Tenable Identity Exposure 主要功能指南

上次修訂時間：2025 年 7 月 2 日

目錄

歡迎使用 Tenable Identity Exposure 主要功能指南

歡迎使用 Tenable Identity Exposure (前稱 Tenable AD)。本文件旨在透過提供產品特性和功能的全面概覽來增強您的體驗，無論產品是在內部部署還是透過 SAAS 部署。此資源的目的在於為您提供協助，無論您是尋求指導的新使用者，還是想要深化了解的有經驗的使用者。

本文件包含多個章節，內容涵蓋各種主題，比如如何最佳化產品使用和如何管理攻擊指標和曝險指標。請務必注意，雖然本文件提供了寶貴的見解，但其並非作為 Tenable Identity Exposure 使用的嚴格規範。相反，本文件提供一系列建議，幫助您流暢且高效率地利用此平台。

關於本指南

本指南根據 **Tenable Identity Exposure SaaS 使用者指南**編寫，建議您參閱該使用者指南，當中提供詳盡的資訊。

本指南中所列舉的例子旨在醒目提示 Tenable Identity Exposure 功能，但並不構成詳盡的功能清單，並且可能無法直接適用於每個獨特的環境。為獲得最佳安全性措施，我們建議您造訪我們的官方說明文件或專業服務，以獲得更多詳細資料和指引。

主要利害關係人

Tenable Identity Exposure 中的各個利害關係人會根據貴組織的規模、結構、安全性原則和預定的使用案例而有所不同。為每個利害關係人建立確切的角色和責任，能促進產品的有效採用與利用。

使用 Tenable Identity Exposure 時，務必了解涉及的不同利害關係人。這些個人和群組在識別、緩解以及報告身分型安全風險方面擔任不同的角色。以下是詳細分類：

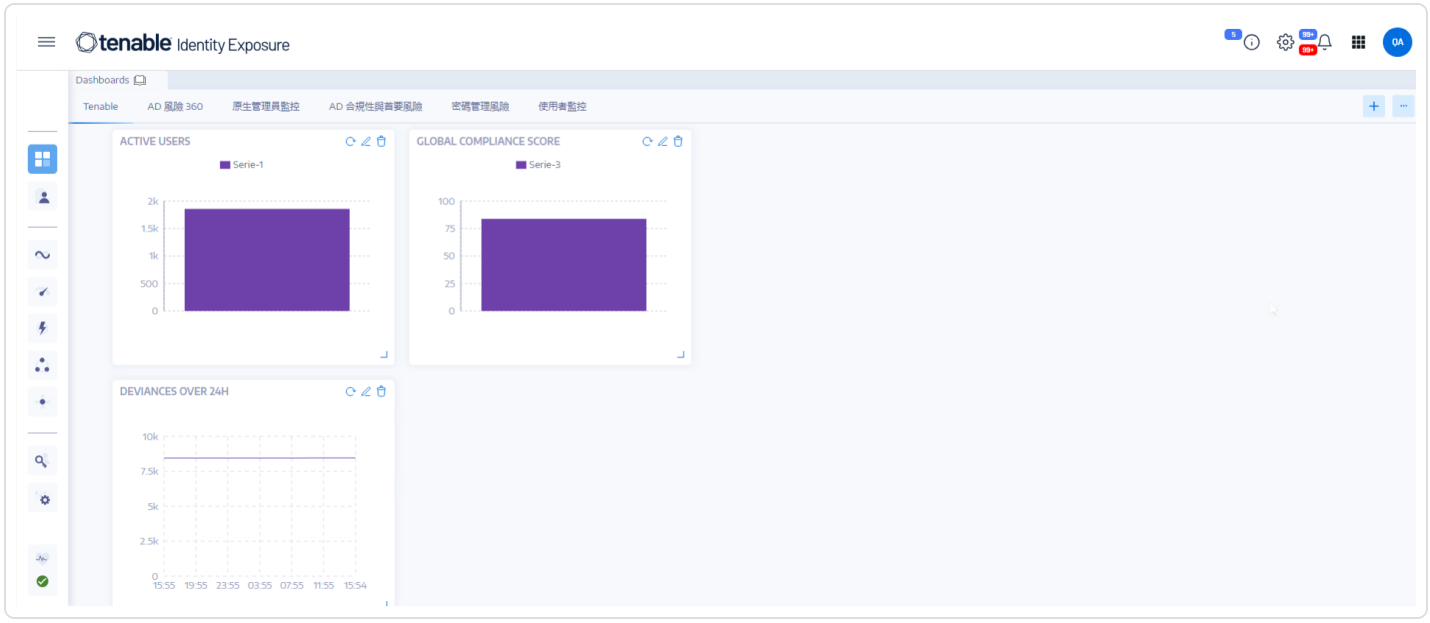
- **安全團隊**：監督與管理 Tenable 解決方案，利用資料分析及時識別弱點和風險並做出應變。
- **IT 營運團隊**：負責為 Tenable 解決方案提供基礎架構和整合支援，確保與其他安全性工具和使用者目錄流暢連線。
- **應用程式開發團隊**：負責保護應用程式的安全，並立即解決 Tenable 所標記的任何洩漏身分。

- **身分和存取管理** (IAM) 團隊：管理使用者帳戶、權限和存取控制，並與 IT 安全團隊密切合作，解決 Tenable Identity Exposure 所發現的問題。
- **業務單位主管**：對其團隊和應用程式的安全狀況負有最終責任。他們負責檢閱報告、排定風險緩解策略的優先順序，並分配資源以增強 Active Directory 安全性措施。

儀表板

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

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



儀表板主要功能

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

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

另請參閱

- 儀表板
- 儀表板教學影片

追蹤流程

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

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

追蹤流程會追蹤下列事件：

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

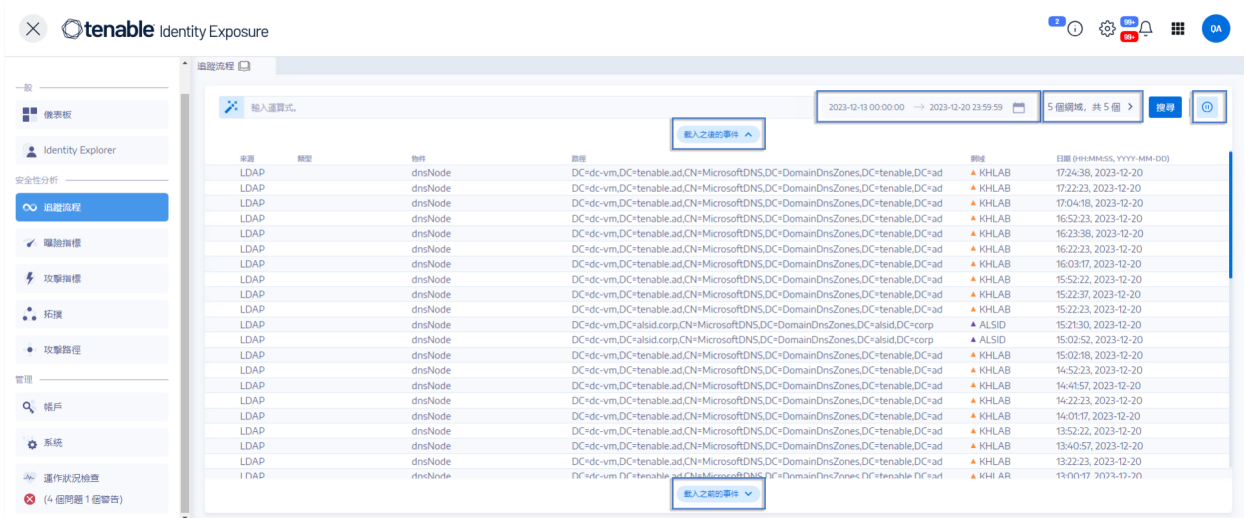
Tenable Identity Exposure 提供以下功能，可用於有效運用追蹤流程資料：

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

如要存取追蹤流程：

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

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



如要選取時間範圍：

如要選取網域：

如要檢視事件：

如要暫停和重新啟動追蹤流程：

如要載入之後或之前的事件：

資料在追蹤流程中如何顯示？

1. 當您在 Active Directory (AD) 介面中執行動作，例如：
    - 建立新使用者帳戶
    - 修改使用者的群組成員資格
    - 重設密碼
    - 停用帳戶
    - 啟用帳戶
    - 刪除帳戶

- 移動物件
- 修改權限

2. Active Directory (AD) 會自動產生事件記錄項目，以擷取操作的詳細資料，包括：
    - 時間戳記
    - 執行動作的系統管理員
    - 受影響的物件
    - 具體變更
3. Tenable Identity Exposure 會持續收集並分析這些事件記錄、關聯事件、識別模式，同時偵測異常情況。
4. 追蹤流程頁面會將操作的流程和影響視覺化：
    - 時間軸：依時間先後順序顯示事件序列，並醒目提示近期的操作。
    - 物件詳細資料：提供有關受影響物件的屬性和關係等特定資訊。
    - 變更歷史記錄：顯示物件修改歷史記錄，包括目前操作。
    - 風險深入解析：識別與操作相關的潛在風險，例如過高特權或是敏感群組中的成員資格。
    - 合規性資訊：指出與操作相關的任何違規行為。

另請參閱

- 追蹤流程 概覽
- Trail Flow Use Cases
- 追蹤流程教學影片

報告中心

Tenable Identity Exposure 中的**報告中心**是一項非常重要的功能，可協助您將重要資料匯出成報告給組織內的主要利害關係人。報告中心提供使用預定義清單建立報告的方法，確保流程有效率且精簡。

所提供的功能如下：

- **精細篩選**：使用日期範圍、網域、攻擊指標 (IoA)、曝險指標 (IoE) 等條件的精細篩選器，讓報告完善精簡，以確保專心進行深入分析。
- **自動傳送**：排定自動產生報告，並依照所需的頻率傳送，簡化安全監控和報告程序。
- **彈性匯出**：匯出 CSV 等多種格式的報告，以便進一步分析、共用報告存取金鑰，或與現有報告工作流程整合。

系統管理員可針對不同使用者建立不同類型的報告，且報告時間範圍可彈性調整，最高為一季。組織如果能夠從 Tenable Identity Exposure 共用重要身分識別資料，就可以主動減輕風險，並發現潛在的身分識別型攻擊。

若要下載報告，使用者會收到一封包含頁面 URL 的電子郵件，使用者需要在此頁面中輸入他們從管理員處收到的報告存取金鑰。使用者可在 30 天內下載報告，超過 30 天後報告便會過期，Tenable Identity Exposure 會將之刪除。只有待使用者下載報告後，Tenable Identity Exposure 才能針對指定的時間範圍產生新的報告並覆寫先前的報告。

如要存取報告中心：

1. 在 Tenable Identity Exposure 中，選取「**系統**」>「**設定**」。
2. 在「**報告**」下方，按一下「**報告中心**」。

   窗格會隨即開啟，其中包含已設定的報告清單及其相關資訊，例如報告名稱、類型、網域、設定檔、期間、重複週期和收件者的電子郵件地址。

另請參閱

- 報告中心
- Set Permissions for a Role

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。

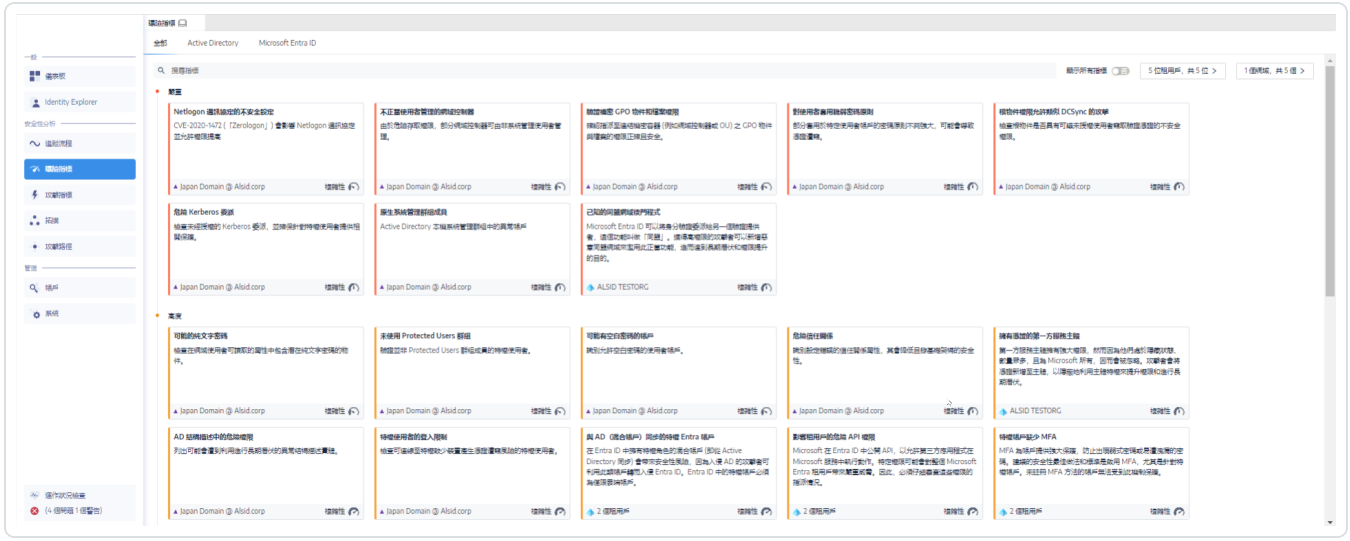
這些曝險指標 (IoE) 已預先設定，任何偏離既定標準的情況都會觸發對應的警示。

如要顯示曝險指標 (IoE)：

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

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

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



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

- **可供搜尋和篩選**：套用樹系和網域的篩選器，輕鬆探索曝險指標 (IoE)。
- **匯出功能**：異常情況物件可讓您匯出 CSV 格式的曝險指標 (IoE)。
- **對曝險指標 (IoE) 資安事端採取的措施**：將曝露的風險從白名單中移除/重新啟用。

曝險指標 (IoE) 的資料包括：

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

嚴重性等級

嚴重性等級可協助您評估偵測到的弱點的嚴重性,並決定修復動作的優先順序。

「**曝險指標**」窗格會按照以下方式顯示曝險指標 (IoE):

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

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

修復的優先順序

您優先處理系統發現的高嚴重性曝險指標 (IoE),以進行修復工作。此外,您可以使用曝險指標 (IoE) 中的風險衡量器,在嚴重類別中進一步排定問題的優先順序。

如果您認為曝險指標 (IoE) 屬於貴組織的管轄範圍或作業職責之中，則可以將其列入允許清單中。

使用案例

以下使用案例著重於名為「擁有永不過期密碼的帳戶」的曝險指標 (IoE)。

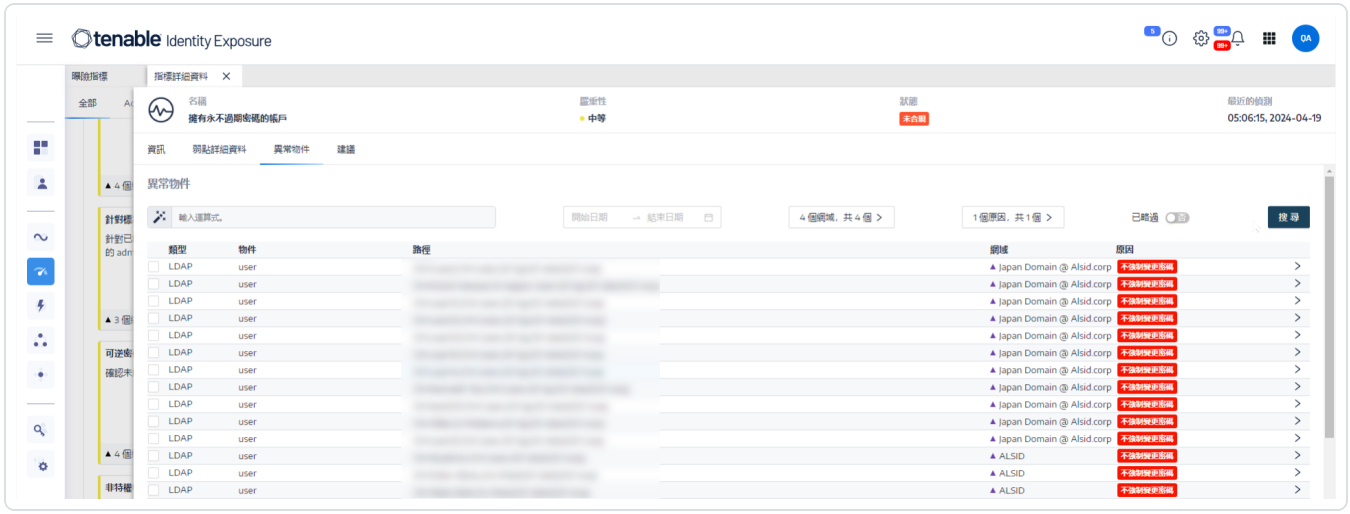
1. 當 Tenable Identity Exposure 標記曝險指標 (IoE) 時，此指標會顯示在曝險指標窗格中：

2. 若要深入了解曝險指標 (IoE)，請按一下「曝險指標 (IoE)」以存取更多詳細資料。在資訊頁面中，您會看到具有簡明概覽的執行摘要、與曝險指標 (IoE) 相關聯的潛在攻擊工具、受影響網域的詳細資料，以及可協助您了解並有效解決問題的相關說明文件。

3. 

4. 如需有關曝險指標 (IoE) 的詳細資料，請按一下「弱點詳細資料」索引標籤。

5. 若要驗證哪些帳戶已啟用「擁有永不過期密碼的帳戶」設定，請按一下「異常物件」。此動作可讓您存取系統內擁有此設定的帳戶清單。



6. 按一下異常物件以查看曝險指標 (IoE) 標記的帳戶。

7. 請諮詢 Active Directory 系統管理員，了解受影響帳戶啟用「擁有永不過期密碼的帳戶」選項的原因。
8. 根據回應，您可以選擇將帳戶列入白名單，或協助您的 Active Directory 系統管理員提出解決問題的建議。
9. 如需建議，請參閱曝險指標 (IoE) 的建議區段。

10. 如果帳戶有例外狀況或已知可如預期運作，您可以透過導覽到「**異常物件**」> 選取相應的異常物件 > **略過**所選物件 (或) 根據要求停止略過所選物件，來略過曝險指標 (IoE)。

另請參閱

- Indicators of Exposure
- 曝險指標教學影片
- Customize an Indicator

攻擊指標

當有最先進的攻擊程式技術試圖入侵您的 Active Directory (AD) 基礎架構時，Tenable Identity Exposure 攻擊指標 (IoA) 可協助貴組織偵測威脅並立即採取行動，包括：

- **前 3 大資安事端**：攻擊指標 (IoA) 的資訊統一呈現在單一介面中，包括即時時間軸、影響 AD 的前三大資安事端，以及攻擊的分布情況。
- **攻擊指標 (IoA) 詳情**：在 Tenable Identity Exposure 中，攻擊指標面板會提供在 AD 中所發生攻擊的相關資訊。
- **涉及攻擊指標 (IoA) 的資安事端**：攻擊指標 (IoA) 資安事端清單會完整詳列以您 AD 為目標之特定攻擊的資訊。您可以利用此資訊根據攻擊指標 (IoA) 的嚴重性等級進行適當應變。

攻擊指標具有一系列功能，可提升您的調查能力：

- **可供搜尋和篩選**：利用時間軸輕鬆探索攻擊指標 (IoA)，或根據樹系、網域和重要性層級套用篩選條件，以有效率地獲得針對性結果。
- **匯出功能**：允許以 PDF、CSV 或 PPTX 格式匯出攻擊指標 (IoA) 資料。
- **修改圖表類型**：提供變更圖表類型的選項，您可以選擇顯示攻擊嚴重性的分布或前三大攻擊及其各自的發生計數。
- **處理攻擊指標 (IoA) 資安事端**：允許您選取要關閉或重新開啟的資安事端。

嚴重性等級

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

等級	說明
嚴重：紅色	偵測到經驗證的後滲透攻擊，此類攻擊需要以網域支配權作為先決條件。
高度：橙色	偵測到允許攻擊者取得網域支配權的重大攻擊。
中度：黃色	與此攻擊相關的攻擊指標 (IoA) 可導致危險的特權提升，或允許攻擊者存取敏感資源。

低度：藍色	與偵察動作或低影響資安事端相關的可疑行為警示。

修復的優先順序

識別符合您特定安全性風險和疑慮的嚴重和高影響攻擊指標 (IoA)。

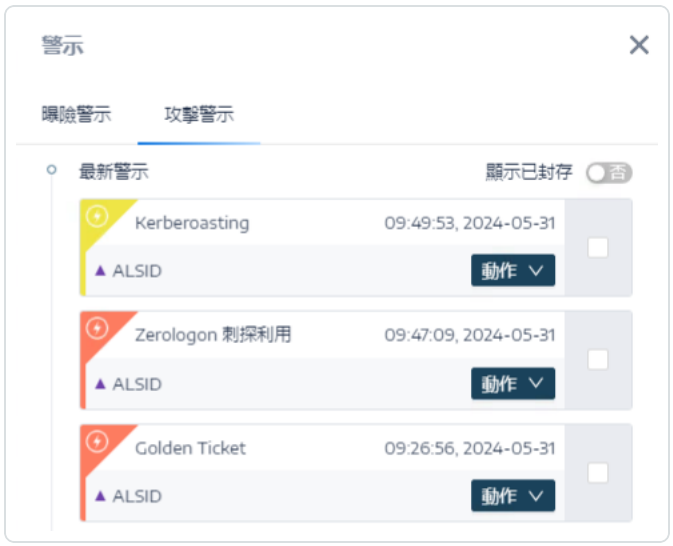
若要減輕誤報或疏忽合法攻擊帶來的風險，請務必根據您的環境校正攻擊指標 (IoA)。為此，您需要：

- 調整臨界值：校正攻擊指標 (IoA) 敏感度以減少誤報，確保警示合理且可作為行動依據。
- 將帳戶和活動列入白名單：將合法活動從觸發攻擊指標 (IoA) 的範圍中排除，以增強警示準確性並簡化調查流程。
- 關聯攻擊指標 (IoA)：分析不同攻擊指標 (IoA) 之間的關係，以識別更多的攻擊模式。

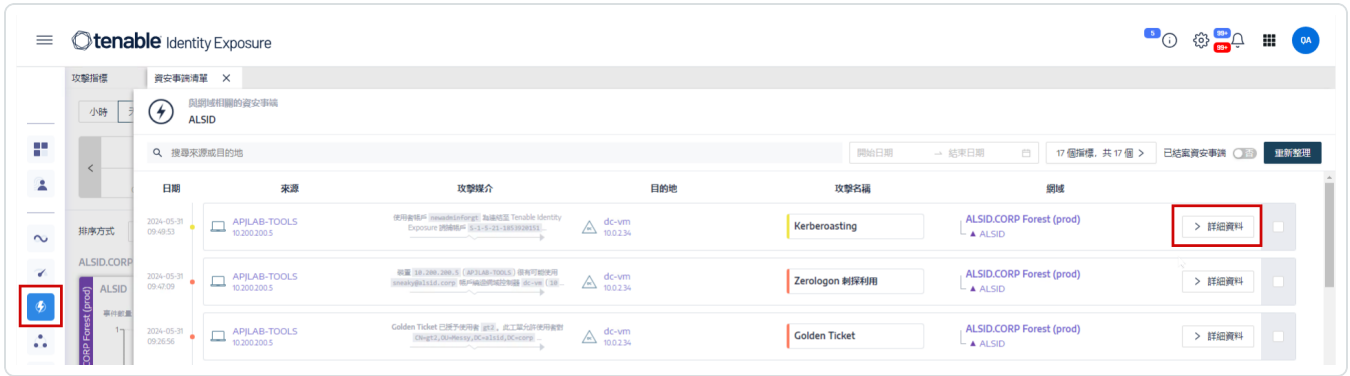
提示：選項和建議值詳情請參閱《Tenable Identity Exposure 攻擊指標參考指南》(可透過 https://zh-tw.tenable.com/downloads/identity-exposure 下載)。將這些選項和值套用至安全設定檔中的每個攻擊指標 (IoA)。

使用案例

1. 在啟用攻擊指標 (IoA) 時，從導覽窗格選取「攻擊指標」，或按一下首頁右上角的鈴鐺圖示。

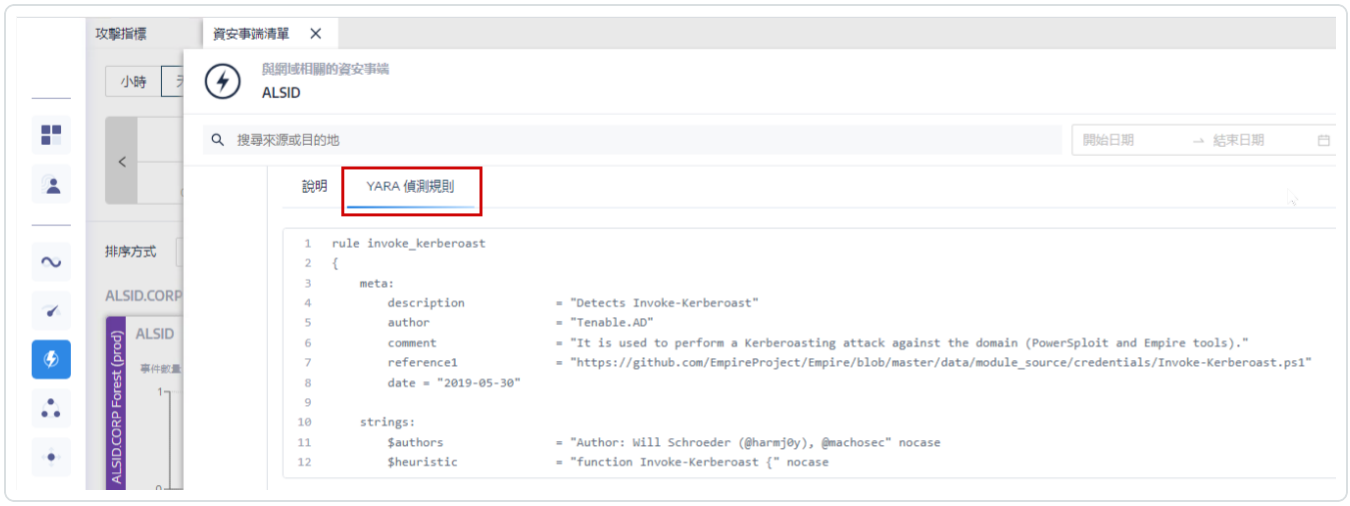


2. 每個指標均提供資安事端的詳細資訊，您在檢閱後便可採取適當行動：
    - 攻擊發生的時間
    - 攻擊說明
    - 攻擊來源
    - 攻擊目標
    - MITRE ATT&CK® 資訊
    - YARA 偵測規則
    - 其他資源
3. 選取「詳細資料」以存取說明，如下圖所示，重點放在「本機管理員列舉」部分。



4. 「說明」索引標籤提供有關在 Active Directory (AD) 發生之特定攻擊的資訊。

5. 「YARA 偵測規則」索引標籤提供有關 Tenable Identity Exposure 用於在網路層級偵測 Active Directory 攻擊的 YARA 規則的資訊，進而增強 Tenable Identity Exposure 的整體偵測功能。



6. 與 Active Directory 系統管理員或相關利害關係人合作，檢查並解決資安事端，決定要關閉或是重新開啟，並實施防止資安事端再次發生的措施。

7. 如果這是已識別或授權的攻擊，您可以選擇相應地自訂攻擊指標 (IoA)，以防止攻擊指標 (IoA) 在未來情況下再次標記攻擊。

另請參閱

- Indicators of Attack
- Customize an Indicator
- 攻擊指標教學影片

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. 檢查網路流量
4. 配置 Microsoft Entra ID 設定
5. 啟用 Microsoft Entra ID 支援
6. 啟用租用戶掃描

先決條件

您需要 Tenable Cloud 帳戶，才能登入「cloud.tenable.com」並使用 Microsoft Entra ID 支援功能。此 Tenable Cloud 帳戶與您的歡迎電子郵件所使用的電子郵件地址相同。如果您不知道「cloud.tenable.com」的電子郵件地址，請聯絡支援服務。具有有效授權 (內部部署或 SaaS) 的所有客戶皆可存取位於「cloud.tenable.com」的 Tenable 雲端。此帳戶可讓您為 Microsoft Entra ID 設定 Tenable 掃描並且收集掃描結果。

注意：您不需要有效的 **Tenable Vulnerability Management** 授權也可存取 Tenable Cloud。目前有效的獨立 Tenable Identity Exposure 授權 (內部部署或 SaaS) 便已足夠。

注意：Tenable Identity Exposure **不支援國家雲端中的 Microsoft Entra ID**，包括中國和美國政府的專用區域。Microsoft Entra ID 提供國家雲端，其為實際隔離的 Azure 執行個體，專為滿足特定法規和合規性需求而設計。Tenable Identity Exposure 僅支援全球 Microsoft Entra ID 環境，不包括中國國家雲端和美國政府國家雲端。如需 Microsoft Entra ID 國家雲端的詳細資訊，請參閱 Microsoft Entra 驗證 & 國家雲端 - Microsoft 身分識別平台。

權限

Microsoft Entra ID 的支援需要收集來自 Microsoft Entra ID 的資料，例如使用者、群組、應用程式、服務主體、角色、權限、原則、記錄等等。它會遵循 Microsoft 的建議，使用 Microsoft Graph API 和服務主體憑證收集此資料。

- 根據 Microsoft 的說明，您必須**以有權在 Microsoft Graph 上授予全租用戶管理員同意的使用者身分登入 Microsoft Entra ID**，而這必須具有全域管理員或特殊權限角色管理員角色 (或任何具有適當權限的自訂角色)。
- 您的 **Tenable Identity Exposure 使用者角色**必須具備適當的權限，才能存取 Microsoft Entra ID 的設定和資料圖表。如需詳細資訊，請參閱 Set Permissions for a Role。

網路流量

允許流量透過連接埠 443 從安全引擎節點伺服器傳入下列位址，以啟用 Entra ID 支援功能：

- sensor.cloud.tenable.com
- cloud.tenable.com

授權計數

只有在 Tenable 雲端同步功能已啟用的情況下，Tenable 才不會將重複的身分計入授權數。若未啟用此功能，系統就無法比對 Microsoft Entra ID 和 Active Directory 中的帳戶，因此必須分別計算每個帳戶。

- **未啟用 Tenable 雲端同步時**：同時擁有 AD 帳戶和 Entra ID 帳戶的使用者將被視為兩名獨立使用者，分別計入授權數。
- **啟用 Tenable 雲端同步時**：系統會將多個帳戶整合為單一身分，確保擁有多個帳戶的使用者只計算一次授權。

配置 Microsoft Entra ID 設定

使用下列程序 (改編自 《Microsoft 快速入門：使用 Microsoft 身分識別平台註冊應用程式》說明文件)，設定 Microsoft Entra ID 中的所有必要設定。

1. **建立應用程式：**

   a. 在 Azure 管理入口網站中，開啟「應用程式註冊」頁面。

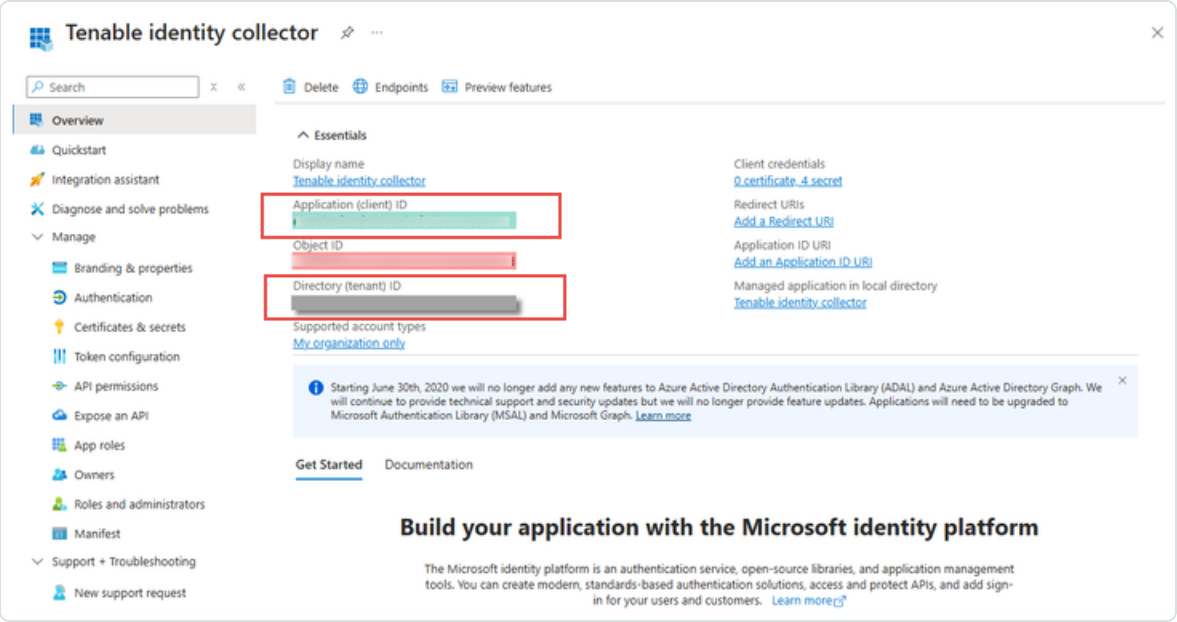
   b. 按一下「**+ 新註冊**」。

   c. 為應用程式命名 (例如：「Tenable Identity Collector」)。其他選項可以保留預設值。

   d. 按一下「**註冊**」。

   e. 在此新建立應用程式的「概覽」頁面上，記下「應用程式 (用戶端) ID」和「目錄 (租用戶) ID」，稍後在 如要新增 Microsoft Entra ID 租用戶： 步驟中將會需要這些資料

   > **注意**：請務必選取**應用程式 ID 而非物件 ID**，設定才能運作。



2. **新增憑證至應用程式：**

   a. 在 Azure 管理入口網站中，開啟「應用程式註冊」頁面。

   b. 按一下您建立的應用程式。

   c. 在左側功能表中，按一下「**憑證與密碼**」。

   d. 按一下「**+ 新用戶端密碼**」。

e. 在「**說明**」方塊中，提供此密碼的實際名稱，以及符合您原則的「**到期**」值。請記得在鄰近到期日前更新此密碼。

f. 將密碼值儲存在安全的位置，因為 Azure 只會顯示一次密碼值，而且一旦密碼遺失就必須重新建立。

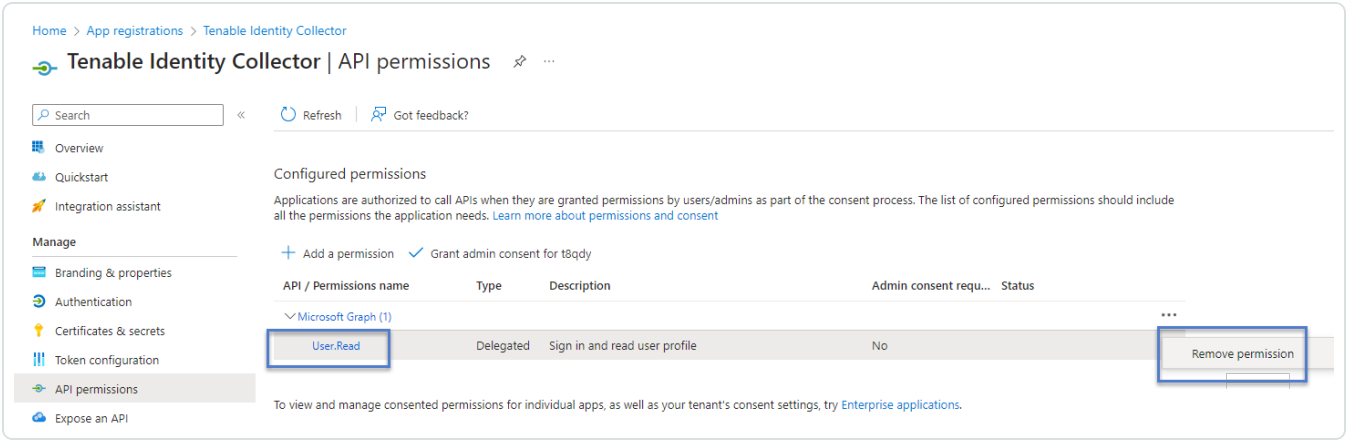
3. **指派權限給應用程式：**

a. 在 Azure 管理入口網站中，開啟「應用程式註冊」頁面。

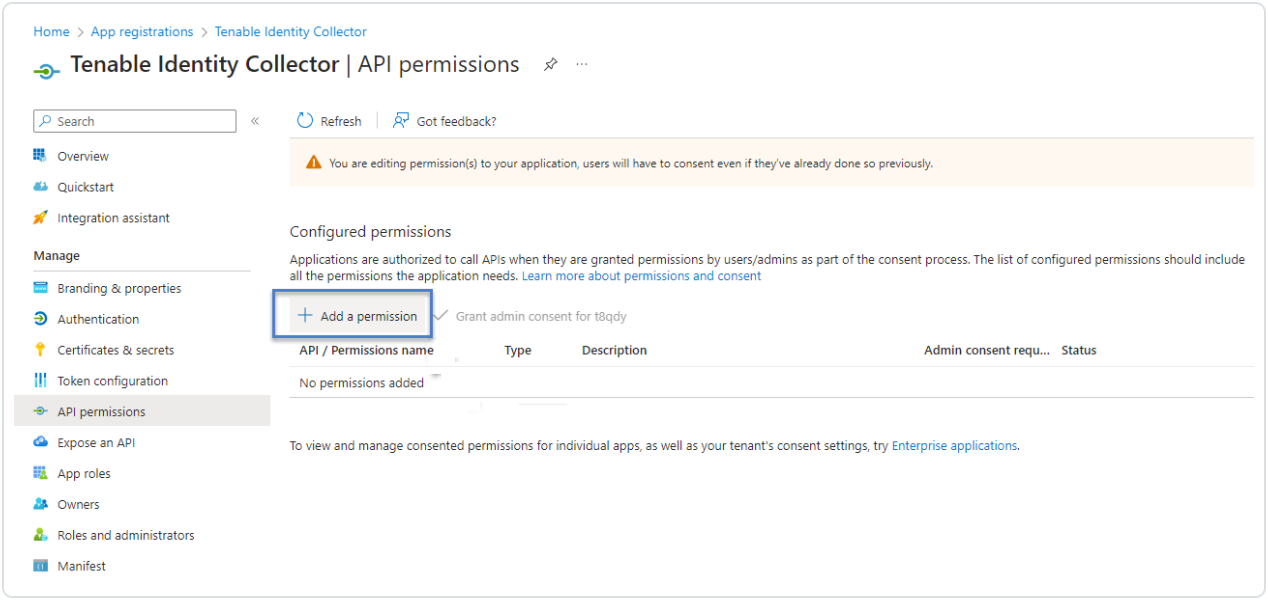
b. 按一下您建立的應用程式。

c. 在左側功能表中，按一下「**API 權限**」。

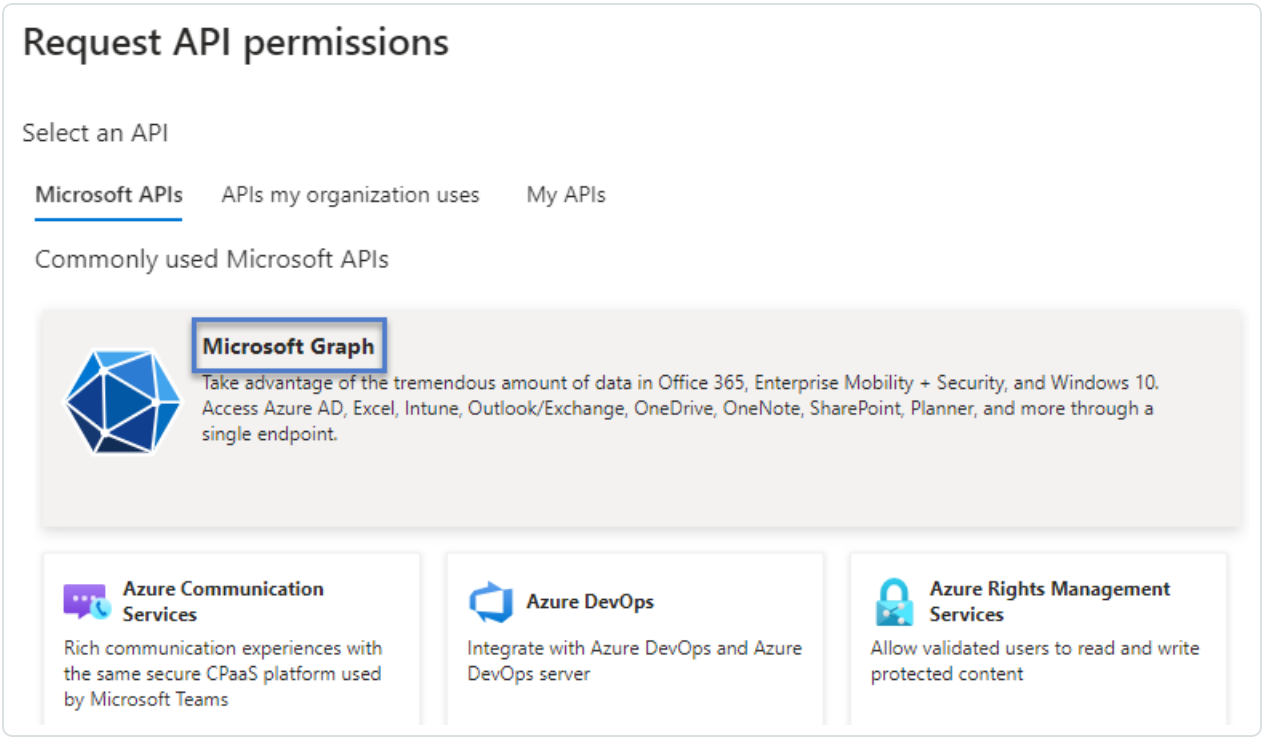
d. 移除現有的 `User.Read` 權限：



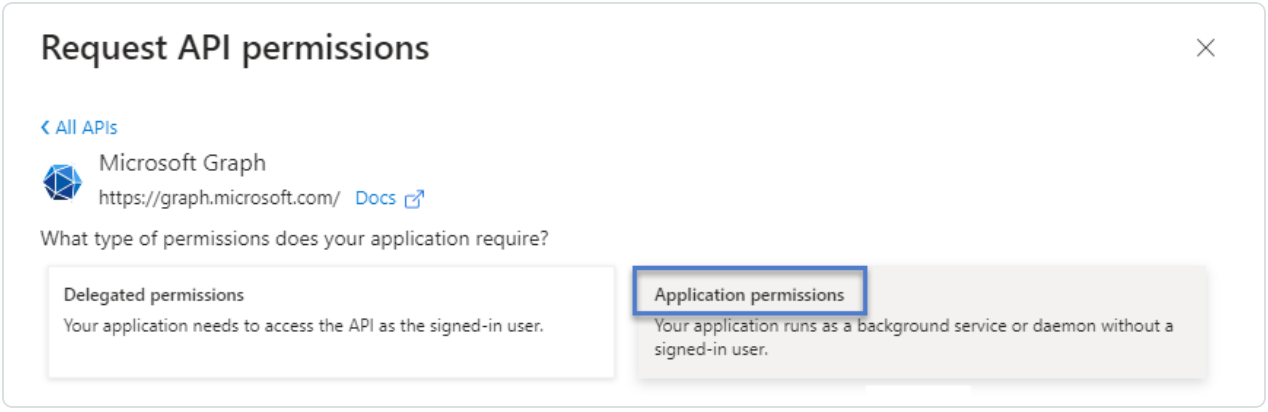
e. 按一下「**+ 新增權限**」：



f. 選取「**Microsoft Graph**」:



g. 選取「**應用程式權限**」(非「委派的權限」)。

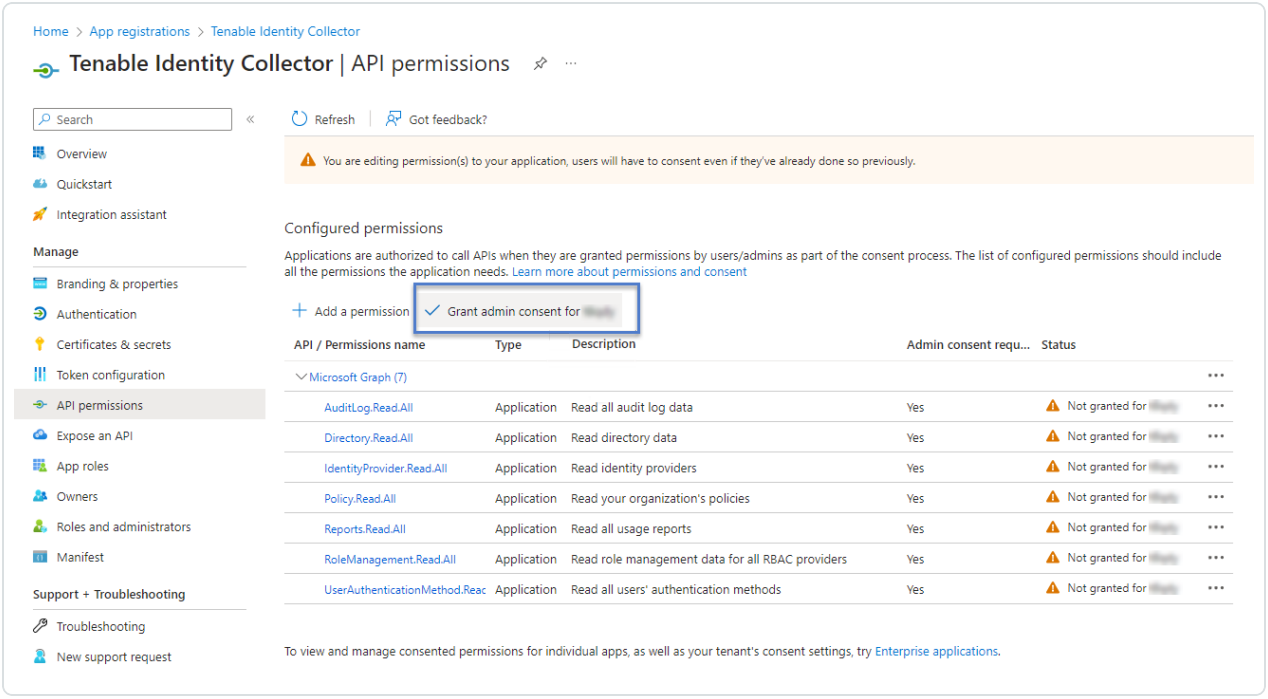


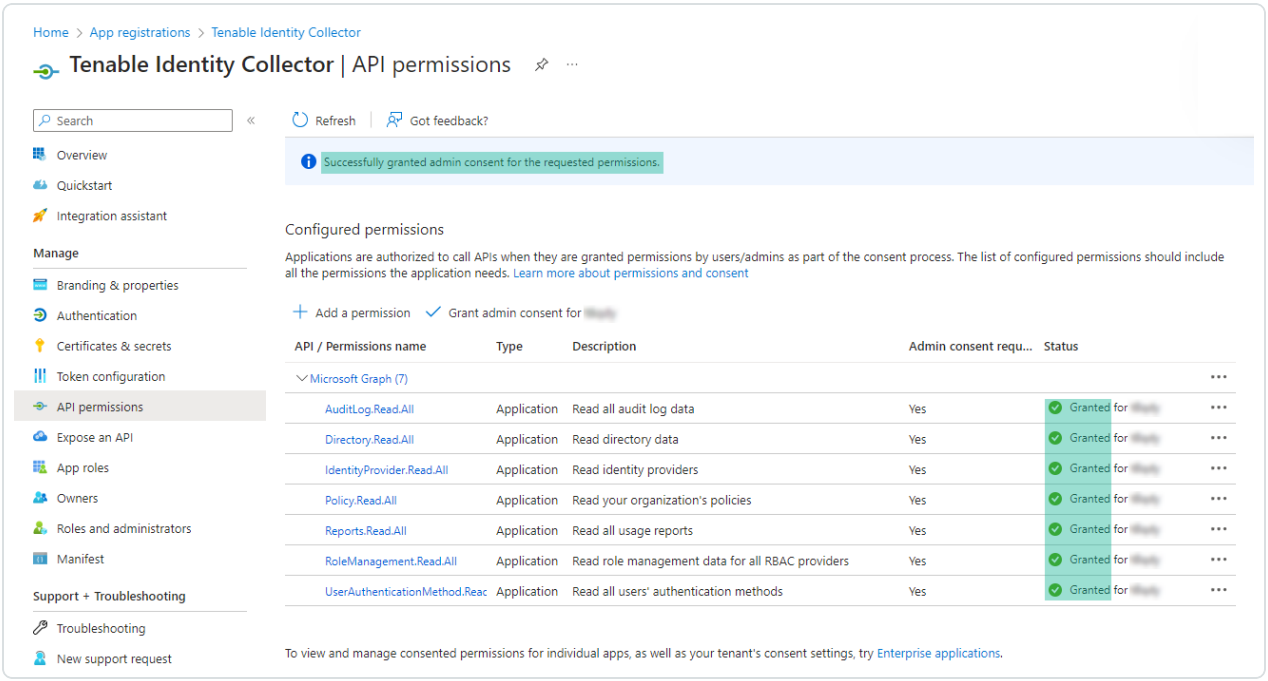
h. 使用清單或搜尋列，尋找並選取下列所有權限：

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

i. 按一下**「新增權限」**。

j. 按一下**「向 <租用戶名稱> 授予管理員同意」**，然後按一下**「是」**確認：





4. 在 Microsoft Entra ID 中配置所有必要設定後：

   a. 在 Tenable Vulnerability Management 中建立 Microsoft Azure 類型的新憑證。

   b. 選取「金鑰」驗證方法，並輸入您在之前程序中擷取的值：租用戶 ID、應用程式 ID 和用戶端密碼。

啟用 Microsoft Entra ID 支援

- 若要使用 **Microsoft Entra ID**，您必須在 Tenable Identity Exposure 設定中啟用該功能。
- 如需指示，請參閱Identity 360, Exposure Center, and Microsoft Entra ID Support Activation 。

啟用租用戶掃描

如要新增 Microsoft Entra ID 租用戶：

新增租用戶連結 Tenable Identity Exposure 與 Microsoft Entra ID 租用戶，以便在該租用戶上執行掃描。

1. 在「設定」頁面中，按一下「**租用戶管理**」索引標籤。

   「**租用戶管理**」頁面隨即開啟。

2. 按一下「**新增租用戶**」。

   「**新增租用戶**」頁面隨即開啟。

3. 在「**租用戶名稱**」方塊中輸入名稱。
4. 在「**憑證**」方塊中，按一下下拉式清單以選取一個憑證。
5. 如果清單中沒有出現您的憑證，您可以：
   - 在 Tenable Vulnerability Management 中建立一個 (「Tenable Vulnerability Management」>「**設定**」>「**憑證**」)。如需詳細資訊，請參閱 Tenable Vulnerability Management 中的建立 Azure 類型憑證的程序。
   - 檢查您對於 Tenable Vulnerability Management 中的憑證是否擁有「可使用」或「可編輯」權限 。您必須具備這些權限，Tenable Identity Exposure 才會在下拉式清單中顯示憑證。
6. 按一下「**重新整理**」以更新憑證的下拉式清單。
7. 選取您建立的憑證。
8. 按一下「**新增**」。

   系統會顯示一則訊息，確認 Tenable Identity Exposure 已新增租用戶。現在，「租用戶管理」頁面的清單中會顯示此租用戶。

針對租用戶啟用掃描：

注意：租用戶掃描並非即時發生，至少需要 45 分鐘後，身分識別總管中才會顯示 Microsoft Entra ID 資料。

- 從清單中選取一個租用戶，然後按一下切換為「**已啟用掃描**」。

Tenable Identity Exposure 會要求對此租用戶進行掃描，掃描結果會顯示在「曝險指標」頁面中。

注意：兩次掃描之間必須至少間隔 **30 分鐘**。

攻擊路徑

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

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

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

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

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

如要顯示攻擊路徑：

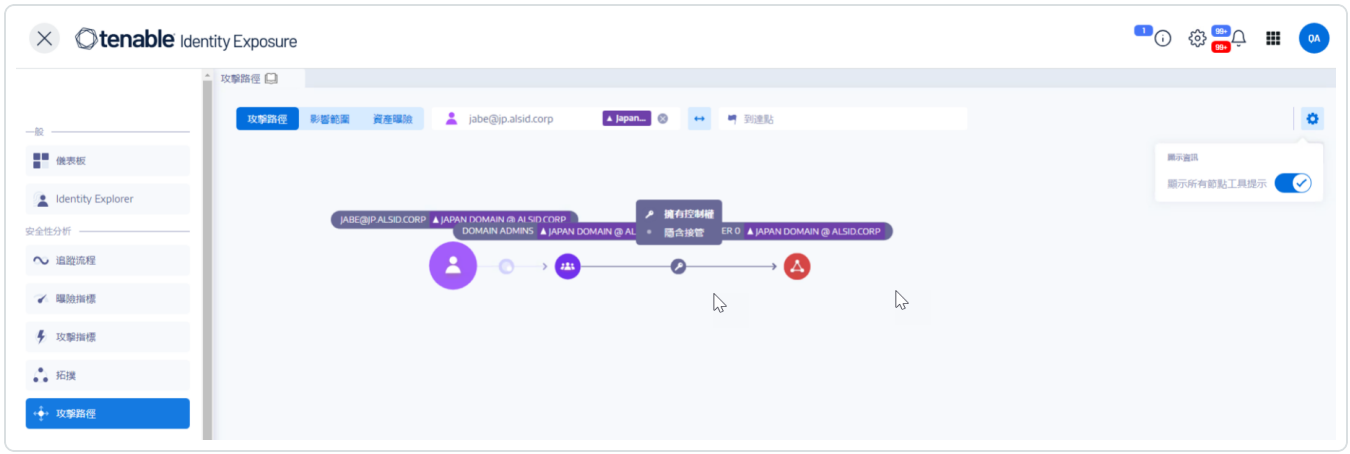
您可以指定起始點，像是 AD 中的任何資產 (例如，使用者帳戶、電腦、群組)。您可以定義到達點，代表攻擊者最終企圖入侵的資產 (例如，網域控制器、敏感資料伺服器)。

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

   「攻擊路徑」窗格會隨即顯示。

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

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



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

如要顯示影響範圍：

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

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

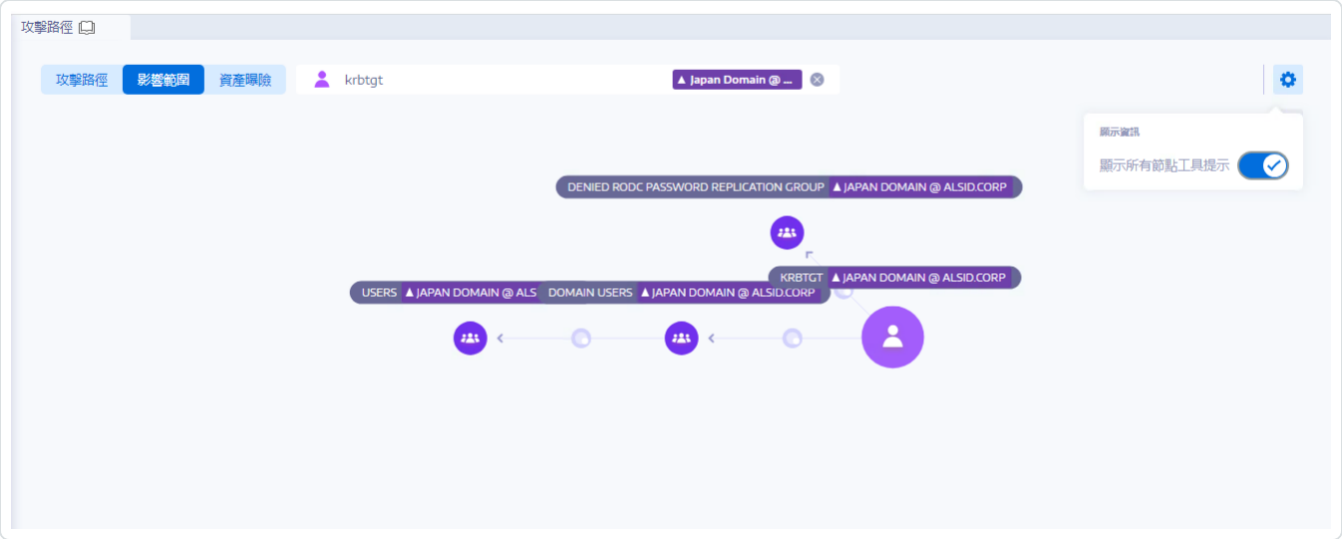
   「攻擊路徑」窗格會隨即顯示。

2. 在橫幅中，按一下**「影響範圍」**。

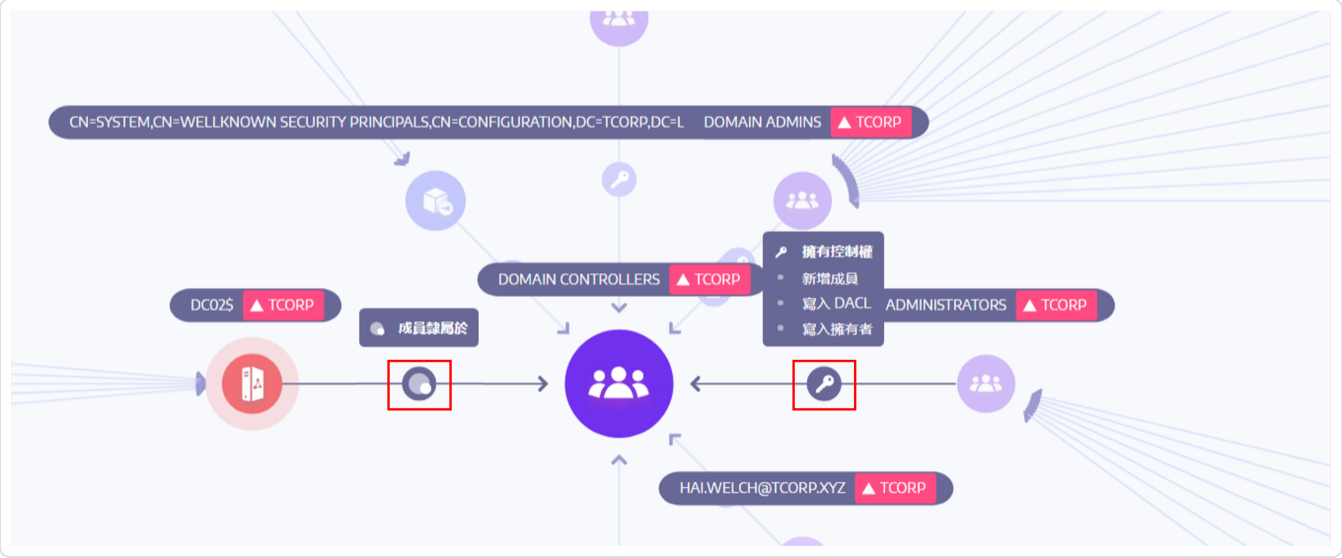
3. 在**「搜尋物件」**方塊中輸入資產的名稱。

4. 按一下 圖示。

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



5. 按一下資產之間箭頭上的圖示以顯示它們之間的關係。



如要顯示資產曝險：

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

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

   「**攻擊路徑**」窗格會隨即顯示。

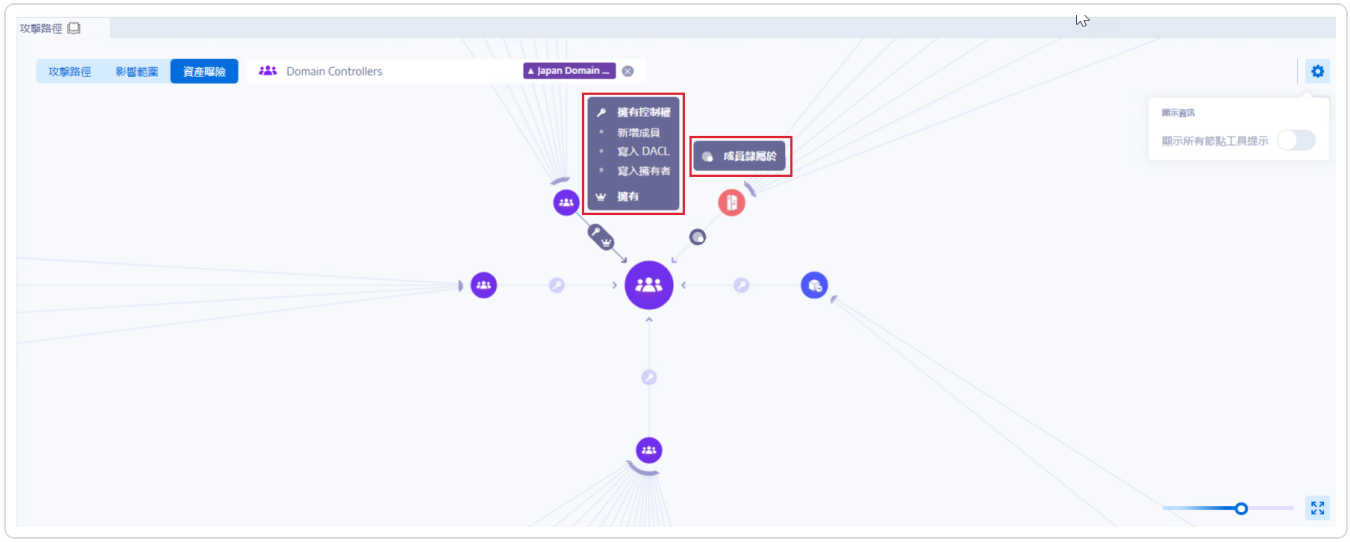
2. 在橫幅中，按一下「**資產曝險**」。

3. 在「**搜尋物件**」方塊中輸入資產的名稱。

4. 按一下 圖示。

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

5. 按一下資產之間箭頭上的圖示以顯示它們之間的關係。



如要釘選攻擊路徑：

另請參閱

- Attack Relations
- Identifying Tier 0 Assets
- Accounts with Attack Paths
- Attack Path Node Types

使用者管理

關鍵要素

- **角色**：預設角色包括管理員、安全分析師、使用者以及訪客，各自擁有不同的權限。自訂角色可以針對特定需求進行精細控制。
- **權限**：權限定義使用者可在 Tenable Identity Exposure 內存取的內容和執行的動作。這包括檢視報告與儀表板、管理使用者、設定指標，以及執行如停用帳戶等動作。
- **範圍設定**：Tenable Identity Exposure 允許將權限範圍限定在 Active Directory 中的特定網域、群組或者甚至是個別物件內。如此可確保使用者僅能根據其角色和責任存取相關資料。

好處

- **增強的 Active Directory 安全性**：精細的存取控制可將未經授權存取敏感身分資料的風險降到最低。
- **改善的效率和工作流程**：使用者可以存取所需的工具和資料，進而簡化調查以及資安事端回應。
- **合規性遵循**：角色型存取控制有助於滿足 Active Directory 內身分和存取管理的合規性要求。

另請參閱

- User Roles

Tenable Identity Exposure 整合

將 Tenable Identity Exposure 與您的 SIEM、SOC 或 SOAR 解決方案整合，以達到即時監控、自動化回應和改善警示管理的目的。

與 Syslog 整合的即時監控

透過嚴密的 Syslog 整合，取得嚴重曝險指標 (IoE) 的即時警示。

主要優勢

- **集中記錄**：將 Tenable Identity Exposure 事件與其他安全性解決方案彙總，以進行全面分析。
- **即時通知**：立即收到有關潛在身分洩漏和攻擊的通知。
- **改良安全性管理**：關聯不同來源的事件，以更快識別複雜威脅。
- **增強 SIEM 能見度**：將 Tenable Identity Exposure 資料與 SIEM 嚴密整合，提升瞭解實際情況和進行相關性分析的能力。
- **簡化工作流程**：根據 Syslog 資料自動化警示分類和回應，藉此最佳化安全性作業。

即時監控的曝險指標 (IoE) 範例

- **ADCS 危險的錯誤設定**：偵測/識別 AD 憑證伺服器的變更，這些變更可能表示「Certified Pre-owned」攻擊。
- **GPO 執行健全性**：偵測/識別透過群組原則內的指令碼執行嘗試安裝後門程式的行為。
- **允許使用者將電腦加入網域**：識別未經授權而加入的網域電腦，這是「RBCD」後門程式攻擊的慣用前置攻擊。

使用 SOAR 平台自動化回應

利用現有的 Security Orchestration、Automation 和 Response (SOAR) 平台，以根據 TIE 資料執行自動化修復動作。主要優勢如下：

- **緩解速度加快**：透過將重要曝險指標 (IoE) 自動化回應，將停機時間和影響降到最低。
- **效率提高**：安全團隊不必執行重複工作，因而能將重點擺在策略性安全計畫。
- **安全性措施增強**：主動解決偵測到的錯誤設定，增強整體安全性狀態。

重要事項：自動化指令碼中的疑難排解或協助超出 Tenable 支援服務的範圍。如需協助，請聯絡我們的專業服務團隊。