管理入口網站

25.01

公司系統管理員指南

版本：2025/2/6

目錄

關於本文件

本文件適用於想要使用雲端管理入口網站建立與管理使用者帳戶、裝置和配額;設定及控制對其雲端組織的存取;以及監視使用狀況和作業的客戶系統管理員。

關於管理入口網站

管理入口網站是提供資料保護服務的雲端平台的 Web 介面。

雖然每個服務各有自己的 Web 介面 (稱為服務主控台), 但管理入口網站可讓系統管理員控制服務使用、建立使用者帳戶和單位、產生報告等等。

支援的網頁瀏覽器

Web 介面支援下列網頁瀏覽器:

- Google Chrome 29 或更新版本
- Mozilla Firefox 23 或更新版本
- Opera 16 或更新版本
- Microsoft Edge 25 或更新版本
- 在 macOS 與 iOS 作業系統中執行的 Safari 8 或更新版本

在其他網頁瀏覽器 (包括在其他作業系統中執行的 Safari 瀏覽器) 中, 使用者介面可能會顯示不正確, 或是部分功能無法正常使用。

我的收件匣

[我的收件匣] 頁面的設計目的是簡化應用程式內的通訊。您可以依照本指南, 有效地管理訊息、保持井井有條, 以及提高生產力。產品收件匣是您在應用程式內接收和管理通訊的中心樞紐。它可讓您隨時掌握工作流程中的重要更新、訊息和警示。

概觀

[我的收件匣] 索引標籤上有一個通知計數器, 可顯示未讀通知的數量。按一下此計數器會顯示未讀通知, 讓您輕鬆追蹤待處理項目。此外, 每個篩選條件 (類別、重要性、動作) 旁的計數器會顯示該特定篩選條件下可用的通知數目, 協助您瞭解每個類別的通知數目。

在您的收件匣中, 您將會收到各種通知, 每個通知都是根據您的帳戶設定和內容, 針對特定用途而設計:功能公告、可用的新訓練、活動和網路研討會的邀請、憑證到期提醒、促銷活動、維護通知、調查等等。

檢查您的通知

檢查您的通知區段

1. 登入 Cyber Protect Cloud 主控台。
2. 在導覽窗格中, 選擇 **[我的收件匣]** 功能表項目。

搜尋我的收件匣

若要搜尋未讀訊息

1. 按一下 **[我的收件匣]** 功能表項目。
2. 切換右上角的 **[僅顯示未讀項目]** 切換按鈕。

若要在收件匣中搜尋重要資訊

1. 從 儀表板存取 **[我的收件匣]**。
2. 在收件匣檢視中，找出最上方的 **[搜尋]** 列。
3. 輸入相關的關鍵字或寄件者名稱以篩選訊息。
4. 按 **Enter** 以檢視搜尋結果。

結果將顯示符合您的搜尋條件的所有通知。

帳戶和單位

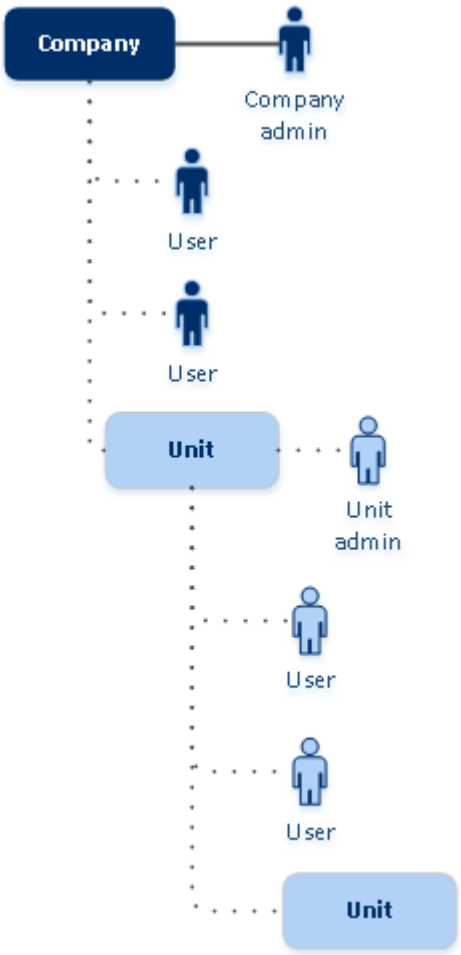
使用者帳戶類型有兩種：系統管理員帳戶和使用者帳戶。

- **系統管理員**擁有管理入口網站的存取權。他們在所有服務中都擁有系統管理員角色。
- **使用者**沒有管理入口網站的存取權。他們對服務的存取權及其在服務中的角色，是由系統管理員定義的。

系統管理員可以建立單位，那些單位通常對應到組織內的單位或部門。每個帳戶都存在於公司層級或單位層級內。

系統管理員可以管理階層中在他們以上或以下層級的單位、系統管理員帳戶，和使用者帳戶。

下圖說明三種階層層級：公司和兩個單位。選擇性使用的單位和帳戶會以虛線表示。



下表摘述管理員和使用者可以執行的選項。

作業	使用者	系統管理員
建立單位	否	是
建立帳戶	否	是
下載及安裝軟體	是	是
使用服務	是	是
建立關於服務使用的報告	否	是

配額管理

配額會限制租用戶使用服務的能力。

在管理入口網站中，您可以依服務供應商檢視配置給貴組織的服務配額，但您無法管理它們。

您可以為您的使用者管理服務配額。

重要事項
產品 UI 中顯示的儲存空間使用狀況值為二進位位元組單位 (Mebibytes (MiB)、Gibibytes (GiB) 及 Tebibytes (TiB)), 即使標籤分別顯示 MB、GB 及 TB, 也是如此。例如, 如果實際使用量為 3105886629888 個位元組, 則 UI 中顯示的值將正確顯示為 2.82, 但標籤會標示為 TB 而非 TiB。

檢視組織的配額

在管理入口網站中, 前往 **[監控]** > **[使用狀況]**。您將會看到一個儀表板, 其中會顯示配置給貴組織的配額。每個服務的配額都會顯示在個別的索引標籤上。

備份配額

您可以指定雲端儲存空間配額、本機備份配額, 以及允許使用者保護的電腦/裝置/網站數量上限。您可以使用下列配額。

裝置的配額

- **工作站**
- **伺服器**
- **虛擬機器**
- **行動裝置**
- **Web 託管伺服器** (執行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板的 Linux 型實體或虛擬伺服器)
- **網站**

只要至少有套用一個保護計劃, 電腦/裝置/網站就會被視為受到保護。第一次備份後, 行動裝置將變成受保護狀態。

當超過一些裝置的超額時, 使用者無法將保護計劃套用至更多裝置。

雲端資料來源的配額

- **Microsoft 365 授權**

  此配額是由服務提供者套用至整個公司。公司系統管理員可以在管理入口網站中檢視配額及其使用情形。超過固定配額時, 無法將備份計劃套用至新的授權。

  此配額的計費取決於 Cyber Protection 的所選計費模式。

  - 在 **[按 GB]** 計費模式中, 計費僅根據儲存空間使用量, 不會計算授權。
  - 在 **[按工作負載]** 計費模式中, 計費是根據受保護的 Microsoft 365 授權數量。系統僅針對未受保護的授權計費儲存空間使用量。

    下表摘要說明 **[按工作負載]** 計費模式。

	備份位置	
	Acronis 託管的儲存空間* 合作夥伴託管的儲存空間	**Microsoft Azure 儲存體 Google 儲存空間**
受保護的授權	計費是根據受保護授權的數量進行的。 受保護授權備份使用的儲存空間不會計費。	受保護的授權和已使用的儲存空間都會計費。
未受保護的授權	未受保護的授權不會計費。 未受保護授權備份使用的儲存空間會計費。	未受保護的授權不會計費。 未受保護授權備份使用的儲存空間會計費。

***** 適用於 Acronis Storage 的公平使用政策。條款與條件可在 https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage 取得。

當 Microsoft 365 使用者擁有以下任一項時，即將授權視為受到保護：

- 套用備份計劃的信箱
- 套用備份計劃的 OneDrive
- 存取受保護的公司層級資源，例如 Microsoft 365 SharePoint Online 網站，或 Microsoft 365 Teams。

  若要瞭解如何檢查 Microsoft 365 SharePoint 或 Teams 網站的成員數量，請參閱本知識庫文章。

在以下情況下，授權會變成未受保護：

- 使用者對受保護公司層級資源 (例如 Microsoft 365 SharePoint Online 網站或 Microsoft 365 Teams) 的存取權遭到撤銷。
- 使用者信箱或 OneDrive 中的所有備份計劃遭到撤銷。
- Microsoft 365 組織中的使用者遭到刪除。

下列 Microsoft 365 資源不收費，也不需要每基座授權：

- 共用信箱
- 房間和設備
- 可存取已備份的 SharePoint 網站和/或 Microsoft Teams 的外部使用者。

注意事項

未擁有受保護的個人信箱或 OneDrive 且僅能存取共用資源 (共用信箱、SharePoint 網站和 Microsoft Teams) 的已封鎖 Microsoft 365 使用者無需付費。已封鎖的使用者是指沒有有效登入且無法存取 Microsoft 365 服務的使用者。若要瞭解如何封鎖 Microsoft 365 組織中所有未授權的使用者，請參閱 "防止未獲授權的 Microsoft 365 使用者登入" (第 12 頁)。

重要事項

本機代理程式和雲端代理程式使用不同的配額。如果您同時使用這兩種代理程式備份相同的工作負載，您將需要支付兩次費用。例如：

- 如果您使用本機代理程式備份 120 個使用者的信箱，並使用雲端代理程式備份相同使用者的 OneDrive 檔案，您將需要支付 240 個 Microsoft 365 授權的費用。
- 如果您使用本機代理程式備份 120 個使用者的信箱，也使用雲端代理程式備份相同信箱，您將需要支付 240 個 Microsoft 365 授權的費用。

若要查看有關 Microsoft 365 授權的常見問題，請參閱 Cyber Protect Cloud：Microsoft 365 按 GB 授權和 Cyber Protect Cloud：Microsoft 365 授權和定價變更。

- **Microsoft 365 SharePoint Online**

  此配額是由服務提供者套用到整個公司。此配額會啟用 SharePoint Online 網站的保護，並設定可以保護的網站集合和群組網站數目上限。

  公司系統管理員可以在管理入口網站中檢視配額。他們也可以在使用情況報告中檢視配額，以及 SharePoint Online 備份所使用的儲存空間量。

- **Microsoft 365 Teams**

  此配額是由服務提供者套用到整個公司。此配額會啟用或停用保護 Microsoft 365 Teams 的功能，並設定可以保護的小組數目上限。若要保護一個團隊，無論有多少個成員或頻道，都需要一個配額。公司系統管理員可以在管理入口網站中檢視配額和使用狀況。

- **電子郵件存檔授權**

  [電子郵件存檔授權]配額可啟用或停用建立電子郵件存檔的功能，並設定可新增至存檔的信箱數目上限。

- **Google Workspace 授權**

  此配額是由服務提供者套用到整個公司。系統可以允許公司保護 **Gmail** 信箱 (包括行事曆和聯絡人)、**Google 雲端硬碟**檔案，或兩者。公司系統管理員可以在管理入口網站中檢視配額和使用狀況。

  如果使用者的信箱或 Google 雲端硬碟至少有套用一個備份計劃，就會將 Google Workspace 授權視為受到保護。

  超過固定額度時，公司系統管理員無法將備份計劃套用至新的授權。

- **Google Workspace 共用磁碟機**

  此配額是由服務提供者套用到整個公司。此配額會啟用或停用保護 Google Workspace 共用磁碟機的功能。如果已啟用配額，則任何數量的共用磁碟機都可以受到保護。公司系統管理員無法在管理入口網站中檢視配額，但可以在使用情況報告中檢視共用磁碟機備份佔用的儲存空間量。

  此外，備份 Google Workspace 共用磁碟機僅適用於至少有一個 Google Workspace 授權配額的客戶。此配額僅經過驗證，不會遭到佔用。

儲存空間的配額

重要事項
產品 UI 中顯示的儲存空間使用狀況值為二進位位元組單位 (Mebibytes (MiB)、Gibibytes (GiB) 及 Tebibytes (TiB)), 即使標籤分別顯示 MB、GB 及 TB, 也是如此。例如, 如果實際使用量為 3105886629888 個位元組, 則 UI 中顯示的值將正確顯示為 2.82, 但標籤會標示為 TB 而非 TiB。

- **雲端資源**
  - **備份儲存**
    - **備份儲存**

      此配額會限制位於雲端儲存空間的備份的大小總計。超過備份儲存空間固定配額時, 備份作業將不會開始。

      在 **[按工作負載]** 計費模式中, 此配額僅適用於與 Microsoft 365 和 Google Workspace 不同的工作負載的備份。Microsoft 365 和 Google Workspace 工作負載的備份儲存空間無限制 *。

      在 **[按 GB]** 計費模式中, 此配額適用於所有備份, 包括 Microsoft 365 和 Google Workspace 工作負載的備份。

      * 適用於 Acronis Storage 的公平使用政策。條款與條件可在 https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage 取得。
    - **存檔儲存位置**

      此配額可限制雲端基礎架構中電子郵件存檔的大小總計。
  - **Advanced Disaster Recovery**

    此區段包含與災難復原相關的配額。
- **本機資源**
  - **本機備份**

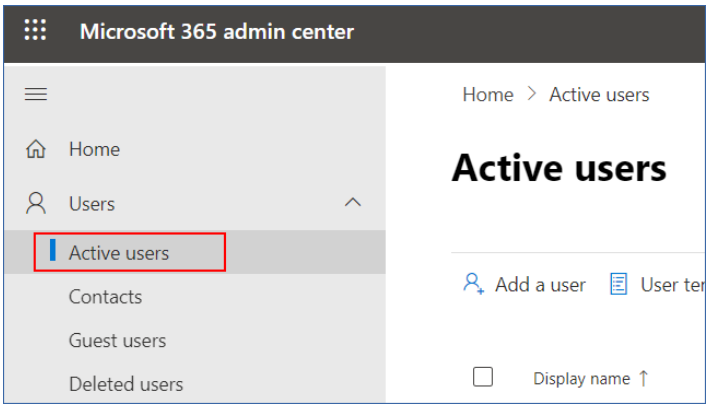
    此配額會限制使用雲端基礎架構建立的本機備份的大小總計。系統無法針對本機備份套用固定配額。

防止未獲授權的 Microsoft 365 使用者登入

您可以透過編輯 Microsoft 365 組織中所有未獲授權使用者的的狀態來防止其登入。

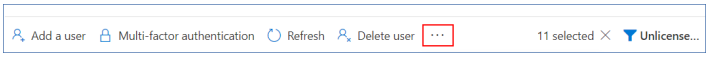
若要防止未獲授權的使用者登入

1. 以全域系統管理員的身分登入 Microsoft 365 系統管理中心 (https://admin.microsoft.com)。
2. 在導覽功能表中, 移至 **[使用者]** > **[有效使用者]**。



3. 按一下 **[篩選]**，然後選擇 **[未獲授權的使用者]**。

4. 選擇使用者名稱旁的核取方塊，然後按一下省略符號 (...) 圖示。



5. 從功能表中，選擇 **[編輯登入狀態]**。
6. 選擇 **[封鎖使用者登入]** 核取方塊，然後按一下 **[儲存]**。

Disaster Recovery 配額

注意事項
Disaster Recovery 產品項目僅可搭配 Disaster Recovery 附加元件使用。

這些配額是由服務供應商套用到整個公司的。公司系統管理員可在管理入口網站中檢視配額和使用狀況，但無法為使用者設定配額。

- **災難復原儲存空間**
  災難復原儲存空間會顯示使用災難復原保護之伺服器的備份儲存大小。災難復原儲存空間的使用量等於使用災難復原伺服器保護之工作負載的備份儲存的使用量。此儲存空間是從建立復原伺服器的時間開始計算 (無論伺服器目前是否正在執行)。如果達到此配額的超額，則無法建立主要伺服器和復原伺服器，或新增/延伸現有主要伺服器的磁碟。如果超過此配額的超額，則無法啟動容錯移轉，或啟動已停止的伺服器。執行中的伺服器會繼續執行。
- **計算點**
  此配額會限制主要伺服器和復原伺服器在計費期間消耗的 CPU 和 RAM 資源。如果達到此配額的超額，則會關閉所有主要伺服器和復原伺服器。除非下一個計費期間開始，否則不能使用這些伺服器。預設的計費期間為一個完整曆月。
  當配額遭到停用時，不論計費期間，都無法使用伺服器。
- **公共 IP 位址**
  此配額會限制可指派給主要伺服器和復原伺服器的公共 IP 位址數量。如果達到此配額的超額，則無法為更多伺服器啟用公共 IP 位址。您可以透過清除伺服器設定中的 **[公共 IP 位址]** 核取方塊，禁止某個伺服器使用公共 IP 位址。然後，您可以允許其他伺服器使用公共 IP 位址，這通常不會是同一個位址。

當配額遭到停用時，使用公共 IP 位址的所有伺服器都會停止，因此會變成無法從網際網路連線。

- **雲端伺服器**

  此配額會限制主要伺服器和復原伺服器的總數。如果達到此配額的超額，則無法建立主要伺服器或復原伺服器。

  當此配額遭到停用時，伺服器會顯示在 Cyber Protect 主控台中，但是唯一可行的操作是 **[刪除]**。
- **網際網路存取**

  此配額會啟用或停用來自主要伺服器和復原伺服器的網際網路存取。

  當此配額遭到停用時，主要伺服器和復原伺服器將無法與網際網路建立連線。

File Sync & Share配額

這些配額是由服務供應商套用到整個公司的。公司系統管理員可以在管理入口網站中檢視配額和使用狀況。

- **使用者**

  此配額會定義可以存取此服務的使用者數量。

  系統管理員帳戶不計入此配額的一部分。
- **雲端儲存**

  這是用於儲存使用者檔案的雲端儲存空間。此配額會為雲端儲存空間中的租用戶定義已配置的空間。

實體資料運送配額

實體資料運送服務配額的耗用是以磁碟機為基礎。您可以將多部電腦的最初備份儲存在一個硬碟機上。

這些配額是由服務供應商套用到整個公司的。公司系統管理員可在管理入口網站中檢視配額和使用狀況，但無法為使用者設定配額。

- **至雲端**

  允許使用硬碟機，將最初備份傳送到雲端資料中心。此配額會定義要傳送到雲端資料中心的最大磁碟機數。

Notary 配額

這些配額是由服務供應商套用到整個公司的。公司系統管理員可以在管理入口網站中檢視配額和使用狀況。

- **Notary 存放區**

  定義已公正的檔案、已簽署的檔案，以及其公證或簽署正在進行中的檔案的最大雲端儲存空間。

  若要減少此配額使用量，您可以從 Notary 儲存空間中刪除已公證或已簽署的檔案。
- **公證**

  定義可以使用 Notary 服務公證的檔案數目上限。

  只要檔案上傳至 Notary 存放區，且其公證狀態變更為**進行中**，就會將該檔案視為已公證。

如果多次公證相同的檔案，每次公證都會視為一個新檔案。

- **電子簽章**
  定義數位電子簽章的數目上限。

定義使用者的配額

配額可讓您限制使用者使用服務的能力。若要為某個使用者設定配額，請在 **[我的公司]** 下的 **[使用者]** 索引標籤上選擇使用者，然後按一下 **[配額]** 區段中的鉛筆圖示。

超過配額時，系統會發送一則通知到使用者的電子郵件地址。如果您沒有設定配額超額，配額會被視為**「彈性」**。這意味著不會套用使用 Cyber Protection 服務的限制。

當您指定配額超額時，配額則會被視為**「硬性」**。**超額**可允許使用者超過指定值的配額。超過超額時，會套用使用服務的限制。

範例

彈性配額：您已經將工作站的配額設為等於 20。當使用者受保護的工作站數目達到 20 時，使用者將會透過電子郵件收到通知，但是 Cyber Protection 服務將仍然可以使用。

硬性配額：如果您已經將工作站的配額設為等於 20，而超額為 5，則使用者將會在受保護的工作站數目達到 20 時，透過電子郵件收到通知，而且 Cyber Protection 服務會在該數目達到 25 時遭到停用。

備份配額

您可以指定備份儲存空間配額，以及允許使用者保護的最多電腦/裝置/網站數量。您可以使用下列配額。

裝置的配額

- **工作站**
- **伺服器**
- **虛擬機器**
- **行動裝置**
- **Web 託管伺服器** (執行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板的 Linux 型實體或虛擬伺服器)
- **網站**

只要至少有套用一個保護計劃，電腦/裝置/網站就會被視為受到保護。第一次備份後，行動裝置將變成受保護狀態。

當超過一些裝置的超額時，使用者無法將保護計劃套用至更多裝置。

儲存空間的配額

重要事項
產品 UI 中顯示的儲存空間使用狀況值為二進位位元組單位 (Mebibytes (MiB)、Gibibytes (GiB) 及 Tebibytes (TiB)), 即使標籤分別顯示 MB、GB 及 TB, 也是如此。例如, 如果實際使用量為 3105886629888 個位元組, 則 UI 中顯示的值將正確顯示為 2.82, 但標籤會標示為 TB 而非 TiB。

- **備份儲存**
  備份儲存空間配額會顯示雲端儲存空間的備份大小總計。當超過備份儲存空間配額超額時, 備份將會失敗。

  重要事項
  本機代理程式和雲端代理程式使用不同的配額。如果您同時使用這兩種代理程式備份相同的工作負載, 您將需要支付兩次費用。例如:
  - 如果您使用本機代理程式備份 120 個使用者的信箱, 並使用雲端代理程式備份相同使用者的 OneDrive 檔案, 您將需要支付 240 個 Microsoft 365 授權的費用。
  - 如果您使用本機代理程式備份 120 個使用者的信箱, 也使用雲端代理程式備份相同信箱, 您將需要支付 240 個 Microsoft 365 授權的費用。

File Sync & Share配額

您可以為使用者定義下列File Sync & Share配額:

- **個人儲存空間**
  為使用者檔案定義已配置的雲端儲存空間。

Notary 配額

您可以為使用者定義下列 Notary 配額:

- **Notary 存放區**
  定義已公正的檔案、已簽署的檔案, 以及其公證或簽署正在進行中的檔案的最大雲端儲存空間。
  若要減少此配額使用量, 您可以從 Notary 儲存空間中刪除已公證或已簽署的檔案。
- **公證**
  定義可以使用 Notary 服務公證的檔案數目上限。
  只要檔案上傳至 Notary 存放區, 且其公證狀態變更為**進行中**, 就會將該檔案視為已公證。
  如果多次公證相同的檔案, 每次公證都會視為一個新檔案。
- **電子簽章**
  定義數位電子簽章的數目上限。

逐步說明

下列步驟會引導您瞭解管理入口網站的基本用法。說明如何執行下列步驟：

- 啟用您的管理員帳戶
- 存取管理入口網站和服務
- 建立單位
- 建立使用者帳戶

啟用系統管理員帳戶

註冊服務後，您會收到包含以下資訊的電子郵件：

- **您的登入。**這是您用來登入的使用者名稱。您的登入也會顯示在帳戶啟用頁面上。
- **啟用帳戶**按鈕。按一下該按鈕，然後設定帳戶的密碼。請確保密碼長度至少 9 個字元。如需有關密碼的詳細資訊，請參閱 "密碼需求" (第 17 頁)。

密碼需求

使用者註冊期間會檢查密碼的複雜性，並將其歸類為下列其中一種類別：

- 弱式
- 中
- 強式

您無法儲存弱式密碼，即使長度符合標準也是如此。與使用者名稱、登入名稱、使用者電子郵件或使用者帳戶所屬租用戶的名稱重複的密碼一律被視為弱式密碼。大多數常用的密碼也被視為弱式密碼。

注意事項
密碼需求可能會變更。

若要強化密碼，請新增更多字元。並非必須使用不同類型的字元(例如數字、大小寫字母及特殊字元)，但這樣做會強化密碼，也會縮短其長度。

存取管理入口網站和服務

1. 移至服務主控台登入頁面。
2. 輸入登入，然後按一下 **[下一步]**。
3. 輸入密碼，然後按一下 **[下一步]**。
4. 執行下列其中一項操作：
   - 若要登入管理入口網站，請按一下 **[管理入口網站]**。
   - 若要登入服務，請按一下服務名稱。

管理入口網站的逾時期限對於作用中工作階段而言為 24 小時，對於閒置工作階段而言則為 1 小時。

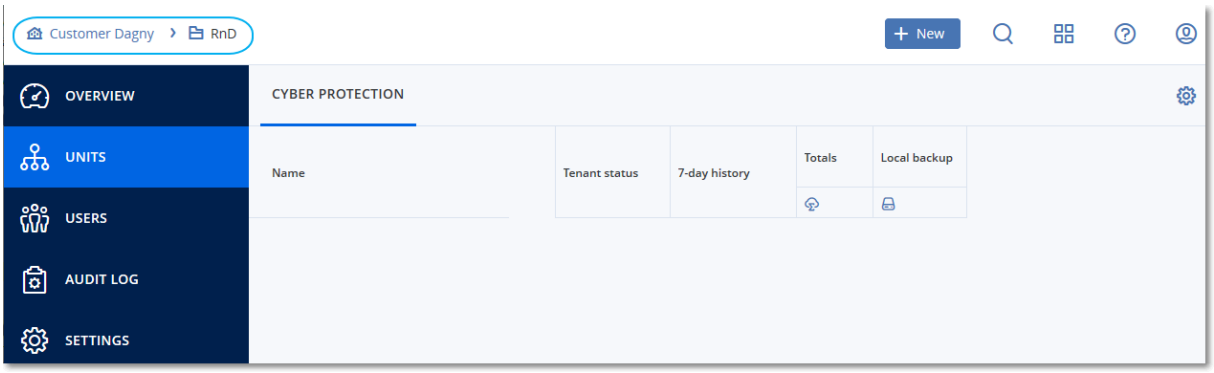
在管理入口網站和服務主控台之間切換

若要在管理入口網站和服務主控台之間切換，按一下右上角的 圖示，然後選擇 **[管理入口網站]** 或您要前往的服務。

在管理入口網站內瀏覽

使用管理入口網站時，不論何時您都是在某個公司或單位內操作。此資訊會在左上角顯示。

依預設，會選擇您可使用的最上層階層層級。按一下裝置名稱以向下鑽研階層。若要瀏覽回上層階層，請按一下它位於左上角的名稱。



使用者介面的所有部分只會顯示您正在操作的公司或單位，也只影響該公司或單位。例如：

- 藉著使用 **[新增]** 按鈕，您只能在此公司或單位內建立單位或使用者帳戶。
- **[單位]** 索引標籤只顯示此公司或單位的直接子單位。
- **[使用者]** 索引標籤只顯示此公司或單位內的使用者帳戶。

建立單位

如果您不將帳戶組織到單位內，則略過此步驟。

如果您打算稍候建立單位，請注意，現有帳戶無法在單位之間移動，也無法在公司和單位之間移動。首先，您必須建立一個單位，然後填入帳戶。

若要建立單位

1. 登入管理入口網站。
2. 瀏覽到您要建立新單位的單位。
3. 按一下右上角的 **[新增]** > **[單位]**。
4. 在 **[名稱]** 中，指定新單位的名稱。
5. [選用] 在 **[語言]** 中，變更此單位內所使用的通知、報告及軟體的預設語言。
6. 執行下列其中一項操作：
   - 若要建立單位系統管理員，請按一下 **[下一步]**，然後依照「建立使用者帳戶」中所述的步驟操作，從步驟 4 開始。

- 若要建立單位，但不建立系統管理員，請按一下 **[儲存並關閉]**。您可在稍後新增系統管理員和使用者到單位。

新建立的單位會出現在 **[單位]** 索引標籤上。

如果您要編輯單位設定或指定連絡資訊，請在 **[單位]** 索引標籤上選擇單位，然後按一下您要編輯的區段內的鉛筆圖示。

建立使用者帳戶

在下列情況中，您可能希望建立額外帳戶：

- 公司系統管理員帳戶 — 以便與其他人員分擔管理責任。
- 單位系統管理員帳戶 — 以便委派服務管理給其他存取權限嚴格限制為對應單位的人員。
- 客戶或單位租用戶內的使用者帳戶 — 以便讓使用者僅存取服務的子集。

建立使用者帳戶

1. 登入管理入口網站。
2. 瀏覽到您要建立新使用者帳戶的單位。
3. 按一下右上角的 **[新增]** > **[使用者]**。
   或者，前往 **[我的公司]** > **[使用者]**，然後按一下 **[+ 新增]**。
4. 為帳戶指定下列連絡資訊：
   - 如果您想要使用不同於電子郵件的登入，請選擇 **[使用不同於電子郵件的登入]** 核取方塊，然後輸入 **[登入]** 和 **[電子郵件]**。

     重要事項
     如果使用者已在 File Sync & Share 服務中註冊，請提供用於 File Sync & Share 註冊的電子郵件。
     請注意，每個客戶使用者帳戶都必須有唯一的電子郵件地址。

     重要事項
     每個帳戶都必須有唯一的登入。

   - [選用] **名字**
   - [選用] **姓氏**
   -
   - 在 **[語言]** 欄位中，變更將用於此帳戶的通知、報告及軟體的預設語言。
5. [選用] 指定公司聯絡人。
   - **[帳單]**—聯絡人，可取得有關平台使用情況報告重要變更的最新資訊。
   - **[技術]**—聯絡人，可取得有關平台重要技術變更的更新。
   - **[業務]**—聯絡人，可取得平台中重要業務相關變更的最新資訊。
     您可以為一個使用者指派多個公司聯絡人。
   您可以在 **[使用者]** 清單的 **[公司聯絡人]** 欄中檢視使用者獲指派的公司聯絡人，然後在需要時，編輯使用者帳戶以變更公司聯絡人。

6. [在合作夥伴/資料夾租用戶中建立帳戶時不適用]選擇使用者可以存取的服務，以及每個服務中的角色。

   可用服務取決於建立使用者帳戶的租用戶所啟用的服務。

   - 如果您選擇 **[公司系統管理員]** 核取方塊，使用者將能夠存取管理入口網站和目前針對該租用戶啟用的所有服務中的系統管理員角色。在未來針對該租用戶啟用的所有服務中，使用者也會擁有系統管理員角色。
   - 如果您選擇 **[單位系統管理員]** 核取方塊，使用者將能夠存取管理入口網站，但不一定擁有服務系統管理員角色，端視服務而定。
   - 否則，使用者將擁有您在針對該使用者啟用的服務中指派的角色。
7. 按一下 **[建立]**。

新建立的使用者帳戶會出現在 **[我的公司]** 下的 **[使用者]** 索引標籤上。

如果您要編輯使用者設定，或指定通知設定和使用者的配額 (不適用於合作夥伴/資料夾系統管理員)，請在 **[使用者]** 索引標籤上選擇使用者，然後在您要編輯的區段內按一下鉛筆圖示。

重設使用者密碼

1. 在管理入口網站中，前往 **[我的公司]** > **[使用者]**。
2. 選擇您要重設其密碼的使用者，然後按一下省略符號圖示 > **[重設密碼]**。
3. 按一下 **[重設]**，確認您的動作。

使用者現在可以依照所收到電子郵件中的指示，完成重設程序。

此帳戶現在可以用於不支援雙重驗證機制的服務 (例如，在 Cyber Infrastructure 中註冊)，您可能需要將使用者帳戶轉換為*服務帳戶*，也就是不需要使用雙重驗證機制的帳戶。

對於不支援雙重驗證機制的服務 (例如，在 Cyber Infrastructure 中註冊)，您可能需要將使用者帳戶轉換為服務帳戶，也就是不需要使用雙重驗證機制的帳戶。

若要將使用者帳戶轉換為服務帳戶

1. 在管理入口網站中，前往 **[我的公司]** > **[使用者]**。
2. 選擇您要將其帳戶轉換為服務帳戶類型的使用者，然後按一下省略符號圖示 > **[標示為服務帳戶]**。
3. 在確認視窗中，輸入雙重驗證機制代碼並確認您的動作。

該帳戶現在已可供不支援雙重驗證機制的服務使用。

適用於每個服務的使用者角色

一個使用者可以有數個角色，但每個服務只能有一個角色。

您可以針對每個服務，定義將指派給使用者的角色。

注意事項
您可使用的服務是由您的服務提供者所設定。

服務	角色	描述
不適用	公司系統管理員	此角色授予所有服務的完整系統管理員權限。 此角色可授予對公司允許名單的存取權。如果為公司啟用防護服務的 Disaster Recovery 附加元件，此角色也可以授予對災難復原功能的存取權。
管理入口網站	系統管理員	此角色可授予對管理入口網站的存取權，讓系統管理員可以在其中管理整個組織內的使用者。
	唯讀系統管理員 合作夥伴等級	此角色對合作夥伴管理入口網站中的所有物件以及此合作夥伴所有客戶的管理入口網站，提供唯讀存取權。此類使用者可以在唯讀模式下，存取組織其他使用者的資料。他們可以編輯保護計劃，但他們無法儲存對指令碼編寫計劃、監控計劃或代理程式計劃所做的任何變更。
	唯讀系統管理員 客戶層級	此角色會針對整個公司之管理入口網站中的所有物件提供唯讀存取權。這類使用者可以在唯讀模式下存取組織其他使用者的資料。
	唯讀系統管理員 單位層級	此角色會針對公司單位和子單位之管理入口網站中的所有物件提供唯讀存取權。這類使用者可以在唯讀模式下存取組織其他使用者的資料。
廠商入口網站	開發人員	此角色可以完整存取廠商入口網站。開發人員可以建立並管理 CyberApp、CyberApp Descriptions 和 CyberApp Versions。他們也可以提交部署要求並監控 CyberApp 指標。
	使用者	此角色可讓使用者建立、管理 CyberApp Descriptions，並要求其核准。
	唯讀使用者	此角色可以唯讀方式存取廠商入口網站。

保護	系統管理員	此角色允許為您的客戶設定和管理防護服務。 執行以下操作時，需要此角色： • 設定和管理Disaster Recovery功能。 • 設定和管理公司允許名單。 • 執行裝置的自動探索。 • 使用 DeployPilot 執行與軟體部署相關的所有動作 (使用軟體部署計劃、軟體存放庫、軟體套件，並執行快速部署動作)。
	網路系統管理員	除了系統管理員角色權限之外，此角色還允許在 [網路指令碼撰寫] 中設定並管理防護服務，以及核准動作。 Cyber 系統管理員角色僅適用於已啟用 Advanced Management 組件的租用戶。
	唯讀系統管理員	此角色會針對防護服務的所有物件提供唯讀存取權。這類使用者可以在唯讀模式下存取組織其他使用者的資料。 唯讀系統管理員無法設定和管理Disaster Recovery功能或公司允許名單，且僅能以唯讀方式存取軟體部署計劃、軟體存放庫和軟體套件。
	使用者	此角色允許使用 Protection 服務，但是沒有系統管理權限。可存取 Endpoint Detection and Response 等功能，但獲指派此角色的使用者無法存取組織中其他使用者的資料。
	還原運算子	此角色可存取 Microsoft 365 和 Google Workspace 組織的備份，並允許其復原，同時可限制對敏感內容的存取。
安全性分析人員	只能在已啟用 Advanced Security + EDR 或 Advanced Security + XDR 套件的客戶租用戶中指派此角色。此角色可存取資安防護主控台，以及讓使用者管理 EDR 事件並執行回應動作。	
File Sync & Share	系統管理員	此角色允許為您的使用者設定和管理 File Sync & Share。
Cyber Infrastructure	系統管理員	此角色允許為您的使用者設定和管理 Cyber Infrastructure。

Notary	系統管理員	此角色允許為您的使用者設定和管理 Notary。
	使用者	此角色允許使用 Notary 服務，但是沒有系統管理權限。這類使用者無法存取組織其他使用者的資料。

唯讀系統管理員角色

擁有此角色的帳戶對於 Cyber Protect 主控台具有唯讀存取權，而且可以執行以下操作：

- 收集系統報告之類的診斷資料。
- 查看備份的復原點，但無法向下鑽研至備份內容，而且無法查看檔案、資料夾或電子郵件。

唯讀系統管理員無法執行以下操作：

- 開始或停止工作。
  例如，唯讀系統管理員無法開始復原或停止執行中的備份。
- 存取來源或目標電腦上的檔案系統。
  例如，唯讀系統管理員無法查看備份電腦上的檔案、資料夾或電子郵件。
- 變更任何設定。
  例如，唯讀系統管理員無法建立保護計劃或變更其任何設定。
- 建立、更新或刪除任何資料。
  例如，唯讀系統管理員無法刪除備份。

系統會隱藏唯讀系統管理員無法存取的所有 UI 物件，但保護計劃的預設設定除外。這些設定會顯示初來，但 **[儲存]** 按鈕未處於啟用狀態。

與帳戶和角色相關的任何變更都會顯示在 **[活動]** 索引標籤上，並包含下列詳細資料：

- 已變更的項目
- 變更者
- 變更日期和時間

還原操作員角色

此角色僅適用於防護服務，且限制為 Microsoft 365 和 Google Workspace 備份。

還原操作員可以執行下列作業：

- 檢視警示與活動。
- 瀏覽並重新整理備份清單。
- 在不存取備份內容的情況下瀏覽備份。還原操作員可以看到備份檔案的名稱，以及備份電子郵件的主旨和寄件者。
- 搜尋備份 (不支援全文檢索)。
- 在原始 Microsoft 365 或 Google Workspace 組織中，將雲端對雲端備份復原到其原始位置。

還原操作員無法執行下列作業：

- 刪除警示。
- 新增或刪除 Microsoft 365 或 Google Workspace 組織。
- 新增、刪除或重新命名備份位置。
- 刪除或重新命名備份。
- 將備份復原至自訂位置時，建立、刪除或重新命名資料夾。
- 套用備份計劃或執行備份。
- 存取備份的檔案或備份信箱的內容。
- 下載備份的檔案或電子郵件附件。
- 將備份的雲端資源 (例如電子郵件或行事曆項目) 當作電子郵件傳送。
- 檢視或復原 Microsoft 365 Teams 對話。
- 將雲端對雲端備份復原到非原始位置，例如，不同的信箱、OneDrive、Google 雲端硬碟或 Microsoft 365 Team。

變更使用者的通知設定

若要變更使用者的通知設定，請導覽至 **[我的公司]** > **[使用者]**。選擇您要為其設定通知的使用者，然後按一下 **[設定]** 區段中的鉛筆圖示。如果建立使用者所在的租用戶啟用 Cyber Protection 服務，可以使用下列通知設定：

- **維護通知** — 通知合作夥伴使用者、子租用戶 (合作夥伴和客戶) 以及個人使用者有關即將在 Cyber Protect 資料中心進行的維護活動的通知。這些通知可以由合作夥伴使用者為其子租用戶啟用，也可以由合作夥伴使用者或公司系統管理員為其組織內的個人使用者啟用。
- **配額過度使用通知** — 有關超出配額的通知。
- **已排程的使用報告** — 在每個月的第一天傳送的使用報告。
- **URL 商標通知** — 憑證即將到期的通知，用於 Cyber Protect Cloud 服務的自訂 URL。這些通知會在憑證到期前的 30 天、15 天、7 天、3 天和 1 天傳送給所選租用戶的所有系統管理員。
- **失敗通知**、**警告通知**和**成功通知** — 關於每個裝置的保護計劃執行結果以及災難復原作業結果的通知。
- **作用中警示的相關每日摘要** — 每日摘要是在產生摘要時，根據 Cyber Protect 主控台中呈現的作用中警示清單所產生。系統會在每天的 10:00 到 23:59 UTC 之間產生並傳送摘要一次。報告產生並傳送的時間取決於資料中心的工作負載。如果當時沒有作用中警示，則不會傳送摘要。摘要不包含不再是作用中之過去警示的資訊。例如，如果使用者找到失敗的備份並清除警示，或在產生摘要前已重試備份且成功，則該警示將不會再出現，因此摘要中將不會包含該警示。
- **裝置控制通知** — 裝置控制模組啟用時，對於嘗試使用受保護計劃限制之週邊裝置和連接埠的通知。
- **復原通知** — 關於下列資源的復原動作的通知：使用者電子郵件訊息和整個信箱、公用資料夾，OneDrive / GoogleDrive：整個 OneDrive 和檔案或資料夾、SharePoint 檔案，Teams：頻道、整個小組、電子郵件訊息和小組網站。

  在這些通知的內容中，會將下列動作視為復原動作：以電子郵件傳送、下載或開始復原作業。
- **資料洩漏防禦通知** — 與網路上此使用者活動相關之資料洩漏防禦警示的通知。
- **安全性事件通知** — 有關主動即時、執行時和按需掃描期間偵測到惡意軟體的通知，以及有關來自行為引擎和 URL 篩選引擎的偵測的通知。

注意事項
安全性事件通知僅會傳送給擁有受保護裝置的使用者。

有兩個可用的選項：**[已緩解]** 和 **[未緩解]**。這些選項與 Endpoint Detection and Response (EDR) 事件警示、來自威脅摘要的 EDR 警示，以及個別警示 (針對未對其啟用 EDR 的工作負載) 相關。

建立 EDR 警示時，相關使用者會收到一封電子郵件。如果事件的威脅狀態變更，就會傳送新的電子郵件。這些電子郵件所包含的動作按鈕可讓使用者查看事件的詳細資料 (如果已緩解)，或調查並修復事件 (如果未緩解)。

- **基礎架構通知** — 有關Disaster Recovery基礎架構問題的通知：當Disaster Recovery基礎架構無法使用時或 VPN 通道無法使用時。

所有通知將傳送至使用者的電子郵件地址。

按通知類型和使用者角色啟用的預設通知設定

預設啟用或停用的通知取決於通知類型和使用者角色。

通知類型\使用者角色	客戶、單位系統管理員 (自助服務)	客戶、單位系統管理員 (由服務提供者管理)
維護通知	否	否
配額過度使用通知	是	否
已排程的使用報告通知	是	否
URL 商標通知	否	否
失敗通知	否	否
警告通知	否	否
成功通知	否	否
作用中警示的相關每日摘要	是	否
裝置控制通知	否	否
復原通知	否	否
資料洩漏防禦通知	否	否
安全性事件通知：已緩解	否	否
安全性事件通知：未緩解	否	否
基礎架構通知	否	否

按裝置類型和使用者角色劃分的預設通知設定 (啟用/停用)

裝置類型\使用者角色	使用者	客戶系統管理員
適用於自攜裝置的通知	是	是
適用於組織中所有裝置的通知	不適用	是 (但 **[安全性事件通知]** 除外)
適用於 Microsoft 365、Google Workspace 和其他雲端式備份的通知	不適用	是

停用與啟用使用者帳戶

您可能需要停用使用者帳戶，才能暫時限制其對雲端平台的存取。

停用使用者帳戶

1. 在管理入口網站中，前往 **[使用者]**。
2. 選擇您要停用的使用者帳戶，然後按一下省略符號圖示 > **[停用]**。
3. 按一下 **[停用]**，確認您的動作。

因此，此使用者將無法使用雲端平台，也無法接收任何通知。

若要啟用已停用的使用者帳戶，請在使用者清單中選擇該使用者帳戶，然後按一下省略符號圖示 > **[啟用]**。

刪除使用者帳戶

您可能需要永久刪除某個使用者帳戶，才能釋出其所使用的資源，例如儲存空間或授權。使用狀況統計資料將在刪除後的一天內更新。若是含有大量資料的帳戶，可能需要更久的時間。

注意事項
刪除使用者後，您可以重複使用已刪除使用者的登入。

刪除使用者帳戶之前，您必須先將其停用。如需有關操作方式的詳細資訊，請參閱「停用與啟用使用者帳戶」。

刪除使用者帳戶

1. 在管理入口網站中，前往 **[使用者]**。
2. 選擇已停用的使用者帳戶，然後按一下省略符號圖示 > **[刪除]**。
3. 若要確認您的動作，輸入登入，然後按一下 **[刪除]**。

結果：

- 針對此帳戶設定的所有通知都將遭到停用。
- 屬於此使用者帳戶的所有資料都將遭到刪除。
- 系統管理員將無法存取管理入口網站。
- 與此使用者相關聯的工作負載的所有備份都將遭到刪除。
- 與此使用者帳戶相關聯的所有電腦都將遭到取消註冊。
- 所有保護計劃都將會從與此使用者相關聯的所有工作負載撤銷。
- 屬於此使用者的所有 File Sync & Share 資料 (例如，檔案和資料夾) 都將遭到刪除。
- 屬於此使用者的 Notary 資料 (例如公證檔案、電子簽名檔案) 將會遭到刪除。
- 您會看到使用者**狀態**為**已刪除**。當您將滑鼠暫留在**已刪除**的狀態時，會看見使用者遭刪除的日期。請注意，您仍然可以在此刪除日期的 30 天內復原所有相關的資料和設定。

轉移使用者帳戶的所有權

如果您要保留對受限使用者資料的存取權，可能需要轉移該使用者帳戶的所有權。

重要事項
您無法重新指派已刪除帳戶的內容。

轉移使用者帳戶的所有權：

1. 在管理入口網站中，前往 **[使用者]**。
2. 選擇您要轉移其所有權的使用者帳戶，然後按一下 **[一般資訊]** 區段中的鉛筆圖示。
3. 將現有的電子郵件取代為未來帳戶擁有者的電子郵件，然後按一下 **[完成]**。
4. 按一下 **[是]**，確認您的動作。
5. 讓未來的帳戶擁有者依照其電子郵件地址所傳送的指示，驗證該電子郵件地址。
6. 選擇您要轉移其所有權的使用者帳戶，然後按一下省略符號圖示 > **[重設密碼]**。
7. 按一下 **[重設]**，確認您的動作。
8. 讓未來的帳戶擁有者依照傳送至其電子郵件地址的指示，重設密碼。

新的擁有者現在可以存取此帳戶。

設定雙重驗證機制

雙重驗證機制 (2FA) 是多重要素驗證的一種類型，可使用兩種不同要素的組合來檢查使用者身分：

- 使用者知道的某個東西 (PIN 或密碼)
- 使用者擁有的某個東西 (權杖)
- 使用者的某個東西 (生物識別)

雙重驗證機制提供額外的保護，使未經授權者無法存取您的帳戶。

此平台支援**基於時間的一次性密碼 (TOTP)** 驗證。如果在系統中啟用 TOTP 驗證，使用者必須輸入其傳統密碼以及一次性的 TOTP 代碼，才能存取系統。換句話說，使用者要提供密碼 (第一個要素)

和 TOTP 代碼 (第二個要素)。TOTP 代碼是在使用者第二要素裝置上，根據平台提供的目前時間和密碼 (QR 碼或英數字代碼)，在驗證應用程式中產生的。

注意事項

對於實際運作模式下的合作夥伴租用戶，預設會啟用雙重驗證機制，且無法停用。

對於客戶租用戶，雙重驗證機制是選擇性的，而且可以停用。

運作原理

1. 您可以在組織層級啟用雙重驗證機制。
2. 所有組織使用者都必須在其第二要素裝置 (行動電話、筆記型電腦、桌上型電腦或平板電腦) 上安裝驗證應用程式。此應用程式將用於產生一次性 TOTP 代碼。建議的驗證器：
   - Google Authenticator
     iOS 應用程式版本 (https://apps.apple.com/app/google-authenticator/id388497605)
     Android 版本 (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)
   - Microsoft Authenticator
     iOS 應用程式版本 (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Android 版本 (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   重要事項

   使用者必須確保安裝驗證應用程式所在裝置上的時間設定正確，並反映實際的目前時間。
3. 您的組織使用者必須重新登入系統。
4. 輸入其登入和密碼之後，系統將會提示他們為其使用者帳戶設定雙重驗證機制。
5. 他們必須使用其驗證應用程式掃描 QR 碼。如果無法掃描 QR 碼，他們可以使用 QR 碼下方所顯示的 32 位數代碼，並在驗證應用程式中手動新增該代碼。

   重要事項

   強烈建議您儲存該代碼 (列印 QR 碼、寫下臨時一次性密碼 (TOTP)、使用支援在雲端備份代碼的應用程式)。遺失第二要素裝置時，您將需要臨時一次性密碼 (TOTP)，才能重設雙重驗證機制。
6. 臨時一次性密碼 (TOTP) 代碼將會在驗證應用程式中產生。該代碼每 30 秒鐘會自動重新產生。
7. 輸入密碼後，使用者必須在 **[設定雙重驗證機制]** 視窗上輸入 TOTP 代碼。
8. 因此，將會設定使用者的雙重驗證機制。

現在，當使用者登入系統時，系統會要求他們提供登入和密碼，以及在驗證應用程式中產生的一次性 TOTP 代碼。使用者可以在登入系統時將瀏覽器標示為受信任，之後透過此瀏覽器登入時，就不會再要求 TOTP 代碼。

若要在新裝置上還原雙重驗證機制

如果您可以存取先前設定的行動版驗證應用程式：

1. 在新裝置上安裝驗證器應用程式。
2. 使用您在裝置上設定 2FA 時所儲存的 PDF 檔案。此檔案包含 32 位數驗證碼，您必須在驗證器應用程式中輸入這個驗證碼，才能將驗證器應用程式再次連結到您的 Acronis 帳戶。

   重要事項
   如果驗證碼正確但沒有作用，請務必同步驗證器行動版應用程式中的時間。

3. 如果您在設定期間錯過了儲存 PDF 檔案：

a. *按一下* ***[重設 2FA]****，然後輸入顯示在先前設定的行動版驗證器應用程式中的一次性密碼。*
b. 依照畫面上的說明操作。

如果您無法存取先前設定的行動版驗證器應用程式：

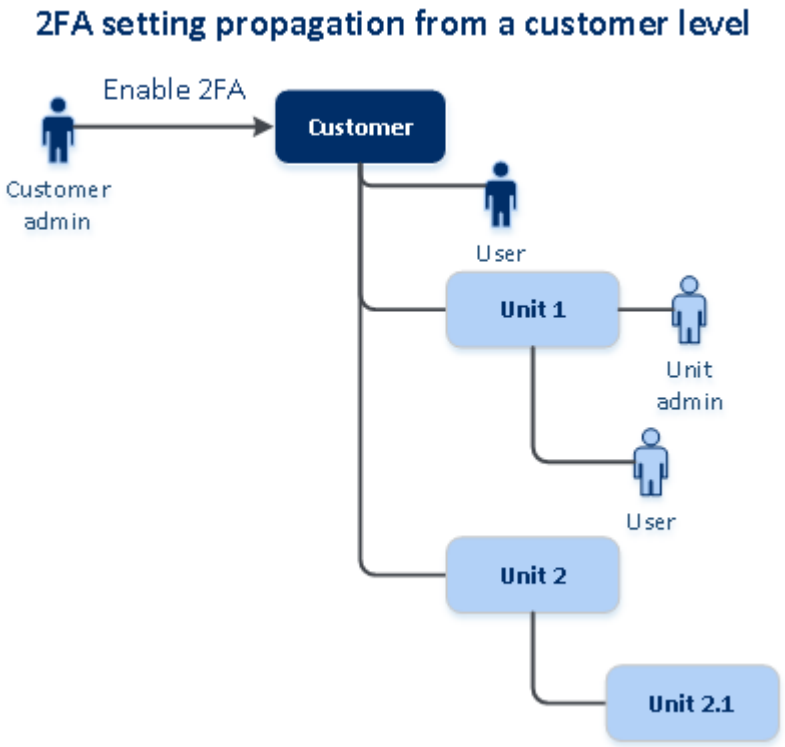
1. 拿一個新的行動裝置。
2. 使用已儲存的 PDF 檔案連結新裝置 (此檔案的預設名稱為 `cyberprotect-2fa-backupcode.pdf`)。
3. 從備份還原對您帳戶的存取權。請確認您的行動版應用程式支援備份。
4. 從另一個行動裝置 (如果受到應用程式支援) 使用相同的帳戶開啟應用程式。

跨租用戶層級的雙重要素設定傳播

雙重驗證機制是在**組織**層級設定的。您僅能針對自己的組織設定雙重驗證機制。

雙重驗證機制設定會跨租用戶層級傳播，如下所示：

- 單位會從其客戶組織自動繼承雙重驗證機制設定。



注意事項

1. 在單位層級上無法設定雙重驗證機制。
2. 您可以為子組織 (單位) 的使用者管理雙重驗證機制設定。

為您的租用戶設定雙重驗證機制

身為公司系統管理員的您可以為組織中的使用者啟用雙重驗證機制。

若要啟用雙重驗證機制

所需的角色:公司系統管理員

1. 登入管理入口網站。
2. 前往 **[設定]** > **[安全性]**。
3. 滑動 **[雙重身份驗證]** 切換開關,然後按一下 **[啟用]**。

現在,組織中的所有使用者都必須為其帳戶設定雙重身份驗證。當他們下次嘗試登入或目前工作階段過期時,系統將提示他們執行此操作。

開關下方的進度列顯示了為其帳戶設定雙重身份驗證的使用者數。若要檢查哪些使用者已經設定其帳戶,請導覽至 **[我的公司]** > **[使用者]** 索引標籤,並檢查 **[雙重驗證機制狀態]** 欄。尚未為其帳戶設定雙重身份驗證的使用者的 2FA 狀態為 **[需要設定]**。

在成功設定雙重身份驗證之後,使用者每次登入服務主控台時必須輸入其登入名稱、密碼和 TOTP 代碼。

若要停用雙重驗證機制

所需的角色:公司系統管理員

1. 登入管理入口網站。
2. 前往 **[設定]** > **[安全性]**。
3. 要停用雙重身份驗證,請關閉切換開關,然後按一下 **[停用]**。
4. [如果至少有一個使用者在組織內設定雙重驗證機制] 在行動裝置上輸入在驗證應用程式中產生的 TOTP 代碼。

因此,系統會為組織停用雙重驗證機制、刪除所有密碼,並忘記所有受信任的瀏覽器。所有使用者都將只能使用自己的登入和密碼登入系統。在 **[我的公司]** > **[使用者]** 索引標籤上,將會隱藏 **[雙重驗證機制狀態]** 欄。

為使用者管理雙重驗證機制

您可以監控您所有使用者的雙重驗證機制設定,並在管理入口網站的 **[我的公司]** > **[使用者]** 索引標籤下重設設定。

監控

在管理入口網站的 **[我的公司]** > **[使用者]** 索引標籤下，您可以看到貴組織中所有使用者的清單。**[雙重驗證機制狀態]** 會指出是否已為使用者設定雙重要素設定。

若要為使用者重設雙重驗證機制

1. 在管理入口網站中，前往 **[我的公司]** > **[使用者]**。
2. 在 **[使用者]** 索引標籤上，尋找您要變更其設定的使用者，然後按一下省略符號圖示。
3. 按一下 **[重設雙重驗證機制]**。
4. 在第二要素裝置上輸入在驗證應用程式中產生的 TOTP 代碼，然後按一下 **[重設]**。

因此，使用者將可以再次設定雙重驗證機制。

若要為使用者重設受信任的瀏覽器

1. 在管理入口網站中，前往 **[我的公司]** > **[使用者]**。
2. 在 **[使用者]** 索引標籤上，尋找您要變更其設定的使用者，然後按一下省略符號圖示。
3. 按一下 **[重設所有受信任的瀏覽器]**。
4. 在第二要素裝置上輸入在驗證應用程式中產生的 TOTP 代碼，然後按一下 **[重設]**。

您已經重設其所有受信任瀏覽器的使用者將必須在下次登入時提供 TOTP 代碼。

使用者可以自行重設所有受信任的瀏覽器，並重設雙重驗證機制設定。這可以在他們登入系統時，按一下個別的連結，然後輸入 TOTP 代碼以確認作業來完成。

若要為使用者停用雙重驗證機制

不建議停用雙重驗證機制，因為這可能會破壞租用戶安全性。

但是，您可以針對某個使用者停用雙重驗證機制，並針對其他所有租用戶使用者保留雙重驗證機制。如果在設定雲端整合的用戶端中啟用雙重驗證機制，而且此整合透過使用者帳戶 (登入密碼) 授權給平台，則可以使用此方法作為因應措施。若要繼續使用整合作為臨時解決方案，可以將使用者轉換到不適用雙重驗證機制的服務帳戶中。

重要事項
不建議將一般使用者轉換成服務使用者來停用雙重驗證機制，因為這會對租用戶的安全性構成威脅。

若要在不針對租用戶停用雙重驗證機制的情況下使用雲端整合，建議的安全解決方案是建立 API 用戶端，並將雲端整合設定為搭配這些 API 用戶端使用。

1. 在管理入口網站中，前往 **[我的公司]** > **[使用者]**。
2. 在 **[使用者]** 索引標籤上，尋找您要變更其設定的使用者，然後按一下省略符號圖示。
3. 按一下 **[標示為服務帳戶]**。因此，使用者會獲得一個稱為**服務帳戶**的特殊雙重驗證機制狀態。
4. [如果某個租用戶中至少有一個使用者已經設定雙重驗證機制] 在第二要素裝置上輸入在驗證應用程式中產生的 TOTP 代碼以確認停用。

若要為使用者啟用雙重驗證機制

您可能需要針對您先前已經為其停用雙重驗證機制的特定使用者啟用雙重驗證機制。

1. 在管理入口網站中，前往 **[我的公司]** > **[使用者]**。
2. 在 **[使用者]** 索引標籤上，尋找您要變更其設定的使用者，然後按一下省略符號圖示。
3. 按一下 **[標示為一般帳戶]**。因此，使用者將需要設定雙重驗證機制，或在進入系統時提供 TOTP 代碼。

在遺失第二要素裝置時重設雙重驗證機制

若要在遺失第二要素裝置時重設您帳戶的存取權，請依照下列其中一個建議的方法進行：

- 從備份還原您的 TOTP 密碼 (QR 碼或英數字代碼)。
  使用其他第二要素裝置，並在此裝置上安裝的驗證應用程式中新增已儲存的 TOTP 密碼。
- 要求系統管理員為您重設雙重驗證機制設定。

暴力密碼破解保護

暴力密碼破解攻擊是在入侵者透過提交許多密碼，並希望猜中其中一個密碼來嘗試取得系統存取權時的一種攻擊。

平台的暴力密碼破解保護機制是以裝置 Cookie 為基礎。

平台所使用的暴力密碼破解保護設定是經過預先定義的：

參數	輸入密碼	輸入 TOTP 代碼
嘗試次數限制	10	5
嘗試次數限制期限 (此限制會在逾時後重設)	15 分鐘 (900 秒)	15 分鐘 (900 秒)
鎖定發生時機	嘗試次數限制 +1 (第 11 次嘗試)	嘗試次數限制
鎖定期限	5 分鐘 (300 秒)	5 分鐘 (300 秒)

如果您已經啟用雙重驗證機制，則只會在使用雙重要素 (密碼和 TOTP 代碼) 成功驗證之後，才會將裝置 Cookie 發給用戶端 (瀏覽器)。

若是受信任的瀏覽器，則會在僅使用單一要素 (密碼) 成功驗證之後，發出裝置 Cookie。

TOTP 代碼輸入嘗試次數是針對每個使用者，而非每個裝置登錄的。也就是說，即使使用者嘗試使用不同的裝置輸入 TOTP 代碼，他們仍然會遭到封鎖。

設定 Cyber Protection 代理程式的自動更新

重要事項
若已啟用 保護 服務，則可存取代理程式更新管理功能。

Cyber Protect 包含三種可以安裝在受保護電腦上的代理程式類型：Windows 用代理程式、Linux 用代理程式和 Mac 用代理程式。

Cyber Files Cloud 包含 Windows 版本和 MacOS 版本的 File Sync & Share 用桌面代理程式，可同步電腦和使用者 File Sync & Share 雲端儲存空間區域間的檔案和資料夾以提升離線工作，以及 WFH (居家辦公) 和 BYOD (攜帶您自己的裝置) 工作方式。

若要簡化多個工作負載的管理，您可以對所有電腦上的所有代理程式，設定或停用自動更新。

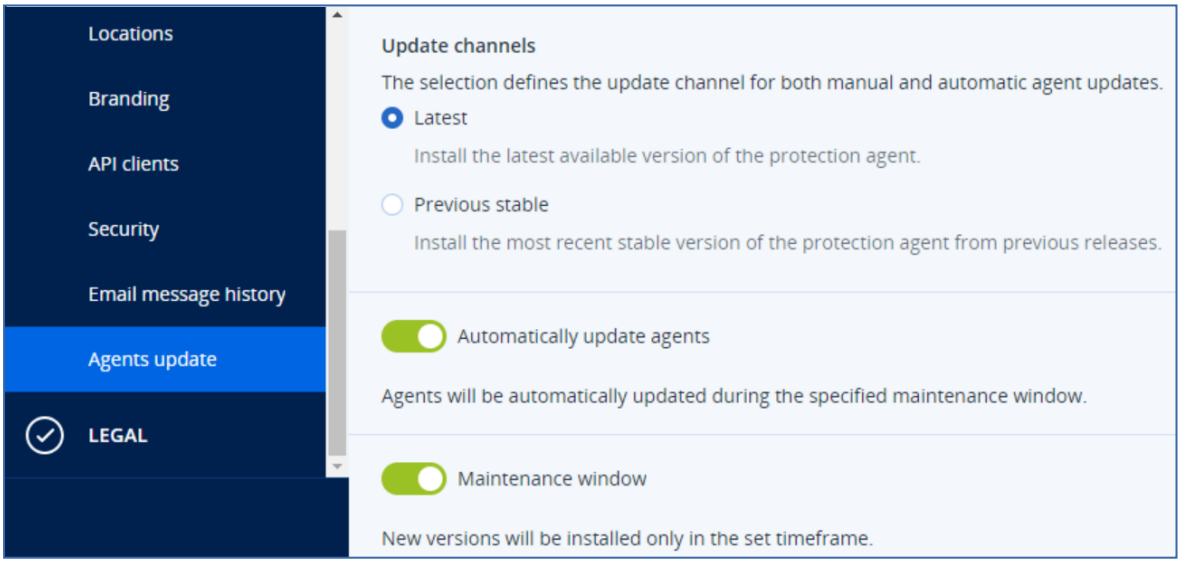
注意事項
若要管理個別電腦上的代理程式，並自訂自動更新設定，請參閱 Cyber Protect 使用指南上的更新代理程式一節。

若要自動更新代理程式

注意事項
如果您未啟用 [保護] 服務，則自動更新 File Sync & Share 用代理程式的設定將繼承自您的服務提供者。

若要從管理入口網站設定代理程式的自動更新

1. 選擇 **[設定] > [代理程式更新]**。



2. 選擇要偵測自動更新的版本。

選項	描述
最新 (預設選擇)	安裝可用的最新版 Cyber Protection 代理程式。
上一個穩定版本	從先前版本安裝最新的穩定版 Cyber Protection 代理程式。

3. 請確認 **[自動更新代理程式]** 選項是否已開啟。
   此選項預設為開啟狀態。

4. 設定維護時段。
   (預設是從 23:00 到 08:00)。

   注意事項
   儘管代理程式更新程序旨在快速無縫，但我們還是建議選擇對使用者造成最小干擾的時段，因為使用者無法阻止或延後自動更新。

5. [選用] 選擇要進行自動更新的具體日期。
6. 選擇 **[儲存]**。

注意事項
自動更新僅適用於：

- Cyber Protect 代理程式 15.0.26986 (2021 年 5 月發行) 版或更新版本。
- File Sync & Share 用桌面代理程式 15.0.30370 版或更新版本。

舊版代理程式則必須先手動更新至最新版本，自動更新才會生效。

若要監控代理程式更新

重要事項
只有在您已啟用 [保護] 模組的情況下，才能監控代理程式更新。

若要監控代理程式更新，請參閱 Cyber Protect 使用指南的「警示」和「活動」章節。

固定儲存空間

固定儲存空間是一種資料儲存類型，可在指定期間內防止備份遭到變更、修改或刪除。它可確保資料保持安全且無法竄改，從而提供額外一層保護，以防止未經授權或意外修改或勒索軟體攻擊。固定儲存空間可用於儲存在支援的雲端儲存空間執行個體中的所有雲端備份。請參閱 "支援的儲存空間和代理程式" (第 35 頁)。

固定儲存空間可讓您在指定的保留期間內存取已刪除的備份。您可從這些備份中復原內容，但無法變更、移動或刪除。當保留期限結束後，將永久刪除已刪除的備份。

不可固定儲存空間下列備份：

- 手動刪除的備份。
- 根據保護計劃的 **[保留時間]** 區段中的設定，或清理計劃的 **[保留規則]** 區段中的設定，自動刪除的備份。

固定儲存空間中已刪除的備份仍然會使用儲存空間，並據以收費。

已刪除的租用戶無需支付任何儲存空間費用，包括固定儲存空間。

固定儲存空間模式

客戶系統管理員可停用及重新啟用固定儲存空間，以及變更其模式和保留期限。

固定儲存空間可在下列模式中使用：

- **治理模式**
  您可以停用後再重新啟用固定儲存空間。您可以變更保留期間或切換到 [合規] 模式。

  注意事項
  從 2024 年 9 月開始，可能會自動為您的公司啟用保留期限為 14 天的固定儲存空間治理模式。如需詳細資訊，請洽詢服務提供者。

- **合規模式**

  警告！
  選擇 [合規] 模式是不可逆的。

  您無法停用固定儲存空間。您無法變更保留期間，也無法切換回 [治理] 模式。

支援的儲存空間和代理程式

- 僅雲端儲存空間支援固定儲存空間。
  - 固定儲存空間適用於使用 Cyber Infrastructure 4.7.1 版或更新版本的 Acronis 託管和合作夥伴託管的雲端儲存空間。
  - 支援可以搭配 Cyber Infrastructure Backup Gateway 使用的所有儲存空間。例如， Cyber Infrastructure 儲存體、Amazon S3 和 EC2 儲存體以及 Microsoft Azure 儲存體。
  - 固定儲存空間要求為 Cyber Infrastructure 中的 Backup Gateway 服務開放 TCP 連接埠 40440。在 4.7.1 版和更新版本中，會自動透過 **[Backup (ABGW) 公用]** 流量類型開放 TCP 連接埠 40440。如需有關流量類型的詳細資訊，請參閱 Acronis Cyber Infrastructure 文件。
- 固定儲存空間需要保護代理程式版本 21.12 (組建 15.0.28532) 或更高版本。
- 僅支援 TIBX(版本 12) 備份。

設定固定儲存空間

2024 年 9 月之後，固定儲存空間治理模式預設為啟用狀態，保留期限為 14 天。如有需要，您可以為組織修改預設設定。

注意事項
為允許存取已刪除的備份，應該在備份儲存上，針對傳入連線啟用連接埠 40440。

若要變更保留期限或固定儲存空間模式

1. 以系統管理員身分，登入管理入口網站，然後移至 **[設定]** > **[安全性]**。
2. 請確認 **[固定儲存空間]** 開關是否開啟。
3. 在 14 到 3650 天範圍內指定保留期間。
   預設保留期間為 14 天。保留期間較長時，將會導致儲存空間使用量增加。
4. 選擇固定儲存空間模式，並在出現提示時，確認您的選擇。

- **治理模式**
  此模式可確保勒索軟體或惡意行為者無法竄改或刪除備份資料，因為所有已刪除的備份在您指定的保留期限內都會保留在固定儲存空間中。此外，它也可保證備份資料的完整性，這對於災難復原至關重要。
  在此模式下，您可以停用後再重新啟用固定儲存空間、變更保留期限或切換到合規模式。
- **合規模式**
  除了治理模式的優點外，合規模式還可以透過防止資料篡改，協助組織符合資料保留和安全性的法規要求。

  警告！
  選擇合規模式是不可逆的。選擇此模式後，您將無法停用固定儲存空間、變更保留期限，或切換回治理模式。

5. 按一下 **[儲存]**。

   警告！
   選擇 **[合規模式]** 是不可逆的。選擇此模式之後，您將無法停用固定儲存空間，也無法變更其模式或保留期間。

6. 若要將現有的存檔新增至固定儲存空間，請手動或排程執行對應的保護計劃，以便在該存檔中建立新的備份。

   警告！
   如果您在將存檔新增至固定儲存空間之前刪除備份，則該備份會遭到永久刪除。

停用固定儲存空間

1. 以系統管理員身分，登入管理入口網站，然後移至 **[設定]** > **[安全性]**。
2. 停用 **[固定儲存空間]** 開關。

   注意事項
   您只能在治理模式下停用固定儲存空間。

   警告！
   停用固定儲存空間不會立即生效。在 14 天的寬限期內，您可以根據其原始的保留期限，存取已刪除的備份。當寬限期結束後，固定儲存空間內的所有備份將遭到永久刪除。

3. 按一下 **[停用]**，確認您的選擇。

檢視固定儲存空間使用狀況

您可以在管理入口網站上產生的**目前使用狀況報告**中，檢視固定儲存空間使用的空間量。

限制

- 報告的值包括儲存空間中所有已刪除備份的大小總計以及備份存檔的中繼資料。中繼資料最多可達報告值的 10%。
- 此值會顯示在產生報告前最多 24 小時的使用狀況。
- 如果實際使用量少於 0.01 GB，則顯示為 0.0 GB。

若要檢視固定儲存空間使用狀況

1. 以系統管理員身分登入管理入口網站。
2. 前往 **[報告]** > **[使用狀況]**。
3. 選擇 **[目前使用狀況]**，然後按一下 **[產生並傳送]**。
   CSV 和 HTML 格式的報告隨即傳送至您的電子郵件地址。
   HTML 檔案會包含在 ZIP 存檔中。
4. 在報告中，勾選 **[計量名稱]** 欄。
   固定儲存空間使用狀況會顯示在 **[雲端儲存 - 固定]** 列中。

固定儲存空間的帳單範例

以下範例顯示一個已刪除的備份，該備份進入固定儲存空間 14 天，也就是預設的保留期限。在這段期間內，已刪除的備份可使用儲存空間。當保留期限結束後，已刪除備份將會遭到永久刪除，因此儲存空間使用量會減少。每個月都會據此收取儲存空間使用量的費用。

日期	備份	儲存空間使用情況	計費
4 月 1 日	建立備份 A (10 GB) 建立備份 B (1 GB)	10 GB + 1 GB = 11 GB	
4 月 20 日	備份 B 遭到刪除，進入固定儲存空間 (保留期限為 14 天)	10 GB + 1 GB = 11 GB	
4 月 30 日			針對 4 月份的 11 GB 收費
5 月 4 日	備份 B 因為保留期限結束而遭到永久刪除	11 GB - 1 GB = 10 GB	
5 月 31 日			針對 5 月份的 10 GB 收費

為您組織中的使用者啟用進階安全意識訓練

「安全意識訓練」由協力廠商 Wizer 提供，整合在 Cyber Protect Cloud 主控台中。如果您的服務提供者已為您的組織啟用此服務，則必須啟用整合，才能允許您的使用者存取訓練材料。

若要為組織啟用與 Wizer 的整合

所需角色：客戶系統管理員、保護系統管理員或資安系統管理員。

注意事項
此初始設定僅會執行一次。

1. 登入 Cyber Protect Cloud 主控台。
2. 在導覽功能表中，按一下 **[安全意識訓練]** > **[意識儀表板]**。
3. 按一下 **[啟用整合]**。
4. 按一下 **[啟用]** 以確認。

一旦已啟用整合，將在 Wizer 平台中為組織佈建新的租用戶。如果您在 Wizer 中已經有帳戶，且想要使用該帳戶而非新的租用戶，請聯絡您的服務提供者。

您可以存取 Wizer 系統管理員面板並手動新增使用者，方法是，匯入 CSV 檔案或使用 Active Directory、Octa、Google 或其他身分識別提供者設定 SSO。請參閱如何新增使用者。

限制 Web 介面的存取權

您可以指定 IP 位址清單，提供 Web 介面存取權給所列位址的使用者登入。

注意事項
此限制也適用於透過 API 存取管理入口網站。

注意事項
此限制只套用到設定該限制的層級。它*不*會套用到子單位的成員。

限制 Web 介面的存取權

1. 登入管理入口網站。
2. 瀏覽到您要限制存取的單位。
3. 按一下 **[設定]** > **[安全]**。
4. 選擇 **[啟用登入控制]** 核取方塊。
5. 在 **[允許的 IP 位址]** 中，指定允許登入的 IP 位址。
   您可以輸入下列任一參數，請使用分號區隔：
   - IP 位址，例如：192.0.2.0
   - IP 範圍，例如：192.0.2.0-192.0.2.255
   - 子網路，例如：192.0.2.0/24
6. 按一下 **[儲存]**。

限制存取您的公司

您可以針對更高層級的系統管理員，限制對公司的存取。

如果身為管理入口網站系統管理員的您限制對公司的存取，則您服務提供者合作夥伴的系統管理員僅能修改您公司的屬性和配額，並取得您公司和客戶的使用狀況報告。他們將無法存取：

- 您租用戶內的任何內容。
- 您的客戶、其使用者、服務、備份和其他資源。

若要限制對公司的存取

1. 登入管理入口網站。
2. 按一下 **[設定]** > **[安全]**。
3. 停用 **[支援存取]** 選項。

監控

若要存取有關服務使用狀況和作業的資訊，請按一下 **[監控]**。

用量

[使用狀況] 索引標籤提供服務使用狀況的概觀，並可讓您存取正在操作的租用戶內的服務。

使用狀況資料包括標準功能和進階功能。

重要事項

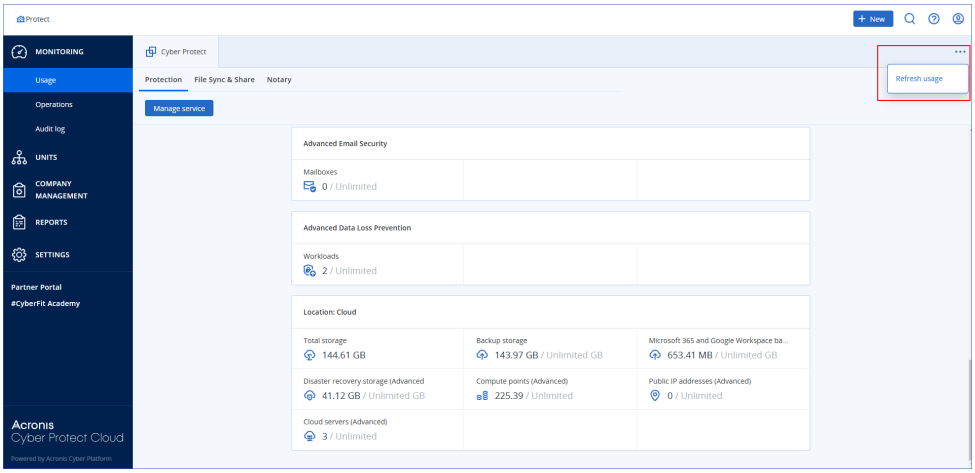
產品 UI 中顯示的儲存空間使用狀況值為二進位位元組單位 (Mebibytes (MiB)、Gibibytes (GiB) 及 Tebibytes (TiB))，即使標籤分別顯示 MB、GB 及 TB，也是如此。例如，如果實際使用量為 3105886629888 個位元組，則 UI 中顯示的值將正確顯示為 2.82，但標籤會標示為 TB 而非 TiB。

Microsoft 365 和 Google Workspace 工作負載的儲存空間使用狀況會與一般備份儲存使用狀況分開報告，並顯示在 **[Microsoft 365 和 Google Workspace 備份]** 區段下。

若要重新整理索引標籤上顯示的使用狀況資料，請按一下畫面右上角的省略符號圖示 (...)，然後選擇 **[重新整理使用狀況]**。

注意事項

擷取資料可能需要最多 10 分鐘的時間。重新載入頁面以查看更新的資料。



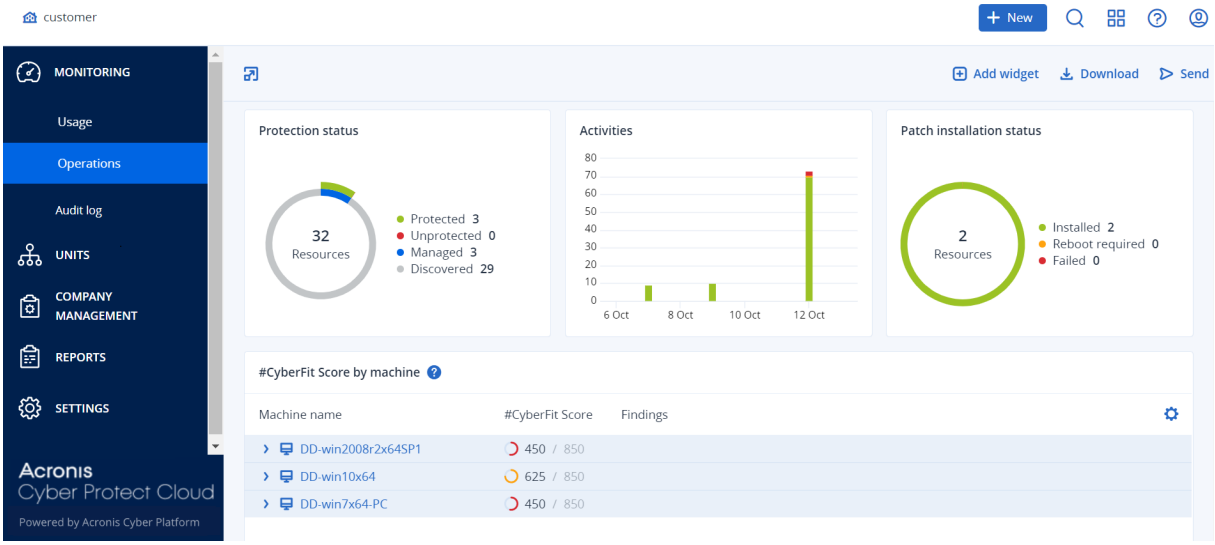
操作儀表板

[操作] 儀表板僅供公司系統管理員在公司層級上操作時使用。

[操作] 儀表板提供許多可自訂的桌面小工具，可概覽與 Cyber Protection 服務有關的作業。

系統會每兩分鐘更新一次動態小工具。動態小工具帶有可按一下的元素，可讓您調查問題並進行疑難排解。您可以透過 .pdf 和/或 .xlsx 格式下載最新狀態的儀表板或透過電子郵件進行傳送。

您可以從各種桌面小工具中選擇:顯示為表格、長條圖和樹狀圖。您可以新增具有不同篩選的相同類型動態小工具。



重新排列儀表板上的動態小工具

透過在動態小工具的名稱上按一下，可拖曳它們。

´編輯動態小工具

按一下動態小工具名稱旁的鉛筆圖示。編輯動態小工具可讓您將它重新命名、變更時間範圍，以及設定篩選。

新增動態小工具

按一下 **[新增動態小工具]**，然後執行下列其中一項操作：

- 按一下您要新增的動態小工具。接著會以預設設定新增動態小工具。
- 若要在新增之前編輯桌面小工具，請在選取桌面小工具時按一下鉛筆圖示。編輯動態小工具之後，按一下 **[完成]**。

移除動態小工具

按一下動態小工具名稱旁的 X 符號。

保護狀態

保護狀態

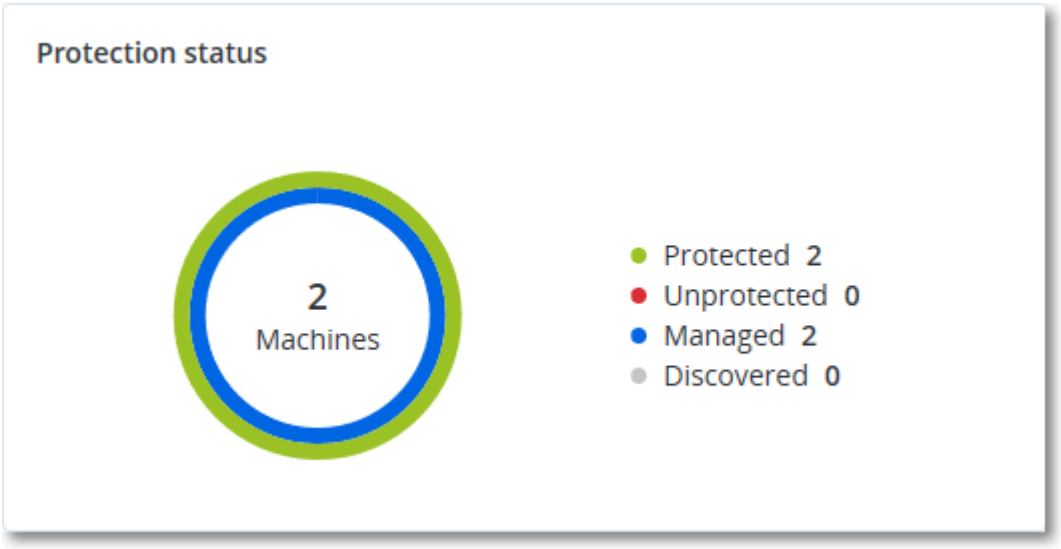
此桌面小工具會顯示所有電腦目前的保護狀態。

電腦可以為下列狀態之一：

- **受保護** – 已套用保護計劃的電腦。
- **未受保護** – 未套用保護計劃的電腦。這些包括已發現和受管理，但未套用保護計劃的電腦。

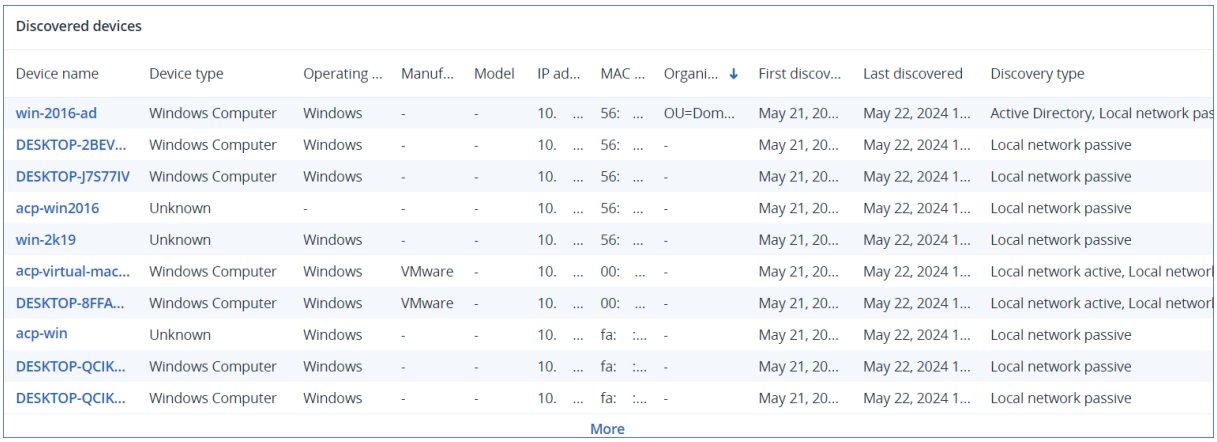
- **受管理** – 已安裝保護代理程式的電腦。
- **已探索** – 未安裝保護代理程式的電腦。

如果您按一下電腦狀態，系統會將您重新導向至具有此狀態之電腦的清單以取得詳細資訊。



已探索到的裝置

此動態小工具會顯示在組織網路中探索到的裝置的詳細資訊。這些裝置資訊包括裝置類型、製造商、作業系統、IP 位址、MAC 位址、探索日期等。



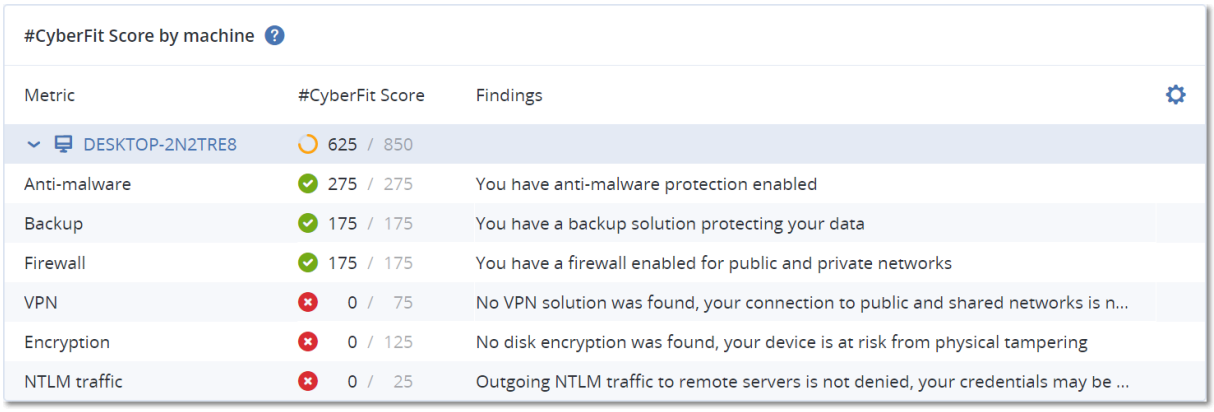
依電腦分類的 #CyberFit 分數

此桌面小工具可針對每部電腦顯示 #CyberFit 總分、其綜合分數，以及每個評估指標的結果：

- 反惡意程式碼
- 備份
- 防火牆
- VPN
- 加密
- NTLM 流量

若要提高每個指標的分數，您可以檢視報告中提供的建議。

如需有關 #CyberFit 分數的詳細資訊，請參閱「電腦的 #CyberFit 分數」。



Endpoint Detection and Response (EDR) 桌面小工具

Endpoint Detection and Response (EDR) 包含可以從 **[操作]** 儀表板存取的多種桌面小工具。

可用的桌面小工具包括：

- 每個工作負載的最高事件分佈
- 事件 MTTR
- 安全性事件待執行工作
- 工作負載網路狀態

每個工作負載的最高事件分佈

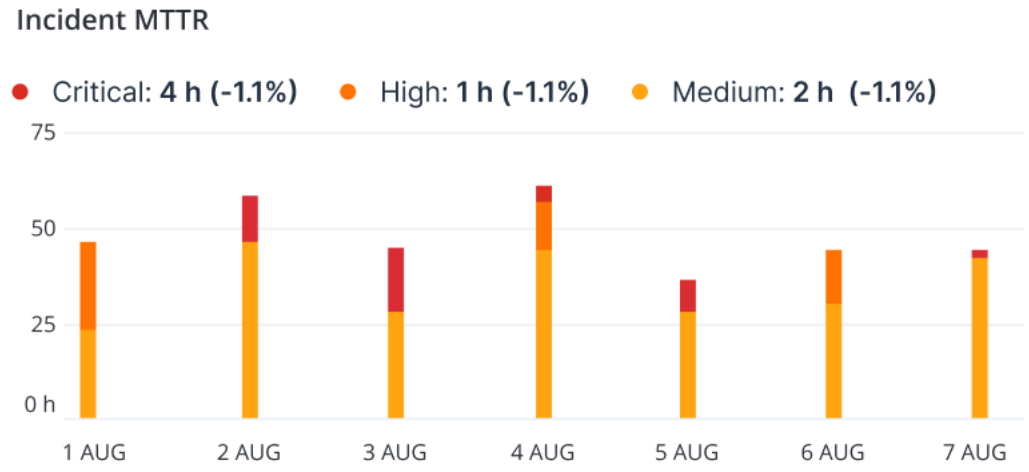
此桌面小工具會顯示包含最多事件的前五個工作負載 (按一下 **[全部顯示]** 可重新導向至根據桌面小工具設定篩選的事件清單)。

將滑鼠暫留在某個工作負載列上可檢視目前事件調查狀態的明細；這些調查狀態包括 **[未開始]**、**[調查中]**、**[已結案]** 以及 **[誤報]**。接著，按一下您要進一步分析的工作負載，然後在顯示的快顯視窗中選擇相關客戶；系統會根據桌面小工具設定，重新整理事件清單。

事件 MTTR

此桌面小工具會顯示安全性事件的平均解決時間。它會指出調查並解決事件的速度。

按一下某個欄可根據嚴重性 (**[重大]**、**[高]** 和 **[中]**) 檢視事件的明細，以及解決不同嚴重性層級所需的時間。顯示在括號中的 % 值表示與前一段時間相比增加或減少。

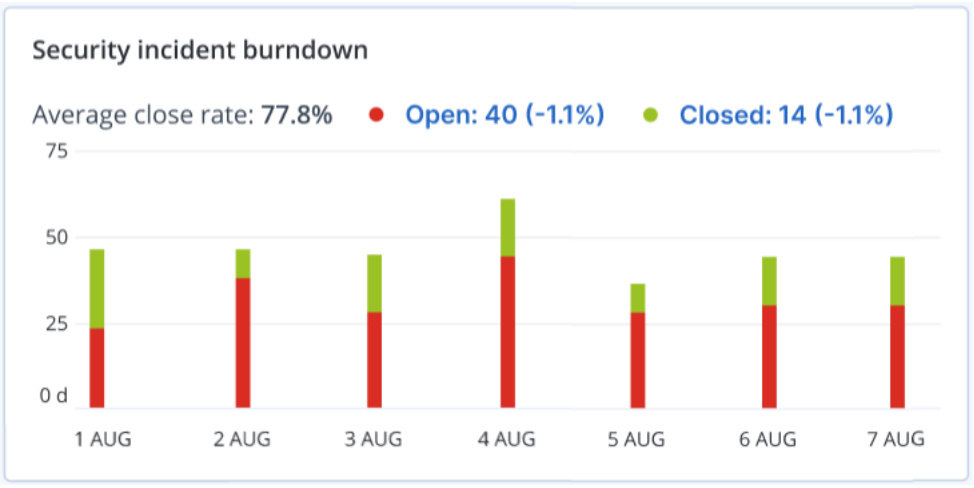


安全性事件待執行工作

此桌面小工具會顯示將事件結案的效率；未結案事件的數目是根據一段時間內已結案事件的數目來衡量的。

將滑鼠暫留在某個欄上可檢視所選日期已結案和未結案事件的明細。如果您按一下 [未結案] 值，便會顯示一個快顯視窗，您可以在其中選擇相關的租用戶；所選租用戶的篩選事件清單隨即顯示，以顯示目前未結案 (處於 **[調查中]** 或 **[未開始]** 狀態) 的事件。如果您按一下 [已結案] 值，便會顯示所選租用戶的事件清單，經過篩選後，即可顯示不再是未結案 (處於 **[已結案]** 或 **[誤報]** 狀態) 的事件。

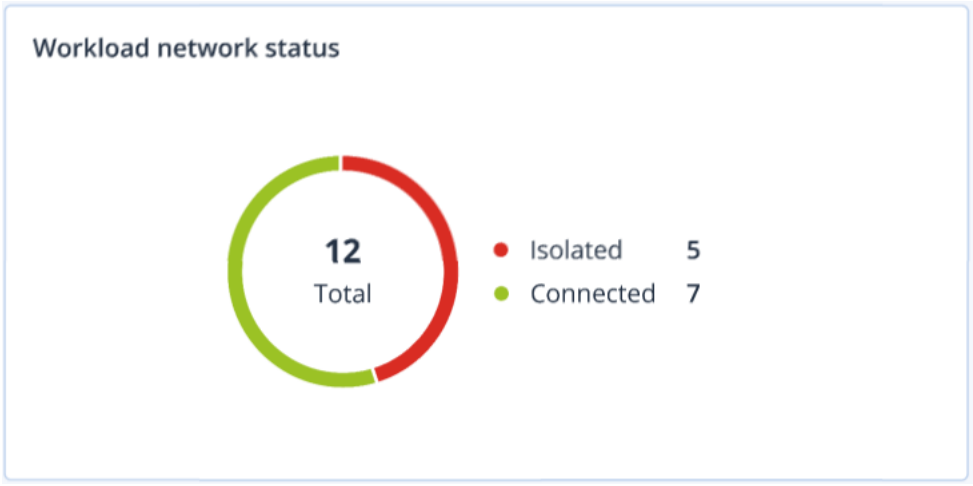
顯示在括號中的 % 值表示與前一段時間相比增加或減少。



工作負載網路狀態

此桌面小工具會顯示您工作負載的目前網路狀態，並指出工作負載隔離的數目以及連線的數目。

按一下 [已隔離] 值，便會顯示一個快顯視窗，您可以在其中選擇相關的租用戶。顯示的工作負載檢視經過篩選後可顯示已隔離的工作負載。按一下 [已連線] 值可檢視包含代理程式清單的工作負載，經過篩選後可顯示已連線的工作負載 (針對所選租用戶)。



磁碟健全狀況監控

「磁碟健全狀況監控」提供目前磁碟健全狀況狀態及其預測的相關資訊，讓您可以防止可能與磁碟故障相關的資料洩漏。HDD 和 SSD 磁碟都受到支援。

限制

- 僅執行 Windows 的電腦支援磁碟健全狀況預測。
- 只有實體機器的磁碟受到監控。虛擬機器的磁碟無法受到監控，而且不會顯示在磁碟健全狀況桌面小工具中。
- 不支援 RAID 設定。磁碟健全狀況桌面小工具不包含實作 RAID 之電腦的任何相關資訊。
- 不支援 NVMe SSD。
- 不支援外接式儲存裝置。

磁碟健全狀況以下列其中一種狀態表示：

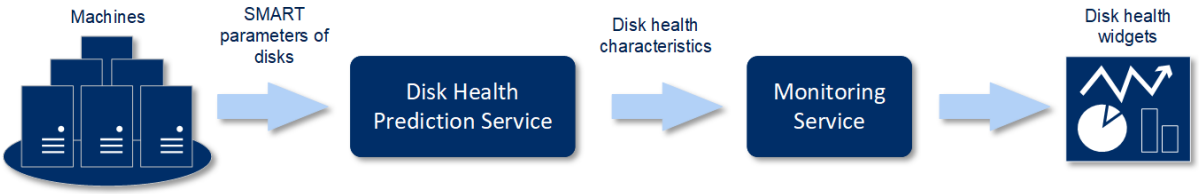
- **正常**
  磁碟健全狀況介於 70% 到 100% 之間。
- **警告**
  磁碟健全狀況介於 30% 到 70% 之間。
- **重大**
  磁碟健全狀況介於 0% 到 30% 之間。
- **正在計算磁碟資料**
  目前的磁碟狀態和預測正在計算中。

運作原理

磁碟健全狀況預測服務使用以 AI 為基礎的預測模型。

1. 保護代理程式會收集磁碟的 SMART 參數，並將此資料傳遞給磁碟健全狀況預測服務：
   - SMART 5 – 重新配置的磁區計數。
   - SMART 9 – 開機時數。
   - SMART 187 – 報告的無法更正錯誤數。
   - SMART 188 – 命令逾時。
   - SMART197 – 目前擱置中的磁區計數。
   - SMART 198 – 離線的無法更正磁區計數。
   - SMART 200 – 寫入錯誤率。
2. 磁碟健全狀況預測服務會處理收到的 SMART 參數、進行預測，然後提供下列磁碟健全狀況特徵：
   - 磁碟健全狀況目前狀態：正常、警告、嚴重。
   - 磁碟健全狀況預測：負面、穩定、正面。
   - 磁碟健全狀況預測機率 (百分比)。

   預測期間為一個月。
3. 監控服務會收到這些特徵，然後在 Cyber Protect 主控台的磁碟健全狀況桌面小工具中顯示相關的資訊。

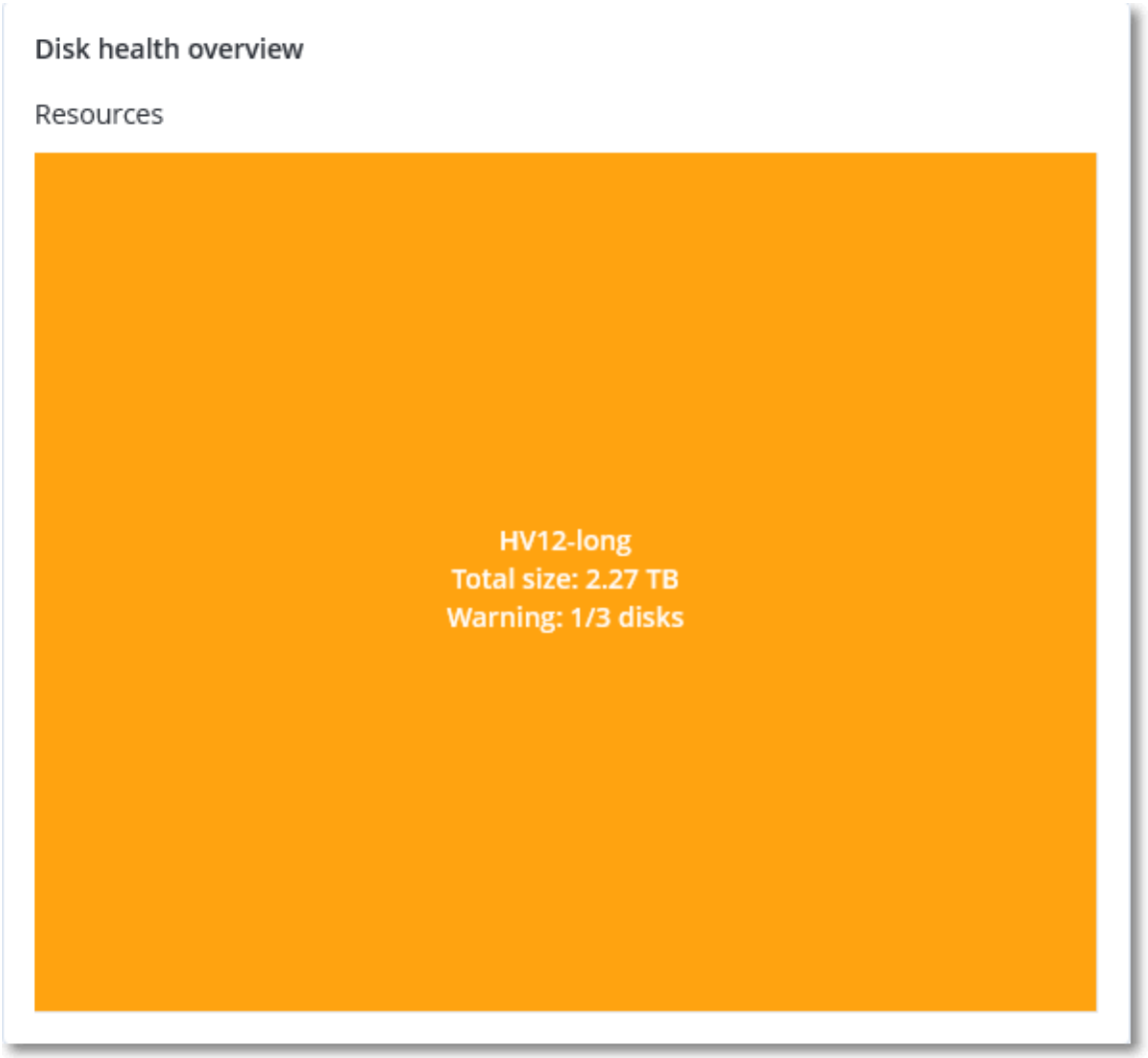


磁碟健全狀況桌面小工具

磁碟健全狀況監控的結果會顯示在 Cyber Protect 主控台中提供的下列桌面小工具內。

- **磁碟健全狀況概觀**是一個樹狀圖桌面小工具，其中包含可以透過查找切換的兩個詳細資料層級。
  - 電腦層級

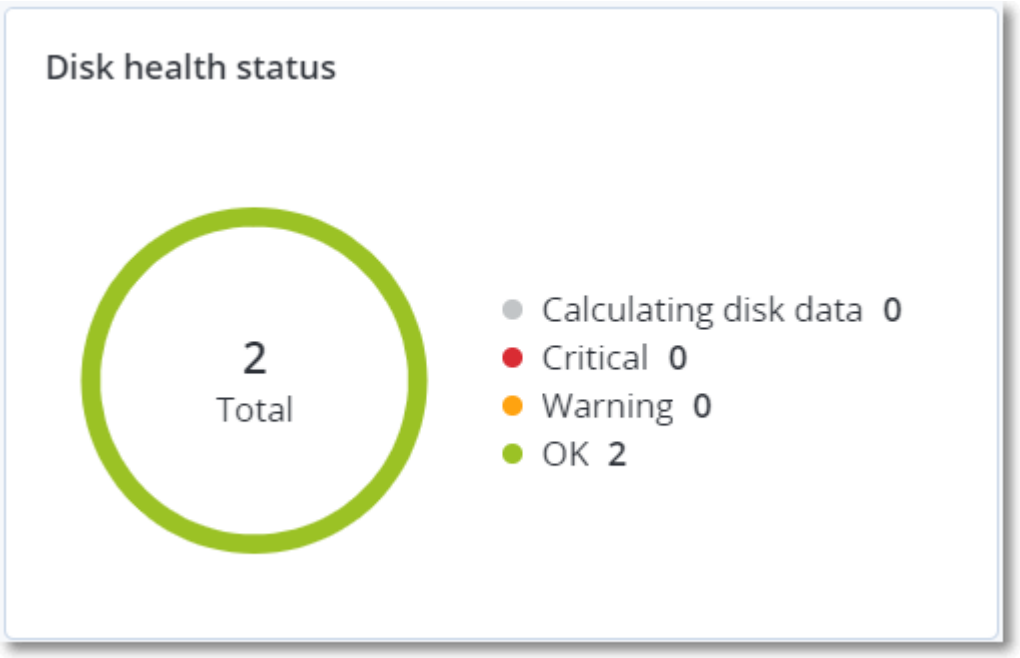
    針對選取的客戶電腦，顯示磁碟健全狀況狀態的摘要資訊。只有最嚴重的磁碟狀態才會顯示。當您將滑鼠暫留在特定區塊時，工具提示中會顯示其他狀態。電腦區塊大小取決於電腦所有磁碟的大小總計。電腦區塊色彩取決於所發現的最關鍵磁碟狀態。



- 磁碟層級
  針對所選電腦，顯示所有磁碟目前的磁碟健全狀況狀態。每個磁碟區塊都會顯示下列其中一個磁碟健全狀況預測及其機率 (百分比):
  - 將降級
  - 將保持穩定

- 將改善

- **磁碟健全狀況狀態**是一個圓形圖桌面小工具，可顯示每個狀態的磁碟數。



磁碟健全狀況狀態警示

磁碟健全狀況檢查每 30 分鐘執行一次，而對應的警示則一天產生一次。當磁碟健全狀況從 **[警告]** 變更為 **[重大]** 時，一律會產生警示。

警示名稱	嚴重性	磁碟健全狀況狀態	描述
磁碟可能故障	警告	(30 – 70)	此電腦上的 <disk name> 磁碟之後可能會故障。請儘速對此磁碟執行完整映像備份、更換該磁碟，然後將映像復原到新的磁碟。
磁碟故障即將發生	重大	(0 – 30)	此電腦上的 <disk name> 磁碟處於嚴重狀態，很可能很快就會發生故障。目前不建議對此磁碟執行映像備份，因為增加的壓力可能會使磁碟故障。請立即備份此磁碟上最重要的檔案，然後更換該磁碟。

資料保護圖

資料保護圖功能可讓您探索對您重要的所有資料，並在樹狀圖的可擴充檢視中，取得所有重要檔案的數目、大小、位置、保護狀態等資訊。

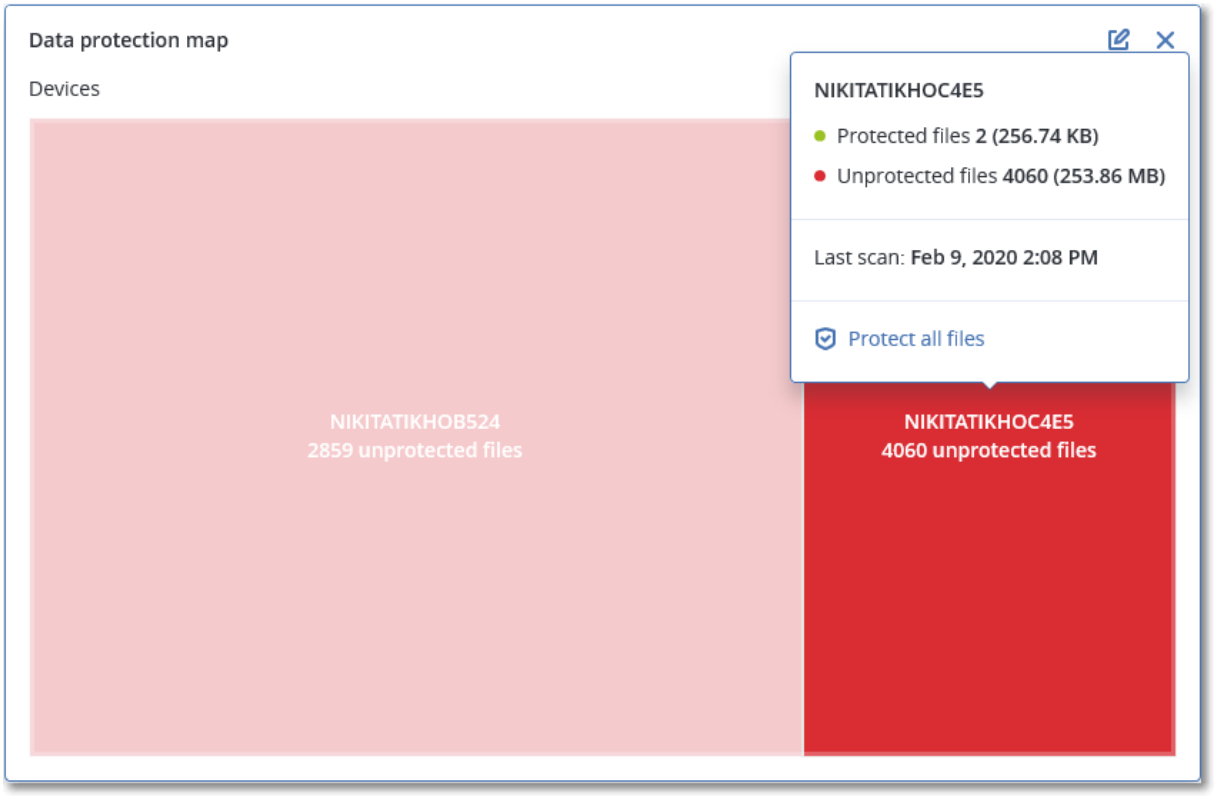
每個區塊大小取決於客戶/電腦所屬所有重要檔案的總數/大小總計。

檔案可以擁有以下保護狀態之一：

- **重大** – 有 51-100% 具有您指定之副檔名的未受保護檔案未針對所選電腦/位置進行備份，而且將不會以現有的備份設定進行備份。
- **低** – 有 21-50% 具有您指定之副檔名的未受保護檔案未針對所選電腦/位置進行備份，而且將不會以現有的備份設定進行備份。
- **中** – 有 1-20% 具有您指定之副檔名的未受保護檔案未針對所選電腦/位置進行備份，而且將不會以現有的備份設定進行備份。
- **高** – 具有您指定之副檔名的所有檔案都針對所選電腦/位置受到保護 (備份)。

資料保護檢查的結果可以在資料保護圖桌面小工具 (顯示電腦層級詳細資料的樹狀圖桌面小工具) 的儀表板上找到：

- 電腦層級 – 針對所選客戶的每部電腦，顯示重要檔案保護狀態的相關資訊。



若要保護未受保護的檔案，請將滑鼠移至該區塊，然後按一下 **[保護所有檔案]**。在對話視窗中，您可以找到未受保護檔案數目及其位置的相關資訊。若要保護這些檔案，按一下 **[保護所有檔案]**。

您也可以下載 CSV 格式的詳細報告。

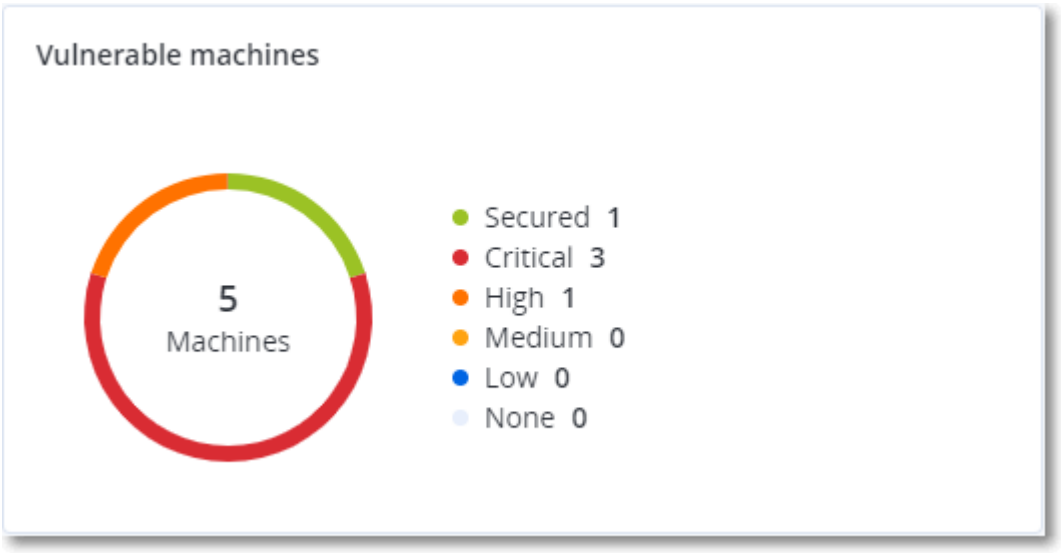
弱點評估桌面小工具

易受攻擊的電腦

此桌面小工具會依弱點嚴重性顯示易受攻擊的電腦。

根據通用弱點評分系統 (CVSS) v3.0，發現的弱點可以擁有以下嚴重性層級之一：

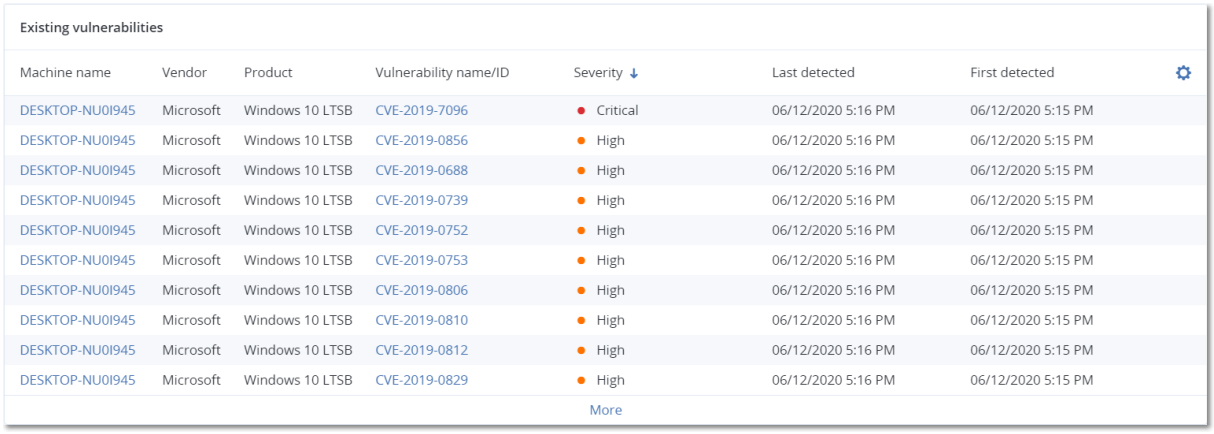
- 受保護：找不到弱點
- 重大：9.0 - 10.0 CVSS
- 高：7.0 - 8.9 CVSS
- 中：4.0 - 6.9 CVSS
- 低：0.1 - 3.9 CVSS
- 無：0.0 CVSS



現有的弱點

此桌面小工具會顯示電腦上目前現有的弱點。在 **[現有的弱點]** 桌面小工具中，有兩欄顯示時間戳記：

- **第一次偵測到的** – 最初在電腦上偵測到弱點的日期和時間。
- **上次偵測到的** – 上次在電腦上偵測到弱點的日期和時間。


Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

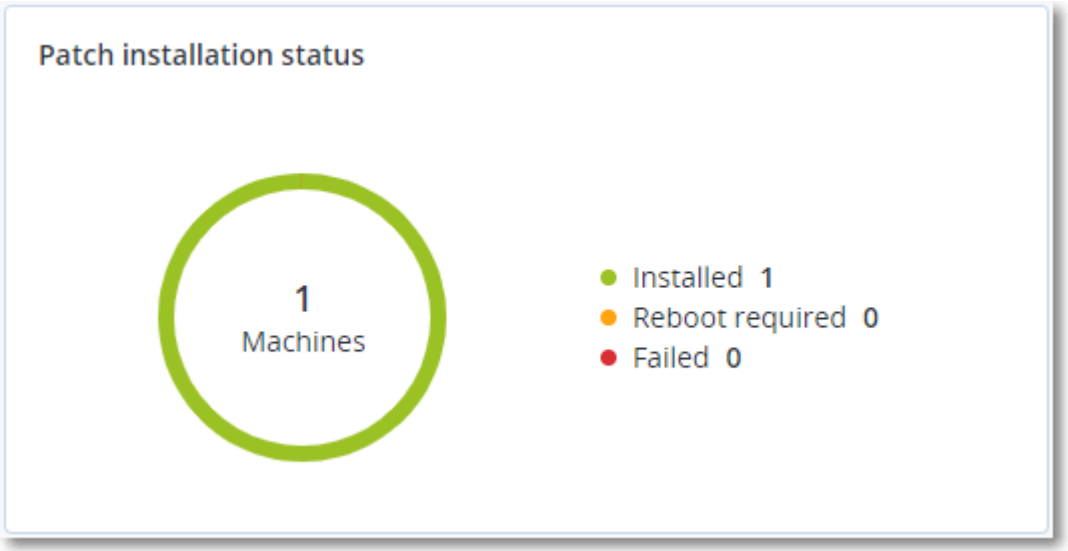
修補程式安裝桌面小工具

有四個與修補程式管理功能相關的桌面小工具。

修補程式安裝狀態

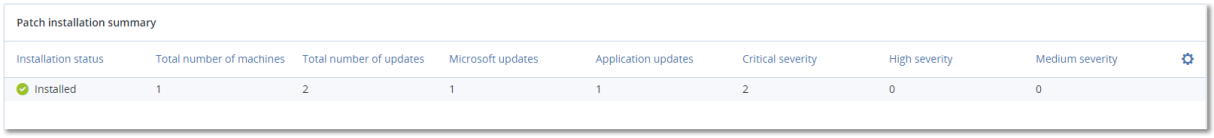
此桌面小工具會顯示依修補程式安裝狀態分組的電腦數目。

- **已安裝** – 電腦上已安裝所有可用的修補程式
- **需要重新開機** – 修補程式安裝之後，電腦需要重新開機
- **失敗** – 在電腦上安裝修補程式失敗



修補程式安裝摘要

此桌面小工具會在電腦上顯示依修補程式安裝狀態排列的修補程式摘要。



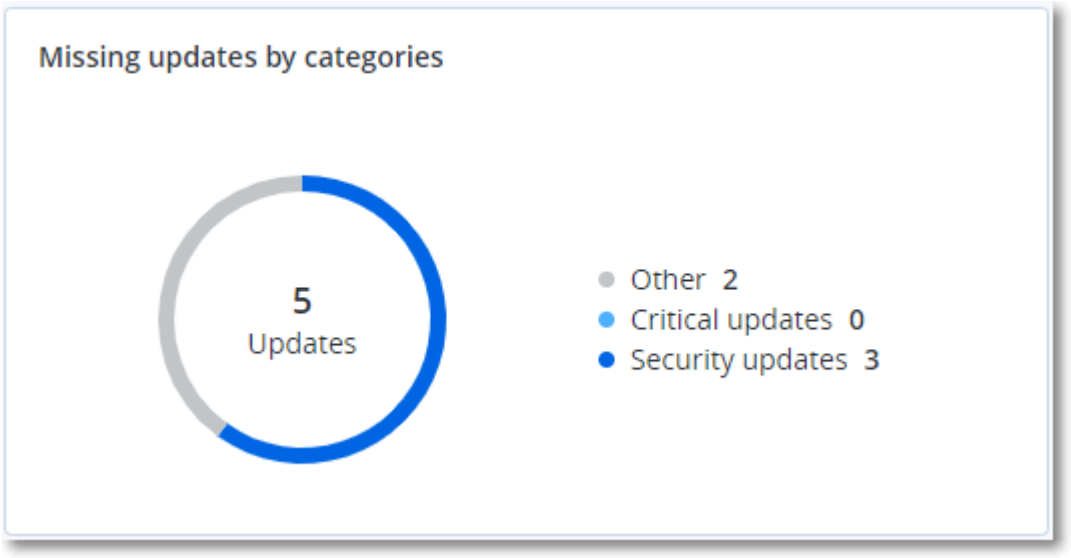
修補程式安裝歷史記錄

此桌面小工具會顯示電腦上修補程式的詳細資訊。

遺漏的更新 (依類別)

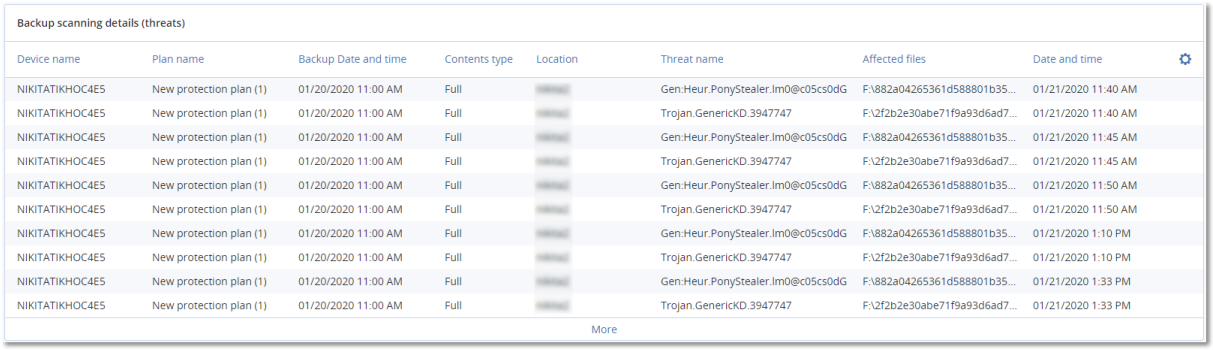
此桌面小工具會依類別顯示遺漏的更新數目。顯示下列類別：

- 安全性更新
- 重大更新
- 其他



備份掃描詳細資料

此桌面小工具會顯示備份中偵測到之威脅的詳細資訊。

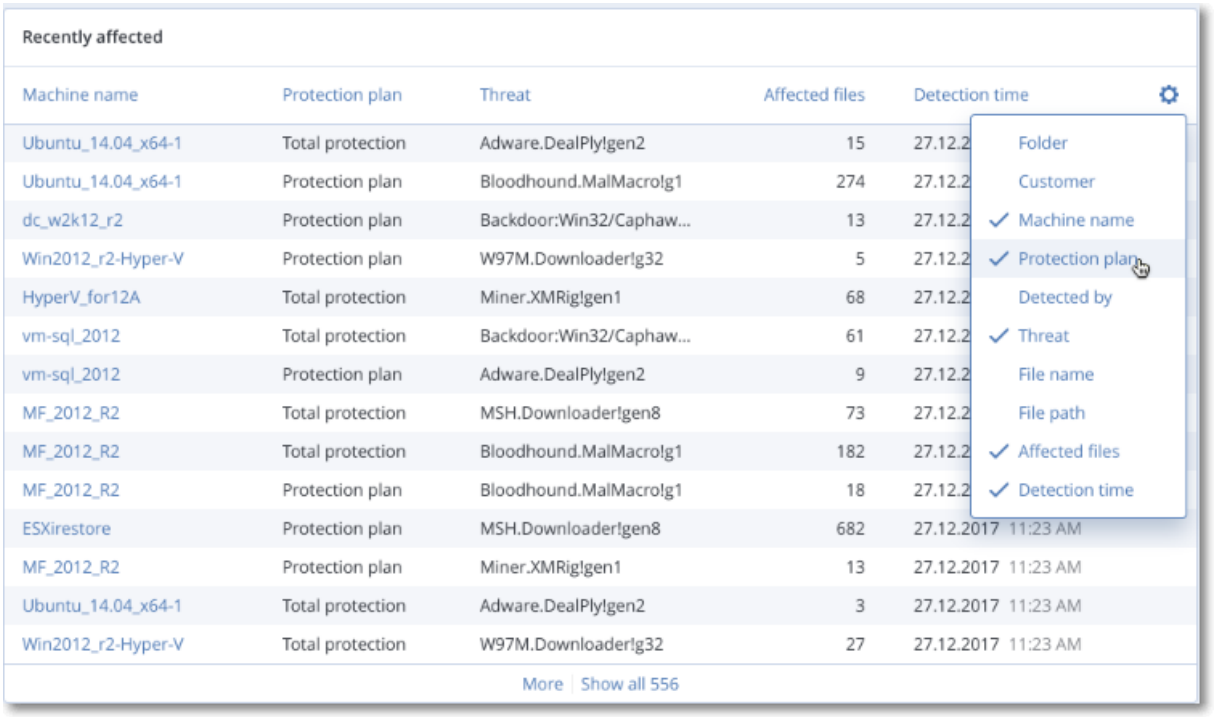

Backup scanning details (threats)

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

最近受影響

此桌面小工具會顯示受到病毒、惡意程式碼和勒索軟體之類威脅影響的工作負載的詳細資訊。您可以找到的相關資訊包括偵測到的威脅、偵測到威脅的時間，以及受感染檔案數目。



下載最近受影響工作負載的資料

您可以下載最近受影響工作負載的資料、產生 CSV 檔案，然後將其傳送給您指定的收件者。

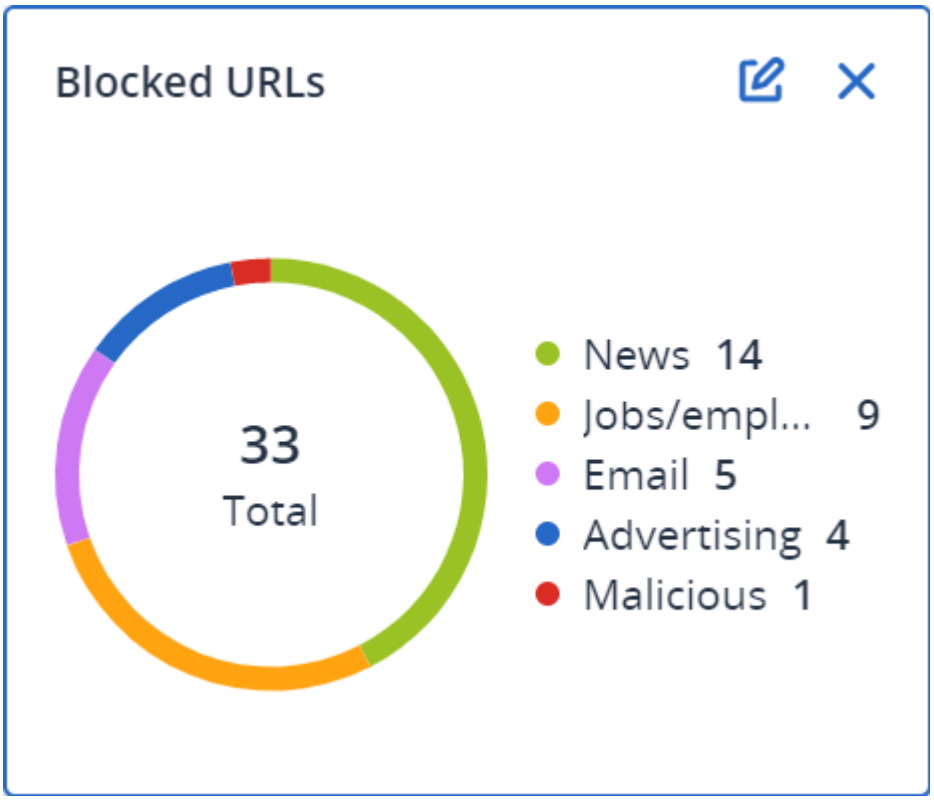
若要下載最近受影響工作負載的資料

1. 在 **[最近受影響]** 桌面小工具中，按一下 **[下載資料]**。
2. 在 **[時間期限]** 欄位中，輸入您要下載資料的天數。您可以輸入的天數上限為 200。
3. 在 **[收件者]** 欄位中，輸入將收到電子郵件的所有人員的電子郵件地址，且電子郵件中會包含用於下載 CSV 檔案的連結。
4. 按一下 **[下載]**。

   系統會使用您指定的時間期限內受影響工作負載的資料，開始產生 CSV 檔案。當 CSV 檔案完成時，系統會傳送一封電子郵件給收件者。接著，每個收件者都可以下載 CSV 檔案。

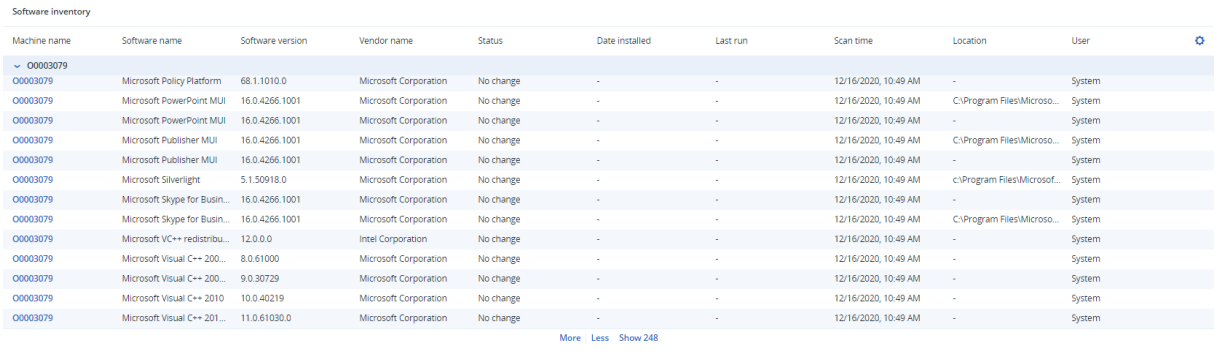
已封鎖的 URL

桌面小工具會依類別顯示已封鎖之 URL 的統計資料。如需有關 URL 篩選和分類的詳細資訊，請參閱網路保護使用指南。



軟體清查桌面小工具

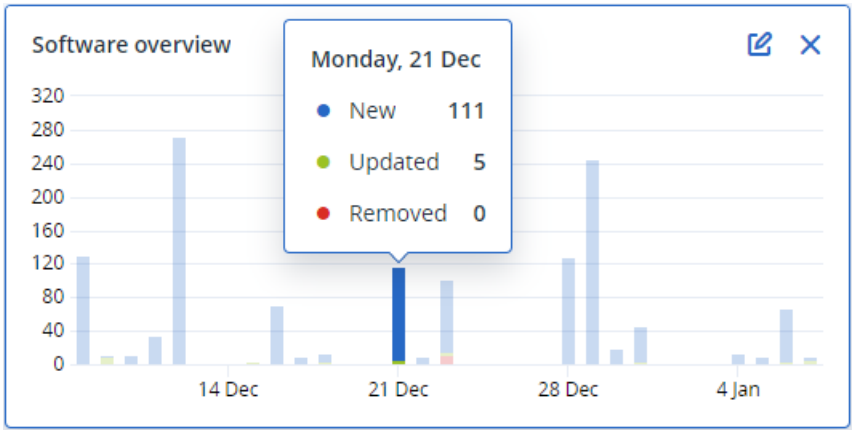
[軟體清查] 表格桌面小工具會顯示安裝在組織中 Windows 和 macOS 裝置上的所有軟體的詳細資訊。


Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
O0003079									
O0003079	Microsoft Policy Platform	68.1.1010.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft PowerPoint MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft Publisher MUI	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Silverlight	5.1.50918.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	c:\Program Files\Microsof...	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Skype for Busin...	16.0.4266.1001	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	C:\Program Files\Microso...	System
O0003079	Microsoft VC++ redistribu...	12.0.0.0	Intel Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	8.0.61000	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 200...	9.0.30729	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 2010	10.0.40219	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System
O0003079	Microsoft Visual C++ 201...	11.0.61030.0	Microsoft Corporation	No change	-	-	12/16/2020, 10:49 AM	-	System

More | Less | Show 248

[軟體概觀] 桌面小工具會顯示指定的期間 (7 天、30 天或當月), 組織中 Windows 和 macOS 裝置上新的、已更新和已刪除的應用程式的數目。



當您將滑鼠暫留在圖表上的某一列時，就會顯示包含下列資訊的工具提示：

新的 - 新安裝的應用程式的數目。

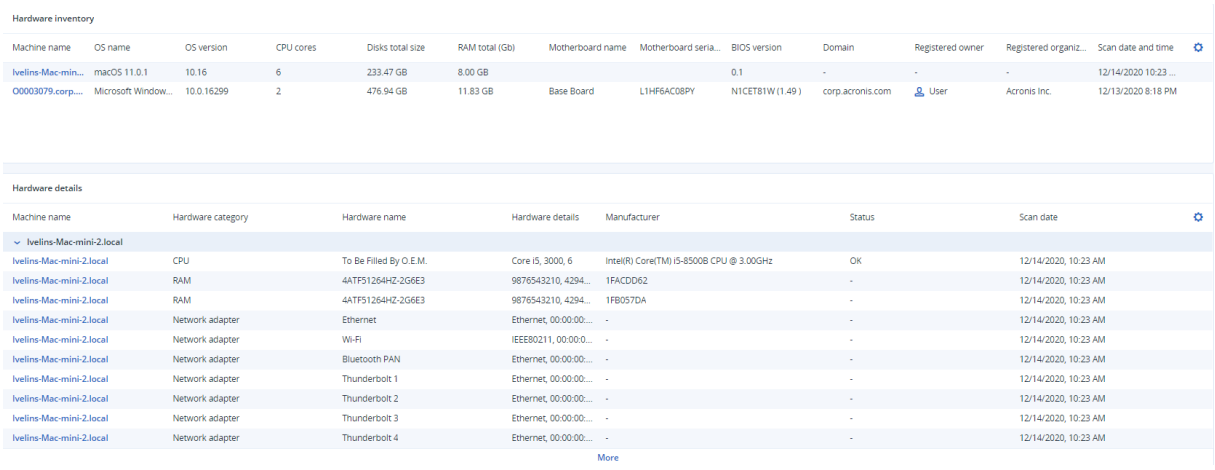
已更新 - 已更新的應用程式的數目。

已移除 - 已移除的應用程式的數目。

當您按一下某個狀態列的部分時，就會將您重新導向至 **[軟體管理]** -> **[軟體清查]** 頁面。系統會針對對應的日期和狀態，篩選頁面中的資訊。

硬體清查桌面小工具

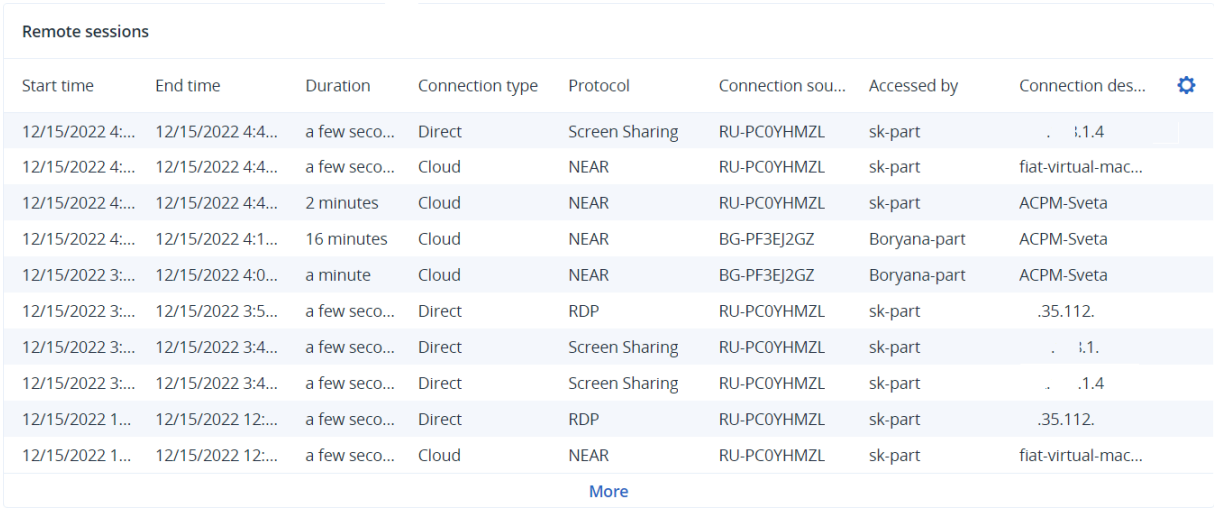
[硬體清查] 和 **[硬體詳細資料]** 表格桌面小工具會顯示安裝在組織中實體與虛擬 Windows 和 macOS 裝置上的所有硬體的相關資訊。



[硬體變更] 表格桌面小工具會顯示指定的期間 (7 天、30 天或當月)，組織中實體與虛擬 Windows 和 macOS 裝置上新增、移除和變更的硬體的相關資訊。

工作階段歷程記錄

該桌面小工具會顯示指定期限內在您的組織中進行之遠端桌面和檔案傳輸工作階段的相關詳細資訊。



稽核記錄

若要檢視稽核記錄，請移至 **[監控]** > **[稽核記錄]**。

稽核記錄針對下列事件，提供按時間順序排列的記錄：

- 使用者在管理入口網站內執行的作業
- 使用者在 Cyber Protect 主控台中執行的作業 (含雲端對雲端資源)
- 使用者在 Cyber Protect 主控台中執行的網路指令碼作業
- 與電子郵件存檔相關的作業
- 已達到配額和配額使用量的相關系統訊息

此記錄會顯示您目前操作的組織或單位及其子單位中的事件。您可以按一下某個事件，檢視其相關的詳細資訊。

稽核記錄儲存在資料中心，且其可用性不會受到使用者電腦上的問題影響。

記錄每天清理一次。事件則會在 180 天後移除。

稽核記錄欄位

記錄會針對每個事件顯示：

- **事件**

  事件的簡短描述。例如，**已建立租用戶**、**已刪除租用戶**、**已建立使用者**、**已刪除使用者**、**已達到配額**、**已瀏覽備份內容**、**已變更指令碼**。
- **嚴重性**

  可能是下列其中一項：
  - **錯誤**

    表示錯誤。
  - **警告**

    表示可能負面的動作。例如，**已刪除租用戶**、**已刪除使用者**、**已達到配額**。
  - **注意事項**

    表示可能需要注意的事件。例如，**已更新租用戶**、**已更新使用者**。
  - **資訊**

    表示中性的資訊變更或動作。例如，**已建立租用戶**、**已建立使用者**、**已更新配額**、**已刪除指令碼計劃**。
- **日期**

  事件發生的日期及時間。
- **物件名稱**

  執行作業所使用的物件。例如，**已更新使用者**事件的物件為變更其屬性的使用者。若是與配額相關的事件，則配額就是物件。
- **租用戶**

  物件所屬單位的名稱。例如，**已更新使用者**事件的租用戶為使用者所在的單位。**已達到配額**事件的租用戶為達到其配額的使用者。
- **起始端**

  起始事件之使用者的登入資訊。若是上層系統管理員所起始的系統訊息和事件，起始端會顯示為**系統**。
- **起始端的租用戶**

  起始端所屬單位的名稱。若是上層系統管理員所起始的系統訊息和事件，此欄位為空白。
- **方法**

  顯示事件透過 Web 介面還是 API 起始。
- **IP**

  起始事件所在電腦的 IP 位址。

篩選與搜尋

您可以依類型、嚴重性或日期篩選事件。您也可以依其名稱、物件、租用戶、起始端和起始端的租用戶搜尋事件。

收集 Cyber Protection 代理程式的效能資料

您可以手動收集效能記錄，或在環境中啟用自動收集受保護 Windows 電腦的效能資料。監控是在每個代理程式的 Cyber Protect Cloud 主控台中設定的，如果系統效能低於預先定義的閾值，則會啟用自動收集診斷資料。請參閱 "設定 ETL 資料收集的效能閾值" (第 59 頁)。

注意事項
此功能在 Cyber Protection 的 Windows 用代理程式 24.4.37758 版或更新版本上受支援。

若要啟用自動收集效能資料

1. 在 Cyber Protect Cloud 主控台中，導覽至 **[設定]** > **[代理程式]**。
2. 在 **[代理程式]** 清單中，找出您要為其啟用效能監視器的代理程式，然後按一下 **[設定]**。
3. 在 **[效能監視器]** 區段中，啟用 **[允許此代理程式自動收集效能記錄]** 切換開關。

自動收集的資料會儲存在受保護電腦的本機磁碟中，資料夾為 `C:\ProgramData\Acronis\ETLTool\ETL\`。

若要手動收集效能資料

您可以按需收集效能資料，而不必啟用效能監視器和自動收集效能資料。

1. 以系統管理員使用者身分，登入受保護的電腦。
2. 在命令提示字元下，執行下列其中一個命令：
   - `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o`
     ETL 追蹤收集將一直執行，直到您按下鍵盤上的 S 鍵為止，或直到 3600 秒的時間上限屆滿為止。
   - `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o -i X`
     其中 X 是以秒為單位的資料收集時間限制，最大值為 3600。您隨時按下鍵盤上的 S 鍵就可以停止收集。

手動收集的資料會儲存在受保護電腦的本機磁碟中，資料夾為 `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`

若要收集效能記錄

1. 以系統管理員使用者身分，登入受保護的電腦。
2. 找出您需要的資料：
   - 自動收集的效能資料位於資料夾 `C:\ProgramData\Acronis\ETLTool\ETL\`
   - 按需收集的效能資料位於資料夾 `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\`

ETL 追蹤也包含在 `sysinfo` 套件中。

設定 ETL 資料收集的效能閾值

您可以在環境中啟用自動收集受保護 Windows 電腦的效能資料。監控是在每個代理程式的 Cyber Protect Cloud 主控台中設定的，並在系統效能低於預先定義的閾值時，啟用自動收集診斷資料。這些閾值的定義會儲存在您啟用效能監控的受保護電腦上。您可以根據需要，修改這些定義。

超過其中一個閾值時，自動收集資料隨即開始，並持續最多 3600 秒，無法修改。

若要修改 ETL 資料收集的預設閾值

1. 以系統管理員使用者身分，登入受保護的電腦
2. 開啟 C:\ProgramData\Acronis\ETLTool\ConfigTemplate\etl-tool.yaml 檔案進行編輯。
3. 視需要修改預設設定。

參數	描述	預設值
"process-memory-consumption"	記憶體過度使用的閾值	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	高磁碟 I/O 使用率的閾值	
"maximum-operations-number"		10000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-file-io"	檔案高 I/O 使用率的閾值	
"maximum-operations-number"		30000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	CPU 高使用量的閾值	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	保護代理程式元件的效能	
"behavioral-engine"	行為引擎的閾值	
"average-system-utilization-percent"		50

參數	描述	預設值
"be-stats-event-number"		10
"avc-scan"	防毒和防惡意軟體防護元件的閾值	
"average-scan-duration-seconds"	平均掃描持續時間上限	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	單一掃描的掃描持續時間上限	5

若要還原至預設值，請使用上表中的值。

報告

若要存取有關服務使用狀況和作業的報告，請按一下 **[報告]**。

注意事項
此功能無法用於 Cyber Protection 服務的 Standard 版本。

使用報告

使用報告會提供關於服務使用的歷程記錄資料。使用報告提供 CSV 和 HTML 格式。

重要事項
產品 UI 中顯示的儲存空間使用狀況值為二進位位元組單位 (Mebibytes (MiB)、Gibibytes (GiB) 及 Tebibytes (TiB))，即使標籤分別顯示 MB、GB 及 TB，也是如此。例如，如果實際使用量為 3105886629888 個位元組，則 UI 中顯示的值將正確顯示為 2.82，但標籤會標示為 TB 而非 TiB。

報告類型

您可以選擇下列其中一種報告類型：

- **目前使用狀況**
  報告中包含目前服務使用狀況計量。
- **期間摘要**
  報告中包含指定期間結束時的服務使用狀況計量，以及指定期間開始與結束計量間的差異。

  注意事項
  只有在單位和客戶租用戶層級，才會報告本機儲存裝置使用情況資料。使用者不會在摘要報告中收到有關本機儲存裝置使用情況的資訊。

- **按日的期限**
  報告中包含服務使用狀況計量及其指定期間內每天的變化。

報告範圍

您可以使用以下所列的值選擇報告範圍：

- **直接客戶和合作夥伴**
  報告將包含僅適用於直接隸屬於您所操作的公司或單位的子單位的服務使用狀況計量。
- **所有客戶和合作夥伴**
  報告將包含您所操作的公司或單位的子單位的服務使用狀況計量。
- **所有客戶及合作夥伴(包括使用者詳細資訊)**
  報告將包含適用於您所操作之租用戶的所有子租用戶和租用戶內所有使用者的服務使用狀況計量。

使用率為零的指標

顯示使用率非零的指標資訊並隱藏使用率為零的指標資訊，您可減少報表中的行數。

設定計劃使用狀況報告

排程報告涵蓋最近一個完整曆月內的服務使用狀況計量。系統會在指定月份第一天的 23:59:59 (UTC 時間) 產生報告，並在該月的第二天傳送報告。報告會傳送給公司的所有系統管理員，或在使用者設定中選取 **[已排程的使用報告]** 核取方塊的單位。

啟用或停用排程報告

1. 登入管理入口網站。
2. 確認您在適用的公司或最上層單位上操作。
3. 按一下 **[報告]** > **[使用狀況]**。
4. 按一下 **[排程]**。
5. 選擇或清除 **[傳送每月摘要]** 報告核取方塊。
6. 在 **[詳細等級]** 中，選擇報告範圍。
7. [選用] 如果要從報表中排除使用率為零的指標，請選擇 **[隱藏使用率為零的指標]**。

設定自訂使用率報告

自訂報告可供隨需產生，但無法設定排程。報告會傳送至您的電子郵件地址。

產生自訂報告

1. 登入管理入口網站。
2. 瀏覽到您要建立報告的單位。
3. 按一下 **[報告]** > **[使用狀況]**。
4. 按一下 **[自訂]**。
5. 在 **[類型]** 中，選擇報表類型。
6. [不適用於 **[目前使用狀況]** 報告類型] 在 **[期間]** 中選擇報告期間：
   - **目前曆月**
   - **上一個曆月**
   - **自訂**
7. [不適用於 **[目前使用狀況]** 報告類型] 如果您要指定自訂報告期間，請選擇開始和結束日期。否則，請跳過此步驟。
8. 在 **[詳細等級]** 中，選擇報告範圍。
9. [選用] 如果要從報表中排除使用率為零的指標，請選擇 **[隱藏使用率為零的指標]**。
10. 若要產生報告，請按一下 **[產生並傳送]**。

使用狀況報告中的資料

使用 Cyber Protection 服務的相關報告包含下列關於公司或單位的資料：

- 依照單位、使用者、裝置類型分類的備份大小。
- 依照單位、使用者、裝置類型分類之受保護裝置的數量。
- 依照單位、使用者、裝置類型分類的價格。
- 備份大小總計。
- 受保護裝置的總數。
- 總價。

如果 Cyber Protection 服務無法偵測裝置類型，該裝置在報表中會顯示為**不具類型**。

重要事項
產品 UI 中顯示的儲存空間使用狀況值為二進位位元組單位 (Mebibytes (MiB)、Gibibytes (GiB) 及 Tebibytes (TiB))，即使標籤分別顯示 MB、GB 及 TB，也是如此。例如，如果實際使用量為 3105886629888 個位元組，則 UI 中顯示的值將正確顯示為 2.82，但標籤會標示為 TB 而非 TiB。

操作報告

[操作] 報告僅供公司系統管理員在公司層級上操作時使用。

關於操作的報告可能包括任何一組 **[操作]** 儀表板動態小工具。所有桌面小工具都會顯示整個公司的摘要資訊。
根據桌面小工具類型，報告包含時間範圍和瀏覽或報告產生時的資料。請參閱 "根據桌面小工具類型回報的資料" (第 78 頁)。

所有歷史桌面小工具都會顯示相同時間範圍的資料。您可在報告設定中變更此範圍。

您可以使用預設報告或建立自訂報告。

您可以下載報告，或透過電子郵件，以 XLSX (Excel) 或 PDF 格式傳送。

預設報告如下所列：

報告名稱	描述
依電腦分類的 #CyberFit 分數	根據每部電腦的安全指標和設定的評估，顯示 #CyberFit 分數以及改進的建議。
警示	顯示指定期間發生的警示。
備份掃描詳細資料	顯示備份中偵測到的威脅的詳細資訊。
每日活動	顯示指定期間所執行活動的摘要資訊。
資料保護圖	顯示電腦上所有重要檔案之數目、大小、位置、保護狀態的詳細資訊。
偵測到的威脅	按照遭封鎖的威脅數目，以及狀況良好與易受攻擊電腦的數目，顯示受影響電腦的詳細資料。
已探索到的裝置	顯示在您的組織網路中探索到的所有裝置。

磁碟健全狀況預測	顯示 HDD/SSD 故障時間的預測以及目前的磁碟狀態。
現有的弱點	顯示組織中作業系統和應用程式現有的弱點。此報告也會針對網路中所列出的每個產品，顯示受影響電腦的詳細資料。
修補程式管理摘要	顯示遺漏的修補程式數目、已安裝的修補程式數目，以及適用的修補程式數目。您可以向下鑽研報告以取得遺漏/已安裝的修補程式資訊，以及所有系統的詳細資料。
摘要	顯示指定期間受保護裝置的摘要資訊。
每週各項活動	顯示指定期間所執行活動的摘要資訊。
軟體清查	顯示安裝在組織中 Windows 和 macOS 電腦上的所有軟體的詳細資訊。
硬體清查	顯示適用於組織中實體與虛擬 Windows 和 macOS 電腦的所有硬體的詳細資訊。
遠端工作階段	顯示指定期限內在您的組織中進行之遠端桌面和檔案傳輸工作階段的相關詳細資訊。

具有報告的動作

新增

若要新增報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在可用報告的清單下，按一下 **[新增報告]**。
3. [新增預先定義的報告] 請按一下預先定義之報告的名稱。
4. [新增自訂報告] 按一下 **[自訂]**，然後將桌面小工具新增到報告。
5. [選用] 拖放桌面小工具將其重新排列。

檢視

若要檢視報告

- 若要檢視報告，請按一下其名稱。

編輯

若要˙編輯報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要編輯的報告。
3. 按一下畫面右上角的 **[設定]**。
4. 編輯報告，然後按一下 **[儲存]**。

刪除

若要刪除報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要刪除的報告。
3. 按一下畫面右上角的省略符號圖示 (...)，然後按一下 **[刪除報告]**。
4. 在確認視窗中，按一下 **[刪除]**。

排程

若要排程報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要排程的報告。
3. 按一下畫面右上角的 **[設定]**。
4. 啟用 **[排程]** 旁的開關。
   - 指定收件者的電子郵件地址。
   - 選擇報告格式。

   - **注意事項**
     一個 PDF 檔案中最多可以匯出 1,000 個項目，而一個 XLSX 檔案中最多可以匯出 10,000 個項目。PDF 和 XLSX 檔案中的時間戳記使用您電腦的當地時間。

   - 選擇報告語言。
   - 配置排程。
5. 按一下 **[儲存]**。

下載

若要下載報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇報告。
3. 按一下畫面右上角的 **[下載]**。
4. 選擇報告格式。

結果，所選格式的檔案隨即下載到您的電腦。

如果選擇 **[Excel 和 PDF]**，則會將 ZIP 檔案下載到您的電腦。

傳送

若要傳送報告

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇報告。
3. 按一下畫面右上角的 **[傳送]**。
4. 指定收件者的電子郵件地址。
5. 選擇報告格式。
6. 按一下 **[傳送]**。

匯出結構

若要匯出報告結構

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇報告。
3. 按一下畫面右上角的省略符號圖示 (...)，然後按一下 **[匯出]**。

結果，報告結構以 JSON 檔案儲存在您的電腦上。

傾印資料

要傾印報告資料

您可以在不篩選的情況下，將自訂期間的所有資料匯出至 CSV 檔案，並將 CSV 檔案傳送給電子郵件收件者。CSV 檔案僅包含報告中包含的小工具的相關資料。

注意事項
一個 CSV 檔案中最多可以匯出 150,000 個項目。CSV 檔案中的時間戳記使用國際標準時間 (UTC)。

1. 在 Cyber Protect 主控台中，移至 **[報告]**。
2. 在報告清單中，選擇您要傾印其資料的報告。
3. 按一下畫面右上角的省略符號圖示 (...)，然後按一下 **[傾印資料]**。
4. 指定收件者的電子郵件地址。
5. 在 **[時間範圍]** 中，指定您要傾印資料的自訂期間。

   注意事項
   準備較長時間的 CSV 檔案需要更多時間。

6. 按一下 **[傳送]**。

執行摘要

執行摘要報告可提供指定時間範圍內，組織環境及受保護裝置的保護狀態概觀。

執行摘要報告包含具有動態桌面小工具的可自訂區段，其中會顯示與下列雲端服務使用相關的主要效能指標：備份、反惡意程式碼保護、弱點評估、修補程式管理、Notary、Disaster Recovery，以及 Files Sync & Share。

您可以使用數種方式自訂報告。

- 新增或刪除區段。
- 變更區段的順序。
- 重新命名區段。
- 將桌面小工具從一個區段移到另一個區段。
- 變更桌面小工具在每個區段中的順序。
- 新增或移除桌面小工具。
- 自訂桌面小工具。

您可以產生 PDF 和 Excel 格式的執行摘要報告，並將其傳送給組織的利害關係人或擁有者，讓他們可以輕鬆地瞭解所提供服務的技術和商業價值。

執行摘要桌面小工具

您可以從執行摘要報告新增或移除區段和桌面小工具，從而控制包含在其中的資訊。

工作負載概觀桌面小工具

下表提供有關 **[工作負載概觀]** 區段中桌面小工具的詳細資訊。

桌面小工具	描述
雲端工作負載保護狀態	此桌面小工具會在報告產生時，依類型顯示受保護和未受保護雲端工作負載的數量。受保護的雲端工作負載是至少已套用一個備份計劃的雲端工作負載。未受保護的雲端工作負載是未套用任何備份計劃的雲端工作負載。圖表中顯示下列雲端工作負載類型 (依 A 到 Z 的字母順序): • Google Workspace 雲端硬碟 • Google Workspace Gmail • Google Workspace 共用磁碟機 • 託管的 Exchange 信箱 • Microsoft 365 信箱 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • 網站 部分工作負載類型使用下列工作負載群組: • Microsoft 365: 使用者、群組、公用資料夾、Teams 和網站集合 • Google Workspace: 使用者和共用磁碟機 • 託管的 Exchange: 使用者 如果一個工作負載群組中有超過 10000 個工作負載，則此桌面小工具不會顯示對應工作負載的任何資料。 例如，如果您組織的 Microsoft 365 帳戶有 10000 個信箱，且 OneDrive 服務供 500 個使用者使用，則它們全都屬於使用者工作負載群組。這些工作負載的加總為 10500，超出 10000 個工作負載群組的限制。因此，此桌面小工具將會隱藏對應的工作負載類型: Microsoft 365 信箱和 Microsoft 365 OneDrive。
網路保護摘要	此桌面小工具會針對指定的時間範圍，顯示網路保護效能的主要指標。 **已備份的資料** - 已在雲端和本機儲存空間建立的存檔的大小總計。 **已緩解的威脅** - 在所有裝置上封鎖的惡意程式碼的總數。 **已封鎖的惡意 URL** - 在所有裝置上封鎖的 URL 的總數。

桌面小工具	描述
	已修補的弱點 - 已透過所有裝置上安裝的軟體修補程式修正的弱點總數。 **已安裝的修補程式** - 在所有裝置上已安裝的修補程式總數。 **已受到 DR 保護的伺服器** - 已受到Disaster Recovery保護的伺服器總數。 **File Sync & Share 使用者** - 使用 Cyber Files 的終端使用者和來賓使用者的總數。 **已公證的檔案** - 已公證檔案的總數。 **已電子簽署的文件** - 已電子簽署的文件的總數。 **已封鎖的週邊裝置** - 已封鎖的週邊裝置的總數。
工作負載網路狀態	此桌面小工具會指出工作負載隔離的數目以及連線 (工作負載的正常狀態) 的數目。
工作負載保護狀態	此桌面小工具會在報告產生時依類型顯示受保護和未受保護的工作負載。受保護的工作負載是至少已套用一個保護或備份計劃的工作負載。未受保護的工作負載是未套用任何保護或備份計劃的工作負載。下列工作負載均包括在內: **伺服器** - 實體伺服器和網域控制站伺服器。 **工作站** - 實體工作站。 **虛擬機器** - 代理程式型虛擬機器和無代理程式虛擬機器。 **Web 託管伺服器** - 已安裝 cPanel 或 Plesk 的虛擬或實體伺服器。 **行動裝置** - 實體行動裝置。 一個工作負載可以屬於多個類別。例如, Web 託管伺服器包含在下列兩個類別中:**[伺服器]** 和 **[Web 託管伺服器]**。
已探索到的裝置	此小工具會顯示指定期間內在您組織的網路中探索到的裝置的下列資訊: **裝置名稱** **裝置類型** **作業系統** **製造商** **型號** **IP 位址** **MAC 位址** **組織單位** 您可以編輯小工具, 並依照組織單位、裝置類型、探索類型、首次探索日期、最後探索日期、IP 位址、MAC 位址和探索類型, 篩選顯示的資訊。

反惡意程式碼保護桌面小工具

下表提供有關 **[威脅防禦]** 區段中桌面小工具的詳細資訊。

桌面小工具	描述
檔案的反惡意程式碼掃描	此桌面小工具會針對指定的日期範圍，顯示對裝置進行反惡意程式碼按需掃描的結果。 **檔案** - 已掃描檔案的總數 **未感染** - 未感染檔案的總數 **已偵測到，已隔離** - 已隔離的受感染檔案的總數 **已偵測到，未隔離** - 未隔離的受感染檔案的總數 **受保護的裝置** - 已套用反惡意程式碼保護政策的裝置的總數 **已註冊裝置的總數** - 報告產生時，已註冊裝置的總數
備份的反惡意程式碼掃描	此桌面小工具會針對指定的日期範圍，使用下列指標顯示對備份進行反惡意程式碼掃描的結果： • 已掃描的復原點總數 • 未感染的復原點數量 • 未感染的復原點數量 (含不支援的磁碟分割) • 受感染的復原點數量。此指標包含受感染的復原點數量 (含不支援的磁碟分割)。
已封鎖的 URL	此桌面小工具會針對指定的日期範圍，顯示依網站類別分組的已封鎖 URL 的數目。 桌面小工具會列出包含最多已封鎖 URL 數目的七個網站類別，並將其餘的網站類別結合到 **[其他]** 中。 如需有關網站類別的詳細資訊，請參閱 Cyber Protection 中的 URL 篩選主題。
安全性事件待執行工作	此桌面小工具會顯示所選公司將事件結案的效率；未結案事件的數目是根據一段時間內已結案事件的數目來衡量的。 將滑鼠暫留在某個欄上可檢視所選日期已結案和未結案事件的明細。顯示在括號中的 % 值表示與前一段時間相比增加或減少。
事件 MTTR	此桌面小工具會顯示安全性事件的平均解決時間。它會指出調查並解決事件的速度。 按一下某個欄可根據嚴重性 (**[重大]**、**[高]** 和 **[中]**) 檢視事件的明細，以及解決不同嚴重性層級所需的時間。顯示在括號中的 % 值表示與前一段時間相比增加或減少。
威脅狀態	此桌面小工具會顯示公司工作負載 (無論有多少工作負載) 的目前威脅狀態，並醒目提示未緩解而且需要調查的目前事件數目。此桌面小工具也會指出已緩解 (系統手動和/或自動) 的事件數目。

桌面小工具	描述
保護技術偵測到的威脅	此桌面小工具會針對指定的日期範圍，顯示依下列保護技術分組的已偵測到威脅的數目： • 反惡意程式碼掃描 • 行為引擎 • 加密採礦保護 • 漏洞利用防禦 • 勒索軟體主動防護 • 即時保護 • URL 篩選

備份桌面小工具

下表提供有關 **[備份]** 區段中桌面小工具的詳細資訊。

桌面小工具	描述
已備份的工作負載	此桌面小工具會依備份狀態顯示已註冊工作負載的總數。 **已備份** - 在報告日期範圍期間已備份的工作負載數量 (至少已執行一個成功備份)。 **未備份** - 在報告日期範圍期間未備份的工作負載數量 (未執行任何成功備份)。
實體裝置的磁碟健全狀況狀態	此桌面小工具會根據實體裝置磁碟的健全狀況狀態，顯示其彙總的健全狀況狀態。 **正常** - 此磁碟健全狀況狀態與值 [70-100] 相關。當裝置的所有磁碟都處於 **[正常]** 狀態時，則裝置的狀態為 **[正常]**。 **警告** - 此磁碟健全狀況狀態與值 [30-70] 相關。當裝置至少有一個磁碟的狀態為 **[警告]** 時，以及當沒有磁碟處於 **[錯誤]** 狀態時，則裝置的狀態為 **[警告]**。 **錯誤** - 此磁碟健全狀況狀態與值 [0-30] 相關。當裝置至少有一個磁碟的狀態為 **[錯誤]** 時，則裝置的狀態為 **[錯誤]**。 **正在計算磁碟資料** - 還未計算裝置的狀態時，裝置的狀態為 **[正在計算磁碟資料]**。
備份儲存空間使用量	此桌面小工具會針對指定的時間範圍，顯示雲端和本機儲存空間中備份的總數和大小總計。

弱點評估和修補程式管理桌面小工具

下表提供有關 **[弱點評估和修補程式管理]** 區段中桌面小工具的詳細資訊。

桌面小工具	描述
已修補的弱點	此桌面小工具會針對指定的日期範圍，顯示弱點評估效能結果。 **總計**- 已修補的弱點總數。 **Microsoft 軟體弱點** - 所有 Windows 裝置上已修正的 Microsoft 弱點總數。 **Microsoft 協力廠商軟體弱點** - 所有 Windows 裝置上已修正的 Microsoft 協力廠商弱點總數。 **已掃描的工作負載** - 在指定的日期範圍內，至少已成功掃描弱點一次的裝置的總數。
已安裝的修補程式	此桌面小工具會針對指定的日期範圍，顯示修補程式管理效能結果。 **已安裝** - 已成功安裝在所有裝置上的修補程式總數。 **Microsoft 軟體修補程式** - 已在所有 Windows 裝置上安裝的 Microsoft 軟體修補程式總數。 **Windows 協力廠商軟體修補程式** - 已在所有 Windows 裝置上安裝的 Windows 協力廠商軟體修補程式總數。 **已修補的工作負載** - 已成功修補的裝置總數 (在指定的日期範圍期間安裝的至少一個修補程式)。

軟體小工具

下表提供有關 **[軟體]** 區段中小工具的詳細資訊。

桌面小工具	描述
安裝狀態	此小工具會顯示按狀態分組的安裝活動總數。按一下環狀圖的某個部分會將您重新導向至 **[活動]** 頁面，其中僅會顯示具有對應狀態的活動，並按時間順序排列。
解除安裝狀態	此小工具會顯示按狀態分組的解除安裝活動總數。按一下環狀圖的某個部分會將您重新導向至 **[活動]** 頁面，其中僅會顯示具有對應狀態的活動，並按時間順序排列。
軟體安裝歷程記錄	此小工具提供受管理裝置上遠端軟體安裝的詳細狀態資訊。按一下 **[安裝狀態]** 欄中的狀態可將您重新導向至 **[活動]** 頁面，其中會依時間順序，顯示具有對應狀態的活動。
軟體解除安裝歷程記錄	此小工具提供受管理裝置上遠端軟體解除安裝的詳細狀態資訊。按一下 **[解除安裝狀態]** 欄中的狀態可將您重新導向至 **[活動]** 頁面，其中會依時間順序，顯示具有對應狀態的活動。

Disaster Recovery 桌面小工具

下表提供有關 **[災難復原]** 區段中桌面小工具的詳細資訊。

桌面小工具	描述
Disaster Recovery 統計資料	此桌面小工具會針對指定的日期範圍，顯示Disaster Recovery 主要效能指標。 **實際執行容錯移轉** - 指定的日期範圍內，實際執行容錯移轉作業的數目。 **測試容錯移轉** - 在指定的時間範圍期間執行的測試容錯移轉作業總數。 **主要伺服器** - 報告產生時主要伺服器的總數。 **復原伺服器** - 報告產生時復原伺服器的總數。 **公用 IP** - 公用 IP 位址的總數 (報告產生時)。 **已耗用的計算點總計** - 在指定的時間範圍期間耗用的計算點總數。
已測試的Disaster Recovery 伺服器	此桌面小工具會顯示已受到Disaster Recovery 保護並使用測試容錯移轉測試的伺服器的相關資訊。 此桌面小工具會顯示下列指標： **受保護的伺服器** - 報告產生時，受Disaster Recovery 保護的伺服器數目 (至少有一部復原伺服器的伺服器)。 **已測試** - 在所選時間範圍期間，受Disaster Recovery 保護的所有伺服器中，受Disaster Recovery 保護且使用測試容錯移轉測試的伺服器數目。 **未測試** - 在所選時間範圍期間，受Disaster Recovery 保護的所有伺服器中，受Disaster Recovery 保護且未使用測試容錯移轉測試的伺服器數目。 此桌面小工具也會顯示報告產生時，Disaster Recovery 儲存空間的大小 (GB)。亦即，雲端伺服器備份大小的加總。
已受到Disaster Recovery 保護的伺服器	此桌面小工具會顯示已受到Disaster Recovery 保護的伺服器以及未受保護的伺服器的相關資訊。 此桌面小工具會顯示下列指標： 報告產生時，在客戶租用戶中註冊的伺服器總數。 **已受保護** - 報告產生時，在所有已註冊的伺服器中，受Disaster Recovery 保護的伺服器數目 (至少有一部復原伺服器以及一個完整的伺服器備份)。 **未受保護** - 報告產生時，在所有已註冊的伺服器中，未受保護的伺服器總數。

資料洩漏防禦桌面小工具

以下主題提供有關 **[資料洩漏防禦]** 區段中已封鎖的週邊裝置的詳細資訊。

此桌面小工具會針對指定的日期範圍，顯示已封鎖裝置總數以及依裝置類型分組的已封鎖裝置總數。

- 卸除式儲存裝置
- 加密的卸除式
- 印表機
- 剪貼簿 - 包括剪貼簿和螢幕擷取畫面擷取裝置類型。
- 行動裝置
- 藍牙
- 光碟機
- 軟碟機
- USB - 包括 USB 連接埠和重新導向的 USB 連接埠裝置類型。
- FireWire
- 對應磁碟機
- 重新導向的剪貼簿 - 包括重新導向的剪貼簿傳入裝置類型和重新導向的剪貼簿傳出裝置類型。

此桌面小工具會顯示已封鎖裝置數目最多的前七個裝置類型，並將其餘的裝置類型結合到 **[其他]** 裝置類型中。

File Sync & Share 桌面小工具

下表提供有關 **[File Sync & Share]** 區段中桌面小工具的詳細資訊。

桌面小工具	描述
File Sync & Share 統計資料	此桌面小工具會顯示下列指標： **已使用的雲端儲存空間總計** - 所有使用者的儲存空間使用量總計。 **終端使用者** - 終端使用者的總數。 **每個終端使用者使用的平均儲存空間** - 每個終端使用者的平均儲存空間使用量。 **來賓使用者** - 來賓使用者的總數。
終端使用者的 File Sync & Share 儲存空間使用量	此桌面小工具會顯示儲存空間使用量在下列範圍內的 File Sync & Share 終端使用者總數： • 0 - 1 GB • 1 - 5 GB • 5 - 10 GB • 10 - 50 GB • 50 - 100 GB • 100 – 500 GB • 500 - 1 TB • 1+ TB

Notary 桌面小工具

下表提供有關 **[Notary]** 區段中桌面小工具的詳細資訊。

桌面小工具	描述
Cyber Notary 統計資料	此桌面小工具會顯示下列 Notary 指標： **已使用的 Notary 雲端儲存空間** - 用於 Notary 服務的儲存空間大小總計。 **已公證的檔案** - 已公證檔案的總數。 **已電子簽署的文件** - 已電子簽署的文件和檔案的總數。
終端使用者已公證的檔案	顯示所有終端使用者已公證檔案的總數。使用者根據他們所擁有的已公證檔案數量進行分組。 • 最多 10 個檔案 • 11 - 100 個檔案 • 101 - 500 個檔案 • 501 - 1000 個檔案 • 1000+ 個檔案
終端使用者已電子簽署的文件	此桌面小工具會顯示所有終端使用者已公證文件和檔案的總數。使用者根據他們所擁有的已電子簽署文件和檔案數量進行分組。 • 最多 10 個檔案 • 11 - 100 個檔案 • 101 - 500 個檔案 • 501 - 1000 個檔案 • 1000+ 個檔案

設定執行摘要報告的設定

您可以更新建立執行摘要報告時設定的報告設定。

若要更新執行摘要報告的設定

1. 在管理主控台中，前往 **[報告]** > **[執行摘要]**。
2. 按一下您要更新的執行摘要報告的名稱。
3. 按一下 **[設定]**。
4. 如有需要，請變更欄位的值。
5. 按一下 **[儲存]**。

建立執行摘要報告

您可以建立執行摘要報告、預覽其內容、設定報告收件者，並排程自動傳送時間。

若要建立執行摘要報告

1. 在管理主控台中，前往 **[報告]** > **[執行摘要]**。
2. 按一下 **[建立執行摘要報告]**。
3. 在 **[報告名稱]** 中，輸入報告的名稱。

4. 選擇報告收件者。
   - 如果您希望將報告傳送給所有聯絡人和使用者，選擇 **[傳送至所有聯絡人和使用者]**。
   - 如果您希望將報告傳送給特定聯絡人和使用者
     a. 清除 **[傳送至所有聯絡人和使用者]**。
     b. 按一下 **[選擇聯絡人]**。
     c. 選擇特定聯絡人和使用者。您可以使用 [搜尋]，輕鬆找到特定聯絡人。
     d. 按一下 **[選擇]**。
5. 選擇範圍：**[30 天]** 或 **[本月]**
6. 選擇檔案格式：**[PDF]**、**[Excel]** 或 **[Excel 和 PDF]**。
7. 設定排程設定。
   - 如果您希望在特定的日期和時間，將報告傳送給收件者：
     a. 啟用 **[排程]** 選項。
     b. 按一下 **[月份日期]** 欄位、清除 [最後一天] 欄位，然後按一下您要設定的日期。
     c. 在 **[時間]** 欄位中，輸入您要設定的小時。
     d. 按一下**[套用]**。
   - 如果您要建立報告，但不傳送給收件者，請停用 **[排程]** 選項。
8. 按一下 **[儲存]**。

自訂執行摘要報告

您可以決定要包含在執行摘要報告中的資訊。您可以新增或刪除區段、新增或刪除桌面小工具、重新命名區段、自訂桌面小工具，並拖放桌面小工具和區段，以變更資訊在報告中出現的順序。

若要新增區段

1. 按一下 **[新增項目]** > **[新增區段]**。
2. 在 **[新增區段]** 視窗中，輸入區段名稱，或使用預設的區段名稱。
3. 按一下 **[新增至報告]**。

若要重新命名區段

1. 在您要重新命名的區段中，按一下 **[編輯]**。
2. 在 **[編輯區段]** 視窗中，輸入新的名稱。
3. 按一下 **[儲存]**。

若要刪除區段

1. 在您要刪除的區段中，按一下 **[刪除區段]**。
2. 在 **[刪除區段]** 確認視窗中，按一下 **[刪除]**。

若要使用預設設定，將桌面小工具新增至區段

1. 在您要新增桌面小工具的區段中，按一下 **[新增桌面小工具]**。
2. 在 **[新增桌面小工具]** 視窗中，按一下您要新增的桌面小工具。

若要將自訂的桌面小工具新增至區段

1. 在您要新增桌面小工具的區段中，按一下 **[新增桌面小工具]**。
2. 在 **[新增桌面小工具]** 視窗中，尋找您要新增的桌面小工具，然後按一下 **[自訂]**。
3. 必要時，請設定欄位。
4. 按一下 **[新增桌面小工具]**。

若要使用預設設定，將桌面小工具新增至報告

1. 按一下 **[新增項目]** > **[新增桌面小工具]**。
2. 在 **[新增桌面小工具]** 視窗中，按一下您要新增的桌面小工具。

若要將自訂的桌面小工具新增至報告

1. 按一下 **[新增桌面小工具]**。
2. 在 **[新增桌面小工具]** 視窗中，尋找您要新增的桌面小工具，然後按一下 **[自訂]**。
3. 必要時，請設定欄位。
4. 按一下 **[新增桌面小工具]**。

若要重設桌面小工具的預設設定

1. 在您要自訂的桌面小工具中，按一下 **[編輯]**。
2. 按一下 **[重設為預設值]**。
3. 按一下**[完成]**。

若要自訂桌面小工具

1. 在您要自訂的桌面小工具中，按一下 **[編輯]**。
2. 必要時，請編輯欄位。
3. 按一下**[完成]**。

傳送執行摘要報告

您可以視需要傳送執行摘要報告。在此情況下，系統會忽略 **[排程]** 設定，並立即傳送報告。傳送報告時，系統會使用在 **[設定]** 中設定的 [收件者]、[範圍] 和 [檔案格式] 值。您可以在傳送報告前，手動變更這些設定。如需詳細資訊，請參閱 "設定執行摘要報告的設定" (第 75 頁)。

若要傳送執行摘要報告

1. 在管理入口網站中，前往 **[報告]** > **[執行摘要]**。
2. 按一下您要傳送的執行摘要報告的名稱。
3. 按一下 **[立即傳送]**。

   系統隨即將執行摘要報告傳送給所選收件者。

報告中的時區

報告中所使用的時區會依報告類型而有所不同。下表包含可供您參考的資訊。

報告位置和類型	報告中所使用的時區
管理入口網站 > [監控] > [營運] (桌面小工具)	報告產生的時間採用執行瀏覽器所在電腦的時區。
管理入口網站 > [監控] > [營運] (匯出至 PDF 或 xslx)	• 已匯出報告的時間戳記採用匯出報告所使用電腦的時區。 • 報告中所顯示活動的時區為 UTC。
管理入口網站 > [報告] > [使用狀況] > [排程報告]	• 系統會在每個月第一天的 23:59:59 (UTC 時間) 產生報告。 • 系統會在每個月第二天傳送報告。
管理入口網站 > [報告] > [使用狀況] > [自訂報告]	報告的時區和日期為 UTC。
管理入口網站 > [報告] > [營運] (桌面小工具)	• 報告產生的時間採用執行瀏覽器所在電腦的時區。 • 報告中所顯示活動的時區為 UTC。
管理入口網站 > [報告] > [營運] (匯出至 PDF 或 xslx)	• 已匯出報告的時間戳記採用匯出報告所使用電腦的時區。 • 報告中所顯示活動的時區為 UTC。
管理入口網站 > [報告] > [營運] (排程交付)	• 報告交付的時區為 UTC。 • 報告中所顯示活動的時區為 UTC。
管理入口網站 > [使用者] > [作用中警示的相關每日摘要]	• 系統會在每天的 10:00 到 23:59 UTC 之間傳送報告一次。報告傳送的時間取決於資料中心的工作負載。 • 報告中所顯示活動的時區為 UTC。
管理入口網站 > [使用者] > [資安防護狀態通知]	• 此報告會在活動完成時傳送。 **注意事項** 根據資料中心的工作負載而定，部分報告可能會延遲傳送。 • 報告中活動的時區為 UTC。

根據桌面小工具類型回報的資料

根據所顯示的資料範圍，儀表板上的桌面小工具有兩種類型：

- 顯示瀏覽或報告產生時實際資料的桌面小工具。
- 顯示歷史資料的桌面小工具。

當您在報告設定中，將資料範圍設定為特定期間的傾印資料時，所選時間範圍僅適用於顯示歷史資料的桌面小工具。若是顯示瀏覽時實際資料的桌面小工具，則時間範圍參數不適用。

下表列出可用的桌面小工具及其資料範圍。

桌面小工具名稱	顯示在桌面小工具和報告中的資料

依電腦分類的 #CyberFit 分數	實際
5 個最新的警示	實際
作用中警示詳細資訊	實際
作用中警示摘要	實際
活動	歷史報告
活動清單	歷史報告
警示歷程記錄	歷史報告
備份的反惡意程式碼掃描	歷史報告
檔案的反惡意程式碼掃描	歷史報告
備份掃描詳細資料 (威脅)	歷史報告
備份狀態	歷史 - 在 **[執行總計]** 和 **[成功執行的數量]** 欄中 實際 - 在其他所有欄中
備份儲存空間使用量	歷史報告
已封鎖的週邊裝置	歷史報告
已封鎖的 URL	實際
雲端應用程式	實際
雲端工作負載保護狀態	實際
Cyber protection	實際
網路保護摘要	歷史報告
資料保護圖	歷史報告
裝置	實際
已測試的災難復原伺服器	歷史報告
災難復原統計資料	歷史報告
已探索到的裝置	實際
磁碟健全狀況概觀	實際
磁碟健全狀況狀態	實際
實體裝置的磁碟健全狀況狀態	實際
終端使用者已電子簽署的文件	實際
現有的弱點	歷史報告

File Sync & Share 統計資料	實際
終端使用者的 File Sync & Share 儲存空間使用量	實際
硬體變更	歷史報告
硬體詳細資料	實際
硬體清查	實際
歷史警示摘要	歷史報告
位置摘要	實際
遺漏的更新 (依類別)	實際
未保護	實際
終端使用者已公證的檔案	實際
Notary 統計資料	實際
修補程式安裝歷史記錄	歷史報告
修補程式安裝狀態	歷史報告
修補程式安裝摘要	歷史報告
已修補的弱點	歷史報告
已安裝的修補程式	歷史報告
保護狀態	實際
最近受影響	歷史報告
遠端工作階段	歷史報告
安全性事件待執行工作	歷史報告
安全性事件 MTTR	歷史報告
已受到災難復原保護的伺服器	實際
軟體清查	實際
軟體概觀	歷史報告
威脅狀態	實際
保護技術偵測到的威脅	歷史報告
每個工作負載的最高事件分佈	實際
易受攻擊的電腦	實際
工作負載網路狀態	實際

已備份的工作負載	歷史報告
工作負載保護狀態	實際

整合

支援整合以提供第三方資安防護、端點管理、客戶管理、監控、分析等功能，並與標準 Cyber Protect 主控台產品並列，同樣透過第三方軟體平台，向客戶提供我們的解決方案。

目前有超過 200 種整合可自動化日常例行工作，並提高我們的合作夥伴及其客戶的效率。

整合項目會列在 整合目錄上。

注意事項
部分整合會要求 API 用戶端存取 應用程式設計介面 (API)。

整合目錄

整合目錄會列出可用的 整合：

- 應用程式目錄。
  此目錄可供公開使用。無法從此目錄啟用整合。
  如果您看到要使用的整合，請聯絡您的合作夥伴以便為您啟用。
- 資料中心 (DC) 目錄。
  這些目錄是資料中心專用的。您可以從這些目錄啟用整合。
  合作夥伴層級管理入口網站系統管理員可以：
  - 查看資料中心上部署的所有整合。
  - 為自己或為客戶啟用在資料中心部署的所有整合。

  客戶層級管理入口網站系統管理員可以：
  - 僅看到整合開發人員明確設定為客戶可見的整合。
  - 僅啟用整合開發人員明確允許客戶啟用的整合。

  注意事項
  合作夥伴層級管理入口網站系統管理員必須在可以由客戶層級管理入口網站系統管理員啟用之前，在合作夥伴層級啟用整合。

目錄項目

目錄項目包含兩個部分：

- 目錄卡片提供整合的概觀。
- 目錄詳細資料頁面可提供更多資訊，例如完整的功能性說明、螢幕擷取畫面、影片、功能清單、聯絡人詳細資料、整合資源的連結等。

開啟您的資料中心整合目錄

在資料中心 (DC) 整合目錄中，每個目錄卡片都會顯示一個簡短的產品描述和兩個按鈕：

- **瞭解更多詳情**

  每個整合目錄項目也會有一個包含整合詳細資料的頁面，其中包括完整的功能性描述、螢幕擷取畫面、影片、功能清單、聯絡人詳細資料、整合資源的連結等。

  按一下此按鈕可開啟整合詳細資料頁面。
- **設定**

  按一下此按鈕可啟用整合。

注意事項
代表非作用中整合的目錄卡片會顯示為灰色，而且會遭到停用。

若要開啟 DC 整合目錄

1. 開啟管理入口網站。
2. 從主功能表中選擇 **[整合]**。

   預設會開啟 **[所有整合]** 索引標籤。這會顯示客戶層級管理入口網站系統管理員可以啟用的整合的目錄卡片。
3. [選用] 選擇類別，並在搜尋欄位中輸入文字以篩選目錄卡片。

檢視已啟用的整合

整合目錄的 **[整合使用中]** 索引標籤會顯示您已啟用的每個整合的卡片。

若要檢視您已啟用的整合

1. 在資料中心中開啟整合目錄。
2. 選擇 **[整合使用中]** 索引標籤。

開啟應用程式目錄

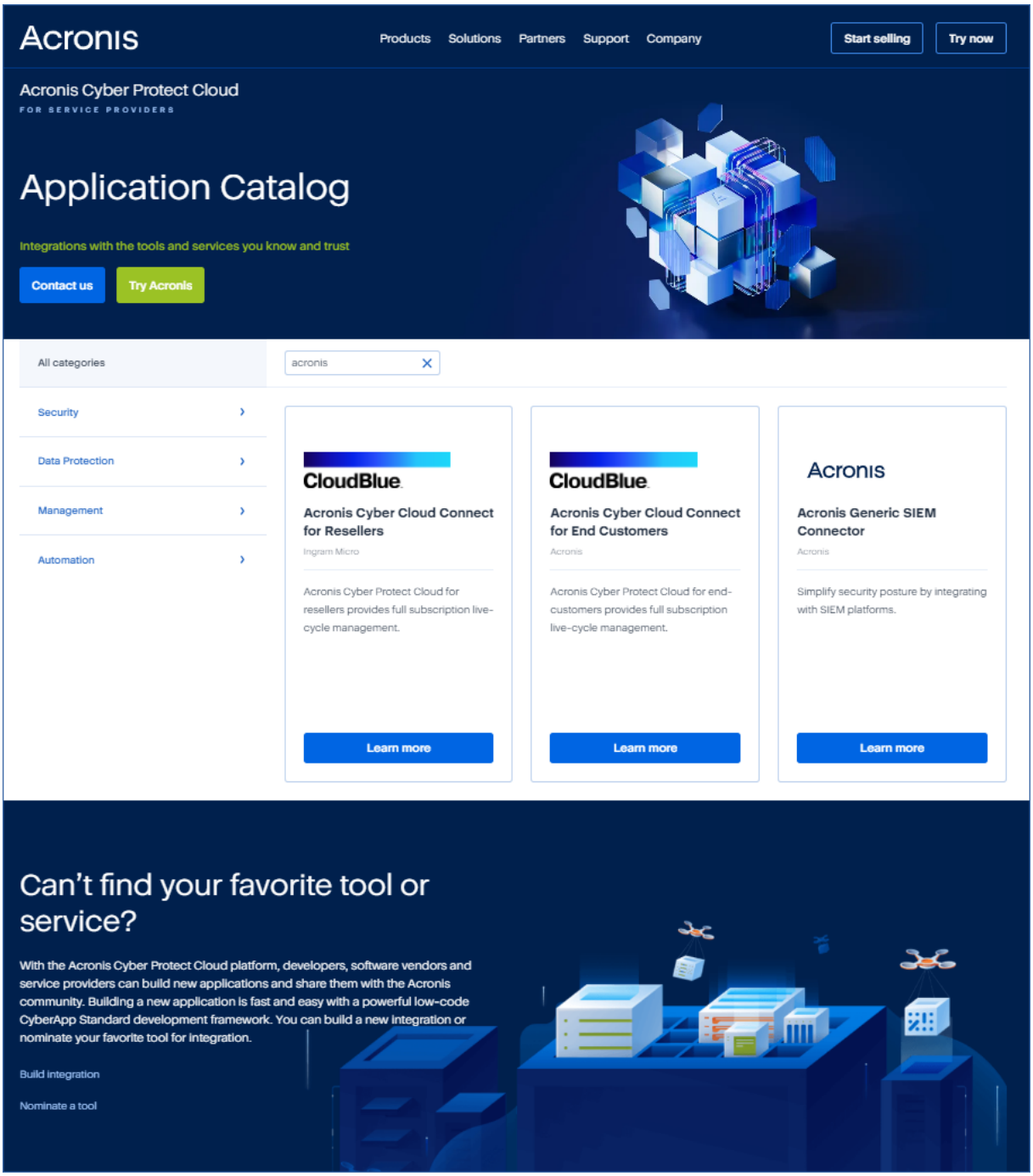
應用程式目錄會列出所有 Cyber Protect Cloud 整合。

注意事項
如果您找出要使用的整合，則必須聯絡您的合作夥伴才能為您啟用。

若要開啟應用程式目錄

1. 瀏覽 solutions.acronis.com。

   初始檢視是所有目錄卡片的網格。
2. [選用] 選擇類別，並在搜尋欄位中輸入文字以篩選目錄卡片。



開啟整合詳細資料頁面

每個目錄項目也會有一個包含整合詳細資料的頁面，例如完整的功能性描述、螢幕擷取畫面、影片、功能清單、聯絡人詳細資料、整合資源的連結等。

若要開啟整合詳細資料頁面

1. 瀏覽 solutions.acronis.com。
2. 找出您感興趣的整合的目錄卡片。
3. 按一下目錄卡片上的 **[深入瞭解]**。

Acronis

Products Solutions Partners Support Company

Start selling Try now

Acronis Cyber Protect Cloud

FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Contact us Try Acronis

← Back to integrations

Have a question or need help?

Acronis

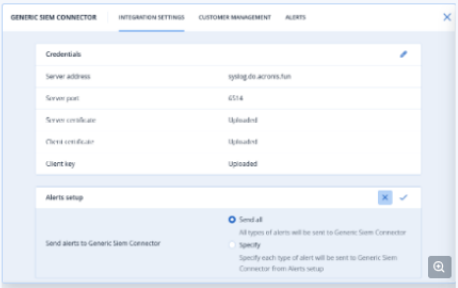
Integration: Acronis Generic SIEM Connector
Category: SIEM
Company: Acronis

Website

Acronis Generic SIEM Connector

SIEM (Security Information and Event Management) platforms are used by many MSPs for security incident investigation and remediation, threat hunting, and compliance. Acronis Generic SIEM Connector allows MSPs to forward Acronis Cyber Protect Cloud alerts to any SIEM system that supports the CEF event format over SYSLOG for further correlation and analysis to reveal patterns of activity that may indicate an attempt of intrusion.

Integration Overview



Simplify security posture by integrating with SIEM platforms.

SIEMs empower MSPs security specialists to identify attack rout across the network and get visibility into compromised files. Now with Acronis Generic SIEM connector, MSPs will gain extra visibility into customers networks, will be able to search for threats across all managed workloads, and correlate events from both security and data protection applications, and run response actions.

Features

Support of core event format
Acronis supports core event format - CEF (Common Event Format), enabling MSPs to work with any SIEM that supports CEF format out of the box. Alerts are transferred to SIEM via syslog server.

Threat hunting across all managed companies
Integration allows MSPs to select which customer tenants in Acronis should send alerts to SIEM. Since alerts are sent to the same SIEM instance, it's possible to run correlation, threat hunting and perform investigation for all customers in the same console. It also empowers MSPs to search for threats, that were discovered on one workload in one customer tenant, in other customers environments.

Simple integration enablement
It's very easy to enable the integration by obtaining server and client certificates, establishing connection to the server and specifying the server port.

Select data you want to see
It is possible to select which alerts should be sent to SIEM. With this functionality, MSPs benefit from reducing the amount of sent to SIEM data and, therefore, lower SIEM invoice. MSPs can select and work only with the data that is necessary.

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

With the Acronis Cyber Protect Cloud platform, developers, software vendors and service providers can build new applications and share them with the Acronis community. Building a new application is fast and easy with a powerful low-code CyberApp Standard development framework. You can build a new integration or nominate your favorite tool for integration.

Build integration

Nominate a tool

Engage with Acronis

啟用整合

注意事項

合作夥伴層級管理入口網站系統管理員必須在可以由客戶層級管理入口網站系統管理員啟用之前，在合作夥伴層級啟用整合。

若要啟用整合

1. 在 DC 上開啟整合目錄。
2. 找出您要啟用的整合的目錄卡片。

   若要篩選整合：

   - [選用] 選擇類別。
   - [選用] 在搜尋欄位中輸入字串。
3. 按一下目錄卡片上的 **[設定]**。
4. 依照畫面上的說明操作。

設定作用中的整合

若要設定作用中的整合

1. 在資料中心中開啟整合目錄。
2. 選擇 **[整合使用中]** 索引標籤。
3. [選用] 選擇類別，並在搜尋欄位中輸入文字以篩選目錄卡片。
4. 找出您要設定的整合的目錄卡片。
5. 按一下 **[設定]**。

   整合設定畫面隨即開啟。
6. 依照畫面上的說明操作。

停用作用中的整合

若要停用整合

1. 在 DC 上開啟整合目錄。
2. 選擇 **[整合使用中]** 索引標籤。
3. 找出您要停用的整合的目錄卡片。
4. 按一下目錄卡片右上角的省略符號 (...) 圖示。
5. 選擇 **[停用]**。
6. 請依照任何畫面上的指示操作。

API 用戶端

第三方系統整合可以使用 應用程式開發介面 (API)。您可以透過 API 用戶端 (平台 OAuth 2.0 授權架構的完整部分) 啟用對這些 API 的存取。

API 用戶端是一個特殊的平台帳戶，代表必須驗證並獲得授權才能存取 平台資料和服務資料的第三方系統。API 用戶端存取僅限於其管理入口網站系統管理員建立用戶端的租用戶和任何子租用戶。

注意事項
API 用戶端會繼承系統管理員帳戶的服務角色，而且之後無法變更這些角色。變更系統管理員帳戶的角色或停用系統管理員帳戶都不會影響用戶端。

API 用戶端認證

API 用戶端認證由唯一識別碼 (ID) 和密碼值組成。這些認證不會過期，且無法用來登入管理入口網站或其他任何服務主控台。

注意事項
您無法為用戶端啟用雙重驗證機制。

API 用戶端流程

1. 管理入口網站系統管理員會建立 API 用戶端。
2. 系統管理員會在第三方系統中啟用 OAuth 2.0 用戶端認證流程。
3. 根據此流程，在透過 API 存取租用戶及其服務之前，系統必須先使用授權 API，將 API 用戶端認證傳送到平台。
4. 平台會產生並傳回安全性權杖，也就是指派給此特定用戶端的唯一加密字串。
5. 第三方系統必須將此權杖新增至所有 API 要求。

注意事項
安全性權杖不需要傳遞具有 API 要求的用戶端認證。
為獲得額外的安全性，安全性權杖將會在兩小時後過期。
此時間之後，權杖過期的所有 API 要求都將失敗，而且系統必須向平台要求新的權杖。

建立 API 用戶端

若要建立 API 用戶端

1. 登入管理入口網站。
2. 按一下 **[設定]** > **[API 用戶端]** > **[建立 API 用戶端]**。
3. 輸入 API 用戶端的名稱。
4. 按 **[下一步]**。
   API 用戶端建立時，預設為 **[作用中]** 狀態。

5. 複製並儲存 API 用戶端的 ID 和密碼值，以及資料中心 URL。在第三方系統中啟用 OAuth 2.0 用戶端認證流程時，您將需要這些資訊。

   重要事項
   基於安全性，密碼值僅顯示一次。如果遺失這個值，則無法擷取，但可以重設。

6. 按一下**[完成]**。

重設 API 用戶端密碼值

如果您遺失 API 用戶端密碼值，則可以產生新的密碼值。用戶端 ID 和資料中心 URL 不會變更。

重要事項
如果您重設密碼值，則指派給用戶端的所有安全性權杖將立即到期，且具有這些權杖的 API 要求將會失敗。

若要重設 API 用戶端密碼值

1. 登入管理入口網站。
2. 按一下 **[設定]** > **[API 用戶端]**。
3. 在清單中尋找所需的用戶端。
4. 按一下 ，然後按一下 **[重設密碼]**。
5. 按一下 **[下一步]** 以確認您的決定。
6. 複製並儲存新的 API 用戶端密碼值。

   注意事項
   基於安全性，密碼值僅顯示一次。如果遺失這個值，則無法擷取，可以透過重複上述步驟重設。

7. 按一下**[完成]**。

停用 API 用戶端

您可以停用 API 用戶端。如果這樣做，具有指派給用戶端的安全性權杖的 API 要求將失敗，但權杖不會立即過期。

注意事項
停用用戶端不會影響權杖的到期時間。

您可以隨時重新啟用 API 用戶端。

若要停用 API 用戶端

1. 登入管理入口網站。
2. 按一下 **[設定]** > **[API 用戶端]**。
3. 在清單中尋找所需的用戶端。

4. 按一下 ，然後按一下 **[停用]**。
5. 確認選項無誤。

啟用已停用的 API 用戶端

如果您啟用已停用的 API 用戶端，則**如果這些權杖尚未過期**，指派給用戶端的安全性權杖的 API 要求將會成功。

若要啟用已停用的 API 用戶端

1. 登入管理入口網站。
2. 按一下 **[設定]** > **[API 用戶端]**。
3. 在清單中尋找所需的用戶端。
4. 按一下 ，然後按一下 **[啟用]**。

   API 用戶端的狀態將會變更為 **[作用中]**。

刪除 API 用戶端

如果您刪除 API 用戶端，則指派給此用戶端的所有安全性權杖將立即到期，且具有這些權杖的 API 要求將會失敗。

重要事項
您無法復原已刪除的用戶端。

若要刪除 API 用戶端

1. 登入管理入口網站。
2. 按一下 **[設定]** > **[API 用戶端]**。
3. 在清單中尋找所需的用戶端。
4. 按一下 ，然後按一下 **[刪除]**。
5. 確認選項無誤。

建立整合

若您有要與 Cyber Protect Cloud 整合的資料或服務，可以使用供應商入口網站建立原生 CyberApp，或使用 API 呼叫。

CyberApp

供應商入口網站是一個線上平台，可讓第三方軟體供應商依照我們的 CyberApp 標準最佳做法，在 Cyber Protect Cloud 中以原生方式整合產品和服務。供應商入口網站整合稱為 CyberApp。

注意事項
如需有關 CyberApps 和供應商入口網站的詳細資訊，請參閱 整合指南。

API 整合

包含 API 用於整合的完整套件。

注意事項

如需有關 API 的詳細資訊，請參閱整合指南的 平台 API 章節。

索引