示<br>• 角色<br>• 實體轉送<br>• 報告 | 讀取、編輯、建立 |
| 使用者實體 | | |
| 此實體控制使用者設定 Tenable Identity Exposure 顯示執行資料分析時所需資訊 | • 喜好設定<br>• 儀表板 | 編輯、建立 |

| | | |
|---|---|---|
| 的能力，以及修改個人資訊和喜好設定的能力。 | • 小工具<br>• API 金鑰<br>• 個人資訊 | |
| **系統設定實體** | | |
| 此實體控制對於 Tenable Identity Exposure 平台和服務的存取權。 | • 應用程式服務 (SMTP、記錄、驗證 Tenable Identity Exposure、攻擊指標、受信任的憑證授權單位)<br>• 透過公用 API 評分<br>• 授權<br>• LDAP 驗證<br>• SAML 驗證<br>**注意**：如果您擁有 Tenable Vulnerability Management 授權，則無法使用 LDAP 和 SAML 驗證權限。<br>• 拓撲<br>• 帳戶鎖定原則<br>• 重新編目網域<br>• 活動記錄<br>• Tenable 雲端服務 (Tenable Cloud 資料收集)<br>• Microsoft Entra ID 支援<br>• 運作狀況檢查<br>• 僅顯示使用者自己的追蹤記錄 | 讀取、編輯 |

| 介面實體 | | |
|---|---|---|
| 此實體定義存取 Tenable Identity Exposure 使用者介面和功能中特定部分的權限。 | 特定 Tenable Identity Exposure 功能的存取路徑。如需詳細資訊，請參閱 設定使用者介面實體的權限 (範例) | 已授予、未授權 |

## 另請參閱

- 使用者帳戶
- 使用者角色

## 設定使用者介面實體的權限 (範例)

Tenable Identity Exposure 會依照存取特定使用者介面功能時使用的路徑套用權限。以下範例顯示如何設定權限以允許設定 Syslog。

如要存取 Syslog 參數，使用者需要在 Tenable Identity Exposure 中依照**「系統」**>**「設定」**>**「SYSLOG」**路徑要求權限：

- 系統設定：**「管理」**>**「系統」**
- 設定參數：**「管理」**>**「系統」**>**「設定」**
- Syslog 警示：**「管理」**>**「系統」**>**「設定」**>**「警示引擎」**>**「SYSLOG」**

如要設定 Syslog 設定的權限：

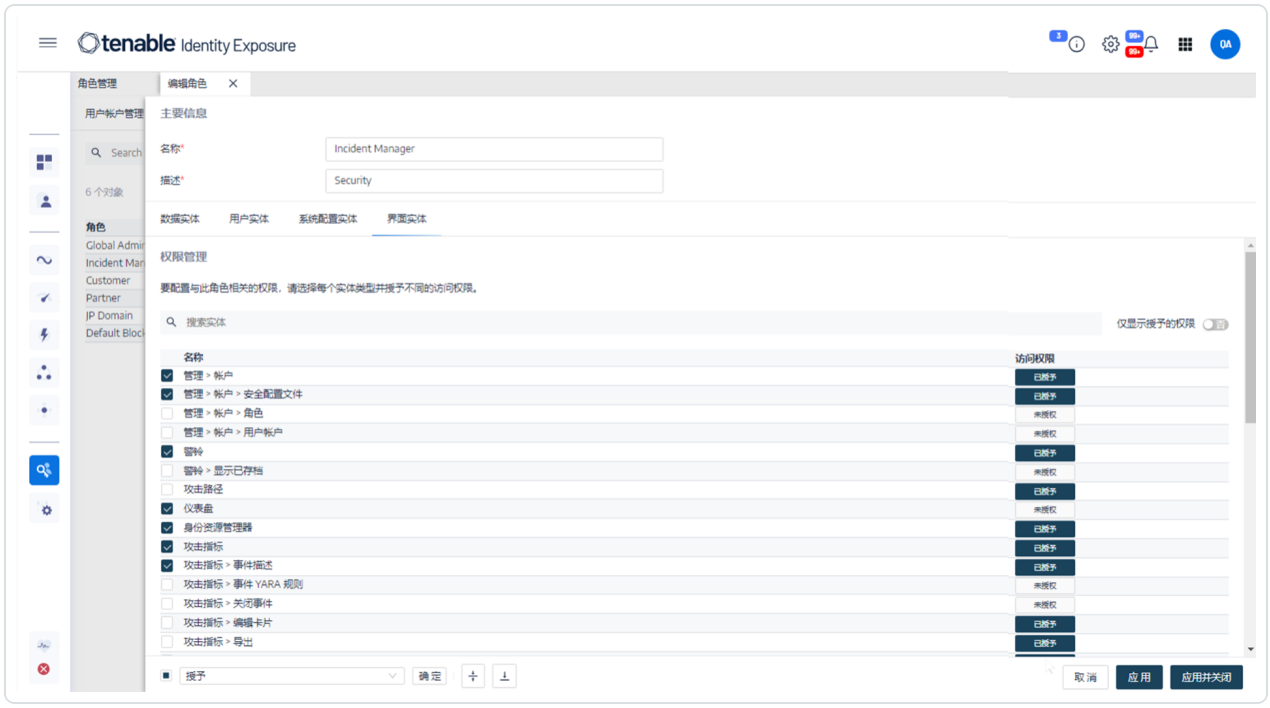
1. 在 Tenable Identity Exposure 中，按一下**「帳戶」**>**「角色管理」**。
2. 將游標停留在需要設定權限的角色上，按一下右側的 圖示。

   **「編輯角色」**窗格會隨即顯示。
3. 在**「權限管理」**下面選取**「介面實體」**。
4. 在實體清單中執行下列動作：
   - 選取**「管理」**>**「系統」**，然後按一下「存取權」切換為**「已授權」**。
   - 選取**「管理」**>**「系統」**>**「設定」**，然後按一下「存取權」切換為**「已授權」**。

- 選取「**管理**」>「**系統**」>「**設定**」>「**警示引擎**」>「**SYSLOG**」，然後按一下「存取權」切換為「**已授權**」。

5. 按一下「**套用**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新實體權限。

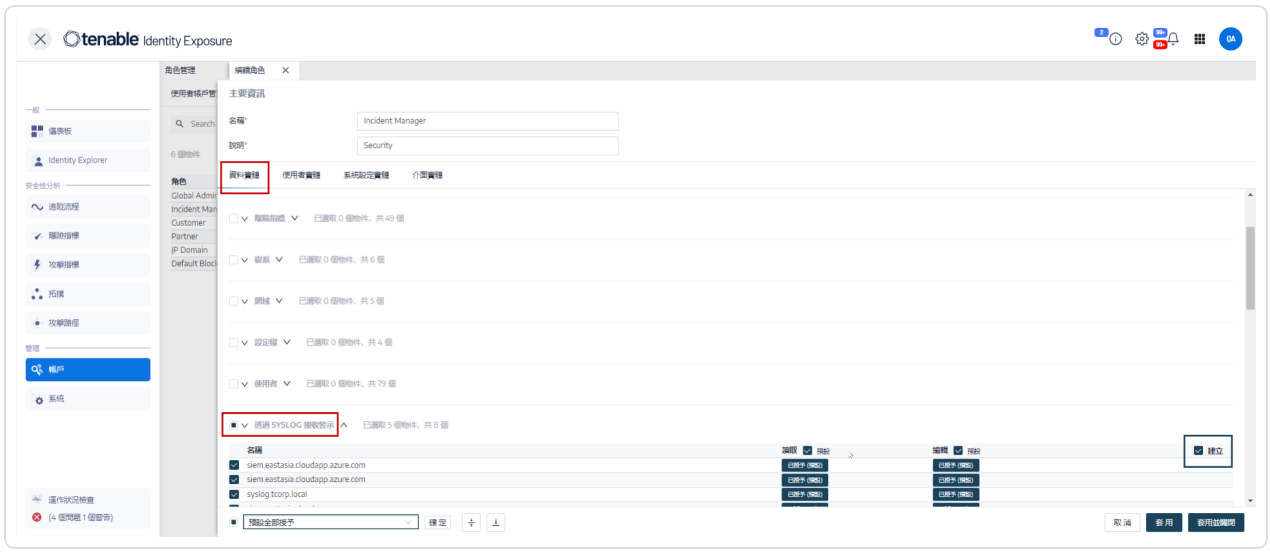



6. 在「**權限管理**」下面選取「**資料實體**」。
7. 在實體區段清單中，選取「**Syslog 警示**」。
8. 選取「**建立**」權限。

   Tenable Identity Exposure 隱含授予「讀取」和「編輯」權限。

9. 按一下「**套用並關閉**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新實體權限。




# 樹系

Active Directory (AD) 樹系是共用通用結構描述、設定和信任關係的網域集合。這個樹系提供階層式結構來管理和組織資源，能夠在組織內實現跨多個網域進行集中管理和安全驗證。

## 管理樹系

**如要新增樹系：**

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**樹系管理**」。
2. 按一下右側的「**新增樹系**」。

   「新增樹系」窗格會隨即顯示。
3. 在「**名稱**」方塊中輸入樹系的名稱。
4. 在「**帳戶**」區段中，為 Tenable Identity Exposure 使用的服務帳戶提供下列內容：
   - **登入**：輸入服務帳戶的名稱。
     **格式**：使用主體名稱，例如「`tenablead@domain.example.com`」(與 Kerberos 驗證 相容時建議使用)，或使用 NetBIOS，例如「`DomainNetBIOSName\SamAccountName`」。
   - **密碼**：輸入服務帳戶的密碼。

**注意**：如果您必須將 Tenable Identity Exposure 的 AD 服務帳戶設定為受保護的使用者群組成員，請確認您的 Tenable Identity Exposure 設定支援 Kerberos 驗證，因為受保護的使用者無法使用 NTLM 驗證。

5. 按一下**「新增」**。

   系統會顯示一則訊息，確認已新增樹系。

**如要編輯樹系：**

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「樹系管理」**。
2. 在樹系清單中，將游標停留在要修改的樹系上，按一下右側的  圖示。

   **「編輯樹系」**窗格會隨即顯示。
3. 視需要進行修改。
4. 按一下**「編輯」**。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新樹系。

## 保護服務帳戶

Tenable 建議保護服務帳戶，以維護安全性，方法是將使用者帳戶控制 (UAC) 屬性正確設定為防止委派、要求預先驗證、使用更強的加密、強制執行密碼到期和要求，以及允許經授權的密碼變更。這些措施可減輕未經授權存取和潛在安全缺口的風險，確保組織系統和資料的完整性。

**如要使用 Windows 原則編輯器修改設定：**

您可以透過適當的系統管理權限，使用 Windows 的本機安全性原則編輯器或群組原則編輯器修改使用者帳戶控制設定。

- 在編輯器中，導覽至**「本機原則」**->**「安全性選項」**，找到並設定下列設定 (可能會因您的 Windows 版本而有所不同)：
  - *「網路存取：不允許儲存網路驗證的密碼和憑證」*：將其設定為**「啟用」**。
  - *「帳戶：不需要 Kerberos 預先驗證」*：將其設定為**「停用」**。

- *「網路安全性:設定 Kerberos 允許的加密類型」*:確認 **未**選取*「針對此帳戶使用 Kerberos DES 加密類型」*選項。
- *「帳戶:密碼最長使用期限」*:設定密碼到期期間 (例如, 30、60 或 90 天, 使 `PasswordNeverExpires = FALSE`)。
- *「帳戶:將本機帳戶使用空白密碼限制為僅限主控台登入」*:將其設定為**「停用」**。
- *「互動式登入:要快取的先前登入次數 (在網域控制器無法使用的情況下)」*:設定所需的值, 例如**「10」**以允許使用者變更其密碼。

**如要使用 Powershell 修改設定:**

- 在託管 AD 的電腦上, 以適當的系統管理權限開啟 PowerShell 並執行下列命令:

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly
$false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired
$false -CannotChangePassword $false
```

其中 `<AD_ACCOUNT>` 是您要修改的 Active Directory 帳戶名稱。

## 網域

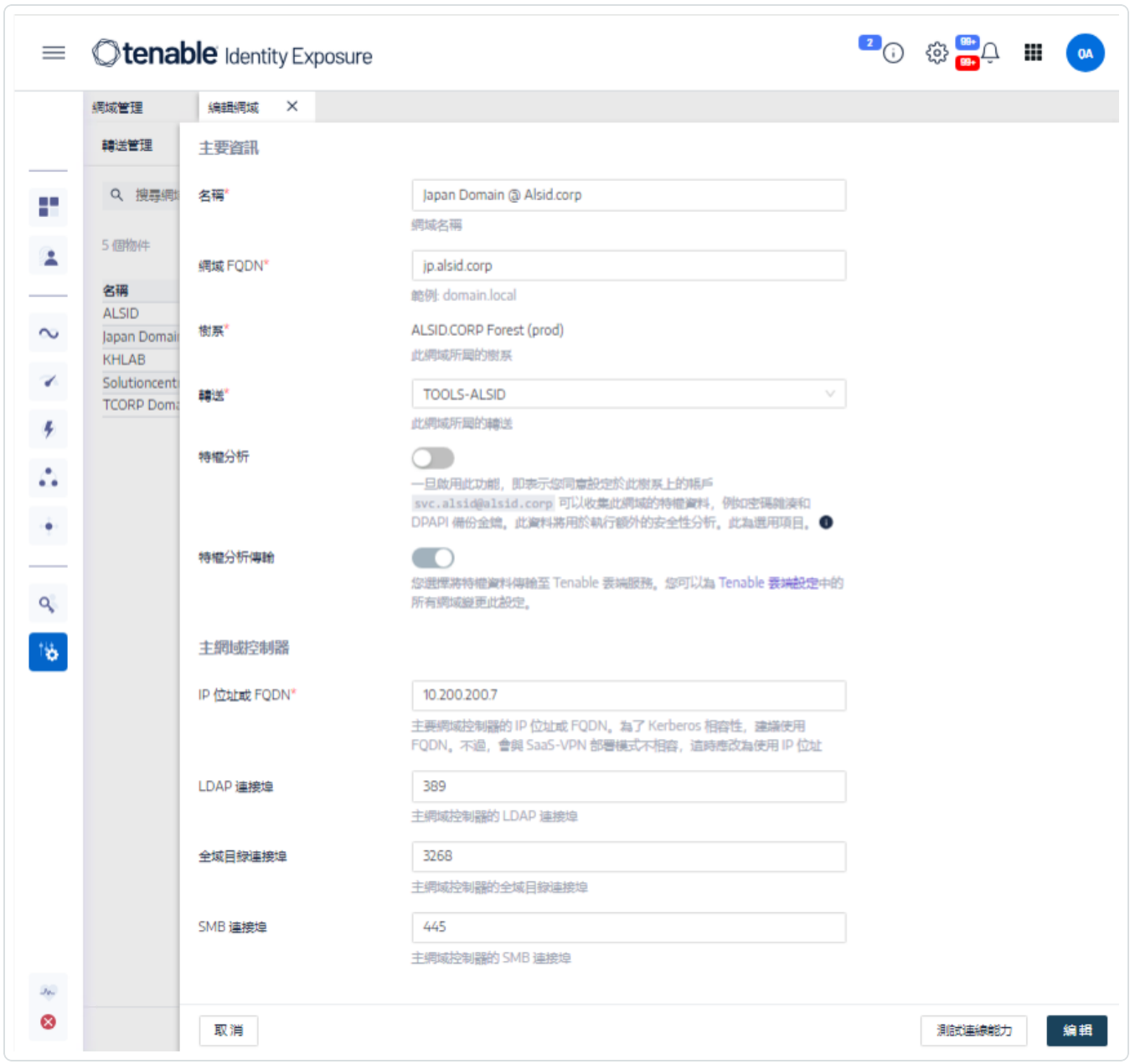
Tenable Identity Exposure 會監控網域, 這些網域以邏輯方式將共用通用設定的物件分組, 以便進行集中管理。

**如要新增網域:**

1. 在 Tenable Identity Exposure 中, 按一下**「系統」**。
2. 按一下**「網域管理」**索引標籤。

   **「網域管理」**窗格會隨即顯示。
3. 按一下右上角的**「新增網域」**。

   **「新增網域」**窗格會隨即顯示。




4. 在「**主要資訊**」區段中提供下列資訊：

   - 在「**名稱**」方塊中輸入網域的名稱。
   - 在「**網域 FQDN**」方塊中輸入網域的完整網域名稱 (FQDN)。
   - 在「**樹系**」下拉式方塊中選取網域所屬的樹系。

5. **特權分析** (選用):如果啟用此切換開關,則允許此樹系上的「dcadmin」帳戶收集此網域上的特權資料,以執行進階安全性分析。
6. **特權分析傳輸**:有關此選項的詳細資訊,請參閱 Tenable Cloud 資料收集
7. 在「**主要網域控制器**」區段中提供下列資訊:
   - 在「**IP 位址或主機名稱**」方塊中輸入主要網域控制器的主機名稱 (與 Kerberos 驗證相容但與 SaaS-VPN 部署模式不相容時為必要項目) 或 IP 位址。

     Tenable Identity Exposure 不支援負載平衡器。
   - 在「**LDAP 連接埠**」方塊中輸入主要網域控制器的 LDAP 連接埠。

     **注意**:如果您使用 TCP/636 (LDAPS) 連接埠連接到您的網域,則 Tenable Identity Exposure 必須有權存取您的 Active Directory 的憑證授權單位 (CA) 憑證,以驗證您的 AD 憑證,然後才能執行連接。在安全轉送環境中,您可以在轉送電腦上安裝 CA 憑證。在 VPN 環境中,無法進行此設定。
   - 在「**全域目錄連接埠**」方塊中輸入主要網域控制器的全域目錄連接埠。
   - 在「**SMB 連接埠**」方塊中輸入主要網域控制器的 SMB 連接埠。
8. 按一下「**新增**」。

   系統將顯示一則訊息,確認 Tenable Identity Exposure 已新增網域。

**如要編輯網域:**

1. 在 Tenable Identity Exposure 中,按一下「**系統**」。
2. 按一下「**網域管理**」索引標籤。

   「**網域管理**」窗格會隨即顯示。
3. 將游標停留在要編輯的網域名稱上,右側會顯示 圖示。
4. 按一下 圖示。

   「**編輯網域**」窗格會隨即顯示。
5. 編輯網域的資訊。

6. 按一下「**編輯**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新網域。

**如要刪除網域及歷史資料：**

1. 在 Tenable Identity Exposure 中，按一下「**系統**」。
2. 按一下「**網域管理**」索引標籤。

   「**網域管理**」窗格會隨即顯示。
3. 將游標停留在要刪除的網域名稱上，顯示  圖示。
4. 按一下  圖示。

   系統會顯示一則訊息，要求您確認刪除「domain_name」網域。
5. 按一下「**刪除**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已刪除網域。
6. 等待系統清理與所刪除網域相關的任何 Active Directory 歷程記錄資料。

## 另請參閱

- 在網域上強制執行資料重新整理
- 誘捕帳戶
- Kerberos 驗證

## 在網域上強制執行資料重新整理

如要在網域上強制執行資料重新整理：

1. 在 Tenable Identity Exposure 中，按一下「**系統**」。
2. 按一下「**網域管理**」索引標籤。

   「**網域管理**」窗格會隨即顯示。

3. 將游標停留在要強制執行資料重新整理的網域名稱上，右側會顯示 圖示。
4. 按一下 圖示。

   系統會顯示一則訊息，其中包含有關資料重新整理動作的資訊。
5. 按一下**「確認」**。

## 另請參閱

- 誘捕帳戶

## 誘捕帳戶

**所需使用者角色**：本機電腦上的管理員

誘捕帳戶是一個誘餌帳戶，其唯一的目的是偵測試圖透過 Active Directory 入侵網路的攻擊者。

這是 Tenable Identity Exposure 的攻擊指標偵測 Kerberoasting 攻擊的先決條件，此攻擊會要求和擷取服務工單，然後離線破解服務帳戶的憑證，藉此取得服務帳戶的存取權。當誘捕帳戶收到登錄嘗試或工單要求時，Kerberoasting 攻擊指標會發出警警示。

您可以為每個網域關聯一個誘捕帳戶。誘捕帳戶與安全性設定檔無關。

**如要新增誘捕帳戶：**

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「網域管理」**。

   **「網域管理」**窗格會隨即顯示。
2. 將游標停留在您要新增誘捕帳戶的網域上。
3. 在**「誘捕帳戶設定狀態」**下面，按一下 **+**。

   **「新增誘捕帳戶」**窗格隨即顯示。
4. 在**「名稱」**方塊中，為使用者帳戶輸入要作為誘捕帳戶使用的辨別名稱 (DN)。

   **提示**：您可以輸入任何字串，如果 Active Directory 中已有此使用者帳戶，則 Tenable Identity Exposure 會在下拉式方塊中搜尋並顯示符合的使用者帳戶名稱。

5. 在「**部署**」區段中，Tenable Identity Exposure 會產生一個具有適當設定的指令碼，您可以在部署誘捕帳戶時執行此指令碼。按一下 以複製此指令碼。

6. 按一下「**新增**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已新增誘捕帳戶。在「網域管理」窗格中，所選網域的「**誘捕帳戶設定狀態**」顯示為橙色 ( )，表示您必須執行誘捕帳戶部署指令碼才能將其啟動。

   > **注意**：如果「**誘捕帳戶設定狀態**」顯示為紅色 ( )，則表示 Tenable Identity Exposure 未在 Active Directory 中找到此使用者帳戶。您必須建立此使用者帳戶，然後繼續執行下一步。

7. 在具有 Active Directory 模組的電腦上，在 Windows PowerShell 中執行您複製的誘捕帳戶部署指令碼。

   在「**網域管理**」窗格中，所選網域的「**誘捕帳戶設定狀態**」會顯示為綠色 ( )，表示其處於作用中狀態。

   > **注意**：Tenable Identity Exposure 可能需要一些時間來處理和啟動誘捕帳戶。

**如要編輯誘捕帳戶：**

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**網域管理**」。

   「**網域管理**」窗格會隨即顯示。

2. 將游標停留在您要新增誘捕帳戶的網域上。

3. 在「**誘捕帳戶設定狀態**」下面，按一下右側的 圖示。

   「**編輯誘捕帳戶**」窗格會隨即顯示。

4. 在「**名稱**」方塊中，視需要修改使用者帳戶。

5. 在「**部署**」區段中，按一下 以複製誘捕帳戶部署指令碼。

6. 按一下「**編輯**」。

系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新誘捕帳戶。在「網域管理」窗格中，所選網域的「**誘捕帳戶設定狀態**」顯示為橙色 ()，表示您必須執行誘捕帳戶部署指令碼才能將其啟動。

> **注意**：如果「**誘捕帳戶設定狀態**」顯示為紅色 ()，則表示 Tenable Identity Exposure 未在 Active Directory 中找到此使用者帳戶。您必須建立此使用者帳戶，然後繼續執行下一步。

7. 在具有 Active Directory 模組的電腦上，在 Windows PowerShell 中執行您複製的誘捕帳戶部署指令碼。

   在「**網域管理**」窗格中，所選網域的「**誘捕帳戶設定狀態**」會顯示為綠色 ()，表示其已完成設定。

   > **注意**：Tenable Identity Exposure 可能需要一些時間來處理和啟動誘捕帳戶。

**如要刪除誘捕帳戶：**

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**網域管理**」。

   「**網域管理**」窗格會隨即顯示。

2. 將游標停留在您要新增誘捕帳戶的網域上。

3. 在「**誘捕帳戶設定狀態**」下面，按一下右側的  圖示。

   「**編輯誘捕帳戶**」窗格會隨即顯示。

4. 按一下「**刪除**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已刪除誘捕帳戶。

## 另請參閱

- 在網域上強制執行資料重新整理

## Kerberos 驗證

Tenable Identity Exposure 會使用您提供的憑證，對已設定的網域控制器進行驗證。這些 DC 接受 NTLM 或 Kerberos 驗證。NTLM 是具有安全性問題記錄的舊版通訊協定，而且 Microsoft 和

所有網路安全標準現在都不鼓勵使用。另一方面，Kerberos 是更健全的通訊協定，您應該予以考慮。Windows 一律會先嘗試 Kerberos，僅在 Kerberos 無法使用時才使用 NTLM。

Tenable Identity Exposure 與 NTLM 和 Kerberos 相容，但有少數例外狀況。Kerberos 符合所有必要條件時，Tenable Identity Exposure 會將其列為優先通訊協定。本節將介紹相關要求，並說明如何設定 Tenable Identity Exposure 以確保 Kerberos 能順利使用。

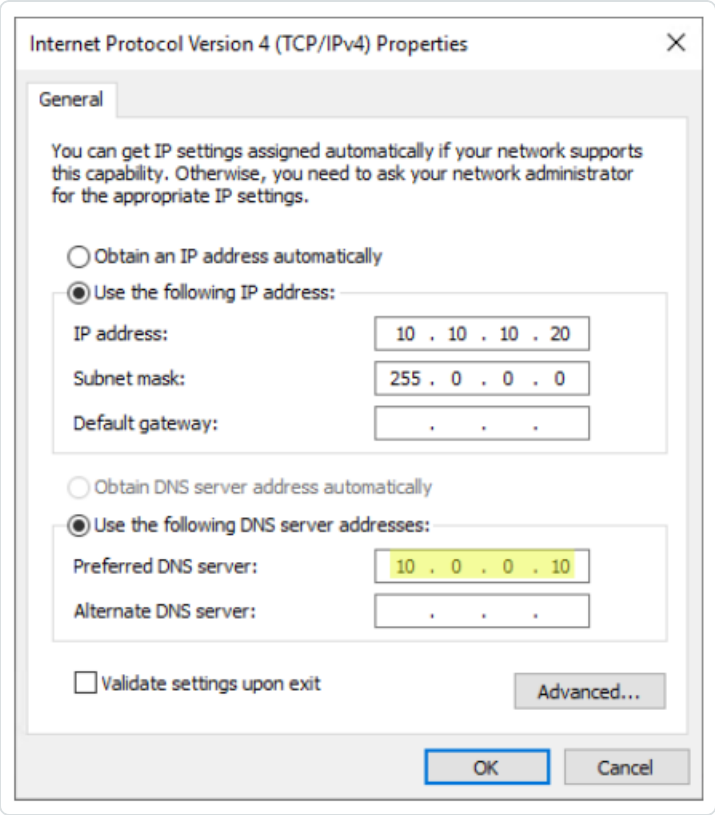
使用 NTLM 而非 Kerberos 也是 SYSVOL 強化干擾 Tenable Identity Exposure 的原因。如需詳細資訊，請參閱 SYSVOL 強化干擾 Tenable Identity Exposure。

## 與 Tenable Identity Exposure 部署模式的相容性

| 部署模式 | Kerberos 支援 |
| --- | --- |
| 內部部署 | 是 |
| SaaS-TLS (舊版) | 是 |
| 採用 Tenable Identity Exposure 的安全轉送 的 SaaS | 是 |
| 採用 VPN 的 SaaS | 否：您必須將安裝切換至 Tenable Identity Exposure 的安全轉送 部署模式。 |

### 技術要求

- **Tenable Identity Exposure 中設定的 AD 服務帳戶必須具有 UserPrincipalName (UPN)**。如需指示，請參閱服務帳戶和網域設定 。
- **DNS 設定和 DNS 伺服器必須允許解析所有必要的 DNS 項目**：您必須將目錄接聽程式或轉送電腦設定為使用知道網域控制器的 DNS 伺服器。如果目錄接聽程式或轉送電腦已加入網域 (Tenable Identity Exposure 不建議這麼做)，您應該已經符合此要求。最簡單的方法是使用網域控制器本身作為優先 DNS 伺服器，這是因為它通常也會執行 DNS。例如：




**注意**：如果目錄接聽程式或轉送電腦已連線至數個網域，且可能在數個樹系中，則請確認設定的 DNS 伺服器可解析所有網域所需的所有 DNS 項目。否則，您需要設定數個目錄接聽程式或轉送電腦。

- **Kerberos「伺服器」(KDC) 的連線能力**：這需要透過連接埠 TCP/88 從目錄接聽程式或轉送電腦連線至網域控制器。如果目錄接聽程式或轉送電腦已加入網域 (Tenable 不建議這麼做)，您應該已經符合此要求。每個已設定的 Tenable Identity Exposure 樹系都要求 Kerberos 網路連線至其包含服務帳戶的個別網域中的至少一個網域控制器，以及每個連線網域中的至少一個網域控制器。

  如需有關要求的詳細資訊，請參閱 Network Flow Matrix。

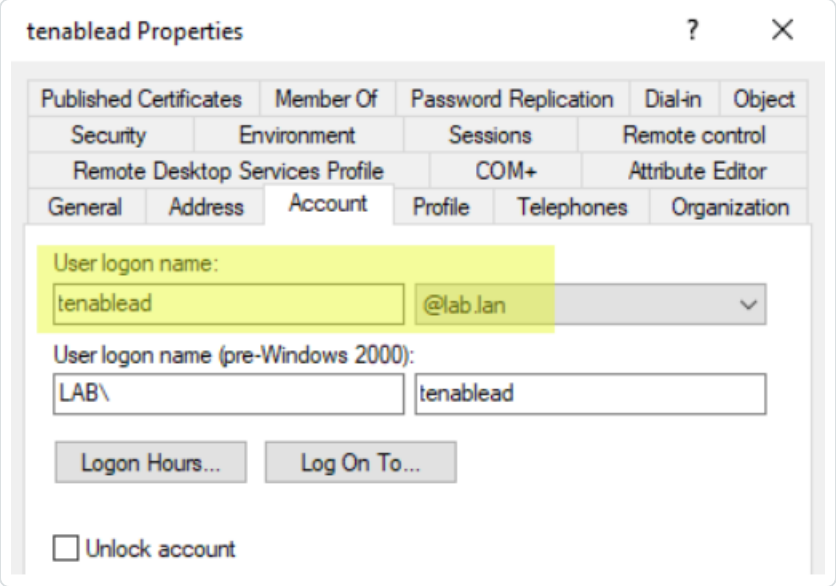
  **注意**：目錄接聽程式或轉送電腦不需加入網域即可使用 Kerberos。

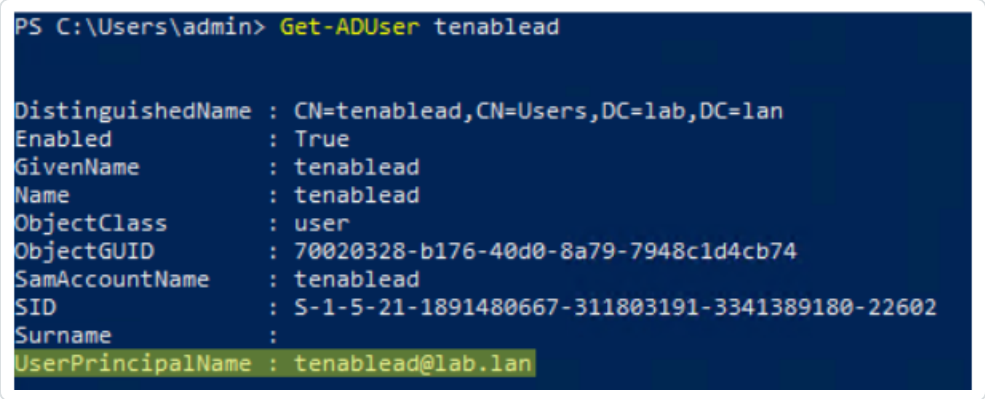
### 服務帳戶和網域設定

如要將 Tenable Identity Exposure 中的 AD 服務帳戶和 AD 網域設定為使用 Kerberos：

1. 使用使用者主體名稱 (UPN) 格式登入。在此範例中，UPN 屬性為「tenablead@lab.lan」。

   a. 在包含服務帳戶的樹系網域中找到 UPN 屬性，如下所示：




> **注意**：UPN 看起來像電子郵件地址，甚至經常 (但不總是) 與使用者的電子郵件地址相同。

b. 在 Tenable Identity Exposure 的樹系設定區段中，設定此 UPN 而非短「username」格式或 NetBIOS「domain\username」格式，如下所示：




2. 使用完整網域名稱 (FQDN) 在 Tenable Identity Exposure 的網域設定中，設定主要網域控制器 (PDC) 的 FQDN，而非其 IP。

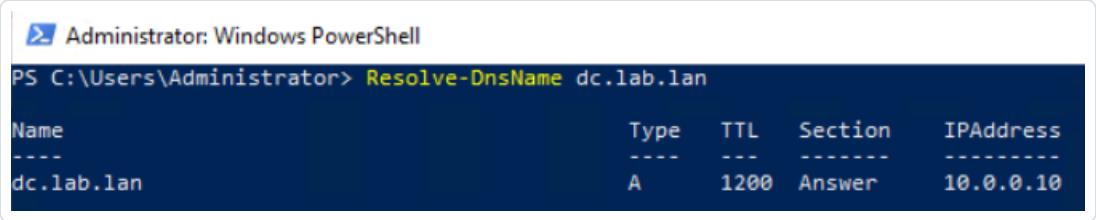



## 疑難排解

Kerberos 需要經過數個設定步驟才能正常運作。否則，Windows 會默默改回 NTLM 驗證，進而使 Tenable Identity Exposure 也是如此。

## DNS

確保目錄接聽程式或轉送電腦上使用的 DNS 伺服器可解析提供的 PDC FQDN，例如：




## Kerberos

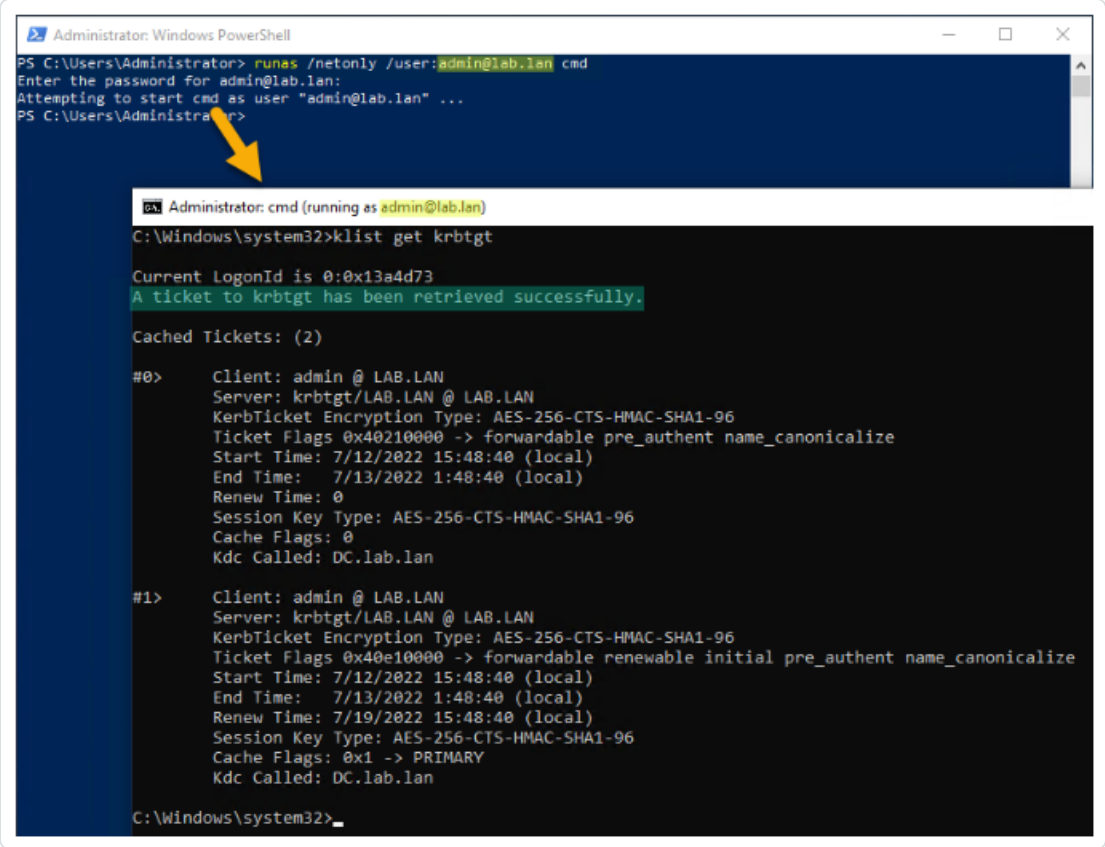
如要驗證 Kerberos 可否與您在目錄接聽程式或轉送電腦上執行的命令搭配使用：

1. 驗證 Tenable Identity Exposure 中設定的 AD 服務帳戶可以取得 TGT：

   a. 在命令列或 PowerShell 中，執行「`runas /netonly /user:<UPN> cmd`」，然後輸入密碼。輸入或貼上密碼時請格外小心，因為有「`/netonly`」標記，無法進行驗證。

   b. 在第二個命令提示下，執行「`klist get krbtgt`」以要求 TGT 工單。

      以下為成功結果範例：

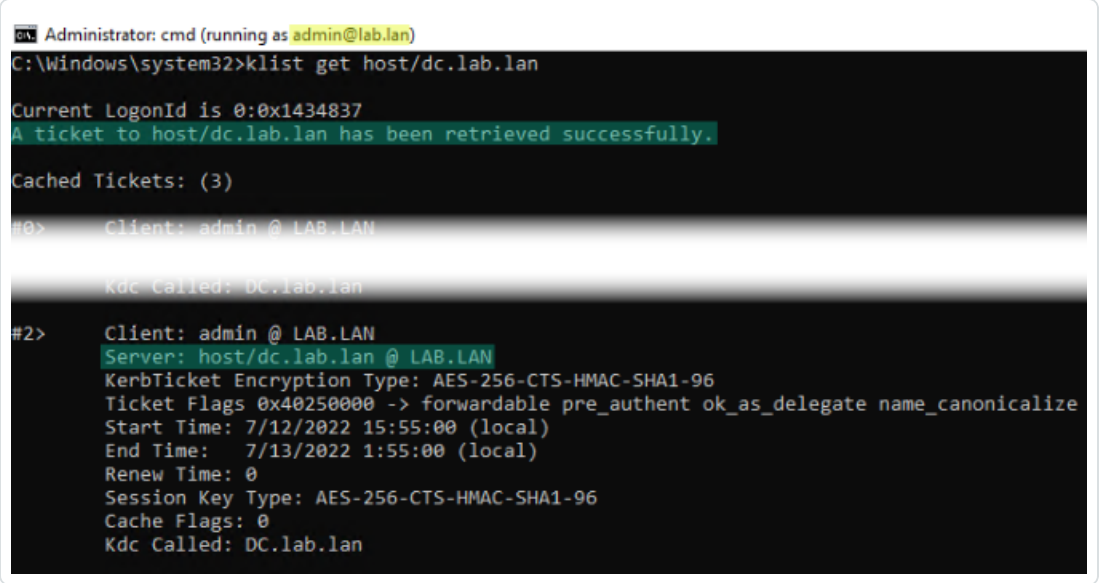



可能的錯誤代碼如下：

- `0xc0000064`:「使用者以拼字錯誤或錯誤的使用者帳戶登入」-> 檢查登入(即 UPN 中「@」之前的部分)。
- `0xc000006a`:「使用者以拼字錯誤或錯誤的密碼登入」-> 檢查密碼。
- `0xc000005e`:「目前沒有任何登入伺服器可用來處理登入要求。」-> 檢查 DNS 解析是否運作正常，以及伺服器是否可聯絡傳回的 KDC，等等。
- 其他錯誤碼：請參閱與 4625 事件相關的 Microsoft 說明文件。

2. 驗證 Tenable Identity Exposure 中設定的網域控制器是否可取得服務工單。在相同的第二個命令提示中，執行「`klist get host/<DC_FQDN>`」(取代「`<DC_FQDN>`」)。

以下為成功結果範例：




## 警示

**需要授權**：根據您要傳送的警示類型，您可能需要攻擊指標或曝險指標的授權。

Tenable Identity Exposure 的警示系統可協助您識別受監控的 Active Directory 上的安全狀態惡化和/或攻擊。它會透過電子郵件或 Syslog 通知，即時推送有關弱點和攻擊的分析資料。

- SMTP 伺服器設定
- 電子郵件警示
- Syslog 警示
- Syslog 和電子郵件警示詳細資料

## SMTP 伺服器設定

Tenable Identity Exposure 需要使用簡單郵件傳輸通訊協定 (SMTP) 設定來傳送警示通知。

部署架構的差異

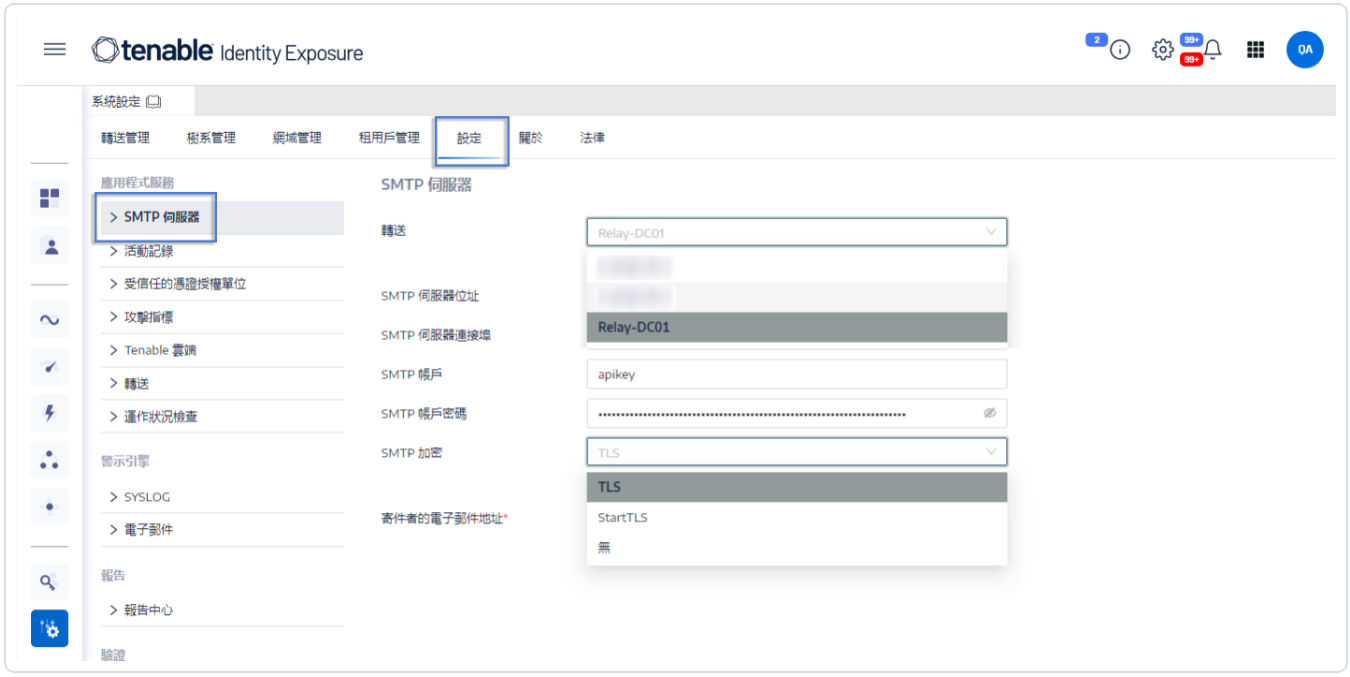
- 針對**安全轉送**架構：
  - 安全轉送已**安裝在客戶的環境中**。
  - 您可以管理安全轉送和 SMTP/SYSLOG 伺服器之間的通訊。
- 針對 **VPN** 架構：
  - 安全轉送服務**託管在 Tenable 的雲端上**。
  - 您向 Tenable 提交支援個案，以管理警示通訊。

## 安全轉送環境的 SMTP 伺服器設定

如要設定**安全轉送**的 SMTP 伺服器：

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「設定」**。
2. 在**「應用程式服務」**下，選取**「SMTP 伺服器」**。

   **「SMTP 伺服器」**窗格會隨即開啟。




3. **如果您的網路使用安全轉送：**在**「轉送」**方塊中按一下箭頭，從下拉式清單中選取要與 SMTP 伺服器通訊的轉送。
4. 提供以下資訊：

- SMTP 伺服器位址
- SMTP 伺服器連接埠
- SMTP 帳戶
- SMTP 帳戶密碼

5. 在「SMTP 加密」方塊中按一下箭頭，從下拉式清單中選取一種加密方法。
6. 在「**寄件者的電子郵件地址**」方塊中，提供 Tenable Identity Exposure 傳送電子郵件時使用的電子郵件地址。
7. 按一下「**儲存**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新 SMTP 參數。

## VPN 環境的 SMTP 伺服器設定

如要設定 **VPN** 的 SMTP 伺服器：

1. 確定 SMTP 伺服器託管在以下哪個位置：
   - 客戶網路**內** (**私有**環境)。
   - 客戶網路**外** (**公用**環境)。
2. 根據您的網路設定：
   - 針對託管在客戶網路**內**的 SMTP 伺服器：
     - 透過開啟支援個案，向 Tenable 提供 SMTP 伺服器的私有 IP 位址。提交將此 IP 列入白名單的要求，以便在 VPN 通道內進行通訊。
     - 等待 Tenable 的開發團隊完成設定。
     - 測試 VPN 通道，確認 Tenable 雲端和內部 SMTP 伺服器之間可否正常連線。
   - 針對託管在客戶網路**外**的 SMTP 伺服器：
     - 確認外部 SMTP 伺服器是否篩選傳入連線：
       - 如果根據來源 IP **篩選**傳入流量：

- 向 Tenable 提交支援個案，要求提供 VPN 通道的警示 IP 位址。
- 與外部 SMTP 供應商合作，將 Tenable 的警示 IP 位址列入白名單。

- 若**未篩選**傳入流量：確定 SMTP 伺服器的公用 IP 可透過 VPN 通道連線。

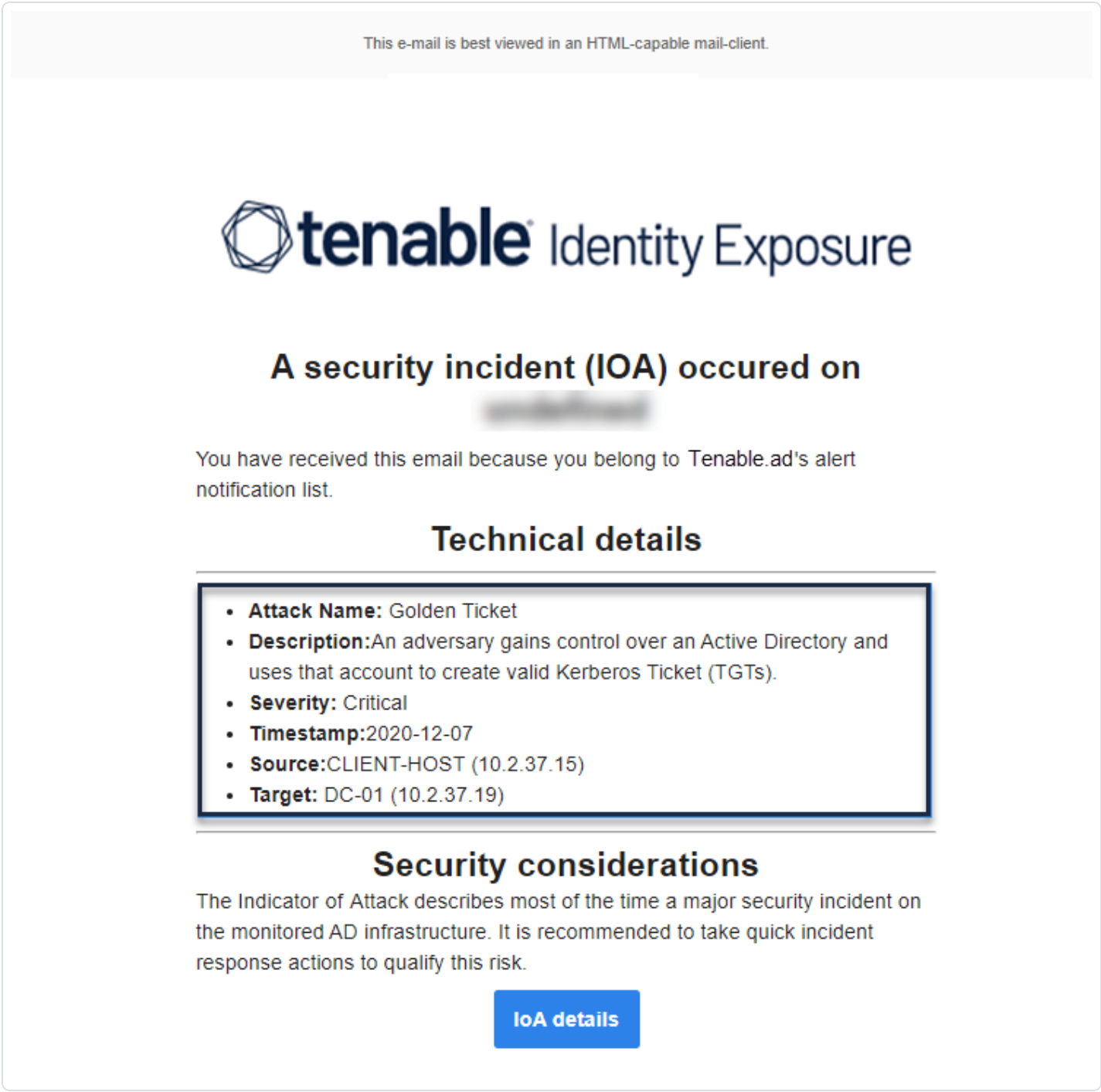
3. **持續維護**：將 SMTP 伺服器私有或公用 IP 位址的任何變更通知 Tenable，以維護 VPN 通道功能。

常見問題疑難排解

- **無法傳送警示** (SMTP/SYSLOG)：
  - 驗證在 VPN 通道內可否連線 SMTP 伺服器 (私有或公用)。
  - 確認 IP 位址在兩端 (Tenable 雲端和 SMTP 伺服器) 均列入白名單。
- **連線逾時**：
  - 檢查 VPN 通道活動和路由設定。

## 電子郵件警示

如果事件達到特定的嚴重性臨界值並需要修復動作，Tenable Identity Exposure 會自動傳送電子郵件警示通知您。以下是電子郵件警示的範例：




## 新增電子郵件警示

1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」>「**電子郵件**」。
2. 按一下右側的「**新增電子郵件警示**」按鈕。

   「**新增電子郵件警示**」窗格會隨即顯示。

3. 在「**主要資訊**」區段下面提供下列資訊：
    - 在「**電子郵件地址**」方塊中輸入收件者用來接收通知的電子郵件地址。
    - 在「**描述**」方塊中輸入有關收件者地址的描述。
4. 在「**觸發警示**」下拉式清單中，選取下列選項之一：
    - **每次發生異常情況時**：Tenable Identity Exposure 會在每次偵測到異常曝險指標 (IoE) 時發出通知。
    - **每次發生攻擊時**：Tenable Identity Exposure 會在每次偵測到異常攻擊指標 (IoA) 時發出通知。
    - **每次運作狀況檢查狀態變更**時：Tenable Identity Exposure 會在每次運作狀況檢查狀態變更時發出通知。
5. 在「**設定檔**」方塊中按一下，選取要用於此電子郵件警示的設定檔 (若適用)。
6. **在初始分析階段偵測到異常情況時傳送警示**：執行下列任一動作 (若適用)：
    - 選取核取方塊：當系統重新啟動觸發警示時，Tenable Identity Exposure 會傳送大量電子郵件通知。
    - 取消選取核取方塊：當系統重新啟動觸發警示時，Tenable Identity Exposure 不會傳送電子郵件通知。
7. **嚴重性臨界值**：按一下下拉式方塊的箭頭，可選取 Tenable Identity Exposure 傳送警示時的臨界值 (若適用)。
8. 視您在前面步驟中選取的警示觸發程序而定：
    - **曝險指標**：如果您將警示設定為**每次發生異常情況時**觸發，請按一下每個嚴重性等級旁邊的箭頭，以展開曝險指標清單並選取要傳送警示的指標。
    - **攻擊指標**：如果您將警示設定為**每次發生攻擊時**觸發，請按一下每個嚴重性等級旁邊的箭頭，以展開攻擊指標清單並選取要傳送警示的指標。
    - **運作狀況檢查狀態變更**：按一下「**運作狀況檢查**」，選取要觸發警示的運作狀況檢查類型，然後按一下「**篩選選取的項目**」。

9. 按一下**「網域」**方塊，以選取 Tenable Identity Exposure 要傳送警示的網域。

   **「樹系和網域」**窗格會隨即顯示。

   a. 選取樹系或網域。

   b. 按一下**「篩選選取的項目」**。

10. 按一下**「測試設定」**。

    系統會顯示一則訊息，確認 Tenable Identity Exposure 已傳送電子郵件警示至伺服器。

11. 按一下**「新增」**。

    系統將顯示一則訊息，確認 Tenable Identity Exposure 已建立電子郵件警示。

### 編輯電子郵件警示

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「設定」**>**「電子郵件」**。
2. 在電子郵件警示清單中，將游標停留在您要修改的警示上，然後按一下此行末尾的 圖示。

   **「編輯電子郵件警示」**窗格會隨即顯示。

3. 按照前文**「**新增電子郵件警示**」**程序中所述進行必要的修改。
4. 按一下**「編輯」**。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新警示。

### 刪除電子郵件警示

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「設定」**>**「電子郵件」**。
2. 在電子郵件警示清單中，將游標停留在您要刪除的警示上，然後按一下此行末尾的 圖示。

   系統會顯示一則訊息，要求您確認刪除。

3. 按一下**「刪除」**。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已刪除警示。

## 另請參閱

- SMTP 伺服器設定
- Syslog 和電子郵件警示詳細資料

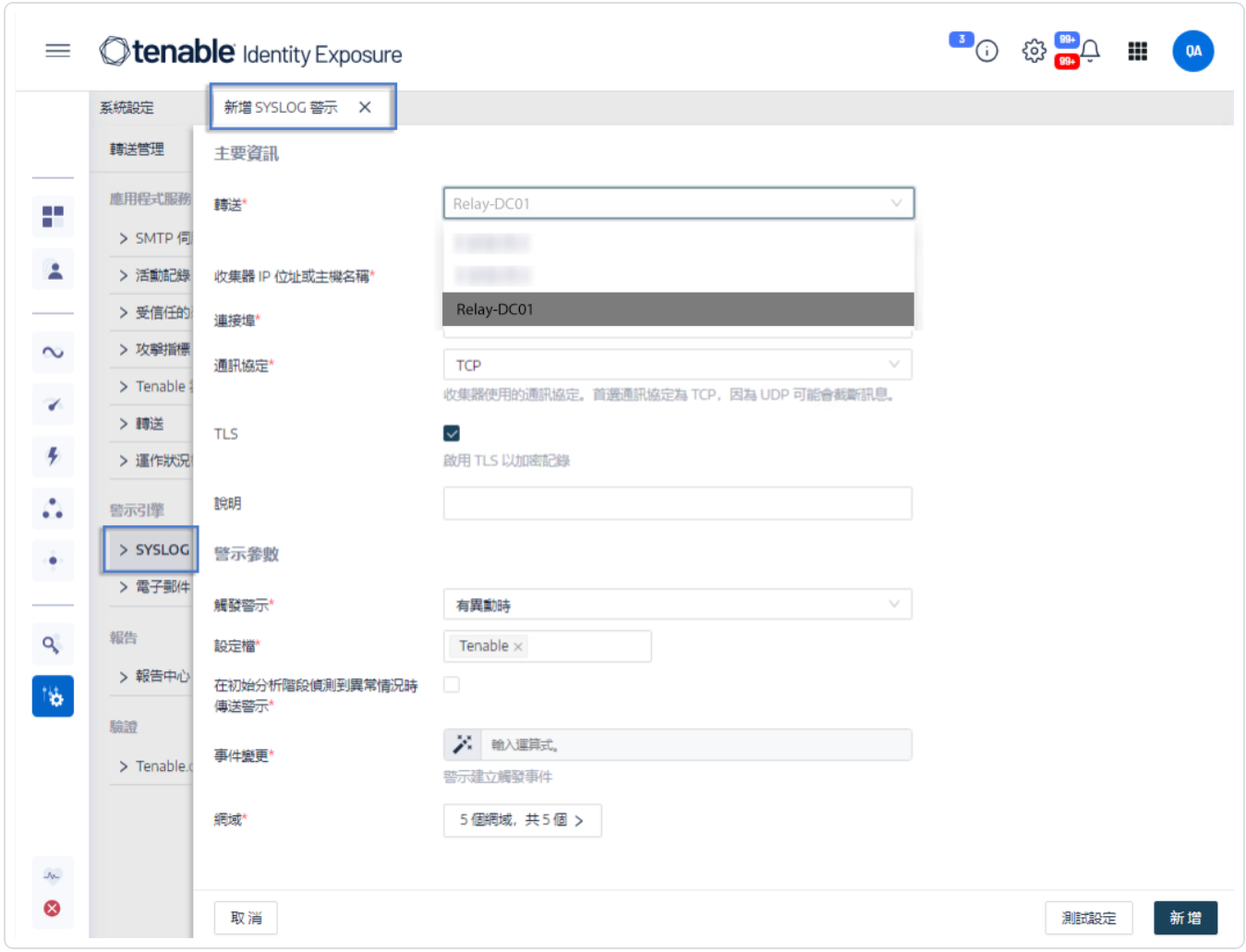
## Syslog 警示

有些組織使用 SIEM (安全性資訊與事件管理) 來收集有關潛在威脅和安全性資安事端的記錄。Tenable Identity Exposure 可將與 Active Directory 相關的安全性資訊推送至 SIEM Syslog 伺服器，以改進其警示機制。

### 新增 Syslog 警示

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「設定」**>**「Syslog」**。
2. 按一下右側的**「新增 Syslog 警示」**按鈕。

   **「新增 Syslog 警示」**窗格會隨即顯示。




3. 在「**主要資訊**」區段下方提供下列資訊：

   - **如果您的網路使用安全轉送：**在「**轉送**」方塊中按一下箭頭，從下拉式清單中選取要與 SIEM 通訊的轉送。
   - 在「**收集器 IP 位址或主機名稱**」方塊中輸入接收通知的伺服器 IP 或主機名稱。
   - 在「**連接埠**」方塊中輸入收集器的連接埠號碼。
   - 在「**通訊協定**」方塊中，按一下箭頭選取 UDP 或 TCP。
     - 如果您選擇 TCP，想要啟用 TLS 安全性通訊協定來加密記錄，請選取「**TLS**」選項核取方塊。
   - 在「**描述**」方塊中輸入有關收集器的簡要描述。

4. 在「**觸發警示**」下拉式清單中，選取一個選項：

   - **變更時**：只要發生您指定的事件，Tenable Identity Exposure 就會發出通知。
   - **每次發生異常情況時**：Tenable Identity Exposure 會在每次偵測到異常曝險指標 (IoE) 時發出通知。
   - **每次發生攻擊時**：Tenable Identity Exposure 會在每次偵測到異常攻擊指標 (IoA) 時發出通知。
   - **每次運作狀況檢查狀態變更時**：Tenable Identity Exposure 會在每次運作狀況檢查狀態變更時發出通知。

5. 在「**設定檔**」方塊中按一下，選取要用於此 Syslog 警示的設定檔 (若適用)。
6. **在初始分析階段偵測到異常情況時傳送警示**：執行下列任一動作 (若適用)：

   - 選取核取方塊：當系統重新啟動觸發警示時，Tenable Identity Exposure 會傳送大量 Syslog 訊息。
   - 取消選取核取方塊：當系統重新啟動觸發警示時，Tenable Identity Exposure 不會傳送 Syslog 訊息。

7. **嚴重性臨界值**：按一下下拉式方塊的箭頭，可選取 Tenable Identity Exposure 傳送警示時的臨界值 (若適用)。
8. 視您在前面步驟中選取的警示觸發程序而定：

   - **事件變更**：如果您將警示設定為「**變更時**」觸發，請輸入一個運算式來觸發事件通知。

     您可以按一下  圖示以使用搜尋精靈，或在搜尋方塊中輸入查詢運算式，然後按一下「**驗證**」。如需詳細資訊，請參閱 自訂追蹤流程查詢。

     > **注意**：Tenable Identity Exposure 會在收到事件後立即套用此篩選器，以便在執行任何其他安全性分析之前將事件轉送至 Syslog。因此，依賴擴充或後處理資料的篩選器在此階段將無法運作。

   - **曝險指標**：如果您將警示設定為**每次發生異常情況時**觸發，請按一下每個嚴重性等級旁邊的箭頭，以展開曝險指標清單並選取要傳送警示的指標。

- **攻擊指標**：如果您將警示設定為**每次發生攻擊時**觸發，請按一下每個嚴重性等級旁邊的箭頭，以展開攻擊指標清單並選取要傳送警示的指標。
- **運作狀況檢查狀態變更**：按一下**「運作狀況檢查」**，選取要觸發警示的運作狀況檢查類型，然後按一下**「篩選選取的項目」**。

9. 按一下**「網域」**方塊，以選取 Tenable Identity Exposure 要傳送警示的網域。

   **「樹系和網域」**窗格會隨即顯示。

   a. 選取樹系或網域。

   b. 按一下**「篩選選取的項目」**。

10. 按一下**「測試設定」**。

    系統會顯示一則訊息，確認 Tenable Identity Exposure 已傳送 Syslog 警示至伺服器。

11. 按一下**「新增」**。

    系統將顯示一則訊息，確認 Tenable Identity Exposure 已建立 Syslog 警示。

### 編輯 Syslog 警示

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「設定」**>**「Syslog」**。
2. 在 Syslog 警示清單中，將游標停留在您要修改的警示上，然後按一下此行末尾的 圖示。

   **「編輯 Syslog 警示」**窗格會隨即顯示。

3. 按照前文**「**新增 Syslog 警示**」**程序中所述進行必要的修改。
4. 按一下**「編輯」**。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新警示。

### 刪除 Syslog 警示

1. 在 Tenable Identity Exposure 中，按一下**「系統」**>**「設定」**>**「Syslog」**。
2. 在 Syslog 警示清單中，將游標停留在您要刪除的警示上，然後按一下此行末尾的 圖示。

系統會顯示一則訊息，要求您確認刪除。

3. 按一下「**刪除**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已刪除警示。

## 另請參閱

- Syslog 和電子郵件警示詳細資料

## Syslog 和電子郵件警示詳細資料

當您啟用 Syslog 或電子郵件警示時，Tenable Identity Exposure 會在偵測到異常情況、攻擊或變更時發出通知。

**注意**：在您收到攻擊指標 (IoA) 警示之前，會有需要考慮的攝取時間。此延遲與您在設定 Syslog 和電子郵件警示時，在「測試設定」階段觀察到的時間不相同。因此，請勿使用來自測試設定的持續時間作為基準，與實際攻擊所觸發的警示時間進行比較。

### 警示標頭

Syslog 警示標頭 (RFC-3164) 使用常見事件格式 (CEF)，這是整合安全性資訊與事件管理 (SIEM) 解決方案中的常用格式。

曝險指標 (IoE) 的警示範例

曝險指標 (IoE) 警示標頭

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "0" "1" "Alsid Forest" "emea.corp" "C-PASSWORD-DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-DONT-EXPIRE-SET" "2434" "TrusteeCn"="Gustavo Fring"
```

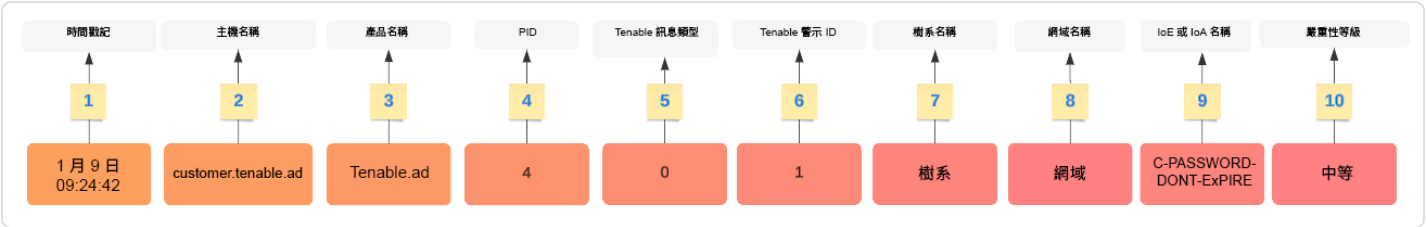
攻擊指標 (IoA) 的警示範例

攻擊指標 (IoA) 警示標頭

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "2" "1337" "Alsid Forest" "emea.corp" "DC Sync" "medium" "yoda.alsid.corp" "10.0.0.1" "antoinex1x.alsid.corp" "10.1.0.1" "user"="Gustavo Fring" "dc_name"="MyDC"
```

### 警示資訊

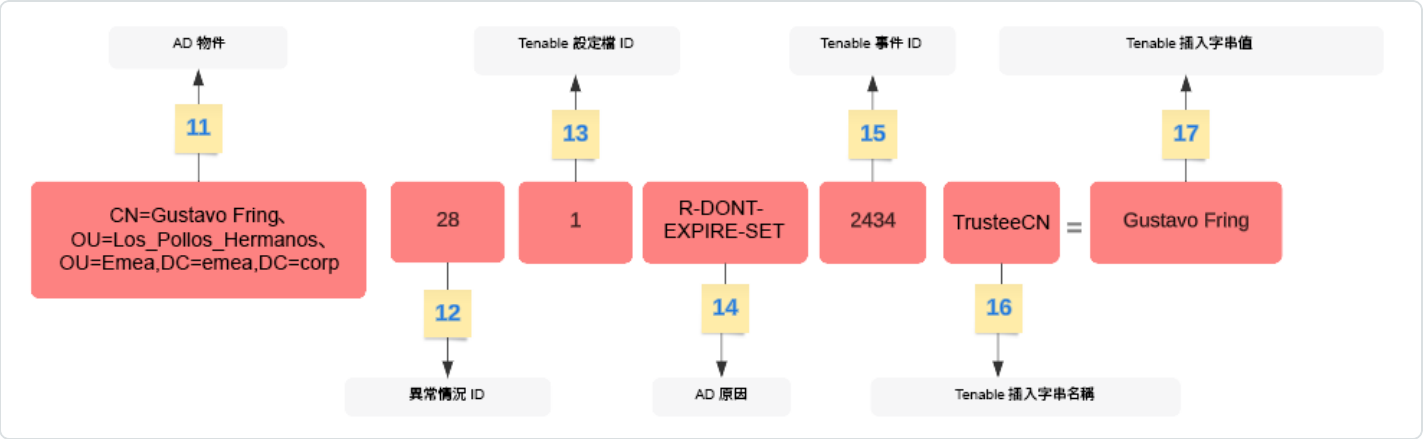
通用元素




標頭結構包含下列部分，如表格中所述。

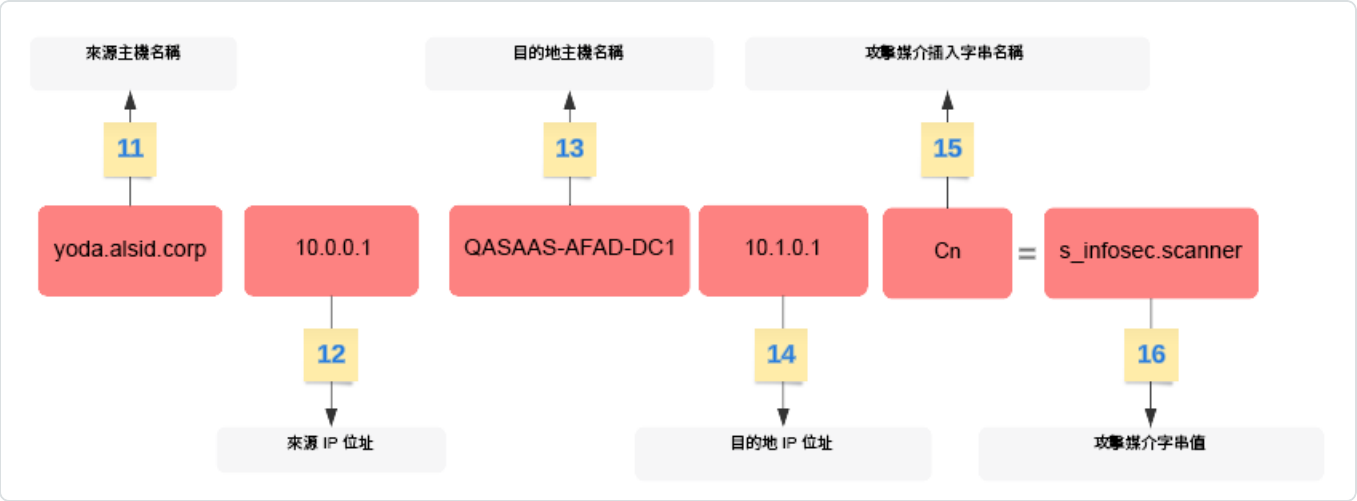
| 部分 | 說明 |
|---|---|
| 1 | **時間戳記**：偵測的日期。範例：「Jun 7 05:37:03」 |
| 2 | **主機名稱**：應用程式的主機名稱。範例：「customer.tenable.ad」 |
| 3 | **產品名稱**：觸發異常情況的產品名稱。範例：「TenableAD」、「AnotherTenableADProduct」 |
| 4 | **PID**：產品 (Tenable Identity Exposure) ID。範例：[4] |
| 5 | **Tenable 訊息類型**：事件來源的識別碼。範例：「0」(= 每個異常情況)、「1」(= 變更)、「2」(= 每次攻擊)、「3」(= 運作狀況檢查狀態變更) |
| 6 | **Tenable Alert ID**：警示的唯一 ID。範例：「0」、「132」 |
| 7 | **樹系名稱**：相關事件的樹系名稱。範例：「Corp Forest」 |
| 8 | **網域名稱**：與事件相關的網域名稱。範例：「tenable.corp」、「zwx.com」 |
| 9 | **Tenable 代碼名稱**：曝險指標 (IoE) 或攻擊指標 (IoA) 的代碼名稱。範例：「C-PASSWORD-DONT-EXPIRE」、「DC Sync」。 |
| 10 | **Tenable 嚴重性等級**：相關異常情況的嚴重性等級。範例：「嚴重」、「高度」、「中等」 |

曝險指標 (IoE) 的特定元素




| 部分 | 說明 |
| --- | --- |
| 11 | **AD 物件**：異常物件的辨別名稱。範例：「CN=s_ infosec.scanner,OU=ADManagers,DC=domain,DC=local」 |
| 12 | **Tenable 異常情況 ID**：異常情況的 ID。範例：「24980」、「132」、「28」 |
| 13 | **Tenable 設定檔 ID**：Tenable Identity Exposure 觸發異常情況的相關設定檔 ID。範例：「1」(Tenable)、「2」(sec_team) |
| 14 | **AD 原因代碼名稱**：異常情況產生原因的代碼名稱。範例：「R-DONT-EXPIRE-SET」、「R-UNCONST-DELEG」 |
| 15 | **Tenable 事件 ID**：觸發異常情況的事件 ID。範例：「40667」、「28」 |
| 16 | **Tenable 插入字串名稱**：異常物件觸發的屬性名稱。範例：「Cn」、「useraccountcontrol」、「member」、「pwdlastset」 |
| 17 | **Tenable 插入字串值**：異常物件觸發的屬性值。範例：「s_infosec.scanner」、「CN=Backup Operators,CN=Builtin,DC=domain,DC=local」 |

攻擊指標 (IoA) 的特定元素




| 部分 | 說明 |
| --- | --- |
| 11 | **來源主機名稱**：攻擊主機的主機名稱。值也可以是「Unknown」。 |
| 12 | **來源 IP 位址**：攻擊主機的 IP 位址。值可以是 IPv4 或 IPv6。 |
| 13 | **目的地主機名稱**：遭攻擊主機的主機名稱。 |
| 14 | **目的地 IP 位址**：遭攻擊主機的 IP 位址。值可以是 IPv4 或 IPv6。 |
| 15 | **攻擊媒介插入字串名稱**：異常物件觸發的屬性名稱。 |
| 16 | **攻擊媒介插入字串值**：異常物件觸發的屬性值。 |

### Syslog 訊息框架

- 針對 UDP 和 TCP syslog 設定，Tenable Identity Exposure 依據 RFC-6587#3.4.2 使用非透明框架方法來分隔訊息。框架字元為 LF (\n)。
- 針對具有 TLS 的 TCP，Tenable Identity Exposure 使用 RFC-6587#3.4.1 中所述的八位元組計數方法。

## 範例

**追蹤流程事件詳細資料**

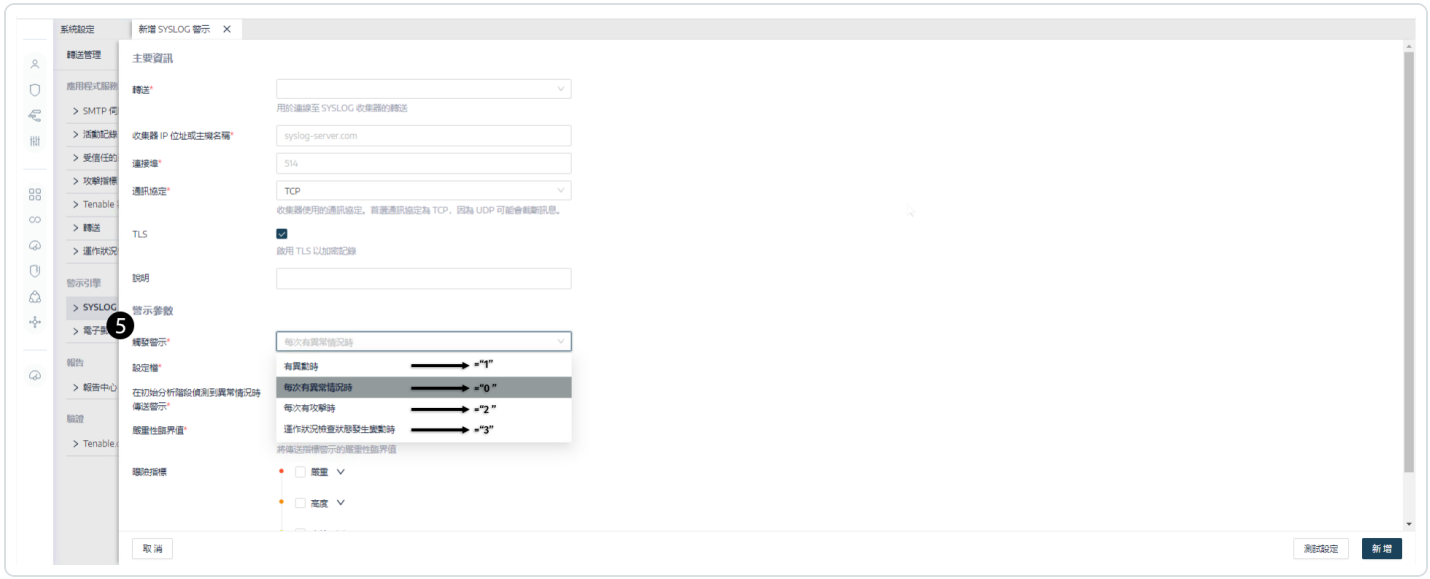
以下範例顯示追蹤流程中事件的詳細資料，其中包含以下內容：

- 時間戳記 (1)
- 異常物件名稱 (11)
- 樹系 (7) 和網域 (8) 名稱
- 異常物件觸發的屬性值 (17)




## 事件來源

此範例顯示事件的來源 (5)。您可以在 Syslog 設定頁面中設定此參數。如需詳細資訊，請參閱 Syslog 警示。




## 警示 ID

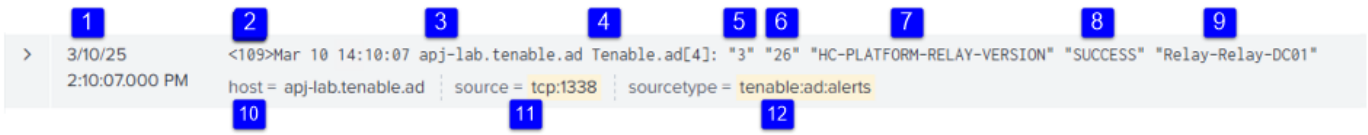
此範例顯示警示的唯一 ID (6)，您可以在 Tenable Identity Exposure 的「系統」>「設定」>「電子郵件」中已設定的電子郵件地址清單中看到。




## 運作狀況檢查

此範例顯示 Tenable Identity Exposure 在您的環境中執行的運作狀況檢查結果。如需詳細資訊，請參閱 運作狀況檢查。



標頭結構包含下列部分，如表格中所述。

| 部分 | 說明 |
|---|---|
| 1 | **時間戳記**：表示偵測到事件的日期和時間。 |
| 2 | **Syslog 優先順序**：這是 syslog 優先順序值，結合了設備和嚴重性等級 (RFC-3164) |
| 3 | **主機名稱**：產生警示的應用程式或裝置的主機名稱。 |
| 4 | **產品名稱和 PID**：指定產品名稱及其處理程序 ID。 |
| 5 | **Tenable 訊息類型**：事件來源的識別碼。範例：「0」(= 每個異常情況)、「1」(= 變更)、「2」(= 每次攻擊)、「3」(= 運作狀況檢查狀態變更) |
| 6 | **Tenable Alert ID**：警示的唯一 ID。範例：「0」、「132」 |
| 7 | **Health Check Codename**：表示執行的特定運作狀況檢查。如需詳細資訊，請參閱 運作狀況檢查。 |
| 8 | **運作狀況檢查狀態**：表示運作狀況檢查的結果。 |
| 9 | **轉送名稱或網域名稱**：識別與此運作狀況檢查相關的轉送或網域控制器。 |
| 10-12 | **中繼資料欄位**：<br>• Host (10)：重複主機名稱以供索引和搜尋之用。<br>• Source (11)：指定記錄的來源。<br>• Sourcetype (12)：分類記錄格式以進行剖析和分析。 |

## 運作狀況檢查

Tenable Identity Exposure 中的**運作狀況檢查功能**讓您可以在整合檢視畫面中即時查看網域和服務帳戶的設定，藉此向下切入調查會導致基礎架構中出現連線或其他問題的任何設定異常。它會驗證所有項目是否已正確設定，以確保 Tenable Identity Exposure 運作順暢，並讓您能夠採取快速精確的動作來解決問題，以及確保您的組態設定最適合讓 Tenable Identity Exposure 有效運作。

系統管理角色依預設可查看運作狀況檢查功能，而特定使用者角色可依權限查看此功能。您也可以在每次運作狀況檢查狀態變更時，建立 Syslog 或電子郵件警示。

## 運作狀況檢查和 DC 同步攻擊偵測

運作狀況檢查可提供有關 Tenable Identity Exposure 服務狀態和可用性的重要資訊。此功能可驗證服務帳戶是否能夠收集敏感資訊，例如用於特權分析的密碼雜湊和 DPAPI 備份金鑰。在運作狀況檢查報告中，Tenable 會嘗試收集敏感資料來判斷服務帳戶是否已正確設定「特權分析」功能，但若此功能未處於使用中狀態，則不會實際收集任何資料。為防止在此處理程序期間偵測 DCSync 攻擊，Tenable 會自動將所提供的 DCSync 攻擊指標服務帳戶列入白名單。

### 網域狀態

Tenable Identity Exposure 會針對每個網域執行下列檢查：

- AD 網域驗證：LDAP 設定和狀態、憑證和 SMB 存取權
- 網域可連線性：動態 RPC 連接埠的工作連線、可連線的 SMB 伺服器、可連線的網域控制器 IP 位址或 FQDN、RPC 連接埠的工作連線、可連線的 LDAP 伺服器，以及可連線的全域目錄 LDAP 伺服器。
- 權限：能夠存取 AD 網域資料和收集特權資料。
- 網域已連結至轉送：網域已正確關聯至轉送服務。
- 攻擊指標：網域控制器活動：Tenable Identity Exposure 會接收來自所有網域控制器的 Windows 事件記錄。
- 攻擊指標：網域安裝：確認 Tenable 攻擊指標 (IoA) GPO 設定正確無誤。

### 平台狀態

Tenable Identity Exposure 會針對您的平台設定執行下列檢查：

- 執行中的轉送服務：轉送設定是否正確包含疑難排解提示。
- 轉送版本一致性：轉送版本是否與 Tenable Identity Exposure 版本一致。
- 執行中的 AD 資料收集器服務：資料收集器服務、代理人和收集器橋接器是否可將資料轉送至其他服務。

**如要存取運作狀況檢查：**

1. 在 Tenable Identity Exposure 頁面左下角，將游標移動至  圖示上可查看基礎架構的全域狀態。
2. 按一下此圖示以開啟**「運作狀況檢查」**頁面。在**「網域狀態」**或**「平台狀態」**索引標籤下，您會看到下列任一項目：
   - 顯示已通過所有運作狀況檢查的訊息
   - 包含特定狀態的警告或問題清單：

| | |
|---|---|
|  | 檢查成功並顯示正常結果。 |
|  | 檢查失敗，並發現一個問題。 |
|  | 檢查失敗，但問題並未阻止 Tenable Identity Exposure 正確運作。<br><br>例如，如果服務帳戶無法收集特權資料，則資料收集檢查會因為用戶端上的 Active Directory 錯誤設定而導致失敗。不過，這不是嚴重問題，因為您尚未在 Tenable Identity Exposure 中的此網域上啟動特權分析功能，因此會出現警告。但是如果您啟動特權分析，檢查會立即失敗。 |
|  | 由於相依檢查失敗，檢查會顯示未知結果。例如，如果驗證檢查失敗，則無法進行網路連線性檢查。 |

**如要查看所有運作狀況檢查：**

- 在右側的運作狀況檢查清單上方，按一下**「顯示成功的檢查」**切換為啟用，以列出 Tenable Identity Exposure 已執行的所有檢查並包含下列資訊：
  - 運作狀況檢查名稱
  - 狀態 (通過、失敗、失敗但未阻礙正常運作或不明)
  - 受影響的網域及其相關聯的樹系 (僅適用於網域狀態檢查)
  - 上次執行檢查的時間
  - 檢查保持此狀態的時間

**如要重新整理運作狀況檢查頁面：**

- 雖然 Tenable Identity Exposure 會定期執行運作狀況檢查，但它不會用結果即時更新此頁面。按一下  以重新整理結果清單。

**如要依運作狀況檢查類型或依網域篩選結果：**

1. 在右側的運作狀況檢查清單上方，按一下**「n/n 運作狀況檢查」**或**「n/n 網域」**(僅限網域狀態)。

   **「運作狀況檢查」**或**「樹系和網域」**窗格會隨即開啟。

2. 選取運作狀況檢查類型或樹系/網域 (若適用)，然後按一下**「篩選選取的項目」**。

**如要深入瞭解每項運作狀況檢查的詳細資訊：**

1. 在運作狀況檢查清單中，按一下某個運作狀況檢查名稱或行尾的藍色箭頭 (→)。

   **「詳細資料」**窗格會隨即開啟，並顯示此檢查的相關描述和相關詳細資料清單。如需詳細資訊，請參閱下方的運作狀況檢查清單。

2. 按一下詳細資料行末尾的箭頭，將其展開並顯示有關結果的更多資訊。

**如要隱藏運作狀況檢查狀態圖示：**

根據預設，Tenable Identity Exposure 會在畫面的左下角顯示運作狀況檢查狀態圖示。

1. 在 Tenable Identity Exposure 中，前往左側導覽列中的**「系統」**，然後選取**「設定」**索引標籤。

   或者，您可以按一下「運作狀況檢查」頁面右上角的 ，然後選取**「設定」**。

2. 在**「應用程式服務」**下，選取**「運作狀況檢查」**。

3. 按一下**「顯示全域運作狀況檢查狀態」**切換為停用。

   Tenable Identity Exposure 會隱藏畫面左下角的運作狀況檢查圖示。

**如要指派運作狀況檢查權限給使用者角色：**

1. 在 Tenable Identity Exposure 中，前往左側導覽列中的**「帳戶」**，然後選取**「角色管理」**索引標籤。
2. 在角色清單中選取使用者角色，然後按一下行尾的 。

   **「編輯角色」**窗格會隨即開啟。
3. 選取**「系統設定實體」**索引標籤。
4. 選取**「運作狀況檢查」**實體，然後按一下權限切換開關，將權限從**「未授權」**切換為**「已授權」**。
5. 按一下**「套用並關閉」**。

如需有關權限的詳細資訊，請參閱設定角色的權限。

**如要設定運作狀況檢查狀態變更警示：**

1. 在 Tenable Identity Exposure 中，前往左側導覽列中的**「系統」**，然後選取**「設定」**索引標籤。

   或者，您可以按一下**「運作狀況檢查」**頁面右上角的 ，然後選取**「警示」**。
2. 在**「警示引擎」**下，選取**「Syslog」**或**「電子郵件」**。
3. 按一下**「新增 Syslog 警示」**或**「新增電子郵件警示」**。

   新窗格會隨即開啟。如需完整程序，請參閱警示。
4. 在**「警示參數」**下的**「觸發警示」**方塊中，從下拉式功能表中選取**「運作狀況檢查狀態變更時」**。
5. 按一下**「運作狀況檢查」**方塊中的箭頭，選取要觸發警示的運作狀況檢查類型，然後按一下**「篩選選取的項目」**。
6. 按一下**「新增」**。

## 運作狀況檢查清單

| 運作狀況檢查名稱 | 類型 | 檢查描述 | 詳細資料 |
|---|---|---|---|
| 網域連線性 | 網域 | 可與 AD 網域連線。 | • 可連線的網域控制器 IP 位址或 |

| | | | |
|---|---|---|---|
| (HC-DOMAIN-REACHABILITY) | | | FQDN<br>• 可連線的全域目錄 LDAP 伺服器<br>• 可連線的 LDAP 伺服器<br>• 可連線的 SMB 伺服器<br>• 與動態 RPC 連接埠的正常連線<br>• 與 RPC 連接埠的正常連線 |
| AD 網域驗證<br>(HC-DOMAIN-AUTHENTICATION) | 網域 | 可在 AD 網域中進行驗證。 | • 有效憑證<br>• 閒置的 LDAP 伺服器<br>• 可用的 LDAP 伺服器<br>• 已授予 LDAP 存取權<br>• 已授予 SMB 存取權 |
| 收集 AD 網域資料的權限<br>(HC-DOMAIN-DATA-COLLECTION) | 網域 | 可收集 AD 網域資料。 | • 收集特權資料的已授予權限 |
| 存取 AD 容器的權限<br>(HC-DOMAIN-CONTAINER-ACCESS) | 網域 | 可存取 AD 容器。 | • 存取已刪除物件容器的已授予權限<br>• 存取密碼設定容器的已授予權限 |

| | | | |
|---|---|---|---|
| 網域已連結至轉送<br><br>(HC-DOMAIN-LINKED-TO-RELAY) | 網域 | 網域已連結至轉送。 | • 網域已連結至轉送 |
| 攻擊指標 (IoA) - 網域控制器活動<br><br>(HC-DOMAIN-EVENT-LOGS-COLLECTION-DOMAIN-CONTROLLER-ACTIVITY) | 網域 | Tenable Identity Exposure 會接收來自所有網域控制器的 Windows 事件記錄。 | • 非作用中的網域控制器 |
| 監控的網域控制器具有 PDCe 角色<br><br>(HC-DOMAIN-PRIMARY-ROLE) | 網域 | 受監控的網域控制器擁有 PDC Emulator (PDCe) 角色，這對於某些安全性功能極為重要。 | • 確保曝險指標 (IoE) 和攻擊指標 (IoA) 以最佳狀態運作 |
| 攻擊指標 (IoA) - 網域安裝<br><br>(HC-DOMAIN-IOA-CONFIGURATION) | 網域 | 確認 Tenable 攻擊指標 (IoA) GPO 設定正確無誤。 | • LDAP 中存在 Tenable 攻擊指標 (IoA) GPO<br>• SYSVOL 中存在 Tenable IoA GPO 資料夾<br>• SYSVOL 中存在 Tenable IoA GPO IoA 資料夾<br>• SYSVOL 中存在 Tenable IoA GPO EVT 訂閱接聽程式檔案<br>• SYSVOL 中存在 Tenable IoA GPO 設定檔案 |

| | | | |
|---|---|---|---|
| | | | • SYSVOL 中存在 Tenable IoA GPO `audit.csv` 檔案 |
| 轉送服務已啟動<br>(HC-PLATFORM-RELAY-UP) | 平台 | 轉送目前正常運作。 | • 執行轉送服務 |
| 轉送服務版本<br>(HC-PLATFORM-RELAY-VERSION) | 平台 | 轉送版本與產品相符。 | • 轉送版本一致性 |
| AD 資料收集器已啟動<br>(HC-PLATFORM-AD-DATA-COLLECTOR-UP) | 平台 | AD 資料收集器目前正常運作。 | • 執行 AD 資料收集器橋接<br>• 執行 AD 資料收集器服務<br>• 執行代理程式 |
| Tenable 雲端與 Tenable Identity Exposure 服務之間的同步處理<br>(HC-PLATFORM-TENABLE-CLOUD-SYNC) | 平台 | 建立的 Tenable 雲端群組、權限和使用者與 Tenable Identity Exposure 資料庫同步。 | • Tenable 雲端可用性 |

## 報告中心

Tenable Identity Exposure 中的**報告中心**是一項非常重要的功能，可協助您將重要資料匯出成報告給組織內的主要利害關係人。報告中心提供使用預定義清單建立報告的方法，確保流程有效率且精簡。

所提供的功能如下：

- **精細篩選**：使用日期範圍、網域、攻擊指標 (IoA)、曝險指標 (IoE) 等條件的精細篩選器，讓報告完善精簡，以確保專心進行深入分析。
- **自動傳送**：排定自動產生報告，並依照所需的頻率傳送，簡化安全監控和報告程序。

- **彈性匯出**：匯出 CSV 等多種格式的報告，以便進一步分析、共用報告存取金鑰，或與現有報告工作流程整合。

系統管理員可針對不同使用者建立不同類型的報告，且報告時間範圍可彈性調整，最高為一季。組織如果能夠從 Tenable Identity Exposure 共用重要身分識別資料，就可以主動減輕風險，並發現潛在的身分識別型攻擊。

若要下載報告，使用者會收到一封包含頁面 URL 的電子郵件，使用者需要在此頁面中輸入他們從管理員處收到的報告存取金鑰。使用者可在 30 天內下載報告，超過 30 天後報告便會過期，Tenable Identity Exposure 會將之刪除。只有待使用者下載報告後，Tenable Identity Exposure 才能針對指定的時間範圍產生新的報告並覆寫先前的報告。

**如要存取報告中心：**

1. 在 Tenable Identity Exposure 中，選取「**系統**」>「**設定**」。
2. 在「**報告**」下方，按一下「**報告中心**」。

   窗格會隨即開啟，其中包含已設定的報告清單及其相關資訊，例如報告名稱、類型、網域、設定檔、期間、重複週期和收件者的電子郵件地址。

## Microsoft Entra ID 支援

除了 Active Directory，Tenable Identity Exposure 也支援 Microsoft Entra ID (前稱 Azure AD 或 AAD) 以擴展組織中的身分識別範圍。此功能會利用著重於 Microsoft Entra ID 特定風險的新曝險指標。

如要將 Microsoft Entra ID 與 Tenable Identity Exposure整合，請仔細依照以下入門程序操作：

1. 交由先決條件
2. 檢查權限
3. 配置 Microsoft Entra ID 設定
4. 啟用 Microsoft Entra ID 支援
5. 啟用租用戶掃描

## 先決條件

您需要 Tenable Cloud 帳戶，才能登入「cloud.tenable.com」並使用 Microsoft Entra ID 支援功能。此 Tenable Cloud 帳戶與您的歡迎電子郵件所使用的電子郵件地址相同。如果您不知道「cloud.tenable.com」的電子郵件地址，請聯絡支援服務。具有有效授權 (內部部署或 SaaS) 的所有客戶皆可存取位於「cloud.tenable.com」的 Tenable 雲端。此帳戶可讓您為 Microsoft Entra ID 設定 Tenable 掃描並且收集掃描結果。

**注意**：您不需要有效的 **Tenable Vulnerability Management** 授權也可存取 Tenable Cloud。目前有效的獨立 Tenable Identity Exposure 授權 (內部部署或 SaaS) 便已足夠。

**注意**：Tenable Identity Exposure **不支援國家雲端中的 Microsoft Entra ID**，包括中國和美國政府的專用區域。Microsoft Entra ID 提供國家雲端，其為實際隔離的 Azure 執行個體，專為滿足特定法規和合規性需求而設計。Tenable Identity Exposure 僅支援全球 Microsoft Entra ID 環境，不包括中國國家雲端和美國政府國家雲端。如需 Microsoft Entra ID 國家雲端的詳細資訊，請參閱 Microsoft Entra 驗證 & 國家雲端 - Microsoft 身分識別平台。

## 權限

Microsoft Entra ID 的支援需要收集來自 Microsoft Entra ID 的資料，例如使用者、群組、應用程式、服務主體、角色、權限、原則、記錄等等。它會遵循 Microsoft 的建議，使用 Microsoft Graph API 和服務主體憑證收集此資料。

- 根據 Microsoft 的說明，您必須**以有權在 Microsoft Graph 上授予全租用戶管理員同意的使用者身分登入 Microsoft Entra ID**，而這必須具有全域管理員或特殊權限角色管理員角色 (或任何具有適當權限的自訂角色)。
- 您的 **Tenable Identity Exposure 使用者角色**必須具備適當的權限，才能存取 Microsoft Entra ID 的設定和資料圖表。如需詳細資訊，請參閱設定角色的權限。

## 授權計數

**只有在 Tenable 雲端同步功能已啟用的情況下，**Tenable 才不會將重複的身分計入授權數。若未啟用此功能，系統就無法比對 Microsoft Entra ID 和 Active Directory 中的帳戶，因此必須分別計算每個帳戶。

- **未啟用 Tenable 雲端同步時**：同時擁有 AD 帳戶和 Entra ID 帳戶的使用者將被視為兩名獨立使用者，分別計入授權數。
- **啟用 Tenable 雲端同步時**：系統會將多個帳戶整合為單一身分，確保擁有多個帳戶的使用者只計算一次授權。

# 配置 Microsoft Entra ID 設定

使用下列程序 (改編自《Microsoft 快速入門：使用 Microsoft 身分識別平台註冊應用程式》說明文件)，設定 Microsoft Entra ID 中的所有必要設定。

1. **建立應用程式：**

   a. 在 Azure 管理入口網站中，開啟「**應用程式註冊**」頁面。

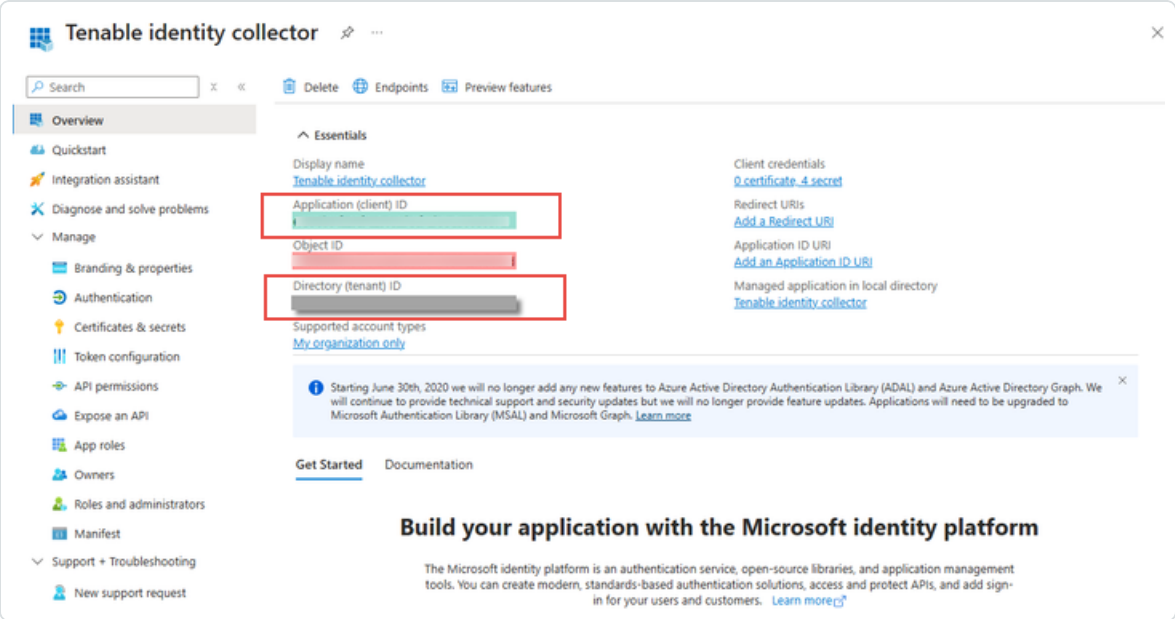
   b. 按一下「**+ 新註冊**」。

   c. 為應用程式命名 (例如：「Tenable Identity Collector」)。其他選項可以保留預設值。

   d. 按一下「**註冊**」。

   e. 在此新建立應用程式的「概覽」頁面上，記下「應用程式 (用戶端) ID」和「目錄 (租用戶) ID」，稍後在 如要新增 Microsoft Entra ID 租用戶： 步驟中將會需要這些資料

   > **注意**：請務必選取**應用程式 ID 而非物件 ID**，設定才能運作。




2. **新增憑證至應用程式：**

   a. 在 Azure 管理入口網站中，開啟「**應用程式註冊**」頁面。

   b. 按一下您建立的應用程式。

c. 在左側功能表中，按一下**「憑證與密碼」**。

d. 按一下**「+ 新用戶端密碼」**。

e. 在**「說明」**方塊中，提供此密碼的實際名稱，以及符合您原則的**「到期」**值。請記得在鄰近到期日前更新此密碼。

f. 將密碼值儲存在安全的位置，因為 Azure 只會顯示一次密碼值，而且一旦密碼遺失就必須重新建立。

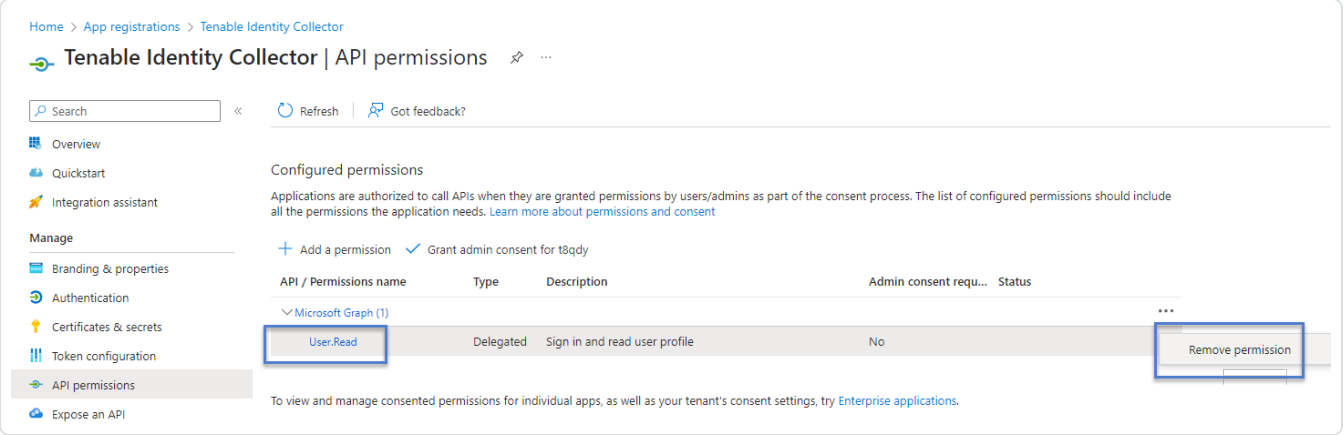
3. **指派權限給應用程式：**

a. 在 Azure 管理入口網站中，開啟**「應用程式註冊」**頁面。

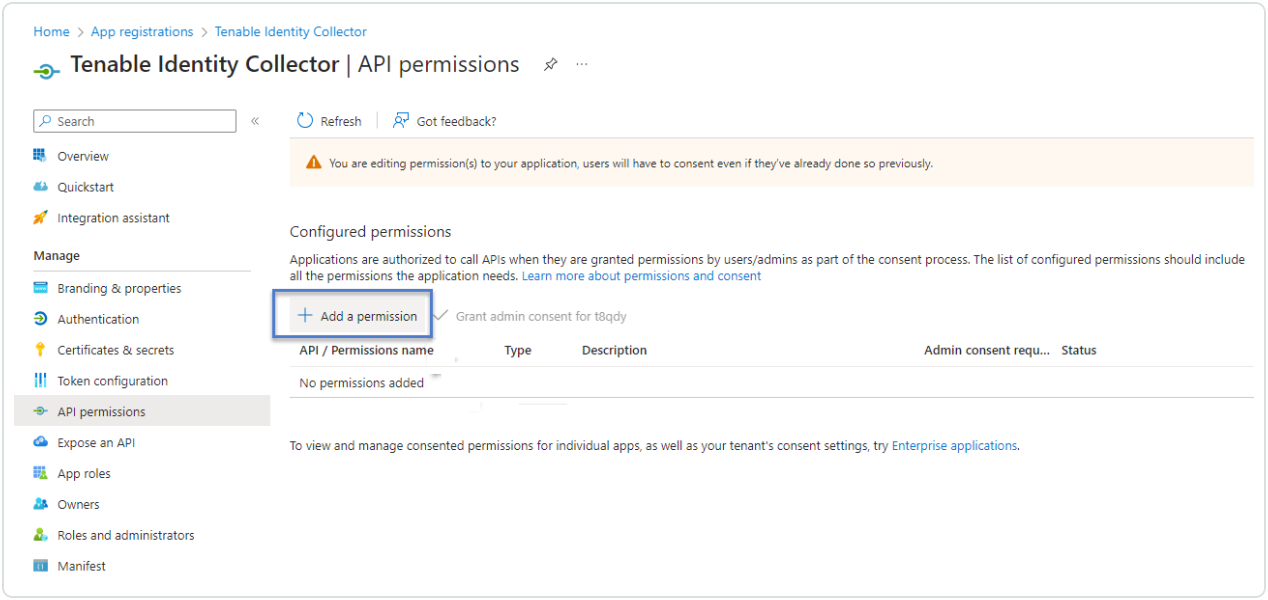
b. 按一下您建立的應用程式。

c. 在左側功能表中，按一下**「API 權限」**。

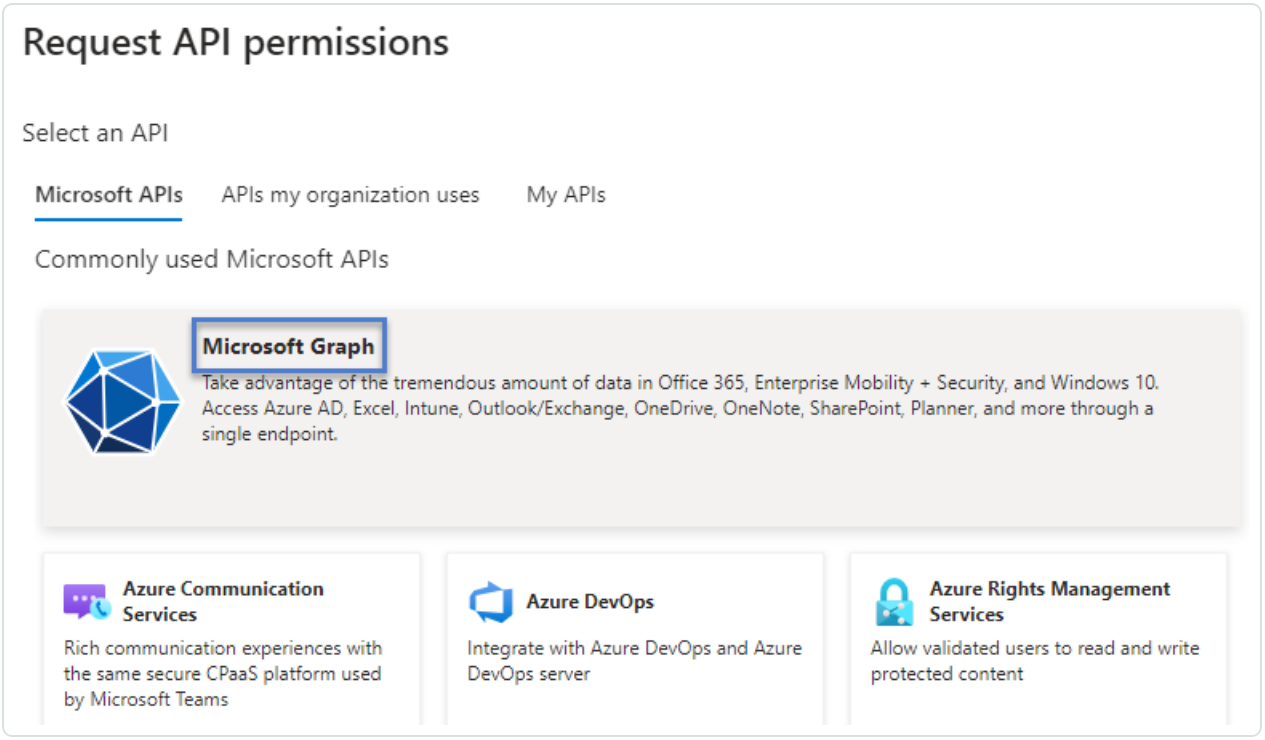
d. 移除現有的 `User.Read` 權限：



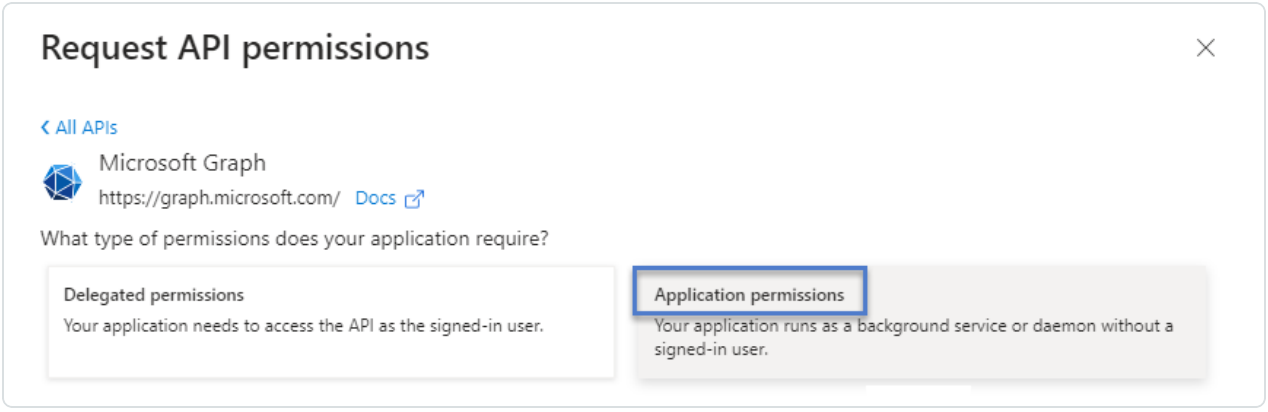

e. 按一下**「+ 新增權限」**：




f. 選取「**Microsoft Graph**」:




g. 選取「**應用程式權限**」(非「委派的權限」)。

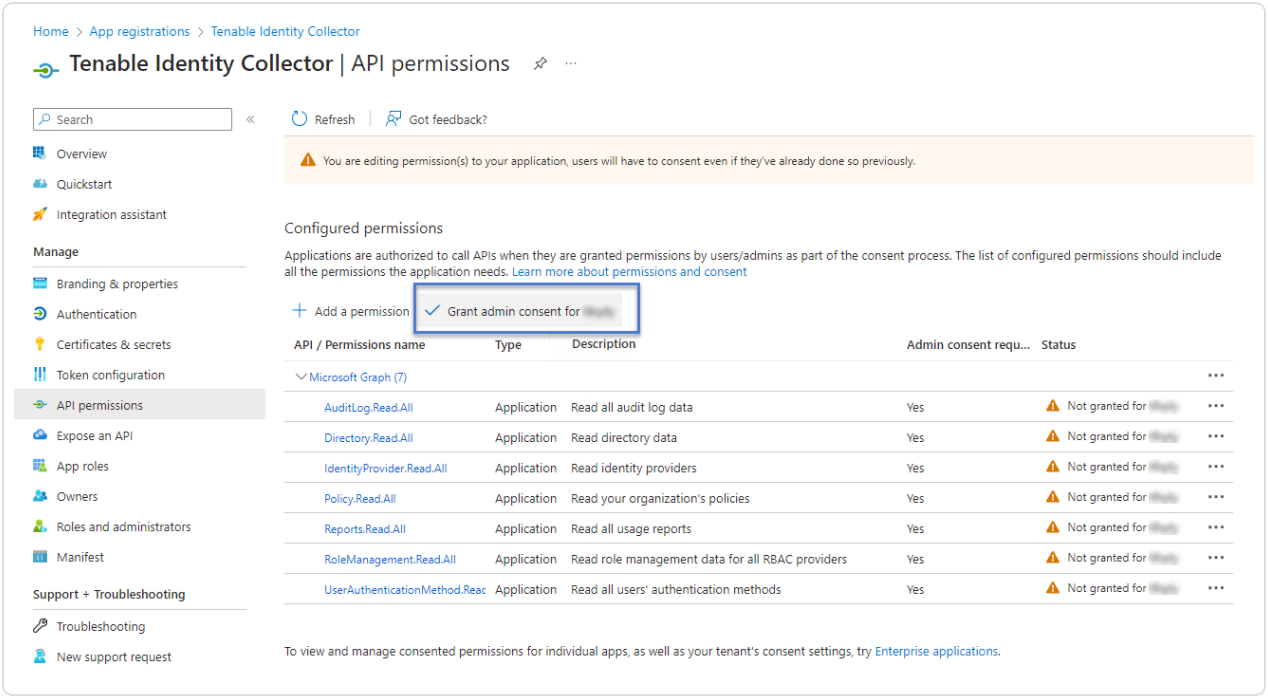


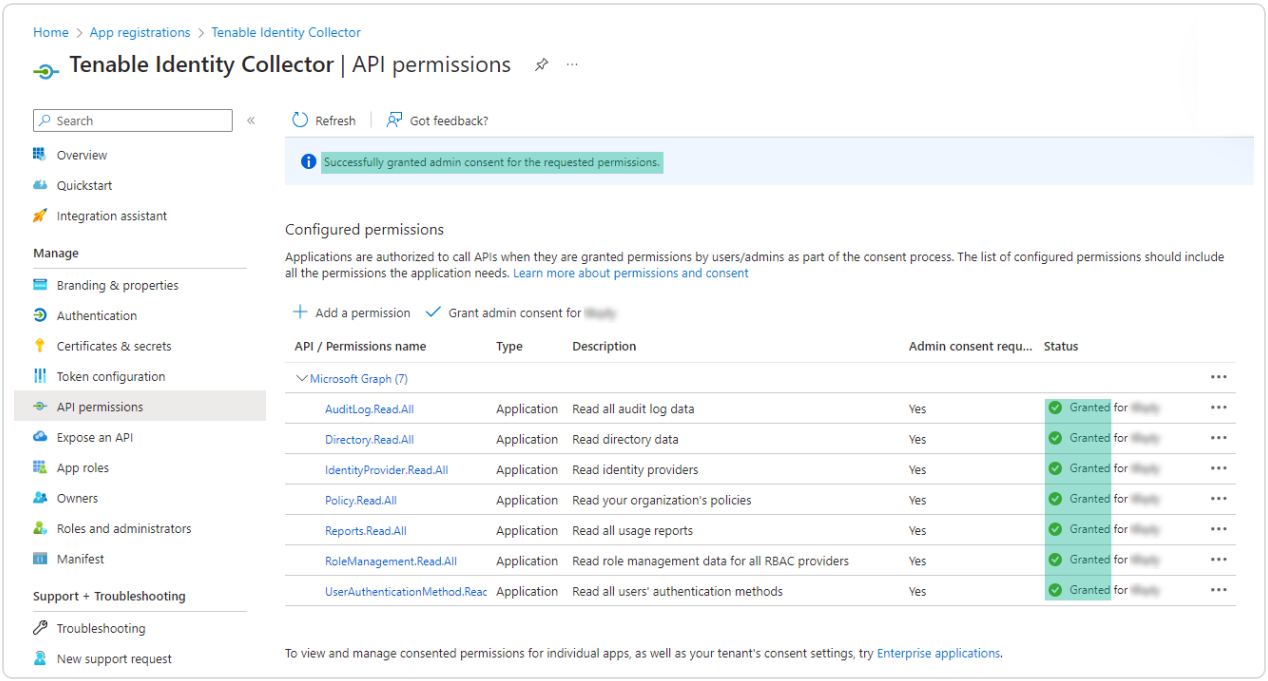

h. 使用清單或搜尋列，尋找並選取下列所有權限：

- `AuditLog.Read.All`
- `Directory.Read.All`
- `IdentityProvider.Read.All`
- `Policy.Read.All`
- `Reports.Read.All`
- `RoleManagement.Read.All`
- `UserAuthenticationMethod.Read.All`

i. 按一下**「新增權限」**。

j. 按一下**「向 <租用戶名稱> 授予管理員同意」**，然後按一下**「是」**確認：




4. 在 Microsoft Entra ID 中配置所有必要設定後：

   a. 在 Tenable Vulnerability Management 中建立 Microsoft Azure 類型的新憑證。

   b. 選取「金鑰」驗證方法，並輸入您在之前程序中擷取的值：租用戶 ID、應用程式 ID 和用戶端密碼。

## 啟用 Microsoft Entra ID 支援

- 若要使用 **Microsoft Entra ID**，您必須在 Tenable Identity Exposure 設定中啟用該功能。
- 如需指示，請參閱啟用 Identity 360、曝險中心和 Microsoft Entra ID 支援。

## 啟用租用戶掃描

**如要新增 Microsoft Entra ID 租用戶：**

新增租用戶連結 Tenable Identity Exposure 與 Microsoft Entra ID 租用戶，以便在該租用戶上執行掃描。

1. 在「設定」頁面中，按一下「**租用戶管理**」索引標籤。

   「**租用戶管理**」頁面隨即開啟。

2. 按一下「**新增租用戶**」。

   「**新增租用戶**」頁面隨即開啟。



3. 在「**租用戶名稱**」方塊中輸入名稱。
4. 在「**憑證**」方塊中，按一下下拉式清單以選取一個憑證。
5. 如果清單中沒有出現您的憑證，您可以：
    - 在 Tenable Vulnerability Management 中建立一個 (「Tenable Vulnerability Management」>「**設定**」>「**憑證**」)。如需詳細資訊，請參閱 Tenable Vulnerability Management 中的建立 Azure 類型憑證的程序。
    - 檢查您對於 Tenable Vulnerability Management 中的憑證是否擁有「可使用」或「可編輯」權限 。您必須具備這些權限，Tenable Identity Exposure 才會在下拉式清單中顯示憑證。
6. 按一下「**重新整理**」以更新憑證的下拉式清單。
7. 選取您建立的憑證。
8. 按一下「**新增**」。

    系統會顯示一則訊息，確認 Tenable Identity Exposure 已新增租用戶。現在，「租用戶管理」頁面的清單中會顯示此租用戶。

**針對租用戶啟用掃描：**

**注意**：租用戶掃描並非即時發生，至少需要 45 分鐘後，身分識別總管中才會顯示 Microsoft Entra ID 資料。

- 從清單中選取一個租用戶，然後按一下切換為「**已啟用掃描**」。




Tenable Identity Exposure 會要求對此租用戶進行掃描，掃描結果會顯示在「曝險指標」頁面中。

**注意**：兩次掃描之間必須至少間隔 **30 分鐘**。

## 重新整理 Entra ID 憑證

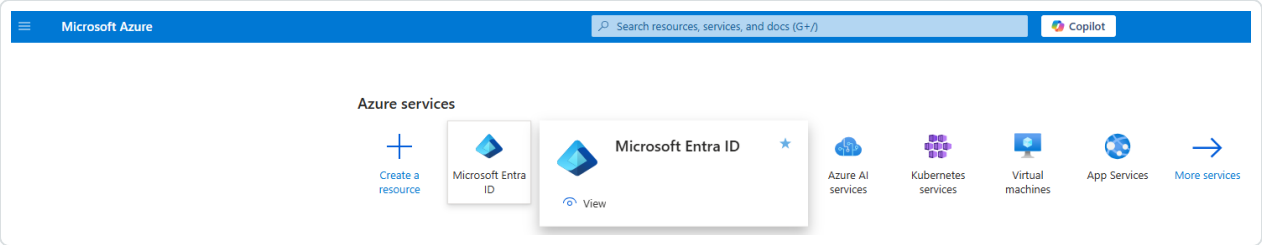
在 Microsoft Entra ID (前稱 Azure Active Directory) 中，憑證過期時間會因憑證類型和貴組織的設定而有所不同。

當您的 Entra ID 憑證過期時，Tenable 雲端會停止從 Entra ID 同步資產和弱點。您會看到一則警告訊息，指出連接器已停止運作。

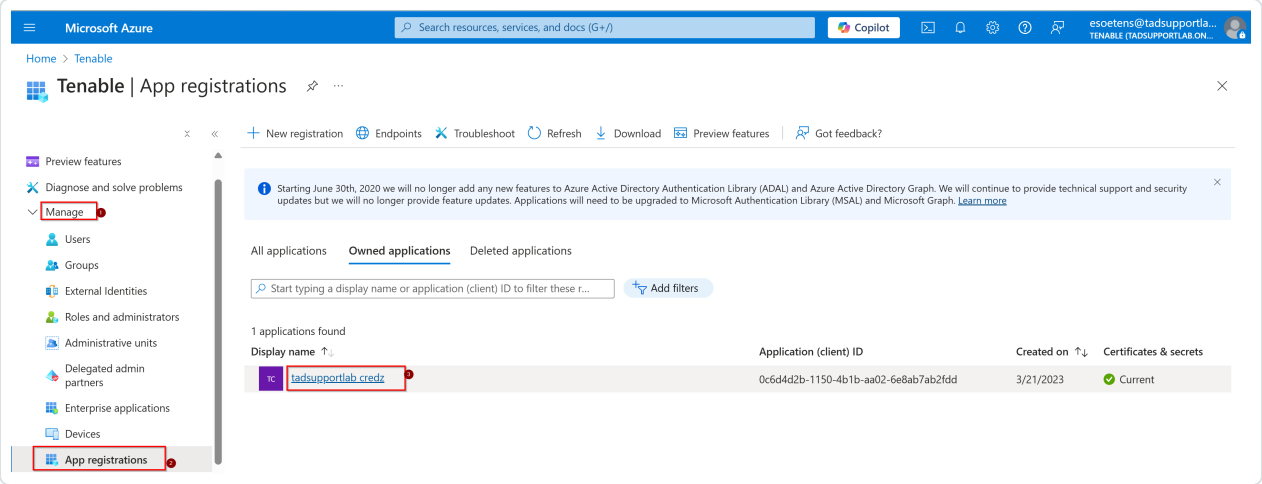
如要重新整理憑證並恢復同步，請按照下列步驟操作：

1. 存取 **Microsoft Entra ID**：

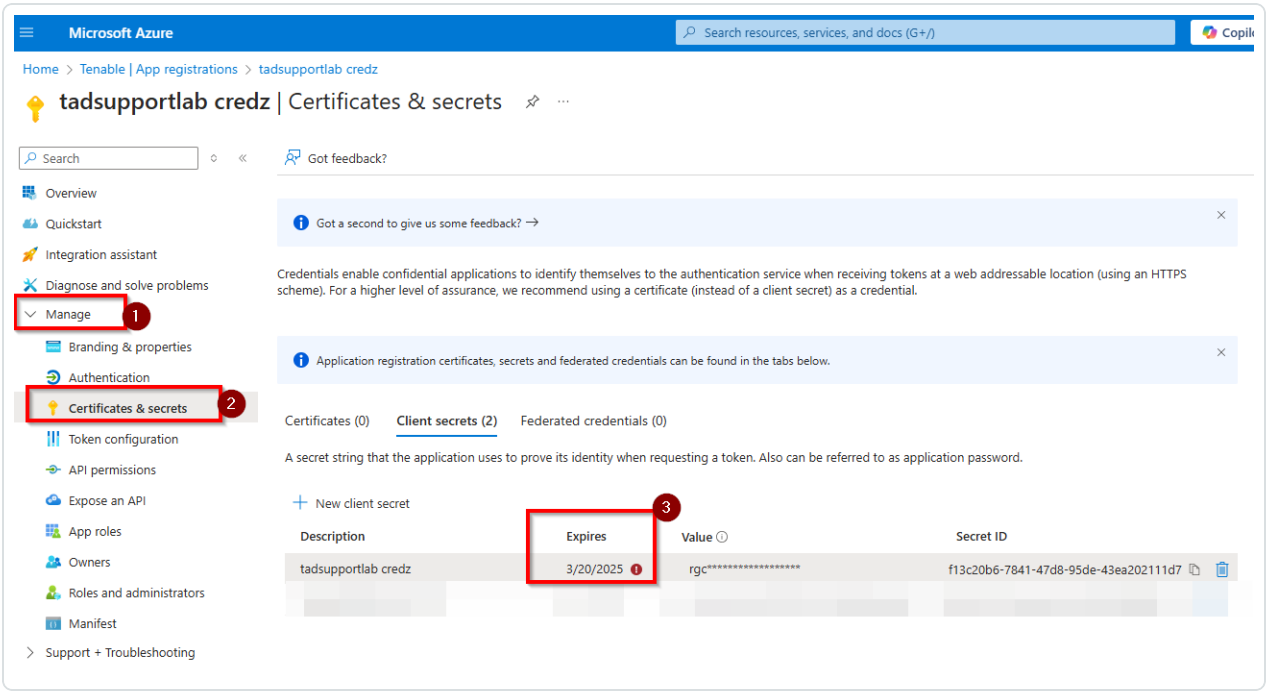
    a. 登入您的 Microsoft Entra ID 租用戶。




    b. 前往「**管理**」→「**應用程式註冊**」。



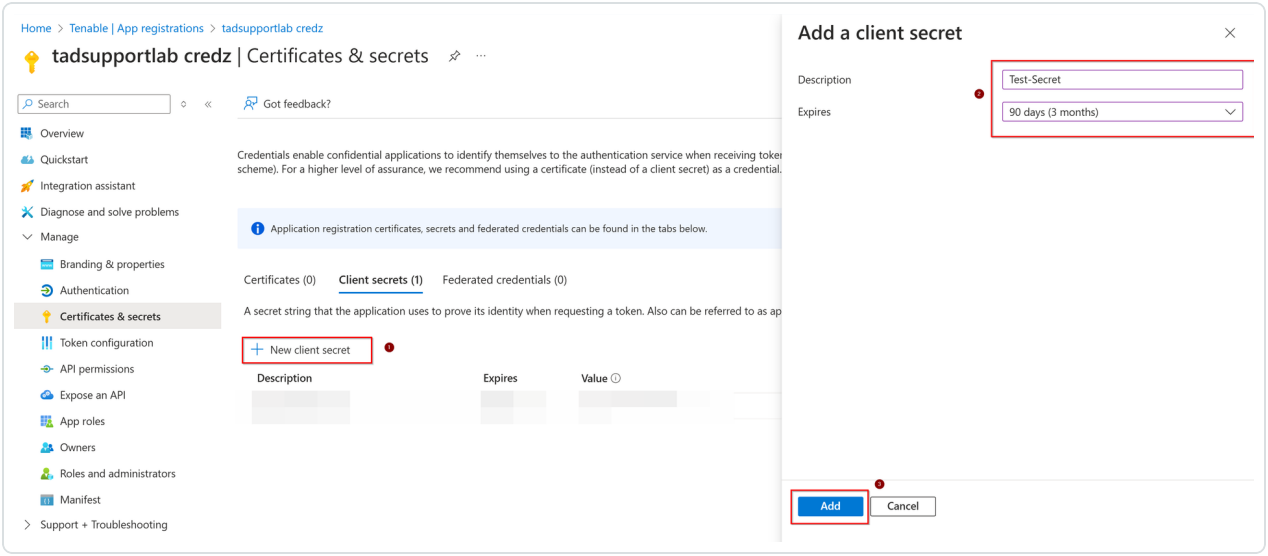
c. 選取您之前為 Tenable Identity Exposure 建立的應用程式。




2. 建立新的用戶端密碼：

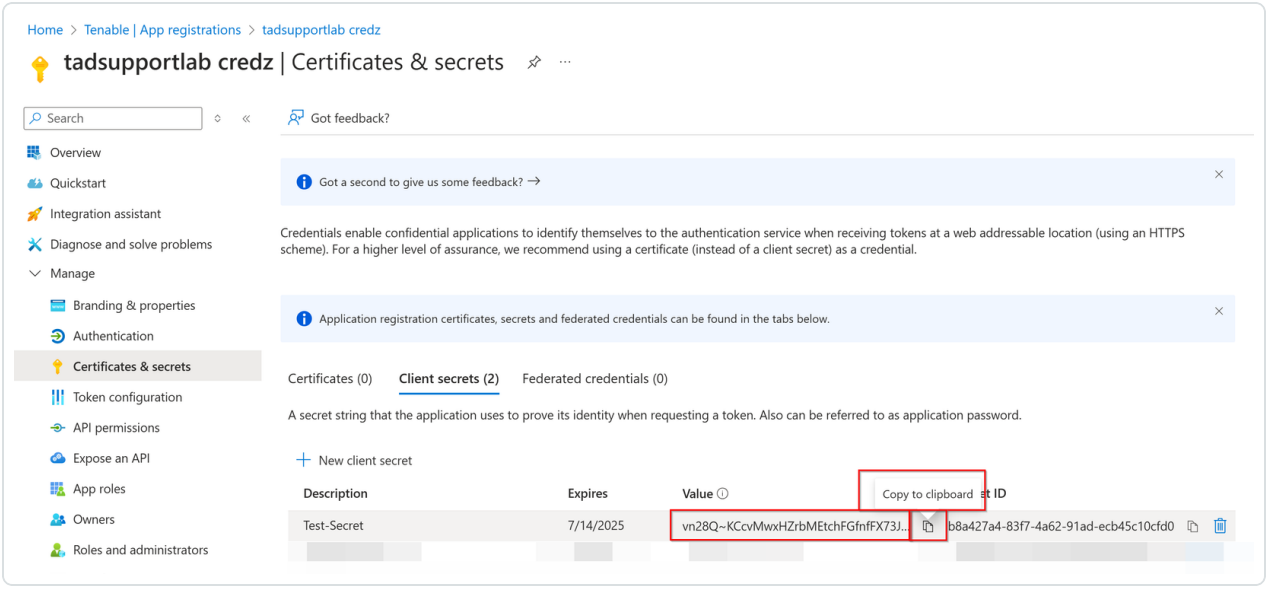
a. 在「**管理**」下方，按一下「**憑證與密碼**」。

b. 按一下「**+ 新用戶端密碼**」。




c. 輸入說明、設定有效期限 (例如 6 或 12 個月)，然後按一下「**新增**」。

d. **重要提示**：請立即複製**用戶端密碼值 (而非密碼 ID)**，並將其安全地儲存在密碼金庫。



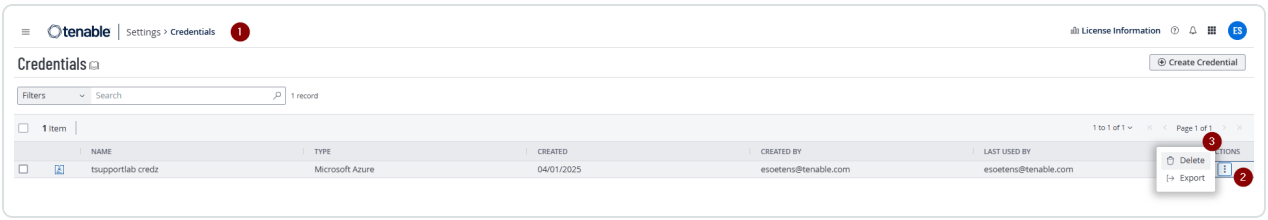

> **注意**：此步驟很重要，因為用戶端密碼值只會在建立的當下**顯示一次**。常見錯誤是複製密碼 ID (此資訊會一直顯示)，而不是實際的密碼值。

3. 更新 Tenable 雲端憑證：

   a. 登入 **Tenable 雲端**。

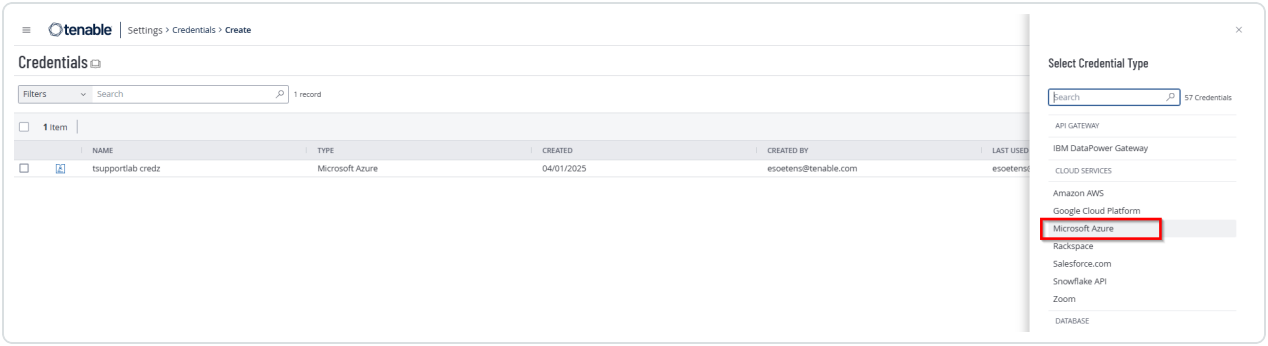
   b. 前往「**設定**」→「**憑證**」。

   c. 找到過期的憑證並將其刪除。




   d. 按一下右上角的「**建立憑證**」。

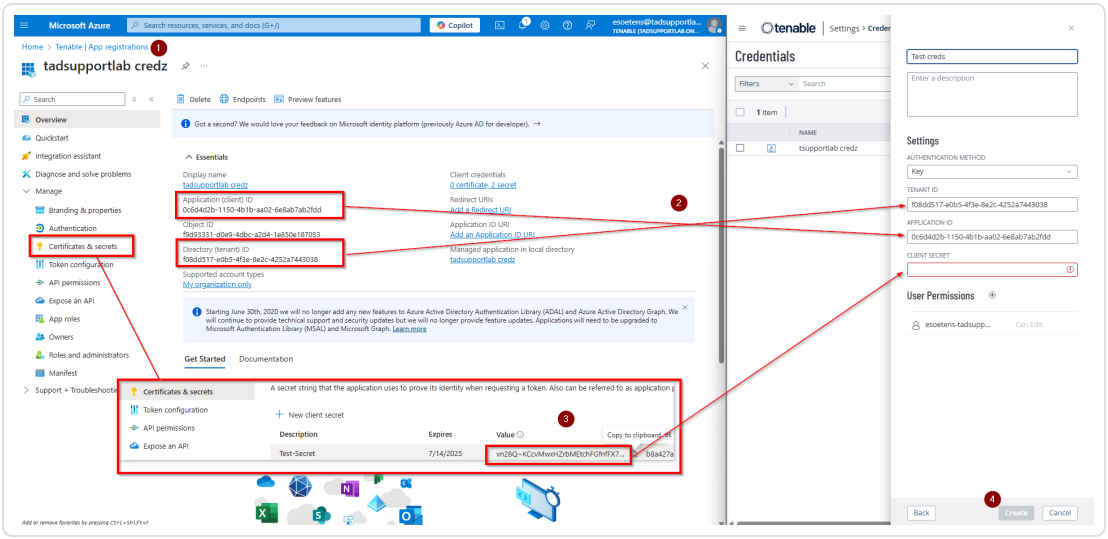
   e. 選取「**Microsoft Azure**」作為憑證類型。




f. 輸入以下內容：

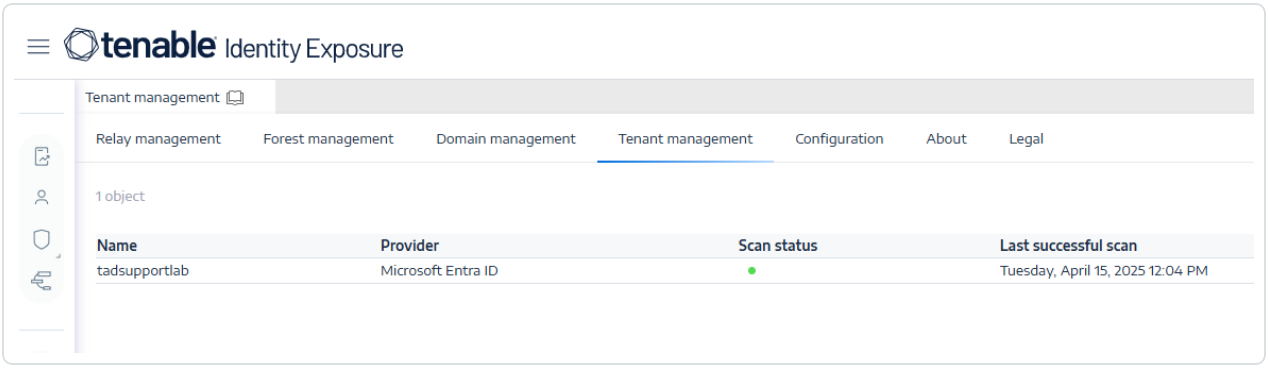
- Entra ID 應用程式註冊中的「**應用程式 ID**」和「**租用戶 ID**」。
- **用戶端密碼** (您之前複製的值)。

g. 按一下「**建立**」。



4. 確認狀態：

   - 儲存新憑證後，請檢查掃描狀態。




     - 綠色狀態表示成功。
     - 如果狀態為橘色，請確定您並未將密碼值和密碼 ID 搞混。如有必要，請從第 2 步開始重新執行。

## Tenable Cloud 資料收集

Tenable Cloud (Tenable Identity Exposure 中的資料收集功能) 可將您的資訊傳輸至其私有雲端，以提供安全性分析和服務。如需有關資料收集的詳細資訊，請參閱 Tenable的信賴與保障聲明。

如要使用 Tenable Cloud：

1. 在 Tenable Identity Exposure 中，按一下側邊導覽列上的「**系統**」，再按一下「**系統**」。

   「**系統設定**」窗格會隨即開啟。

2. 選取「**設定**」索引標籤。

3. 在「**應用程式服務**」區段下面，按一下「**Tenable Cloud**」。

   「**Tenable Cloud**」窗格會隨即開啟。

4. 按一下「使用 Tenable 雲端服務」切換為「**啟用**」。

系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新資訊傳輸設定。




## 特權分析

特權分析是 Tenable Identity Exposure 中的一個選用功能，需要更多權限才能擷取其他受保護的資料並提供更多安全性分析 (這點與其他功能相反)。

## 先決條件

若要使用「特權分析」，您必須開放動態 RPC 連接埠 **TCP/49152-65535** 和 **UDP/49152-65535**。如需其他資訊，請參閱Network Flow Matrix。

## 資料擷取

> 注意：特權分析功能需要更高的權限。請參閱 特權分析的存取權。

特權分析功能啟用後會擷取下列額外資料：

- **密碼雜湊**：Tenable Identity Exposure 擷取 LM 和 NT 雜湊以進行密碼分析。Tenable Identity Exposure 擷取 LM 雜湊只是為了警告它們的存在 (因為它們使用舊的弱式演算法)，但不會將其儲存。雜湊收集範圍包括：

- 所有已啟用的使用者帳戶
- 所有已啟用的網域控制器電腦帳戶

## 資料保護

Active Directory (AD) 本身不會直接儲存使用者密碼，而是僅儲存其使用 LM 或 NT 雜湊演算法的雜湊 (不允許復原原始密碼)。Tenable Identity Exposure 不儲存 LM 雜湊。

除了將轉送託管在 SAAS-VPN 平台上的客戶外，密碼不會離開客戶的基礎架構，因為只有轉送會處理這些密碼。轉送不會儲存密碼或密碼雜湊，而是會在每次需要分析時擷取使用者的密碼雜湊，將其暫時保留 (通常只會保留幾毫秒) 在快取中。

不過，Tenable Identity Exposure 會保留最少位數的密碼雜湊資料。這些資料會安全地儲存在轉送的 RAM 中，僅供執行 K-anonymity 分析使用，以檢查是否有使用者具有相同的密碼。

**注意**：對於 SaaS-VPN 平台用戶端，轉送的行為方式相同，但託管您轉送的是 Tenable。

## 活動記錄

Tenable Identity Exposure 中的活動記錄可用來檢視 Tenable Identity Exposure 平台上發生的所有活動痕跡，這些活動與特定 IP 位址、使用者或動作有關。

**如要設定活動記錄：**

1. 在 Tenable Identity Exposure 側邊導覽窗格中的**「管理」**下面，按一下**「系統」**。

   **「系統設定」**窗格會隨即開啟。

2. 在**「應用程式服務」**區段下面，按一下**「活動記錄」**。

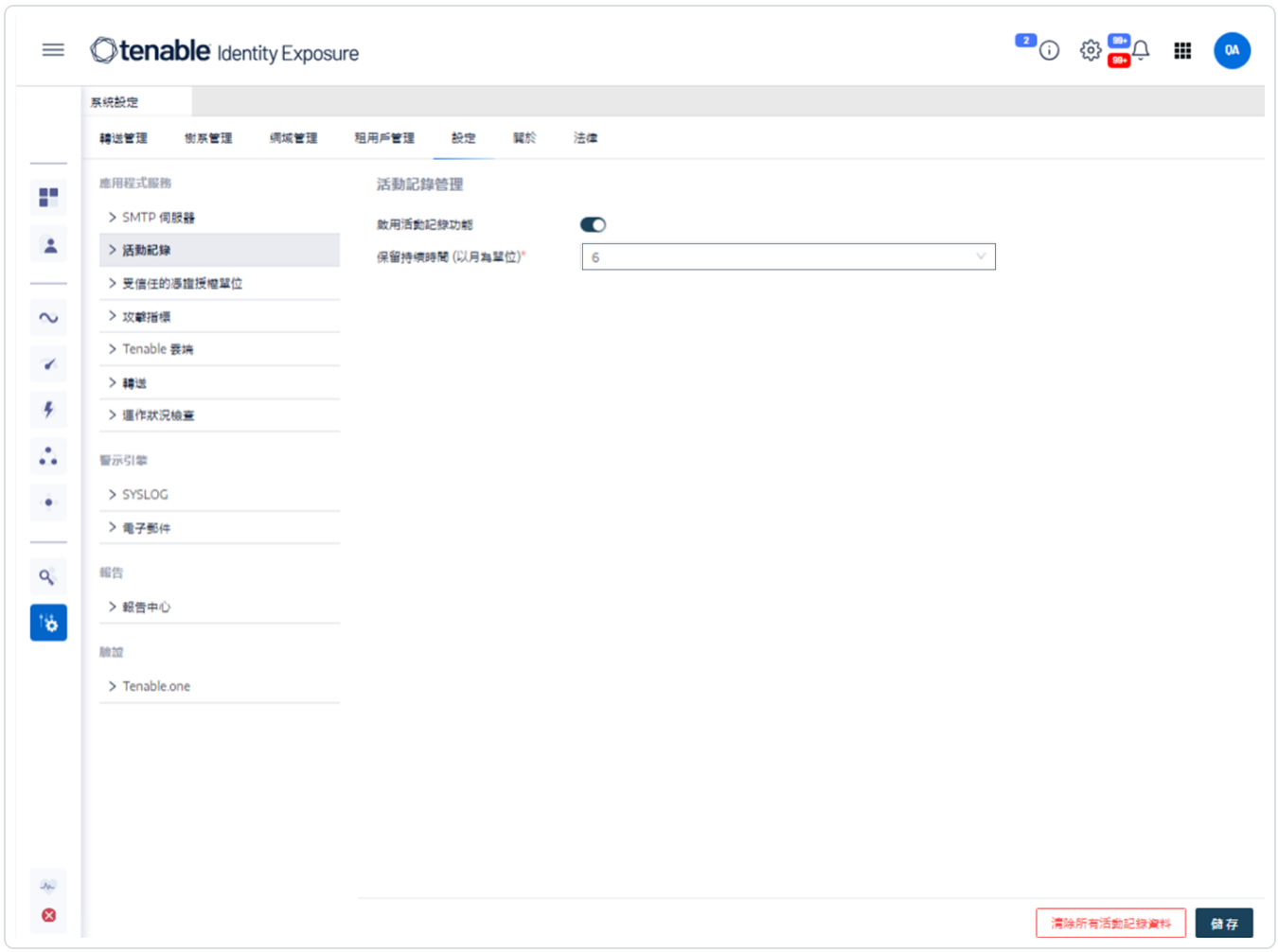
   **「活動記錄管理」**窗格會隨即開啟。

3. 如要啟用活動記錄功能，請按一下切換到**「啟用」**。

4. 在「保留期限 (以月為單位)」方塊中，按一下 **>** 選取記錄活動的月數。

5. 按一下**「儲存」**。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新設定。




**如要清除活動記錄資料：**

1. 在 Tenable Identity Exposure 側邊導覽窗格中的**「管理」**下面，按一下**「系統」**。

   **「系統設定」**窗格會隨即開啟。

2. 在**「應用程式服務」**區段下面，按一下**「活動記錄」**。

   **「活動記錄管理」**窗格會隨即開啟。

3. 在**「清除所有活動記錄資料」**下面，按一下**「清除」**。

   系統會顯示一則訊息，要求您確認。

4. 按一下**「確認」**。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新設定。

**如要為使用者自己的活動記錄設定權限：**

1. 在 Tenable Identity Exposure 側邊導覽窗格中的「**管理**」下面，按一下「**帳戶**」。

   「**使用者帳戶管理**」窗格會隨即開啟。

2. 選取「**角色管理**」索引標籤。

3. 在角色清單中，將游標停留在需要此權限的使用者角色上，然後按一下此行末尾的 圖示。

   「**編輯角色**」窗格會隨即開啟。

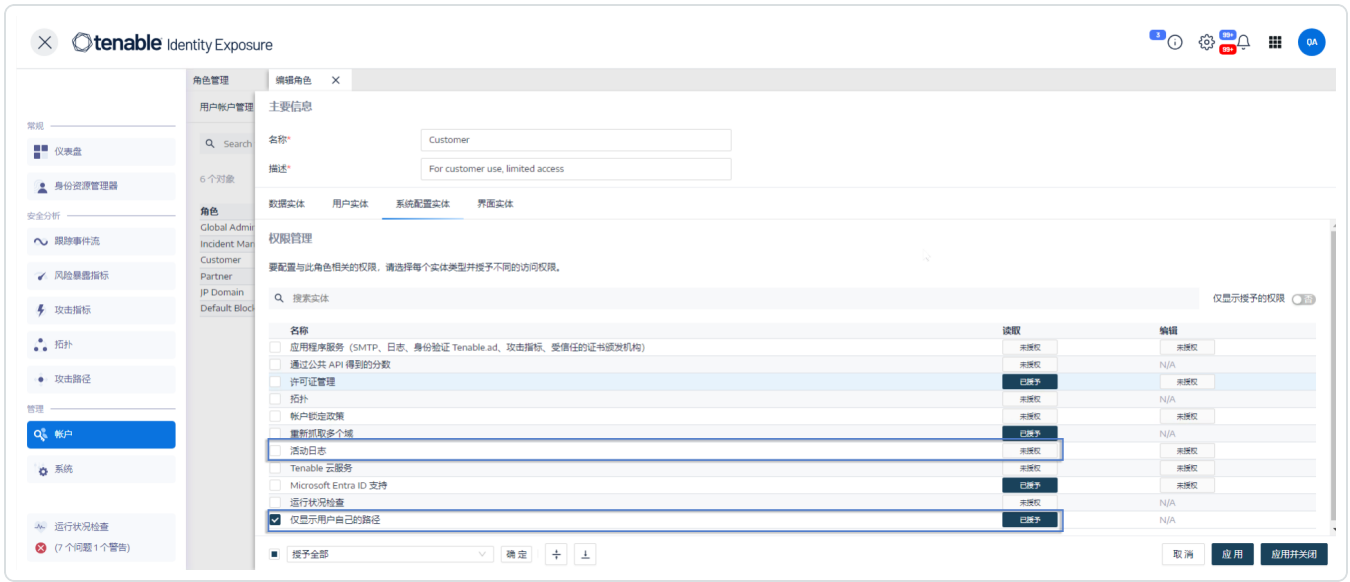
4. 在「**主要資訊**」區段下，選取「**系統設定實體**」索引標籤。

5. 在「**權限管理**」區段下執行下列動作：

   - 取消選取「**活動記錄**」的權限，設定為「*未授權*」。
   - 選取「**僅顯示使用者自己的追蹤記錄**」權限，設定為「*已授予*」。

6. 按一下「**套用並關閉**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新使用者角色。



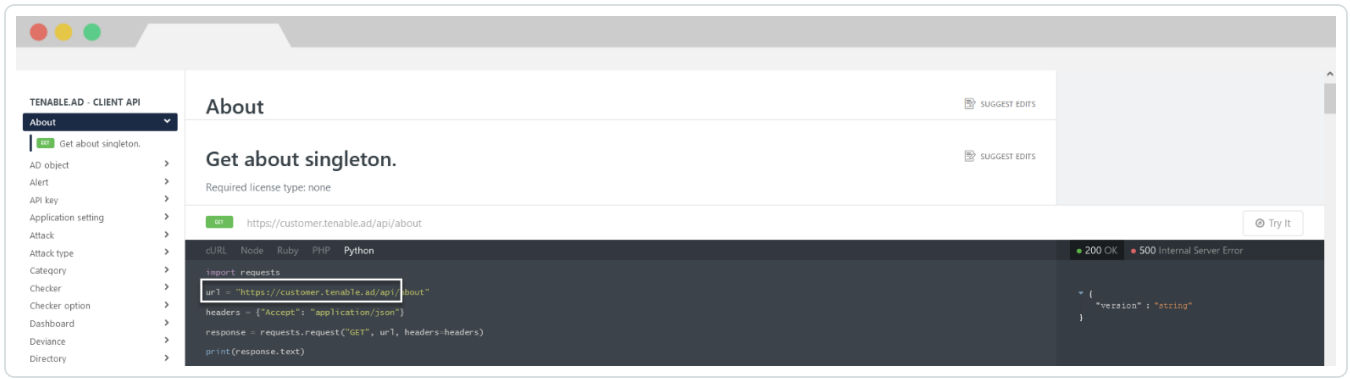

# Tenable Identity Exposure 公用 API

Tenable Identity Exposure 的 API 可協助您與其資料庫服務通訊。

包含 Tenable Identity Exposure 的 API 結構和資源的 OpenAPI 檔案可於此處取得。

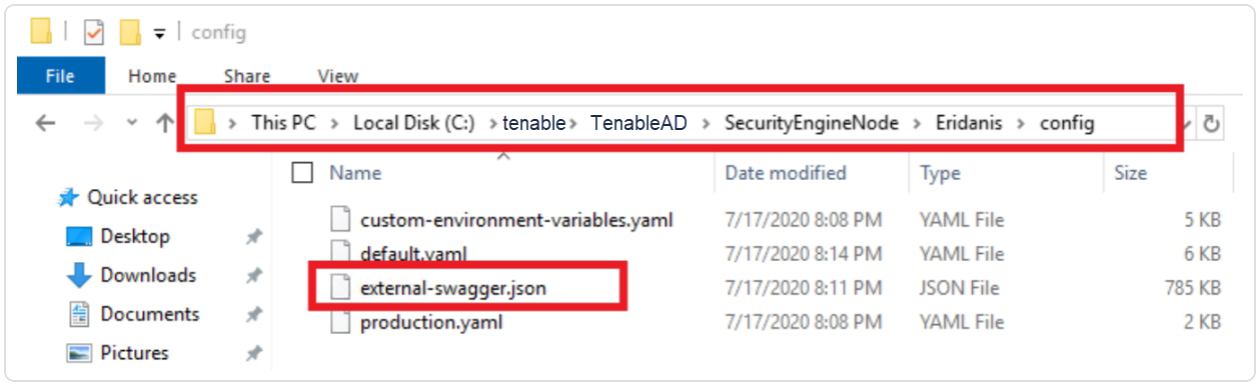
### 如要存取 Tenable Identity Exposure 執行個體的 API：

- 在瀏覽器中開啟此 URL：




### 如要下載 OpenAPI 檔案：

- 對於內部部署安裝，請使用此安全引擎節點的路徑：




- 針對 SaaS 安裝，請前往 Tenable Identity Exposure API Explorer。

### 如要擷取 API 金鑰：

1. 在 Tenable Identity Exposure 中按一下您的使用者設定檔圖示，然後選取「**喜好設定**」。

   「喜好設定」窗格會隨即開啟。

2. 從功能表中選取「**API 金鑰**」。

Tenable Identity Exposure 將顯示您目前的 API 金鑰。

3. 如要將 API 金鑰複製到剪貼簿，請按一下 。

**如要重新整理 API 金鑰：**

如果您按一下「**重新整理 API 金鑰**」或者如果您失去產生 API 金鑰或存取權杖的權限，存取權杖將過期。此過期與時間或 API 要求數量無關。產生或重新整理 API 金鑰僅目前使用者可以使用，不會干擾其他帳戶的 API 金鑰。您在取得 API 金鑰時，也會收到重新整理權杖。您可以使用此重新整理權杖來擷取新的 API 金鑰。

**注意**：當您重新整理 API 金鑰時，Tenable Identity Exposure 會停用目前的 API 金鑰，您還會收到一個重新整理權杖。

1. 按一下「**重新整理 API 金鑰**」。

   系統會顯示一則訊息，要求您確認。

2. 按一下「**確認**」。

## 資料管理

Tenable Identity Exposure 會將 Microsoft Entra ID 和 Active Directory 中的資料保留最多 15 個月。

| 功能 | 保留時間 |
|---|---|
| 攻擊路徑 | 6 個月 |
| 拓撲 | |
| 追蹤流程 | |
| 儀表板和報告 | 12 個月 |
| 曝險中心 | 最多 15 個月 |
| Identity 360 | |
| 曝險指標 (Entra ID) | |

| | |
|---|---|
| 曝險指標 (Active Directory) | • 作用中問題：無限期保留<br>• 解決的問題：保留 6 個月 |
| 攻擊指標 (Active Directory) | |

詳情請參閱 Tenable Cloud 平台資料。

## 部署區域

Tenable Identity Exposure SaaS 目前部署在下列 Azure 區域：

| 國家/地區 | Azure 區域 |
|---|---|
| **美洲** | |
| 巴西：聖保羅 | 巴西南部 |
| 加拿大：魁北克市 | 加拿大東部 |
| 加拿大：多倫多 | 加拿大中部 |
| 美國：加州 | 美西 |
| 美國：愛荷華州 | 美中 |
| 美國：維吉尼亞州 | 美東 2 |
| **歐洲、中東、非洲** | |
| 法國：巴黎 | 法國中部 |
| 愛爾蘭 | 北歐 |
| 荷蘭 | 西歐 |
| 南非：約翰尼斯堡 | 南非北部 |
| 瑞士：蘇黎世 | 瑞士北部 |
| 阿拉伯聯合大公國：杜拜 | 阿拉伯聯合大公國北部 |
| 英國：倫敦 | 英國南部 |
| **亞太地區** | |

| | |
|---|---|
| 澳洲:新南威爾斯州 | 澳洲東部 |
| 澳洲:維多利亞州 | 澳洲東南部 |
| 香港 | 東亞 |
| 印度:浦納 | 印度中部 |
| 日本:大阪 | 日本西部 |
| 新加坡 | 東南亞 |

## Tenable Identity Exposure 授權

本主題將聚焦於 Tenable Identity Exposure 這個獨立產品，詳細介紹產品的授權流程，同時也會說明資產如何計算，以及超出授權配額或授權到期時會發生的情況。

## 授權 Tenable Identity Exposure

Tenable Identity Exposure 有雲端和內部部署兩個版本。在某些情況下，Tenable 也會提供訂閱價格。

如要使用 Tenable Identity Exposure，請根據組織需求和環境詳細情況購買授權。Tenable Identity Exposure 接著會將這些授權指派給您的*資產*(您目錄服務中處於啟用狀態的使用者)。

當您的環境擴大規模時，資產數量也會增加，因此您會購買更多授權，以應對這種變動情況。Tenable 授權採用累進計費模式，因此購買的授權越多，單價就越低。如果想瞭解價格資訊，請聯絡您的 Tenable 代表。

**提示**:如要檢視目前的授權數量和可用的資產，請在 Tenable 頂端的導覽列中按一下「⚙」，然後按一下「**授權資訊**」。詳情請參閱授權資訊頁面。

**注意**:Tenable 為受管理安全服務供應商 (MSSP) 提供簡化計費模式。詳情請洽您的 Tenable 代表。

## 資產如何計算

每購買一個 Tenable Identity Exposure 授權，就可以掃描一位使用者的個別身分或數位身分資訊。Tenable 不會重複計算身分。例如，在 Microsoft Active Directory 和 Microsoft Entra ID 中相同身分的已啟用使用者帳戶會計為使用一個 Tenable 授權。

使用此 PowerShell 指令碼追蹤 AD 中已啟用的使用者帳戶：

```
(Get-ADuser -Filter 'enabled -eq $true').count
```

使用此 PowerShell 指令碼追蹤 Entra ID 中已啟用的使用者帳戶：

```
(Get-MgUser -All -Filter "accountEnabled eq true" -Property onPremisesSyncEnabled | where {
$_.onPremisesSyncEnabled -ne $true }).Count
```

## Tenable Identity Exposure 元件

Tenable Identity Exposure 的兩個版本皆隨附下列元件：

- 追蹤流程
- 拓撲
- 曝險指標
- 攻擊指標
- 攻擊路徑
- 曝險中心
- Microsoft Entra ID 支援

## 收回授權

購買授權後，除非購買更多授權，否則授權總數量在合約期間將維持不變，但如果您從環境的目錄服務中刪除已啟用的使用者，Tenable Identity Exposure 會即時收回授權。

## 超出授權限制

Tenable 授權採取彈性做法，可以接受因為硬體更新、環境突然擴大規模或非預期威脅所導致的使用量高峰，您可以暫時超出授權身分數量上限。然而，如果掃描的身分數量超過授權配額，Tenable 會明確告知超額量，然後分三階段限制功能。

**注意：**如果內部部署環境使用 Tenable Identity Exposure 3.77 以上版本，系統會立即強制執行授權限制。

| 情境 | 結果 |
| --- | --- |
| 您啟用的身分數量已經連續 3 天超過授權配額 | Tenable Identity Exposure 中會顯示一則訊息。 |
| 您已經有 15 天以上啟用超過授權配額的身分 | Tenable Identity Exposure 中會顯示訊息和警示，通知功能將受限。 |
| 您啟用的身分數量超過授權配額的時間已超過 30 天 | Tenable Identity Exposure 中會顯示一則訊息，且您無法在使用者介面或 API 中使用曝險指標功能。 |

## 授權到期

您購買的 Tenable Identity Exposure 授權在合約期內有效。在授權到期的 30 天前，使用者介面中會顯示一則警示。在此續約期內，請聯絡 Tenable 代表以新增或移除產品，或變更授權數量。

授權到期後，您將無法登入 Tenable 平台。

## 管理您的授權

Tenable Identity Exposure 需要 Tenable 或授權企業合作夥伴提供的授權檔案。計算的授權使用者人數涵蓋所有已啟用的使用者和服務帳戶。

您必須上傳授權檔案才能設定和使用 Tenable Identity Exposure。

**提示**：授權檔案位於 Tenable Community 入口網站中「My Products」(我的產品) 部分 (您必須是 Tenable Community 的管理員，才能檢視授權檔案)。

**注意**：如果沒有將有效的授權套用至 SaaS 平台，Tenable 會在一段時間後將其淘汰。

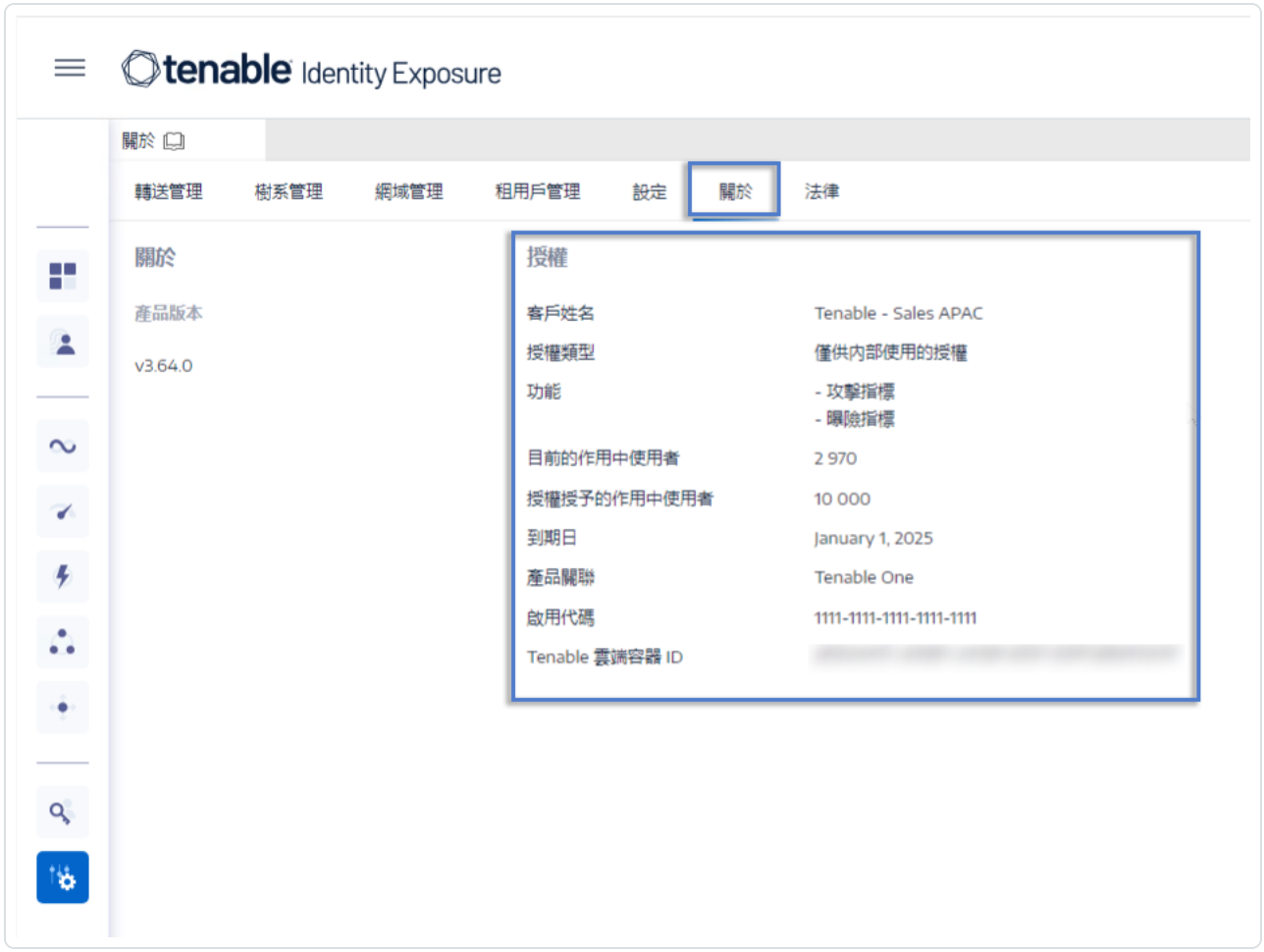
Tenable Identity Exposure 授權可能包含：

- 攻擊指標
- 曝險指標
- 以上兩者

**如要檢視您的授權：**

- 在 Tenable Identity Exposure 中，按一下「**系統**  」>「**關於**」索引標籤。

  授權會隨即顯示。




## 授權的使用

對於內部部署安裝，當可以連線網際網路時，Tenable Identity Exposure 會追蹤授權使用情況。

### 防止容器 UUID 不相符

在 Tenable Identity Exposure 中，每個授權都包含一個唯一的容器 UUID，可將應用程式連結至特定的 Tenable 雲端容器。此容器 UUID 必須保持一致，以確保無縫整合並避免操作問題。

為了防止容器 UUID 不一致 (例如，在續約後上傳新授權時)，Tenable Identity Exposure 可以偵測容器 UUID「不相符」。

如果您嘗試上傳容器 UUID 不同的授權，則會出現「無法變更 Tenable 雲端容器」訊息。您可能會處於下列其中一種情況：

- 從 Tenable Identity Exposure 單機版移轉至 Tenable One 授權。
- 將您的容器從一個 Tenable AWS 網站移轉至另一個。
- 前容器到期且要建立新容器。

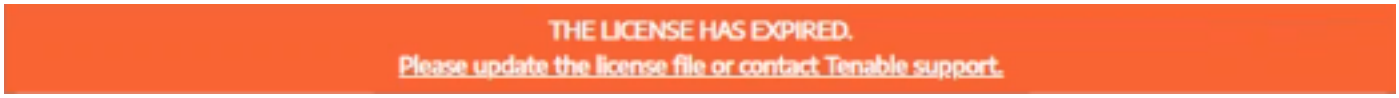
如果您處於上述其中一種情況，請聯絡 Tenable，討論如何變更此 Tenable Identity Exposure 平台的 Tenable 雲端容器。

## 授權有效性

只要您符合下列條件，Tenable Identity Exposure 授權便保持有效：

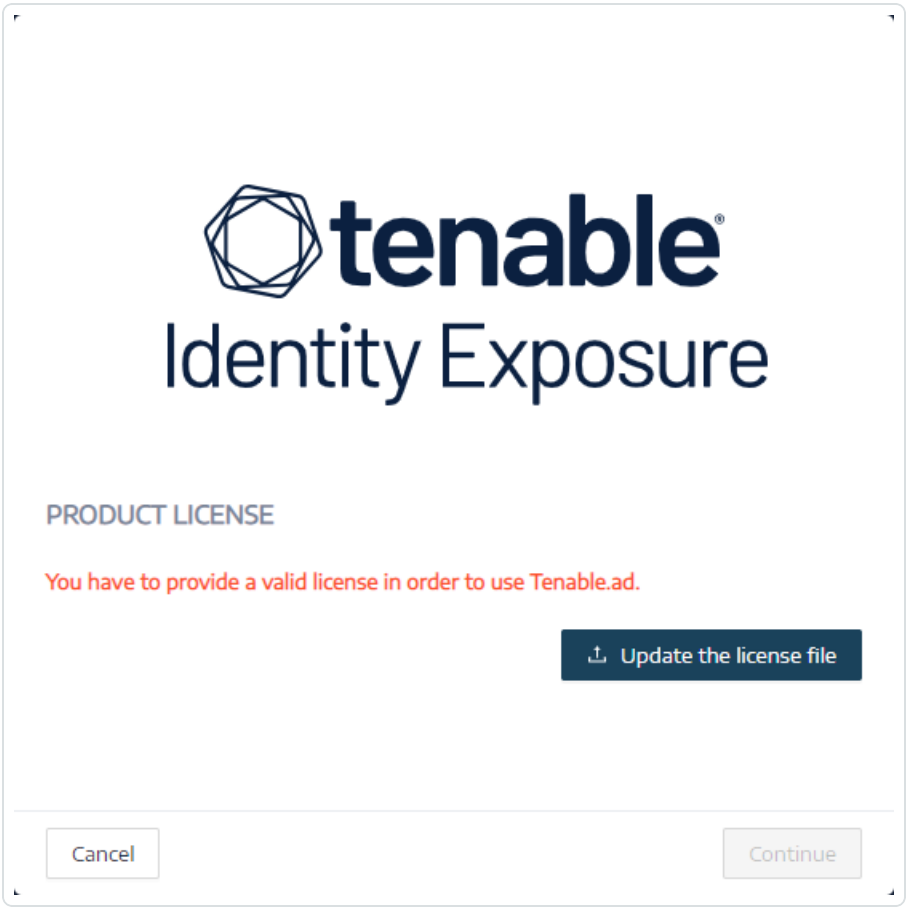
- 作用中使用者數量不超過授權授予的數量。視您的情況而定，Tenable Identity Exposure 會顯示三種類型的警告訊息。
    - 作用中使用者數量**接近授權條件上限**時，則您必須更新授權。
    - 作用中使用者數量**超過授權條件上限**時，則您必須更新授權。
    - 作用中使用者數量 **超過授權條件 (10%)** 時，則不再擁有「曝險指標」頁面的存取權，且必須更新授權。
- 未過到期日。

如果您不符合上述任一條件，Tenable Identity Exposure 會顯示警告，提示您更新授權：



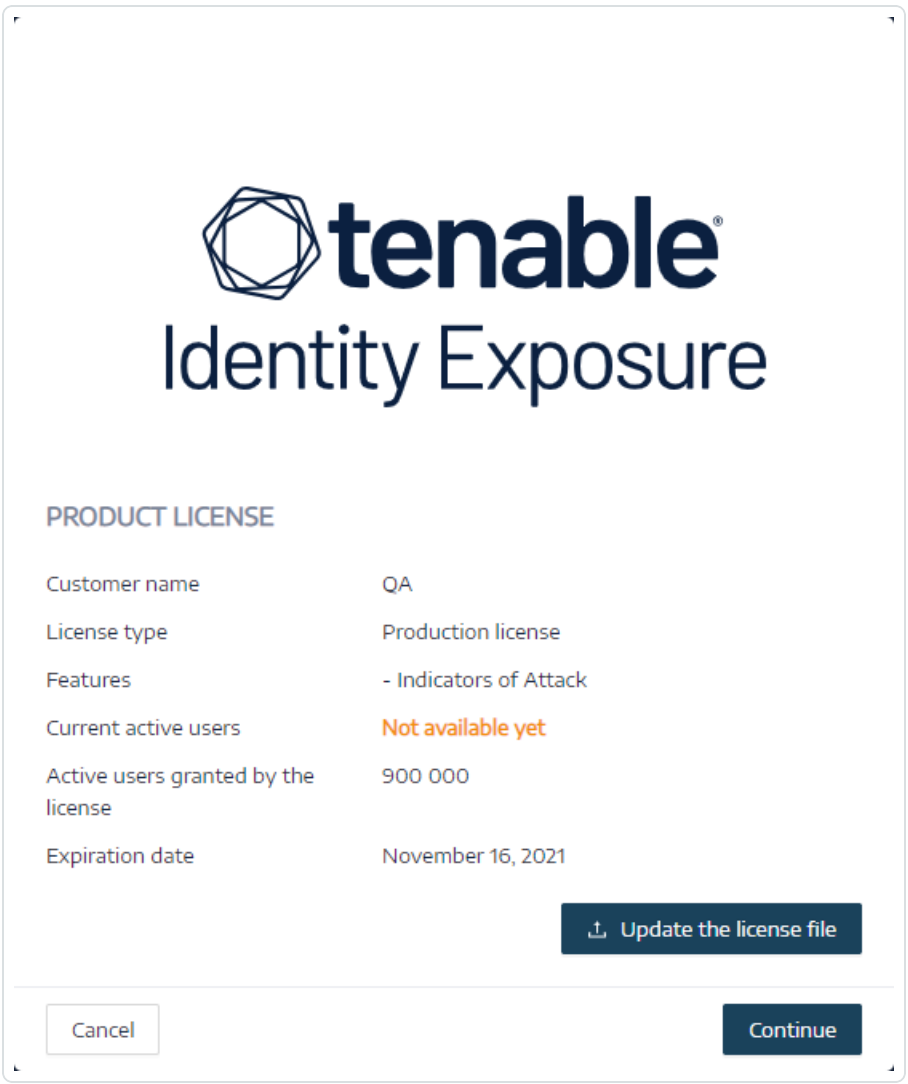

**如要上傳授權檔案：**

1. 在登錄視窗中，按一下「**更新授權檔案**」。




2. 瀏覽至您的授權檔案的位置，然後按一下「**開啟**」。

   以下是成功套用授權檔案的範例：




3. 按一下**「繼續」**以開啟 Tenable Identity Exposure。

**如要更新授權檔案：**

1. 在 Tenable Identity Exposure 中按一下**「系統」**和**「關於」**。
2. 按一下**「更新授權檔案」**。
3. 瀏覽至您的授權檔案的位置，然後按一下**「開啟」**。

   Tenable Identity Exposure 會更新您的授權檔案。若授權檔案無效，請聯絡客戶支援人員。

## 長期支援 (LTS) 版本與一般版本：主要差異和好處

### 什麼是 LTS?

LTS (長期支援) 版本是我們延長維護期限 (18 個月) 的軟體版本。在此期間，我們會提供定期更新，例如安全性修補程式和重大錯誤修復，而不會引入可能會中斷現有功能的新功能。

LTS 版是為較重視穩定性、可靠性和長期維護而非擁有最新功能的客戶所設計。對於頻繁更新或變更可能導致停機或額外測試和部署成本的環境，就非常適合這類版本。

### 什麼是一般版本?

一般版本是我們的標準軟體版本，其中包含新功能、改善功能和更新。這類版本的動態性更強，更新頻率更高 (每 6 個月一次)，但相較於 LTS 版本，獲得的支援期限更短。

即使需要更頻繁升級，但想保持領先技術並定期採用新功能和更新的客戶，就非常適合一般版本。

### LTS 和一般版本之間的主要差異:

- **支援期限**:LTS 版本可獲得 18 個月的支援，而一般版本可獲得 6 個月的支援。
- **穩定性與創新**:LTS 著重於穩定性和安全性，且功能變更最少，而一般版本則強調創新，更頻繁地推出新功能。
- **升級頻率**:使用 LTS 版本的客戶較不常升級，而使用一般版本的客戶可能需要更頻繁地升級，才能保持最新狀態。

### 為何選擇 LTS?

LTS 版本非常適合停機時間成本高的關鍵任務系統或環境。這類版本可確保版本長期維持穩定並受到支援，讓您高枕無憂。

### 為什麼要選擇一般版本?

如果您重視擁有最新的功能和改善功能，則一般版本會更適合。雖然可能需要更頻繁更新，卻能支援最新功能。

## 排解 Tenable Identity Exposure 問題

下列主題說明可協助您解決使用 Tenable Identity Exposure (前稱 Tenable.ad) 時可能遇到的問題:

- SYSVOL 強化干擾 Tenable Identity Exposure
- 系統公用程式 (handle.exe)

## SYSVOL 強化干擾 Tenable Identity Exposure

SYSVOL 是位於 Active Directory 網域中每個網域控制器 (DC) 上的共用資料夾，其中儲存了群組原則 (GPO) 的資料夾和檔案。SYSVOL 的內容會在所有 DC 之間複製，且可透過通用命名慣例 (UNC) 路徑存取，例如：`\\<example.com>\SYSVOL` 或 `\\<DC_IP_or_FQDN>\SYSVOL`。

**SYSVOL 強化**是指使用「UNC 強化路徑」參數，也稱為「UNC 強化存取」、「強化的 UNC 路徑」、「UNC 路徑強化」或「強化路徑」等。此功能的出現是為了回應群組原則中的 MS15-011 (KB 3000483) 弱點。許多網路安全標準 (例如 CIS Benchmarks) 都要求強制執行此功能。

當您在伺服器訊息區 (SMB) 用戶端上套用此強化參數時，它實際上會提高加入網域之電腦的安全性，確保電腦從 SYSVOL 擷取的 GPO 內容不會遭到網路上的攻擊者竄改。但在某些情況下，此參數也會干擾 Tenable Identity Exposure 的運作。

如果您發現強化的 UNC 路徑會中斷 Tenable Identity Exposure 和 SYSVOL 共用之間的連線，請遵照本疑難排解章節中的指引採取動作。

## 受影響的環境

下列 Tenable Identity Exposure 部署選項可能會遇到此問題：

- 內部部署
- 採用安全轉送的 SaaS

此部署選項不受影響：

- 採用 VPN 的 SaaS

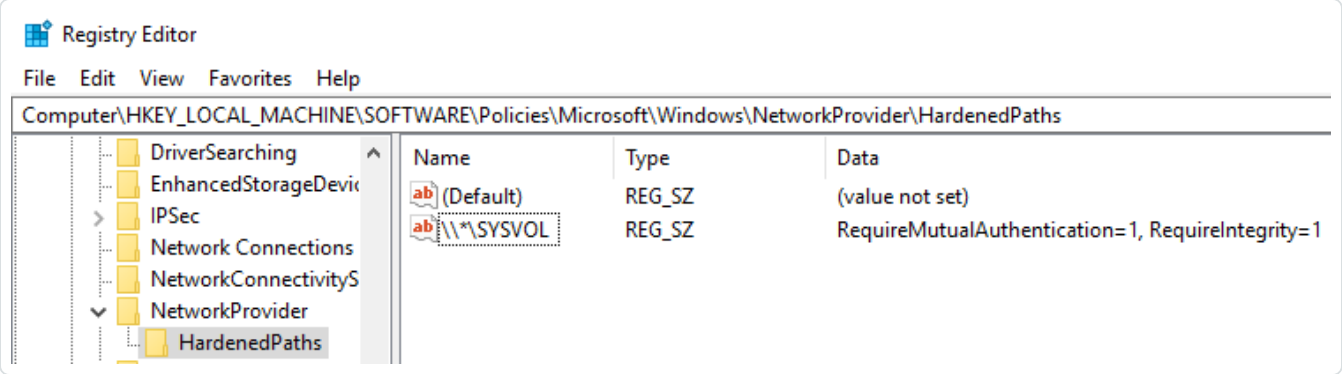
**SYSVOL 強化是一個用戶端參數**，表示它是在連線至 SYSVOL 共用的電腦上運作，而非在網域控制器上運作。

**Windows 會依預設啟用此參數，但可能會干擾 Tenable Identity Exposure**。

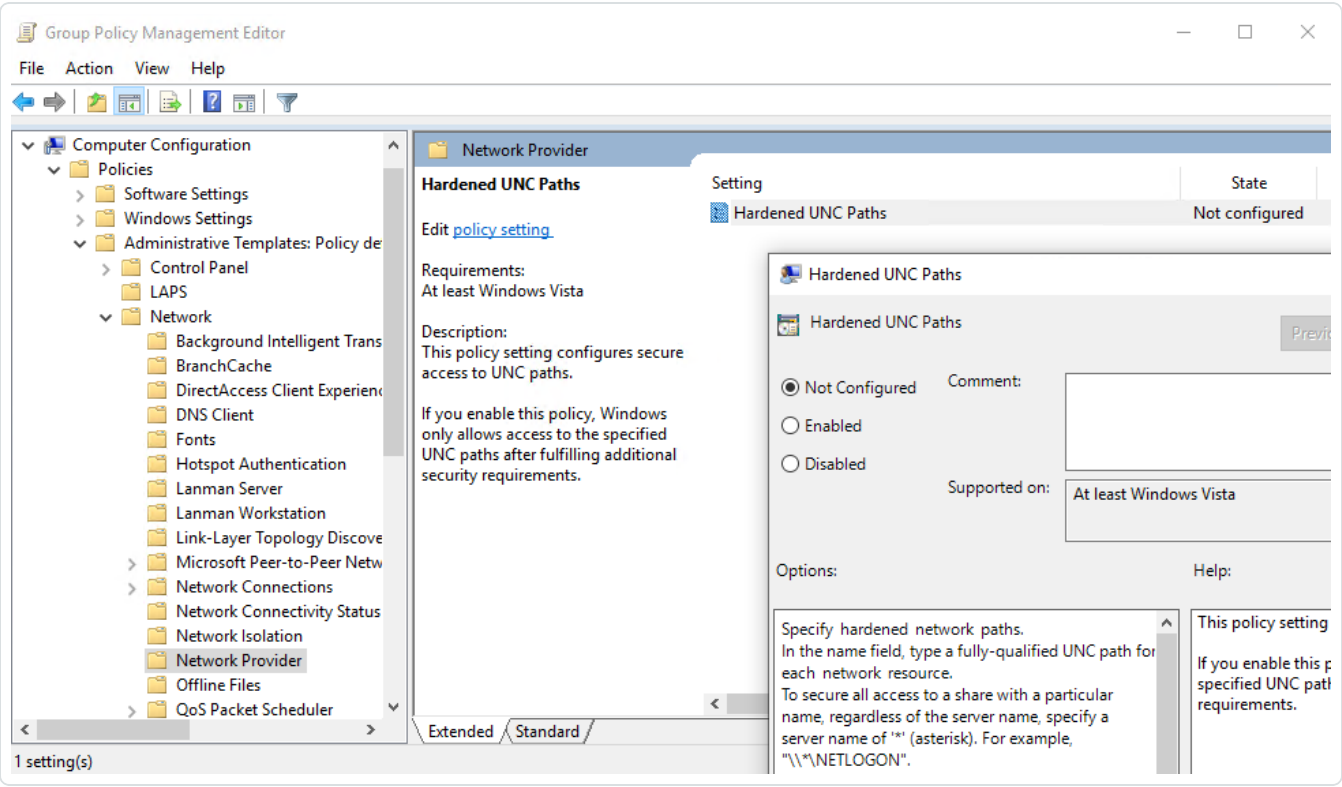
有些組織也希望確保啟用此參數，並透過使用相關的 GPO 設定或直接設定對應的登錄機碼來強制執行此參數。

- 您可以在「`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`」

下找到與 UNC 強化路徑相關的登錄機碼：




- 您可以在「Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths」下找到對應的 GPO 設定：



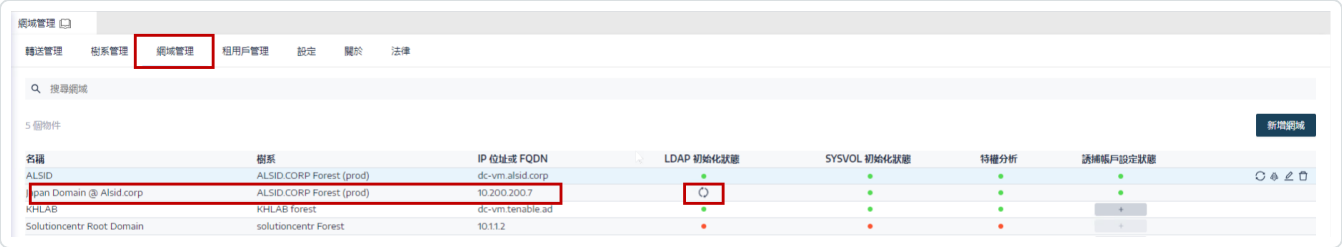

當參照 SYSVOL 的 UNC 路徑 (例如「*\SYSVOL」) 將參數「RequireMutualAuthentication」和「RequireIntegrity」的值設定為「1」時，就會發生 SYSVOL 強化強制執行。

## SYSVOL 強化問題的徵兆

當您懷疑 SYSVOL 強化對 Tenable Identity Exposure 造成干擾時，請檢查下列項目：

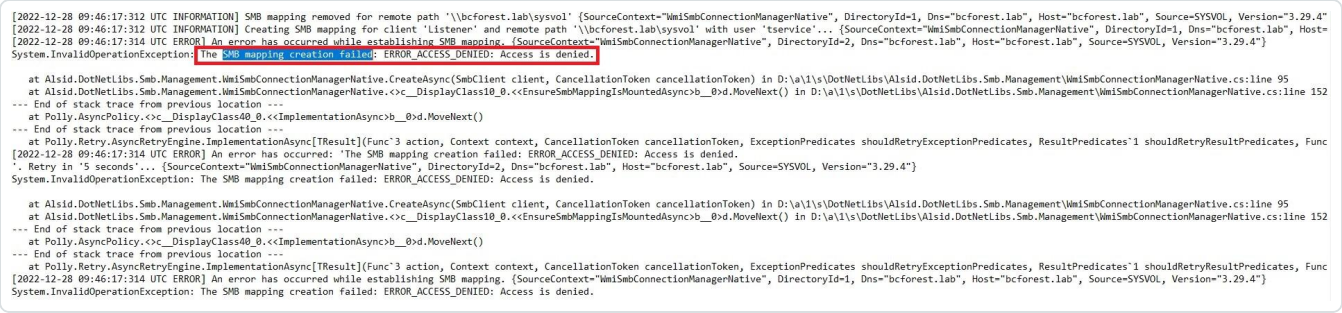
1. 在 Tenable Identity Exposure 中，前往「**系統**」>「**網域管理**」，查看每個網域的 LDAP 和 SYSVOL 初始化狀態。

   正常連線的網域會顯示綠色指示器，而具有連線問題的網域可能會顯示無限持續的抓取指示器。




2. 在目錄接聽程式或轉送電腦上，開啟記錄資料夾：`<Installation Folder>\DirectoryListener\logs`。

3. 開啟 Ceti 記錄檔並搜尋字串「SMB 對應建立失敗」或「存取遭到拒絕」。包含此詞組的錯誤記錄表示目錄接聽程式或轉送電腦上可能已執行 UNC 強化。




## 修復選項

可能的修復選項有兩種：切換為 Kerberos 驗證 或 停用 SYSVOL 強化。

### 切換為 Kerberos 驗證

**此為建議選項，因為可避免停用強化功能。**

只有在使用 NTLM 驗證連線至受監控的網域控制器時，SYSVOL 強化才會干擾 Tenable Identity Exposure。這是因為 NTLM 與「`RequireMutualAuthentication=1`」參數不相容。Tenable Identity Exposure 也支援 Kerberos。如果您正確設定和使用 Kerberos，則不需要停用 SYSVOL 強化。如需詳細資訊，請參閱 Kerberos 驗證

## 停用 SYSVOL 強化

**如果無法切換至 Kerberos 驗證，您也可以選擇停用 SYSVOL 強化。**

Windows 預設會啟用 SYSVOL 強化，因此僅移除登錄機碼或 GPO 設定是不夠的。您必須明確將其停用，並只在託管目錄接聽程式 (內部部署) 或轉送 (採用安全轉送的 SaaS) 的電腦上套用此變更。這不會影響其他電腦，而且您永遠不需要在網域控制器上停用 SYSVOL 強化。

託管目錄接聽程式 (內部部署) 或轉送 (採用安全轉送的 SaaS) 的電腦上使用的 Tenable Identity Exposure 安裝程式已在本機停用 SYSVOL 強化。不過，您環境中的 GPO 或指令碼可能會移除或覆寫登錄機碼。

可能會有兩種情況：

- 如果目錄接聽程式或轉送電腦**未加入網域**：您無法使用 GPO 來設定電腦。您必須在登錄檔中停用 SYSVOL 強化 (請參閱登錄檔：GUI 或登錄檔：PowerShell)。
- 如果目錄接聽程式或轉送電腦**已加入網域** (Tenable Identity Exposure 不建議這麼做)：您可以在登錄檔中直接套用設定 (請參閱登錄檔：GUI 或登錄檔：PowerShell)，或使用 GPO。不論使用哪種方法，您都必須確保 GPO 或指令碼不會覆寫登錄機碼。您可以透過以下任一方式執行此操作：
  - 仔細檢閱此電腦上套用的所有 GPO。
  - 套用變更並稍等片刻，或使用「`gpupdate /force`」強制套用 GPO，然後檢查登錄機碼的值是否保持不變。

在您重新啟動目錄接聽程式或轉送電腦之後，修改後網域上的抓取指示器應變成綠色指示器：

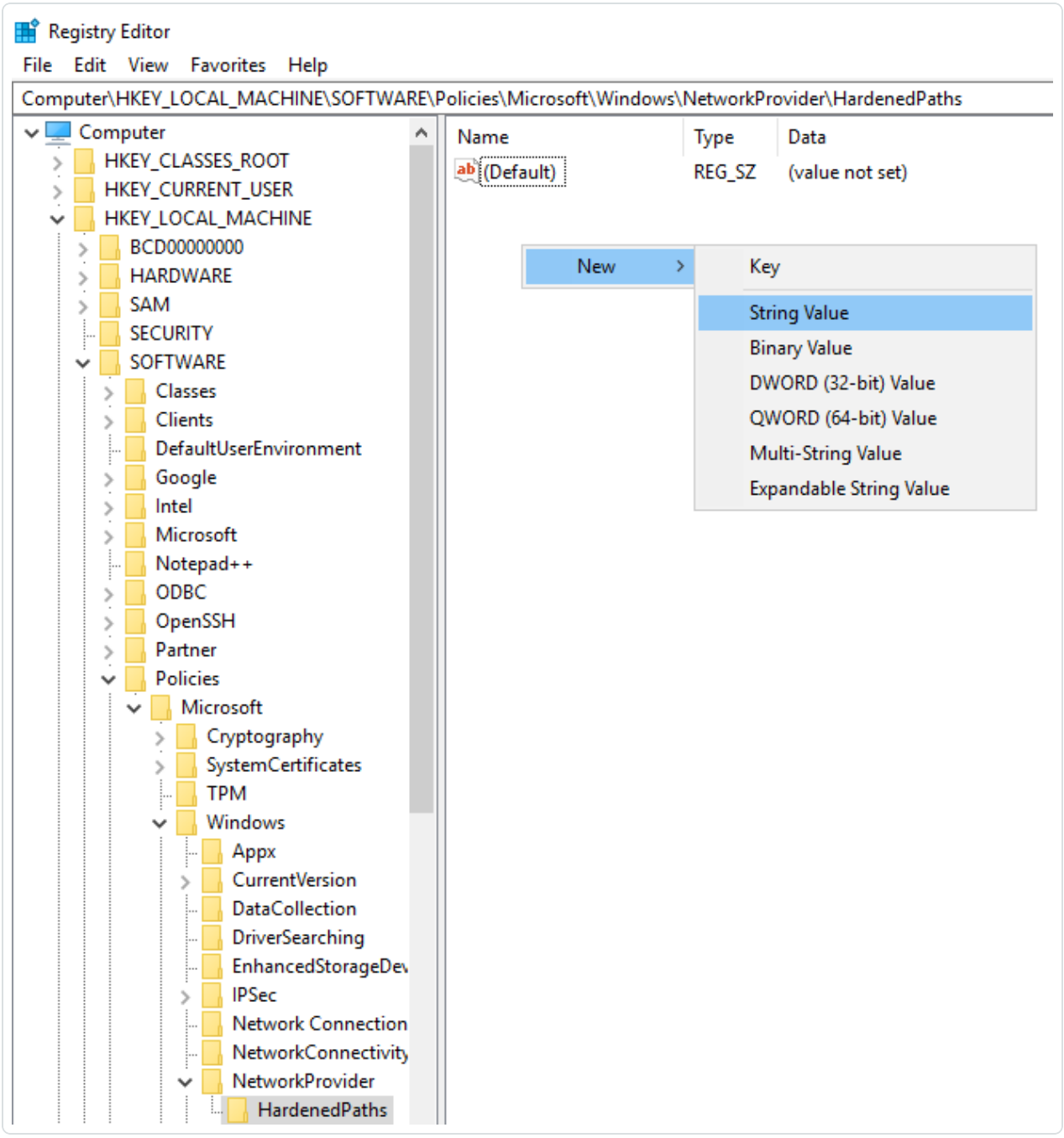



## 登錄檔：GUI

如要使用 GUI 在登錄檔中停用 SYSVOL 強化：

1. 以系統管理權限連線至目錄接聽程式或轉送電腦。
2. 開啟登錄檔編輯器並瀏覽至:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths。
3. 建立名為「*\SYSVOL」的機碼 (若尚不存在), 如下所示:

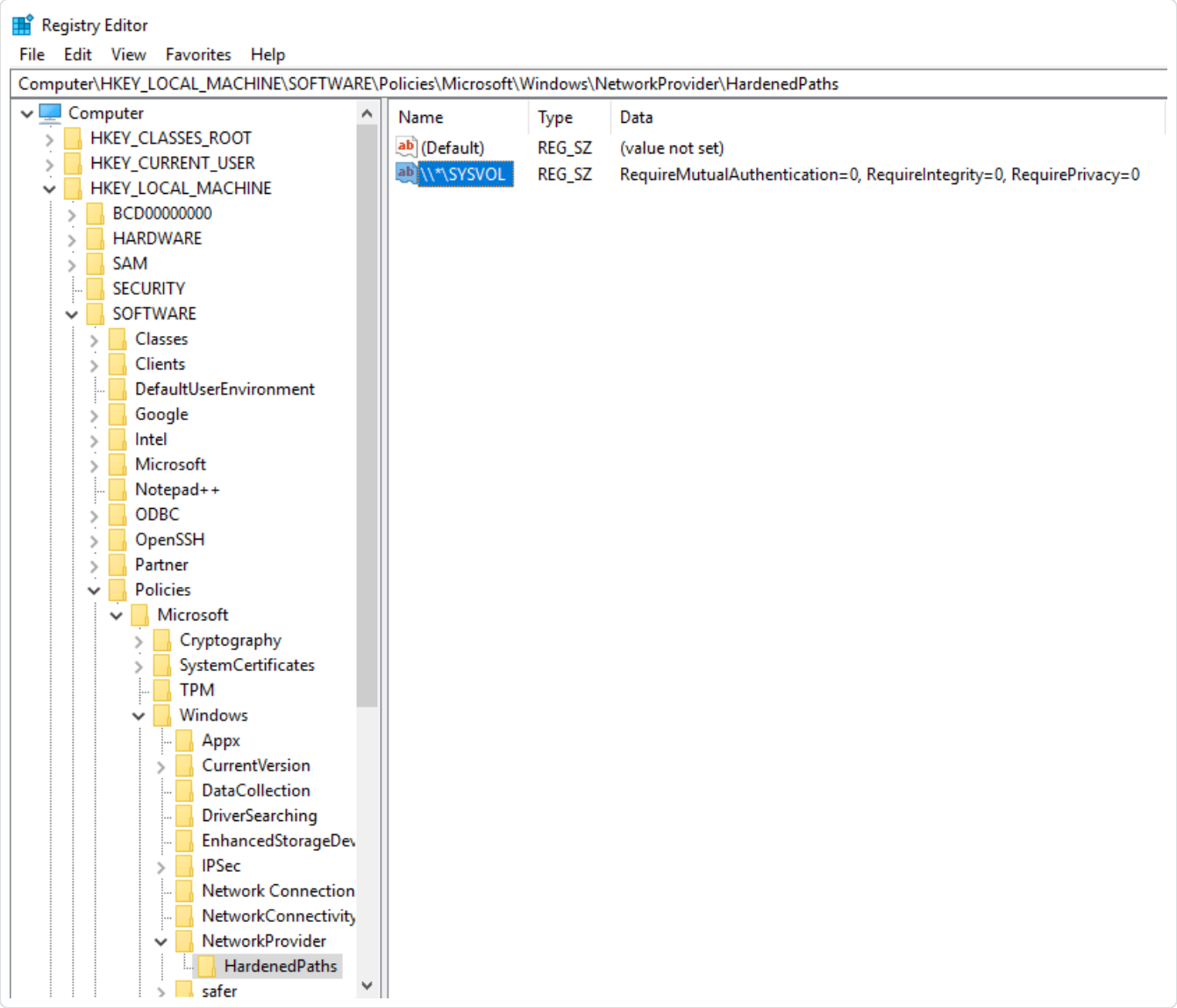
a. 在右側窗格中按一下滑鼠右鍵，然後選擇「**新建**」>「**字串值**」。




b. 在「名稱」欄位中，輸入 *\SYSVOL。

4. 連按兩下「*\SYSVOL」機碼 (新建立或先前存在的機碼) 以開啟「**編輯字串**」視窗。
5. 在「**值**」資料欄位中輸入下列值：`RequireMutualAuthentication=0`、`RequireIntegrity=0`、`RequirePrivacy=0`
6. 按一下「**儲存**」。

   結果應如下所示：




7. 重新啟動電腦。

### 登錄檔：PowerShell

如要使用 PowerShell 在登錄檔中停用 SYSVOL 強化：

1. 使用此 PowerShell 命令收集 UNC 強化路徑登錄機碼的最新值，用於參照：

```
Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
```

2. 設定建議值：

```
New-ItemProperty -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -
Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
```

3. 重新啟動電腦。

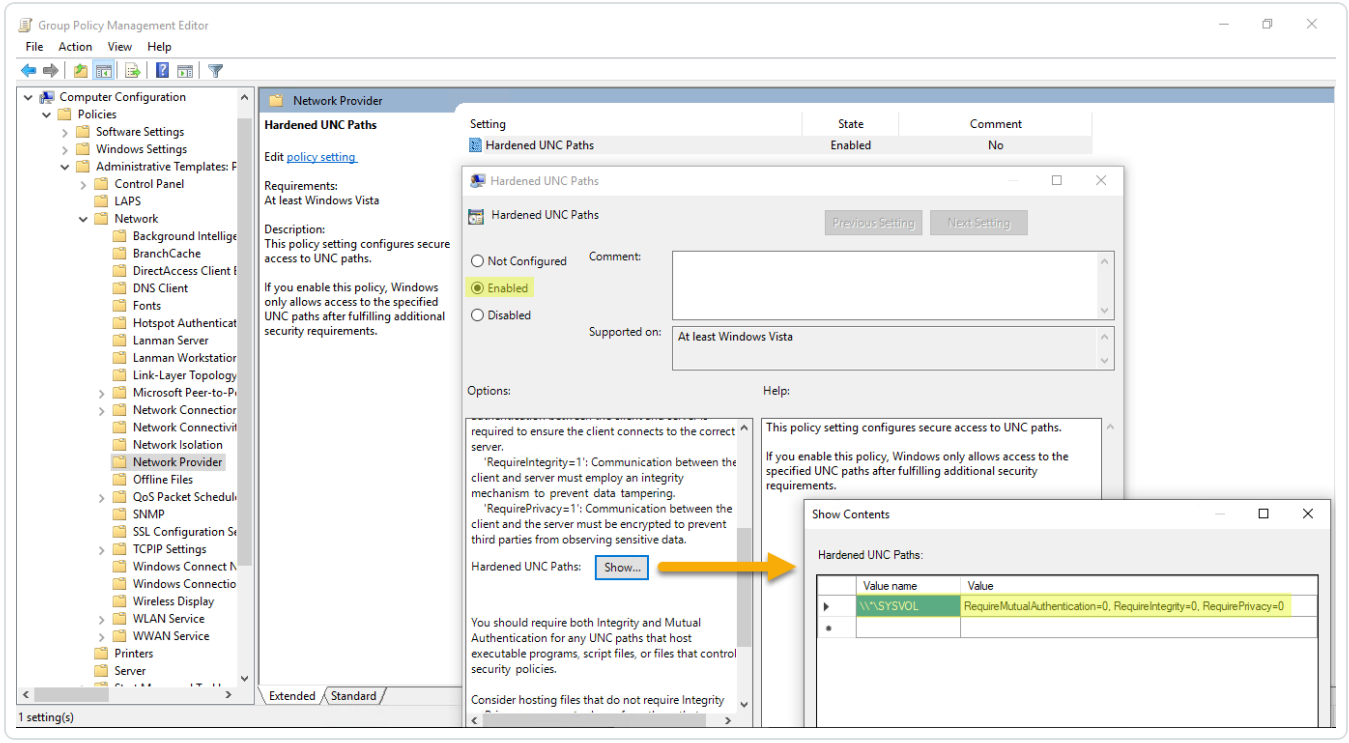
### GPO

**先決條件**：您必須以 Active Directory 使用者身分連線，並且必須有權限在網域上建立 GPO 並將 GPO 連結至包含 Tenable Identity Exposure 目錄接聽程式或轉送電腦的組織單位。

如要使用 GPO 停用 SYSVOL 強化：

1. 開啟群組原則管理主控台。
2. 建立新的 GPO。
3. 編輯 GPO 並瀏覽至下列位置：`Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths`。
4. 啟用此設定並使用下列項目建立新的強化 UNC 路徑：
   - 值名稱 = `\\*\SYSVOL`
   - 值 = `RequireMutualAuthentication=0`、`RequireIntegrity=0`、`RequirePrivacy=0`

   結果應如下所示：



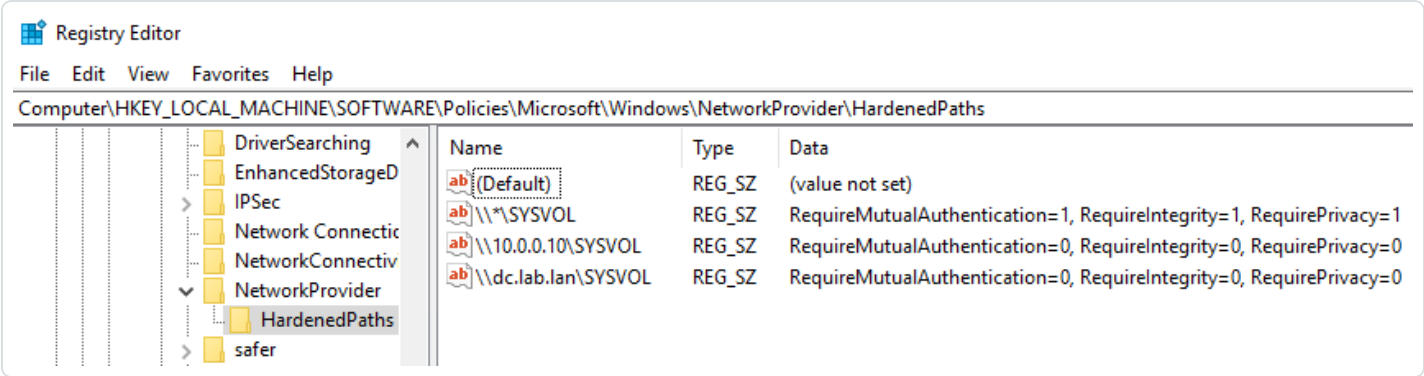

5. 按一下「**確認**」。

6. 將此 GPO 連結至包含 Tenable Identity Exposure 目錄接聽程式或轉送電腦的組織單位。您也可以使用安全性群組篩選 GPO 功能，確保此 GPO 僅適用於此電腦。

## 特定 UNC 路徑例外狀況

前述程序會停用使用萬用字元 UNC 路徑的 SYSVOL 強化：「`\\*\SYSVOL`」。您也可以只針對特定 IP 位址或 FQDN 將其停用。這表示您可以針對「`\\*\SYSVOL`」維持啟用 UNC 強化路徑設定 (值為「`1`」)，並讓 Tenable Identity Exposure 中設定的網域控制器的每個 IP 位址或 FQDN 對應一個例外狀況。

下圖顯示為所有伺服器 (「`*`」) 啟用 SYSVOL 強化的範例，其中「`10.0.0.10`」和「`dc.lab.lan`」除外，這是我們在 Tenable Identity Exposure 中設定的網域控制器：




您可以使用上述登錄檔或 GPO 方法來新增這些額外的設定。

**注意**:您必須指定在 Tenable Identity Exposure 中設定的確切值 (例如，如果 Tenable Identity Exposure 設定使用 FQDN，則您無法指定 IP 位址。)。此外，每次在 Tenable Identity Exposure 網域管理頁面中變更 IP 位址或 FQDN 時，請記得更新這些機碼。

## 停用 SYSVOL 強化時的風險

SYSVOL 強化是一項安全功能，若停用可能會導致嚴重問題。

- 未加入網域的電腦:停用 SYSVOL 強化沒有風險。這些電腦未套用 GPO，因此不會從 SYSVOL 共用取得內容並執行之。
- 加入網域的電腦 (目錄接聽程式或轉送電腦) (Tenable Identity Exposure不建議這麼做):如果在目錄接聽程式或轉送電腦與網域控制器之間可能存在便於攻擊者執行「攔截式攻擊」的風險，則停用 SYSVOL 強化是不安全的行為。在此情況下，Tenable Identity Exposure 建議您改用 Kerberos 驗證。

此停用的範圍僅限於目錄接聽程式或轉送電腦，非其他網域電腦，並且絕對不包括網域控制器。

## 系統公用程式 (handle.exe)

`Handle.exe` 是一種合法的 Windows 處理程序，Tenable Identity Exposure 可將其用於取得系統資源使用量的詳細資訊，特別是任何系統處理程序的開放處理程序。如需詳細資訊，請參閱 Microsoft 說明文件。

請確認您的防毒軟體未封鎖該程式。