Tenable Identity Exposure 3.x 使用者與管理員指南

上次修訂日期：2024 年 4 月 5 日

目錄

歡迎使用 Tenable Identity Exposure

上次更新時間：2024/4/30

Tenable Identity Exposure（前稱 Tenable.ad）可協助您預測威脅、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。

> 攻擊指標和曝險指標功能是否可用取決於您購買的授權。

如要開始使用，請參閱 Tenable Identity Exposure 入門。

> **注意：**Tenable Identity Exposure 可以單獨購買，也可做為 Tenable One 套件的一部分購買。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、日文、德文、韓文、簡體中文和繁體中文版本。此 *Tenable Identity Exposure* 使用者介面有英文、日文、德文、法文、韓文、簡體中文和繁體中文版本。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。

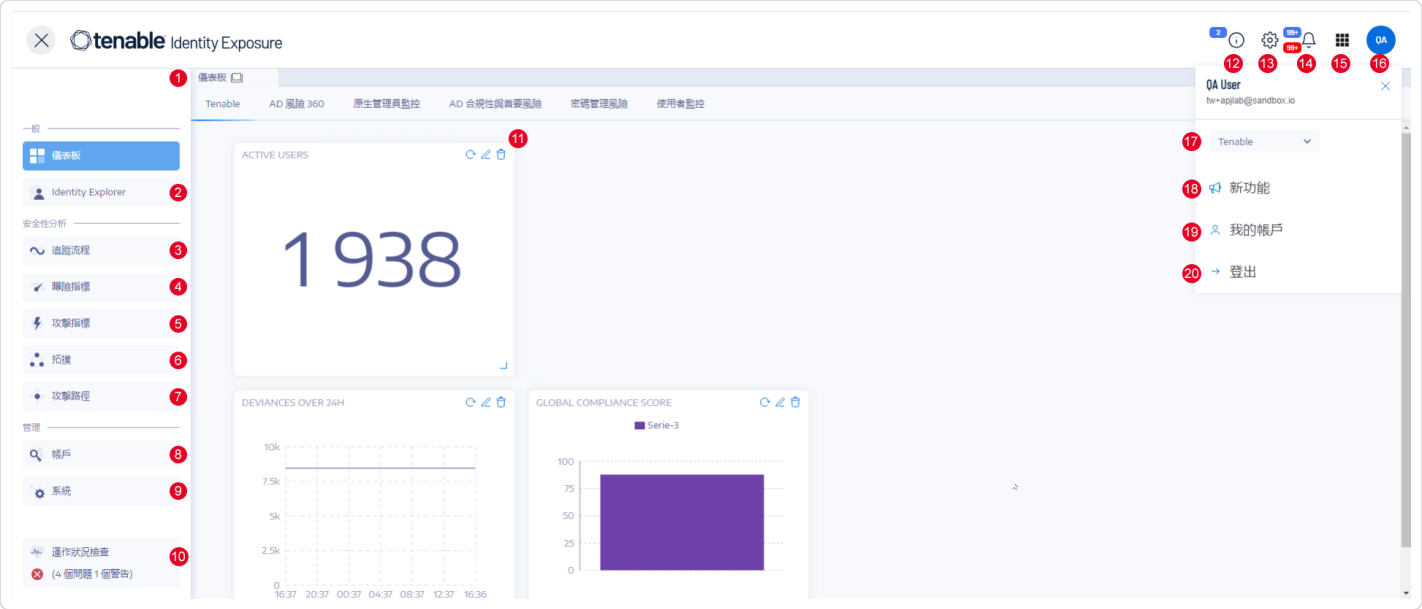
提示：如需 Tenable One 產品使用入門的其他資訊，請參閱 Tenable One 部署指南。

導覽 Tenable Identity Exposure

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 **X**。



#	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	身分識別總管	Tenable Identity Exposure 的身分識別總管檢視整合了 Active Directory 和 Microsoft Entra ID 中的身分識別資訊。此檢視畫面會顯示每個所列資產的身分風險評分 (測試版)，以及遭入侵身分的潛在影響範圍。
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	Topology	「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： • 影響範圍：評估 AD 中可能遭入侵資產的橫向移動。 • 攻擊路徑：預期權限提升技倆從特定進入點到達資產。 • 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 **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： • 帳戶：使用者帳戶、角色和安全性設定檔。 • 系統：樹系和網域、應用程式服務、警示和身分驗證。 如需詳細資訊，請參閱 Tenable Identity Exposure 管理員指南。

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	應用程式切換器	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。

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，請選取以下選項之一：

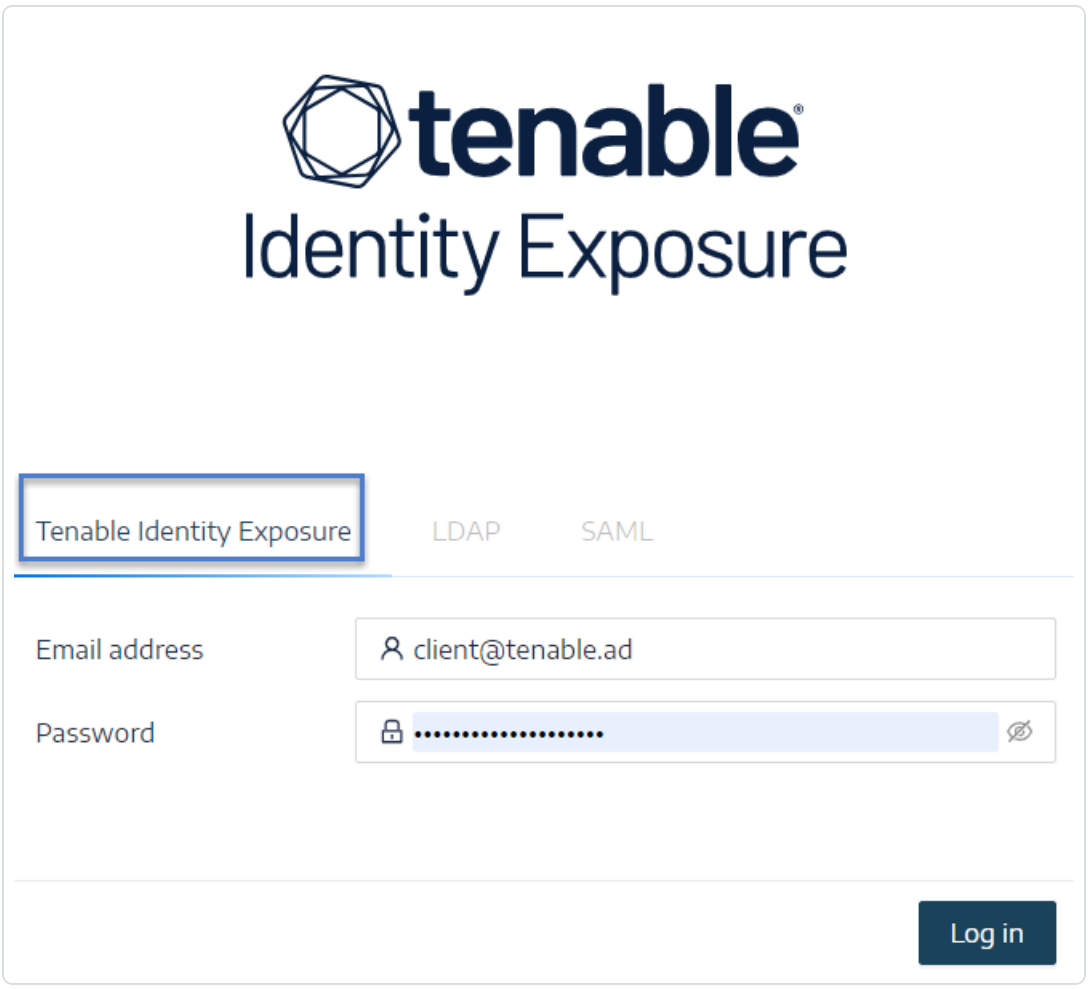
- ◦ 使用 Tenable Identity Exposure 帳戶
  ◦ 使用 LDAP 帳戶
  ◦ 使用 SAML

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**」。

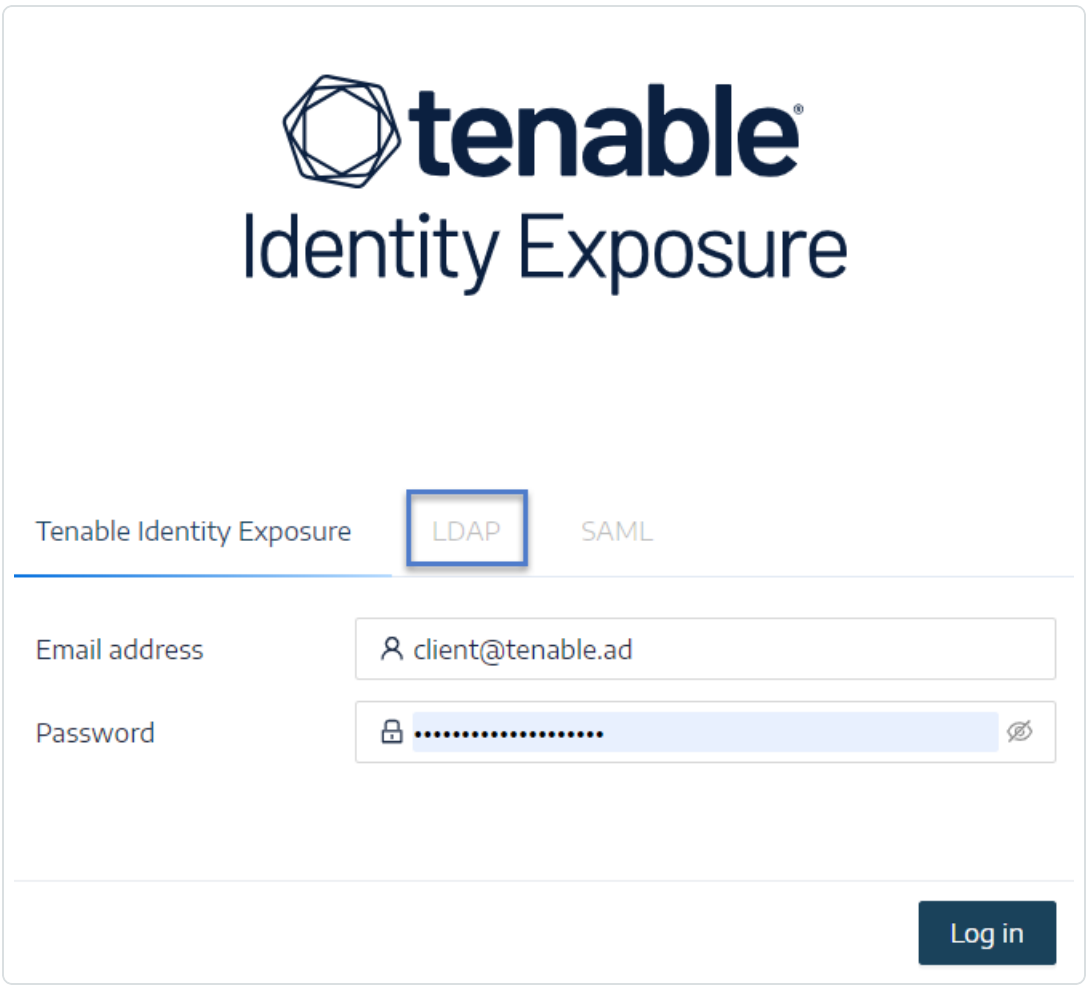
   Tenable Identity Exposure 頁面會隨即開啟。

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**」。

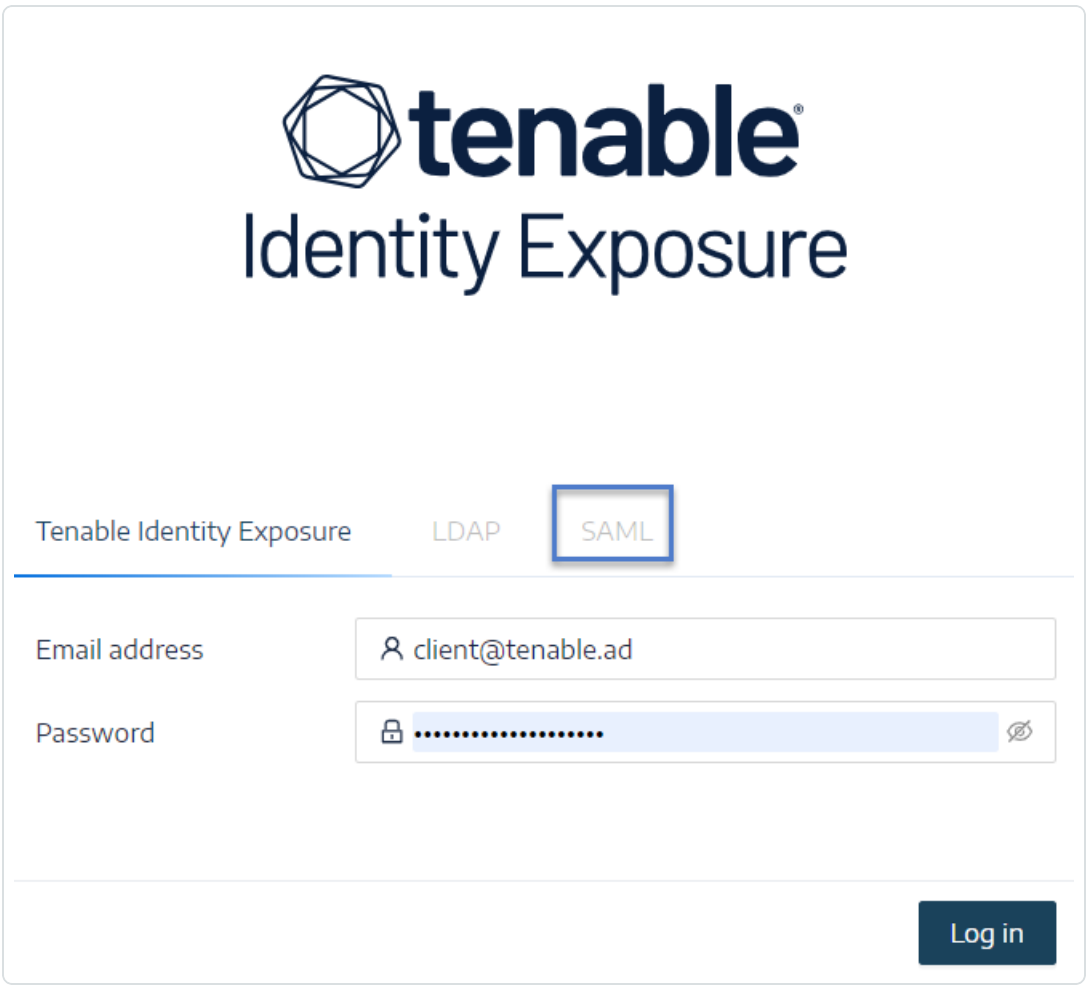
   Tenable Identity Exposure 頁面會隨即開啟。

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。

存取工作區

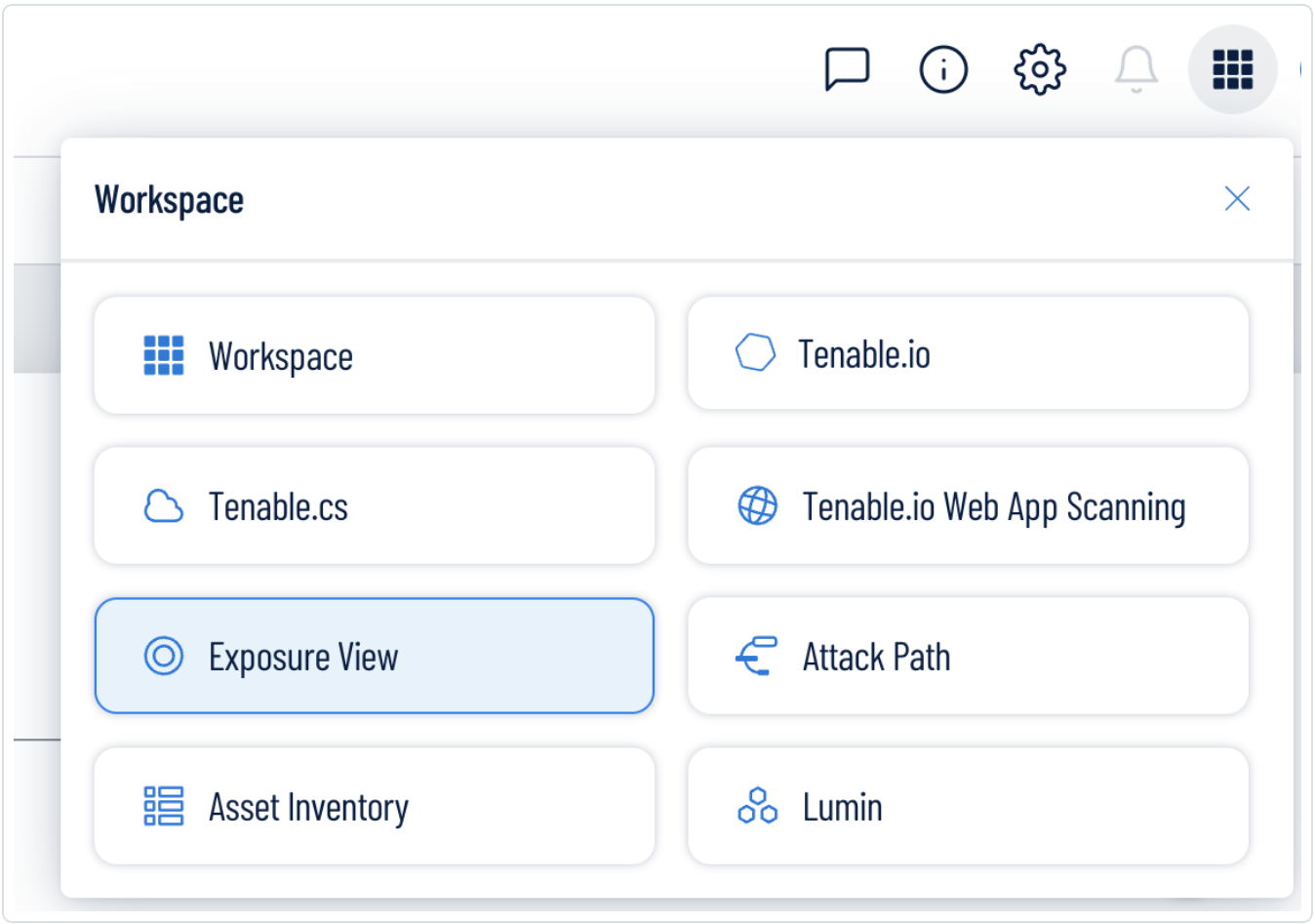
當您登入 Tenable 時，預設會顯示**工作區**頁面。在**工作區**頁面中，您可以在 Tenable 應用程式之間切換，或將預設的應用程式設定為日後略過**工作區**頁面。您也可以前往頂端導覽列中的**工作區**功能表，即可在應用程式之間切換。

開啟工作區功能表

開啟**工作區**功能表的步驟如下：

1. 開啟任何 Tenable 應用程式，並在右上角按一下 ▦ 按鈕。

   工作區功能表隨即會顯示。



2. 按一下應用程式圖塊以開啟。

檢視工作區頁面

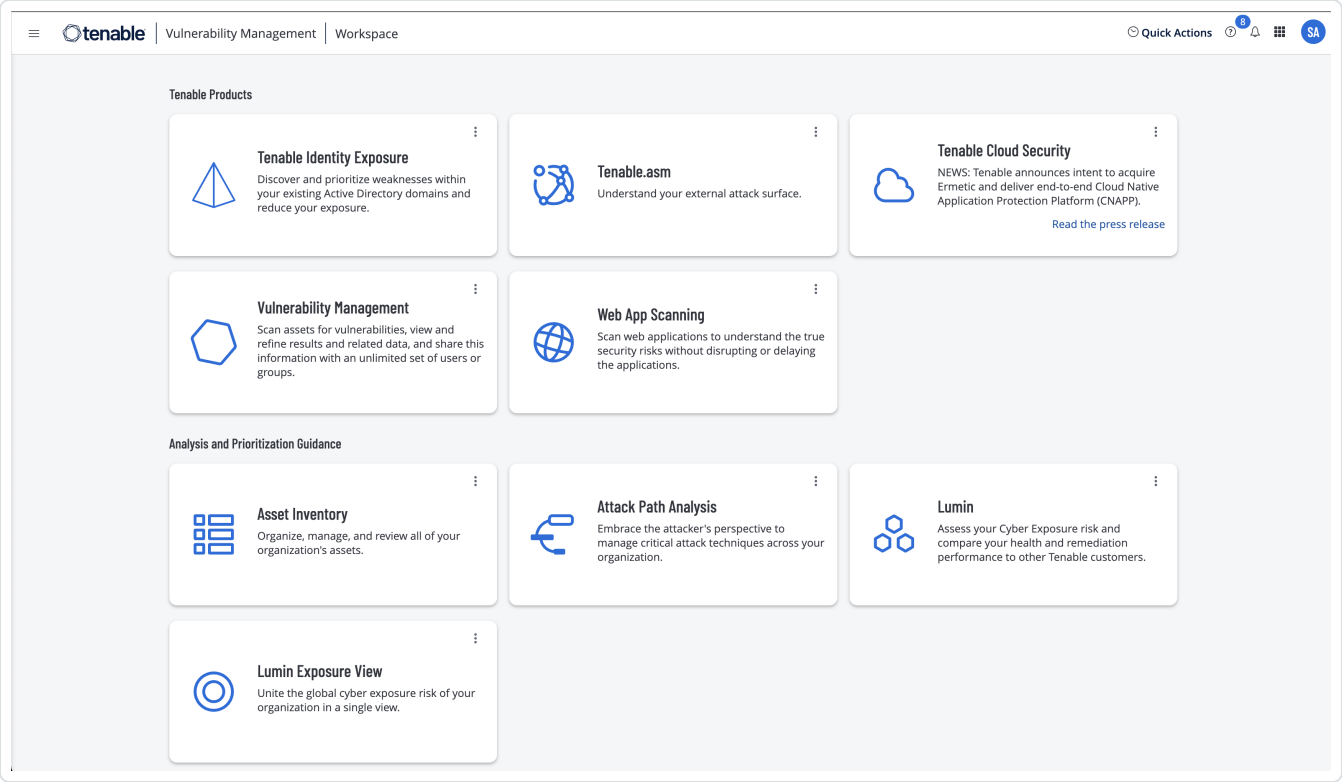
檢視工作區頁面的步驟如下：

1. 開啟任何 Tenable 應用程式，並在右上角按一下 按鈕。

   工作區功能表隨即會顯示。

2. 在**工作區**功能表中，按一下**「工作區」**。

   工作區頁面隨即會顯示。



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。

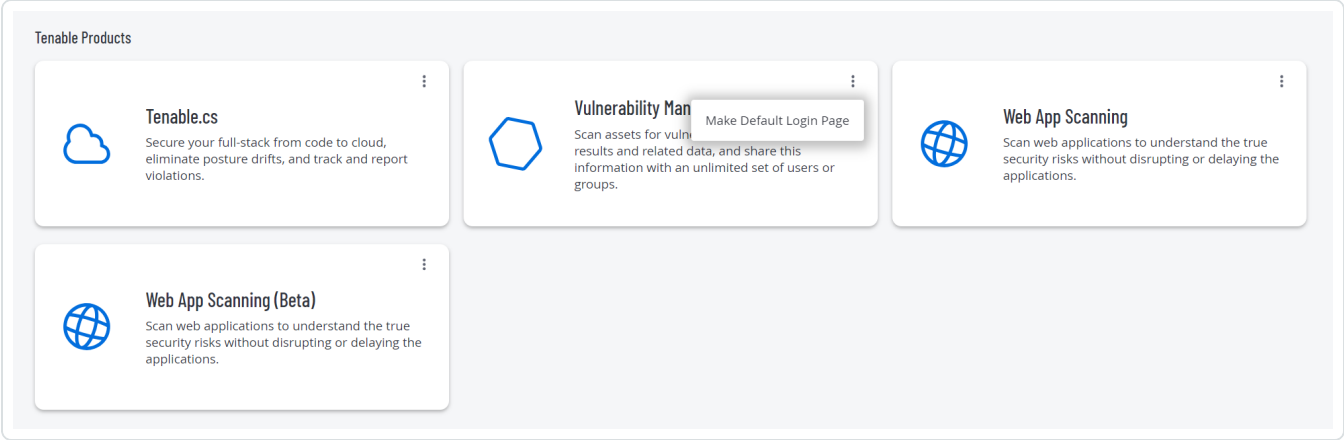
設定預設登入應用程式的步驟如下：

1. 登入 Tenable。

   工作區頁面隨即會顯示。

2. 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。



3. 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. 登入 Tenable。

   工作區頁面隨即會顯示。

2. 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。

3. 按一下**「移除預設登入頁面」**。

   現在**工作區**頁面會在您登入時顯示。

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. 提供以下內容：

- 您的舊密碼。
- 您的新密碼。

c. 在**新密碼確認**方塊中，重新輸入新密碼。

d. 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。

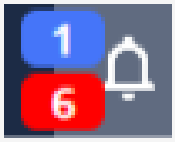
系統會顯示一則訊息，要求您確認。

> **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。

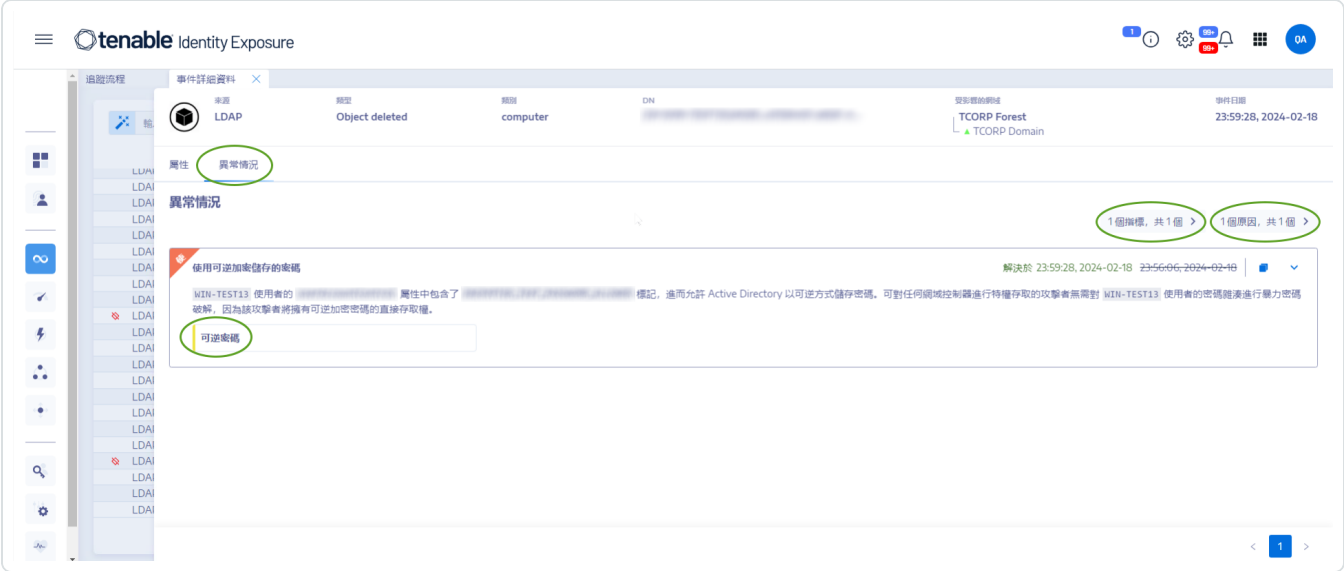
如要檢視與警示關聯的事件：

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 提供了儀表板範本，以便您用來集中處理與貴組織有關的優先問題，其中包括下列範本：

- **AD 合規性和主要風險**：合規性分數、演進和風險嚴重性符合情況
- **AD Risk 360**：按曝險指標嚴重性等級劃分的異常情況演進和問題
- **密碼管理風險**：密碼相關問題
- **使用者監控**：AD 使用者演進、使用者類別計數
- **本機管理員監控**：管理帳戶指標

如要使用範本建立新的儀表板：

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. 您可以執行下列任一動作：
   - 如果窗格為空，請按一下「**新增儀表板**」。
   - 如果窗格已包含至少一個儀表板，請按一下右上角的 >「**新增儀表板**」。

   「**設定儀表板範本**」窗格會隨即開啟。
3. 選取要新增的儀表板。
4. 按一下「**新增儀表板**」。
5. 系統將顯示一則訊息，確認 Tenable Identity Exposure 已建立儀表板和小工具。新的儀表板會顯示在「**儀表板**」窗格的索引標籤下。

如要新增自訂儀表板：

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. 按一下右上角的「  」>「**新增儀表板**」。

   「**設定儀表板範本**」窗格會隨即開啟。
3. 選取底部的「**自訂儀表板**」範本。
4. 輸入儀表板的名稱。
5. 按一下「**新增儀表板**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已建立儀表板。新的儀表板會顯示在「**儀表板**」窗格的索引標籤下。
6. 如需瞭解關於如何將小工具新增至儀表板的資訊，請參閱 小工具。

如要重新命名儀表板：

1. 在「**儀表板**」窗格中，選取要重新命名的儀表板索引標籤。
2. 按一下右上角的 >「**編輯名稱**」。

   「**設定儀表板**」窗格會隨即開啟。
3. 在「**名稱**」方塊中輸入儀表板的另一個名稱。
4. 按一下「**編輯**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已更新儀表板。

如要刪除儀表板：

1. 在「**儀表板**」窗格中，選取要刪除的儀表板索引標籤。
2. 按一下右上角的 >「**刪除儀表板**」。

   系統將開啟「**刪除儀表板**」窗格，並要求您確認刪除。
3. 按一下「**刪除**」。

   系統將顯示一則訊息，確認 Tenable Identity Exposure 已刪除儀表板。

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。 「**曝險指標**」窗格會隨即開啟。 b. 從清單中選取一個或多個指標。或者，您還可以： ■ 在搜尋方塊中輸入指標名稱。 ■ 選取所有指標。 ■ 選取特定嚴重性層級 (嚴重、高度、中度或低度) 的所有指標。 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。 「**樹系和網域**」窗格會隨即開啟。 b. 從清單中選取一個網域。或者，您還可以： ■ 在搜尋方塊中輸入網域名稱。 ■ 選取所有網域。 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

身分識別總管

權限：您的使用者角色必須具備適當的權限才能存取 Microsoft Entra ID 的設定和資料視覺化。如需詳細資訊，請參閱設定角色的權限。

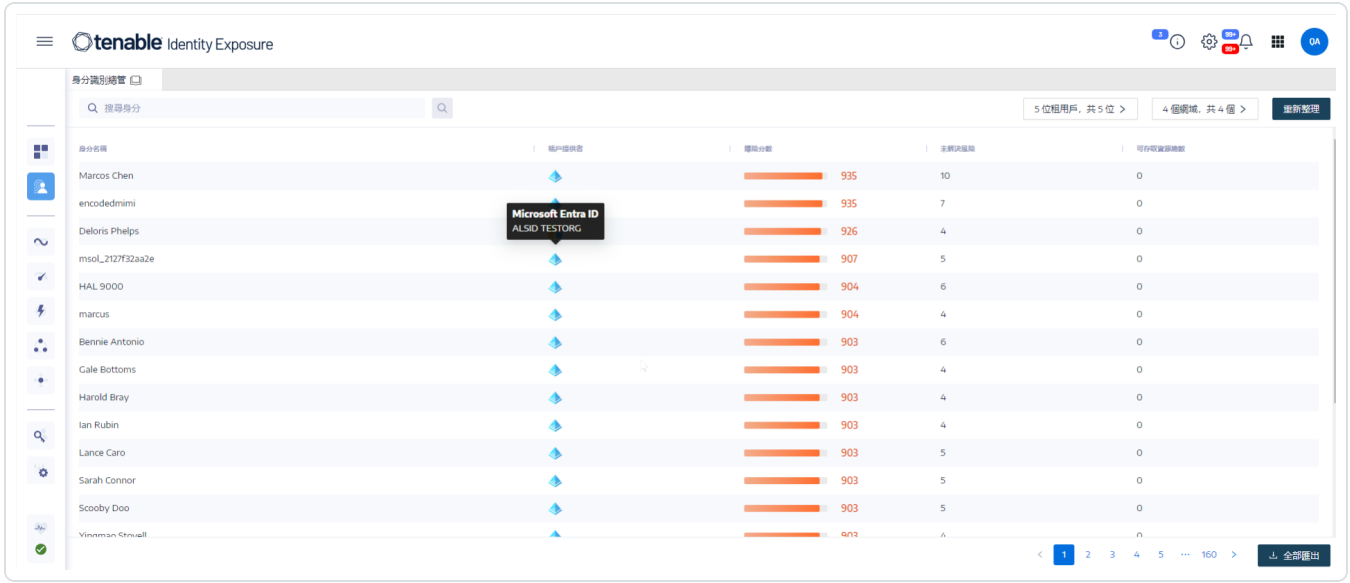
Tenable Identity Exposure 的身分識別總管檢視整合了 Active Directory 和 Microsoft Entra ID 中的身分識別資訊。此檢視畫面會顯示每個所列資產的身分風險評分 (測試版)，以及遭入侵身分的潛在影響範圍。

如要存取身分識別總管：

注意：您只有在使用 Microsoft Entra ID 功能時，才能看到身分識別總管。如需詳細資訊，請參閱 Microsoft Entra ID 支援。

- 在 Tenable Identity Exposure 中，按一下左側導覽列中的身分識別總管圖示 。

  「**身分識別總管**」窗格會隨即開啟。



「**身分識別總管**」窗格會顯示可存取資源總數的下列資訊：

- **身分識別名稱**：身分識別提供者下方的使用者帳戶名稱。
- **帳戶提供者**：身分識別提供者。

- **曝險分數**：Tenable Identity Exposure 透過評估資產或身分及其弱點對於每個身分識別提供者的重要性來計算此指標，並將其彙總以提供指定身分的整體曝險分數。

  注意：Tenable Identity Exposure 只會在您擁有 Tenable One 授權的情況下顯示曝險分數。

- **未解決的風險**：Microsoft Entra ID 曝險指標在掃描資產時偵測到的結果數量。如需詳細資訊，請參閱與 Microsoft Entra ID 相關的曝險指標。
- **可存取資源總數**：此資產可存取 (讀取、寫入等) 的任何類型資源的數量

如要搜尋身分識別資訊：

1. 在「**身分識別總管**」窗格的「**搜尋**」方塊中輸入使用者或帳戶的名稱。
2. 按一下 圖示。

   Tenable Identity Exposure 會顯示比對結果。

如要匯出身分識別資訊：

1. 在「**身分識別總管**」窗格底部，按一下「**全部匯出**」。

   「**匯出身分識別資訊**」窗格會隨即開啟。
2. 按一下「**全部匯出**」。

   Tenable Identity Exposure 會將檔案下載到本機。

追蹤流程

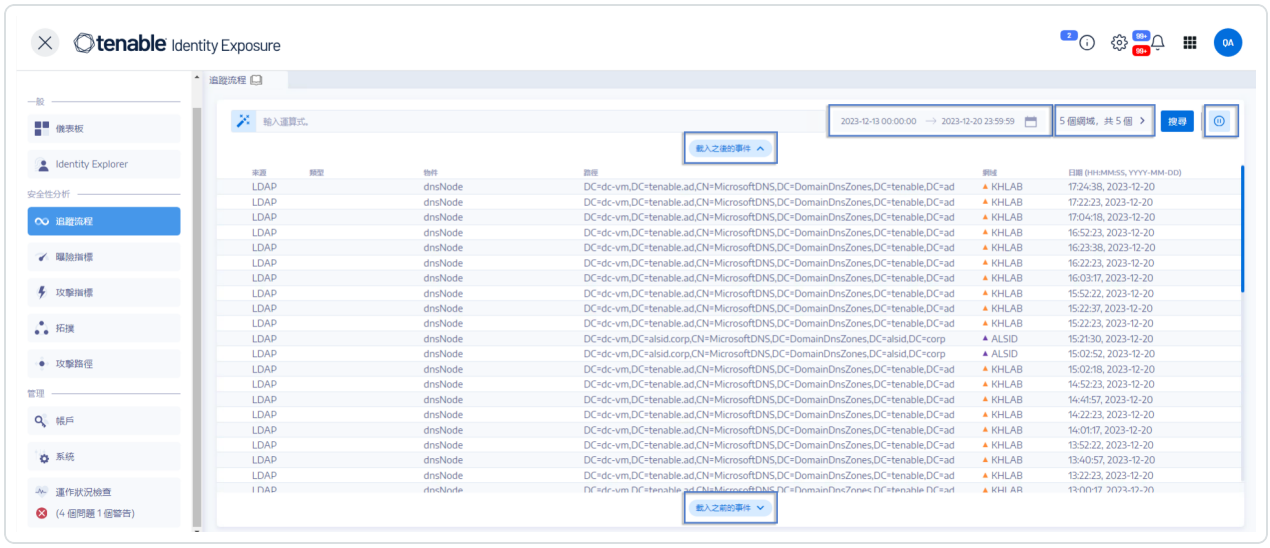
Tenable Identity Exposure 的追蹤流程顯示對於影響 AD 基礎架構事件的即時監控和分析。您可以用它來識別嚴重弱點及其建議的修復方法。

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。

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：

1. 在**追蹤流程**頁面頂端，按一下日曆方塊。
2. 選取開始日期和結束日期。
3. 按一下「**搜尋**」。

   Tenable Identity Exposure 將使用選取的時間範圍更新追蹤流程表。

如要選取網域：

1. 在**追蹤流程**頁面頂端，按一下「**n/n 網域 >**」。

   「**樹系和網域**」窗格會隨即開啟。

2. 選取樹系和網域。

3. 按一下「**篩選選取的項目**」。

   Tenable Identity Exposure 將使用所選的樹系和網域資訊更新追蹤流程表。

如要檢視事件：

- 在追蹤流程表中，按一下包含您要瀏覽之事件的行。

  「事件詳細資料」窗格會隨即開啟。如需詳細資訊，請參閱事件詳細資料。

如要暫停和重新啟動追蹤流程：

- 執行下面的其中一項動作：
  - 按一下 ⏸ 圖示可暫停追蹤流程。

    暫停追蹤流程會停止最近事件的自動垂直捲動，但分析會在幕後繼續執行，您還可以對事件執行搜尋。
  - 按一下 ▶ 圖示可重新啓動追蹤流程。

如要載入之後或之前的事件：

- 在追蹤流程頁面中，執行下面的一個動作：
  - 按一下「載入之後的事件」
  - 按一下「載入之前的事件」

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。 可能有兩個來源： • 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)。 • 用於共用檔案、印表機等的伺服器訊息區 (SMB) 通訊協定。 **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。 **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： • ACL 已變更 • SPN 已變更 • 成員已移除 • 新成員 • 新信任 • 已新增未知的檔案類型 • 新物件 • 物件已刪除 • 密碼已變更 • UAC 已變更

	• 已連結新的 GPO • GPO 連結已刪除 • 所有者變更 • 已重新命名檔案 • 已建立 SPN • 驗證重設失敗 • 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

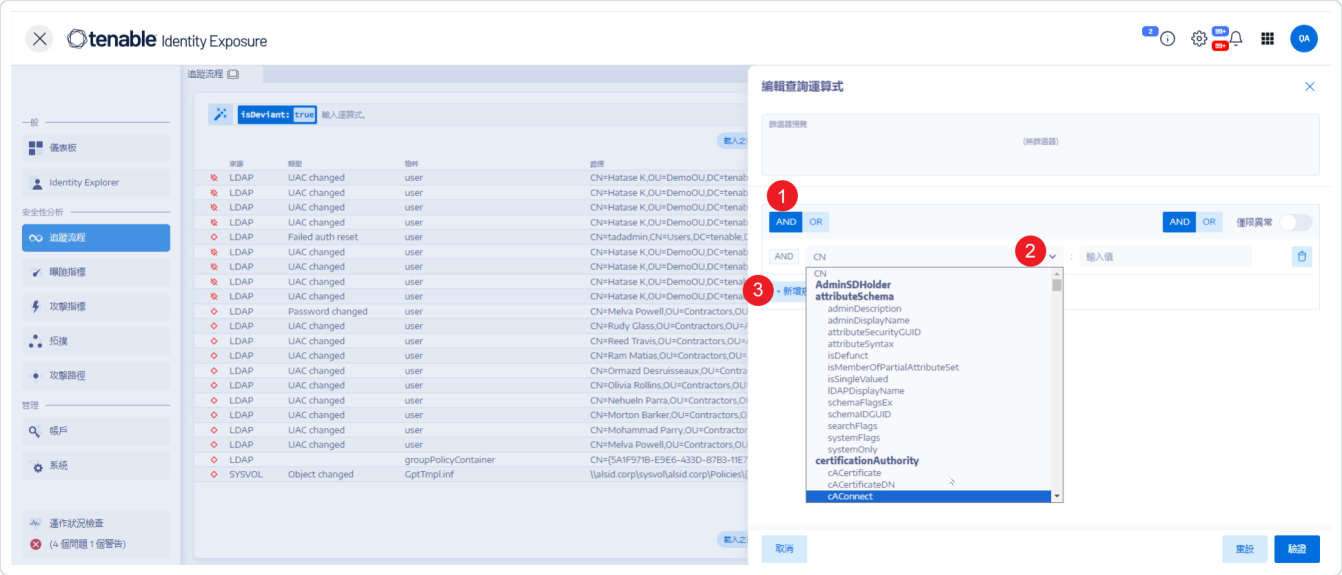
搜尋精靈允許您建立和組合查詢運算式。

- 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：

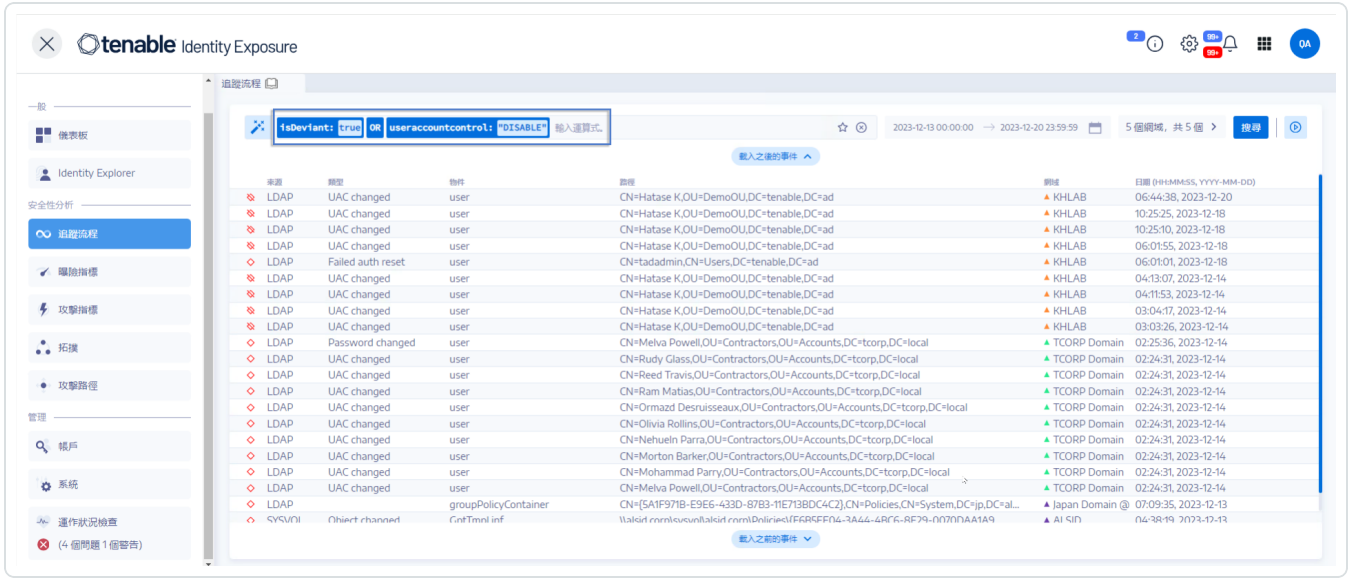
1. 在 Tenable Identity Exposure 中，按一下「**追蹤流程**」以開啟追蹤流程頁面。
2. 在搜尋方塊中輸入查詢運算式。
3. 您可以按如下方式篩選搜尋結果：
    - 按一下「**日曆**」方塊以選取開始日期和結束日期。
    - 按一下「**n/n 網域**」以選取樹系和網域。
4. 按一下「**搜尋**」。

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

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。



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"`

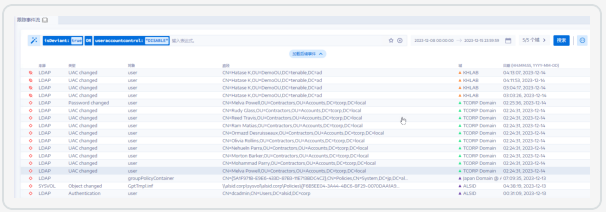
  > **注意**：此處的 `type` 是指物件屬性，而非欄標頭。

自訂追蹤流程查詢

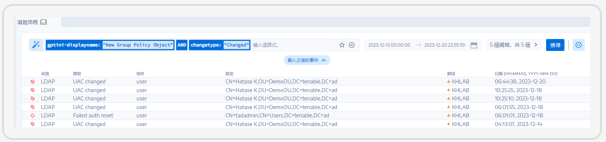
追蹤流程允許您擴展 Tenable Identity Exposure 的功能，而不限於預設的攻擊指標和曝險指標監控。您可以建立自訂查詢以快速擷取資料，也可以將查詢用作 Tenable Identity Exposure 可向您的安全資訊和事件管理 (SIEM) 系統傳送的自訂警示。

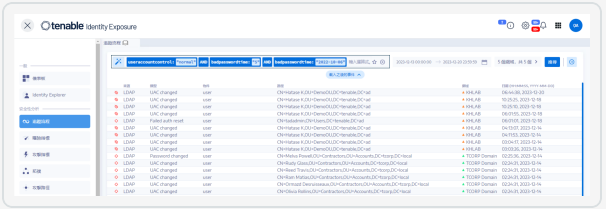
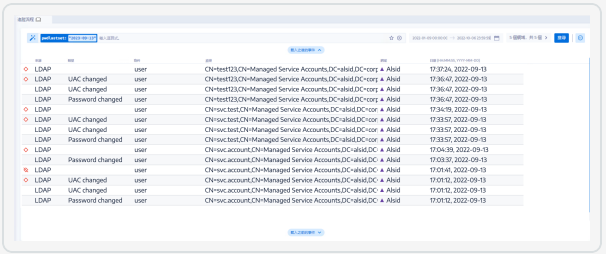
以下範例顯示 Tenable Identity Exposure 中實用的自訂查詢。

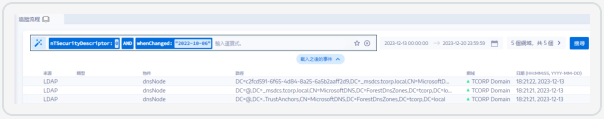
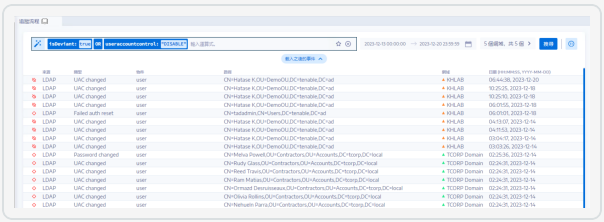
使用案例	說明

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。
	• **啟動路徑中的指令碼查詢：**
	`globalpath: "sysvol" AND types: "Scriptsini"`
	注意：此處的 `types` 是指物件屬性，而不是欄標題。
	• **SYSVOL 監控查詢**：
	`globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")`
	 

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。 • **GPO 監控查詢：**

	`gptini-displayname:"New Group Policy Object" AND changetype:"Changed"` 

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。
	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。
	• **驗證失敗查詢：**
	`useraccountcontrol:"Normal" AND badpwdcount:"<ACCOUNT_LOCKOUT_THRESHOLD>" AND badpasswordtime:"<DATE_TIME_STAMP>"`
	 
	• **密碼重設查詢：**
	`pwdlastset:"<DATE_TIME_STAMP"`
	 

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。 **注意**：您必須提供日期/時間變數。 • **物件權限查詢：** `ntsecuritydescriptor:0 AND whenchanged:"DATE_TIME_STAMP"` 
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。 • **管理員變更查詢：** `isDeviant:true AND cn:"admins"` 

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

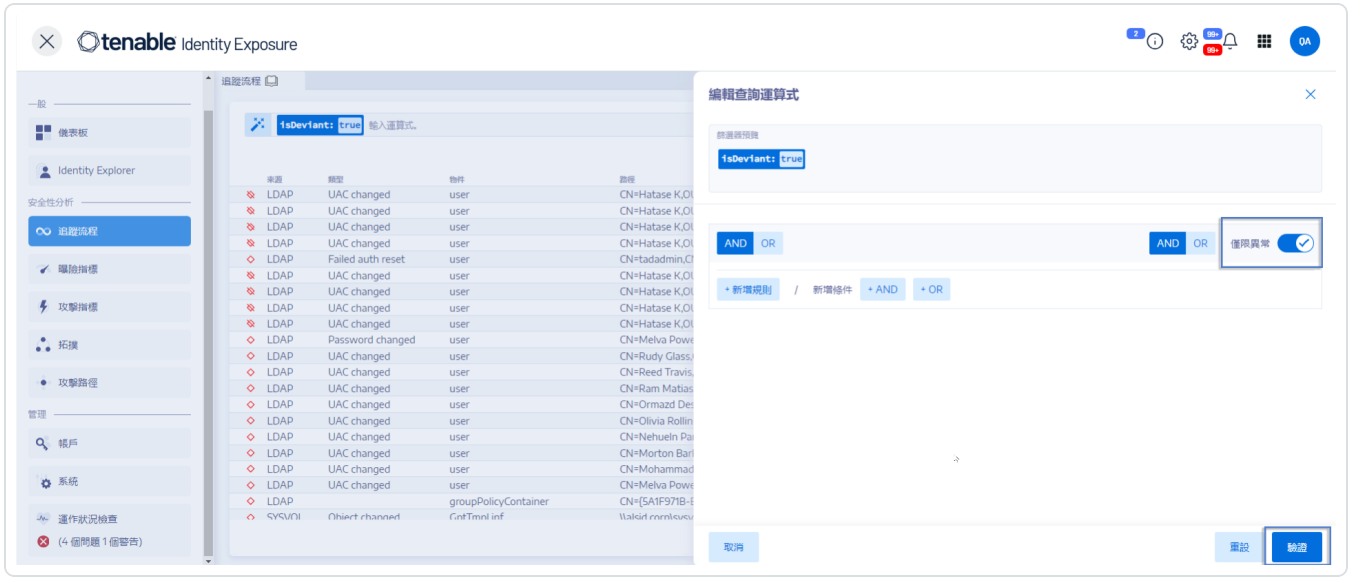
顯示異常事件

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：

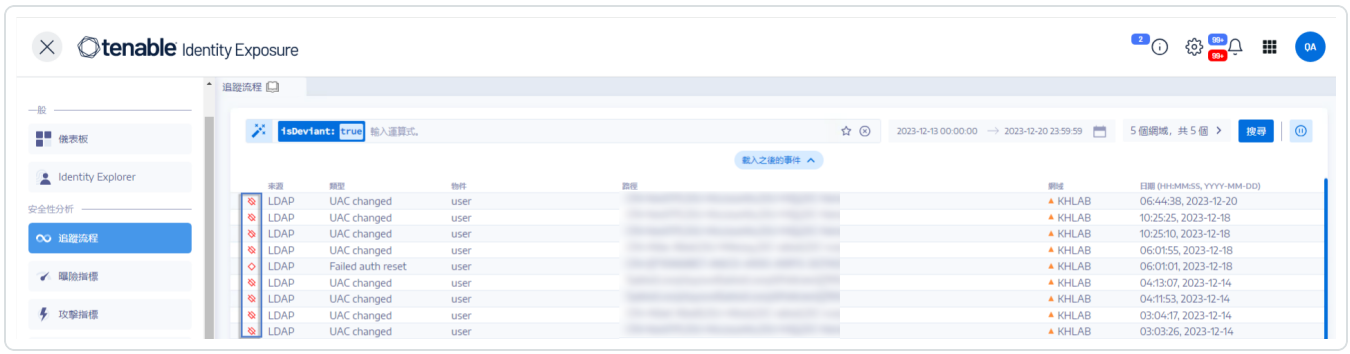
1. 在 Tenable Identity Exposure 中，按一下「**追蹤流程**」以開啟追蹤流程頁面。
2. 按一下搜尋方塊旁邊的 圖示。

   「**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。

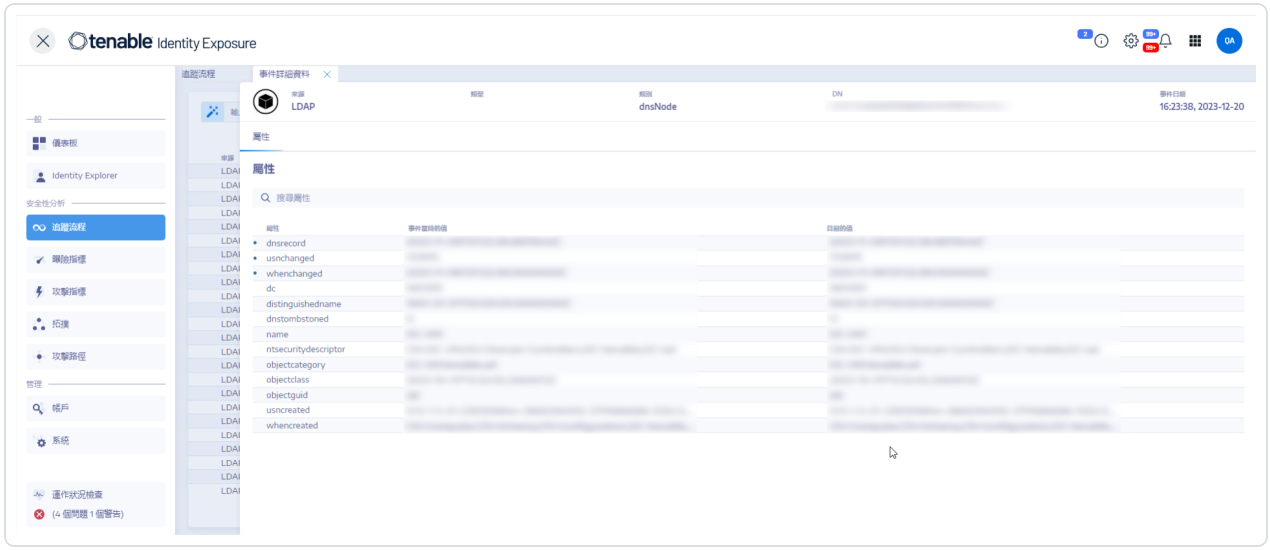
如要檢閱事件詳細資料：

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**是一個技術元素 (可以單獨存在或是與另一個異常物件相關聯)，會讓曝險指標 (IoE) 的攻擊媒介起作用。



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。

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：

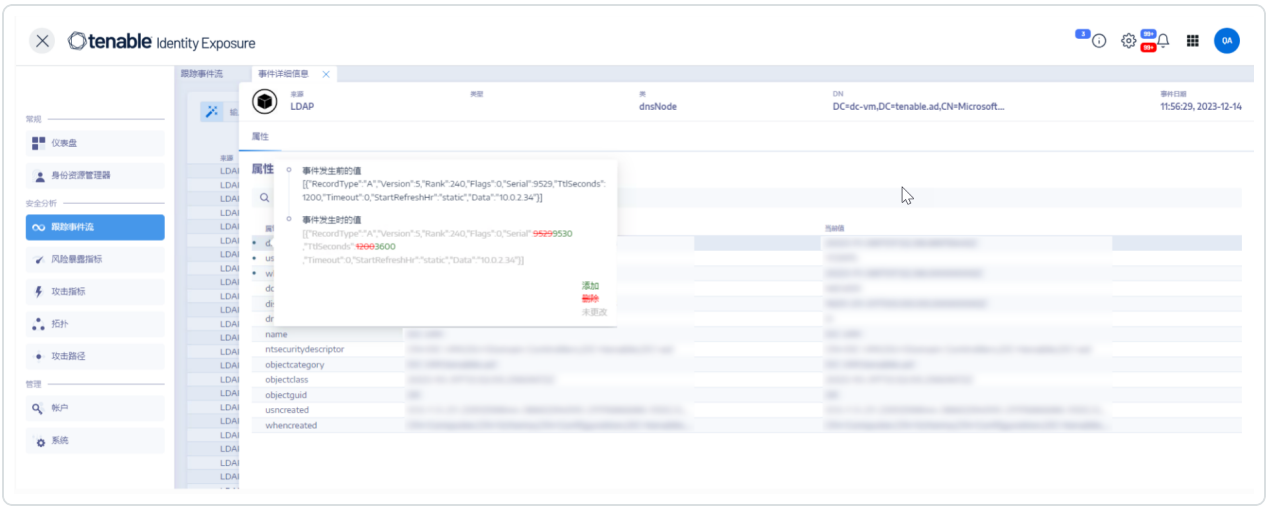
1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的「**追蹤流程**」。

   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**



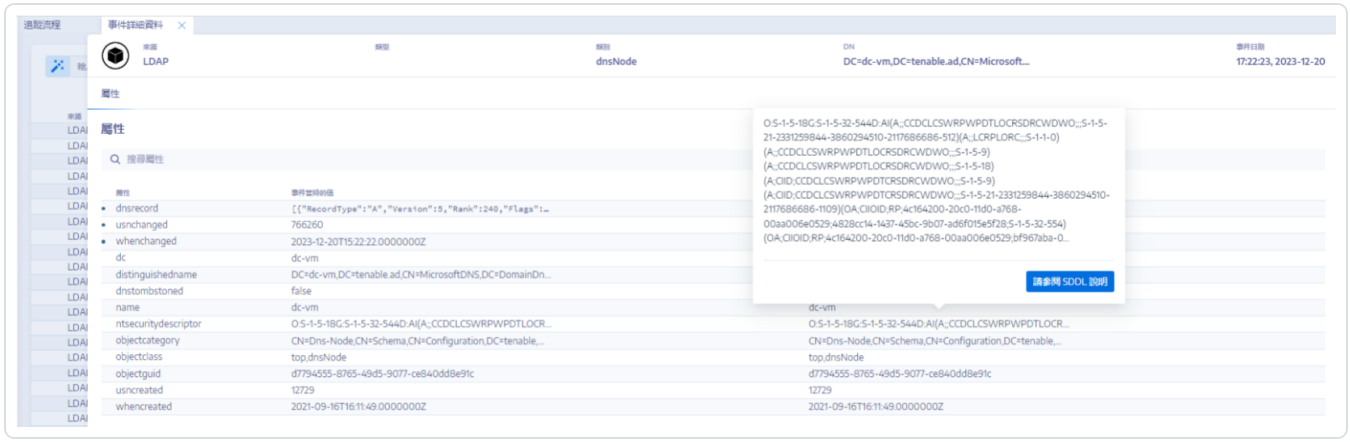
「ntsecuritydescriptor」屬性

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：

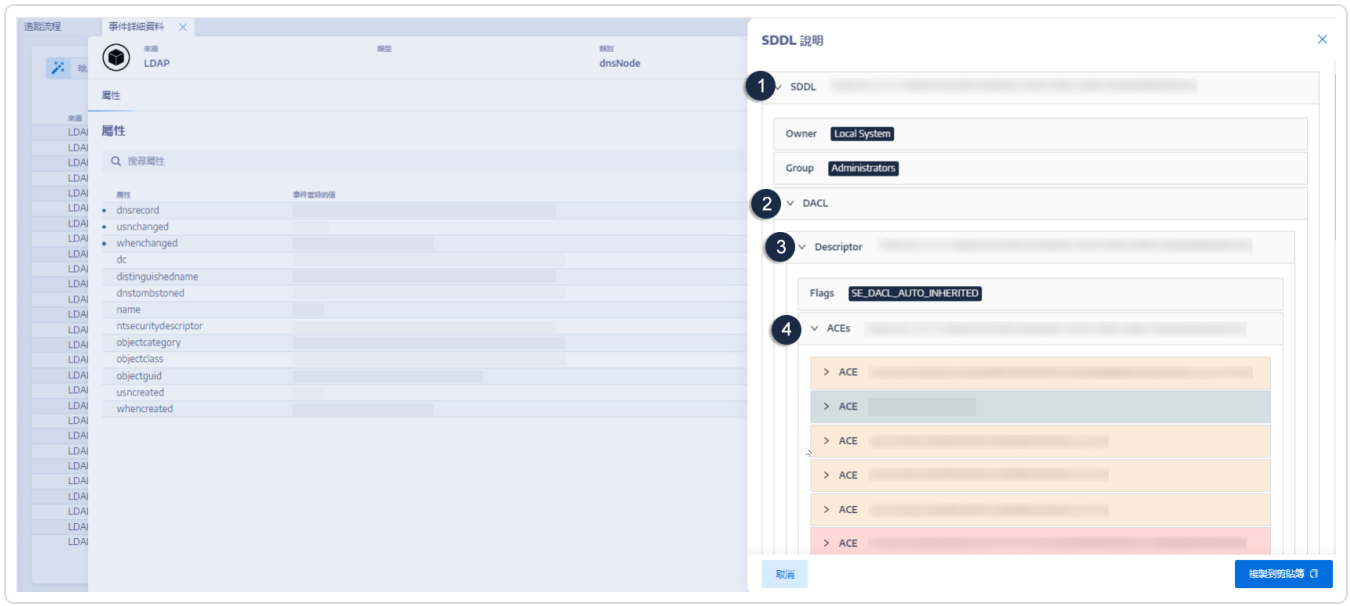
1. 在 Tenable Identity Exposure 中，按一下「**追蹤流程**」以開啟追蹤流程頁面。
2. 按一下以選取追蹤流程表中的項目。

   「**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**。



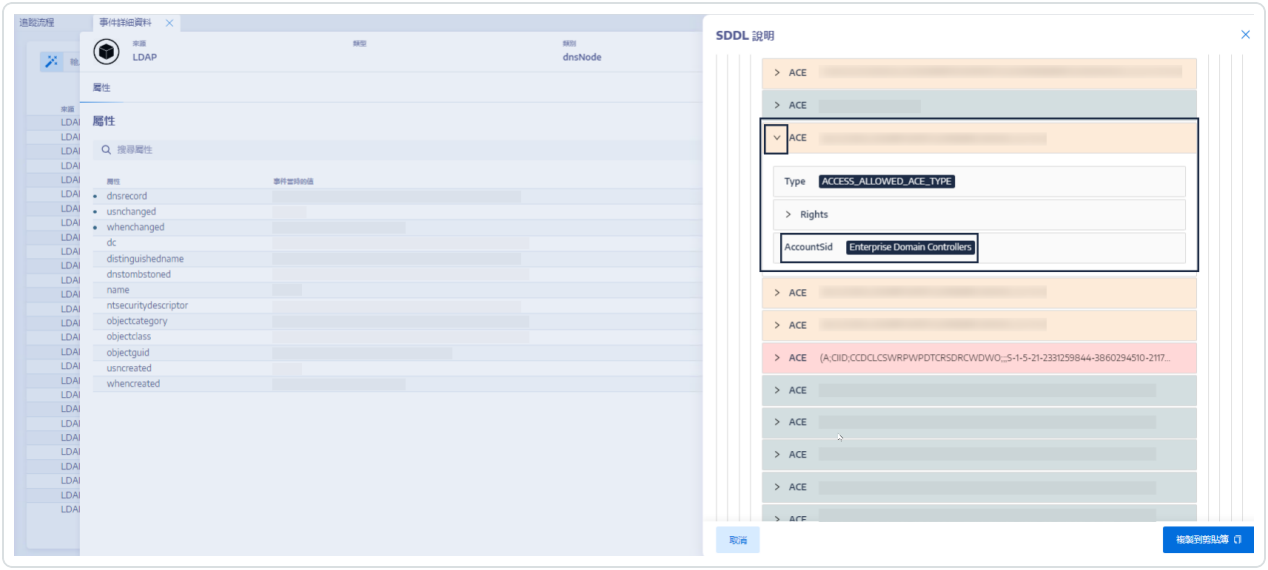
4. 按一下「**檢閱 SDDL 描述**」。

   「n**SDDL 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

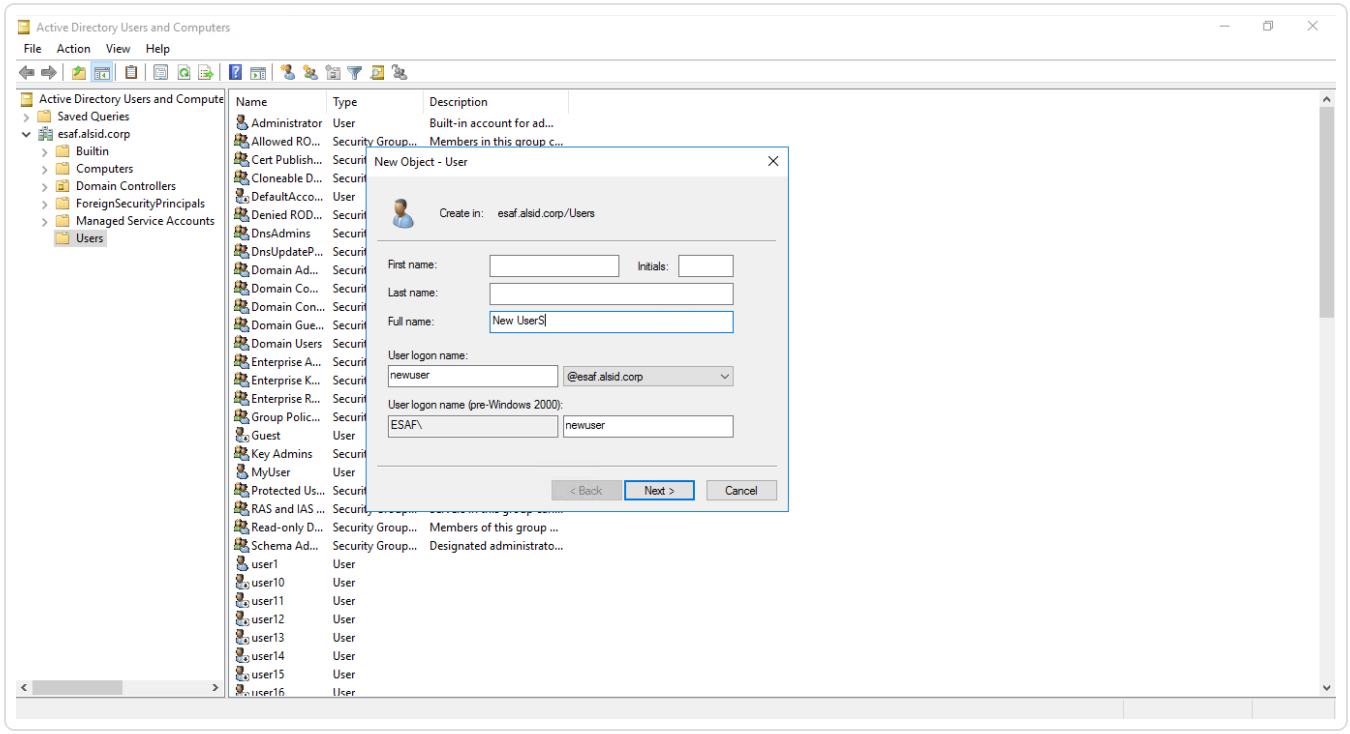
為幫助瞭解追蹤流程的行為，下面透過兩個範例說明您在 Active Directory (AD) 介面中執行的作業如何反映在追蹤流程頁面中。

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。

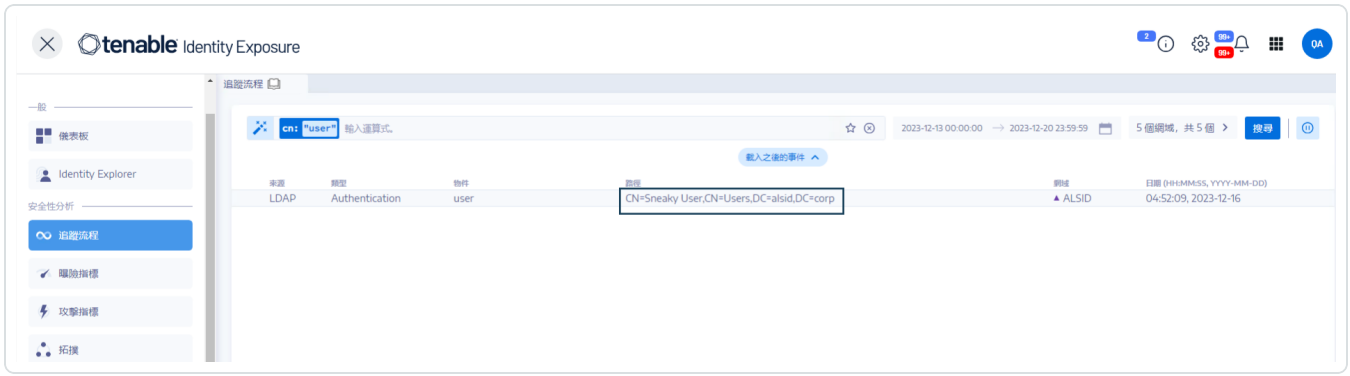
注意：這些範例並不詳盡，無法涵蓋所有可能的情況。

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。

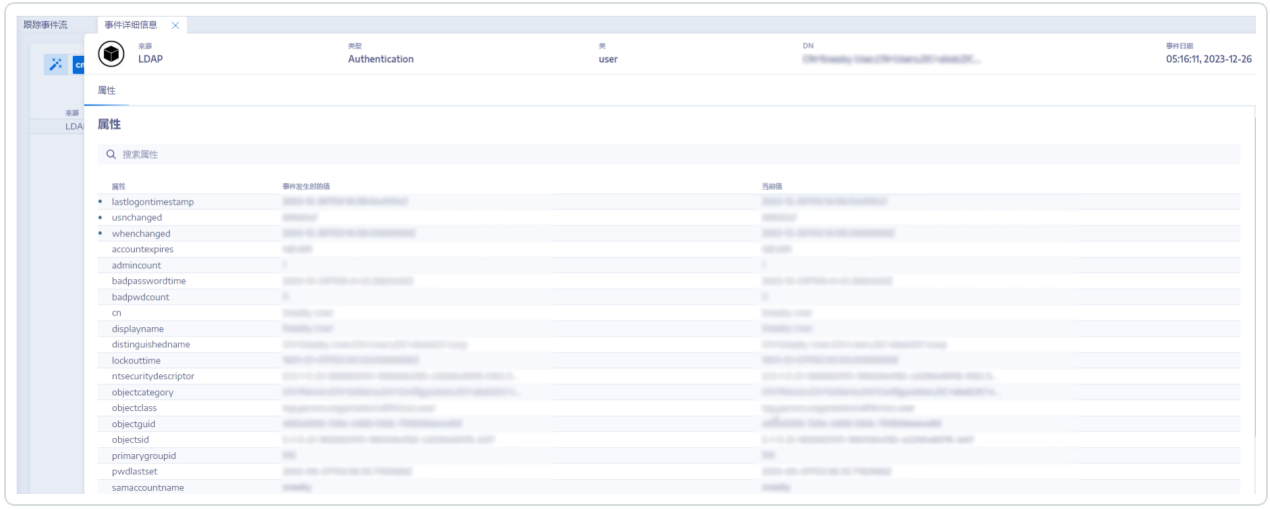


- 在最終使用者端，Tenable Identity Exposure 會更新**追蹤流程**頁面。請參閱指示*新物件*的**類型**欄。



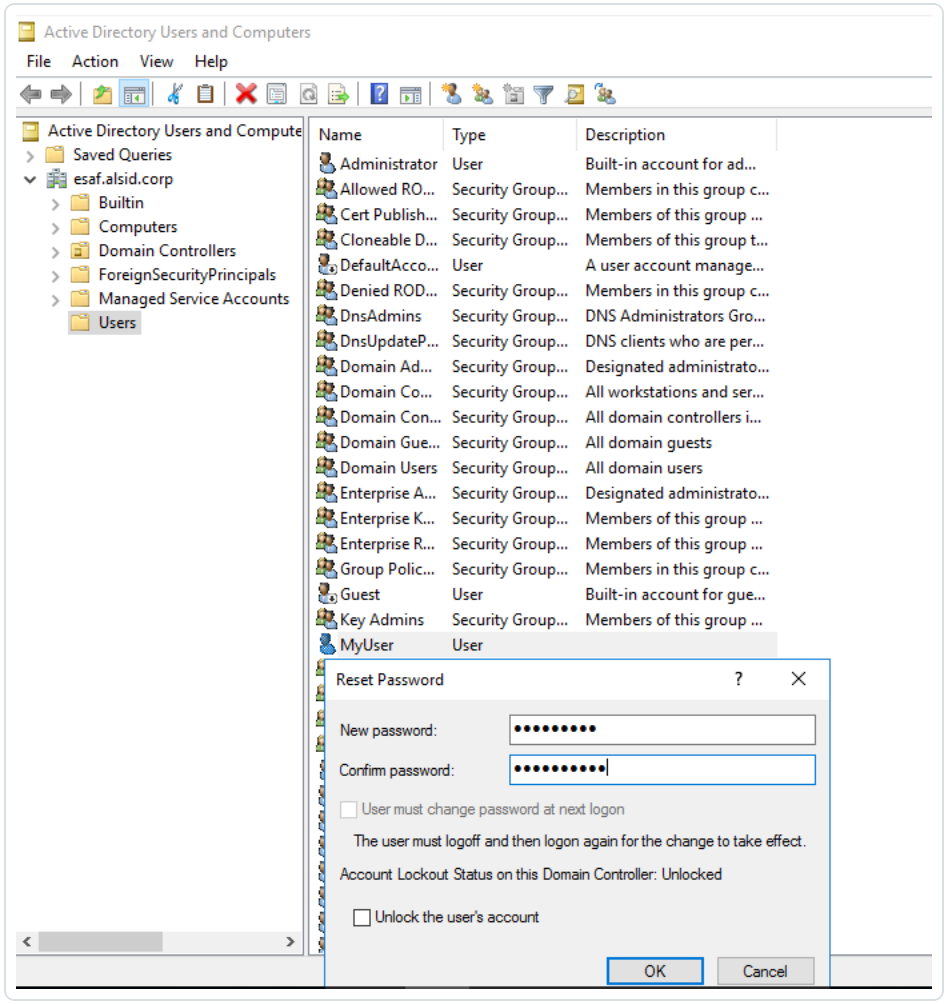
- **事件詳細資料**頁面也會反映這一變化。屬性名稱左側的藍點表示發生了更新。

  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？

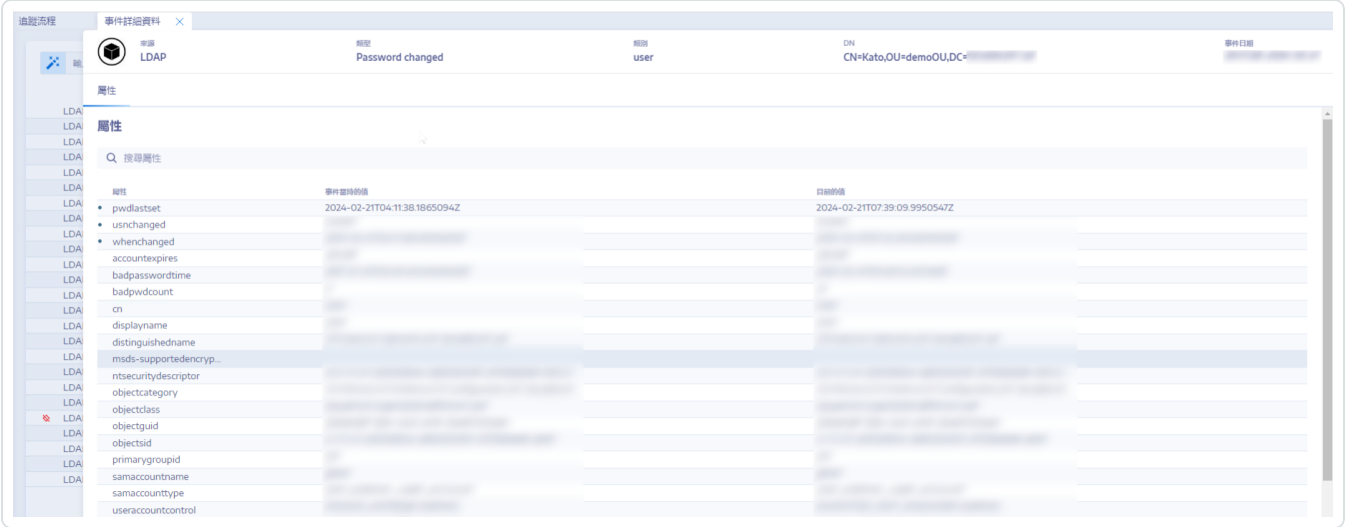
- 在管理員端，您輸入重設使用者密碼所需要的各種資訊。



- 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

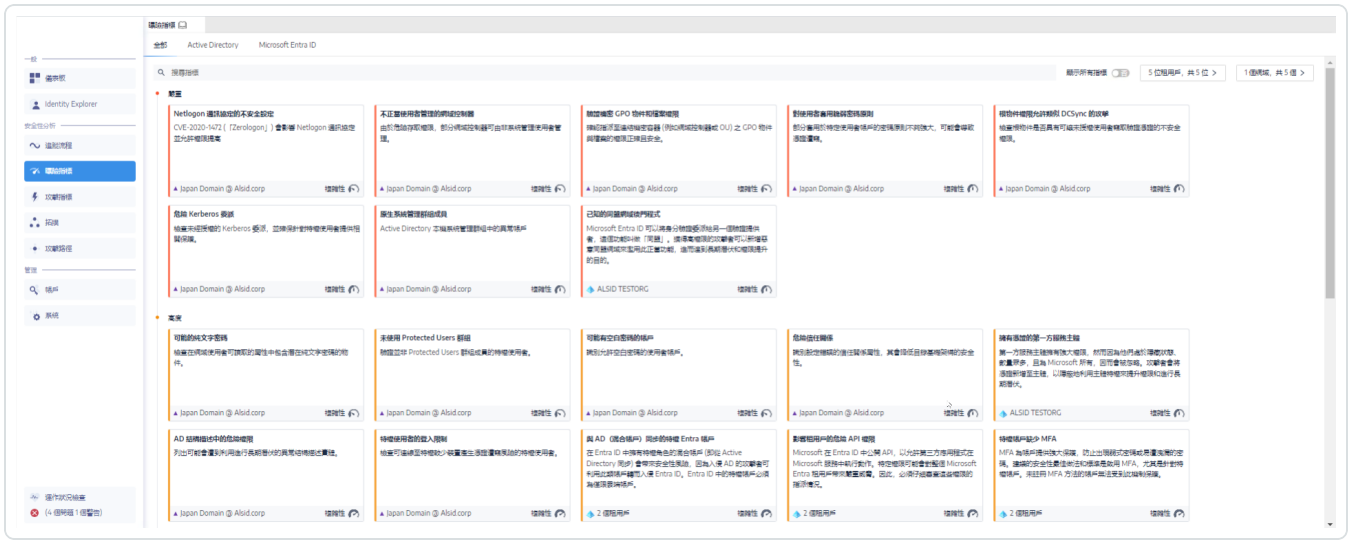
Tenable Identity Exposure 會透過曝險指標 (IoE) 衡量您 AD 基礎架構的安全成熟度，並向其監控和分析的事件流程指派嚴重性等級。Tenable Identity Exposure 在偵測到安全性降低時會觸發警示。

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」**。



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。只有在管理員出現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。

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
- 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： • 執行摘要 - 問題概覽，有助於您做出適當決策。 • 文件 - 曝險指標 (IoE) 上外部資源的連結。 • 攻擊者已知工具 - 入侵攻擊工具的名稱。 • 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。 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： • 執行摘要提供 Tenable Identity Exposure 建議的解決方案概覽。 • 「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。 • 「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
- 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」**。

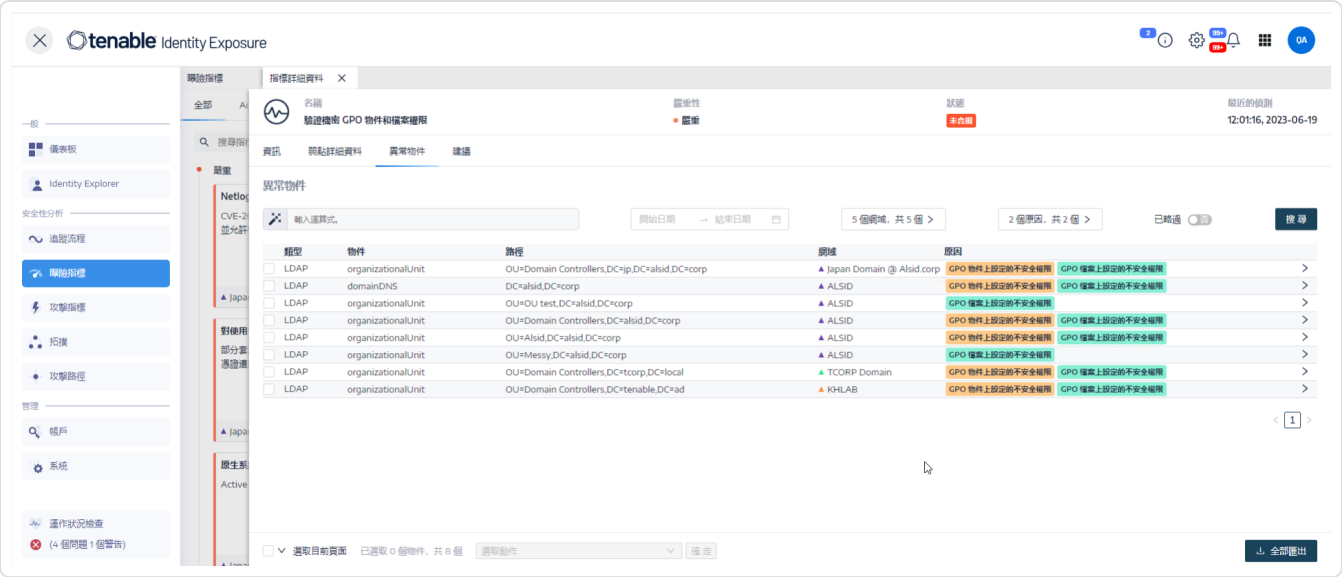
   「曝險指標」頁面會隨即開啟。根據預設，Tenable Identity Exposure 僅顯示包含異常情況的曝險指標 (IoE)。

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
- 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

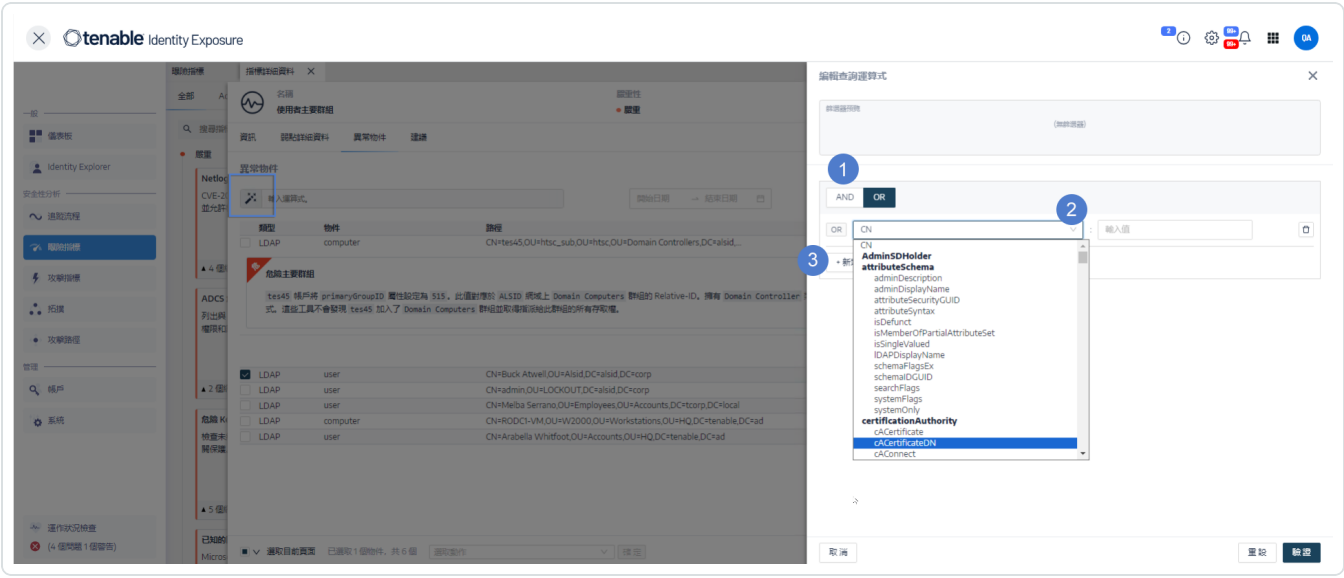
搜尋精靈可以協助您建立查詢運算式。

- 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。

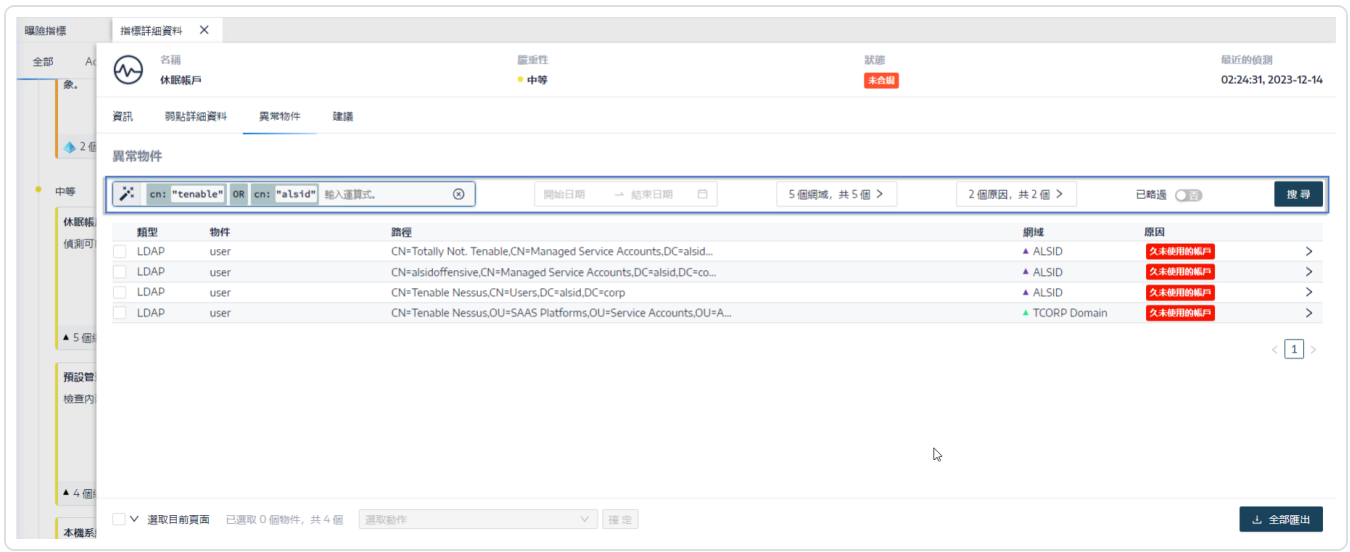
6. 按一下「**驗證**」以執行搜尋，或按一下「**重設**」以修改您的查詢運算式。

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
- 罪證屬性

略過異常物件

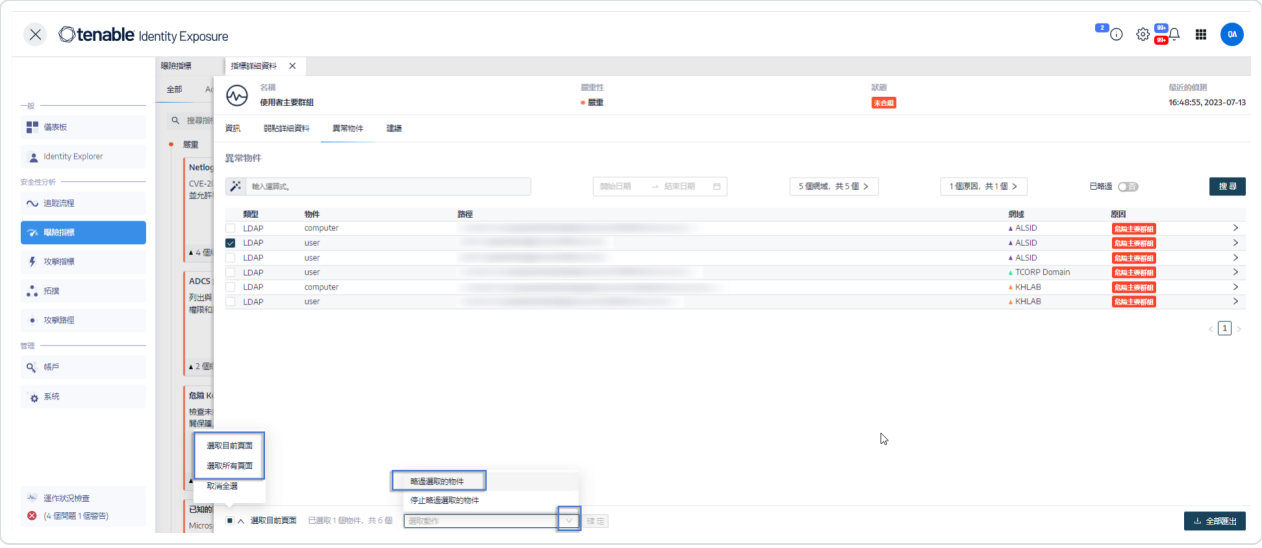
為防止調查或報告時畫面雜亂，您可以強制 Tenable Identity Exposure 在特定時段內略過某些異常物件，以篩除這些物件。您可以選擇略過一個或多個異常物件。您可以立即套用自訂篩選器，也可以指定啟動篩選器的時間範圍。

注意：略過物件不會導致 Tenable Identity Exposure 解析此物件。

如要略過異常物件：

1. 在 Tenable Identity Exposure 中顯示 異常物件 清單
2. 選取要略過異常物件前面的核取方塊。
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 會顯示略過的異常物件。

另請參閱

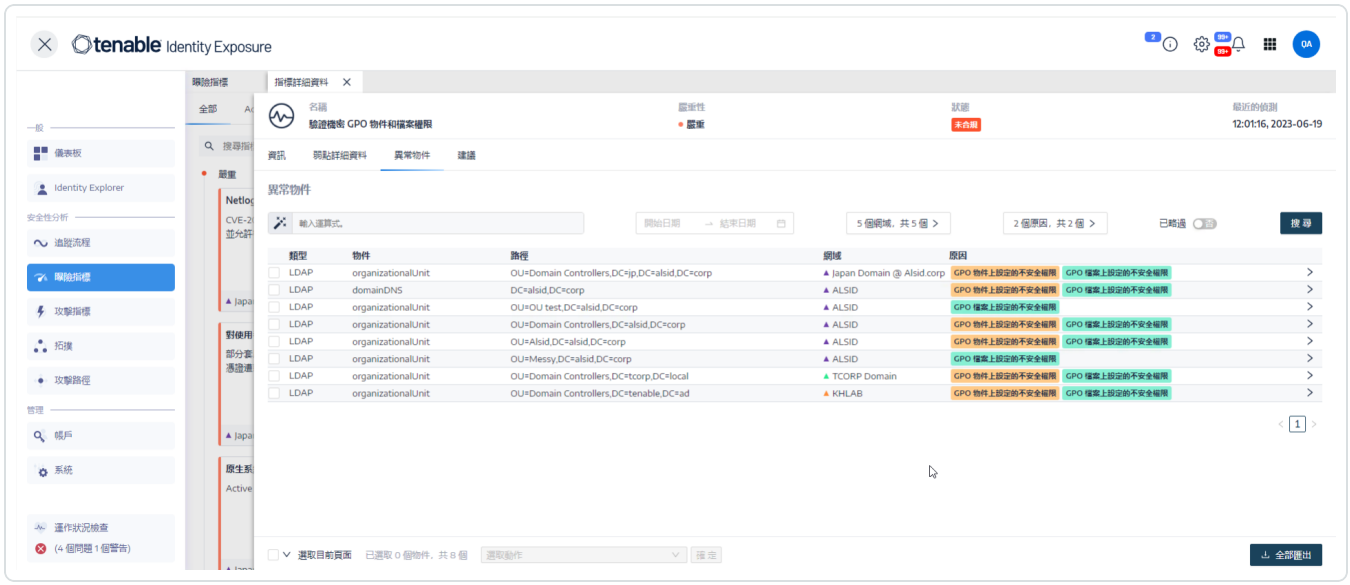
- 曝險指標
- 曝險指標詳細資料
- 異常物件
- 搜尋異常物件
- 罪證屬性

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。

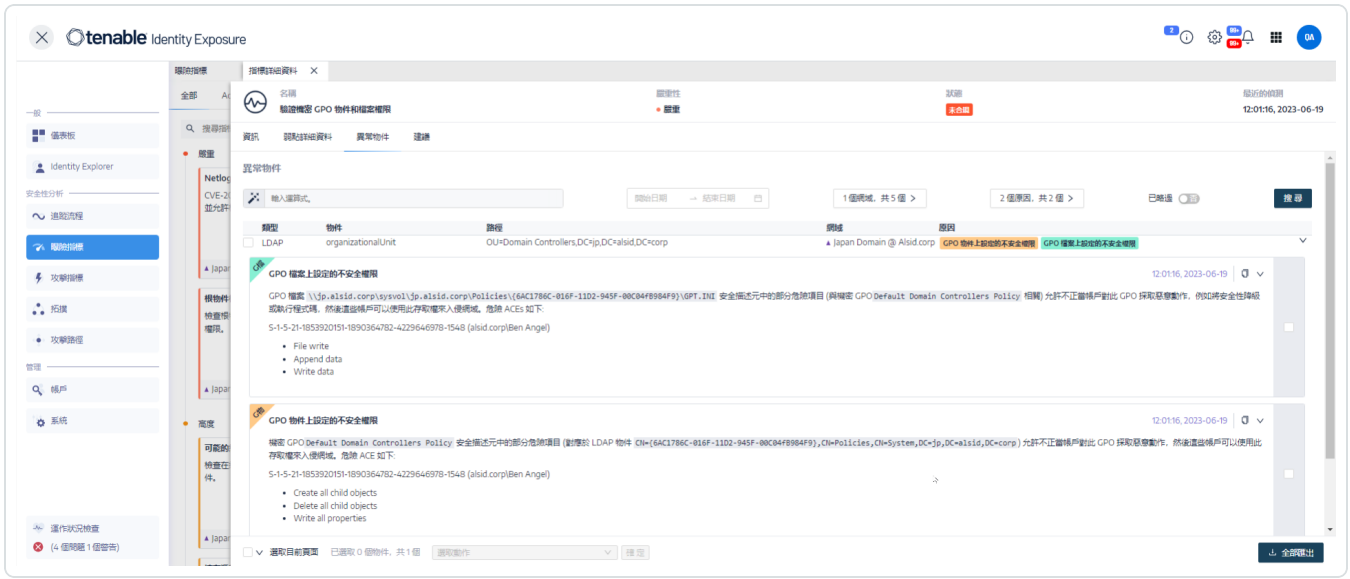
如要檢視罪證屬性：

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

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。

與 Microsoft Entra ID 相關的曝險指標

Microsoft Entra ID 特定的曝險指標

Tenable Identity Exposure 有專用的曝險指標 (IoE), 可針對 Microsoft Entra ID 中資產的潛在弱點發出警示。

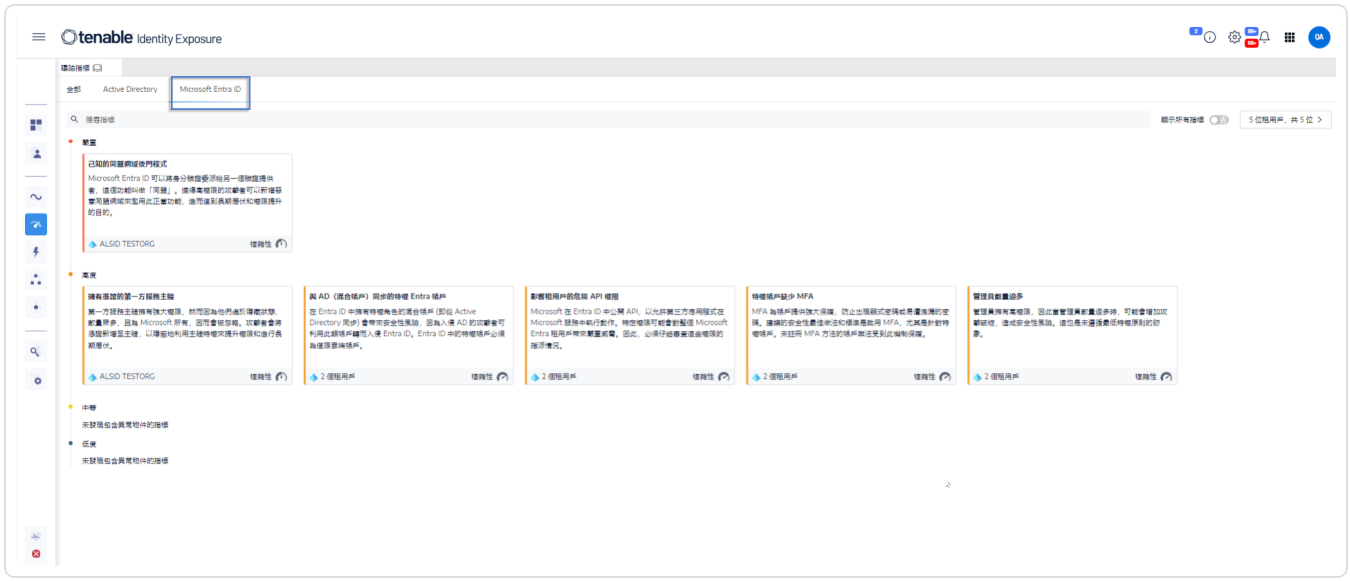
如要顯示 Microsoft Entra ID 曝險指標 (IoE):

1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的曝險指標 (IoE) 圖示 。

   「曝險指標 (IoE)」窗格會隨即開啟。

2. 按一下「**Microsoft Entra ID**」索引標籤。

   Tenable Identity Exposure 會顯示觸發結果與 Microsoft Entra ID 相關的曝險指標 (IoE)。



3. 按一下您要調查的曝險指標 (IoE) 圖塊。

4. 「指標身分識別詳細資料」窗格會隨即開啟，其中包含以下資訊：

   - **弱點資訊**：曝險如何導致潛在攻擊發生。
   - **結果**：有關身分識別提供者類型的詳細資料和風險說明。
   - **建議**：修復威脅的步驟。

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

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)。

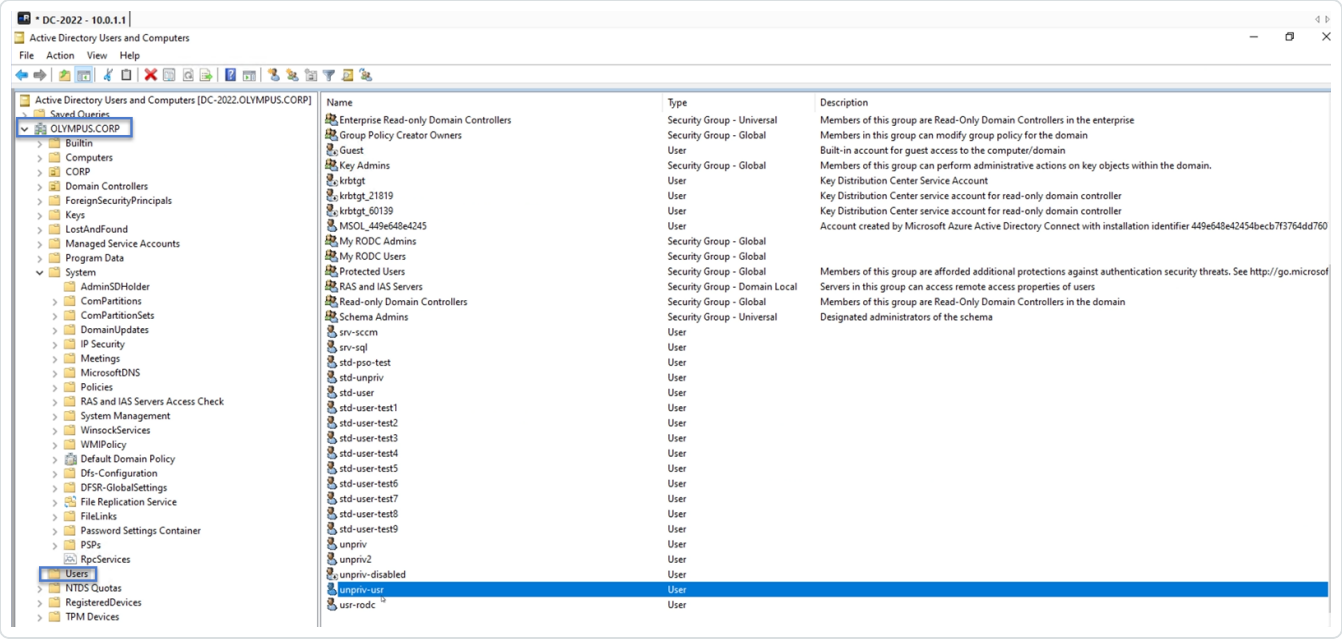
2. 按一下**標準使用者上設定的 AdminCount 屬性**曝險指標 (IoE) 的圖塊。

   「指標詳細資料」窗格會隨即開啟。

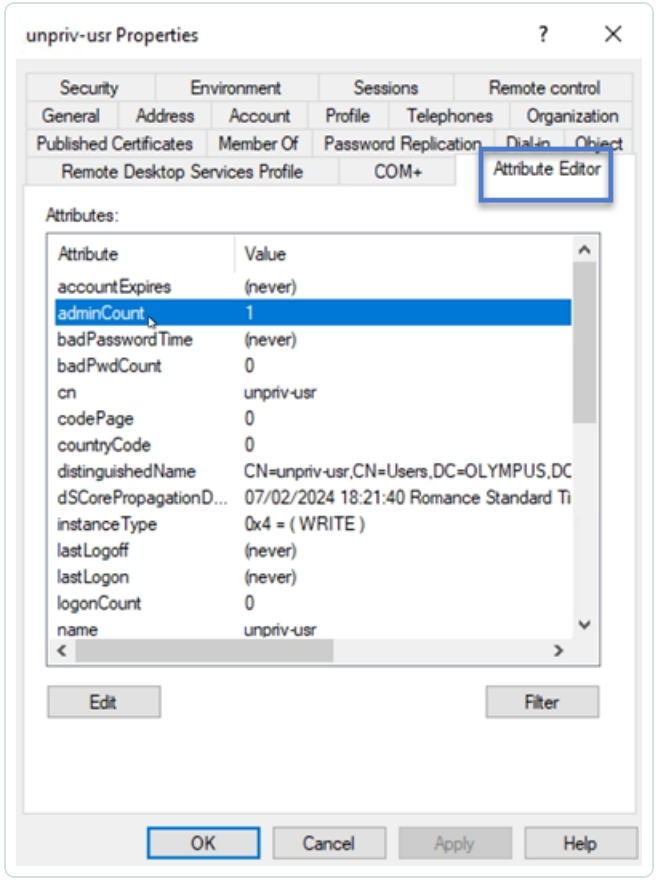
3. 將游標停留在異常物件上並按一下即可顯示詳細資料，記下網域名稱和帳戶 (在此範例中：網域為 OLYMPUS.CORP，標準帳戶為 unpriv-usr)。

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。

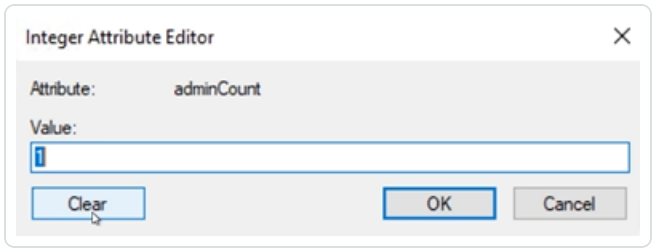
> **必要權限**：您必須擁有網域的管理員帳戶才能執行程序。



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。

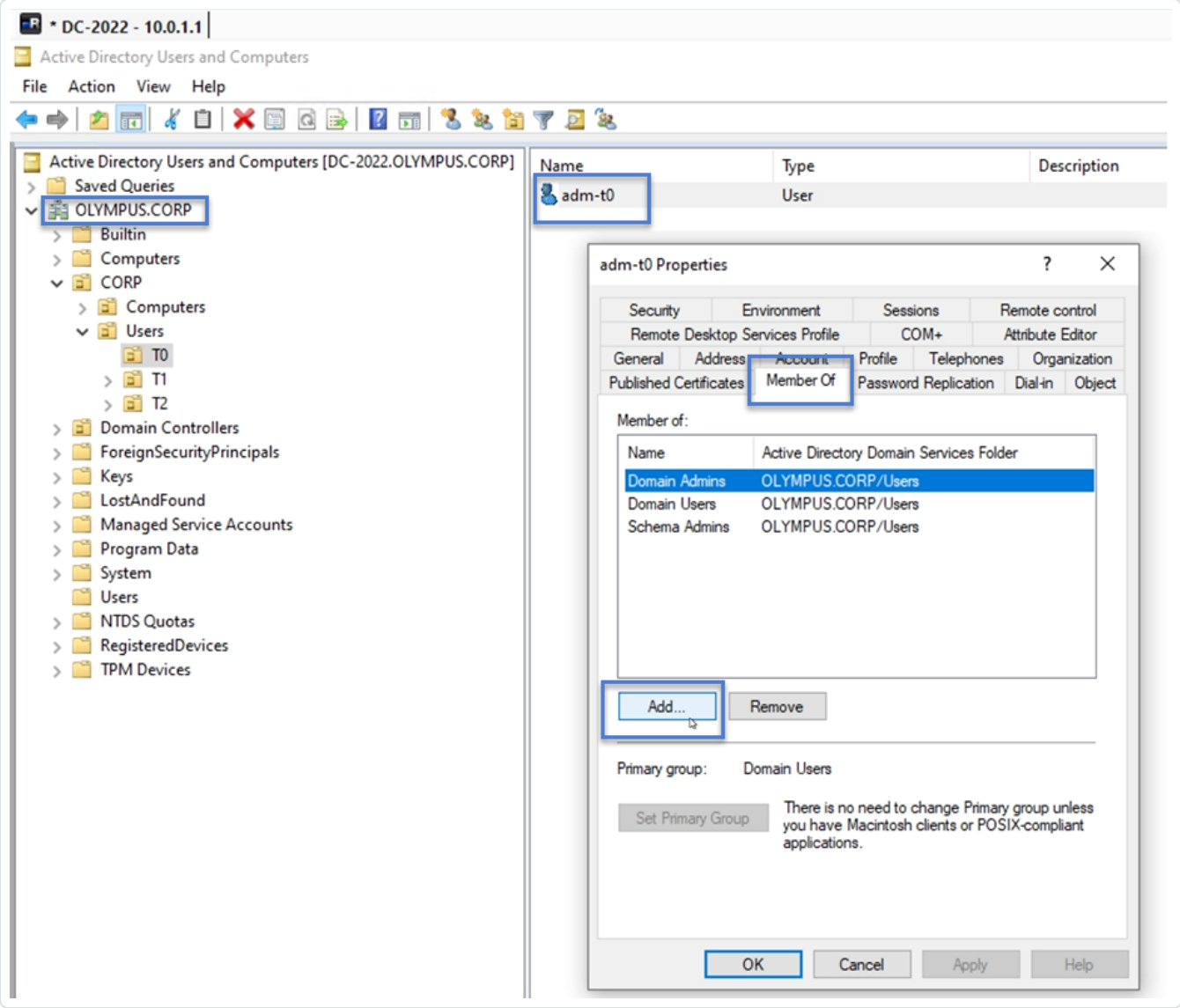
   「指標詳細資料」窗格會隨即開啟。

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。

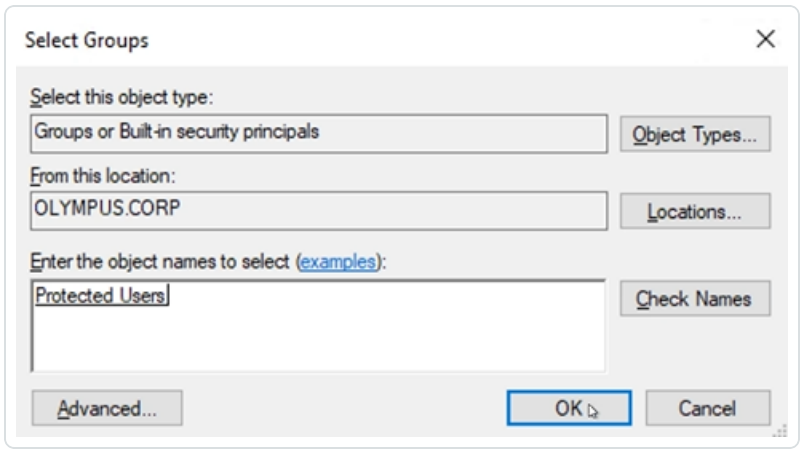
> **必要權限**：您必須擁有網域的管理員帳戶才能執行程序。

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**」。



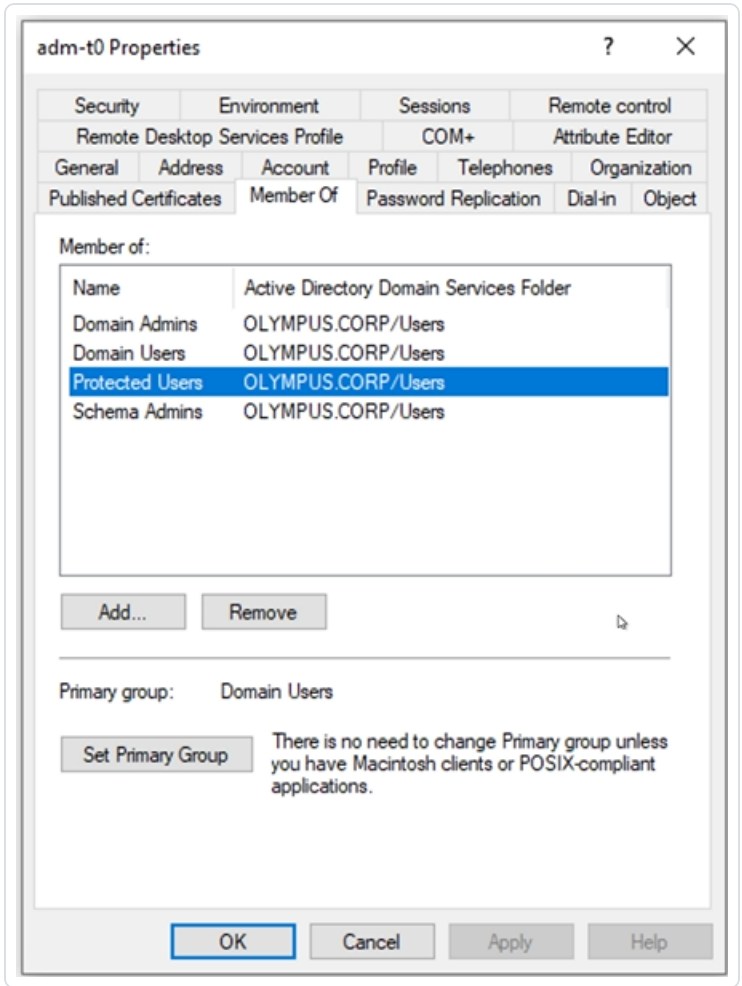
「**選取群組**」對話方塊會隨即顯示。

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。

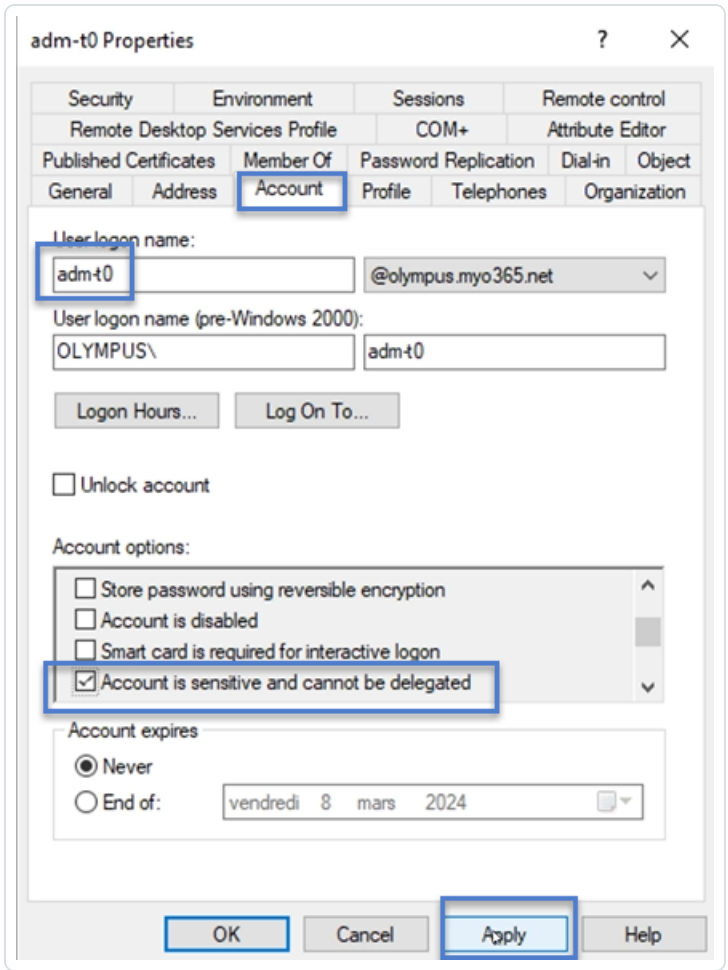
    清單中不會再出現異常物件。

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。

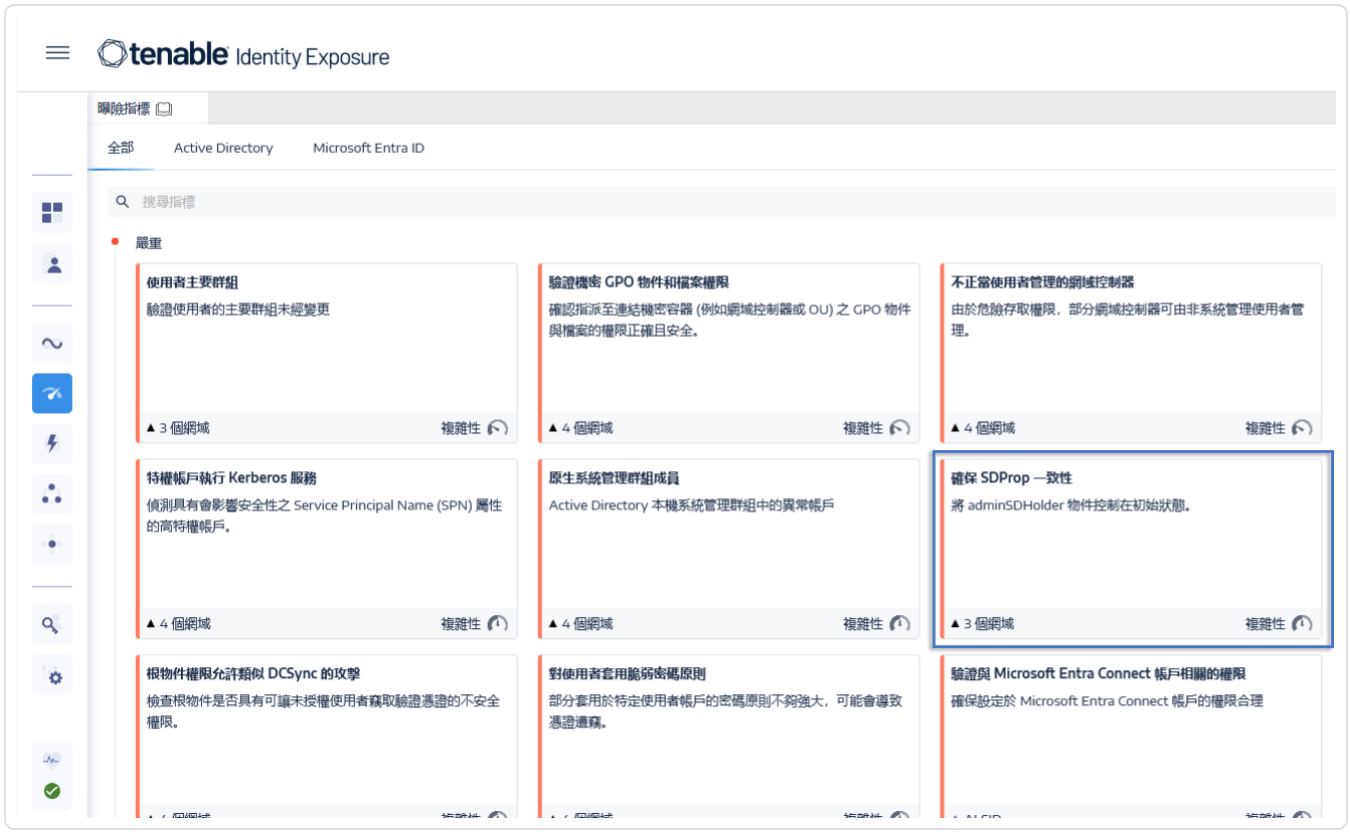
此嚴重曝險指標 (IoE) 會檢查 `adminSDHolder` 物件上設定的權限是否只允許對管理帳戶進行特權存取。

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。

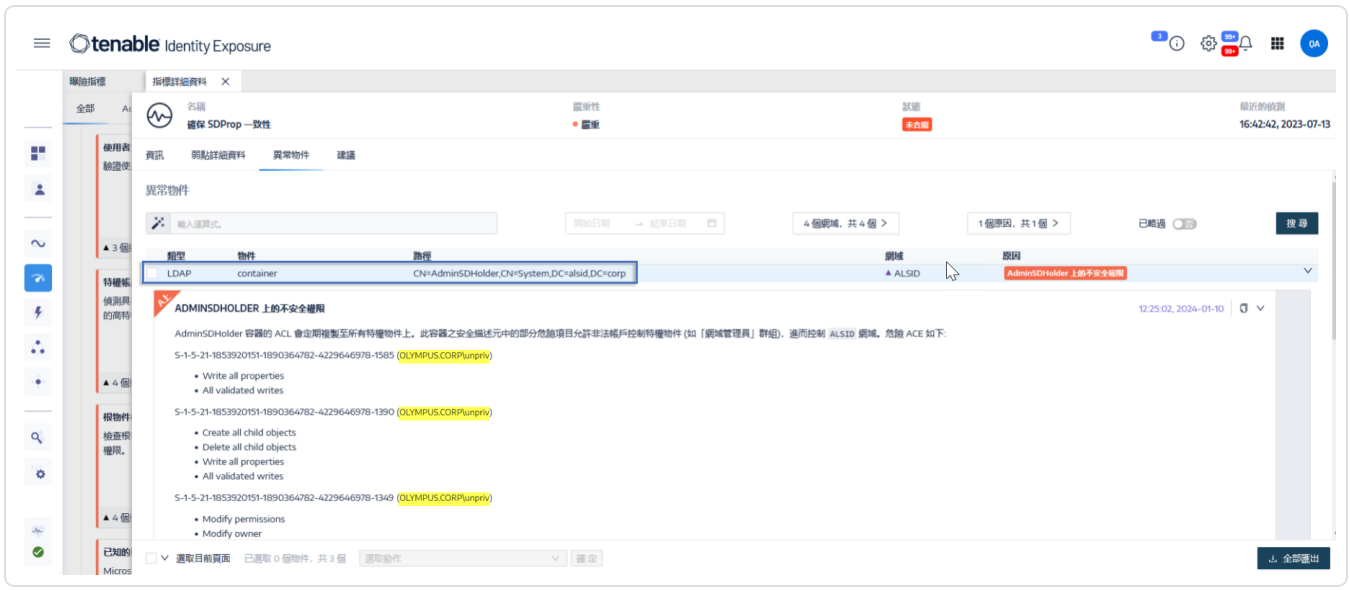
   根據預設，Tenable Identity Exposure 僅會顯示包含異常物件的曝險指標 (IoE)。

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。

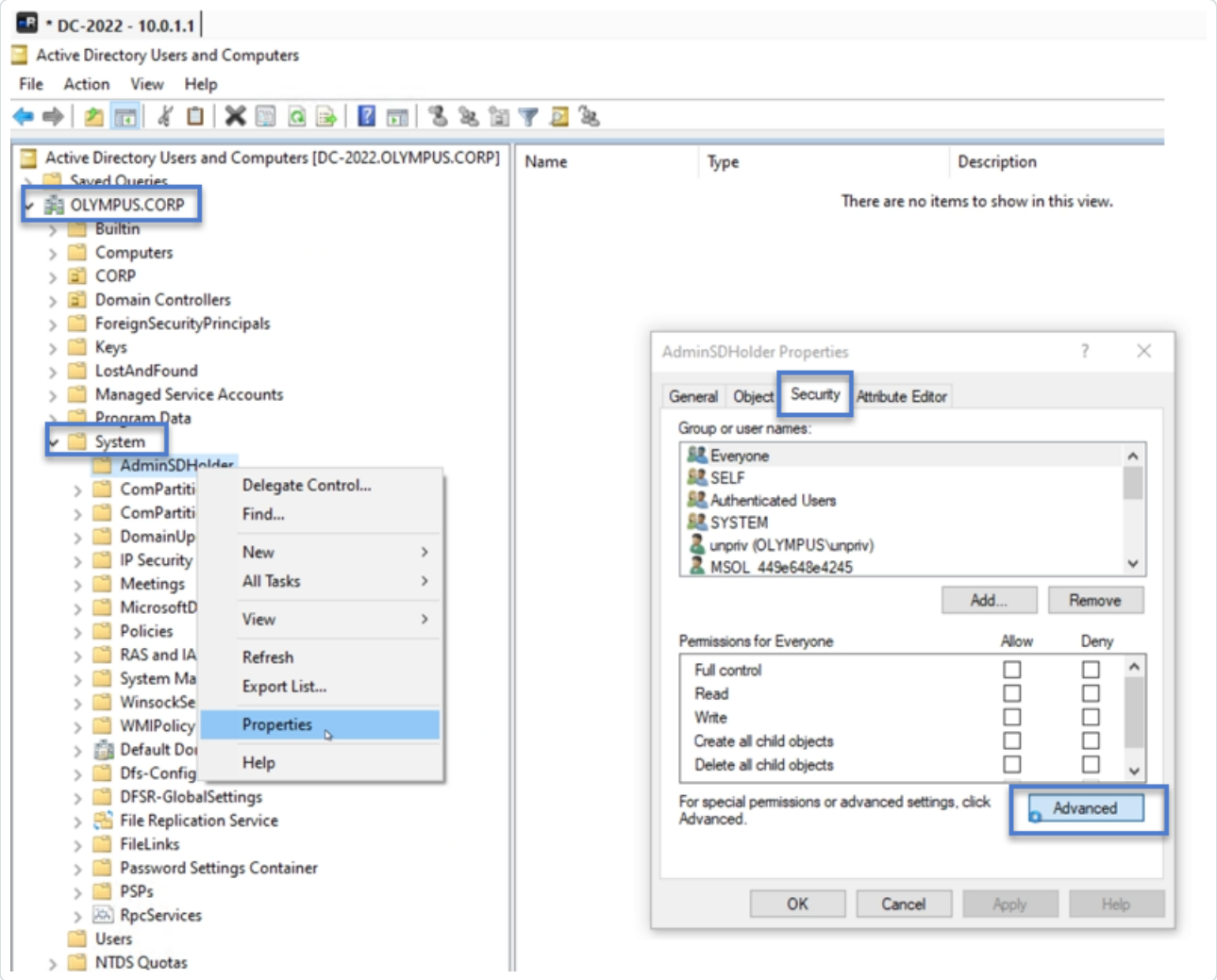
3. 將游標停留在異常物件上並按一下即可顯示詳細資料，記下 Tenable Identity Exposure 標記的網域名稱和相關權限 (在此範例中：`OLYMPUS.CORP .\unpriv`)。



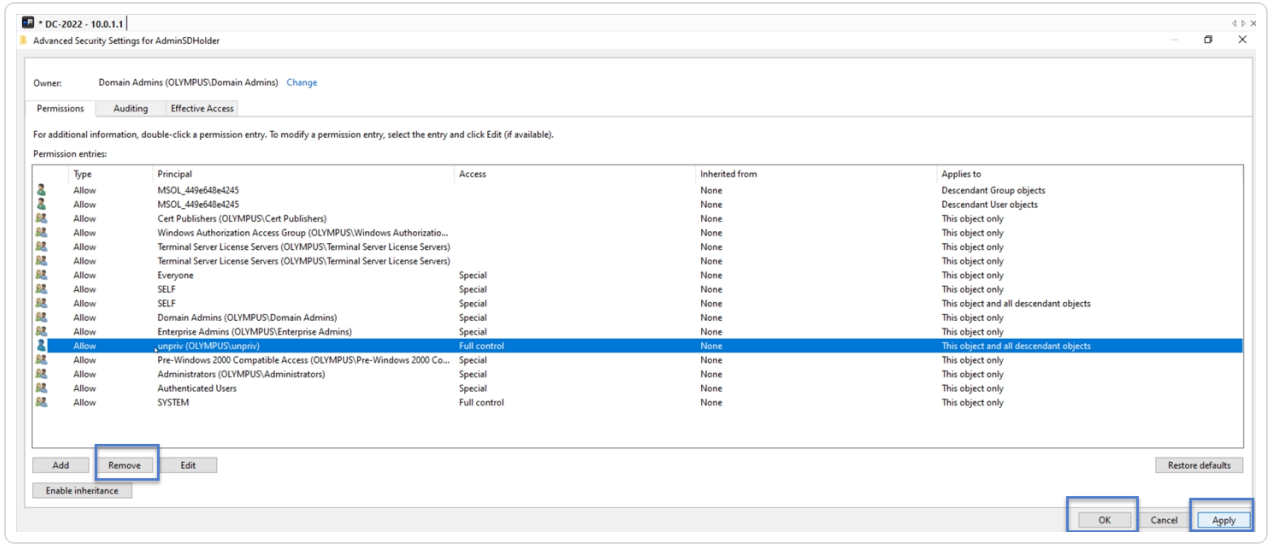
4. 在 Remote Desktop Manager (或類似工具) 中，找到網域名稱並導覽至「**系統**」> 「**AdminSDHolder**」。

> **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佈情況。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。

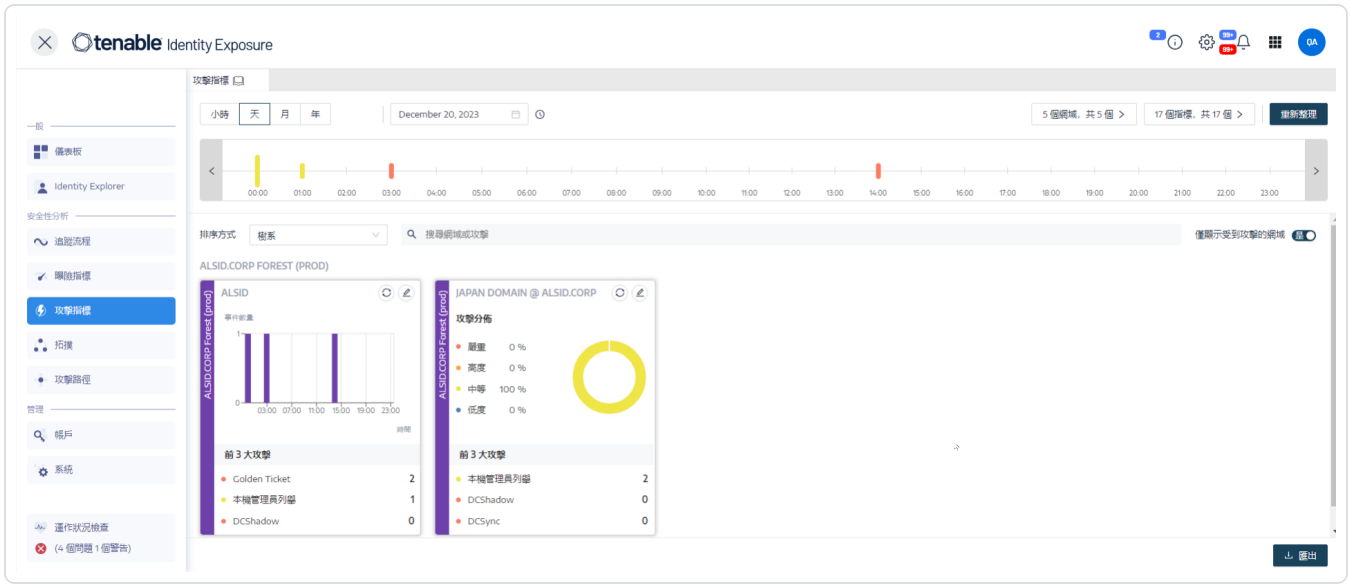
如需有關特定攻擊指標 (IoA) 的詳細資訊,請參閱 Indicators of Attack and the Active Directory。

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) 可導致危險的權限提升，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。

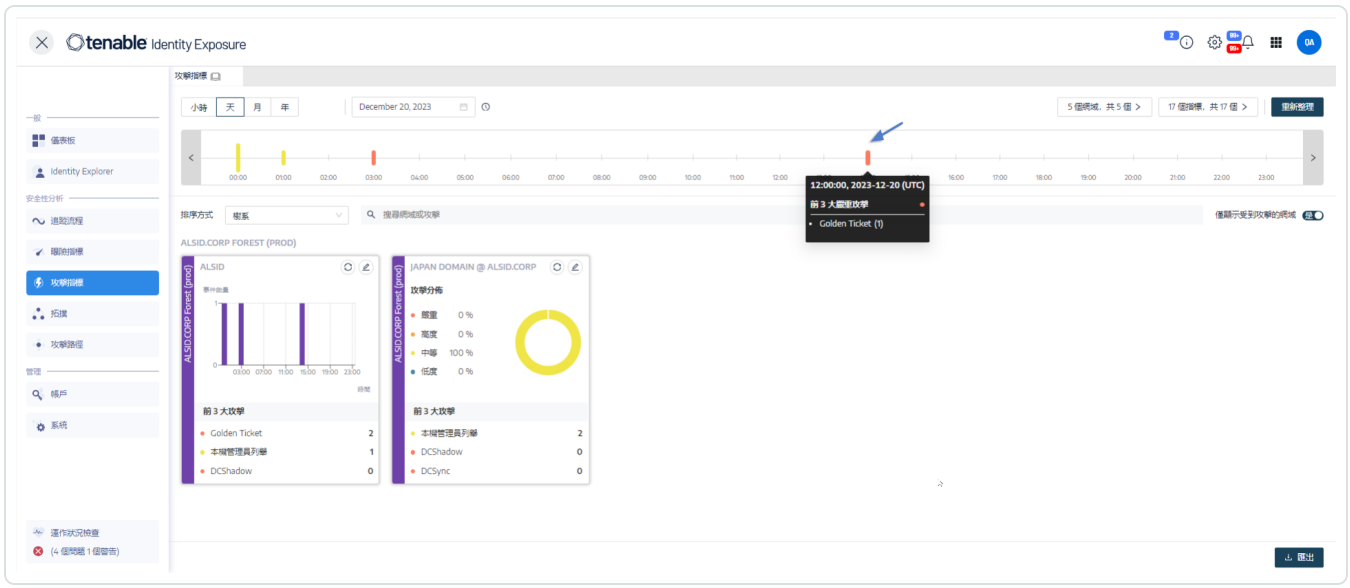
如要檢視攻擊指標：

- 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。



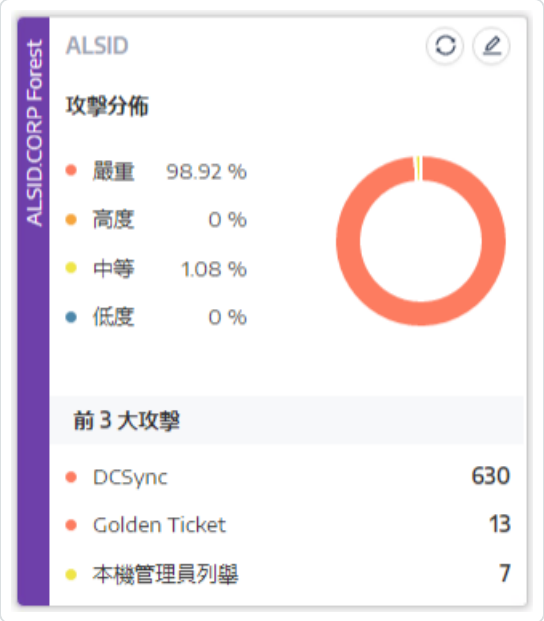
如要變更圖表類型：

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：

- **攻擊分佈**：顯示攻擊嚴重性的分佈狀況。



- **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。

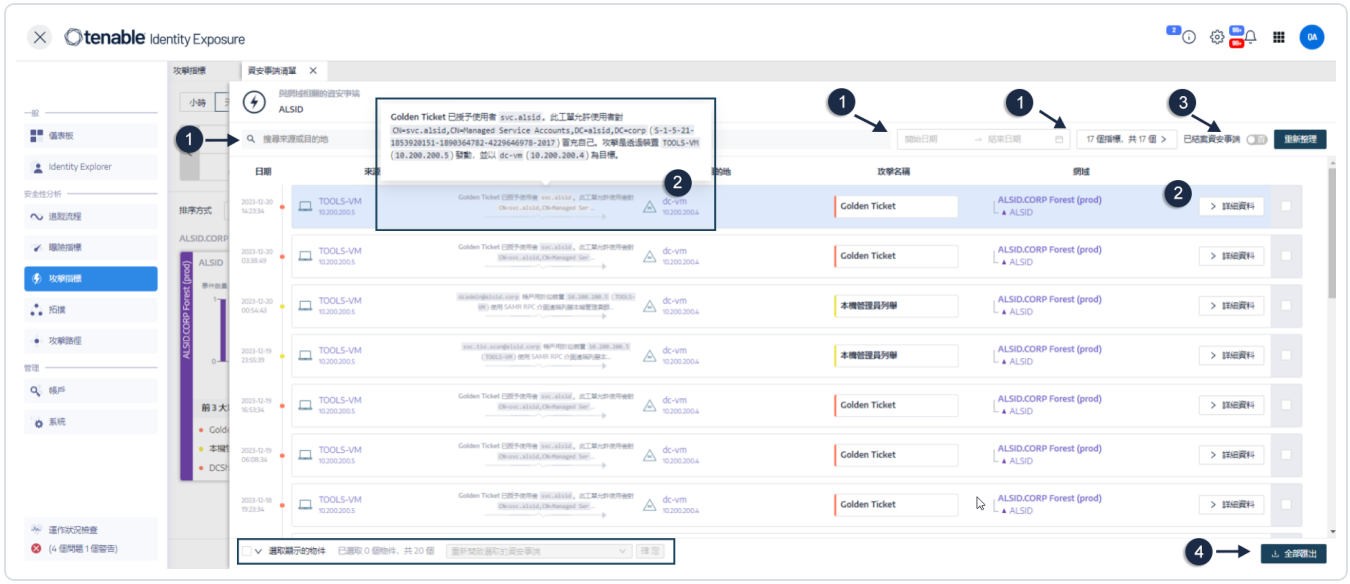
如要檢視攻擊資安事端：

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❶。
   - 存取與影響 AD 的攻擊相關的詳細說明❷。
   - 關閉或重新開啟資安事端❸。
   - 下載顯示所有資安事端的報告❹。

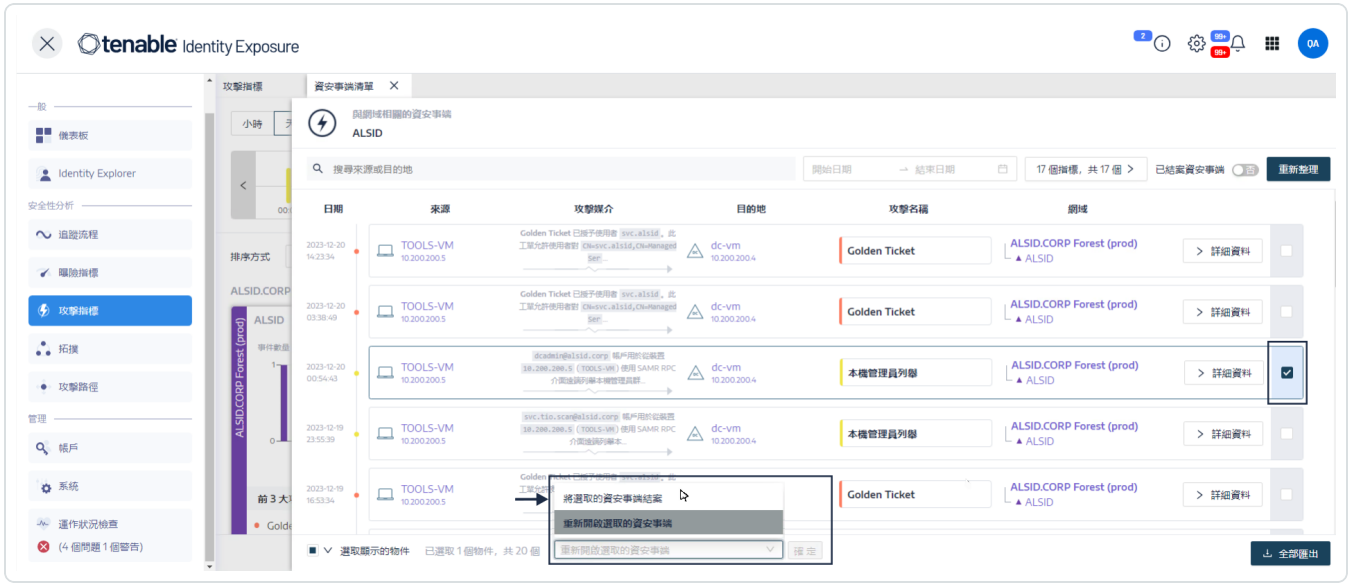
如要搜尋資安事端：

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**」。

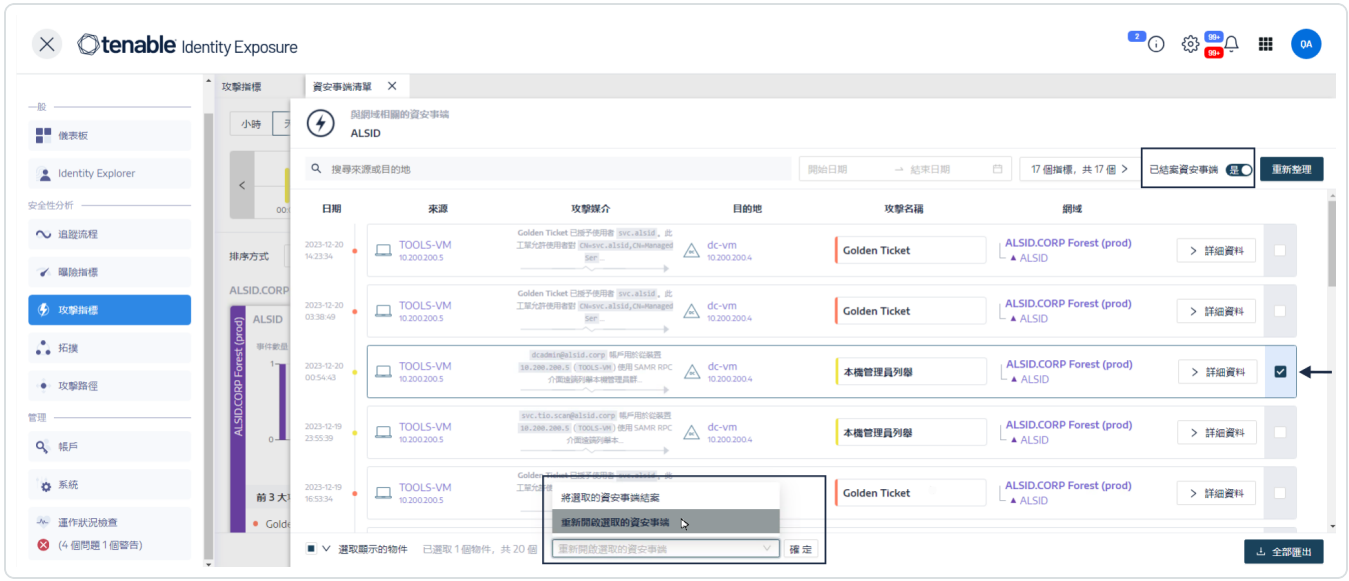
   系統會顯示一則訊息，確認 Tenable Identity Exposure 已關閉資安事端，並且不再顯示。

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**」。

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。

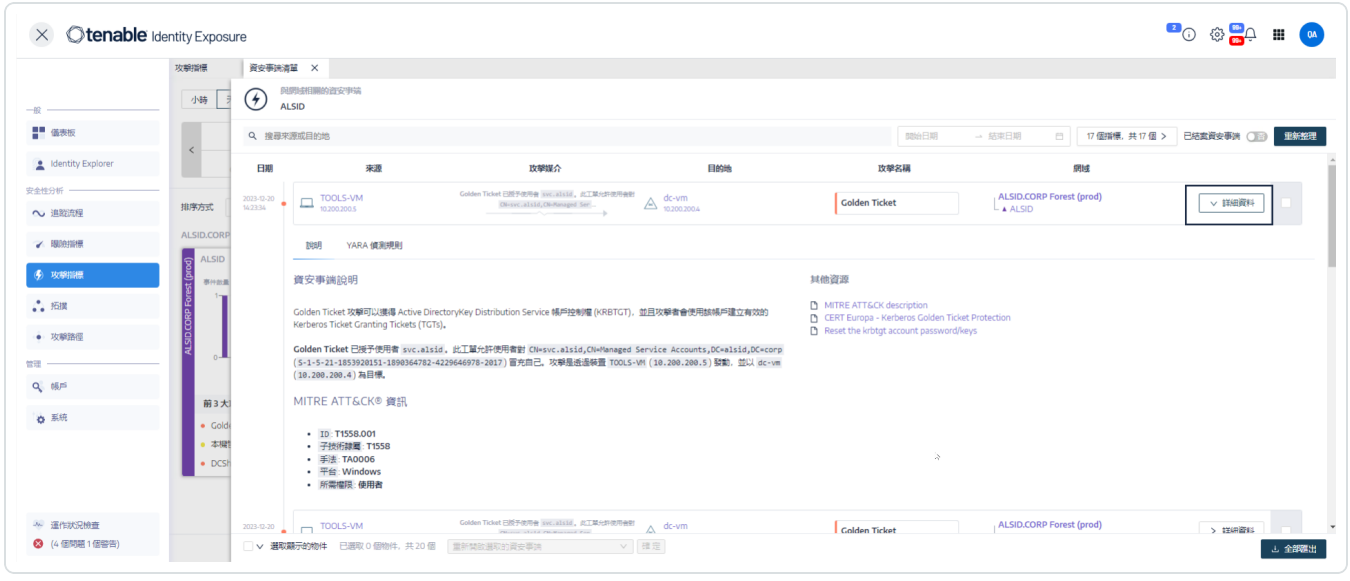
  提示：若按一下**資安事端清單**中的多個互動元素 (連結、動作按鈕等)，Tenable Identity Exposure 最多可以顯示五個窗格。如要同時關閉所有窗格，請按一下頁面上的任意位置。

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

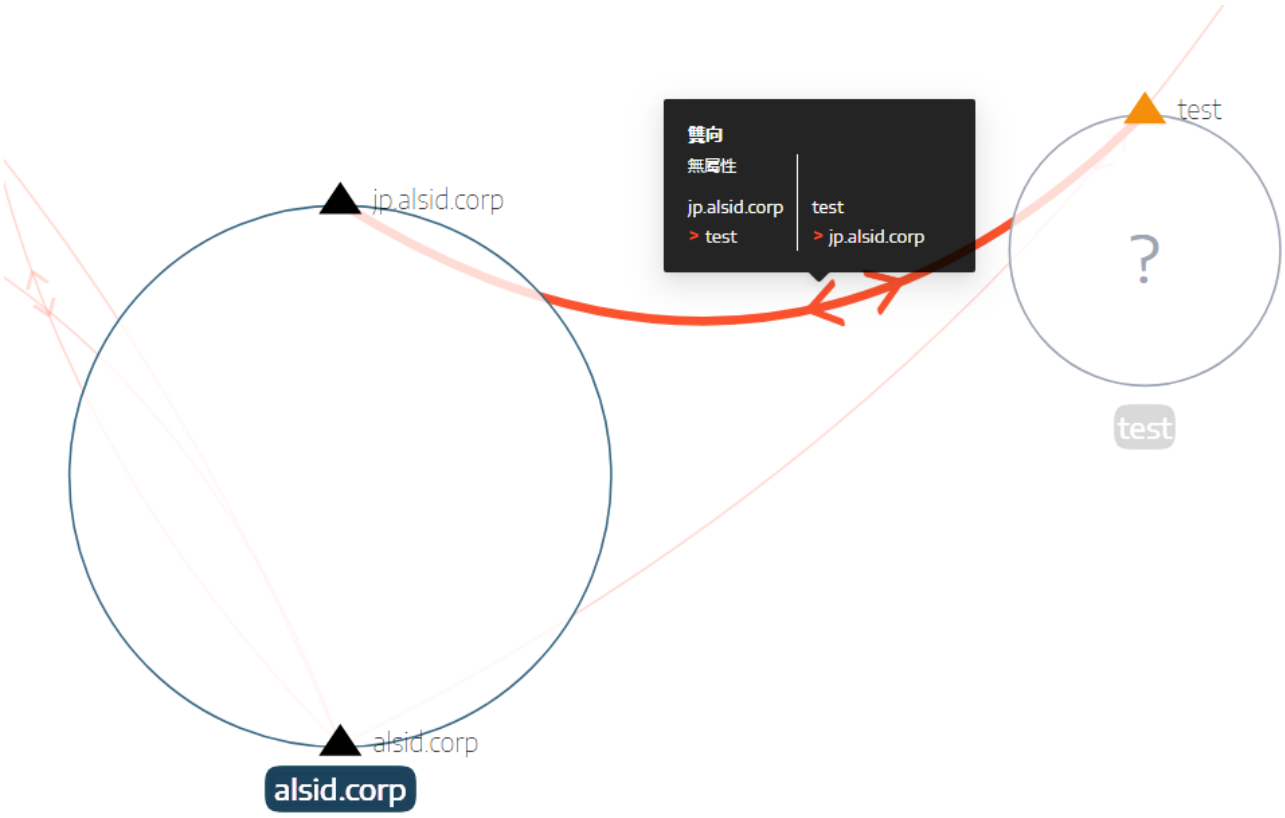
信任關係

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：

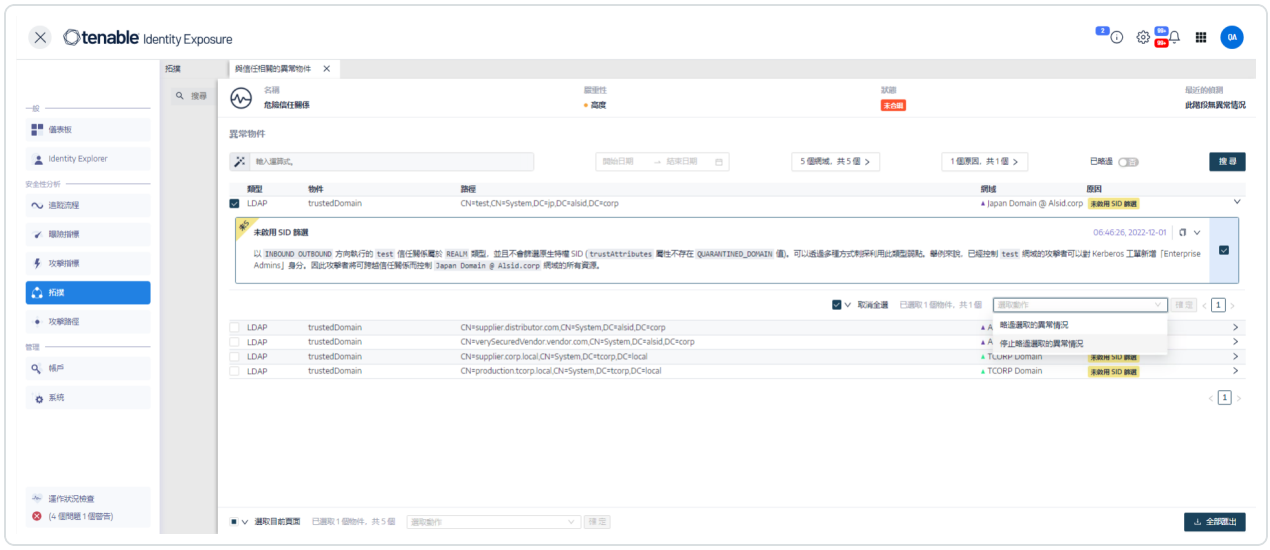
- **紅色**表示危險信任
- **橙色**表示普通信任
- **藍色**表示未知的信任

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。

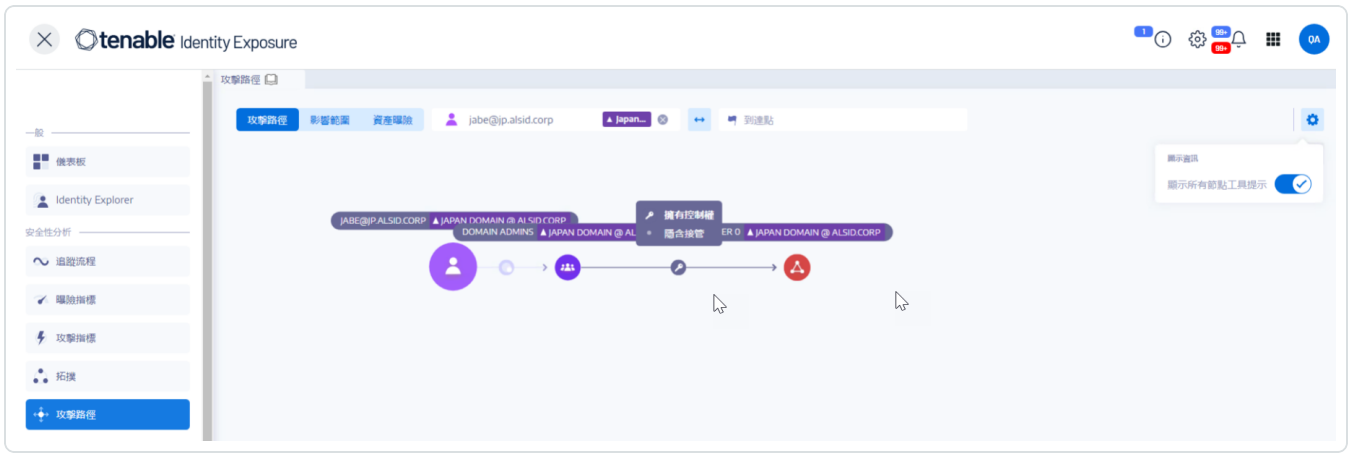
如要顯示攻擊路徑：

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。



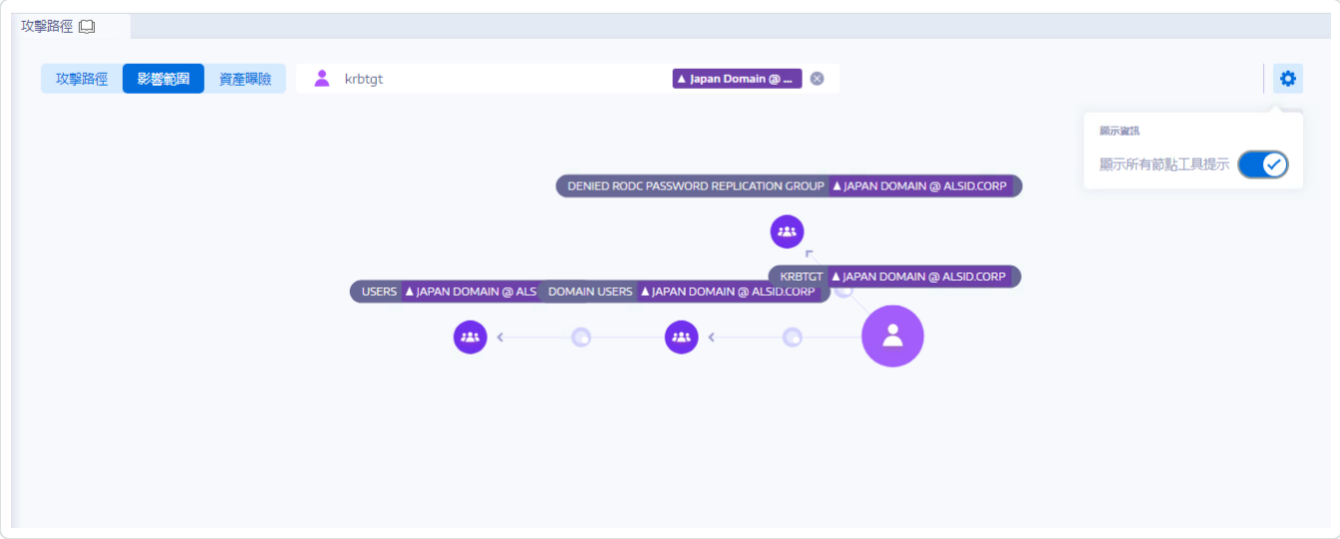
6. 或者，您可以按一下 圖示來執行以下動作：
    - 按一下**「縮放」**滑桿以調整圖形的放大倍數。
    - 按一下**「顯示所有節點工具提示」**開關以顯示有關資產的信息。

如要顯示影響範圍：

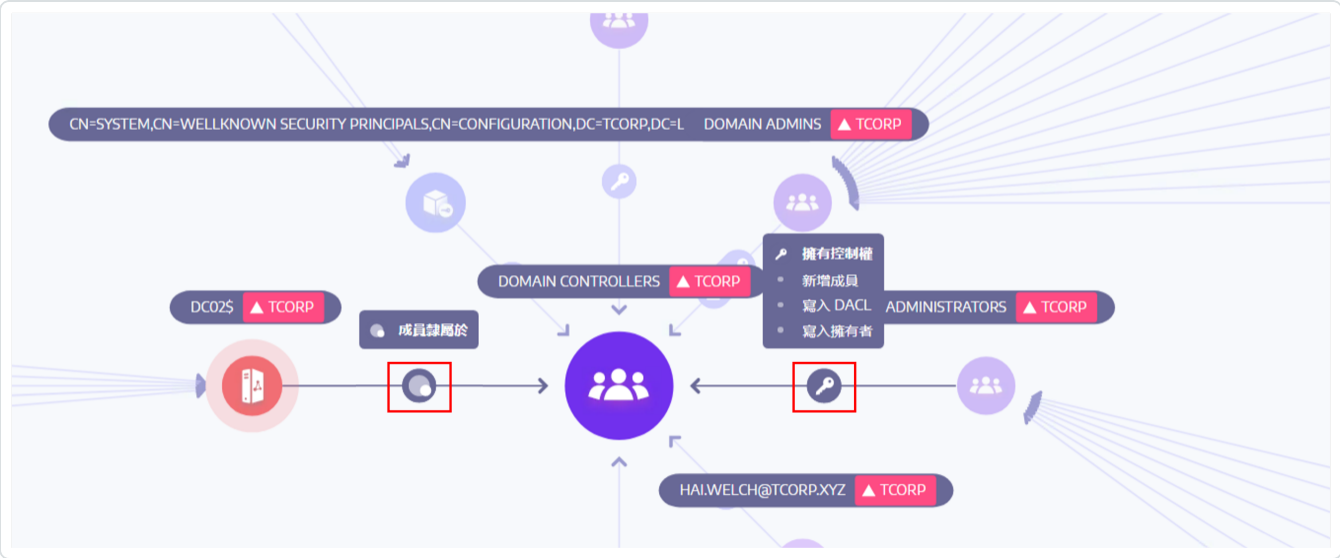
1. 在 Tenable Identity Exposure 中，按一下側邊欄功能表上的**「攻擊路徑」**。

    「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：

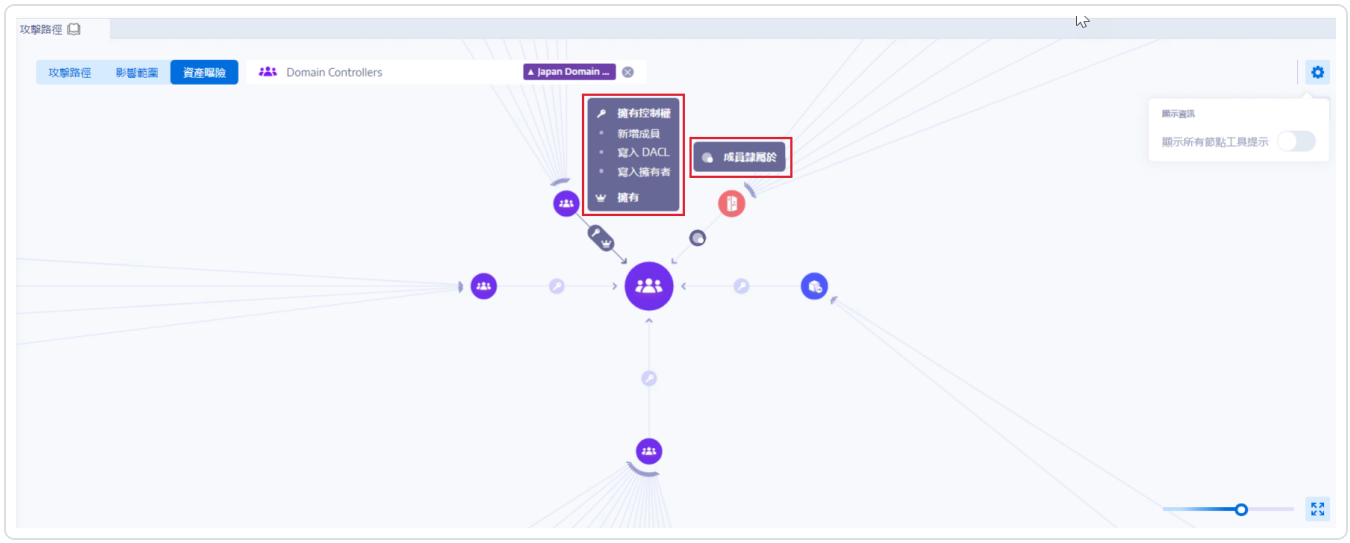
1. 如要顯示影響範圍：
2. 在 Tenable Identity Exposure 中，按一下側邊欄功能表上的「**攻擊路徑**」。

   「**攻擊路徑**」窗格會隨即顯示。
3. 在橫幅中，按一下「**資產曝險**」。
4. 在「**搜尋物件**」方塊中輸入資產的名稱。

5. 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。

6. 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：

1. 按一下要醒目提示的攻擊路徑上的節點。

   Tenable Identity Exposure 會在螢幕上釘選此攻擊路徑。

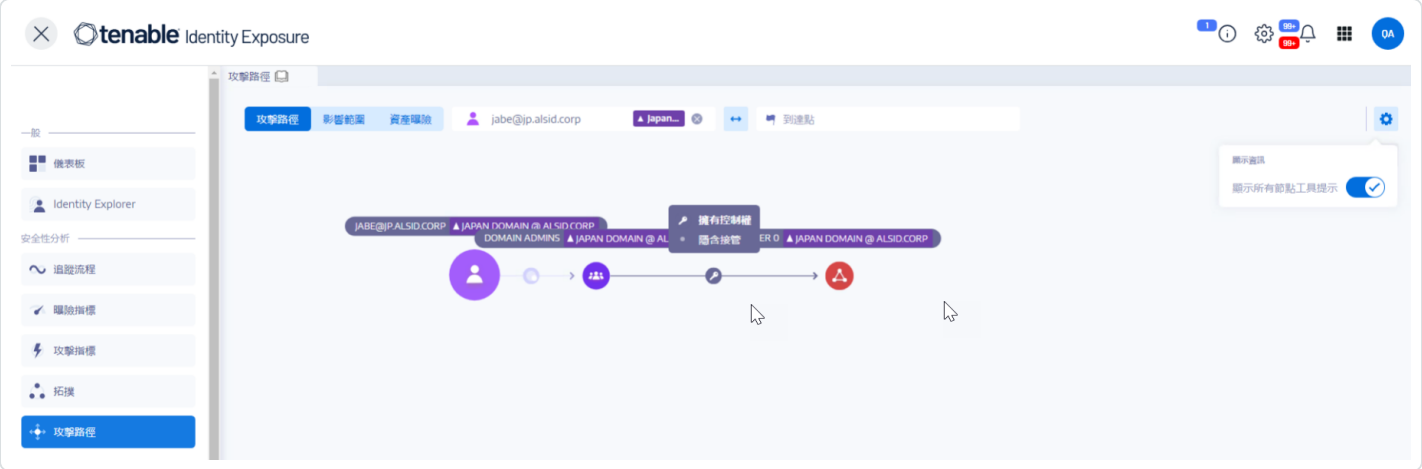
2. 如要取消釘選攻擊路徑，請按一下 圖示或不同攻擊路徑上的另一個節點。

另請參閱

- 攻擊關係

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有權限的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有權限的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較高權限 (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權限的一組 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)，則存在權限提升風險。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，因為這是權限提升的機會。

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，並且具有高權限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。

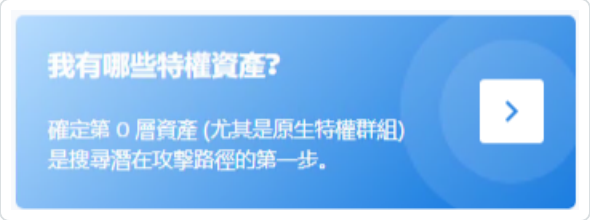
Tenable Identity Exposure 會列出您的第 0 層資產和帳戶，以及通往此資產的潛在攻擊路徑。

如要列出第 0 層資產：

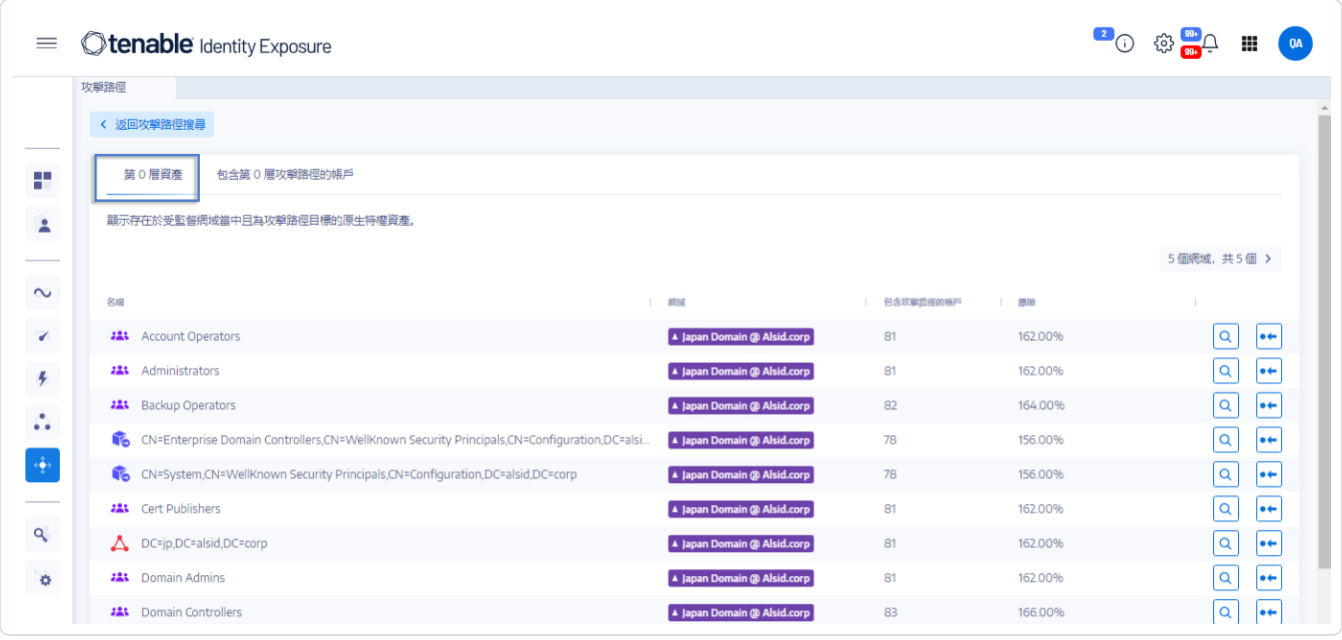
1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的攻擊路徑圖示 。

   「**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。

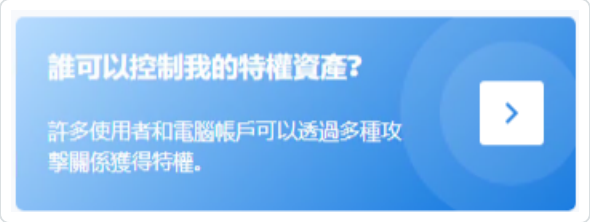
如需詳細資訊，請參閱識別第 0 層資產。

如要顯示包含攻擊路徑的資產：

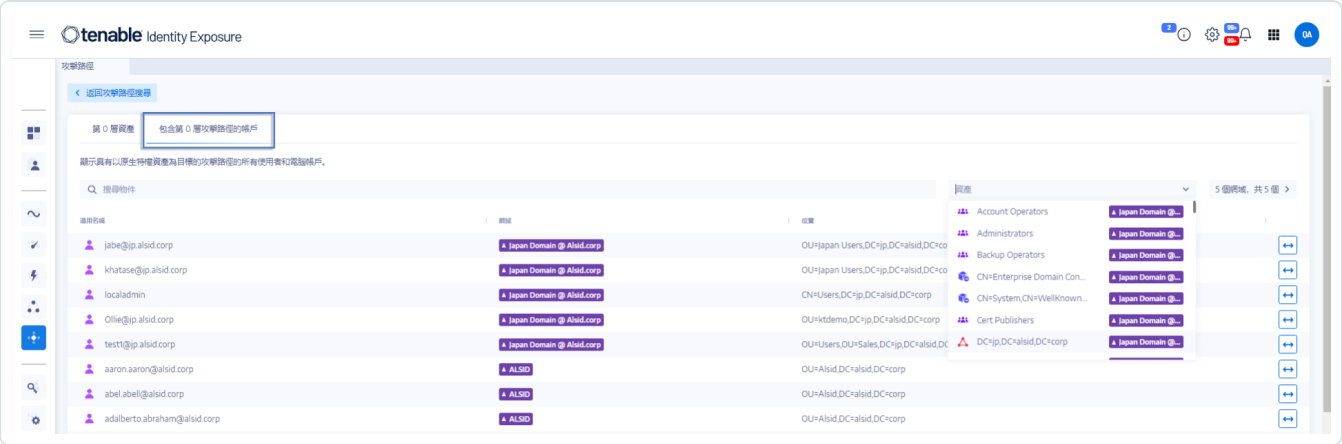
1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的攻擊路徑圖示 。

   「**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。

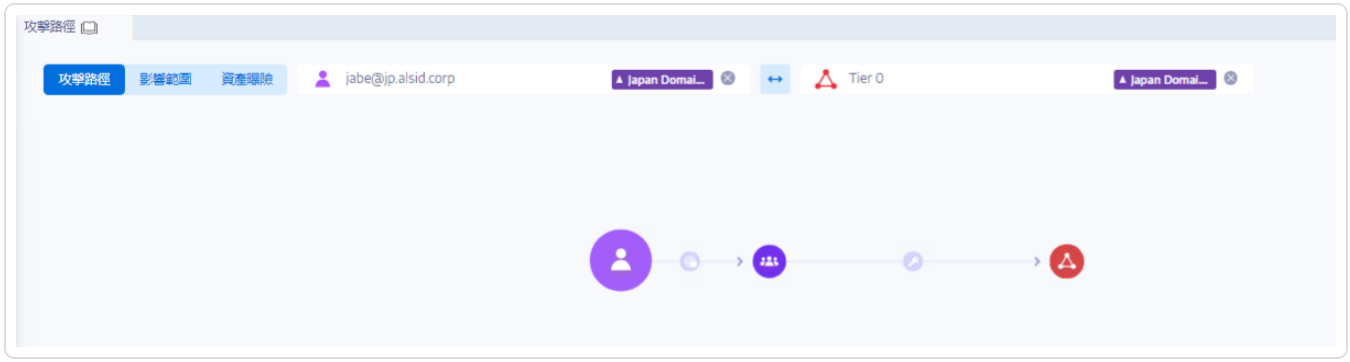
2. 按一下「**篩選選取的項目**」。

   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 `class` 群組的 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。 `primaryGroupID` 屬性不等於 516 (DC) 或 521 (RODC)。 **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 儲存區	LDAP		`objectClass` 屬性包含 `certificationAuthority` 類別的 LDAP 物件。
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)。 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)。

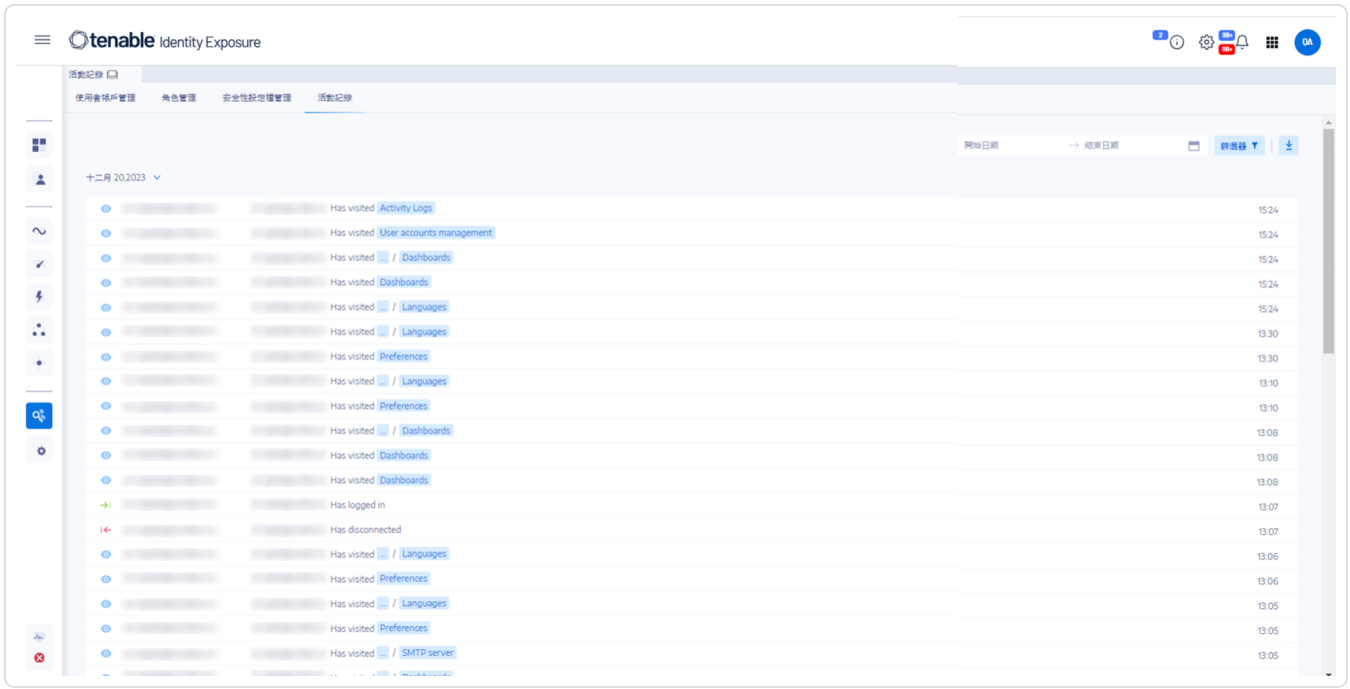
如要檢視活動記錄：

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。

Tenable Identity Exposure 管理員指南

上次更新時間：年月日

本管理員指南提供 Tenable Identity Exposure（前稱 Tenable.ad）的管理工作相關資訊。

Tenable 建議進行以下幾件事項，以便在 Tenable Identity Exposure 中開始擔任管理員：

- 準備和安裝
- 設定設定檔和使用者
- 偵測和監控

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)

準備和安裝

如要準備並完成 Tenable Identity Exposure 安裝：

- 依照《*Tenable Identity Exposure 安裝指南*》中的說明安裝 Tenable Identity Exposure。
- 連線並登入 Tenable Identity Exposure。

設定設定檔和使用者

接下來，我們建議您透過下列互動來設定和瀏覽 Tenable Identity Exposure 介面：

- 設定設定檔喜好設定：設定預設語言、變更密碼，以及設定設定檔的其他喜好設定
- 建立使用者並將其新增至您的 Tenable Identity Exposure 執行個體。
- 設定角色型存取控制 (RBAC)，以保護組織內的資料與功能存取安全。

偵測和監控

根據您的業務需求設定並調整 Tenable Identity Exposure 之後，您就可以開始使用您的資料：

- 部署攻擊指標模組。
- 使用 Tenable Identity Exposure 入口網站來管理和接收受監控基礎架構安全狀態的相關資訊。
- 選取 Tenable Identity Exposure 要在特定網域上監控的攻擊類型，以定義攻擊情境。

注意：Tenable Identity Exposure 可以單獨購買，也可做為 Tenable One 套件的一部分購買。如需詳細資訊，請參閱 Tenable One。

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。

如需詳細資訊，請參閱下列內容：

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。

如要授予對 AD 物件或容器的存取權:

- 在網域控制器的命令列介面中,執行下列命令以授予對 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此命令。

  ```
  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：

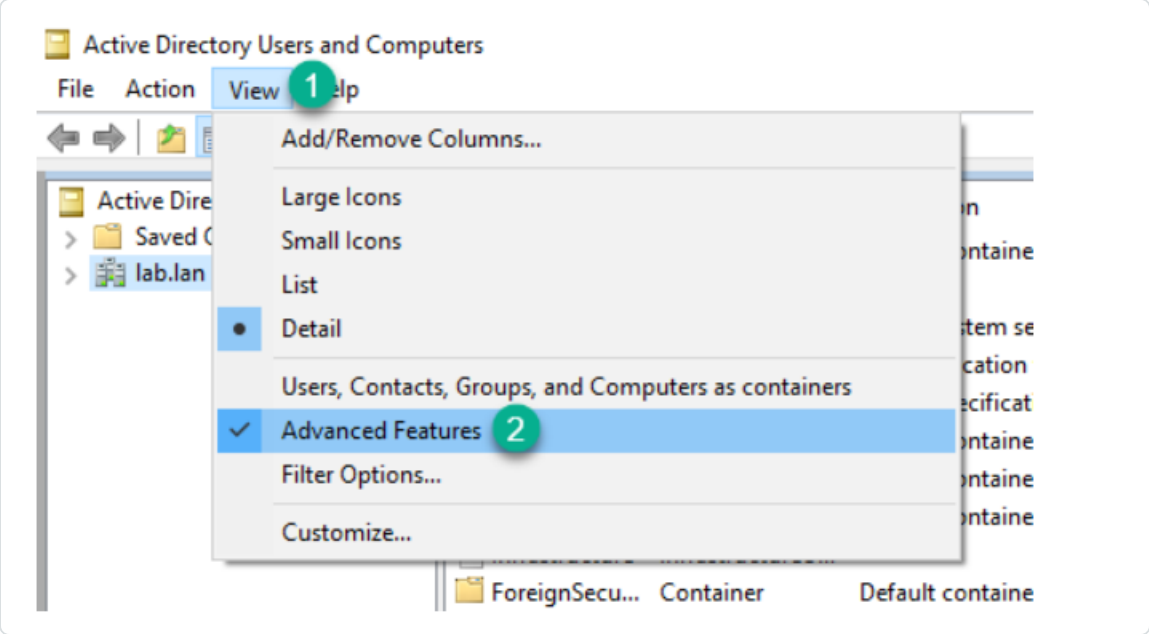
```
dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
```

  其中：

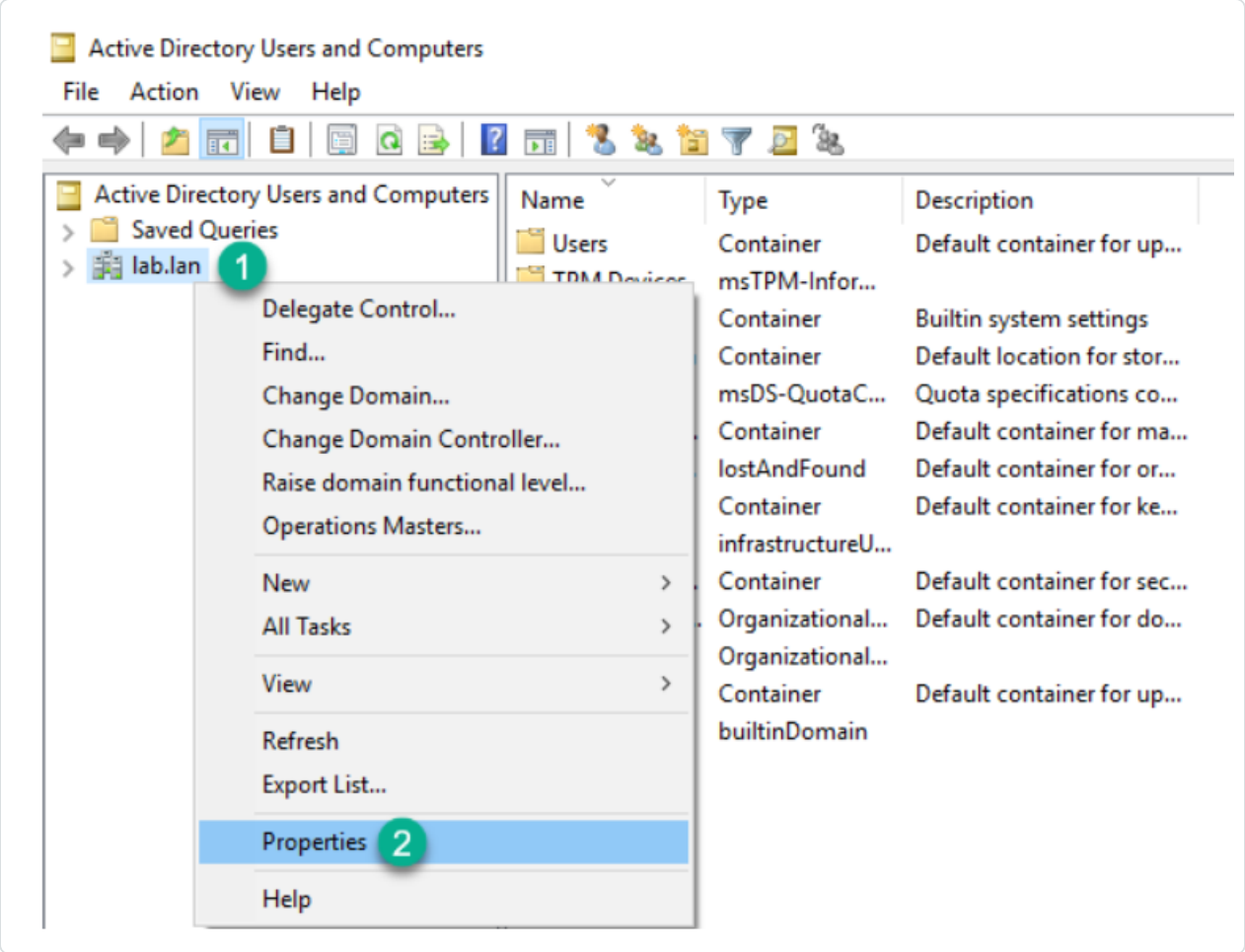
  - <__DOMAIN_ROOT__> 指的是網域 root 的辨別名稱。範例：“DC=<DOMAIN>,DC=<TLD>”
  - <__SERVICE_ACCOUNT__> 指的是 Tenable Identity Exposure 使用的服務帳戶。範例：“DOMAIN\tenablead”。

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**」。

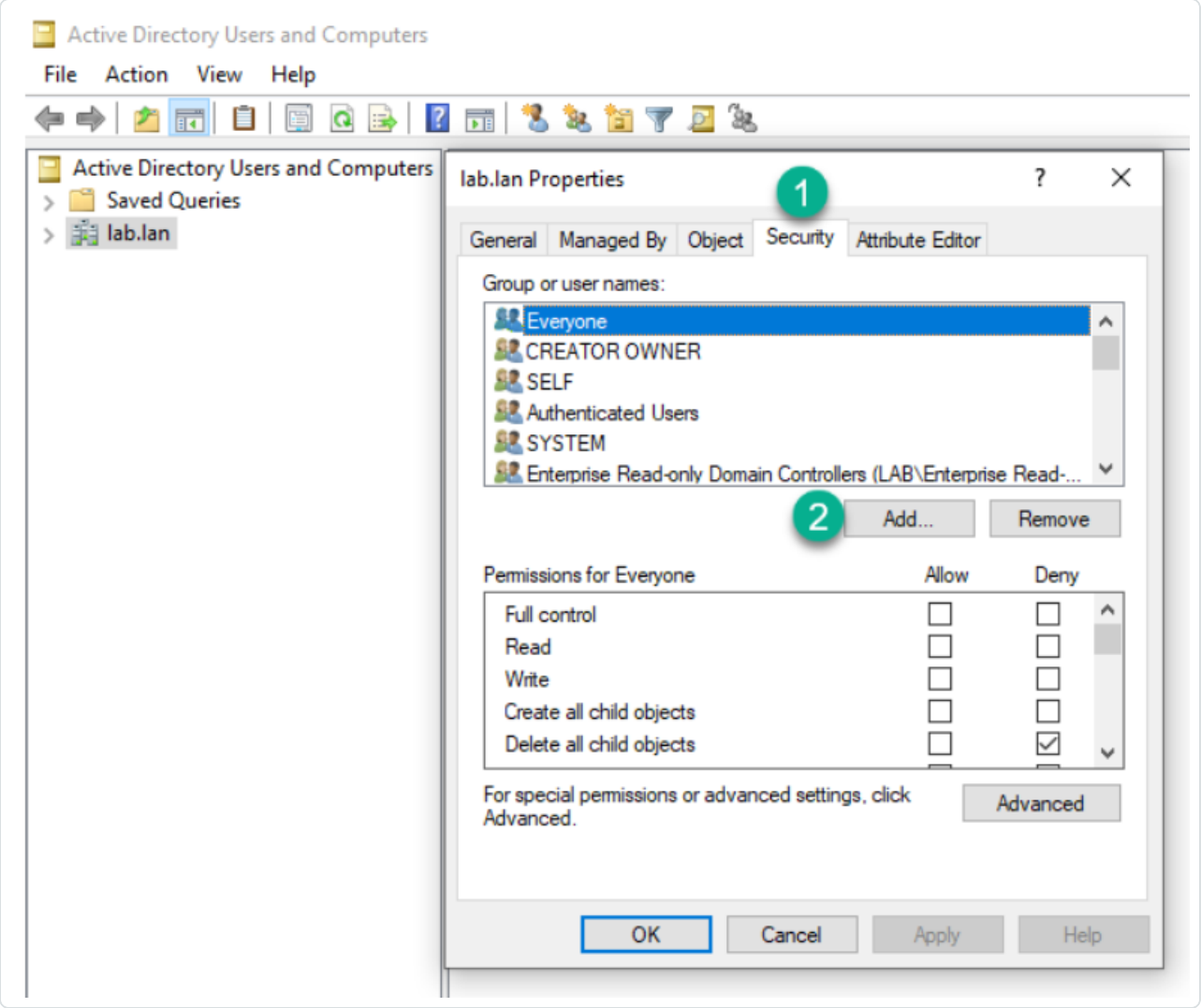


3. 右鍵按一下網域 root 並選取「**屬性**」。



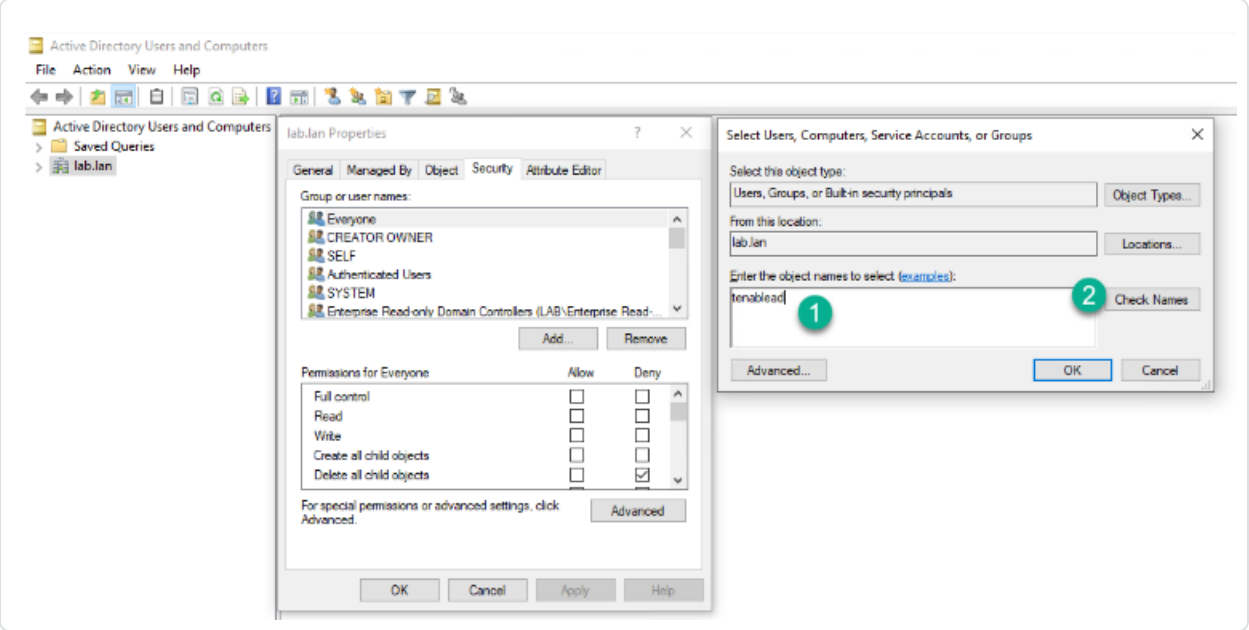
網域 root 的屬性窗格會隨即開啟。

4. 按一下「**安全性**」索引標籤，然後按一下「**新增**」。



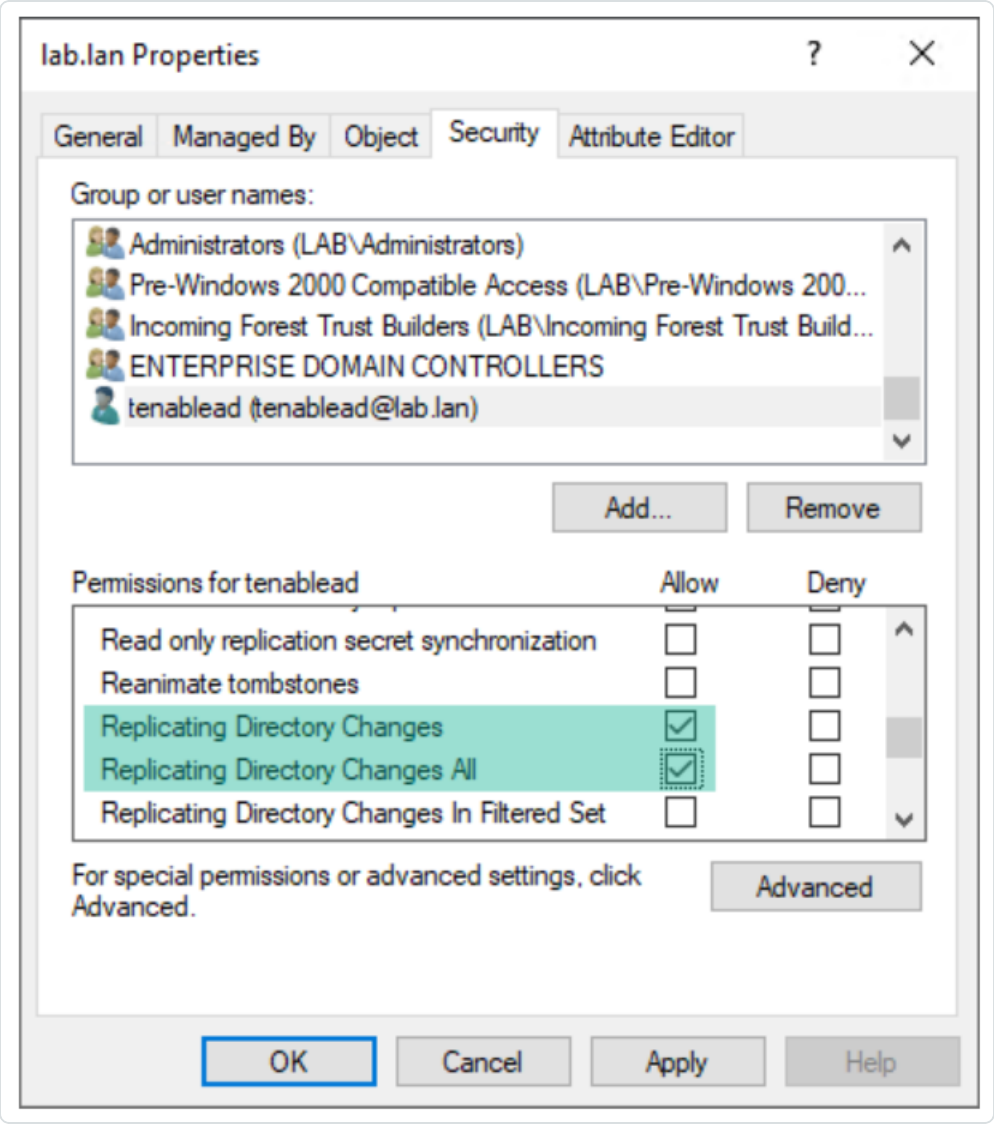
5. 尋找 Tenable Identity Exposure 服務帳戶：

> **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**。

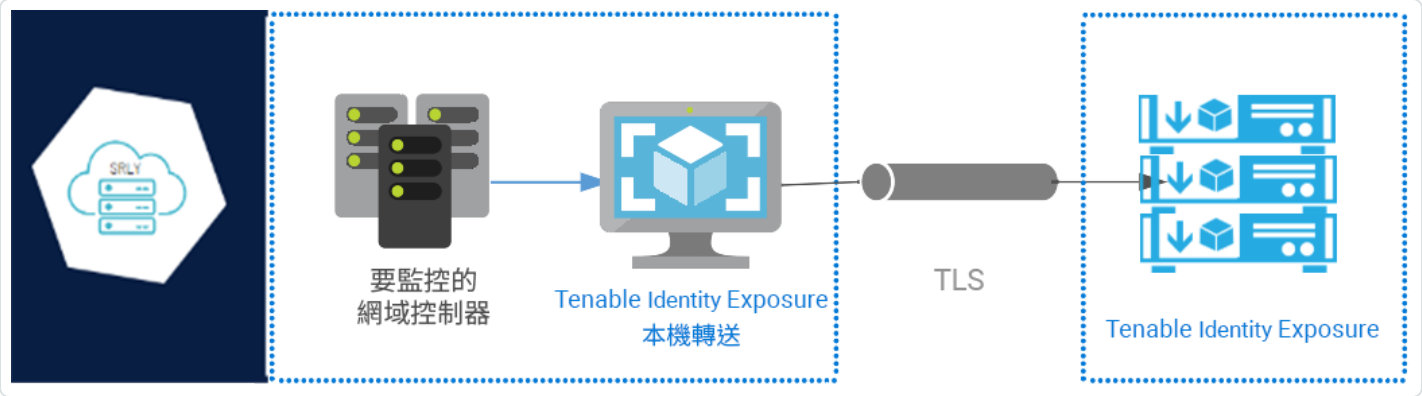
您必須**在網域 root 層級**指派額外的權限。Active Directory 不支援指派給組織單位或特定使用者的權限 (例如將「特權分析」限制為 OU 或使用者)，因此這不會產生任何影響。

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。

安全轉送

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。

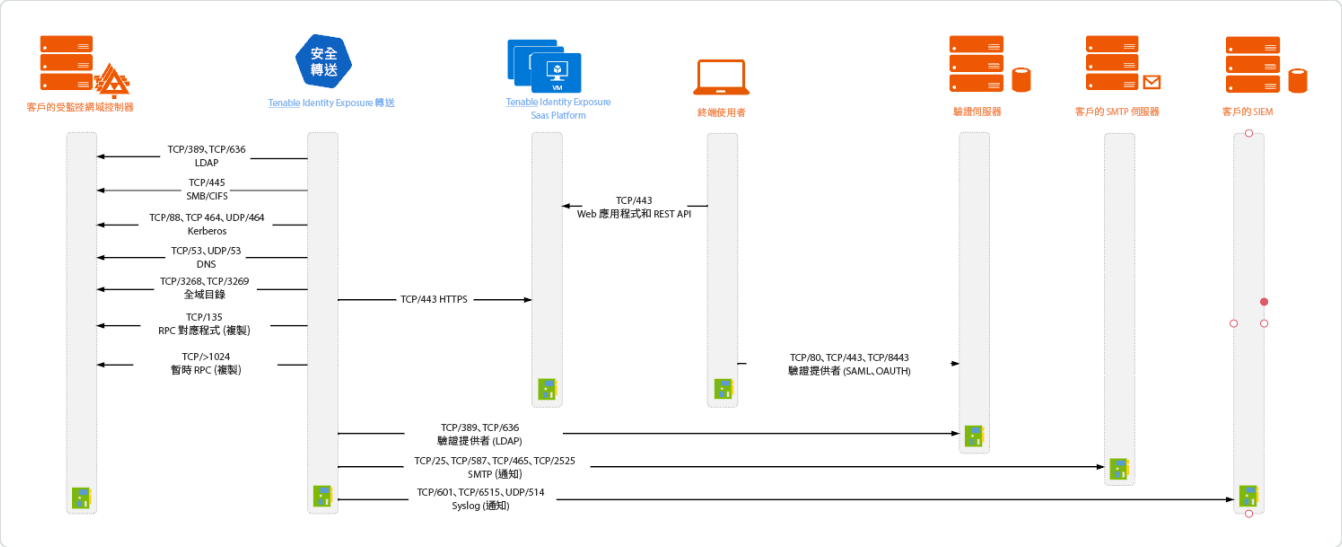


注意：安全轉送功能目前僅在 Tenable Identity Exposure 將您的平台佈建為使用安全轉送時才適用。無法手動將佈建從 VPN 切換為安全轉送。如需我們協助您將平台從 VPN 移轉到安全轉送，請聯絡 Tenable Identity Exposure 客戶支援代表。

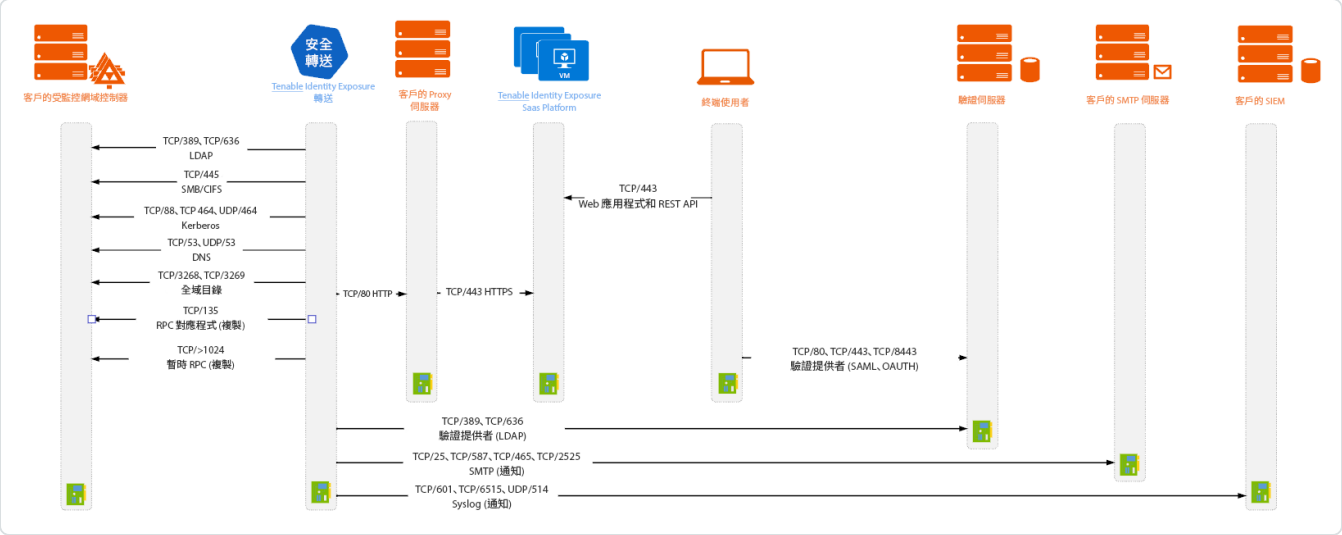
網路流量

安全轉送的必要連接埠

- 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：



TLS 需求

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
   ```

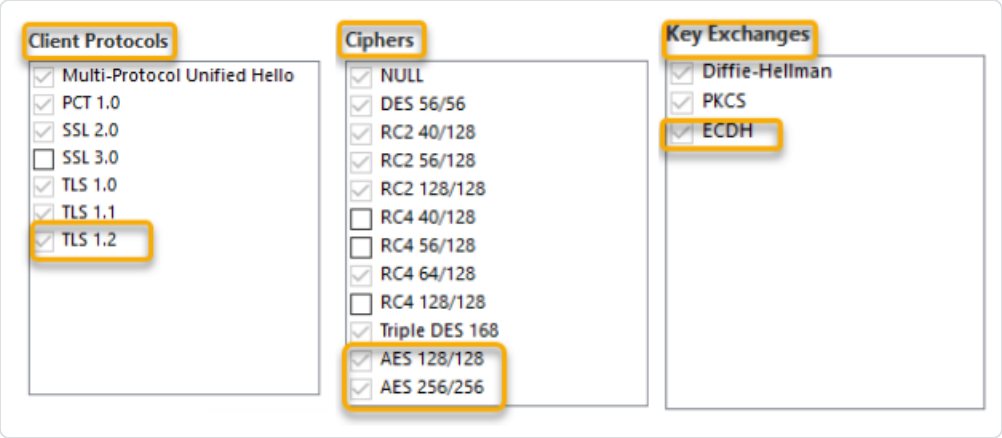
5. 檢查您是否有曲線 **25519**。若無，請啟用。

```
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。

事前準備

先決條件

虛擬機器

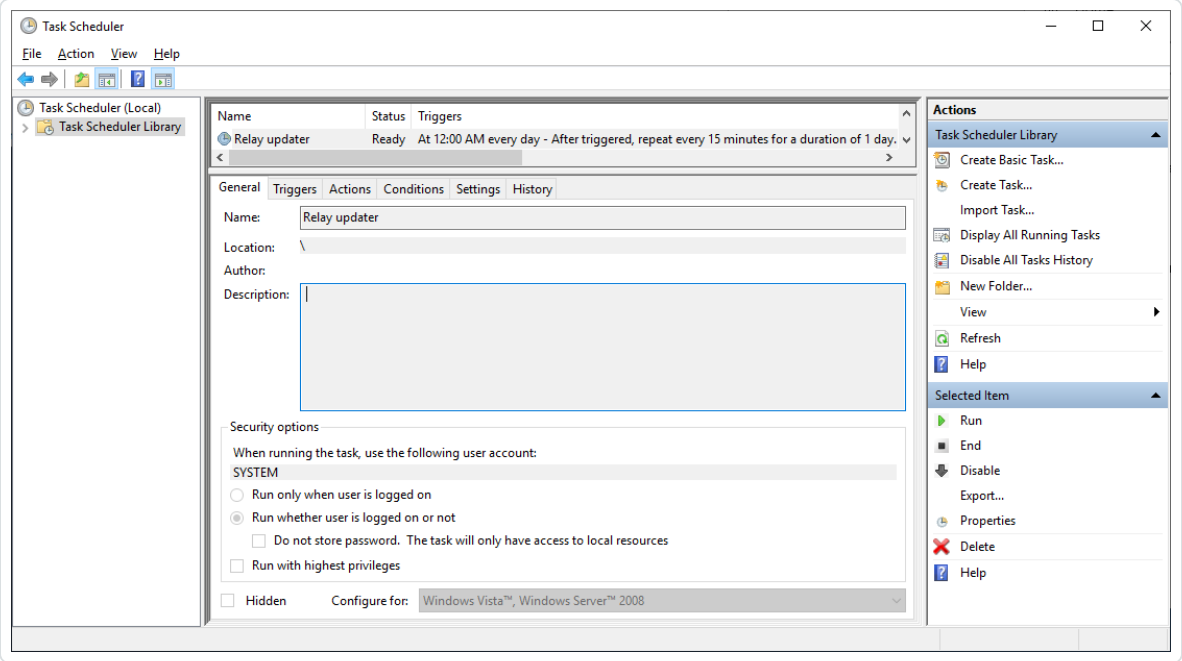
代管安全轉送的虛擬機器 (VM) 需要符合以下要求：

客戶規模	Tenable Identity Exposure 服務	需要執行個體	記憶體 (每個執行個體)	vCPU (每個執行個體)	磁碟拓撲	可用磁碟空間 (每個執行個體)
任何大小	• `tenable_Relay` • `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

VM 還必須具備：

- 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：



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

如需詳細資訊，請參閱設定角色的權限。

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）。

允許下列檔案和處理程序：

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

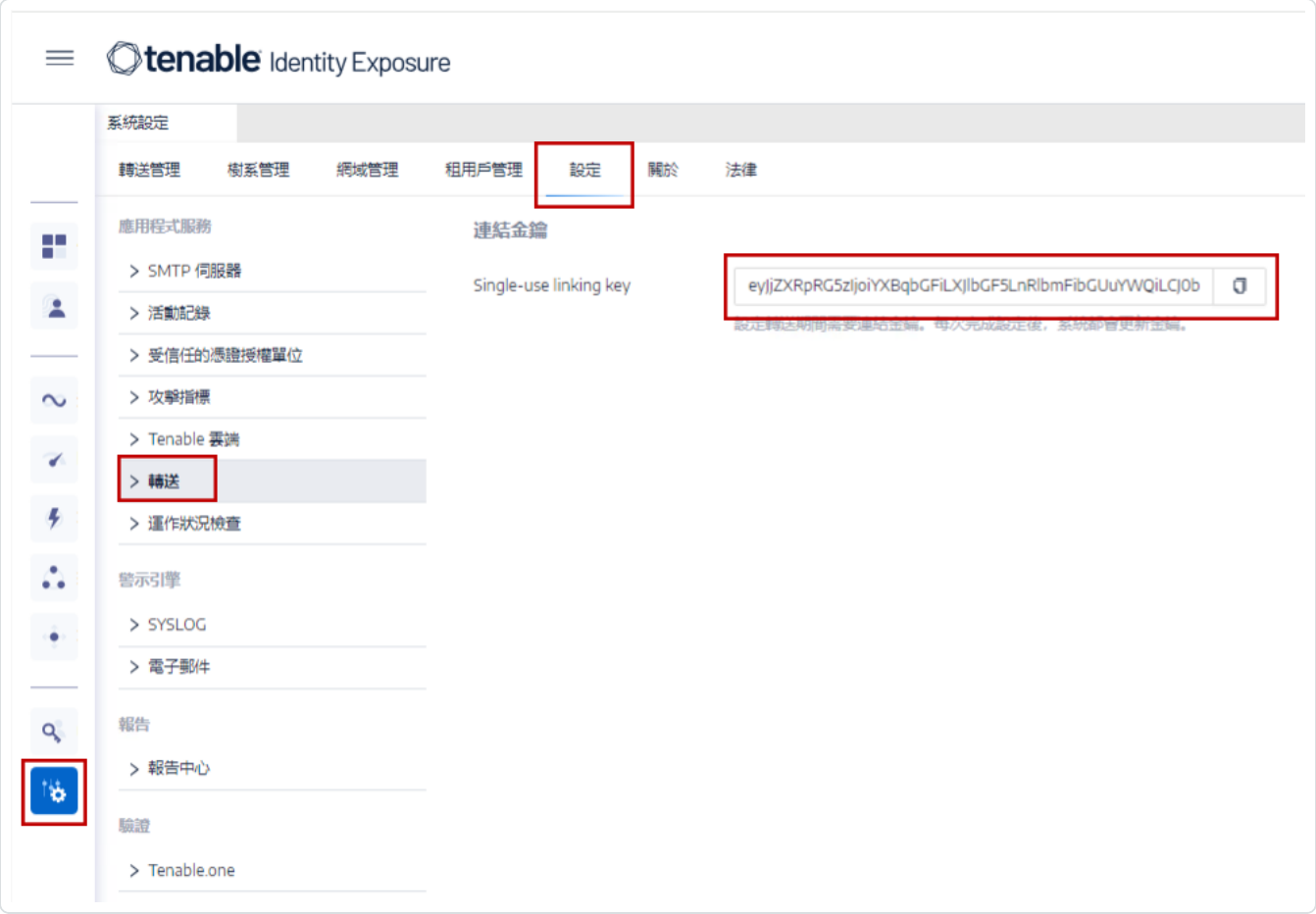
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad 安全轉送

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 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。

安裝

如要安裝安全轉送：

- 選擇安裝方法：
  - 安裝安全轉送 (GUI)
  - 安裝安全轉送 (Tenable Nessus Agent)

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。

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。

另請參閱

安全轉送的完整資訊請參閱 Tenable Identity Exposure 管理員指南中的「安全轉送」章節。

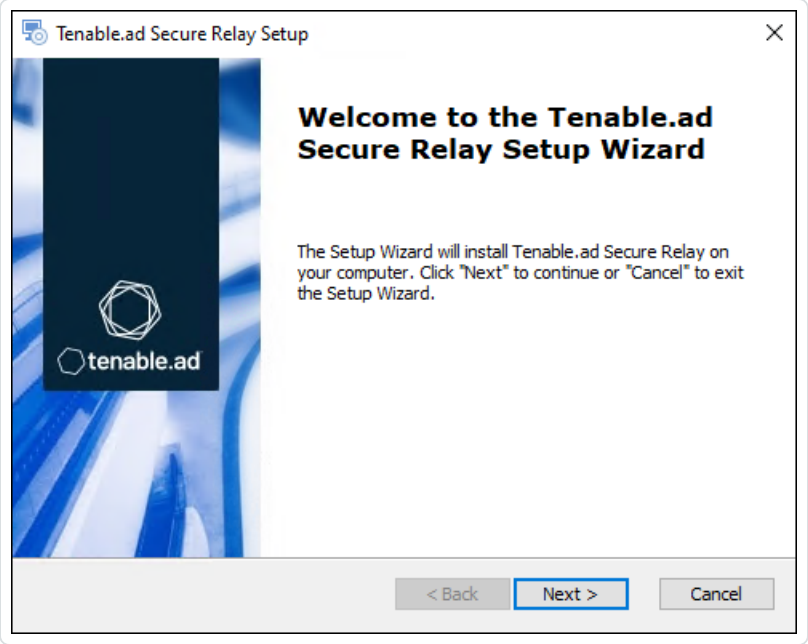
安裝安全轉送 (GUI)

以下程序使用 Windows 安裝程式安裝安全轉送。開始之前，請檢查您是否具備 安全轉送 中所述必要的先決條件和**必要的連結金鑰**

如要安裝安全轉送：

1. 從 Tenable Identity Exposure 下載入口網站 將安裝程式下載到您的虛擬機器。
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。

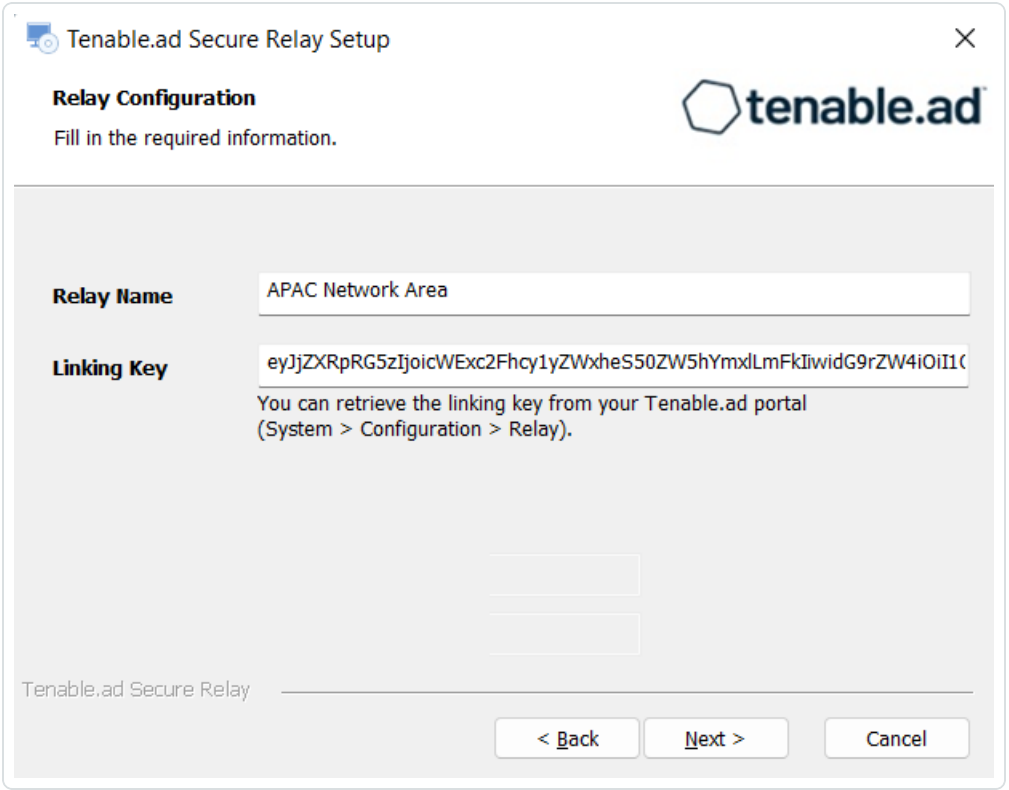


3. 按一下「**下一步**」。

   「**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：

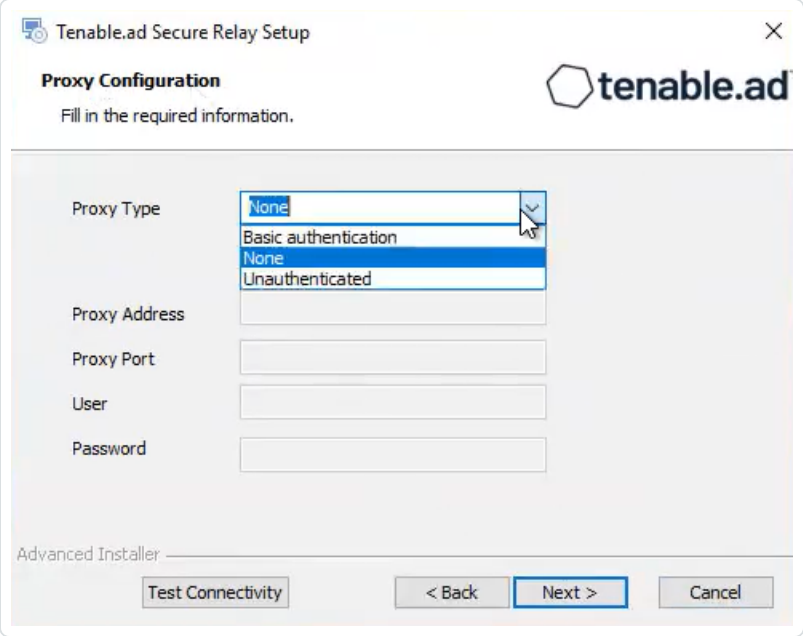
   a. 在「**轉送名稱**」方塊中輸入安全轉送的名稱。

   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」**。

下一步做什麼

- 安裝後檢查

另請參閱

- 安全轉送
- 安裝安全轉送 (Tenable Nessus Agent)
- 安裝後檢查
- 設定轉送

安裝安全轉送 (Tenable Nessus Agent)

以下程序使用 Tenable Nessus Agent 安裝安全轉送。

事前準備

- 檢查您是否已下載並安裝 Tenable Nessus Agent。

  注意：Tenable Nessus 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**。

如要安裝安全轉送：

1. 在託管 Tenable Nessus Agent 並作為轉送的電腦上，開啟 Tenable Nessus 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：

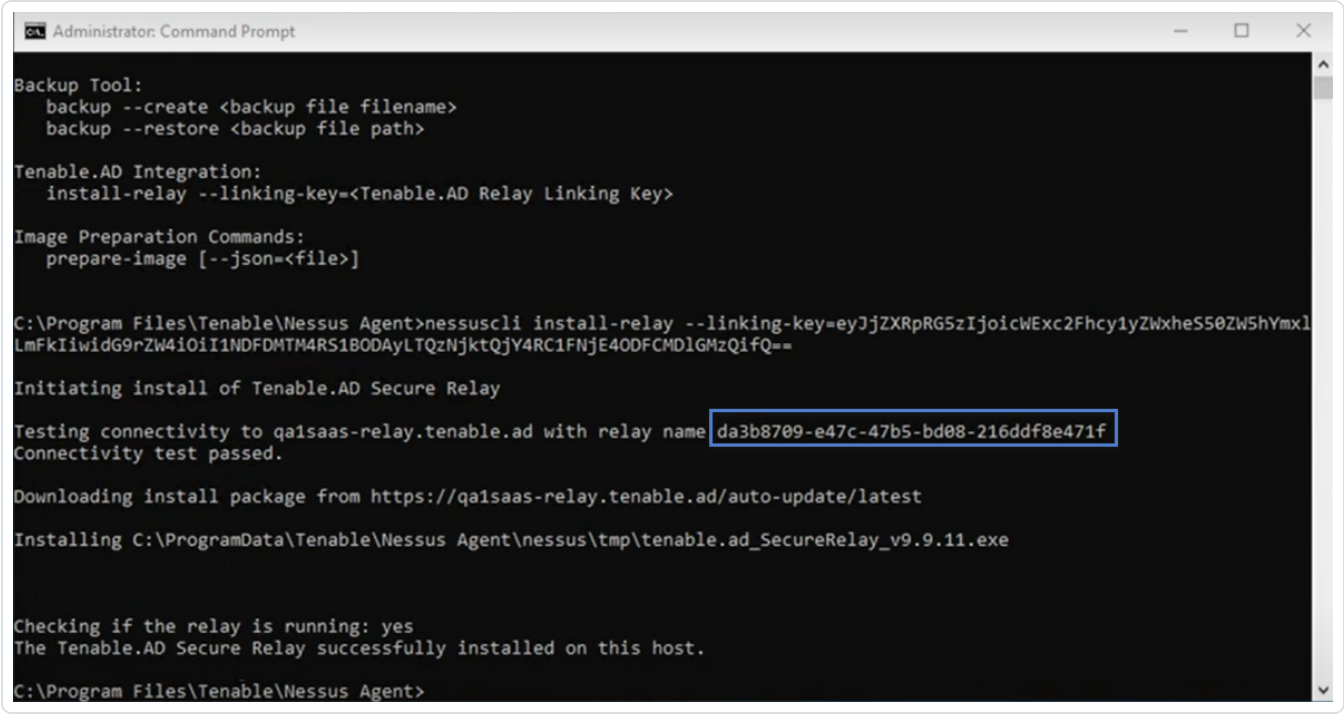
   安全轉送的安裝

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

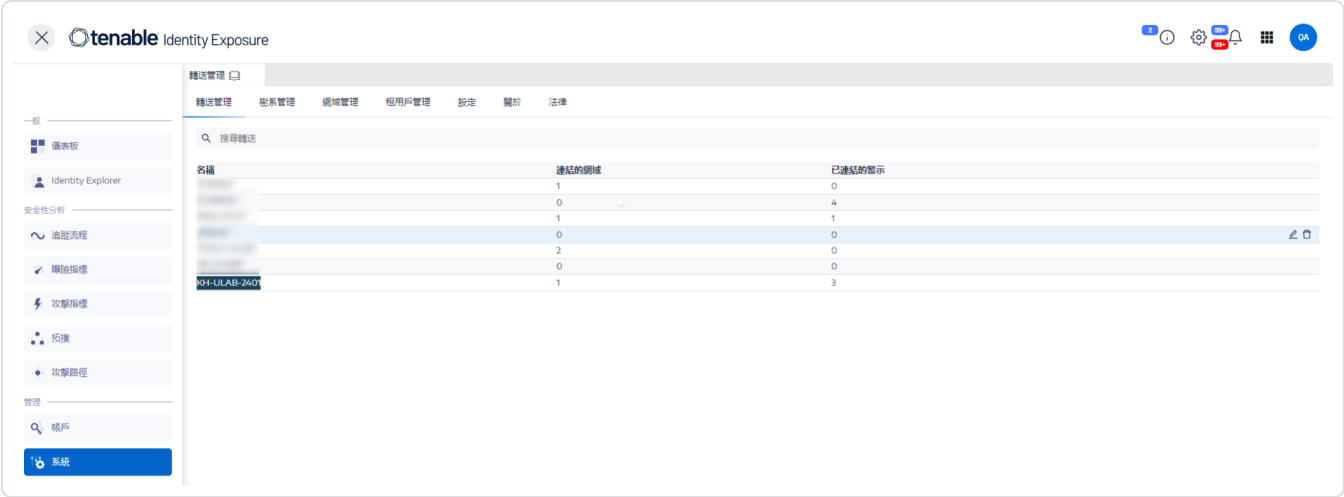
2. 將 <Tenable Identity Exposure Relay Linking Key> 替換為您之前從 Tenable Identity Exposure 執行個體複製的值，如果您使用 Proxy 伺服器，請提供 Proxy 位址和連接埠號碼。

   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。



後續步驟

- 安裝後檢查

另請參閱

- 安全轉送
- 安裝安全轉送 (GUI)
- 安裝後檢查
- 設定轉送

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

此安裝項目還新增了 4 個名稱以「ALSID」開頭且與安全轉送相關的新環境變數。如果您選擇使用 Proxy 伺服器，還會有另外 2 個與 Proxy 伺服器 IP 和連接埠有關的變數。

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。

後續步驟

- 設定轉送

另請參閱

- 安全轉送
- 安裝安全轉送 (GUI)
- 安裝安全轉送 (Tenable Nessus Agent)

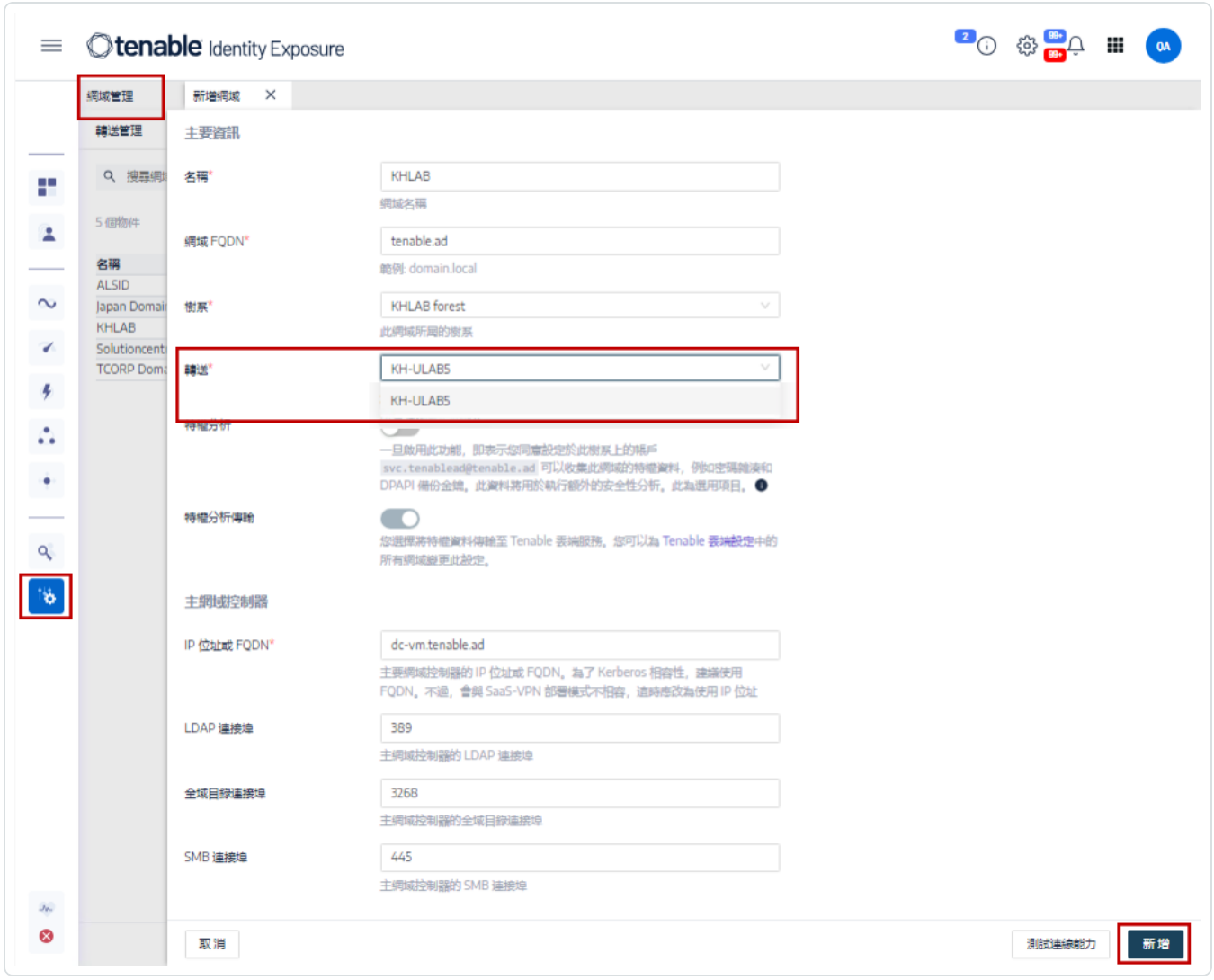
設定轉送

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。

如要將網域連結至安全轉送：

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。



4. 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。

另請參閱

- 安全轉送
- 安裝安全轉送 (GUI)
- 安裝安全轉送 (Tenable Nessus Agent)
- 安裝後檢查

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。

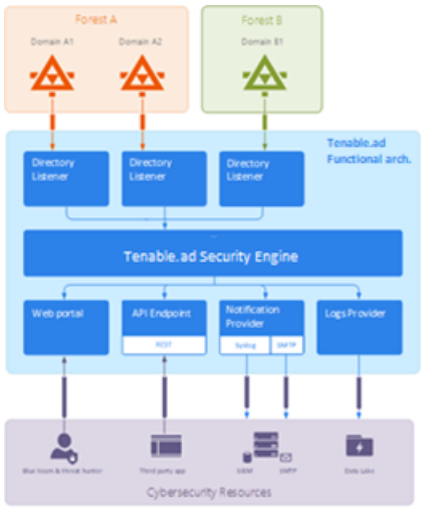
Tenable Identity Exposure 會使用沒有管理權限的一般使用者帳戶連線至標準 API,以實現安全性監控功能。

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。
- 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，因為它無法在 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。

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。

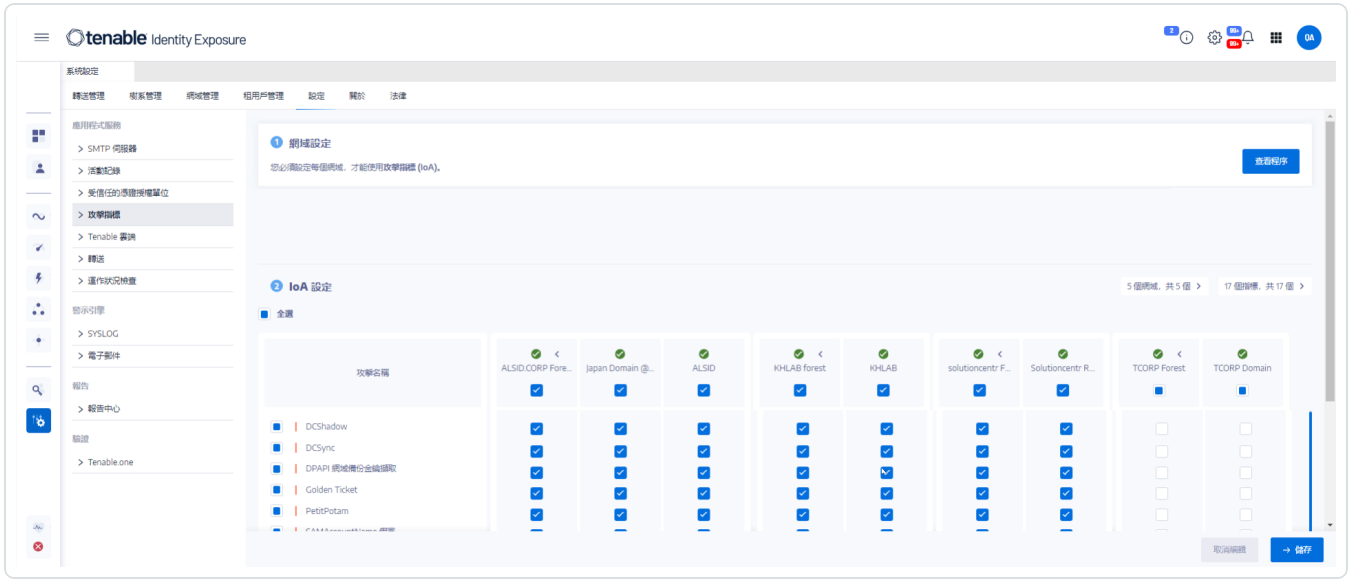
如要設定攻擊指標 (IoA) 的網域：

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。

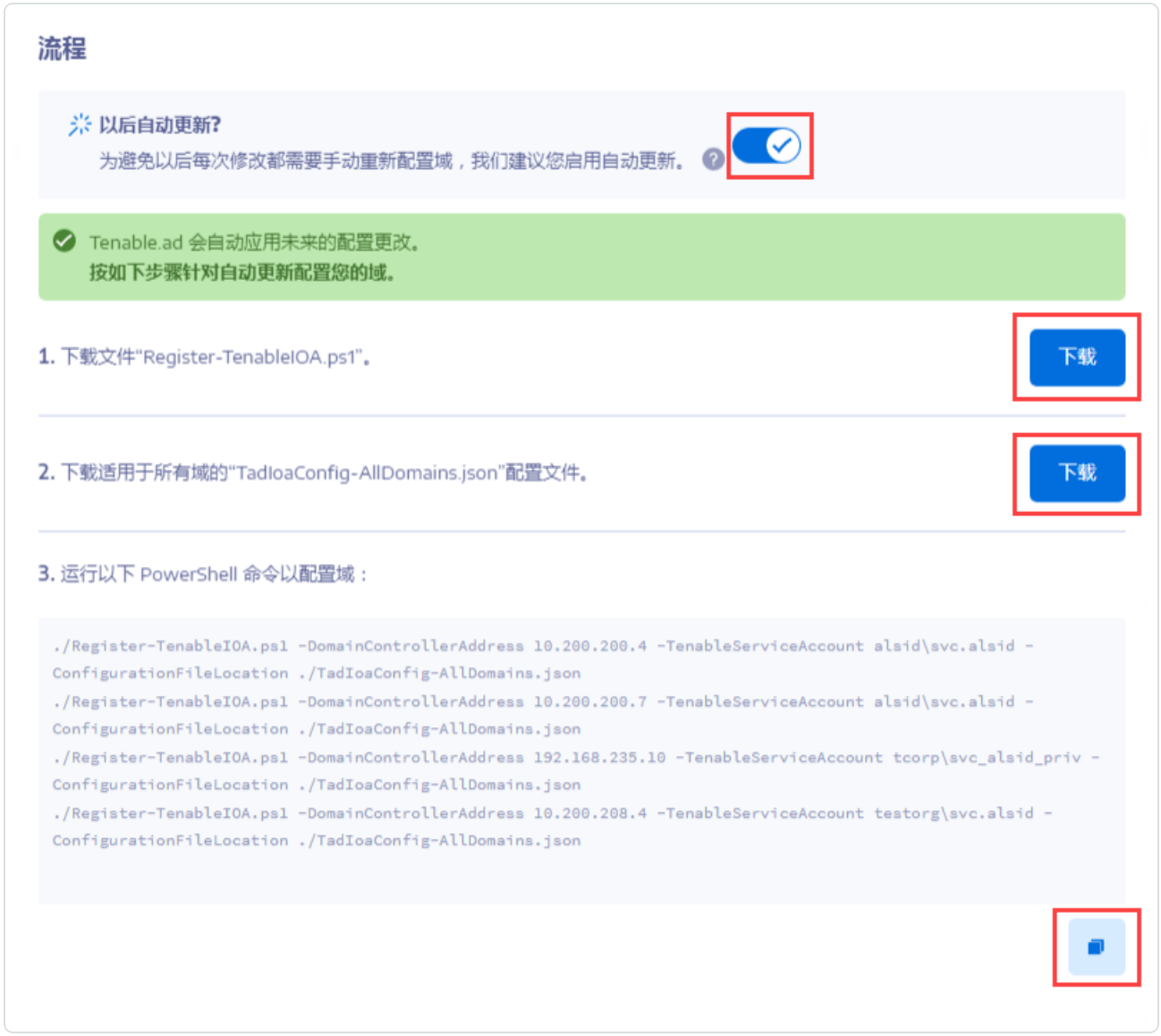
2. 按一下「**攻擊指標**」。

   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。

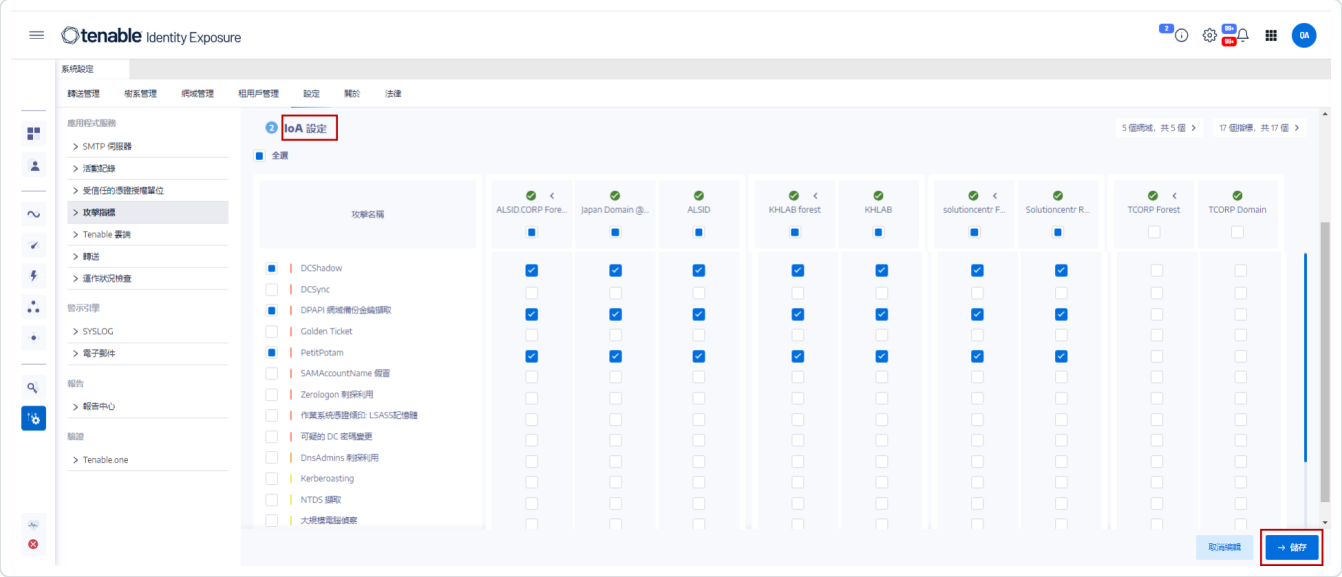
- 如果您關閉此選項，系統會顯示一則訊息，要求您將其開啟以取得未來自動更新。按一下「**查看程序**」並切換為「**啟用**」。

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 權限提升弱點

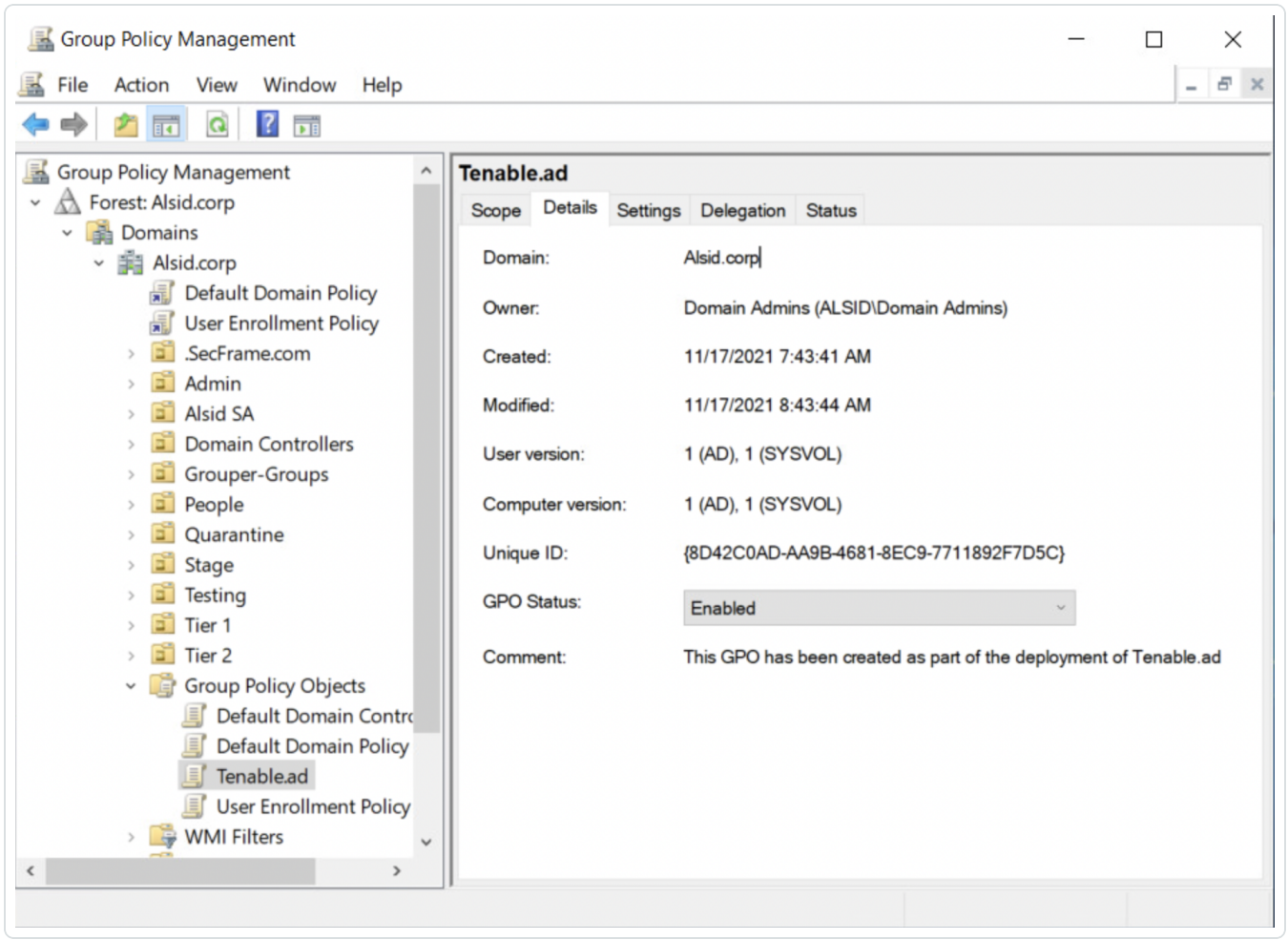
(Netlogon Elevation of Privilege Vulnerability) 中的資訊。確認 DC 的安全性之後，您可以安全地停用此攻擊指標 (IoA) 以避免收到不必要的警示。

2. 按一下「**儲存**」。

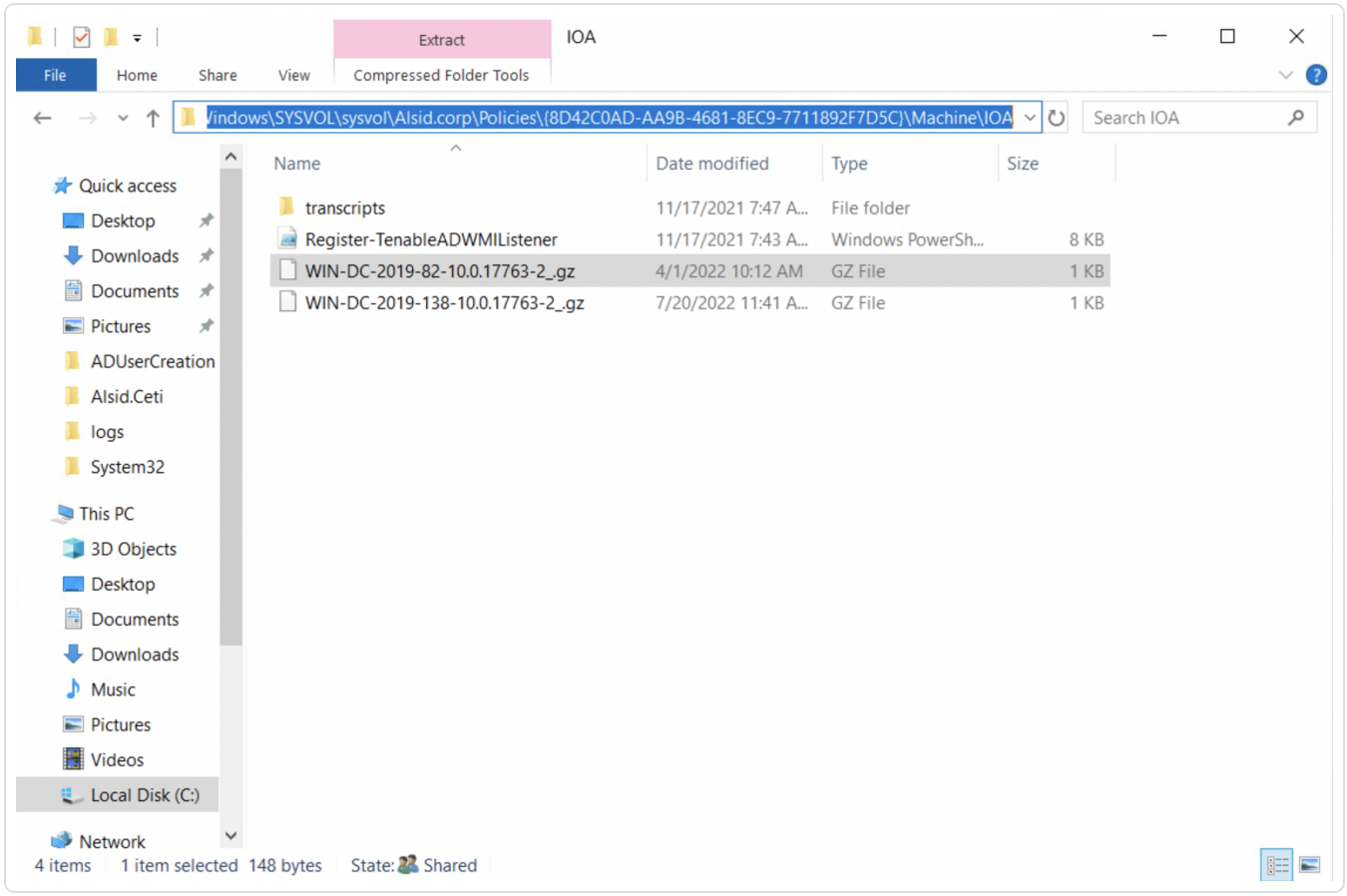
   - 如果您已啟用「**未來自動更新**」，Tenable Identity Exposure 會儲存並自動更新您的新設定。等待幾分鐘後，此更新才會生效。
   - 如果您未啟用「**未來自動更新**」，系統會顯示程序視窗，指引您 [如要設定攻擊指標 (IoA) 的網域：]

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「IOA」文件夾並選取「**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. 檢查是否已啟用「寫入」權限。

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>
```

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。 • 檢查服務帳戶是否具有修改檔案內容的

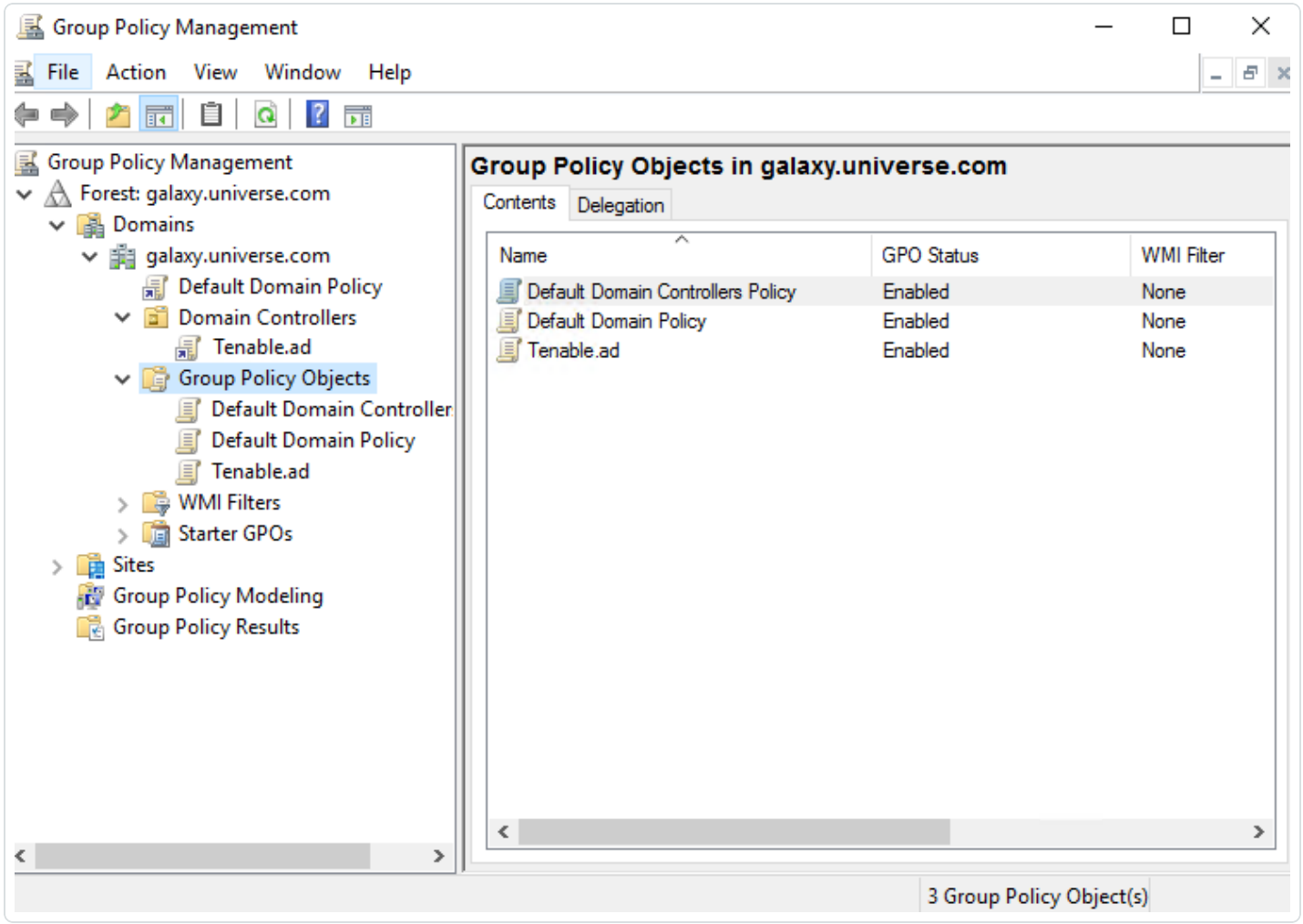
	權限。 • 如果您不想向服務帳戶授予權限，請停用「自動更新」開關，並按一下「查看程序」以取得有關在每次修改攻擊指標 (IoA) 設定時如何進行手動更新的說明。
「目標資料夾 <targetFolder> 包含無法執行自動更新的 Tenable Identity Exposure 版本。」	目前安裝的指令碼是使用 WMI 的舊版本。解除安裝目前版本，然後下載新的安裝指令碼，並執行此指令碼。
「設定檔部署遇到意外錯誤。」	解除安裝指令碼，然後按一下「查看程序」以獲取重新安裝指令碼的說明。如果這行不通，請聯絡您的客戶支援代表。

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)

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

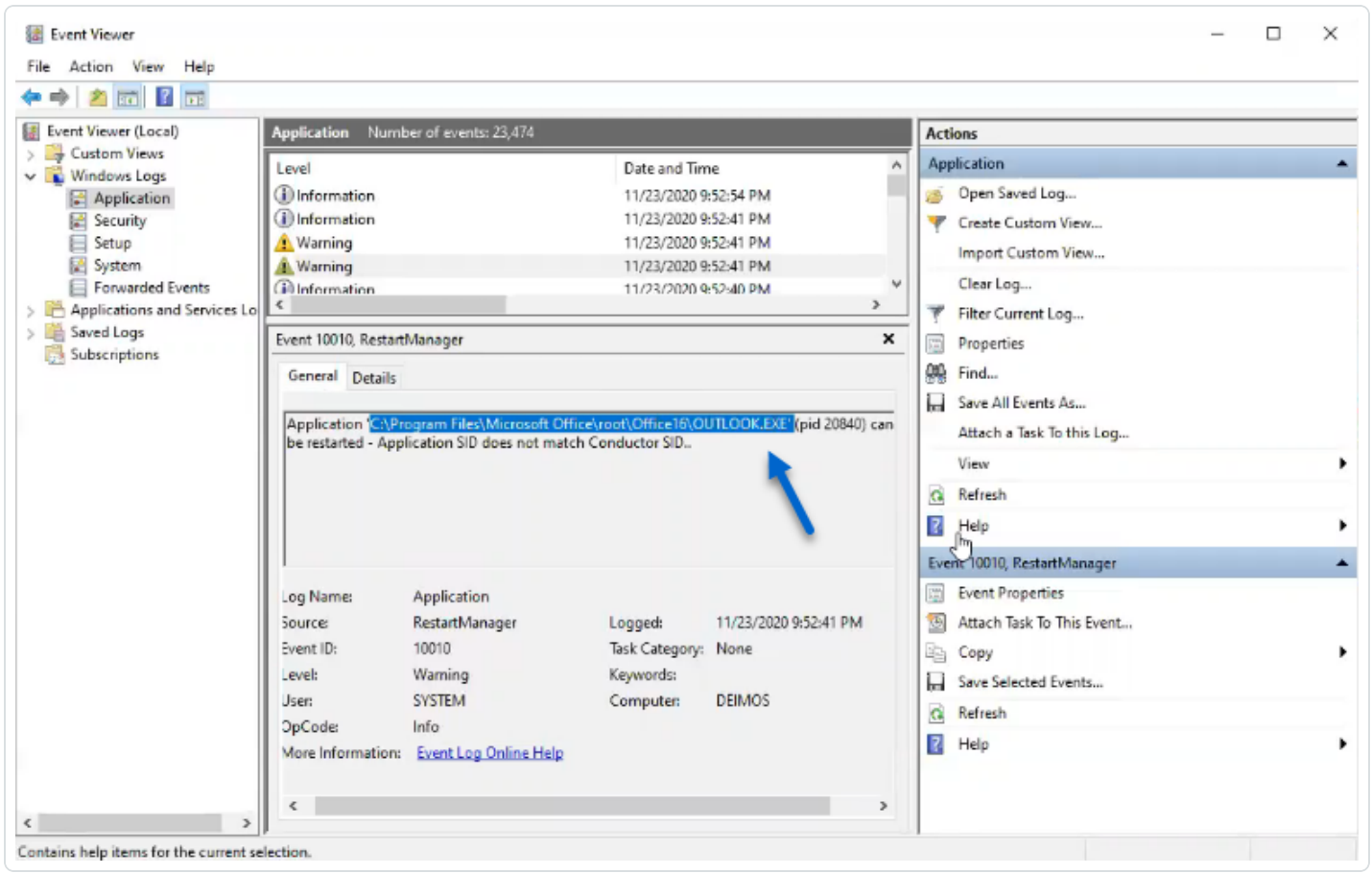
錄通道。

- 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 的內容都會被排清到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 複製和群

	上啟動 Tenable Identity Exposure 的 IoA 部署	機系統	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 資料夾	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。

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)

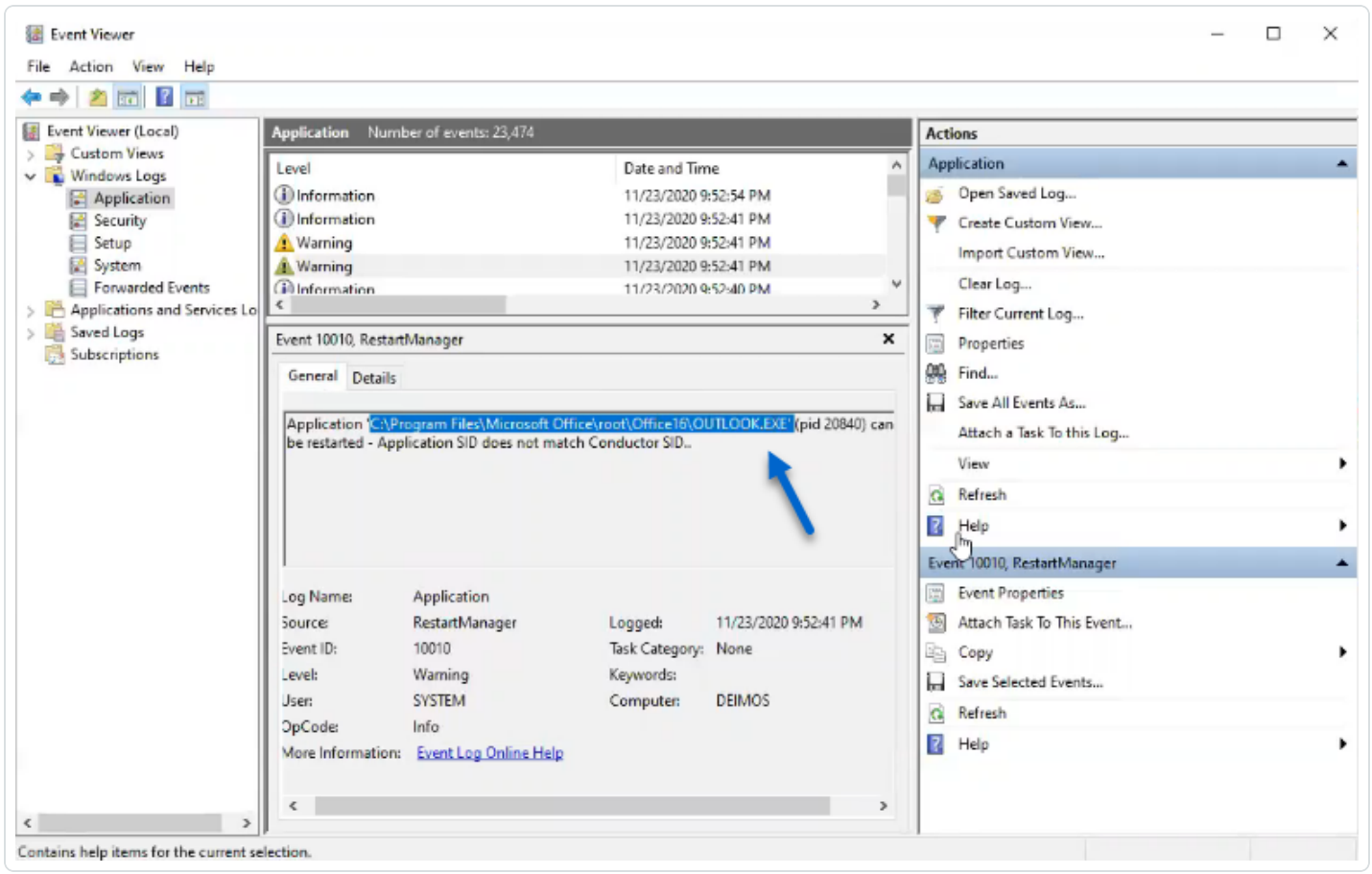
GPO 包含所有 DC 為收集相關資料而在本機執行的 PowerShell 指令碼，如下所示：

- 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，然後將它們清除至 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 複製和群

	上啟動 Tenable Identity Exposure 的 IoA 部署	機系統	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

- Indicators of Attack and the Active Directory
- 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:

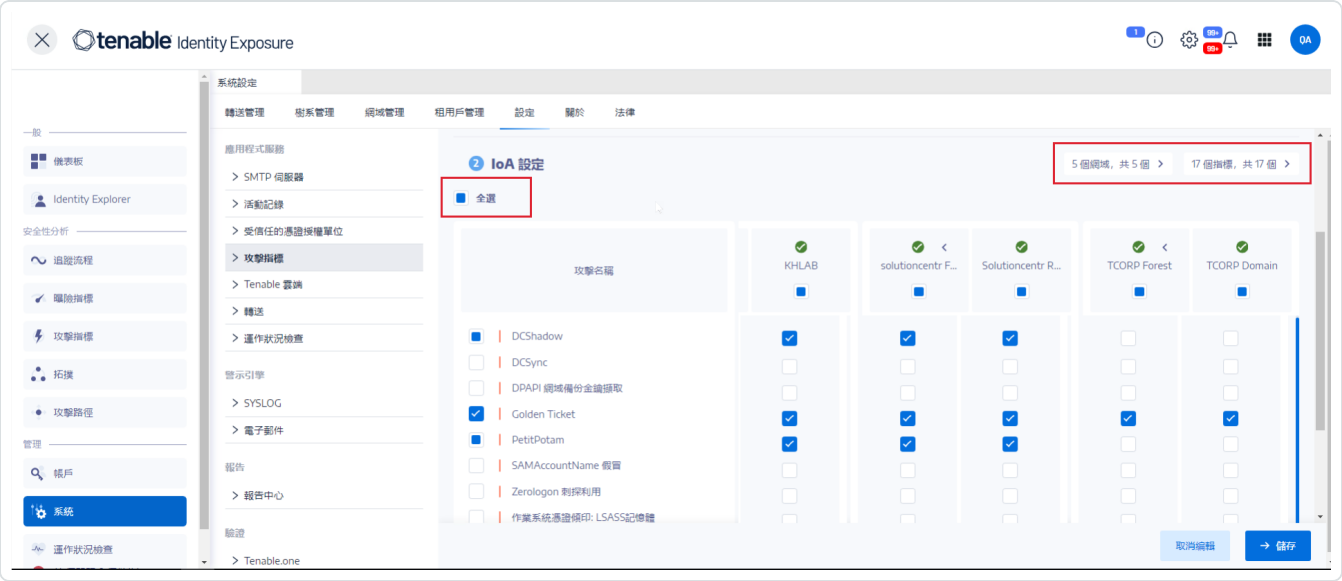
- 在**資料實體**中,以下項目的「讀取」存取權:
  - 所有攻擊指標
  - 所有網域
- 在**介面實體**中,以下項目的存取權:
  - 管理 > 系統 > 設定
  - 管理 > 系統 > 設定 > 應用程式服務 > 攻擊指標
  - 管理 > 系統 > 設定 > 應用程式服務 > 攻擊指標 > 下載安裝檔案

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：

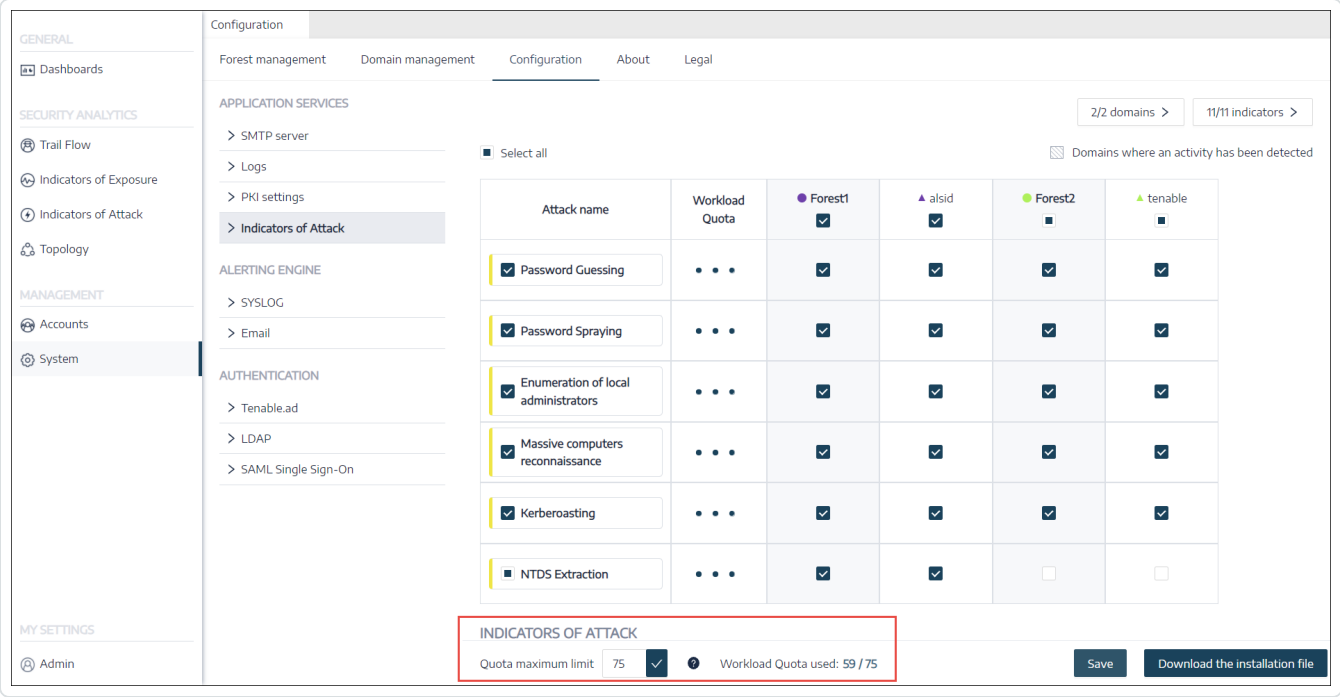
- 增加：在增加之後監控統計資料，以確保有適當的餘量。
- 減少：停用部分攻擊指標以維持在此配額之下，這會降低針對攻擊的安全範圍。

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
   ```

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

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 進階稽核原則需求。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。

如要修正 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 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
```

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
```

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

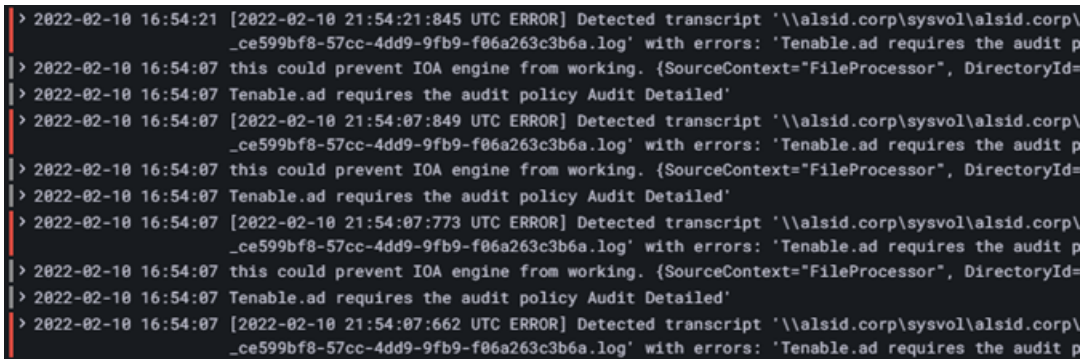
- 檢查 CETI 記錄中是否有下列錯誤訊息：

```
[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"}
```

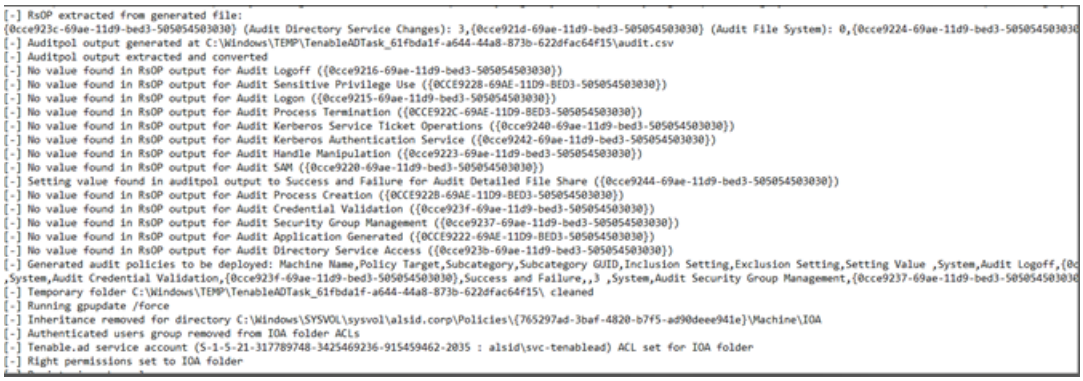
- 如果您看到此訊息，請驗證 GPO 設定和 WMI 消費者是否在上述錯誤訊息中所列的網域控制器 (DC) 上執行。

稽核設定

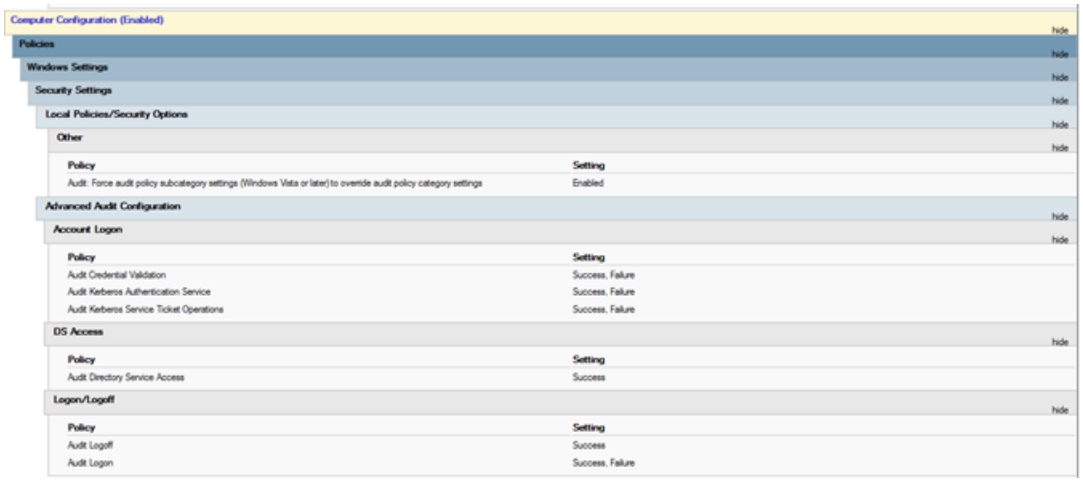
- 如果您看到與下列類似的錯誤：「Tenable Identity Exposure 需要稽核原則...」，請檢查您現有的 GPO，確保您沒有將所需的稽核原則設定為「無稽核」。



- 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

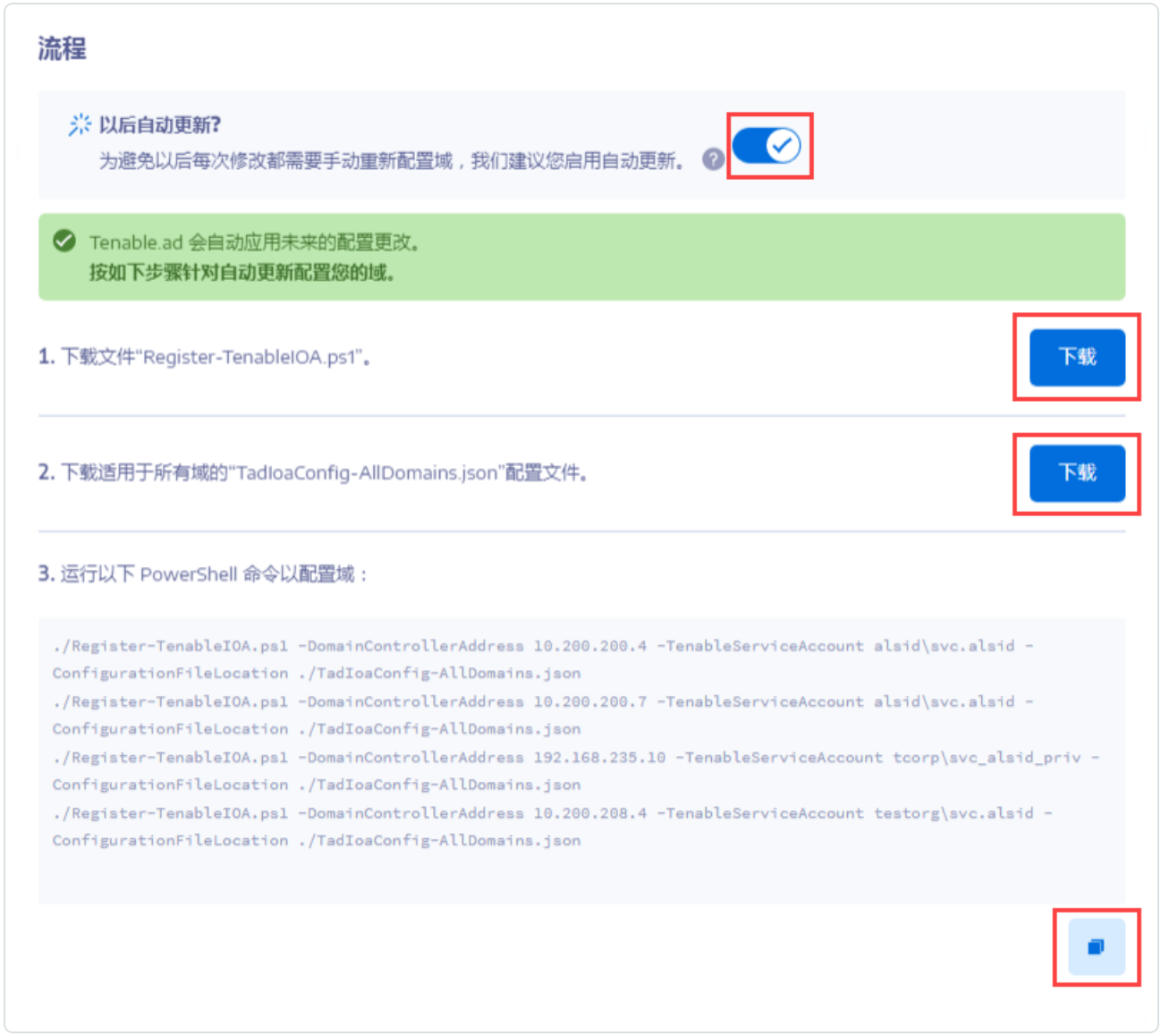
`-EventLogsFileWriteFrequency X` 參數的值 [X] 是 Tenable Identity Exposure 接聽程式在非 PDCe 網域控制器 (DC) 上產生事件記錄檔的頻率。Tenable Identity Exposure 接聽程式所使用的預設建議值為 15 秒。不過，自訂值不適用於 PDCe DC，且會維持其預設的 15 秒間隔，以確保攻擊偵測功能可完全運作。Tenable 建議您僅在基礎架構面臨或容易受到 DFS 複製問題影響時，才使用此參數，並將其值從預設的 15 秒增加到 300 秒 (5 分鐘)。

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。

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。 • **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。 如要設定鎖定持續時間： 1. 按一下滑桿以設定鎖定持續時間。 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**」。 **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。 如要設定挽回期： 1. 按一下滑桿以設定時間間隔。 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。請參閱程序 如要為 LDAPS 新增自訂的受信任憑證授權單位 (CA) 憑證： 以完成 LDAP 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辨別名稱或 UserPrincipalName，請保留「**啟用 SASL 繫結**」為停用狀態。
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 ⊕ 圖示以新增允許的群組。
8. 按一下「**儲存**」。

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**」。

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：

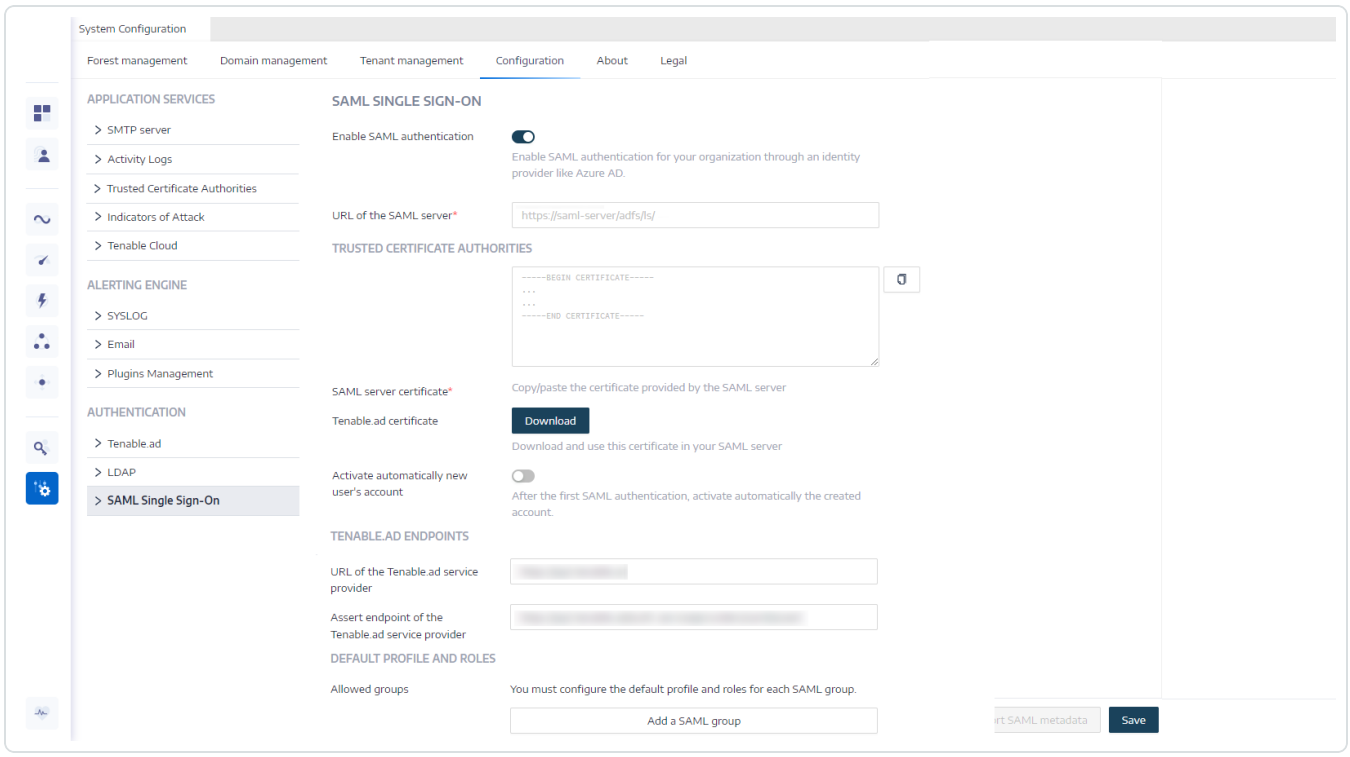
1. 在 Tenable Identity Exposure 中，按一下「**系統**」>「**設定**」。

   「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 ⊕ 圖示以新增允許的群組。
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 - 包含所有權限的管理員角色。
- 使用者 - 僅擁有業務資料唯讀權限的簡單使用者角色

如需詳細資訊，請參閱：

- 建立使用者
- 編輯使用者
- 停用使用者
- 刪除使用者

建立使用者

所需的使用者角色：具有適當權限的管理員或組織使用者。

注意：下列指引適用於 Tenable Identity Exposure 的獨立執行個體。針對與 Tenable Vulnerability Management 連結的執行個體，如果您在 Tenable Vulnerability Management 中建立使用者，之後會散佈至 Tenable Identity Exposure。

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。

另請參閱

- 編輯使用者
- 停用使用者
- 刪除使用者

編輯使用者

所需的使用者角色:具有適當權限的管理員或組織使用者。

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。

另請參閱

- 建立使用者
- 停用使用者
- 刪除使用者

停用使用者

所需的使用者角色:具有適當權限的管理員或組織使用者。

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。

另請參閱

- 建立使用者
- 編輯使用者
- 刪除使用者

刪除使用者

所需的使用者角色:具有適當權限的管理員或組織使用者。

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。

另請參閱

- 建立使用者
- 編輯使用者
- 停用使用者

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。「**設定檔組態**」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。

   「**設定檔組態**」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. 按一下要自訂的指標的名稱。

   「**指標自訂**」窗格會隨即顯示。

6. 對指標進行必要的自訂。

   注意:某些指標選項需要使用正則運算式 (regex)。規則運算式的比對結果以包含相符內容為準,而非與內容完全相符的結果。範例:當您提供「`admin`」作為輸入選項時,您可以將具有「`samAccountName=admin`」的使用者以及具有「`samAccountName=admintoto`」的使用者列入白名單。
   - 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「**設定檔組態**」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「**設定檔組態**」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。

   「設定檔組態」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。

   「第 1 個自訂」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 • 曝險指標 • 樹系 • 網域 • 設定檔 • 使用者 • 電子郵件警示 • Syslog 警示 • 角色 • 實體轉送 • 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的能力，以及修改個人資訊和喜好設定的能力。	• 喜好設定 • 儀表板 • 小工具 • API 金鑰 • 個人資訊	編輯、建立
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	讀取、編輯

	位) • 透過公用 API 評分 • 授權 • LDAP 驗證 • SAML 驗證 **注意**:如果您擁有 Tenable Vulnerability Management 授權,則無法使用 LDAP 和 SAML 驗證權限。 • 拓撲 • 帳戶鎖定原則 • 重新編目網域 • 活動記錄 • Tenable 雲端服務 (Tenable Cloud 資料收集) • Microsoft Entra ID 支援 • 運作狀況檢查 • 僅顯示使用者自己的追蹤記錄	
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：

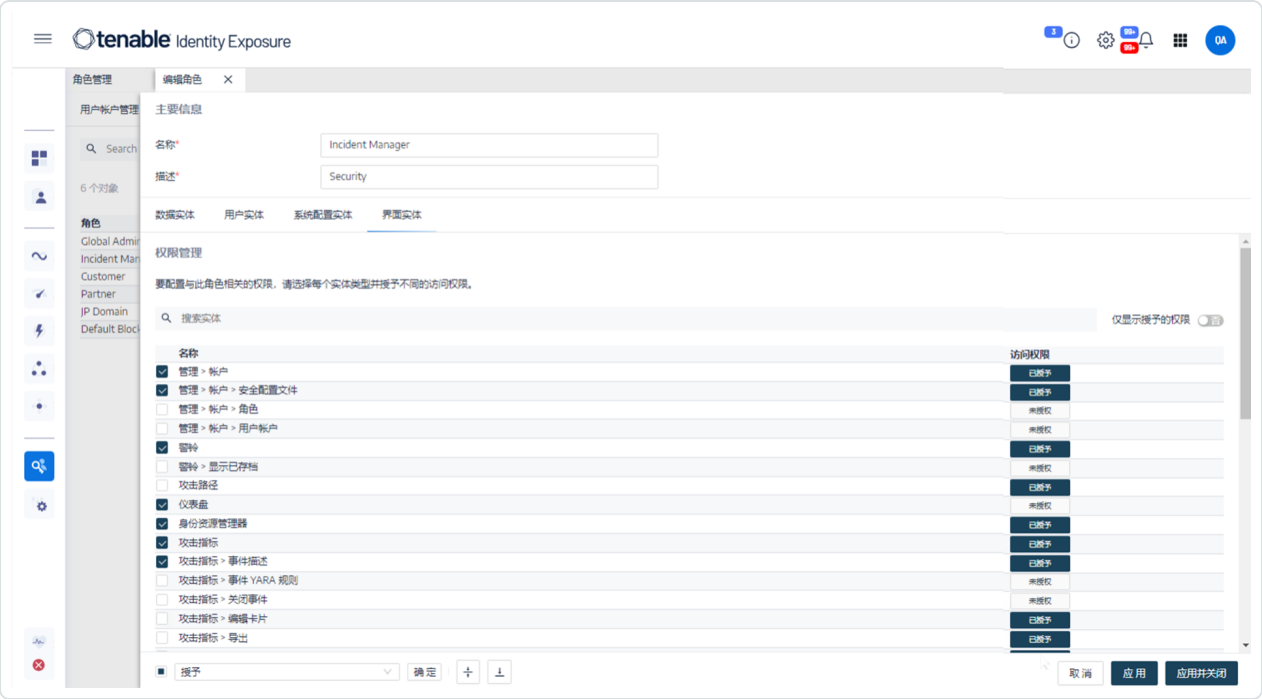
- 系統設定：「**管理**」>「**系統**」
- 設定參數：「**管理**」>「**系統**」>「**設定**」
- Syslog 警示：「**管理**」>「**系統**」>「**設定**」>「**警示引擎**」>「**SYSLOG**」

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**」。

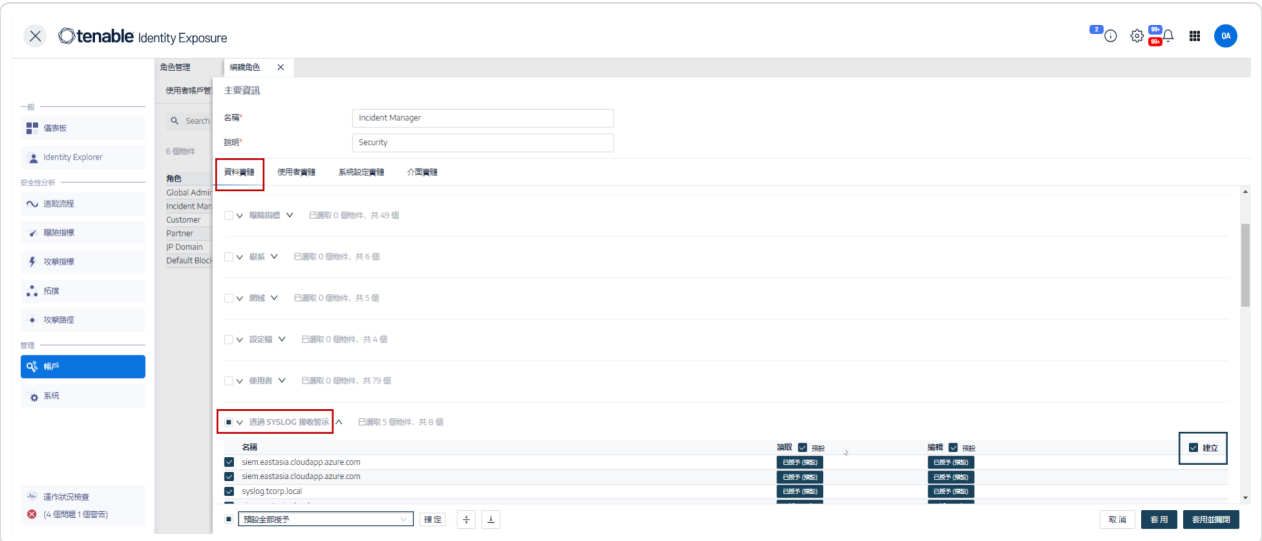
   系統會顯示一則訊息，確認 Tenable Identity Exposure 已更新實體權限。



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

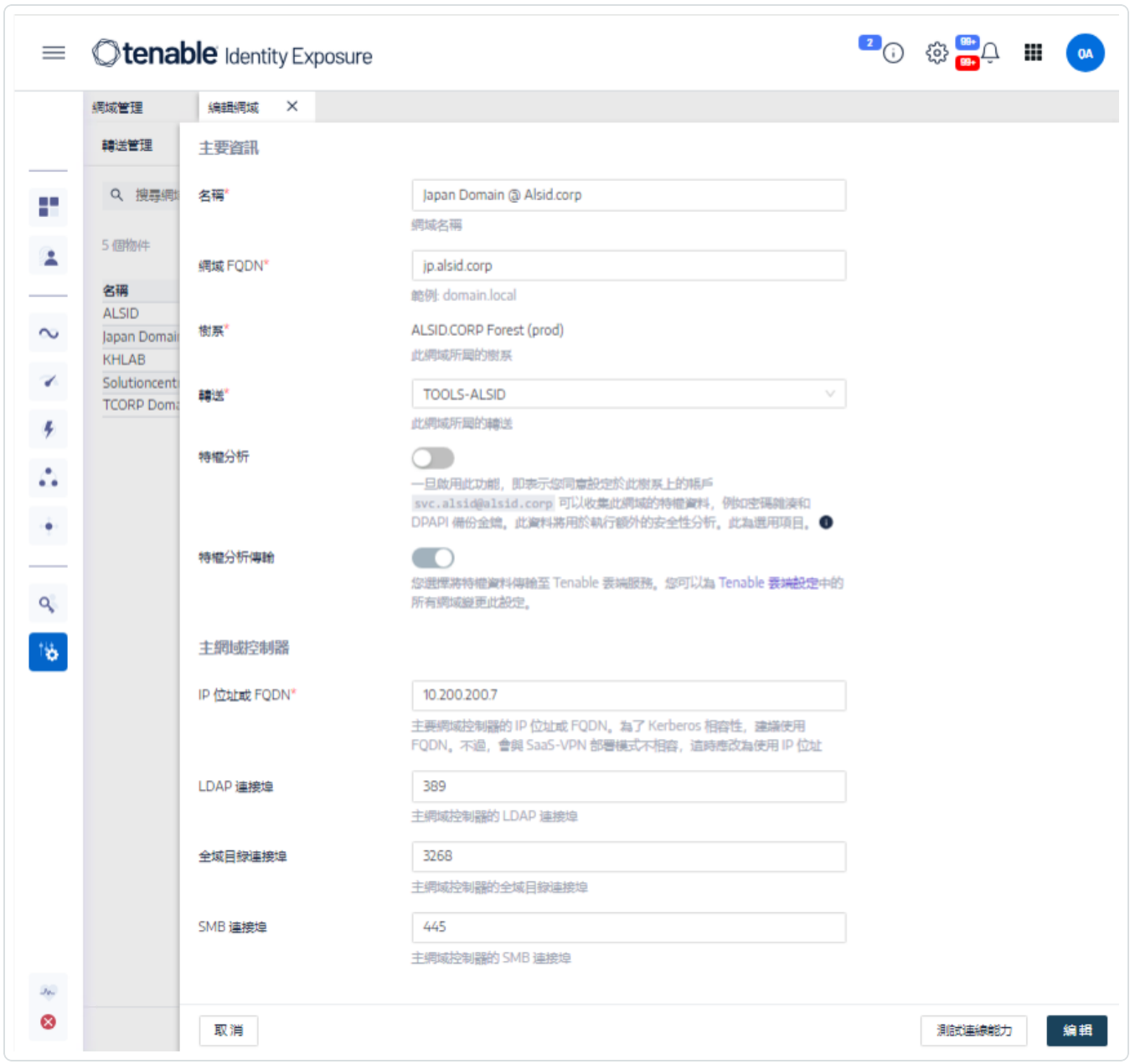
Tenable Identity Exposure 會監控網域，這些網域以邏輯方式將共用通用設定的物件分組，以便進行集中管理。

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：

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。
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。

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。

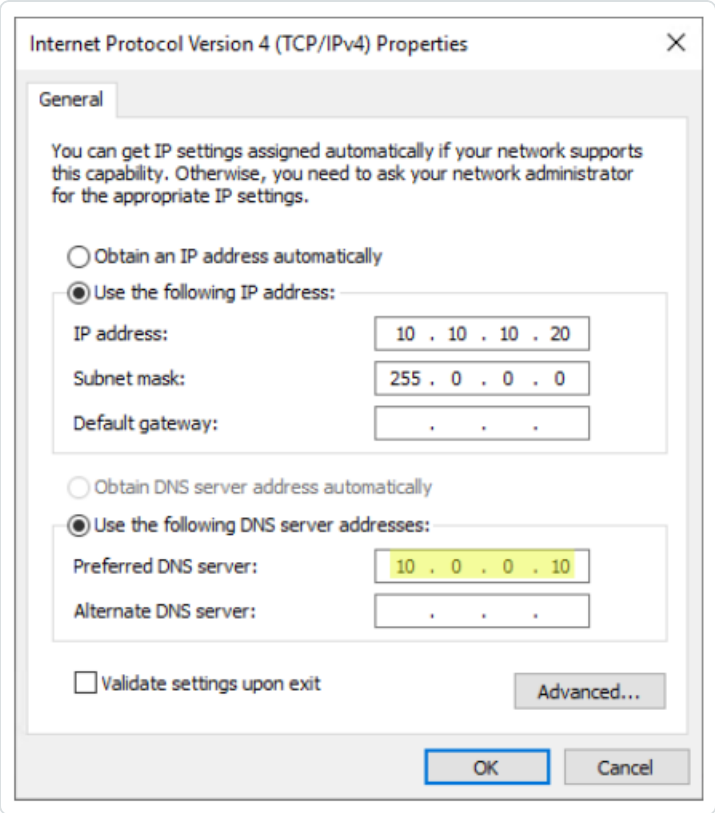
使用 NTLM 而非 Kerberos 也是 SYSVOL 強化干擾 Tenable Identity Exposure 的原因。如需詳細資訊，請參閱SYSVOL 強化干擾 Tenable Identity Exposure。

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 安全轉送 的 SaaS	是
採用 VPN 的 SaaS	否 - 您必須將安裝切換至 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，請參閱網路流對照表和 TLS 網路對照表。

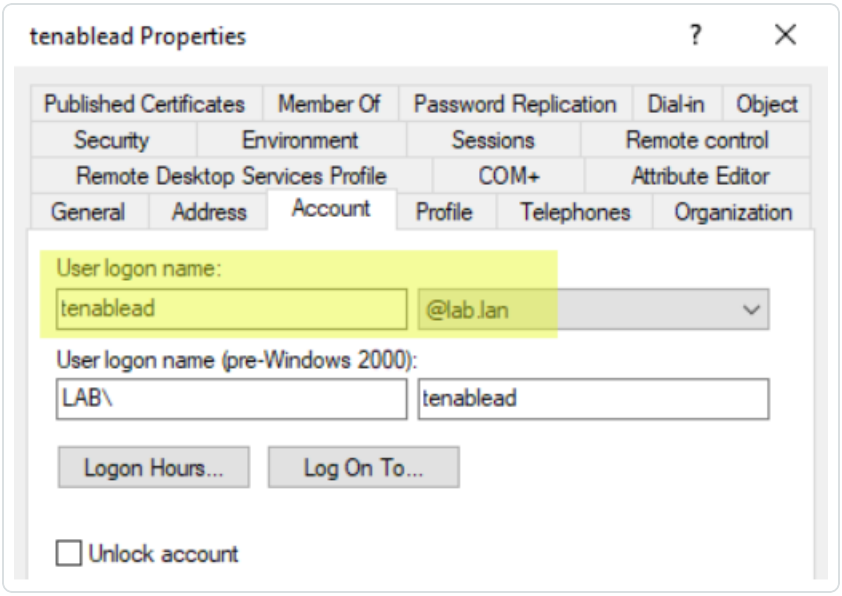
  注意：目錄接聽程式或轉送電腦不需加入網域即可使用 Kerberos。

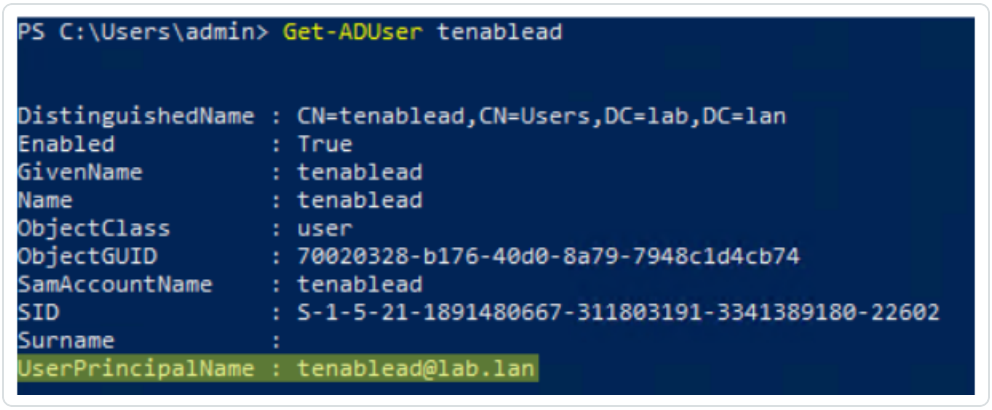
服務帳戶和網域設定

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：

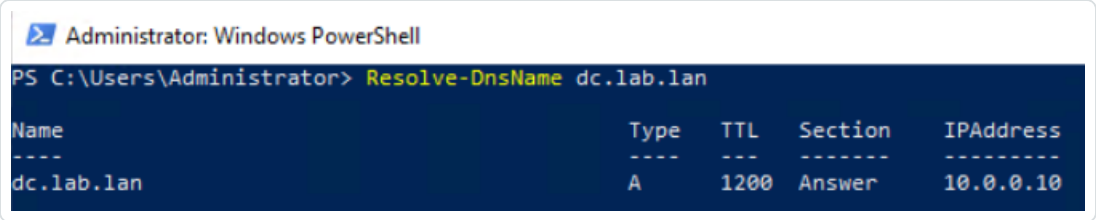
2. 使用完整網域名稱 (FQDN) 在 Tenable Identity Exposure 的網域設定中，設定主要網域控制器 (PDC) 的 FQDN，而非其 IP。

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

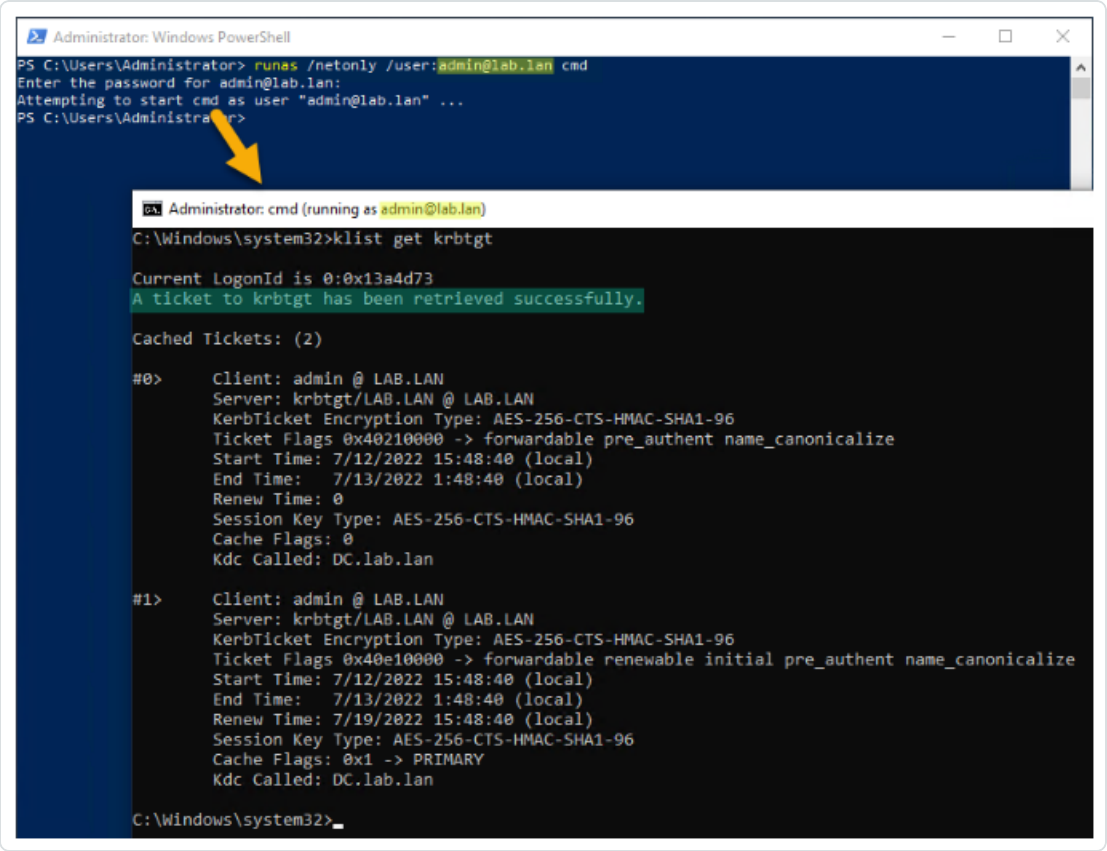
如要驗證 Kerberos 可否與您在目錄接聽程式或轉送電腦上執行的命令搭配使用：

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：

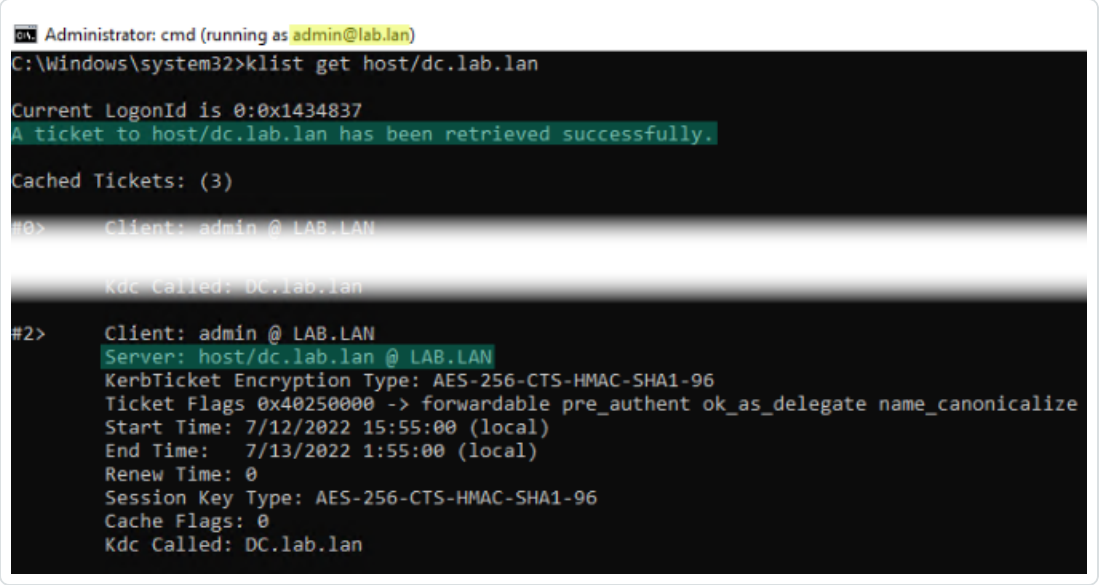


可能的錯誤代碼如下：

- `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：


Administrator: cmd (running as admin@lab.lan)
C:\Windows\system32>klist get host/dc.lab.lan
Current LogonId is 0:0x1434837
A ticket to host/dc.lab.lan has been retrieved successfully.
Cached Tickets: (3)
#0> Client: admin @ LAB.LAN
Kdc Called: DC.lab.lan
#2> Client: admin @ LAB.LAN
Server: host/dc.lab.lan @ LAB.LAN
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40250000 -> forwardable pre_authent ok_as_delegate name_canonicalize
Start Time: 7/12/2022 15:55:00 (local)
End Time: 7/13/2022 1:55:00 (local)
Renew Time: 0
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: DC.lab.lan

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

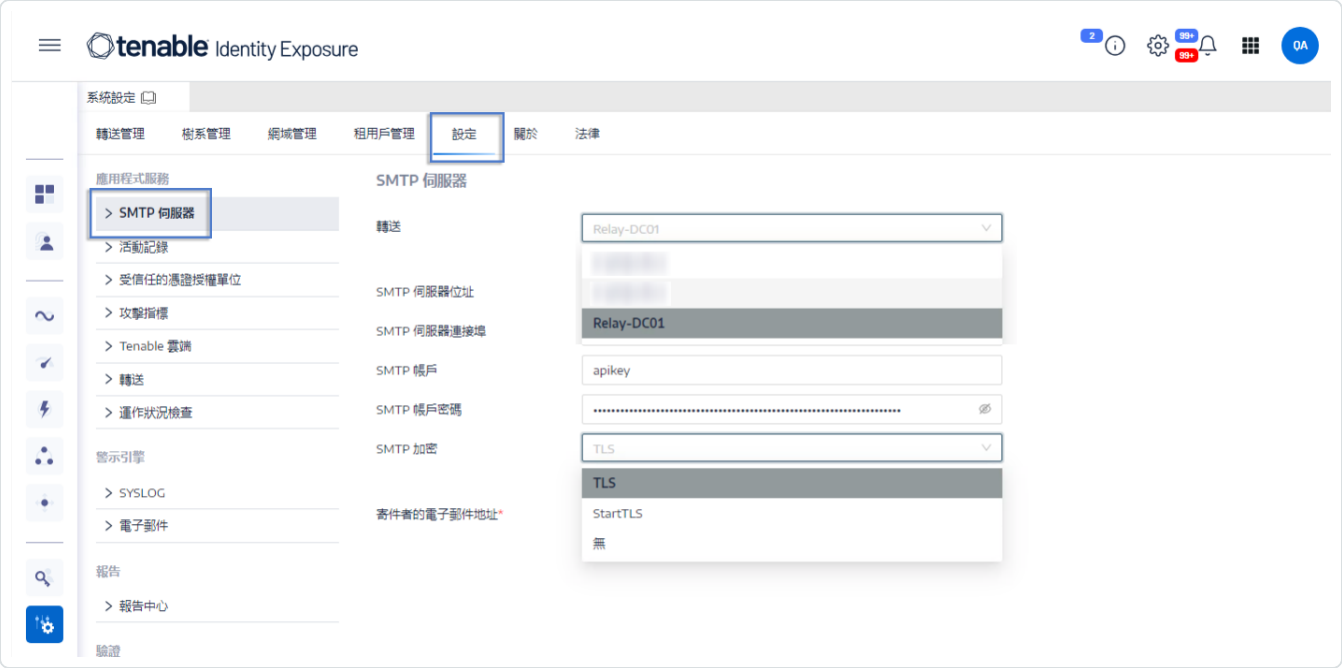
SMTP 伺服器設定

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。

如要設定 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。



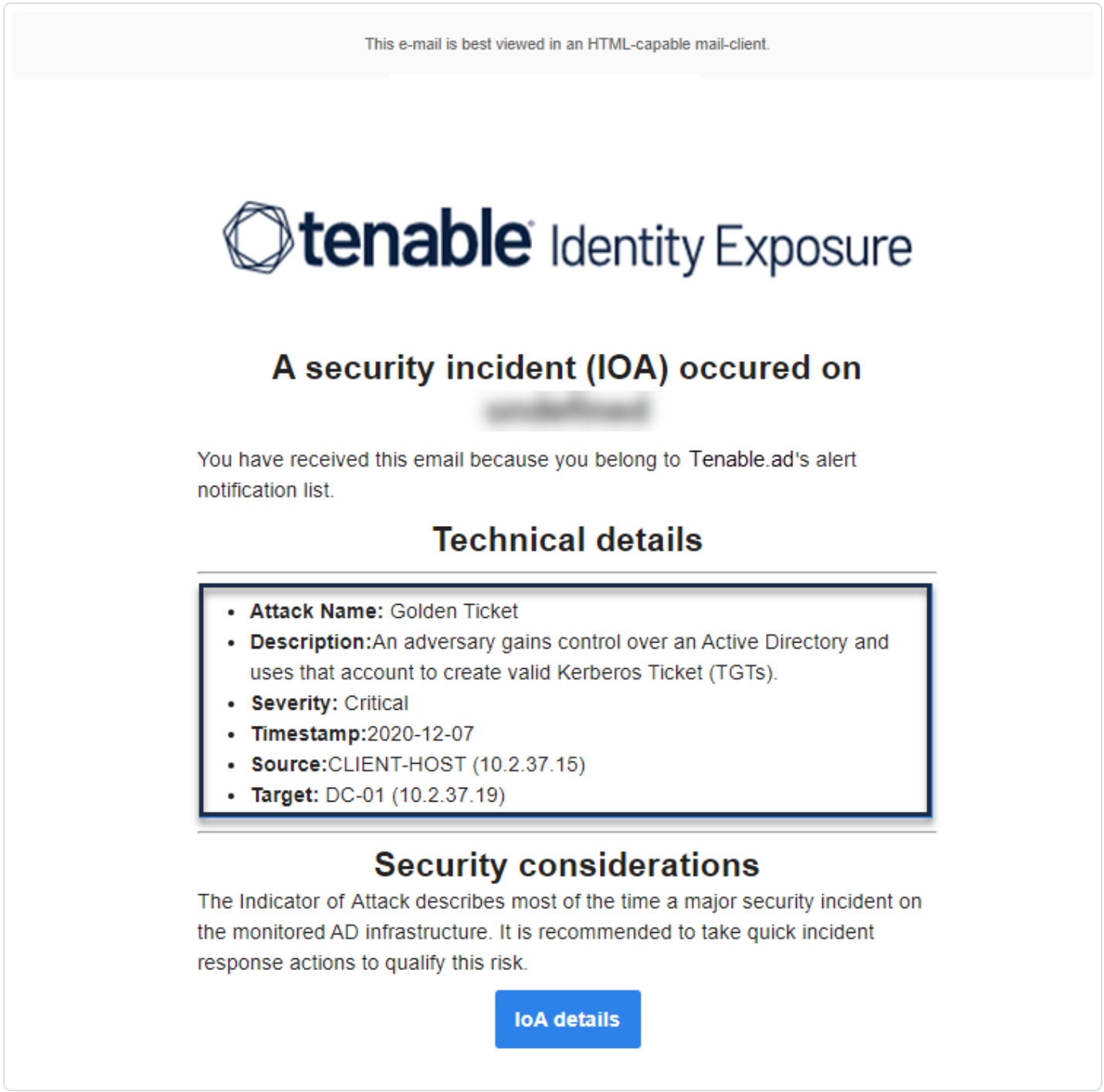
3. **如果您的網路使用安全轉送：**在「**轉送**」方塊中按一下箭頭，從下拉式清單中選取要與 SMTP 伺服器通訊的轉送。
4. 提供以下資訊：
   - SMTP 伺服器位址
   - SMTP 伺服器連接埠
   - SMTP 帳戶
   - SMTP 帳戶密碼

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。

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：



如要新增電子郵件警示：

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。

如要編輯電子郵件警示：

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 如要新增電子郵件警示：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。

如要刪除電子郵件警示：

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

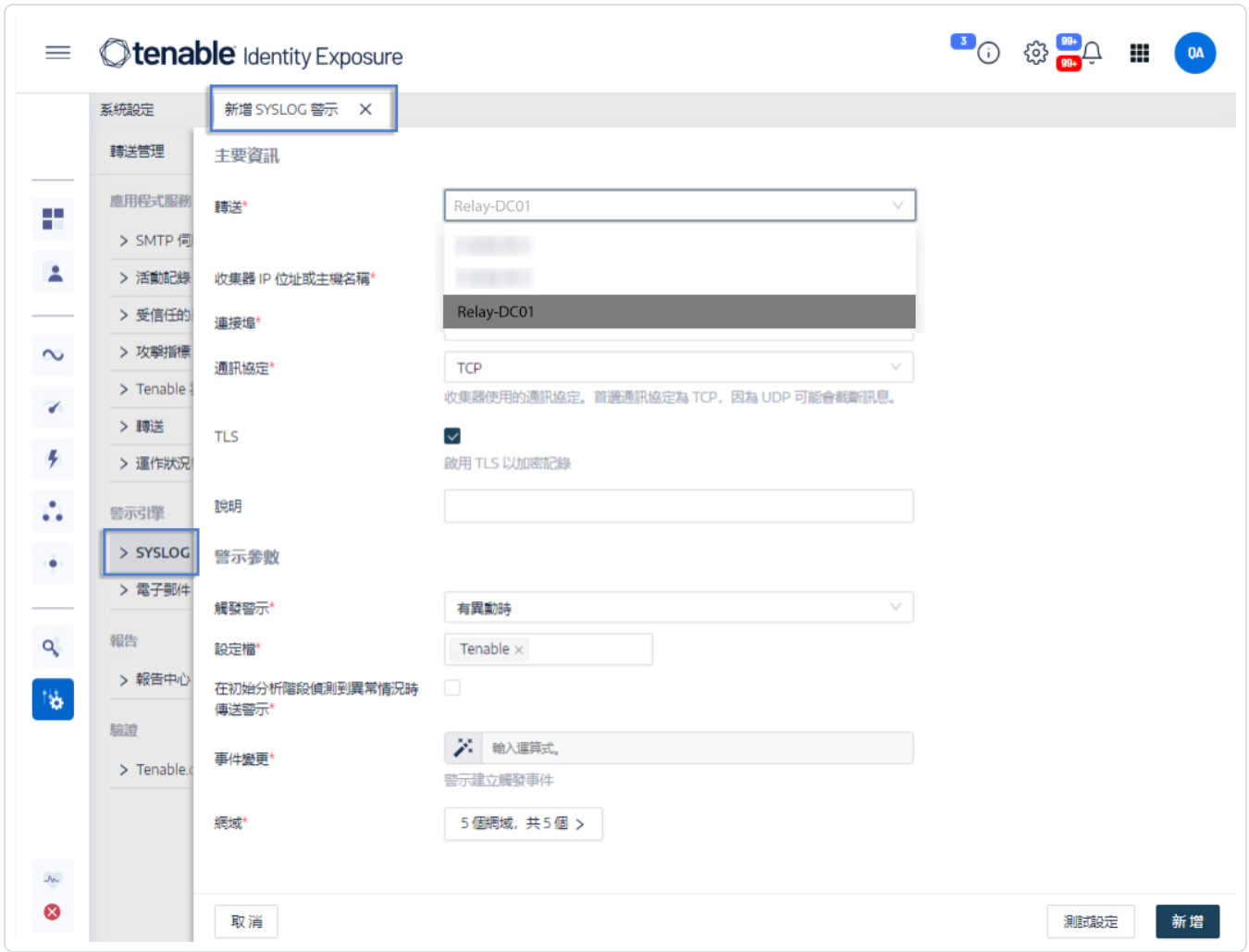
Syslog 警示

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。

如要新增 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：

- **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。

- **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。

如要編輯 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 如要新增 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。

如要刪除 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。

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"
```

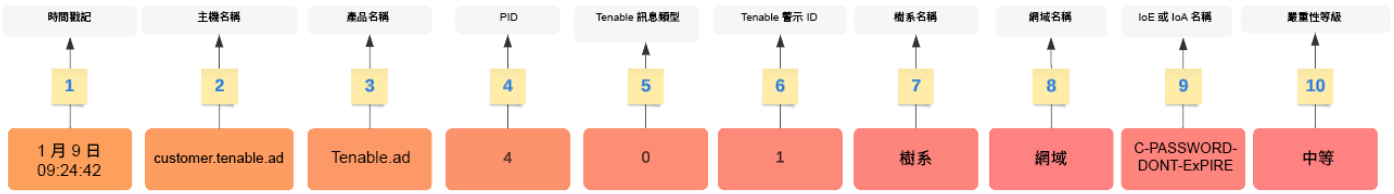
攻擊指標 (IoA) 的警示範例

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

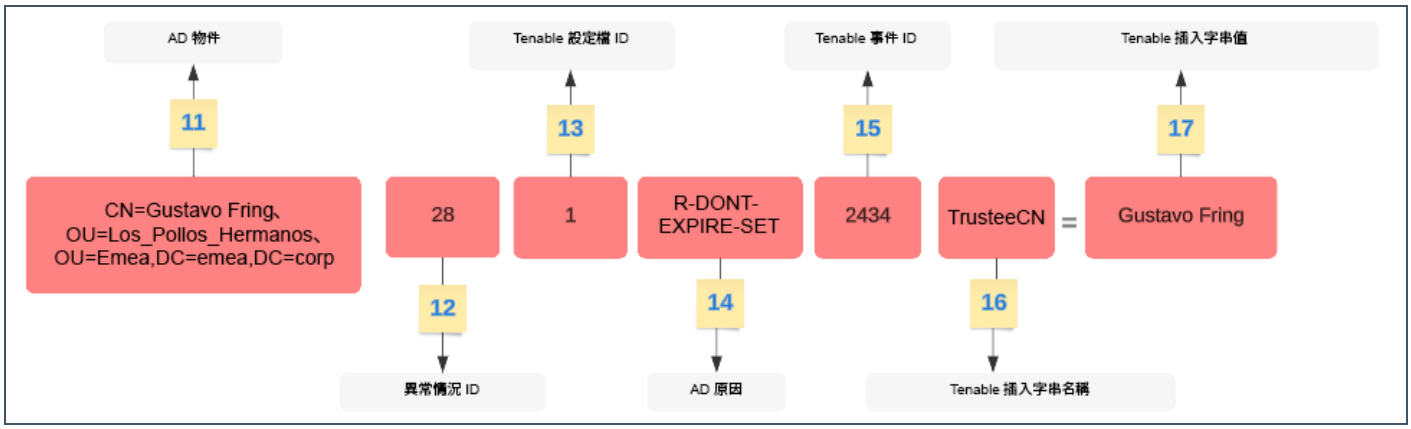


標頭結構包含下列部分，如表格中所述。

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)
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」

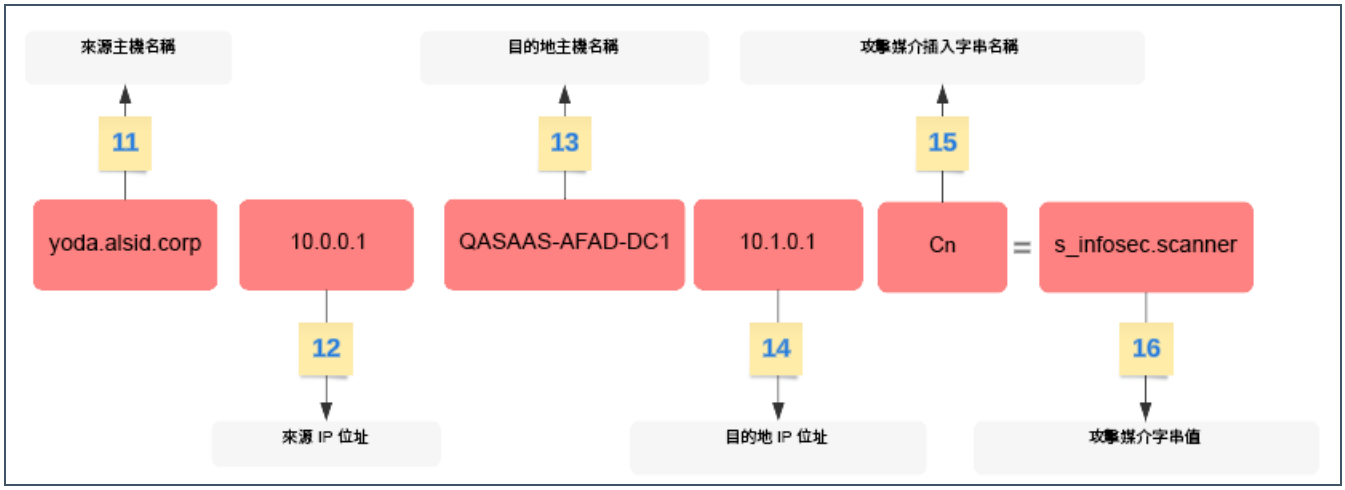
曝險指標 (IoE) 的特定元素



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。

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它。


系統設定
轉送管理
樹系管理
網域管理
租用戶管理
設定
關於
法律
應用程式服務
SMTP 伺服器
活動記錄
受信任的憑證授權單位
攻擊指標
Tenable 雲端
轉送
運作狀況檢查
6
電子郵件
5 個物件
新增電子郵件警示
ID
位址
嚴重性臨界值
網域
說明
4 khatase@tenable.com 低度 Japan Domain @ Alsid.corp
5 khatase@tenable.com 中等 Japan Domain @ Alsid.corp
9 kteo@tenable.com 中等 3 個網域
10 bmudie@tenable.com 中等 3 個網域
13 khatase@tenable.com 低度 2 個網域
1

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 網域資料和收集有權限的資料。
- 網域已連結至轉送：網域已正確關聯至轉送服務。

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。 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。

運作狀況檢查名稱	類型	檢查描述	原因
網域連線性	網域	可與 AD 網域連線	• IP-UNREACHABLE R-LDAP-GLOBAL-CATALOG-UNREACHABLE • LDAP-SERVER-UNREACHABLE • SMB-SERVER-UNREACHABLE • DYNAMIC-RPC-CONNECTION-NOT-WORKING

			• RPC-CONNECTION-NOT-WORKING
AD 網域驗證	網域	可在 AD 網域中進行驗證	• INCORRECT-CREDENTIALS • LDAP-SERVER-BUSY • LDAP-SERVER-UNAVAILABLE • LDAP-SERVER-ACCESS-DENIED • SMB-SERVER-ACCESS-DENIED
收集 AD 網域資料的權限	網域	可收集 AD 網域資料	• MISSING-PERMISSIONS-PRIVILEGED-DATA
存取 AD 容器的權限	網域	可存取 AD 容器	• MISSING-PERMISSIONS-DELETED-OBJECTS-ACCESS • MISSING-PERMISSIONS-PASSWORD-SETTINGS-ACCESS
網域已連結至轉送	網域	網域已連結至轉送	• LINKED-TO-RELAY-DOWN
轉送服務已啟動	平台	轉送目前正常運作	• RELAY-DOWN
轉送服務版本	平台	轉送版本與產品相符	• VERSION-MISMATCH
AD 資料收集器已啟動	平台	AD 資料收集器目前正常運作	• DATA-COLLECTOR-SERVICE-DOWN • DATA-COLLECTOR-BRIDGE-DOWN • BROKER-DOWN

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**」。

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。

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。

如要建立報告：

1. 在「**報告中心**」窗格中，按一下「**建立報告**」。

   「**報告設定**」窗格會隨即開啟。
2. 在「**報告類型**」下方完成下列資訊：
   a. 在「**報告類型**」中，選取「**異常情況**」或「**攻擊**」。
   b. 在「**指標**」中，按一下「**n/n 指標**」以選取「**曝險指標**」(針對異常情況)或「**攻擊指標**」(針對攻擊)」，然後按一下「**篩選選取的項目**」。
   c. 在「**網域**」中，按一下「**n/n 網域**」以選取報告的樹系或網域，然後按一下「**篩選選取的項目**」。
   d. 在「**設定檔**」中，按一下箭頭，然後從下拉式功能表中選取設定檔。

3. 在「**報告名稱**」中輸入報告的名稱。
4. 在「**產生參數**」下方選取下列設定：
   a. **資料時間範圍**：報告包含目前時間之前的期間，例如前一天、前一週、前一個月或前一季。
   b. **重複週期**：Tenable Identity Exposure 會針對您定義的每個時間範圍產生新報告：按一下箭頭，從下拉式功能表中選取對應的值。
   c. **時區**：與報告相關聯的時區。
5. 在「**接收者**」下方，按一下「**新增電子郵件**」，然後輸入收件者的電子郵件地址。您可以根據需要新增任意數量的收件者。

   如需瞭解如何設定報告收件者的電子郵件，請查看 SMTP 伺服器設定
6. 按一下「**建立報告**」。

如要允許使用者下載報告：

- 在「**報告中心**」窗格頂端的「**報告存取金鑰**」下方，按一下 以複製。必須使用此存取金鑰，才能從傳送給收件者的電子郵件中的連結下載報告。此存取金鑰針對所有使用者與報告皆是唯一的。
- 如有必要，請按一下 以產生新的存取金鑰。

  注意：產生新的存取金鑰後，先前的存取金鑰將無法使用。僅有新存取金鑰才能授予現有報告的存取權。

如要編輯報告設定：

1. 在報告清單中選取一個報告，然後按一下行尾的 以開啟「**報告設定**」窗格。
2. 視需要進行修改。
3. 按一下「**儲存**」。

如要刪除報告：

1. 在報告清單中選取一個報告，然後按一下行尾的 將其刪除。

   系統會顯示一則訊息，要求您確認刪除。

2. 按一下「**刪除**」。

   與此報告設定相關聯的最近產生報告不再可供下載。

如要授予角色權限：

- 在「**權限管理**」中的「**資料實體**」>「**報告**」下方，管理員可以向使用者角色授予建立、讀取或編輯所有或特定報告設定的權限。

  如需詳細資訊，請參閱設定角色的權限。

另請參閱

- 小工具

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

您必須擁有 **Tenable Vulnerability Management 帳戶**，才能使用 Microsoft Entra ID 支援功能。此帳戶可讓您為 Microsoft Entra ID 設定 Tenable 掃描，並收集這些掃描的結果。

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。

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」。

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。

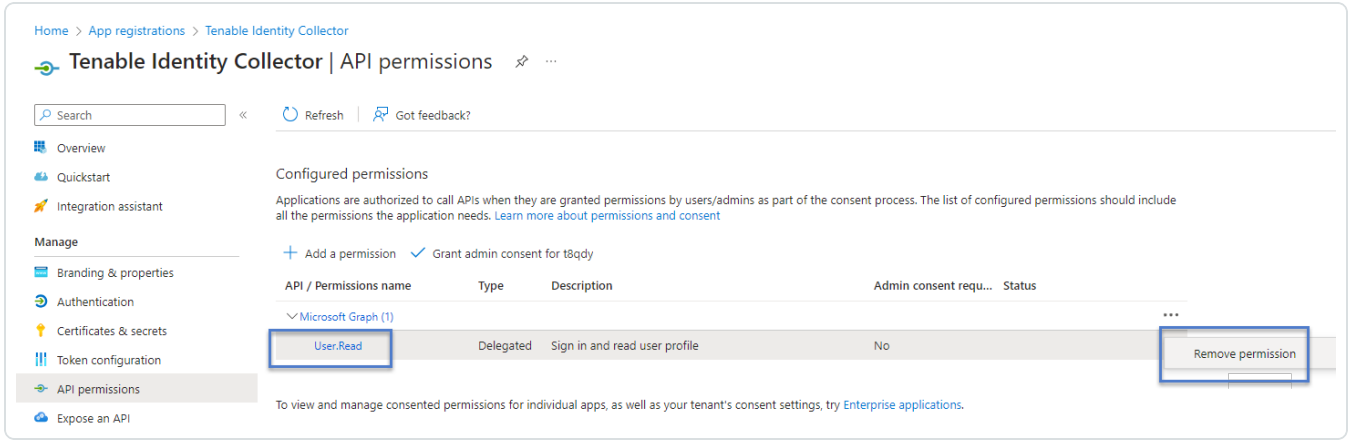
3. **指派權限給應用程式：**

   a. 在 Azure 管理入口網站中，開啟「應用程式註冊」頁面。

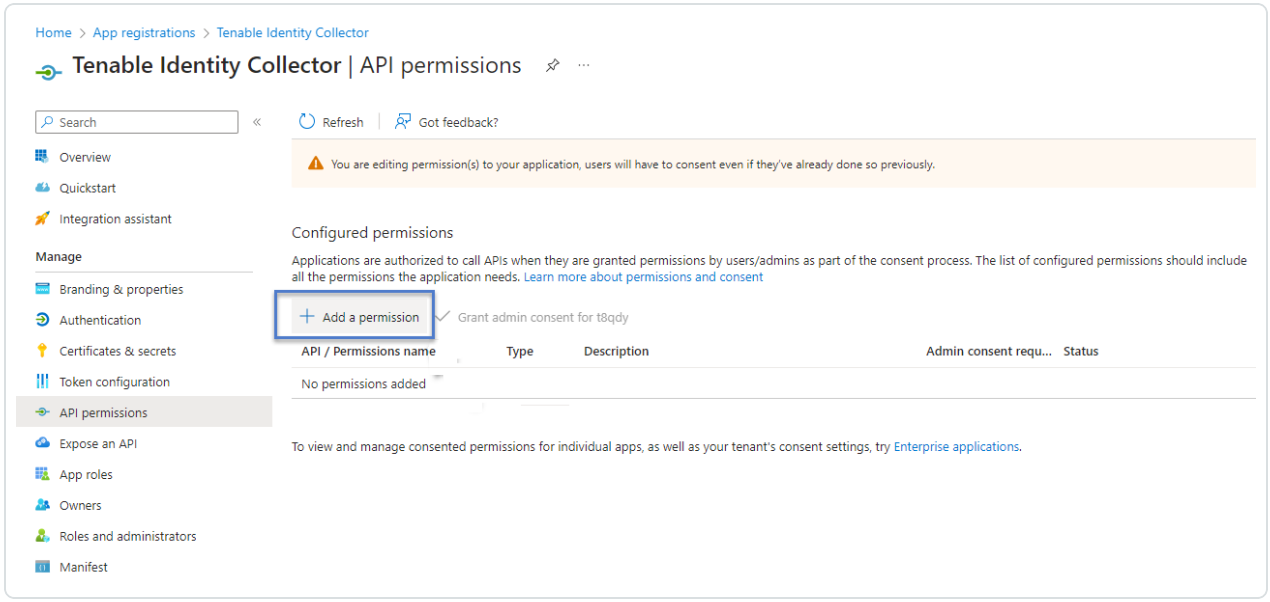
   b. 按一下您建立的應用程式。

   c. 在左側功能表中，按一下「**API 權限**」。

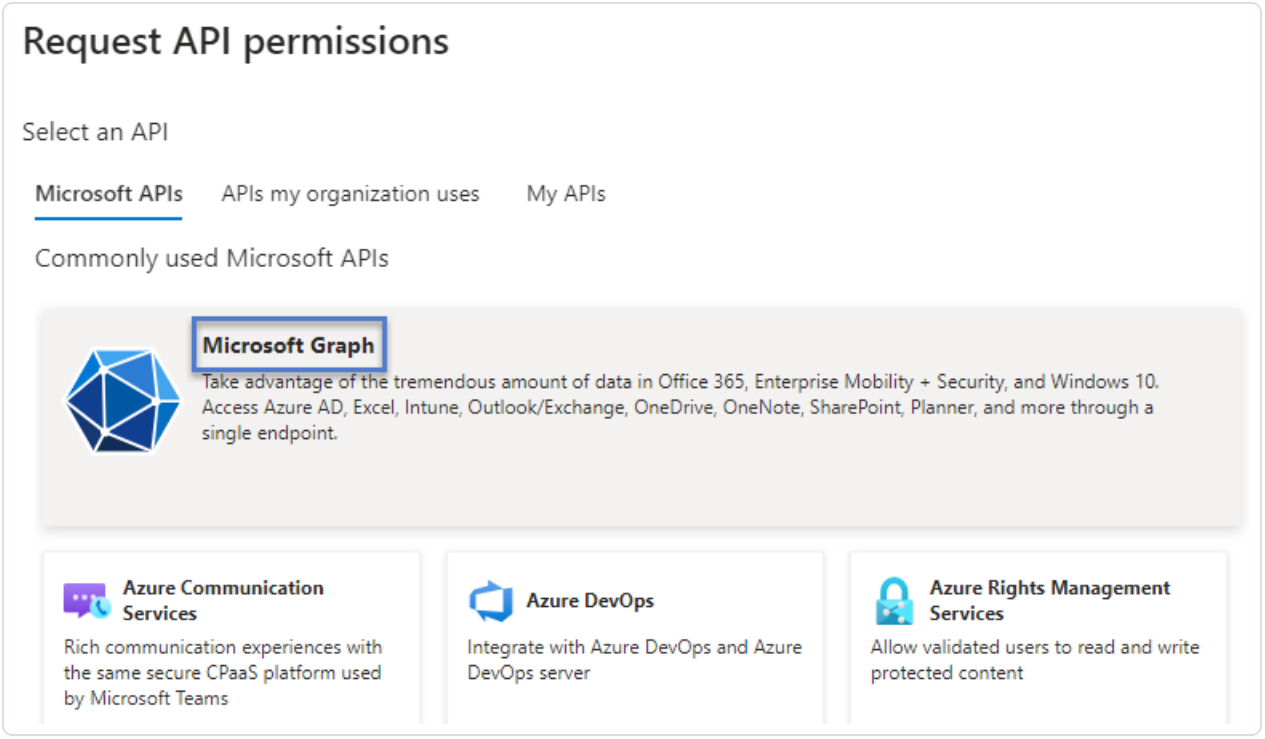
   d. 移除現有的 `User.Read` 權限：



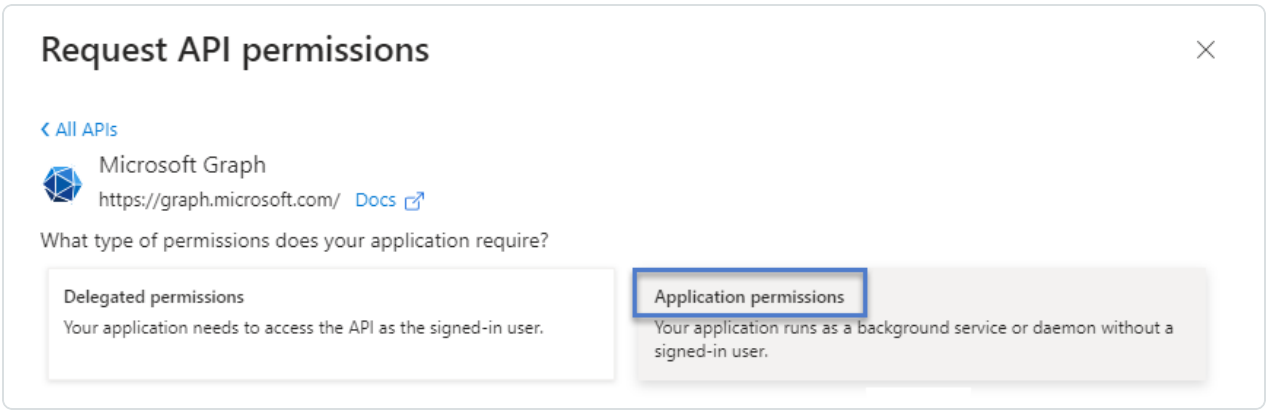
e. 按一下「**+ 新增權限**」：



f. 選取「**Microsoft Graph**」：



g. 選取「**應用程式權限**」(非「委派的權限」)。



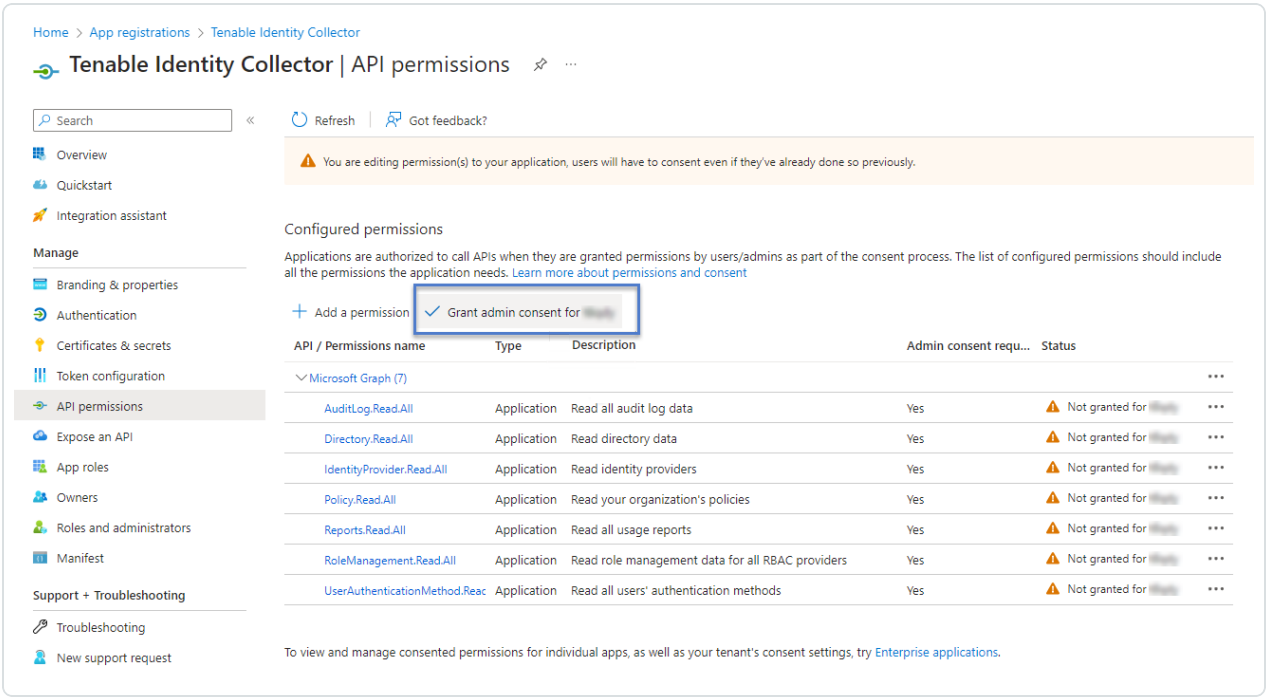
h. 使用清單或搜尋列，尋找並選取下列所有權限：

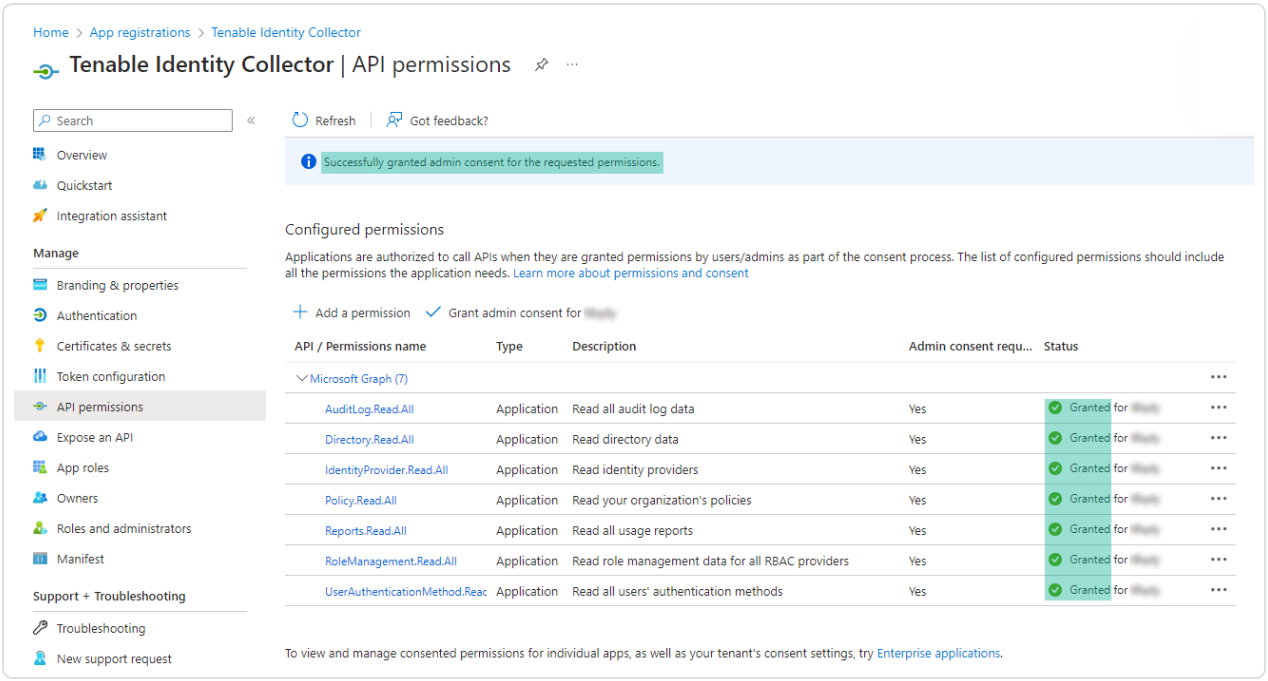
- `AuditLog.Read.All`
- `Directory.Read.All`
- `IdentityProvider.Read.All`
- `Policy.Read.All`
- `Reports.Read.All`

- `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

啟用支援的步驟如下：

注意：如要成功啟用此功能，已建立存取權和私密金鑰的 Tenable Cloud 使用者必須在 Tenable Identity Exposure 授權所引用的 Tenable Cloud 容器中擁有管理權限。如需詳細資訊，請參閱Tenable Identity Exposure 授權。

1. 在 Tenable Identity Exposure 中，按一下左側導覽列中的系統圖示  。
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 Microsoft Entra ID 支援**」中，按一下切換為啟用。
5. 如果您之前未曾登入 Tenable Cloud，請按一下連結前往登入頁面：

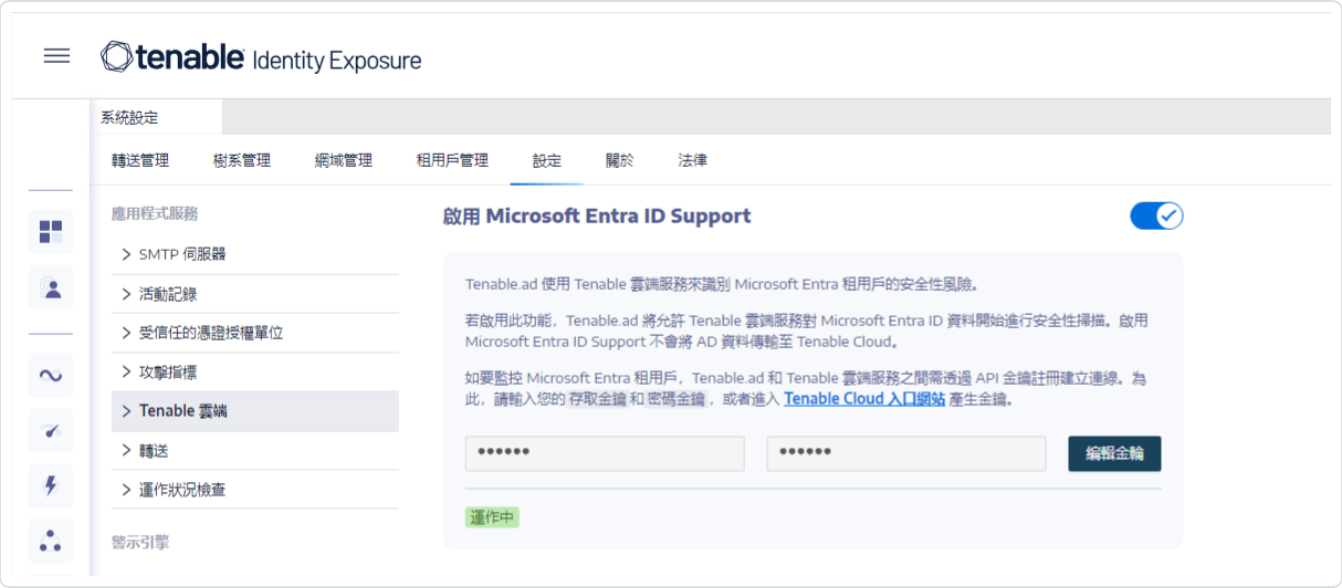
    a. 按一下「**忘記密碼?**」以要求重設密碼。

    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。

啟用租用戶掃描

新增租用戶的步驟如下：

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。

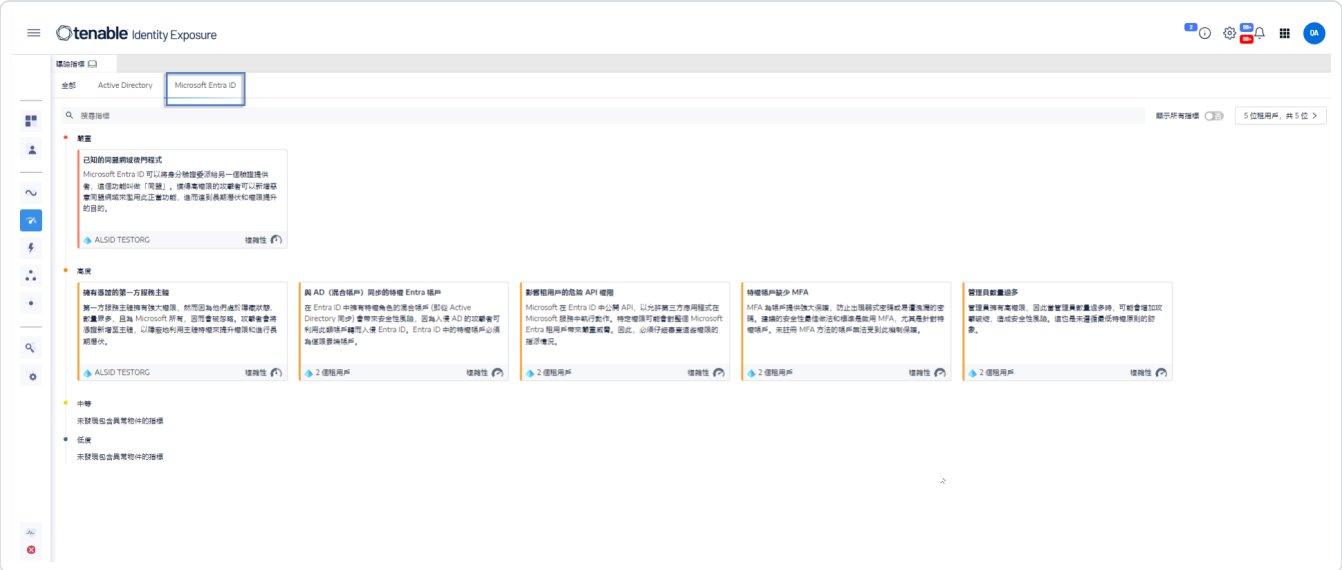
針對租用戶啟用掃描：

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**。



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云端，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 Cloud 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)。

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。

除了在 SAAS-VPN 平台中主控其轉送的用戶端外，密碼永遠不會離開用戶端的基礎架構，因為只有轉送會處理這些密碼。轉送不會儲存密碼，而是會在每次需要分析時擷取使用者的密碼，將其暫時保留在快取中，通常只有幾毫秒。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」**。

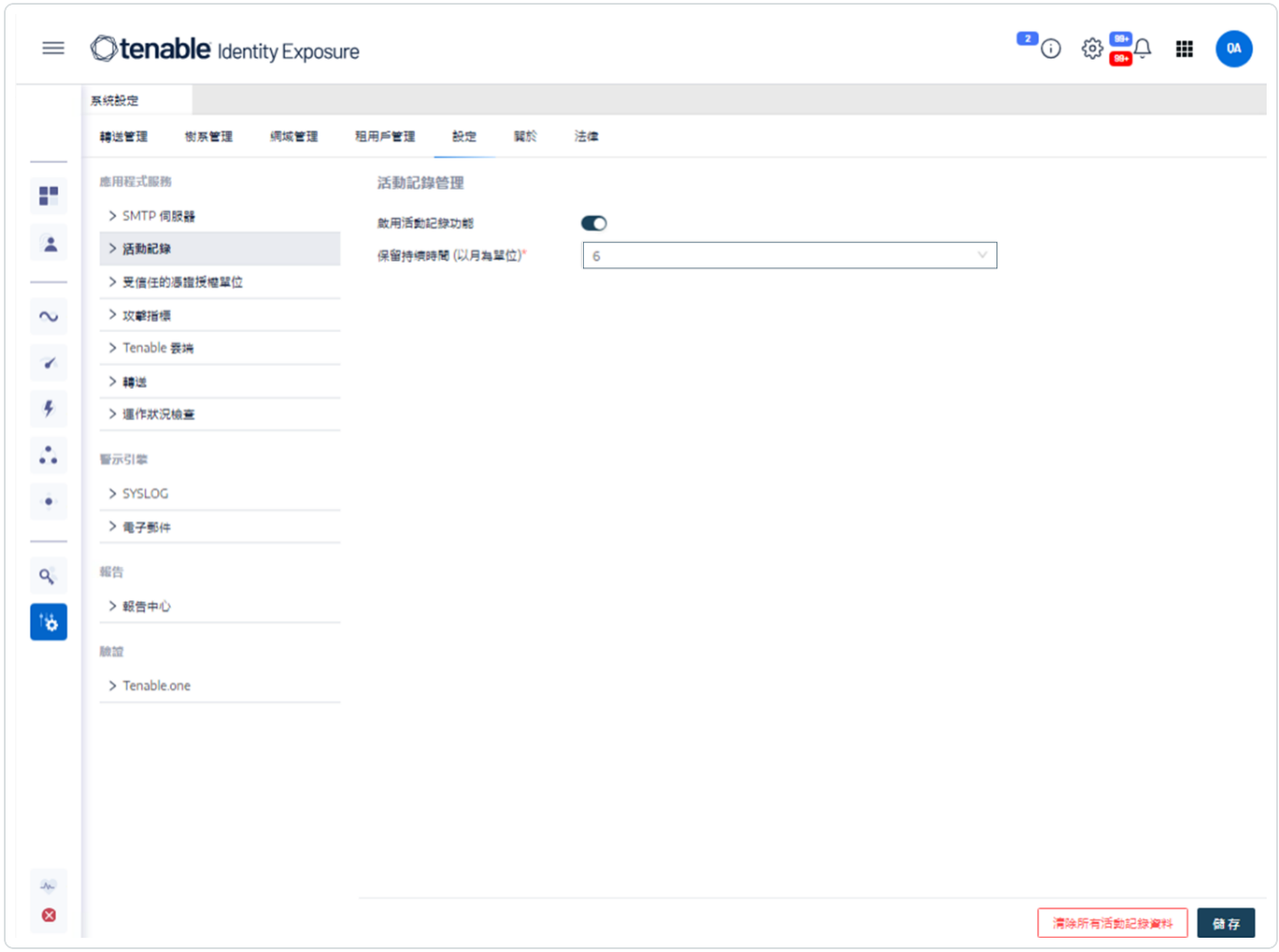
   「活動記錄管理」窗格會隨即開啟。

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。

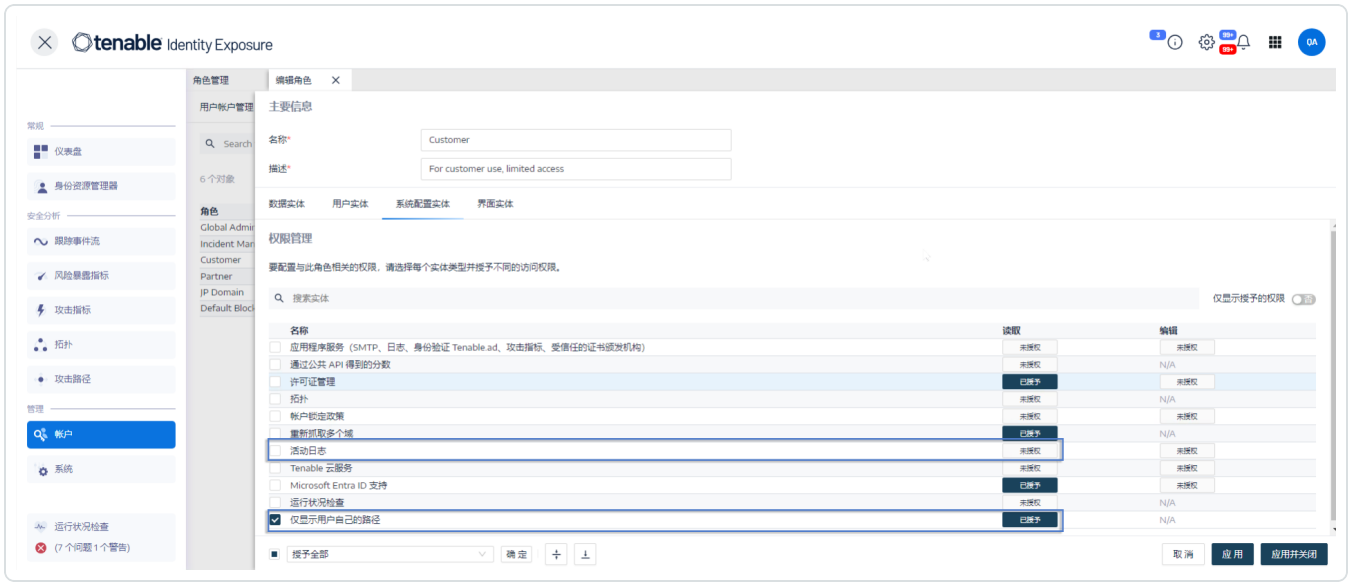
4. 在「**主要資訊**」區段下，選取「**系統設定實體**」索引標籤。

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。



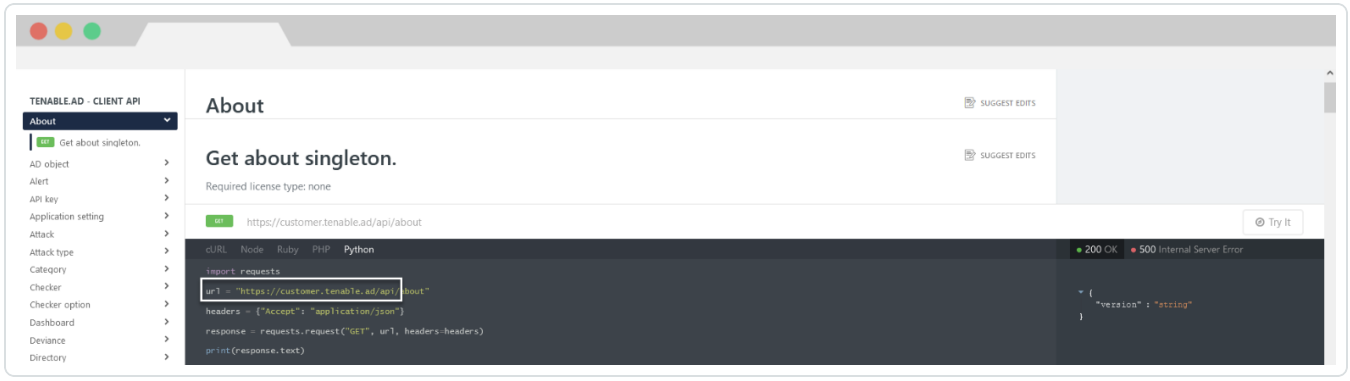
Tenable Identity Exposure 公用 API

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。

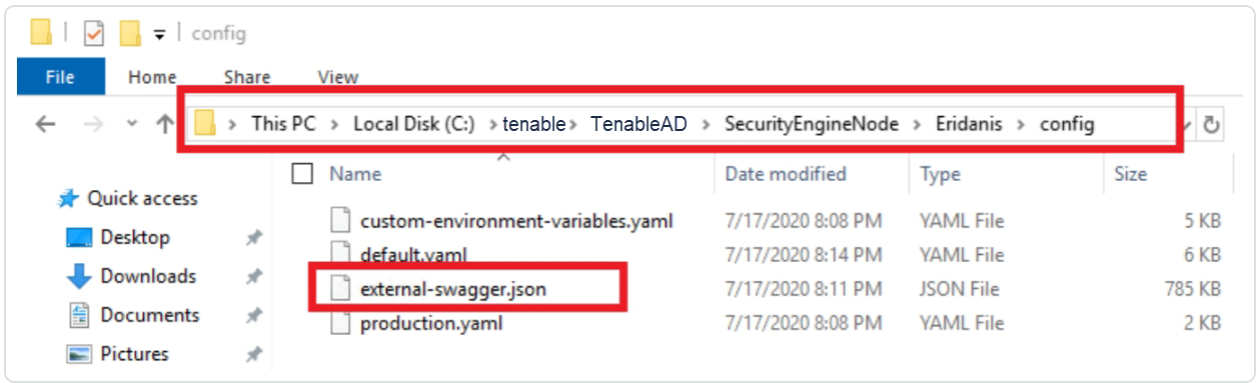
如要存取 Tenable Identity Exposure 執行個體的 API:

- 在瀏覽器中開啟此 URL:



如要下載 OpenAPI 檔案:

- 對於內部部署安裝,請遵循此安全性引擎節點的路徑:



- 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 圖示。

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 會將資料保留 6 個月。此資料管理期間不可設定。

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。如果想瞭解如何使用 Tenable Identity Exposure，請參閱《Tenable Identity Exposure 使用者指南》。

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。

Tenable Identity Exposure 元件

Tenable Identity Exposure 的兩個版本皆隨附下列元件：

- 追蹤流程檢視
- 拓撲檢視
- 曝險指標

- 攻擊指標
- 攻擊路徑
- 身分識別總管
- 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，但如果您掃描的資產數量超過授權配額，Tenable 會明確告知超額量，然後分三個階段限制功能。

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。
您已經有 45 天以上啟用超過授權配額的身分	Tenable Identity Exposure 中會顯示一則訊息；匯出功能會無法使用。

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。

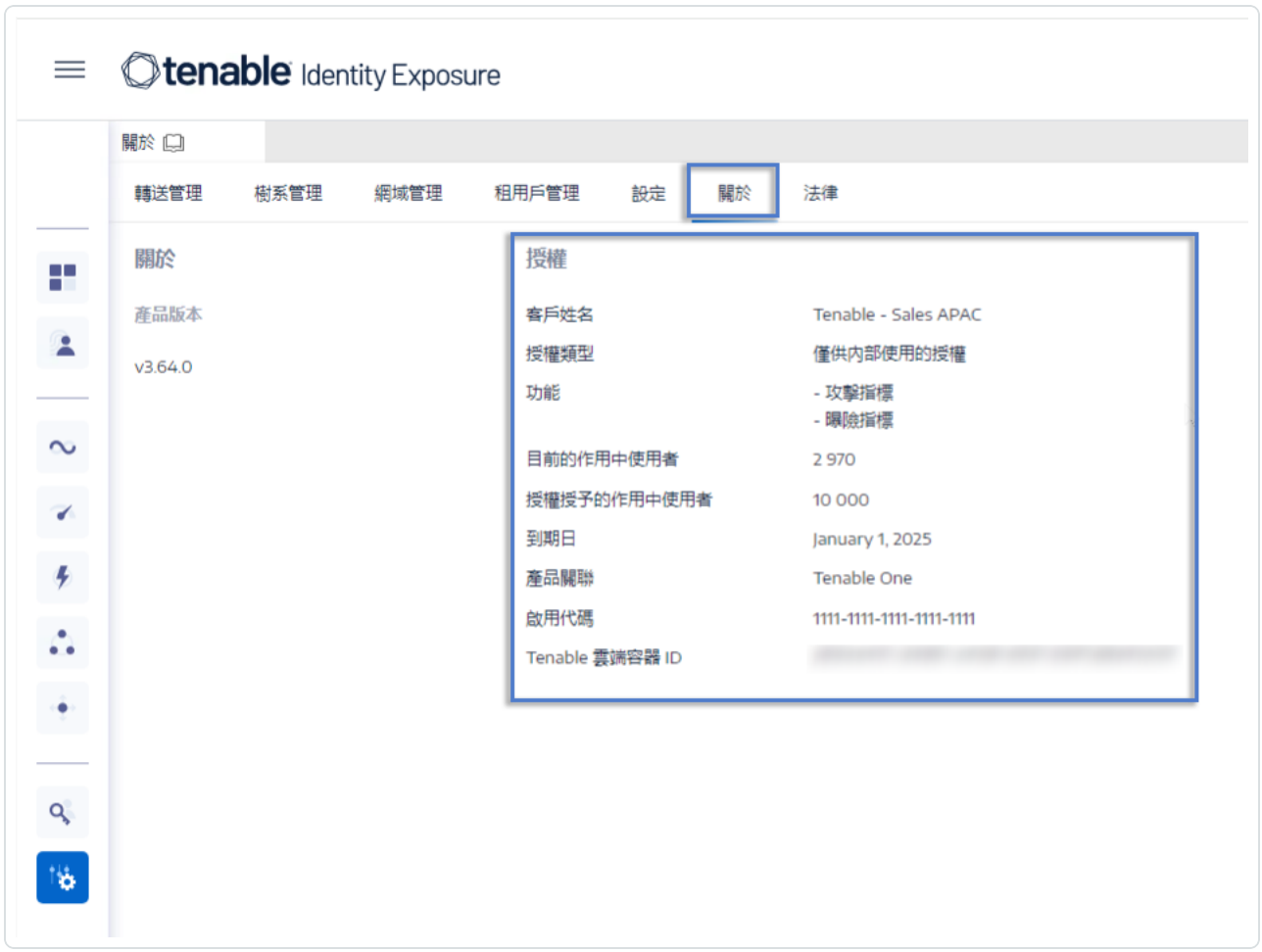
Tenable Identity Exposure 授權可能包含：

- 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

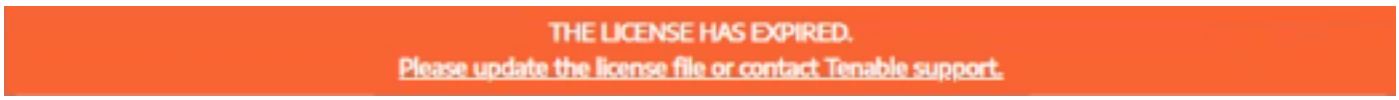
若是內部部署安裝，如果有可用的網際網路連線，Tenable Identity Exposure 會追蹤授權使用情況。

授權有效性

只要您符合下列條件，Tenable Identity Exposure 授權便保持有效：

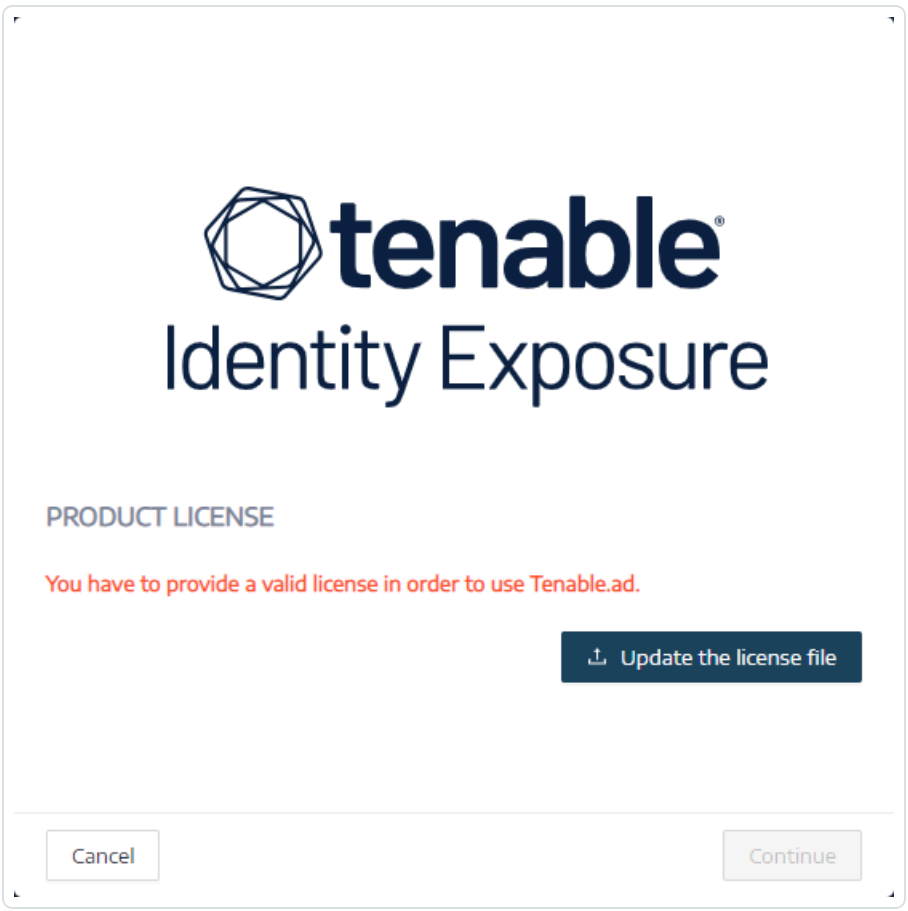
- 使用者數量不超過授權授予的數量。
- 未過到期日。

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：



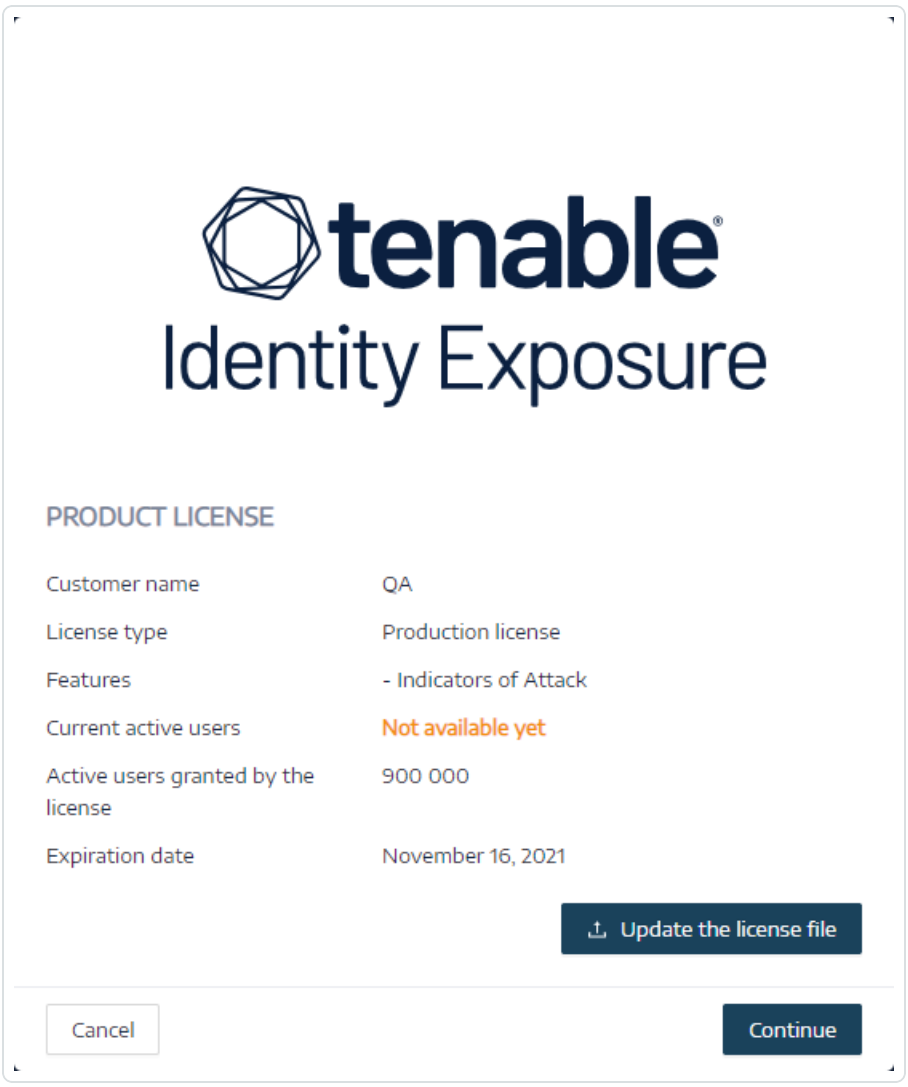
如要上傳授權檔案：

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。

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：

- Tenable Identity Exposure 診斷工具
- SYSVOL 強化干擾 Tenable Identity Exposure

Tenable Identity Exposure 診斷工具

Tenable Identity Exposure 提供的診斷工具可協助您擷取與 Tenable Identity Exposure 安裝相關的記錄資訊，以便客戶支援人員分析並協助您解決任何問題。

您可以從 Tenable 下載入口網站下載此診斷工具。

注意：此診斷工具僅適用於 Tenable Identity Exposure 的**內部部署安裝**。

診斷工具可執行下列動作：

- 判斷目前電腦（您啟動可執行檔的位置）是否託管了儲存管理員 (SM)、安全引擎節點 (SEN) 或目錄接聽程式 (DL)。
- 掃描環境以尋找您網路上可用的其他 Tenable Identity Exposure 安裝。
- 偵測與您的 Tenable Identity Exposure 安裝相關的記錄來源清單，以據此測試和擷取其相關資訊。
- 擷取關於 Tenable Identity Exposure 安裝嘗試失敗的 MSI 記錄。

取得最佳結果的訣竅

- 在 SEN 上執行診斷工具。
- 以提升的使用者權限執行診斷工具，來啟動大部分的或所有記錄來源。
- 若要偵測 SM 或其他安裝，請檢查您是否符合下列條件：
  - 設定允許在遠端電腦上執行遠端命令 (Invoke-Command cmdlet)。
  - 設定允許遠端存取磁碟。
  - WMI 已啟用且目前的使用者帳戶允許使用。

如要執行診斷工具：

1. 從 Tenable 下載入口網站下載檔案 `TenableAdDiagnosticTool.OnPrem.Console.exe`。
2. 在 Tenable Identity Exposure 電腦上以管理員身分執行可執行檔，建議在託管 SEN 的電腦上執行。
3. 出現提示時，輸入下列其中一個選項：

- `E`:所有記錄 (預設選項)
- `Msi`:與 Tenable Identity Exposure 安裝相關的記錄
- `Tenable`:與 Tenable Identity Exposure 相關的記錄

4. 按 Enter 鍵。

   診斷工具會掃描您的安裝。掃描完成時,產生的輸出會以壓縮檔案形式儲存在您目前的目錄中。

5. 將此壓縮檔案傳送給 Tenable Identity Exposure 客戶支援人員。請勿以任何方式更改檔案內容。

如要使用命令列執行診斷工具:

1. 在命令列中,在 Tenable Identity Exposure 電腦上以管理員身分執行可執行檔 `TenableAdDiagnosticTool.OnPrem.Console.exe`,建議在託管 SEN 的電腦上執行。

   診斷工具會掃描您的安裝。掃描完成時,產生的輸出會以壓縮檔案形式儲存在您目前的目錄中。

2. 將此壓縮檔案傳送給 Tenable Identity Exposure 客戶支援人員。請勿以任何方式更改檔案內容。

其他選項

診斷工具也提供下列使用命令列的選項:

- `-- help`:關於診斷工具用法的簡短描述。
- `-- commands`:用於測試電腦功能和掃描其他安裝的 Powershell / WMI 查詢清單。

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

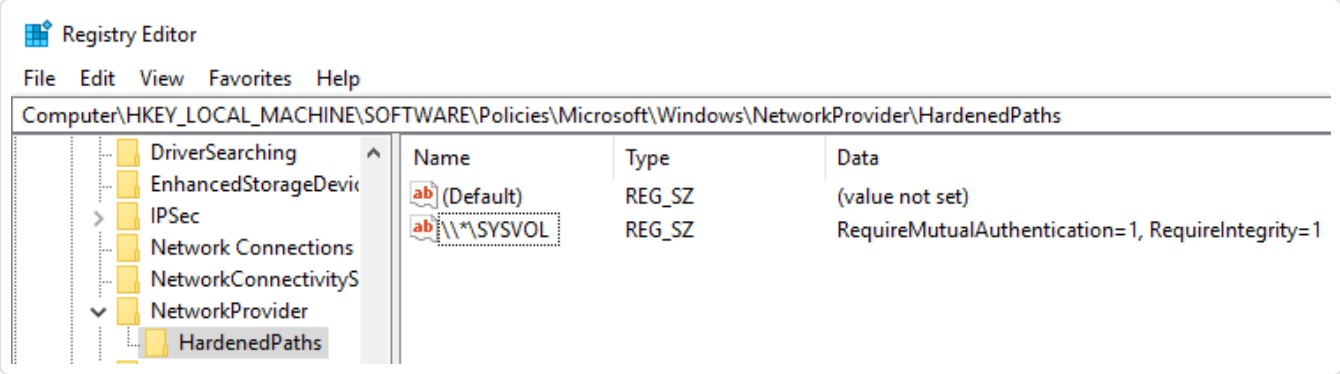
SYSVOL 強化是一個用戶端參數，表示它是在連線至 SYSVOL 共用的電腦上運作，而非在網域控制器上運作。

Windows 會依預設啟用此參數，但可能會干擾 Tenable Identity Exposure。

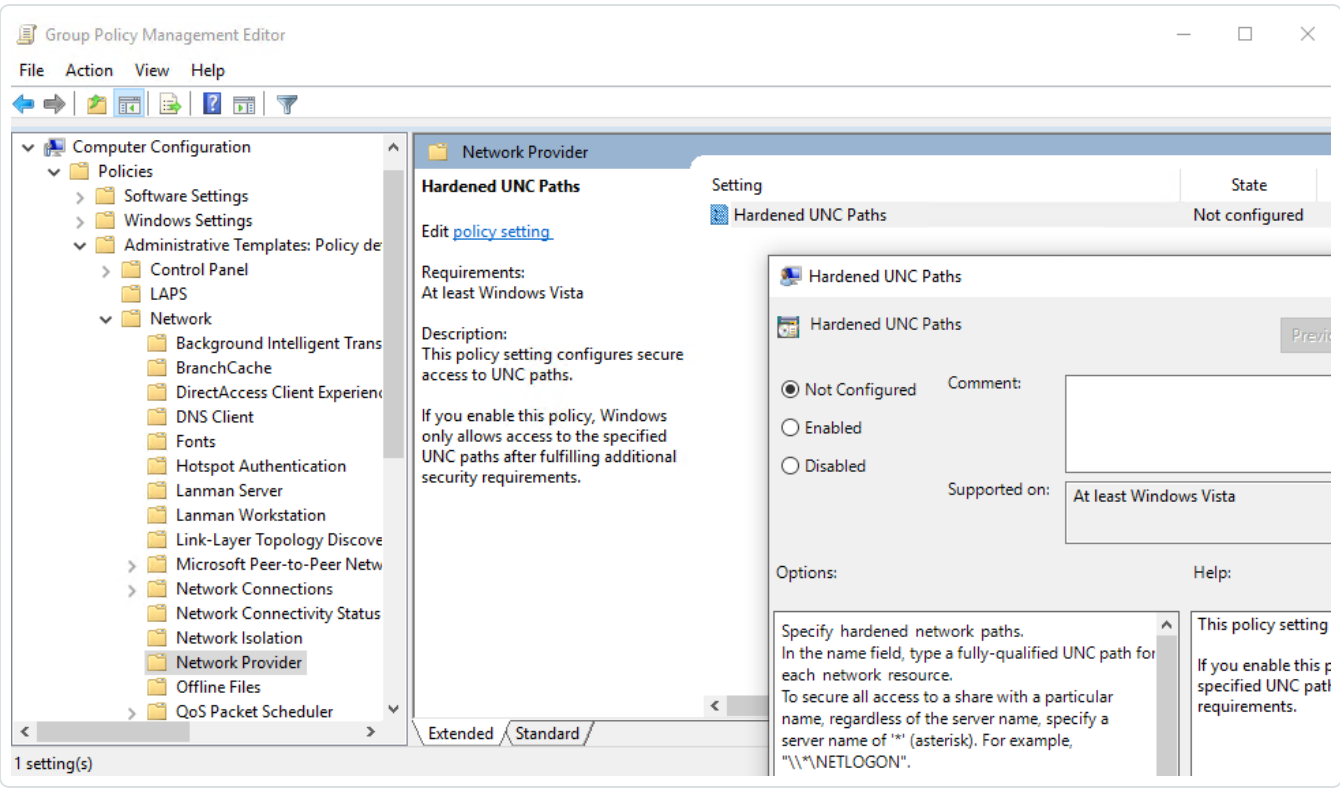
有些組織也希望確保啟用此參數，並透過使用相關的 GPO 設定或直接設定對應的登錄機碼來強制執行此參數。

- 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：



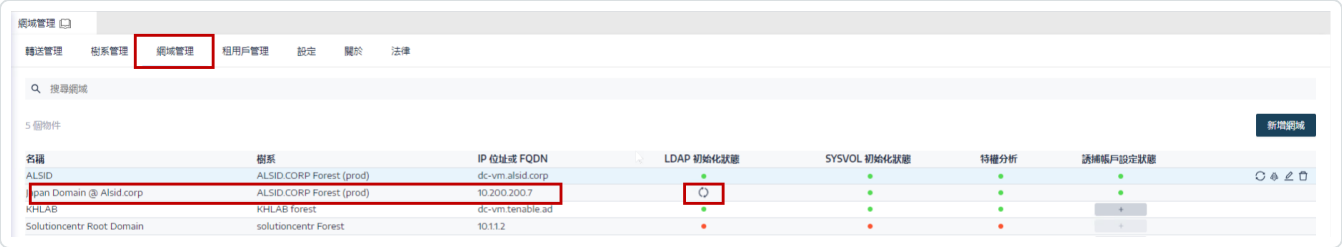
當參照 SYSVOL 的 UNC 路徑 (例如「*\SYSVOL」) 將參數「RequireMutualAuthentication」和「RequireIntegrity」的值設定為「1」時，就會發生 SYSVOL 強化強制執行。

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：

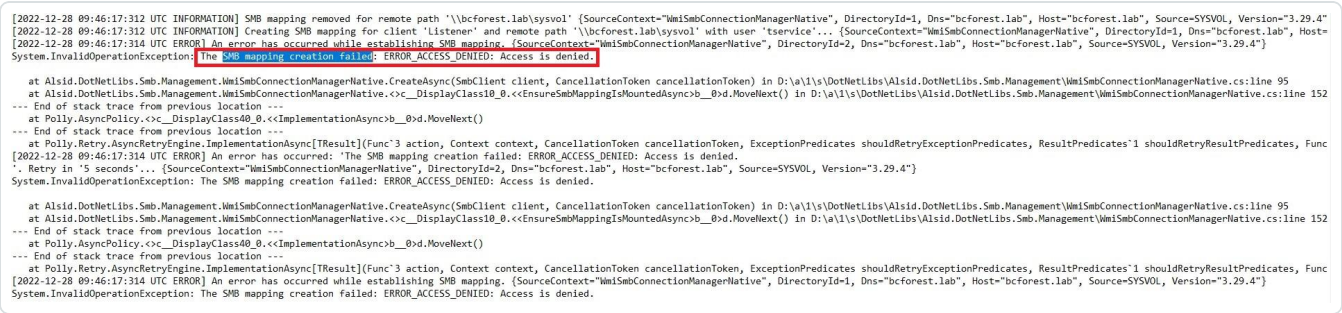
1. 在 Tenable Identity Exposure 中，前往「**系統**」>「**網域管理**」，查看每個網域的 LDAP 和 SYSVOL 初始化狀態。

   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。

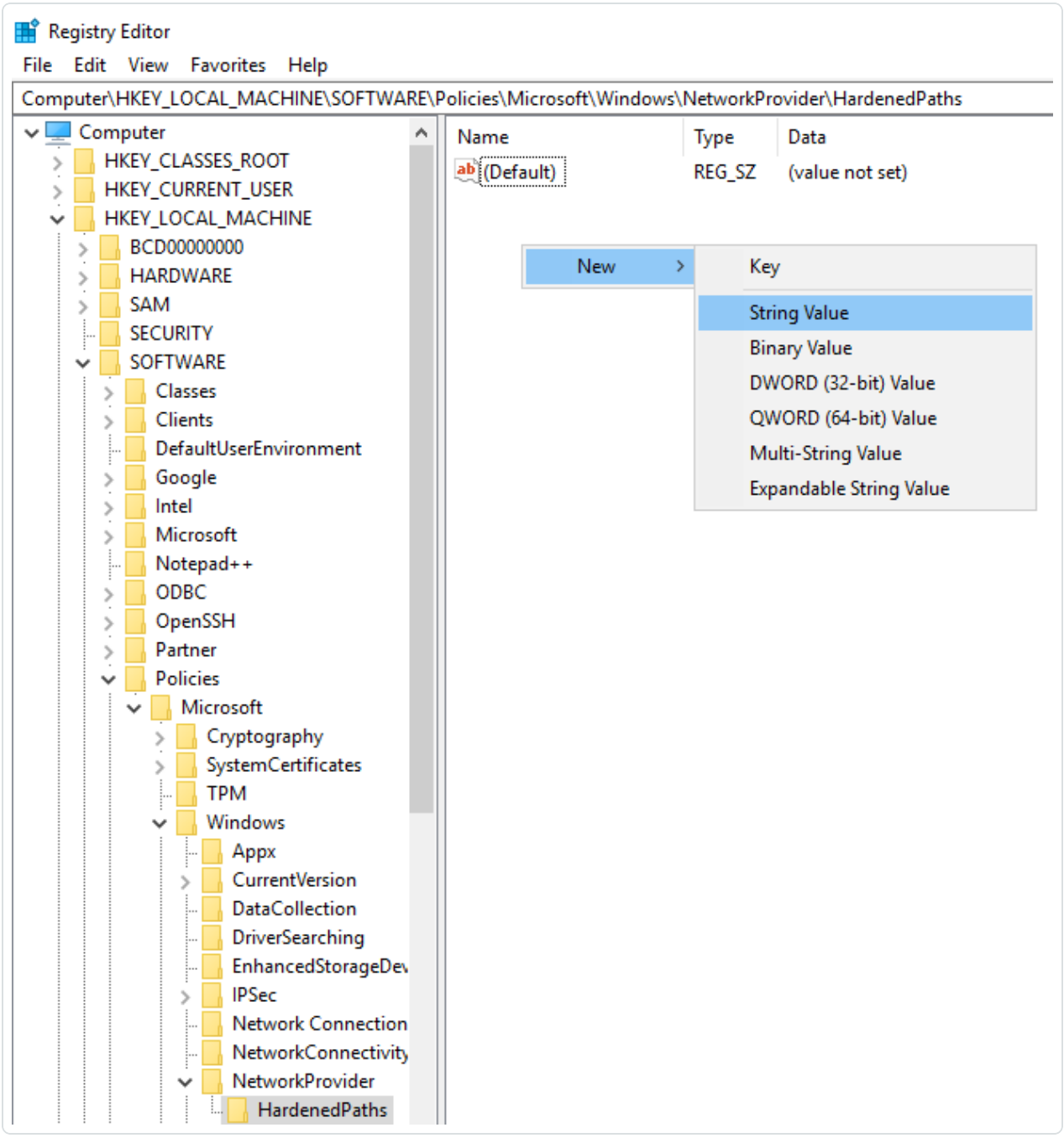
在您重新啟動目錄接聽程式或轉送電腦之後，修改後網域上的抓取指示器應變成綠色指示器：

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**」。

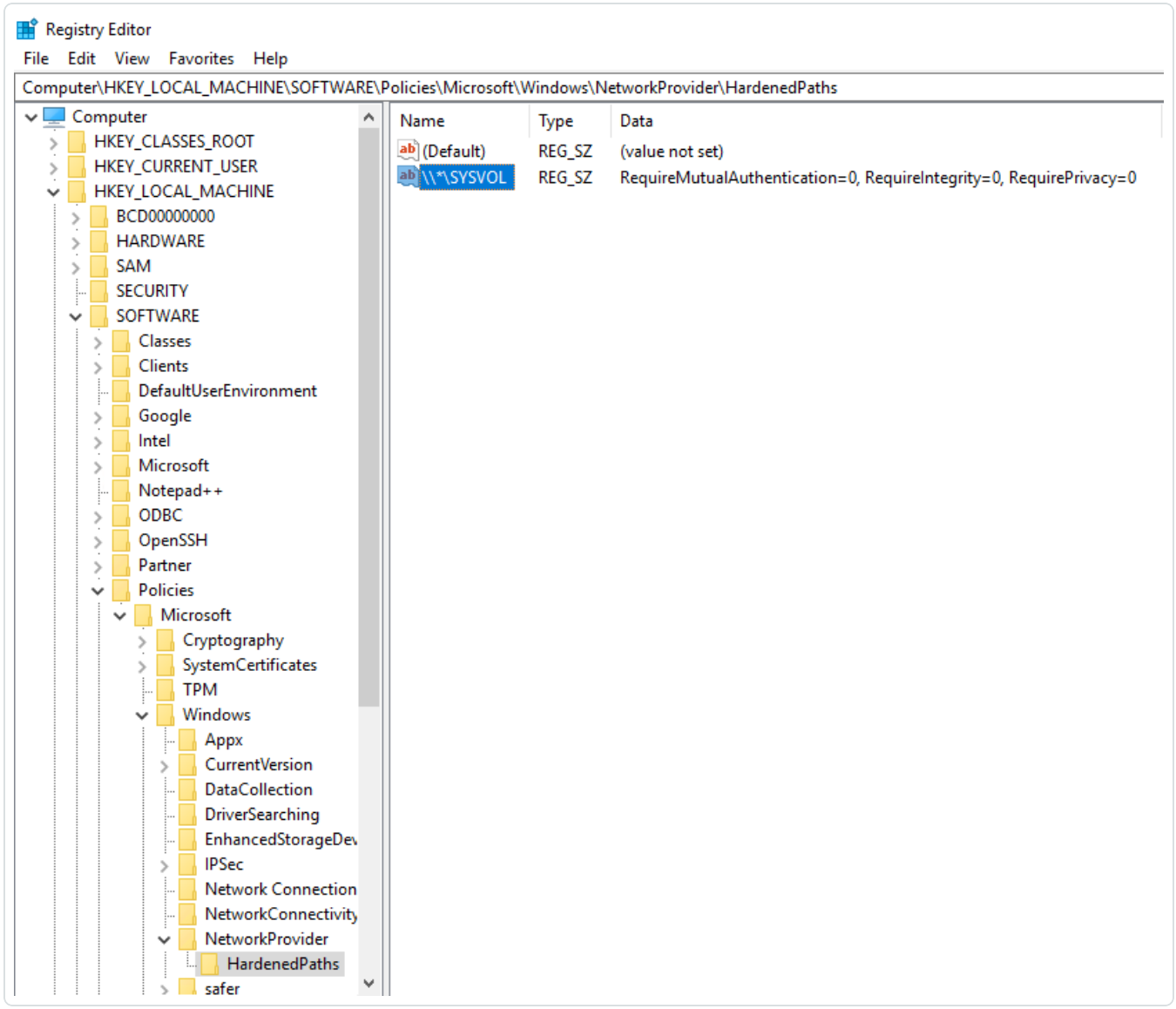


b. 在「名稱」欄位中，輸入 `\\*\SYSVOL`。

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。

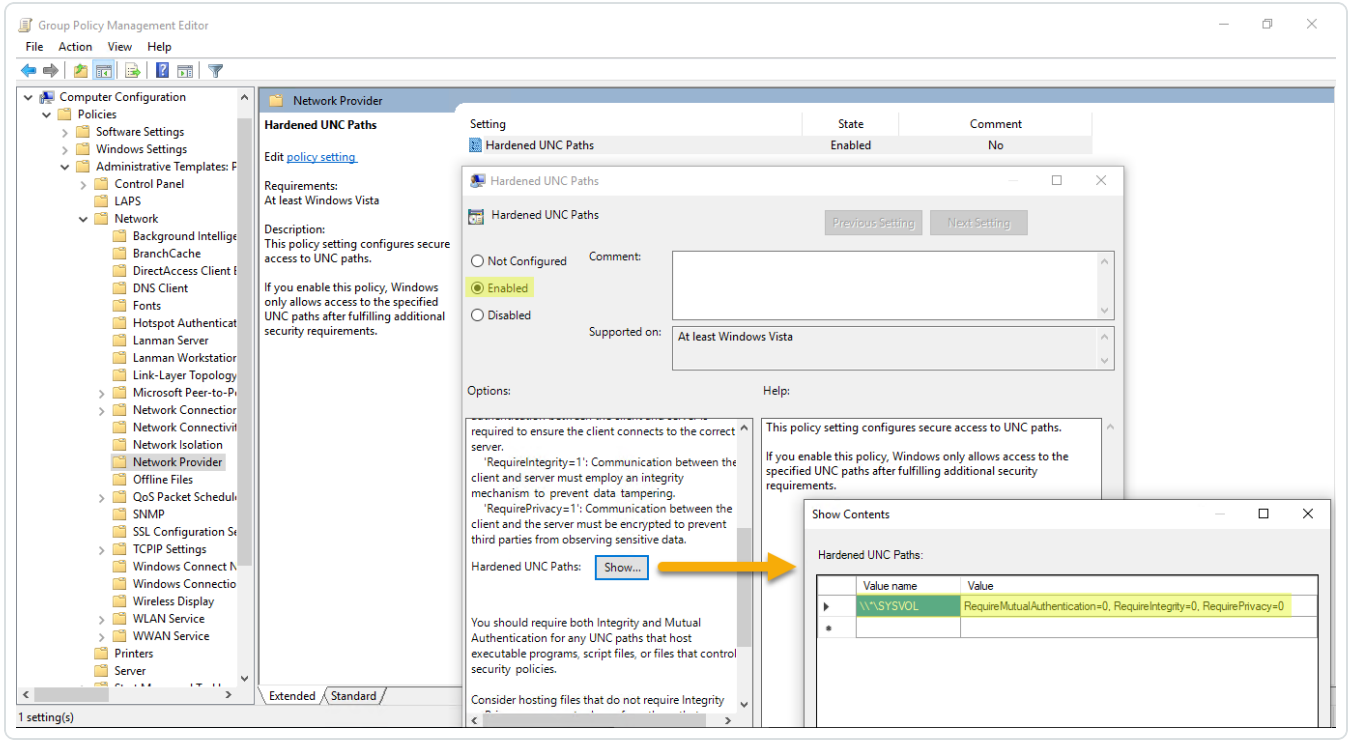
GPO

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：

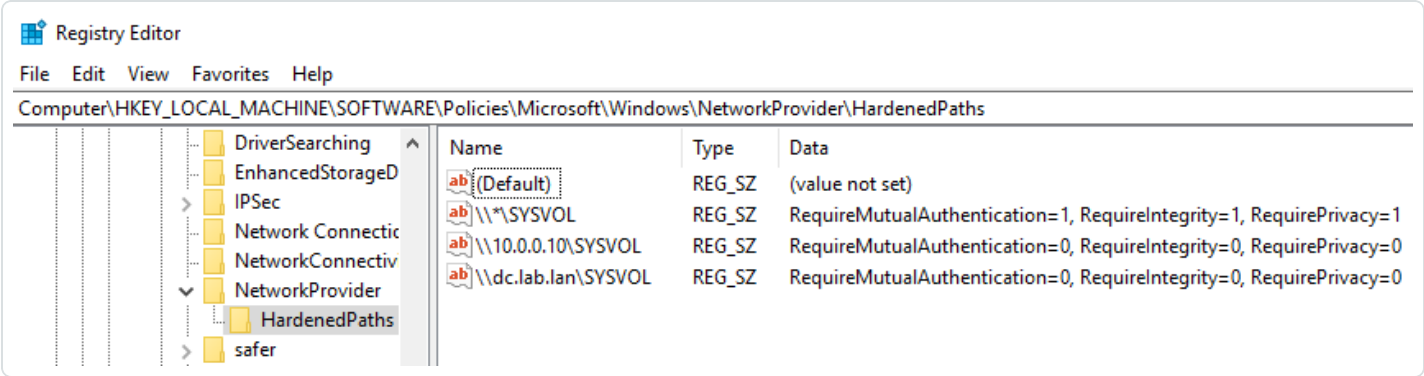


5. 按一下「**確認**」。
6. 將此 GPO 連結至包含 Tenable Identity Exposure 目錄接聽程式或轉送電腦的組織單位。您也可以使用安全性群組篩選 GPO 功能，確保此 GPO 僅適用於此電腦。

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。