Cyber Protect Cloud

24.03

合作夥伴系統管理員指南

版本：2024/4/10

目錄

關於本文件

本文件適用對象為想要使用 Cyber Protect Cloud 為其用戶端提供服務的合作夥伴系統管理員。

本文件說明如何使用管理入口網站設定及管理 Cyber Protect Cloud 中提供的服務。

關於 Cyber Protect

Cyber Protect 是一款雲端平台，可供服務提供者、經銷商和代理商為其合作夥伴和客戶提供資料保護服務。

服務由合作夥伴層級提供，下有客戶公司層級和終端使用者層級。

服務管理可透過名為**服務主控台**的 Web 應用程式來執行。租用戶和使用者帳戶管理可透過名為**管理入口網站**的 Web 應用程式來執行。

管理入口網站可讓系統管理員執行以下事項：

- 監控服務使用狀況及存取服務主控台
- 管理租用戶
- 管理使用者帳戶
- 設定租用戶的服務和配額
- 管理儲存空間
- 管理商標
- 產生關於服務使用狀況的報告

Cyber Protect 服務

本節說明 2021 年 3 月推出的功能集以及新的計費模型。請在 Cyber Protect 產品說明中閱讀更多關於新計費模型的優點。

Cyber Protect Cloud 提供下列服務和功能集：

- **Cyber Protect**
  - **保護** - 完整的網路保護，其中包含基礎產品中隨附的安全性和管理功能，以及災難復原、備份和復原、自動化與電子郵件安全性等按用量付費功能。使用進階保護套件可以擴展此功能，但需要額外付費。
    進階保護套件是一組獨特的功能，可在特定的功能區域解決更複雜的案例，例如 Advanced Backup、Advanced Security + EDR 等等。進階套件可擴展標準 Cyber Protect 服務中可用的功能。
    如需有關進階保護套件的詳細資訊，請參閱 "進階保護套件" (第 111 頁)。
  - **File Sync & Share** - 隨時隨地在任何裝置上安全地共用公司內容的一種解決方案。
  - **實體資料運送** - 透過將硬碟上的資料傳送到雲端資料中心來協助您節約時間和網路流量的一種解決方案。
  - **Notary** - 可確保共用內容真實性的一種區塊鏈型解決方案。
- **Cyber Infrastructure SPLA**

在管理入口網站中，您可以選擇您的租用戶可以使用的服務和功能集。當您佈建或編輯租用戶時，會為每個租用戶進行設定，如建立租用戶中所述。

Cyber Protect 的計費模式

計費模式是一種用於對服務及其功能的使用進行計算和計費的方案。計費模式可決定將當作定價計算基礎使用的單位。計費模式可以由合作夥伴在客戶層級設定。

授權引擎會根據保護計劃中所要求的功能，自動取得產品項目。使用者可以透過自訂其保護計劃，將保護層級和成本最佳化。

注意事項
每個客戶租用戶僅能使用一種計費模式。

保護 元件的計費模式

保護 有兩種計費模式：

- 按工作負載
- 按 GB

兩種計費模式的功能集都相同。

在兩種計費模式中，保護服務包括涵蓋大多數網路安全風險的標準保護功能。使用者可以免費使用這些功能。隨附功能的使用將會列入計算，但不會計費。如需隨附產品項目與可計費產品項目的完整清單，請參閱 "Cyber Protect 服務" (第 7 頁)。

雖然進階套件是針對客戶啟用的，但只會在客戶開始使用隨附在保護計劃中的功能之後，才會開始計費。在保護計劃中套用進階功能時，授權引擎會將所需的授權自動指派給受保護的工作負載。

不再使用進階功能時，便會撤銷授權，並停止計費。授權引擎會自動指派反映功能實際使用量的授權。

您僅能指派標準 Cyber Protect 服務功能的授權。進階功能會根據使用量計費，且無法手動修改其授權。授權引擎會自動指派和取消指派這些授權。您可以手動變更工作負載的授權類型，但在使用者修改該工作負載的保護計劃之後，將會重新指派授權。

注意事項
啟用進階保護功能時，並不會開始計費。只有在客戶開始使用保護計劃中的進階功能之後，才會開始計費。已啟用的功能集將會列入計算並包含在使用情況報告中，但是除非使用這些功能，否則將不會計費。

File Sync & Share 的計費模式

File Sync & Share 有下列計費模式：

- 按使用者
- 按 GB

您也可以套用舊版 File Sync & Share 的計費規則。

注意事項

The billing for Advanced File Sync & Share does not start when you enable it.Billing starts only after a customer starts using its advanced features.The enabled advanced feature set will be accounted for and included in usage reports, but will not be billed for, unless its features are used.

實體資料運送的計費

實體資料運送的計費遵循按用量付費模式。

Notary 的計費

Notary 的計費遵循按用量付費模型。

搭配舊版使用計費模式

如果您仍未移轉至目前的計費模型，請在其中一種計費模式下使用產品項目以取代舊版。授權引擎會自動將指派給客戶的授權最佳化，以便將可計費的金額減至最少。

注意事項

您無法將版本與計費模式混合使用。

從舊版切換到目前的授權模型

您可以編輯租用戶的設定檔並為其選擇產品項目，以手動切換其產品項目。如需有關切換程序的詳細資訊，請參閱 "在版本和計費模式之間切換" (第 9 頁)。

若要為多個客戶從舊版切換到計費模式，請參閱適用於多個客戶的大量版本切換 (67942)。

在版本和計費模式之間切換

在管理入口網站中，您可以將租用戶帳戶修改為在計費模式之間切換 (從按工作負載切換到按 GB，反之亦然)，以及在舊版和計費模式之間切換。

如需有關大量切換租用戶的資訊，請參閱適用於多個客戶的大量版本切換 (67942)。

切換程序包括下列步驟。

1. 將新的產品項目佈建到客戶租用戶 (啟用產品項目和配額設定) 以符合在原始產品項目中提供的功能。
2. 取消指派未使用的產品項目，並根據保護計劃中使用的功能，將產品項目指派給工作負載 (使用量協調)。

下表說明兩個方向的程序。

	切換方向	
	版本 > 計費模式	**計費模式 > 計費模式**
產品	啟用產品項目以實現在來源版本中提供的功能。	系統將會啟用一組相同的產品項目。

	切換方向	
	版本 > 計費模式	**計費模式 > 計費模式**
項目切換		
配額切換	配額將會從來源產品項目複寫到目的地產品項目。來源標準 → 目的地標準產品。來源標準 → 目的地套件。 **注意事項** 如果您要從包含子版本的版本切換 (例如，「Cyber Protect (按工作負載)」)，將會摘要說明配額。	配額將會從來源產品項目複寫到目的地產品項目。
使用量切換	根據在工作負載上指派的保護計劃中要求的功能，產品項目將會重新指派給這些工作負載。	

範例：將 Cyber Protect Advanced 版本切換到按工作負載計費

在此案例中，客戶租用戶在 8 個工作站上使用 Cyber Protect Advanced 版本，且配額設定為 10 個工作負載。其中 3 個工作站在其保護計劃中使用軟體清查和修補程式管理、2 個工作站在其保護計劃中啟用 URL 篩選、1 部電腦使用連續資料保護。下表說明如何將版本轉換到新的產品項目。

來源產品項目 - 使用量/配額	目的地產品項目 - 使用量/配額
Cyber Protect Advanced Workstation 8/10	• 工作站 - 8/10 • Advanced Security + EDR - 2/10 • 進階備份工作站 - 1/10 • 進階管理 - 3/10

在切換期間會執行下列步驟：

1. 系統會自動啟用涵蓋在來源版本中提供的功能的產品項目。
2. 配額在新產品項目上會遭到複寫。
3. 使用量會根據保護計劃中的實際使用量加以協調：三個工作站使用進階管理套件的功能、兩個使用 Advanced Security + EDR 套件的功能、一個使用 Advanced Backup 套件的功能。

範例：Cyber Protect 按工作負載版本到按工作負載計費

在此範例中，客戶針對工作負載指派了多個版本。每個工作負載僅能獲指派一個版本或一個計費模式。

來源產品項目 - 使用量/配額	目的地產品項目 - 使用量/配額
Cyber Protect Essentials Workstation - 6/12	• 工作站 - 14/42 • 進階備份工作站 - 2/42 • Advanced Security + EDR - 13/42 • 進階管理 - 5/42
Cyber Protect Standard Workstation - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Cyber Backup Standard 工作站 - 1/10	

在切換期間會執行下列步驟：

1. 系統會自動啟用涵蓋在所有來源版本中提供之功能的產品項目。透過計費模式，可以視需要，將多個產品項目指派到一個工作站。
2. 系統會摘要說明並複寫配額。
3. 使用量會根據保護計劃加以協調。

變更合作夥伴租用戶的計費模式

若要變更合作夥伴租用戶的計費模式

1. 在管理入口網站中，前往 **[用戶端]**。
2. 選擇您要變更其計費模式的合作夥伴租用戶，按一下省略符號圖示 ，然後按一下 **[設定]**。
3. 在 **[Cyber Protect]** 索引標籤中，選擇您要變更其計費模式的服務，然後按一下 **[編輯]**。
4. 選擇所需的計費模式，並視需要啟用或停用可用的產品項目。
5. 按一下 **[儲存]**。

變更客戶租用戶的計費模式

您可以透過下列方式，變更客戶租用戶的計費：

- 啟用或停用產品項目，以編輯原始計費模式。
- 切換到全新的計費模式。

如需有關如何編輯可用產品項目的詳細資訊，請參閱啟用或停用產品項目。

若要切換客戶租用戶的計費模式

1. 在管理入口網站中，前往 **[用戶端]**。
2. 選擇您要變更其版本的客戶租用戶，按一下省略符號圖示 ，然後按一下 **[設定]**。
3. 在 **[設定]** 索引標籤的 **[服務]** 底下，選擇新的計費模式。
   接著會彈出一個對話方塊，告知您有關變更為新計費模式的後果。
4. 輸入您的使用者名稱以確認您的選擇。

注意事項
此變更最多可能需要 10 分鐘的時間才能完成。

產品項目和配額管理

本節描述下列內容:

- 什麼是服務和產品項目?
- 如何啟用或停用產品項目?
- 什麼是計費模式?
- 什麼是進階保護套件?
- 什麼是舊版和子版本?
- 什麼是彈性配額和硬性配額?
- 什麼時候可能會超過硬性配額?
- 什麼是備份配額轉換?
- 產品項目可用性如何影響 Cyber Protect 主控台中的工作負載類型可用性?

服務和產品項目

服務

雲端服務是由合作夥伴,或在一般客戶私有雲端上託管的一組功能。通常,服務是以訂閱形式或按用量付費的方式銷售。

Cyber Protect 服務可整合網路安全、資料保護和管理,以保護您的端點、系統和資料免於網路安全威脅。Cyber Protect 服務由數個元件所組成:保護、File Sync & Share、Notary,以及實體資料運送。透過進階保護套件,可以使用進階功能擴展其中的部分功能。如需有關隨附功能和進階功能的詳細資訊,請參閱 "Cyber Protect 服務" (第 7 頁)。

產品項目

產品項目是按特定工作負載類型或功能分組的一組服務功能,例如儲存、災難復原基礎架構等等。您可以透過啟用特定的產品項目,決定能夠保護的工作負載、可以保護的工作負載數量 (透過設定配額),以及將提供給您合作夥伴、客戶和終端使用者的保護程度 (透過啟用或停用進階保護套件)。

除非您設定追加銷售案例,否則客戶和使用者將看不到未啟用的功能。如需有關追加銷售案例的詳細資訊,請參閱 "設定適用於客戶的追加銷售案例" (第 58 頁)。

功能使用量是從服務收集的,並反映在產品項目上,以用於報告和進一步計費。

計費模式和版本

使用舊版時,您可以為每個工作負載啟用一個產品項目。功能透過計費模式分割,因此您可以為每個工作負載啟用多個產品項目 (服務功能和進階套件),以便更適合您客戶的需求,而且僅針對您客戶實際使用的功能,套用更精確的計費。

如需有關 Cyber Protect 的計費模式的詳細資訊,請參閱 "Cyber Protect 的計費模式" (第 8 頁)。

您可以使用計費模式或版本，設定提供給您租用戶的服務。您可以為每個客戶租用戶選擇一個計費模式或一個版本。因此，若要針對不同的服務功能套用不同的計費模式，您需要為一個客戶建立多個租用戶。例如，如果客戶希望對 Microsoft 365 信箱採用按 GB 計費模式，並對 Teams 採用按工作負載計費模式，則您必須為此客戶建立兩個不同的客戶租用戶。

若要限制某個產品項目中的服務使用量，您可以為該產品項目定義配額。請參閱 "彈性配額和硬性配額" (第 14 頁)。

啟用或停用產品項目

您可以啟用適用於指定版本或計費模式的所有產品項目，如建立租用戶中所述。

注意事項
停用某個服務的所有產品項目並不會自動停用該服務。

停用產品項目有一些限制，如下表中所列。

產品項目	停用	結果
備份儲存	可以在使用量等於零時停用。	雲端儲存空間將變得無法當做客戶租用戶內備份的目的地使用。
本機備份	可以在使用量等於零時停用。	本機儲存空間將變得無法當做客戶租用戶內備份的目的地使用。
資料來源 (包括 Microsoft 365 和 Google Workspace)*	可以在使用量等於零時停用。	遭停用資料來源 (包括 Microsoft 365 和 Google Workspace) 的保護將變得無法在客戶租用戶內使用，如下所示：
所有 Disaster Recovery 產品項目	可以在使用量大於零時停用。	請參閱「彈性配額和硬性配額」中的詳細資料。
所有 Notary 產品項目	可以在使用量等於零時停用。	Notary 服務將無法在客戶租用戶內使用。
所有File Sync & Share產品項目	無法個別啟用或停用產品項目。	File Sync & Share服務將無法在客戶租用戶內使用。
所有實體資料運送產品項目	可以在使用量等於零時停用。	實體資料運送服務將無法在客戶租用戶內使用。

對於無法在使用量大於零時停用的產品項目，您可以手動移除使用量，然後再停用對應的產品項目。

* 您可以在 Cyber Protect 主控台中新增的工作負載相關產品項目。如需詳細資訊，請參閱 "工作負載對產品項目的相依性" (第 21 頁)。下表摘述了當管理入口網站中沒有啟用產品項目、產品項目組合，或進階套件時，將無法使用的工作負載類型。

若您停用這些產品項目或進階套件	您將無法新增這些類型的工作負載
以下組合： • Microsoft 365 授權 • Microsoft 365 SharePoint online • Microsoft 365 Teams	Microsoft 365 商務版
以下組合： • Google Workspace • Google Workspace 共用磁碟機	Google Workspace
以下組合： • 伺服器 • 虛擬機器	• Microsoft SQL Server • Microsoft Exchange Server • Microsoft Active Directory
以下產品項目： • NAS	Synology
以下產品項目： • 行動	• iOS 裝置 • Android 裝置
以下進階套件： • 進階備份	Oracle 資料庫

彈性配額和硬性配額

配額可讓您限制租用戶使用服務的能力。若要設定配額，在 **[用戶端]** 索引標籤上選取用戶端、選取 [服務] 索引標籤，然後按一下 **[編輯]**。

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。當客戶受保護的工作站數目達到 20 時，客戶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，則您的客戶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 服務將會在該數目達到 25 時遭到停用。

達到硬性配額時，服務會受到限制 (無法保護其他工作負載或無法使用更多儲存空間)。超過硬性配額時，系統會發送一則通知到使用者的電子郵件地址。

可以定義配額的層級

配額可以在下表中列出的層級上設定。

租用戶/使用者	彈性配額 (僅配額)	硬性配額 (配額和超額)
合作夥伴	是	否
資料夾	是	否
客戶	是	是
單位	否	否
使用者	是	是

彈性配額可以在合作夥伴和資料夾層級上設定。在單位層級上無法設定任何配額。硬性配額可以在客戶和使用者層級上設定。

在使用者層級上設定的硬性配額總數不得超過相關客戶的硬性配額。

設定彈性配額和硬性配額

若要為您的用戶端設定配額

1. 在管理入口網站中，前往 **[用戶端]**。
2. 選擇您想設定配額的客戶端。
3. 選擇 **[保護]** 索引標籤，然後按一下 **[編輯]**。
4. 選擇您要設定的配額類型。例如，選擇**[工作站]** 或 **[伺服器]**。
5. 按一下右側的 **[無限制]** 連結，以開啟 **[配額編輯]** 視窗。
   - 若您想得知用戶端的配額且不希望限制用戶端使用服務的能力，請在 **[軟性配額]** 欄位中設定配額值。

     達到配額時用戶端將收到電子郵件通知，但仍將可以使用 Cyber Protection 服務。
   - 若您想限制用戶端使用服務的能力，請在下方 **[硬性配額]** 欄位中選擇 **硬性配額** 並設定配額值。

     達到配額時用戶端將收到電子郵件通知，且將停用 Cyber Protection 服務。
6. 在 **[配額編輯]** 視窗中，按一下 **[完成]**，然後按一下 **[儲存]**。

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到整個公司。公司系統管理員可以在管理入口網站中檢視配額和使用狀況。

  Microsoft 365 授權的授權取決於針對 Cyber Protection 選取的計費模式。

  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。

  在 **[按工作負載]** 計費模式下，**Microsoft 365 授權** 名額根據每位不重複使用者計數。不重複使用者是至少具有以下特性之一的使用者：

  - 受保護的信箱
  - 受保護的 OneDrive
  - 存取至少一個受保護的公司層級資源：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。

  注意事項

  沒有受保護個人信箱或 OneDrive，而且僅能存取共用資源 (共用信箱、SharePoint 網站和 Microsoft Teams) 的遭封鎖 Microsoft 365 使用者不收費。

  遭封鎖的使用者是沒有有效的登入且無法存取 Microsoft 365 服務的使用者。若要瞭解如何在 Microsoft 365 組織中封鎖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 18 頁)。

  下列 Microsoft 365 授權不收費，也不需要每基座授權：

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

如需有關按 GB 計費模式之授權選項的詳細資訊，請參閱 Cyber Protect Cloud：Microsoft 365 按 GB 授權。

如需有關按工作負載計費模式之授權選項的詳細資訊，請參閱 Cyber Protect Cloud：Microsoft 365 授權和定價變更。

- **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。

- **Microsoft 365 SharePoint Online**

  此配額是由服務提供者套用到整個公司。此配額會啟用或停用保護 SharePoint Online 網站的功能，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 備份佔用的儲存空間量。

- **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。

- **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。

只要使用者的信箱或 OneDrive 至少有套用一個保護計劃，Microsoft 365 授權就會被視為受到保護。只要使用者的信箱或 Google 雲端硬碟至少有套用一個保護計劃，Google Workspace 授權就會被視為受到保護。

當超過一些授權的超額時，公司系統管理員就無法將保護計劃套用至更多授權。

儲存空間的配額

- **本機備份**

  [本機備份]配額會限制使用雲端基礎架構建立的本機備份大小總計。無法針對此配額設定超額。

- **雲端資源**

  雲端資源配額會結合備份儲存空間的配額和災難復原的配額。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。

超過用於備份儲存空間的配額

不得超過備份儲存空間配額。保護代理程式憑證的技術配額等於租用戶的備份配額 + 超額。如果超出配額，則無法開始備份。如果在備份建立期間達到憑證中的配額，但未達到超額，備份將會成功完成。如果在備份建立期間達到超額，備份將會失敗。

範例：

使用者租用戶有 1 TB 的配額可用空間，而針對此使用者設定的超額為 5 TB。使用者開始備份。例如，如果所建立備份的大小為 3 TB，備份將會成功完成，因為未超過超額。如果所建立備份的大小超過 6 TB，當超過超額時，備份將會失敗。

備份配額轉換

一般而言，這是取得備份配額以及產品項目對應到資源類型運作的方式：系統會比較可用的產品項目和資源類型，然後取得相符產品項目的配額。

還有一個指派其他產品項目配額的功能，即使它與資源類型完全不相符，也是如此。這稱為**備份配額轉換**。如果沒有相符的產品項目，系統會嘗試尋找一個更適合資源類型的昂貴配額 (自動備份配額轉換)。如果找不到適當的配額，則您可以在 Cyber Protect 主控台中，將服務配額手動指派到資源類型。

範例

您想要備份虛擬機器 (工作站，代理程式型)。

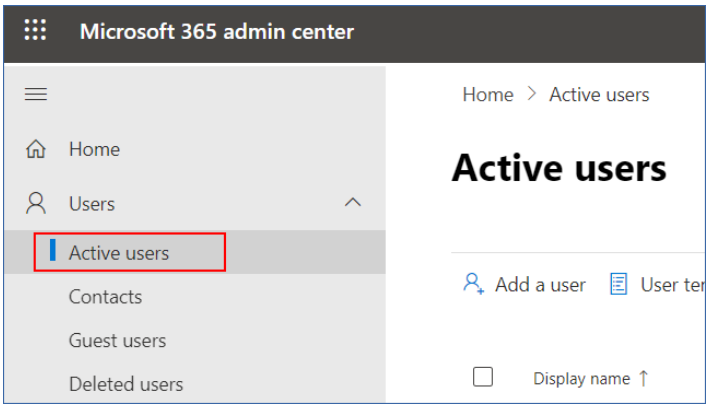
首先，系統將會檢查是否有已配置的**虛擬機器**配額。如果找不到，則系統會自動嘗試取得**工作站**配額。如果還是找不到，將不會自動取得其他配額。如果您有比**虛擬機器**配額還要昂貴，而且適用於虛擬機器的足夠配額，則您可以登入 Cyber Protect 主控台，並手動指派**伺服器**配額。

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。

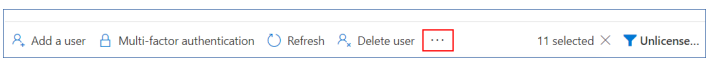
若要防止未獲授權的使用者登入

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]**。

災難復原配額

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

您可以為租用戶定義下列 File Sync & Share 配額：

- **使用者**
  這會定義 File Sync & Share 使用者數目的限制。

注意事項
只有 [使用者] 和 [使用者 + 系統管理員] 使用者角色才會計入此配額。
[系統管理員] 和 [來賓使用者] 角色會排除在此配額之外。

- **雲端儲存**
  這會定義針對租用戶配置的雲端儲存空間限制。

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。

您可以為租用戶定義下列實體資料運送配額：

- **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

您可以為租用戶定義下列 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。

變更電腦的服務配額

電腦的保護層級是由套用到該電腦的服務配額所定義。服務配額與適用於註冊電腦所在租用戶的產品項目有關。

保護計劃第一次套用到電腦時，便會自動指派服務配額。

系統會根據受保護電腦的類型、其作業系統、所需的保護層級，以及配額可用性，指派最適當的配額。如果貴組織無法使用最適當的配額，則會指派次佳配額。例如，如果最適當的配額為 **Web 託管伺服器**但無法使用，則會指派**伺服器**配額。

配額指派的範例：

- 執行 Windows Server 或 Linux Server 作業系統 (例如 Ubuntu Server) 的實體機器會獲指派**伺服器**配額。

- 執行 Windows 或 Linux Desktop 作業系統 (例如 Ubuntu Desktop) 的實體機器會獲指派**工作站**配額。
- 執行已啟用 Hyper-V 角色之 Windows 10 的實體機器會獲指派**工作站**配額。
- 在虛擬桌面基礎架構上執行且客體作業系統內部安裝其保護代理程式 (例如，Windows 用代理程式) 的桌上型電腦會獲指派**虛擬機器**配額。如果無法使用**虛擬機器**配額，此類型的電腦也可以使用**工作站**配額。
- 在虛擬桌面基礎架構上執行且在無代理程式模式 (例如，VMware 用代理程式或 Hyper-V 用代理程式) 下備份的桌上型電腦會獲指派**虛擬機器**配額。
- Hyper-V 或 vSphere 伺服器會獲指派**伺服器**配額。
- 具有 cPanel 或 Plesk 的伺服器會獲指派 **Web 託管伺服器**配額。根據網頁伺服器執行所在電腦的類型，如果無法使用 Web 託管伺服器配額，也可以使用**虛擬機器**或**伺服器**配額。
- 即使是針對工作站，應用程式感知備份也需要使用**伺服器**配額。

您之後可以手動變更原始指派。例如，若要將更進階的保護計劃套用到相同的電腦，您可能需要升級電腦的服務配額。如果目前指派的服務配額不支援此保護計劃所需的功能，保護計劃將會失敗。

或者，如果您在指派原始配額之後購買更多合適的配額，則可以變更服務配額。例如，**工作站**配額會被指派給虛擬機器。在您購買**虛擬機器**配額之後，可以手動將其指派給此機器，而不是指派原始的**工作站**配額。

您也可以釋出目前指派的服務配額，然後將此配額指派給其他機器。

您可以變更個別機器的服務配額，或一組機器的服務配額。

若要變更個別機器的服務配額

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 選擇所需的電腦，然後按一下 **[詳細資料]**。
3. 在 **[服務配額]** 區段中，按一下 **[變更]**。
4. 在 **[變更配額]** 視窗中，選擇所需的服務配額或 **[無配額]**，然後按一下 **[變更]**。

若要變更一組機器的服務配額

1. 在 Cyber Protect 主控台中，移至 **[裝置]**。
2. 選擇多部機器，然後按一下 **[指派配額]**。
3. 在 **[變更配額]** 視窗中，選擇所需的服務配額或 **[無配額]**，然後按一下 **[變更]**。

工作負載對產品項目的相依性

根據啟用的產品項目，將可以使用 主控台中的**新增裝置**窗格內不同的工作負載類型。在下表中，您可以看到不同產品項目中可使用的工作負載類型。

工作負載類型 (代理程式安裝程式)	已啟用的產品項目							
	伺服器	工作站	虛擬機器	Microsoft 365 授權	Google Workspace 授權	行動裝置	Web 託管伺服器	網站
工作站 – Windows 用代理程式		+	+					+
工作站 – macOS 用代理程式		+	+					+
伺服器 – Windows 用代理程式	+		+				+	+
伺服器 – Linux 用代理程式	+		+				+	+
Hyper-V 用代理程式			+					
VMware 用代理程式			+					
Virtuozzo 用代理程式			+					
SQL 用代理程式	+		+					
Exchange 用代理程式	+		+					
Active Directory 用代理程式	+		+					
Microsoft 365 商務版工作負載				+				
Google Workspace 工作負載					+			
Windows 用完整安裝程式	+	+	+				+	+
行動裝置 (iOS 和 Android)						+		

使用管理入口網站

下列步驟會引導您瞭解管理入口網站的基本用法。

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。

啟用系統管理員帳戶

簽署合夥公司協議後，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 23 頁)。

密碼需求

使用者帳戶的密碼必須至少包含 9 個字元。還會檢查密碼的複雜性，並將其歸入下列其中一個類別：

- 弱式
- 中
- 強式

您不能儲存弱式密碼，即使它可能包含 9 個以上字元。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之租用戶的名稱重複的密碼一律被視為弱式密碼。大多數常用密碼也被視為弱式密碼。

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

1. 請移至服務登入頁面。
2. 登入頁面網址包含在您收到的啟用電子郵件訊息中。
3. 輸入登入，然後按一下 **[下一步]**。

4. 輸入密碼，然後按一下 **[下一步]**。

注意事項
為防止 Cyber Protect Cloud 遭到暴力密碼破解攻擊，入口網站將會在嘗試登入失敗 10 次將您鎖定。鎖定期限為 5 分鐘。登入失敗的嘗試次數會在 15 分鐘後重設。

5. 使用右側功能表瀏覽管理入口網站。

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。

有些服務包含從服務主控台切換至管理入口網站的功能。

在公司設定檔精靈中設定聯絡人

您可以為您的公司設定聯絡人資訊。我們會將平台新功能和其他重要變更的更新傳送給您提供的聯絡人。

當您第一次登入管理入口網站時，公司設定檔精靈會引導您完成要提供的公司和聯絡人的基本資訊。

您可以從 Cyber Protect 平台中存在的使用者建立聯絡人，或新增無法存取服務之人員的聯絡人資訊。

若要使用公司設定檔精靈設定公司聯絡人

1. 在 **[公司資訊]** 中，指定公司的下列詳細資料：
   - **正式 (法定) 公司名稱**
   - **公司法定地址 (總部地址)**
     - **國家/地區**
     - **郵遞區號**
2. 按 **[下一步]**。
3. 在 **[公司聯絡人]** 中，設定下列用途的聯絡人：
   - **帳單聯絡人** — 將取得有關平台中使用者報告重要變更之更新的聯絡人。
   - **業務聯絡人** — 將取得有關平台中業務相關重要變更之更新的聯絡人。
   - **技術聯絡人** — 將取得有關平台中重要技術變更之更新的聯絡人。

   您可以將一位聯絡人用於多種用途。

   選擇一個選項以建立聯絡人。
   - **從現有的使用者建立**。從下拉式清單中選擇使用者。
   - **建立新的聯絡人**。提供下列聯絡人資訊：
     - **名字** — 聯絡人的名字。此為必填欄位。
     - **姓氏** — 聯絡人的姓氏。此為必填欄位。
     - **公司電子郵件** — 聯絡人的電子郵件地址。此為必填欄位。
     - **公司電話** — 此為選填欄位。
     - **職稱** — 此為選填欄位。

4. 如果您打算將帳單聯絡人也當作業務聯絡人或技術聯絡人使用，請在 **[帳單聯絡人]** 區段中選擇對應的旗標：
   - **請為業務聯絡人使用相同的聯絡人**
   - **請為技術聯絡人使用相同的聯絡人**
5. 按一下**[完成]**。

   結果會建立聯絡人。您可以在管理主控台的 **[公司管理] > [公司設定檔]** 區段中編輯資訊，以及設定其他聯絡人，如設定公司聯絡人中所述。

從管理入口網站存取 Cyber Protect 主控台

1. 在管理入口網站，前往 **[監控] > [使用情形]**。
2. 在 **[Cyber Protect]**，選取 **[保護]**，然後按一下 **[管理服務]**。

   或者，在 **[用戶端]**，選取客戶，然後按一下 **[管理服務]**。

最後系統會將您重新導向至 Cyber Protect 主控台。

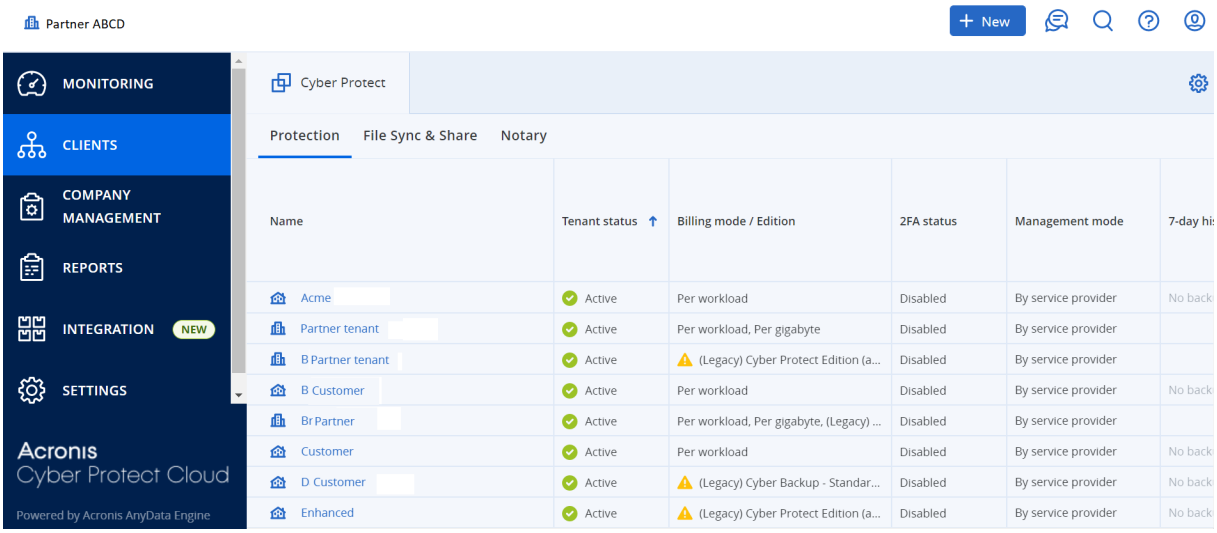
重要事項

如果客戶位於**自助服務**管理模式下，則您無法為其管理服務。只有客戶系統管理員可以將客戶模式變更為 **[由服務提供者管理]**，然後就可以管理服務。

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租用戶內操作。此租用戶的名稱會在左上角顯示。

預設會選擇您可使用的最高階層層級。按一下清單中的租用戶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租用戶，也只影響該租用戶。例如：

- **[用戶端]** 索引標籤只顯示您正在操作的租用戶的直接子租用戶。
- **[公司管理]** 索引標籤會顯示公司設定檔以及您正在操作的租用戶內存在的使用者帳戶。

- 藉著使用 **[新增]** 按鈕，您只能在正在操作的租用戶內建立租用戶或新使用者帳戶。請注意，此功能表中可能還有其他選項，端視您訂閱的服務而定。

管理入口網站中的新功能

發佈 Cyber Protect Cloud 的新功能時，您會在登入管理入口網站時看到一個快顯視窗，其中包含這些功能的簡短描述。

您也可以按一下管理入口網站主視窗左下角的 **[新增功能]** 連結來檢視新功能的描述。

限制 Web 介面的存取權

系統管理員可以指定 IP 位址清單，提供 Web 介面存取權給所列位址的租用戶成員登入。

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。它不會套用到子租用戶的成員。

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租用戶。
3. 按一下 **[設定]** > **[安全]**。
4. 啟用 **[登入控制]** 開關。
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]**。

注意事項
對於使用 Cyber Infrastructure (混合模型) 的服務提供者：

如果在管理入口網站中的 **[設定]** > **[安全性]** 底下啟用 **[登入控制]** 開關，請將 Cyber Infrastructure 節點的一個或多個外部公共 IP 位址新增到 **[允許的 IP 位址]** 清單。

存取服務

[概觀] 索引標籤

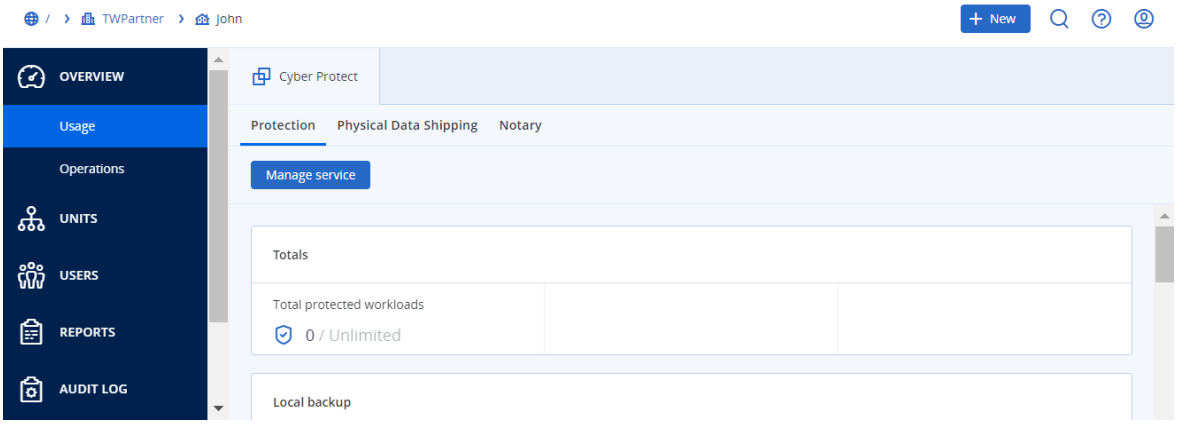
[概觀] > **[使用狀況]** 區段提供服務使用狀況的概觀，並可讓您存取正在操作的租用戶內的服務。

使用 [概觀] 索引標籤管理租用戶的服務

1. 瀏覽到您要管理服務的租用戶，然後按一下 **[概觀]** > **[使用狀況]**。

   請注意，部分服務可在合作夥伴租用戶和客戶租用戶層級管理，但是其他服務只能在客戶租用戶層級管理。
2. 按一下您要管理之服務的名稱，然後按一下 **[管理服務]** 或 **[設定服務]**。

   如需使用服務的資訊，請參閱服務主控台提供的使用指南。

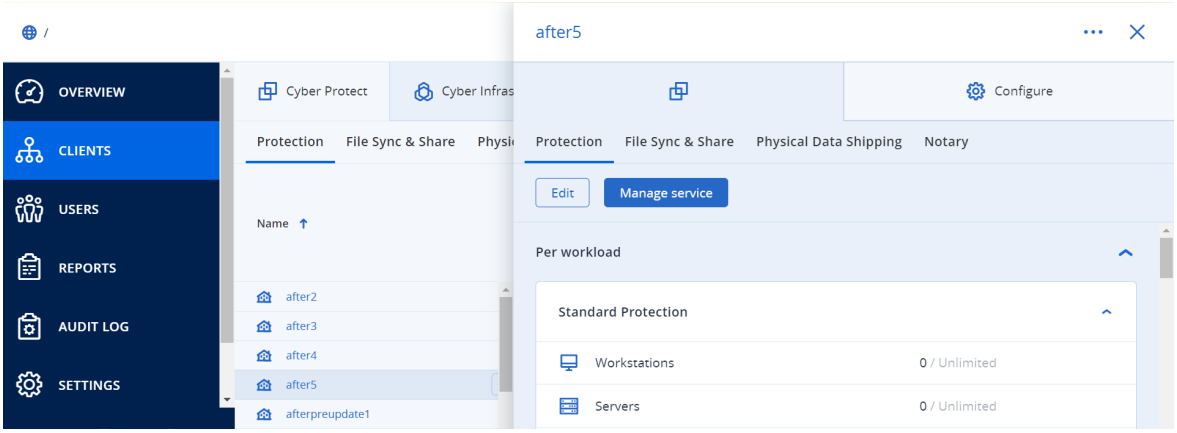


[用戶端]索引標籤

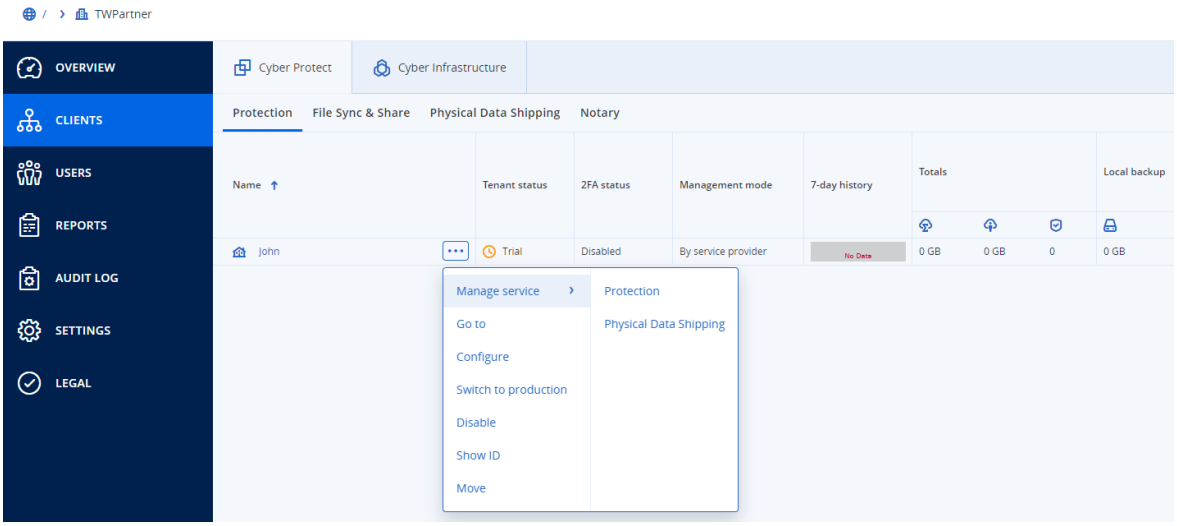
[用戶端] 索引標籤會顯示您正在操作的租用戶內的子租用戶，並可讓您存取那些子租用戶內的服務。

使用 [用戶端] 索引標籤管理租用戶的服務

1. 執行下列其中一項操作：
   - 按一下 **[用戶端]**、選取您要管理其服務的租用戶、按一下您要管理之服務的名稱或圖示，然後按一下 **[管理服務]** 或 **[設定服務]**。



   - 按一下 **[用戶端]**、按一下您要管理其服務之租用戶名稱旁邊的省略符號圖示、按一下 **[管理服務]**，然後選取您要管理的服務。



請注意，部分服務可在合作夥伴租用戶和客戶租用戶層級管理，但是其他服務只能在客戶租用戶層級管理。

如需使用服務的資訊，請參閱服務主控台提供的使用指南。

7 天的歷程記錄列

在 **[用戶端]** 畫面上，**[7 天的歷程記錄]** 列會針對過去七天的客戶租用戶，顯示工作負載備份的狀態。此列分為 168 條彩色線條。每條線都代表一小時的間隔，並顯示對應一小時間隔內最差的備份狀態。

下表提供每個線條顏色所代表之意義的相關資訊。

顏色	描述
紅色	在一小時期間內至少其中一個備份失敗
橙色	在一小時期間內至少其中一個備份完成並出現警告，但沒有任何備份錯誤
綠色	在一小時期間內至少有一個成功備份，沒有任何備份錯誤和警告
灰色	在一小時期間內沒有任何完成的備份

在收集到對應的統計資料之前，**[7 天的歷程記錄]** 列會顯示「無備份」。

若是合作夥伴租用戶，**[7 天的歷程記錄]** 列則是空白的，因為不支援彙總的統計資料。

使用者帳戶與租用戶

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。

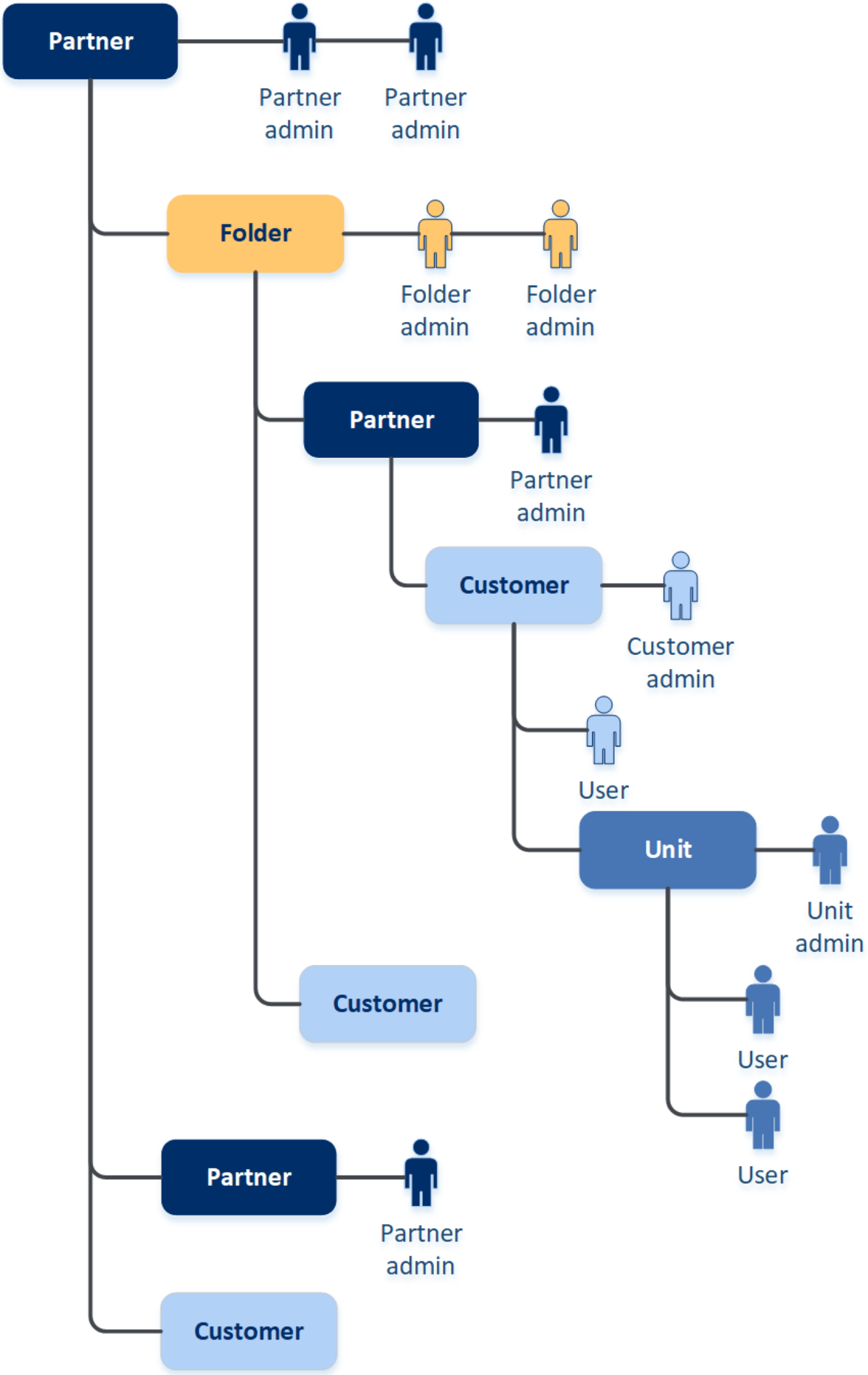
每個帳戶均屬於一個租用戶。租用戶是專用於合作夥伴或客戶的管理入口網站資源 (例如使用者帳戶和子租用戶) 和服務產品 (啟用的服務和其中的產品項目) 的一部分。租用戶階層應該符合服務使用者和提供者之間的用戶端/供應商關係。

- **[合作夥伴]** 租用戶類型一般對應於轉售服務的服務供應商。
- **[資料夾]** 租用戶類型一般是合作夥伴系統管理員所使用的補充租用戶，用來將合作夥伴和客戶分組，以便設定個別產品和/或不同商標。
- **[客戶]** 租用戶類型一般對應到使用服務的組織。
- **[單位]** 租用戶類型一般對應到組織內的單位或部門。

系統管理員可以建立和管理階層中在他們以上或以下層級的租用戶、系統管理員帳戶，和使用者帳戶。

合作夥伴類型父租用戶的系統管理員可以充當**客戶**或**合作夥伴**類型租用戶中最低層級的系統管理員，其管理模式為 **[由服務提供者管理]**。因此，合作夥伴層級系統管理員可以管理使用者帳戶和服務，或存取子租用戶中的備份和其他資源。但是，較低層級的系統管理員可以限制更高層級的系統管理員存取其租用戶。

下圖說明合作夥伴、資料夾、客戶和單位租用戶的層級範例。


Partner
Partner admin
Partner admin
Folder
Folder admin
Folder admin
Partner
Partner admin
Customer
Customer admin
User
Unit
Unit admin
User
User
Customer
Partner
Partner admin
Customer

下表摘述管理員和使用者可以執行的選項。

作業	使用者	客戶和單位管理員	合作夥伴和資料夾管理員
建立租用戶	否	是	是
建立帳戶	否	是	是
下載及安裝軟體	是	是	否*
管理服務	是	是	是
建立關於服務使用的報告	否	是	是
設定商標	否	否	是

注意事項
您可以從任何類型的租用戶建立使用者，而且只要是按照從最高權限到最低權限的順序建立使用者，就可以擁有共用的電子郵件地址。例如，合作夥伴租用戶可以建立資料夾、客戶和單位租用戶，而客戶租用戶無法建立資料夾租用戶。

管理租用戶

Cyber Protect 提供下列租用戶：

- **[合作夥伴]** 租用戶一般是針對每個簽署合作協議的合作夥伴建立的 。
- **[資料夾]** 租用戶一般是為了將合作夥伴和客戶分組而建立的，以便設定個別產品和/或不同商標。
- **[客戶]** 租用戶一般是針對註冊備份服務的每個組織建立的。
- **[單位]** 租用戶是在客戶租用戶內建立的，可將服務擴展至新的組織單位。

建立並設定租用戶的步驟視您所建立的租用戶而有所不同，但一般而言，程序包含下列步驟：

1. 建立租用戶。
2. 選擇租用戶的服務。
3. 設定租用戶的產品項目。

建立租用戶

1. 登入管理入口網站。
2. 瀏覽到您要建立租用戶的租用戶。
3. 按一下右上角的 **[新增]**，然後視您要建立的租用戶類型而定，按一下下列其中一個項目：
   - **[合作夥伴]** 租用戶一般是針對每個簽署合作協議的合作夥伴建立的 。
   - **[資料夾]** 租用戶一般是為了將合作夥伴和客戶分組而建立的，以便設定個別產品和/或不同商標。
   - **[客戶]** 租用戶一般是針對註冊備份服務的每個組織建立的。
   - **[單位]** 租用戶是在客戶租用戶內建立的，可將服務擴展至新的組織單位。

可用類型取決於父租用戶類型。

4. 在 **[名稱]** 中，指定新租用戶的名稱。
5. [僅適用於建立合作夥伴租用戶時] 輸入 **[正式 (法定) 公司名稱]** (必填) 和 **[VAT 編號/統一編號/公司註冊號碼]** (選填)。
6. [僅適用於建立客戶租用戶] 在 **[模式]** 中，選擇要讓租用戶以試用模式或實際運作模式使用服務。每月服務使用量報告包含兩種模式下租用戶的使用量資料。

   重要事項

   試用模式提供 30 天的評估期，在這段期間內將對產品提供完整存取權。請注意，一旦客戶切換到 [實際運作] 模式，其使用量將自動計入最近的計費週期中。

   您可以隨時切換到 [實際運作] 模式。但是無法從 [實際運作] 模式還原到 [試用] 模式。

   如果您決定取消客戶的試用，則您也必須刪除對應的客戶租用戶。否則，30 天試用期滿後，客戶將自動切換到 [實際運作] 模式，而且對應的使用量將計入最近的計費週期。如需詳細資訊，請參閱本知識庫文章。

7. 在 **[管理模式]** 中，選擇下列其中一個模式以管理租用戶的存取權：
   - **自助服務** – 此模式會針對父租用戶的系統管理員限制此租用戶的存取權：他們僅能修改租用戶屬性，但無法存取或管理其內部的任何項目 (例如租用戶、使用者、服務、備份和其他資源)。
   - **由服務提供者管理** – 此模式會針對父租用戶的系統管理員授予租用戶的完整存取權：修改屬性；管理租用戶、使用者、服務；存取備份和其他資源。預設選擇此模組。

   如果是 **[自助服務]**，則只有您建立之租用戶的系統管理員可以變更 [管理模式]。因此，所建立之租用戶的系統管理員可以前往 **[設定]** > **[安全性]**，然後設定 **[支援存取]** 開關。

   您可以在 **[用戶端]** 索引標籤中，檢查您子租用戶的所選管理模式。
8. 在 **[安全性]** 中，啟用或停用租用戶的雙重驗證機制。

   若已啟用，此租用戶的所有使用者必須為其帳戶設定雙重驗證機制，才能更安全地進行存取。使用者必須在其第二要素裝置上安裝驗證應用程式，並使用產生的一次性 TOTP 代碼以及傳統的登入和密碼，才能登入主控台。如需詳細資訊，請參閱「設定雙重驗證機制」。若要檢視您客戶的雙重驗證機制狀態，前往 **[用戶端]**。
9. [僅適用於在合規模式下建立客戶租用戶時] 在 **[安全性]** 中，選擇 **[合規模式]** 核取方塊。

   使用此模式時，僅允許加密備份。您必須在受保護的裝置上設定加密密碼，如果沒有加密密碼，建立備份將會失敗。需要將加密密碼提供給雲端服務的所有作業都無法使用。如需詳細資訊，請參閱 "合規模式" (第 33 頁)。

   重要事項

   您無法在建立租用戶後停用 [合規] 模式。

10. 在 **[建立系統管理員]** 中，設定系統管理員帳戶。

    注意事項

    當 **[管理模式]** 設為 **[自助服務]** 時，客戶租用戶和合作夥伴租用戶必須建立系統管理員。

a. 輸入系統管理員帳戶的電子郵件。此電子郵件也當作登入使用。
b. 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，然後輸入系統管理員帳戶的登入名稱和電子郵件。
   其餘是選填欄位，但請提供更多通訊管道，以防我們需要聯絡系統管理員。
c. 選擇語言。
   如果您沒有選擇語言，系統預設會使用英文。
d. 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。

11. 在 **[語言]** 中，變更此租用戶內所使用的通知、報告及軟體的預設語言。
12. 執行下列其中一項操作：
    - 若要完成租用戶建立，請按一下 **[儲存並關閉]**。在此情況下，將會啟用該租用戶的所有服務。保護 服務的計費模式將設定為按工作負載。
    - 若要選擇租用戶的服務，按一下 **[下一步]**。請參閱 "選擇租用戶的服務" (第 34 頁)。

合規模式

合規模式是針對具有更高安全性需求的用戶端而設計。此模式要求強制加密所有備份，而且僅允許在本機設定加密密碼。

使用合規模式時，在客戶租用戶及其單位中建立的所有備份都會自動使用 AES 演算法和 256 位元金鑰加密。使用者僅能在受保護的裝置上設定加密密碼，而且無法在保護計劃中設定加密密碼。

重要事項
合作夥伴系統管理員僅能在建立新的客戶租用戶時啟用合規模式，而且之後無法停用此模式。您無法針對現有的租用戶啟用合規模式。

限制

- 合規模式僅與版本為 15.0.26390 或更新版本的代理程式相容。
- 合規模式不適用於執行 Red Hat Enterprise Linux 4.x 或 5.x 及其衍生產品的裝置。
- 雲端服務無法存取加密密碼。基於此限制，部分功能在合規模式下無法用於租用戶。

不支援的功能

下列功能在合規模式下無法用於租用戶：

- 透過 Cyber Protect 主控台復原
- 透過 Cyber Protect 主控台瀏覽檔案層級的備份
- 雲端對雲端備份
- 網站備份
- 應用程式備份

- 備份行動裝置
- 備份的反惡意程式碼掃描
- 安全復原
- 自動建立公司白名單
- 資料保護圖
- 災難復原
- 與無法使用之功能相關的報告和儀表板

選擇租用戶的服務

當您建立新的租用戶時，預設會啟用所有服務。您可以選擇將提供給租用戶及其子租用戶中使用者的服務。

您也可以使用一個動作，為多個現有的租用戶選擇並啟用服務。如需詳細資訊，請參閱 "為多個現有的租用戶啟用服務" (第 35 頁)。

此程序不適用於單位租用戶。

若要選擇租用戶的服務

1. 在建立/編輯租用戶對話方塊的 **[選擇服務]** 區段中，選擇一個計費模式或一個版本。
   - 選擇 **[按工作負載]** 或 **[按 GB]** 計費模式，然後清除您要為租用戶停用的服務的核取方塊。兩種計費模式的服務集都相同。

     若是進階版災難復原，如果您以您的帳戶註冊自己的災難復原位置，可以從下拉式清單中選擇災難復原的位置。
   - 若要使用舊版，請選擇 **[舊版]** 選項按鈕，然後從下拉式清單中選擇一個版本。

   租用戶及其子租用戶內的使用者將無法看到停用的服務。
2. 執行下列其中一項操作：
   - 若要完成租用戶建立，請按一下 **[儲存並關閉]**。在此情況下，將會針對擁有無限配額的租用戶，啟用所選服務的所有產品項目。
   - 若要設定租用戶的產品項目，按一下 **[下一步]**。請參閱 "設定租用戶的產品項目" (第 34 頁)。

設定租用戶的產品項目

當您建立新的租用戶時，會啟用所選服務的所有產品項目。您可以選擇將提供給租用戶及其子租用戶中使用者的產品項目，並為其設定配額。

此程序不適用於單位租用戶。

若要設定租用戶的產品項目

1. 在建立/編輯租用戶對話方塊的每個服務索引標籤底下的**[設定服務]** 區段上，清除您要停用的產品項目的核取方塊。

   租用戶及其子租用戶內的使用者將無法使用與已停用的產品項目相對應的功能。
2. 您可以針對部分服務選擇提供給新租用戶的儲存空間。儲存空間依位置分組。您可以從租用戶可用的位置和儲存空間清單中選擇。

- 建立合作夥伴/資料夾租用戶時，您可以為每個服務選擇多個位置和儲存空間。
- 建立客戶租用戶時，必須選擇一個位置，然後在此位置內，每個服務選擇一個儲存空間。您稍後可以變更指派給客戶的儲存空間，但是只能在其使用量為 0 時，亦即，在客戶開始使用儲存空間之前，或在客戶從此儲存空間移除所有備份之後。關於儲存空間使用狀況的資訊並不會即時更新。資訊更新請等待最多 24 小時。

如需有關儲存空間的詳細資訊，請參閱「管理位置和儲存空間」。

3. 若要指定某個項目的配額，按一下產品項目旁邊的 **[無限制]** 連結。
這些配額為「軟性限制」。如果超過其中任一數值，則會傳送電子郵件通知至租用戶系統管理員以及父租用戶的系統管理員。不會套用使用服務的限制。若是合作夥伴租用戶，由於建立合作夥伴租用戶時無法設定超額，因此預計產品項目使用量可能會超過配額。
4. [僅適用於建立客戶租用戶的情況] 指定配額超額。
超額是指定允許客戶租用戶超過配額多少數值。當超過超額時，會套用使用相對應服務的限制。
5. 按一下 **[儲存並關閉]**。

新建立的租用戶會出現在管理主控台的 **[用戶端]** 索引標籤上。

如果您要編輯租用戶設定或變更系統管理員，請在 **[用戶端]** 索引標籤上選擇租用戶，然後按一下您要編輯的區段內的鉛筆圖示。

為多個現有的租用戶啟用服務

您可以為多個租用戶 (一個工作階段最多 100 個租用戶) 大量啟用服務、版本、套件和產品項目。

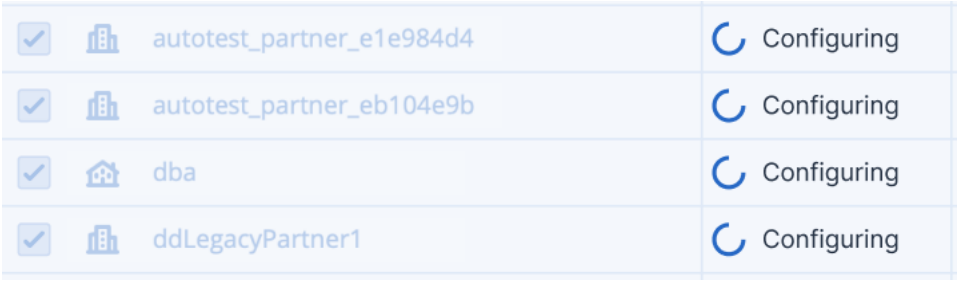
此程序適用於子根目錄、合作夥伴、資料夾和客戶租用戶。您可以同時選擇以上任何不同類型的租用戶。

若要為多個租用戶啟用服務

1. 在管理入口網站中，前往 **[用戶端]**。
2. 按一下右上角的 **[設定服務]**。
3. 選擇租用戶名稱旁的核取方塊，以便選擇您要為其啟用服務的每個租用戶，然後按一下 **[下一步]**。
4. 在 **[選擇服務]** 區段中，選擇您要套用到所有所選租用戶的相關服務，然後按一下 **[下一步]**。

> **注意事項**
> 您無法在此畫面中停用先前啟用的服務。在您開始此程序之前選擇的所有服務、版本和產品項目都將維持啟用狀態。

5. 在 **[設定服務]** 區段中，選擇您要為所選租用戶啟用的服務功能和產品項目，然後按一下 **[下一步]**。
6. 在 **[摘要]** 區段中，檢閱將套用到所選租用戶的變更。
您可以按一下 **[全部展開]** 以查看將套用的所有租用戶的所選服務和產品項目。或者，您可以展開每個租用戶，以檢視該租用戶專屬的所選服務和產品項目。
7. 按一下 **[套用變更]**。為每個租用戶設定服務時，會停用租用戶，而且 **[租用戶狀態]** 欄會指出目前正在設定服務和產品項目，如下所示。



8. 當服務和產品項目的設定成功套用到所選租用戶時，就會顯示一則確認訊息。
   如果基於特定原因而無法將服務和產品項目套用到租用戶，**[租用戶狀態]** 欄會顯示 **[未套用]**。按一下 **[再試一次]** 以檢閱所選租用戶的設定。

啟用維護通知

身為合作夥伴使用者，您可以允許您的子租用戶 (合作夥伴和客戶) 直接從 Cyber Protect 資料中心收到維護通知電子郵件，並收到管理入口網站內部的產品內維護通知。這將有助於減少維護相關請求支援的次數。

注意事項
維護通知電子郵件由資料中心署名。這些通知不支援自訂署名。

若要為子租用戶或客戶啟用維護通知

1. 以合作夥伴使用者的身分登入管理入口網站，按一下 **[客戶]**，然後針對您要啟用維護通知的合作夥伴或客戶租用戶，按一下其名稱。
2. 按一下 **[設定]**。
3. 在 **[一般設定]** 索引標籤上，找出 **[維護通知]** 選項並加以啟用。
   如果您沒有看到 **[維護通知]** 選項，請與您的服務提供者聯絡。

注意事項
系統會啟用 [維護通知]，但在所選租用戶為其使用者啟用通知，或進一步將此選項傳播給子合作夥伴或客戶，以為其使用者啟用通知之前，不會傳送這些通知。

若要為使用者啟用維護通知

1. 以合作夥伴使用者或公司系統管理員的身分，登入管理入口網站。
   身為合作夥伴，您可以針對您所管理的所有租用戶，存取其使用者。
2. 導覽至 **[公司管理]** > **[使用者]**，然後按一下您要為其啟用維護通知之使用者的名稱。
3. 在 **[服務]** 索引標籤的 **[設定]** 區段中，按一下鉛筆圖示可編輯選項。
4. 選擇 **[維護通知]** 核取方塊，然後按一下 **[完成]**。

所選使用者將收到資料中心即將進行維護活動的電子郵件通知。

設定自我管理的客戶設定檔

身為合作夥伴，您可以為您管理的租用戶，設定自我管理的客戶設定檔。此選項可讓您控制租用戶設定檔和聯絡人資訊對每個客戶的能見度。

若要設定自我管理的客戶設定檔

1. 在管理入口網站中，前往 **[用戶端]**。
2. 選擇您想要為其設定自我管理的客戶設定檔的客戶。
3. 選擇 **[設定]** 索引標籤，然後選擇 **[一般設定]** 索引標籤。
4. 啟用或停用 **[啟用自我管理的客戶設定檔]** 開關。

啟用自我管理的客戶設定檔時，此客戶將會在導覽功能表中看到 **[公司設定檔]** 區段，並在 [建立使用者精靈] (**[公司電話]**、**[公司聯絡人]** 和 **[職稱]**) 中看到聯絡人相關欄位。

停用自我管理的客戶設定檔時，將會隱藏導覽功能表中的 **[公司設定檔]** 區段，以及 [建立使用者精靈] 中的聯絡人相關欄位。

設定公司聯絡人

身為合作夥伴，您可以為您的公司和您管理的租用戶，設定聯絡人資訊。我們將向此清單的聯絡人針對平台新功能和其他重要變更傳送更新。

您可以新增多個聯絡人，並指派公司聯絡人，端視使用者角色而定。您可以從 Cyber Protect 平台中存在的使用者建立聯絡人，或新增無法存取服務之人員的聯絡人資訊。

若要設定公司的聯絡人

1. 在管理主控台中，前往 **[公司管理]** > **[公司設定檔]**。
2. 在 **[聯絡人]** 區段中，按一下 **+**。
3. 選擇一個選項以建立聯絡人。
   - **從現有的使用者建立**
     - 從下拉式清單中選擇使用者。
     - 選擇一個公司聯絡人。
       - **[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。

       如果您從公司設定檔中的聯絡人清單刪除與某個使用者相關聯的聯絡人，該使用者將不會遭到刪除。系統將會取消指派該使用者的所有公司聯絡人，使其不再出現在 **[使用者]** 清單的 **[公司聯絡人]** 欄中。

       如果您要變更與該使用者相關聯之聯絡人的電子郵件地址，系統將會要求驗證新定義的地址。此時將會傳送一封電子郵件到這個地址，而使用者需要確認變更。
   - **建立新的聯絡人**
     - 提供聯絡資訊。
       - **[名字]**—聯絡人名字。此欄位為必填欄位。
       - **[姓氏]**—聯絡人姓氏。此欄位為必填欄位。
       - **[公司電子郵件]**—聯絡人電子郵件地址。此欄位為必填欄位。
       - **[公司電話]**—此欄位為選填。
       - **[職稱]**—此欄位為選填。

- 選擇 **[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。

4. 按一下 **[新增]**。

若要設定租用戶的聯絡人

注意事項

如果您修改子租用戶的聯絡人資訊，租用戶也將看得到您的變更。

---

1. 在管理入口網站中，前往 **[用戶端]**。
2. 按一下租用戶，然後按一下 **[設定]**。
3. 在 **[聯絡人]** 區段中，按一下 **+**。
4. 選擇一個選項以建立聯絡人。
   - **從現有的使用者建立**
     - 從下拉式清單中選擇使用者。
     - 選擇一個公司聯絡人。
       - **[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。

       如果您從公司設定檔中的聯絡人清單刪除與某個使用者相關聯的聯絡人，該使用者將不會遭到刪除。系統將會取消指派該使用者的所有公司聯絡人，使其不再出現在 **[使用者]** 清單的 **[公司聯絡人]** 欄中。

       如果您要變更與該使用者相關聯之聯絡人的電子郵件地址，系統將會要求驗證新定義的地址。此時將會傳送一封電子郵件到這個地址，而使用者需要確認變更。
   - **建立新的聯絡人**
     - 提供聯絡資訊。
       - **[名字]**—聯絡人名字。此欄位為必填欄位。
       - **[姓氏]**—聯絡人姓氏。此欄位為必填欄位。
       - **[公司電子郵件]**—聯絡人電子郵件地址。此欄位為必填欄位。
       - **[公司電話]**—此欄位為選填。
       - **[職稱]**—此欄位為選填。
     - 選擇 **[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。
5. 按一下 **[新增]**。

重新整理租用戶的使用狀況資料

使用狀況資料預設以固定的時間間隔重新整理。您可以手動重新整理租用戶的使用狀況資料。

1. 在管理主控台中，前往 **[用戶端]**。
2. 按一下租用戶，然後按一下租用戶行中的省略符號。
3. 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。

4. 重新載入頁面以查看更新的資料。

停用與啟用租用戶

您可能需要暫時停用租用戶。例如，如果您的租戶有使用服務的欠款。

若要停用租用戶

1. 在管理入口網站中，前往 **[用戶端]**。
2. 選取您要停用的租用戶，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：

- 租用戶及其所有子租用戶將會遭到停用，且其服務將會遭到停止。
- 租用戶及其子租用戶將會繼續計費，因為其資料將會保留並存放在 Cyber Protect Cloud 中。
- 租用戶及其子租用戶內的所有 API 用戶端都將遭到停用，而且使用這些用戶端的所有整合都將停止運作。

若要啟用租用戶，請在用戶端清單中選取該租用戶，然後按一下省略符號圖示 > **[啟用]**。

將租用戶移至另一個租用戶

管理入口網站可讓您將租用戶從一個父租用戶移至另一個父租用戶。如果您要將客戶從一個合作夥伴移轉到另一個合作夥伴，或者如果您建立了一個資料夾租用戶來組織您的用戶端，並且要將其中一些移到新建立的資料夾租用戶時，此功能就派上用場。

可以移動的租用戶類型

租用戶類型	可以移動	目標租用戶
合作夥伴	是	合作夥伴或資料夾
資料夾	是	合作夥伴或資料夾

租用戶類型	可以移動	目標租用戶
客戶	是	合作夥伴或資料夾
單位	否	無

需求與限制

- 只有當目標父租用戶具有相同或更大組的服務，而且產品項目與原始父租用戶相同時，才能移動租用戶。
- 移動客戶租用戶時，原始父租用戶中指派給該客戶租用戶的所有儲存空間都必須存在於目標父租用戶中。這是必要的，因為客戶服務相關資料無法從一個儲存空間移至另一個儲存空間。
- 在服務提供者管理的客戶租用戶中，可能有適用於服務提供者層級中客戶工作負載的計劃 (例如，指令碼計劃)。

  移動此種客戶租用戶時，將會從客戶工作負載中撤銷服務提供者的計劃，而且與這些計劃相關聯的所有服務都將針對此客戶停止運作。
- 您可以移動合作夥伴帳戶階層內的租用戶。您也可以將部分客戶租用戶移動到合作夥伴帳戶階層外的目標租用戶。若要瞭解是否可能進行該作業，請聯絡您的客戶經理。
- 僅限系統管理員 (例如，管理入口網站的系統管理員或公司系統管理員) 可以將租用戶移動到不同的父租用戶。

如何移動租用戶

1. 登入管理入口網站。
2. 尋找並複製您要將用戶端移過去的目標合作夥伴或資料夾租用戶的 **[內部 ID]**。執行下列作業：
   a. 在 **[用戶端]** 索引標籤上，選取您要將用戶端移過去的目標租用戶。
   b. 在租用戶屬性面板上，按一下垂直省略符號圖示，然後按一下**[顯示 ID]**。
   c. 複製 **[內部 ID]** 欄位中顯示的文字字串，然後按一下 **[取消]**。
3. 選擇您要移動的租用戶，然後將其移動到目標合作夥伴/資料夾。執行下列作業：
   a. 在 **[用戶端]** 索引標籤上，選取您要移動的租用戶。
   b. 在租用戶屬性面板上，按一下垂直省略符號圖示，然後按一下**[移動]**。
   c. 貼上目標租用戶的內部識別碼，然後按一下 **[移動]**。

此作業會立即開始，而且最多可能需要 10 分鐘。

如果您要移動的租用戶有子租用戶 (例如，該租用戶是內含客戶租用戶的合作夥伴或資料夾租用戶)，則整個租用戶子樹狀結構都將移動到目標租用戶。

將合作夥伴租用戶轉換為資料夾租用戶及反向操作

管理入口網站可讓您將合作夥伴租用戶轉換為資料夾租用戶。

如果您過去基於分組目的而使用合作夥伴租用戶，而現在想要適當組織您的租用戶基礎架構，此功能很實用。如果您希望 [作業儀表板] 包含有關租用戶的彙總資訊，這也很有用。

您也可以將資料夾租用戶轉換為合作夥伴租用戶。

注意事項
此轉換是很安全的作業，而且不會影響租用戶內的使用者和任何與服務有關的資料。

轉換租用戶

1. 登入管理入口網站。
2. 在 **[用戶端]** 索引標籤，選取您要轉換的租用戶。
3. 執行下列其中一項操作：
   - 按一下租用戶名稱旁的省略符號圖示。
   - 選取租用戶，然後按一下租用戶屬性面板上的省略符號圖示。
4. 按一下 **[轉換為資料夾]** 或 **[轉換為合作夥伴]**。
5. 確認選項無誤。

限制存取您的租用戶

在客戶層級或客戶層級以上的管理員，可以限制更高層級的系統管理員存取其租用戶。

如果對租用戶的存取不受限制，父租用戶的系統管理員將對您的租用戶擁有完整存取權。他們將能夠執行以下操作：

- 修改屬性
- 管理租用戶、使用者和服務
- 存取備份和其他資源

如果限制存取租用戶，則父租用戶系統管理員只能修改租用戶屬性。他們完全無法看到帳戶和子租用戶。

防止更高層級的系統管理員存取您的租用戶

1. 登入管理入口網站。
2. 前往 **[設定]** > **[安全性]**。
3. 停用 **[支援存取]** 開關。

因此，父租用戶的系統管理員對於租用戶的存取受限。他們僅能修改租用戶屬性，但無法存取或管理其內部的任何項目 (例如租用戶、使用者、服務、備份和其他資源)。

刪除租用戶

您可能想要刪除某個租用戶，以釋出其所使用的資源。使用狀況統計資料將在刪除後的一天內更新。若是大型租用戶，則需要更久的時間。

刪除租用戶之前，您必須先將其停用。如需有關操作方式的詳細資訊，請參閱「停用與啟用租用戶」。

注意事項
雖然 Cyber Protect 提供復原租用戶的機會，但請注意，File Sync & Share 服務不支援復原。

刪除租用戶

1. 在管理入口網站中，前往 **[用戶端]**。
2. 選擇您要刪除的已停用租用戶，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：

- 租用戶及其子租用戶都將遭到刪除。
- 在租用戶及其子租用戶內啟用的所有服務都將遭到停止。
- 租用戶及其子租用戶內的所有使用者都將遭到刪除。
- 租用戶及其子租用戶中的所有電腦都將遭到取消註冊。
- 租用戶及其子租用戶中與服務相關的所有資料 (例如，備份和已同步的檔案) 都將遭到刪除。
- 租用戶及其子租用戶內的所有 API 用戶端都將遭到刪除，而且使用這些用戶端的所有整合都將停止運作。
- 您會看到**租用戶狀態**為**已刪除**。當您將滑鼠暫留在**已刪除**的狀態時，會看見租用戶遭刪除的日期。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。

復原租用戶

租用戶有可能遭不慎刪除，因此 Cyber Protect 提供復原租用戶的機會。

在下列情況中，您可能會需要復原租用戶：

- 合作夥伴不慎刪除其租用戶。
- 合作夥伴開發團隊在測試整合時，不慎刪除部分甚至整個租用戶階層。
- 合作夥伴整合不慎取消佈建應用程式而非切換至新版本，而您需要復原資料。
- 合作夥伴切換至新授權時不慎停用應用程式，而您需要復原已停用應用程式中的資料。

若要復原租用戶

1. 在管理入口網站中，前往 **[用戶端]**。
2. 在 **Cyber Protect** 索引標籤上，尋找您要復原的租用戶。其狀態顯示為**已刪除**。
3. 將滑鼠暫留在租用戶上，然後按一下省略符號圖示 。
4. 按一下 **[復原]**。
   您會看到確認視窗，說明租用戶將會復原到刪除前的相同狀態，且將預設為停用。
5. [可選]如果您需要啟用租用戶，請選擇核取方塊**我想啟用租用戶**。您之後可以隨時啟用租用戶。
6. 按一下 **[復原]**。

結果：

- 租用戶及其子租用戶都將復原。
- 在租用戶及其子租用戶內啟用的所有服務都將重新啟動。

注意事項
File Sync & Share 服務不支援復原。

- 租用戶及其子租用戶內的所有使用者都將復原。
- 租用戶及其子租用戶中的所有電腦都將重新註冊。
- 租用戶及其子租用戶中與服務相關的所有資料 (例如，備份) 都將復原。
- 租用戶及其子租用戶內的所有 API 用戶端都將復原，而且使用這些用戶端的所有整合都將再次開始運作。
- 若您已啟用租用戶，則會看到**租用戶狀態**為**使用中**，若尚未啟用租用戶，會看到狀態為**已停用**。

管理使用者

合作夥伴系統管理員、客戶系統管理員以及單位系統管理員可以設定並管理他們可以存取的租用戶下的使用者帳戶。

建立使用者帳戶

在下列情況中，您可能希望建立額外帳戶：

- 合作夥伴/資料夾系統管理員帳戶 — 以便與其他人員分擔服務管理責任。
- 客戶/潛在客戶/單位系統管理員帳戶 — 委派服務管理給其他存取權限被嚴格限制為相對應的客戶/潛在客戶/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。

請注意，現有帳戶無法在租用戶之間移動。首先，您必須建立一個租用戶，然後填入帳戶。

建立使用者帳戶

1. 登入管理入口網站。
2. 瀏覽到您要建立使用者帳戶的租用戶。請參閱 "在管理入口網站內瀏覽" (第 25 頁)。
3. 按一下右上角的 **[新增]** > **[使用者]**。
   或者，前往 **[公司管理]** > **[使用者]**，然後按一下 **[+ 新增]**。
4. 為帳戶指定下列連絡資訊：
   a. **電子郵件**。此電子郵件也當作登入使用。
   b. 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
      每個帳戶都必須有唯一的登入。

      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。

   c. **名字**
   d. **姓氏**

e. [選用] **[公司電話]**

> **注意事項**
> 只有在上層合作夥伴為客戶租用戶啟用了 [啟用自我管理的客戶設定檔] 選項時，使用者建立精靈中才會顯示 **[公司電話]**、**[職稱]** 和 **[公司聯絡人]** 等欄位。否則不會顯示這些欄位。

f. [選用] **[職稱]**

g. 在 **[語言]** 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，使用者將擁有您在所選服務內選擇的角色。
7. 按一下 **[建立]**。

新建立的使用者帳戶會出現在 **[公司管理]** 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 **[公司管理]** > **[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。

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*，也就是不需要雙重驗證機制的帳戶。

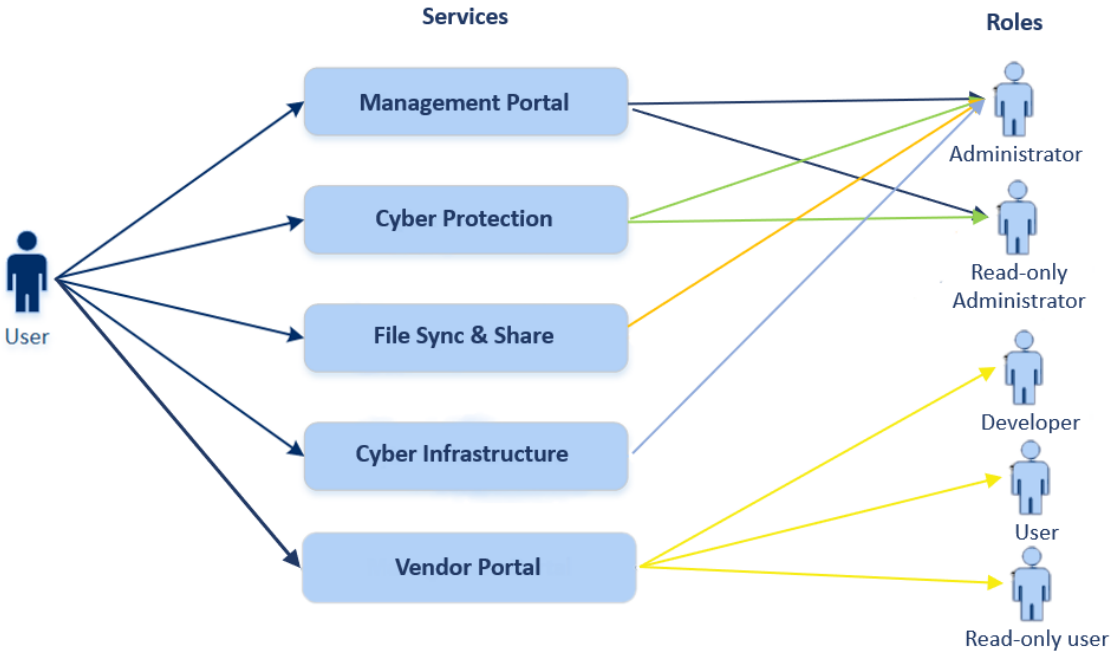
若要將使用者帳戶轉換為服務帳戶類型

1. 在管理入口網站中，前往 **[公司管理]** > **[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。

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 Cyber Protection 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 描述和 CyberApp 版本。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 描述，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。
Cyber Protection	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 Cyber Scripting 設定並管理 Cyber Protection 服務，以及核准動作。 Cyber 系統管理員角色僅適用於已啟用進階管理組件的租用戶。
	系統管理員	此角色允許為您的客戶設定和管理 Cyber Protection。 設定和管理災難復原功能和公司允許清單時，需要此角色。
	唯讀系統管理員	此角色會針對 Cyber Protection 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災難復原功能或公司允許名單。
	使用者	此角色允許使用 Protection 服務，但是沒有系統管理權限。可存取端點偵測與回應等功能，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。
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。
合作夥伴入口網站	合作夥伴入口網站使用者可以獲指派多種角色。如需詳細資訊，請參閱 "合作夥伴入口網站角色" (第 109 頁)。	

注意事項

供應商入口網站僅供 2023 年 10 月 04 日之後在 Acronis 技術生態系統網站上註冊的技術合作夥伴使用。

如果您是希望與 Acronis 整合的供應商，而且需要存取供應商入口網站和專用沙箱，請依照指示進行。

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 Cyber Protection 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。

使用者角色及網路指令碼權限

指令碼及指令碼計劃的可用操作取決於指令碼狀態及您的使用者角色。

系統管理員可以管理其自己租用戶及其子系租用戶。他們無法查看或存取上級管理等級的對象，如果有。

較低層級的系統管理員僅能以唯讀方式存取上層系統管理員套用至其工作負載的指令碼計劃。

以下角色提供有關網路指令碼的權限：

- **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。關於網路指令碼，其與網路系統管理員角色授予相同的權限。
- **網路系統管理員**
  此角色授予完整權限，包含核准可在租用戶使用的指令碼，以及具有執行 **[測試]** 狀態指令碼的能力。
- **系統管理員**
  此角色授予部分權限，並能執行核准的指令碼，使用核准的指令碼來建立並執行指令碼計劃。
- **唯讀系統管理員**
  此角色授予有限權限，並能檢視使用者使用的指令碼及保護計劃。
- **使用者**
  此角色授予部分權限，並能執行核准的指令碼，使用核准的指令碼來建立並執行指令碼計劃，但僅能在使用者自己的電腦執行。

下表列出所有可用的操作，取決於指令碼狀態及使用者角色而定。

角色	物件	指令碼狀態		
		草稿	正在測試	已核准
網路系統管理員 **公司系統管理員**	指令碼計劃	編輯(從計劃移除草稿指令碼) 刪除 撤回 停用	建立 編輯 套用 啟用 執行	建立 編輯 套用 啟用 執行

		停止	刪除 撤回 停用 停止	刪除 撤回 停用 停止
	指令碼	建立 編輯 變更狀態 複製 刪除 取消執行	建立 編輯 變更狀態 執行 複製 刪除 取消執行	建立 編輯 變更狀態 執行 複製 刪除 取消執行
系統管理員 **使用者** (針對自己的工作負載)	指令碼計劃	檢視 撤回 停用 停止	檢視 取消執行	建立 編輯 套用 啟用 執行 刪除 撤回 停用 停止
	指令碼	建立 編輯 複製 刪除 取消執行	檢視 複製 取消執行	執行 複製 取消執行
唯讀系統管理員	指令碼計劃	檢視	檢視	檢視
	指令碼	檢視	檢視	檢視

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 **[公司管理]** > **[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：

- **配額過度使用通知** (預設為啟用)
  已超出配額的相關通知。
- **已排程的使用報告** (預設為啟用狀態)
  在每個月的第一天傳送的使用報告。
- **URL 商標通知** (預設為停用)
  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** (預設為啟用)
  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** (預設為啟用)
  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** (預設為停用狀態)
  啟用裝置控制模組時，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** (預設為停用狀態)
  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** (預設為停用狀態)
  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** (預設為停用狀態)
  有關主動即時、執行時和按需掃描期間偵測到惡意程式碼的通知，以及有關來自行為引擎和 URL 過濾引擎的偵測通知。
  有兩個可用的選項：**[已緩解]** 和 **[未緩解]**。這些選項與端點偵測與回應 (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**(預設為停用)
  有關災難復原基礎架構問題的通知：當災難復原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。

使用者角色收到的通知

Cyber Protection 所傳送的通知取決於使用者角色。

通知類型\使用者角色	使用者	客戶和單位管理員	合作夥伴和資料夾系統管理員
適用於自攜裝置的通知	是	是	不適用*
適用於子租用戶所有裝置的通知	不適用	是 (但 **[安全性事件通知]** 除外)	是
適用於 Microsoft 365、Google Workspace 和其他雲端式備份的通知	不適用	是	是

* 合作夥伴系統管理員無法登錄自攜裝置，但是可以建立自己的客戶系統管理員帳戶，並使用這些帳戶新增自攜裝置。請參閱使用者帳戶與租用戶。

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。

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。

復原使用者帳戶

使用者帳戶有可能遭不慎刪除，因此 Cyber Protection 提供復原使用者帳戶的機會。

在下列情況中，您可能會需要復原使用者帳戶：公司系統管理員刪除離開公司的使用者，但您仍需要登錄在該使用者下的所有資源。

若要復原使用者帳戶

1. 在管理入口網站中，前往 **[公司管理]** > **[使用者]**。
2. 在**使用者**索引標籤上，尋找您要復原的使用者帳戶。其狀態顯示為**已刪除**。
3. 將滑鼠暫留在使用者帳戶上，然後按一下省略符號圖示 。
4. 按一下 **[復原]**。
   您會看到確認視窗，說明使用者帳戶將會復原到刪除前的相同狀態，且將預設為停用。
5. [可選]如果您需要啟用使用者帳戶，請選擇核取方塊**我想啟用使用者**。您之後可以隨時啟用使用者帳戶。
6. 按一下 **[復原]**。

結果：

- 此使用者帳戶將復原。
- 屬於此使用者帳戶的所有資料都將復原。
- 與此使用者帳戶相關聯的所有電腦都將重新註冊。
- 若您已啟用使用者帳戶，則會看到使用者狀態為**使用中**，若尚未啟用使用者帳戶，會看到狀態為**已停用**。

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。

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。

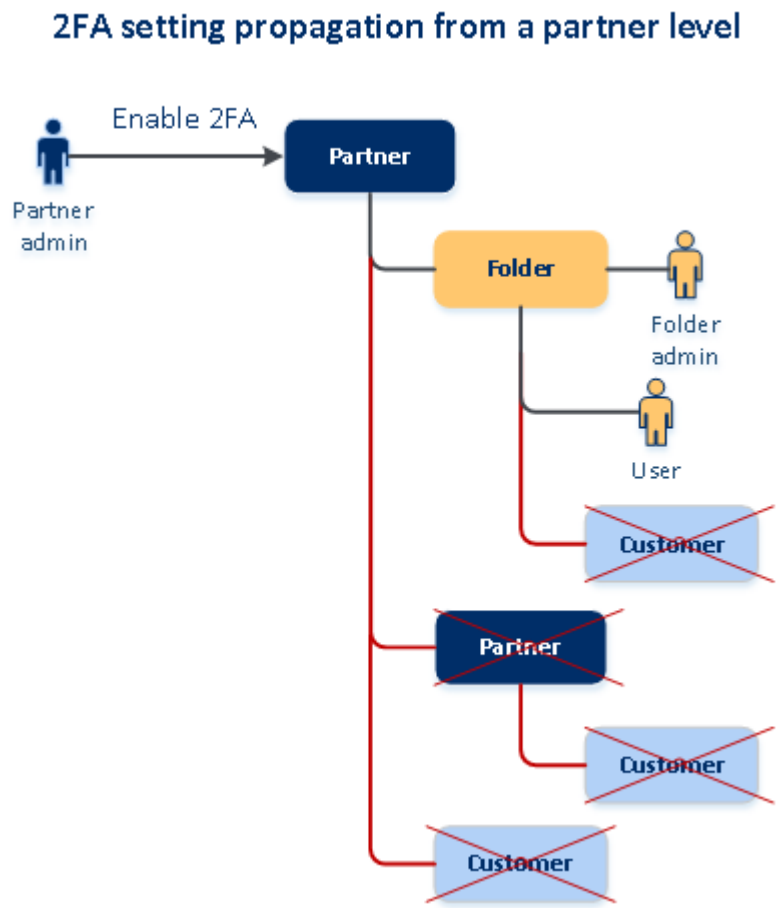
跨租用戶層級的雙重要素設定傳播

雙重驗證機制是在**組織**層級設定的。您可以啟用或停用雙重驗證機制：

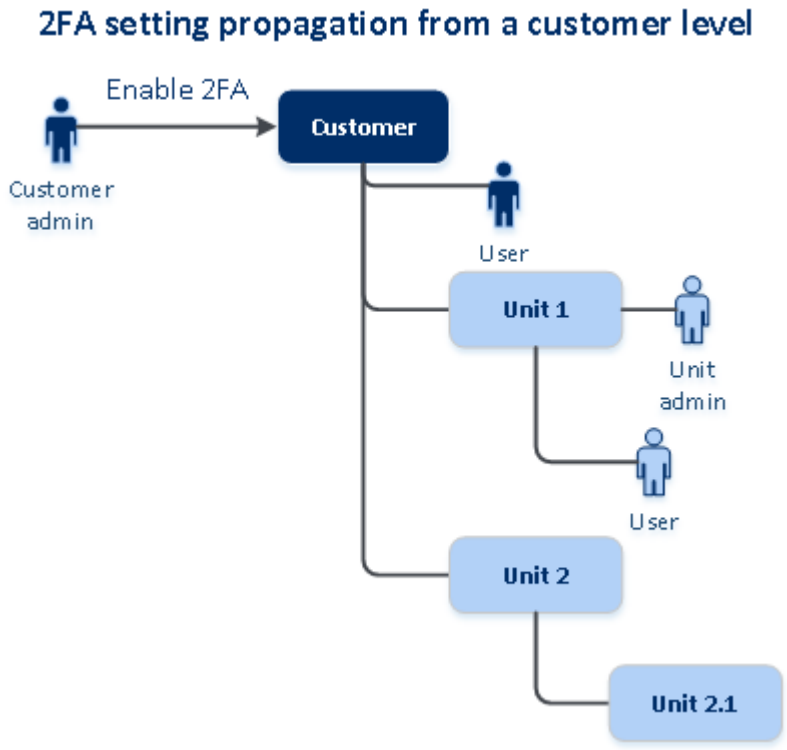
- 針對您自己的組織。
- 針對您的子租用戶 (只有在該子租用戶內啟用 **[支援存取]** 選項時)。

雙重驗證機制設定會跨租用戶層級傳播，如下所示：

- 資料夾會從其合作夥伴組織自動繼承雙重驗證機制設定。在以下的配置中，紅色線條表示無法傳播雙重驗證機制設定。



- 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. 您只有在該子組織內啟用 **[支援存取]** 選項時，才能針對您的子組織啟用或停用雙重驗證機制。
2. 您只有在該子組織內啟用 **[支援存取]** 選項時，才能針對子組織的使用者，管理雙重驗證機制設定。
3. 在資料夾或單位層級上無法設定雙重驗證機制。
4. 即使您的父組織沒有啟用此設定，您還是可以設定雙重驗證機制設定。

為您的租用戶設定雙重驗證機制

作為管理員，您可以為組織啟用雙重身份驗證。

若要為您的租用戶啟用雙重驗證機制

1. 在管理入口網站中，前往 **[設定]** > **[安全性]**。
2. 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 **[公司管理]** > **[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。

若要為您的租用戶停用雙重驗證機制

1. 在管理入口網站中，前往 **[設定]** > **[安全性]**。
2. 要停用雙重身份驗證，請關閉切換開關，然後按一下 **[停用]**。
3. [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，系統會為貴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 **[公司管理]** > **[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 **[公司管理]** > **[使用者]** 索引標籤下重設設定。

監控

在管理入口網站的 **[公司管理]** > **[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 **[公司管理]** > **[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 **[公司管理]** > **[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 **[公司管理]** > **[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 **[公司管理]** > **[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。

設定適用於客戶的追加銷售案例

追加銷售是邀請您的客戶購買額外功能的一種技術。

Cyber Protection 有數個舊版，所有版本在功能和價格上都不同。您可能會想要對使用基本版本的現有客戶推銷功能更進階的更昂貴版本。

您可以針對客戶，啟用或停用追加銷售功能。追加銷售選項預設為停用狀態。如果您為客戶啟用追加銷售選項，他們將會看到在購買促銷版本之前無法使用的其他功能。這個額外的功能會以標籤標示，其上顯示促銷版本的名稱或圖示，而且全部都以橘色醒目提示。這些追加銷售點將會向客戶顯

示，以刺激他們購買更昂貴的版本。按一下這些追加銷售點時，客戶將會看到一個對話方塊，建議他們購買更昂貴的版本，以啟用想要的功能。

動作項目取決於客戶使用者的類型。您可以使用平台 API 設定使用者的類型 (購買者或非購買者)。如需詳細資訊，請參閱 API 文件。如需有關向客戶顯示之動作項目的詳細資訊，請參閱下表：

客戶租用戶中的使用者類型	動作項目
系統管理員；購買者	**[立即購買]** 按鈕會顯示在使用者介面中。*
系統管理員；非購買者	「若要升級版本，請與您的合作夥伴聯絡」這則訊息會顯示在使用者介面中。
使用者；購買者	「若要升級版本，請與您的合作夥伴聯絡」這則訊息會顯示在使用者介面中。
使用者；非購買者	「若要升級版本，請與您的合作夥伴聯絡」這則訊息會顯示在使用者介面中。

* 將客戶重新導向至某個網站以購買更進階版本的 **[立即購買]** 按鈕連結可以在 **[設定]** > **[商標]** 中設定。在 **[追加銷售]** 區段中，您可以指定 **[購買 URL]**。商標設定將會套用到設定商標所在租用戶的所有直接和間接的子合作夥伴/資料夾以及客戶。

針對客戶啟用或停用追加銷售功能

1. 在管理入口網站中，前往 **[用戶端]**。
2. 選擇客戶，移至右窗格，然後按一下 **[設定]** 索引標籤。
3. 在 **[追加銷售]** 區段中，執行下列作業：
   - 啟用 **[宣傳其他進階版]** 可開啟客戶的追加銷售案例。
   - 停用 **[宣傳其他進階版]** 可關閉客戶的追加銷售案例。

向客戶顯示的追加銷售點

弱點清單

弱點清單可以在 Cyber Protect 主控台的 **[軟體管理]** > **[弱點]** 中找到。當使用者按一下切換圖示時，將會開啟版本宣傳對話方塊，以提示使用者購買更昂貴的版本。

建立或編輯保護計劃

這可以在 Cyber Protect 主控台的 **[計劃]** > **[保護]** 中找到。按一下 **[建立計劃]**。Cyber Backup 版本僅啟用 **[備份]** 和 **[弱點]** 模組；其餘模組僅能在 Cyber Protect 版本中使用。您的客戶將能夠在購買其中一個 Cyber Protect 版本之後，啟用所有模組。

自動探索精靈

此精靈可以在 Cyber Protect 主控台的 **[裝置]** > **[所有裝置]** 中找到。您的客戶應該按一下 **[新增]**，再移至 **[多個裝置]** 區段，然後按一下 **[僅限 Windows]**，以啟動自動探索精靈。自動探索電腦方法將僅

能在 Advanced 版本中使用。

裝置清單中的動作

此清單可以在 Cyber Protect 主控台的 **[裝置]** > **[所有裝置]** 中找到。您的客戶應該選擇電腦，然後兩個額外的選項就會顯示在左窗格中：

- **透過 HTML5 用戶端連線**
- **修補程式**

只有在客戶購買比現有版本還要昂貴的版本時，才能使用這些選項。

管理位置和儲存空間

[設定] > **[位置]** 區段會顯示您可以用來提供 **Cyber Protection** 和 **File Sync & Share** 服務給合作夥伴和客戶的雲端儲存空間和災難復原基礎架構。

在未來版本中，針對其他服務所設定的儲存空間將會顯示在 **[位置]** 區段上。

位置

位置是一種容器，可讓您以便利的方式，將雲端儲存空間和災難復原基礎架構群組在一起。位置可以代表您選擇的任何項目，例如，特定的資料中心，或基礎架構元件的地理位置。

您可以建立任何數量的位置，並填入備份儲存空間、災難復原基礎架構，以及**File Sync & Share**儲存空間。一個位置可以包含多個雲端儲存空間，但僅能包含一個災難復原基礎架構。

如需儲存空間作業的資訊，請參閱「管理儲存空間」。

選擇合作夥伴和客戶的位置和儲存空間

建立合作夥伴/資料夾租用戶時，您可以選擇在每個服務的新租用戶中將可使用的多個位置和多個儲存空間。

建立客戶租用戶時，必須選擇一個位置，然後在此位置內，每個服務選擇一個儲存空間。您稍後可以變更指派給客戶的儲存空間，但是只能在其使用量為 0 時，亦即，在客戶開始使用儲存空間之前，或在客戶從此儲存空間移除所有備份之後。

指派給客戶租用戶的儲存空間相關資訊，會在 **[用戶端]** 索引標籤上選擇租用戶時顯示在租用戶詳細資料面板上。關於儲存空間使用狀況的資訊並不會即時更新。資訊更新請等待最多 24 小時。

如需異地備援的相關資訊，請參閱 "異地備援儲存空間" (第 65 頁)。

位置的相關作業

若要建立新位置，按一下 **[新增位置]**，然後指定位置名稱。

若要將儲存空間或災難復原基礎架構移到另一個位置，選取該儲存空間或基礎架構、按一下 **[位置]** 欄位中的鉛筆圖示，然後選取目標位置。

若要為位置重新命名，按一下位置名稱旁邊的省略符號圖示、按一下 **[重新命名]**，然後指定新的位置名稱。

若要刪除位置，按一下位置名稱旁邊的省略符號圖示、按一下 **[刪除]**，然後確認您的決定。僅能刪除空位置。

管理儲存空間

新增儲存空間

- **Cyber Protection** 服務：
  - 依預設，備份儲存空間位於 資料中心。
  - 如果上層系統管理員已針對合作夥伴租用戶啟用 **[合作夥伴擁有的備份儲存空間]** 產品項目，則合作夥伴系統管理員可以使用 Cyber Infrastructure 軟體，在合作夥伴自己的資料中心中組織儲存空間。按一下 **[位置]** 區段上的 **[新增備份儲存空間]**，以尋找有關在您自己的資料中心中組織備份儲存空間的資訊。
  - 如果上層系統管理員已針對合作夥伴租用啟用了 **[合作夥伴擁有的災難復原基礎架構]** 產品項目，則合作夥伴系統管理員可以在合作夥伴自己的資料中心中組織災難復原基礎架構。如需有關新增災難復原基礎架構的資訊，請聯絡技術支援。

注意事項

資料中心使用的公有雲端物件儲存體 (例如 Amazon S3、Microsoft Azure、Google Cloud Storage 和 Wasabi) 無法進行備份驗證。

合作夥伴使用的公有雲端物件儲存體可以進行備份驗證。但是，不建議啟用此功能，因為驗證作業會增加來自這些公用物件儲存體的出口流量，而且可能會導致大量費用。

- 如需有關新增其他服務將使用的儲存空間的資訊，請聯絡技術支援。

刪除儲存空間

您可以刪除由您或您的子租用戶新增的儲存空間。

如果儲存空間是指派給任何客戶租用戶，則您必須先針對所有客戶租用戶停用使用該儲存空間的服務，然後才刪除儲存空間。

刪除儲存空間

1. 登入管理入口網站。
2. 瀏覽到新增儲存空間的租用戶。
3. 按一下 **[設定]** > **[位置]**。
4. 選擇您要刪除的儲存空間。
5. 在儲存空間屬性面板上，按一下省略符號圖示，然後按一下**[刪除儲存空間]**。
6. 確認選項無誤。

不可變動儲存空間

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。

不可變動儲存空間包含下列備份：

- 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。

您可以在合作夥伴層級和客戶層級上設定固定儲存空間。

重要事項
這些層級不是互相依存的。及使未在父合作夥伴租用戶中啟用固定儲存空間，客戶系統管理員也可以為其租用戶啟用固定儲存空間。只有在子租用戶中未套用任何自訂設定時，子租用戶才會繼承父租用戶的設定。

設定固定儲存空間設定必須在系統管理員帳戶所屬的租用戶中，使用雙重驗證機制。

固定儲存空間模式

針對合作夥伴租用戶，沒有固定儲存空間模式的選擇。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間。

針對客戶租用戶，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。
- **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。

注意事項
從 21.12 版開始，預設會針對新的合作夥伴租用戶啟用保留期間為 14 天的固定儲存空間。對於現有租用戶，您需要手動啟用固定儲存空間。

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。

啟用和停用固定儲存空間

設定固定儲存空間設定必須在系統管理員帳戶所屬的租用戶中，使用雙重驗證機制。

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。

啟用固定儲存空間

在合作夥伴租用戶中

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. 啟用 **[固定儲存空間]** 開關。
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. 按一下 **[儲存]**。

在客戶租用戶中

1. 以系統管理員身分，登入管理入口網站，然後移至 **[用戶端]**。
2. 若要為客戶租用戶編輯設定，請按一下其名稱。
3. 在導覽功能表中，移至 **[設定]** > **[安全性]**。
4. 啟用 **[固定儲存空間]** 開關。
5. 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。
6. 選擇固定儲存空間模式，然後在出現提示時確認您的選擇。
7. 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。

8. 若要讓現有的存檔支援固定儲存空間，請在該存檔中建立新備份。
   若要建立新備份，請手動或依排程執行保護計劃。

   警告！
   如果您在讓存檔支援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

在合作夥伴租用戶中

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。

   重要事項
   所有不使用固定儲存空間之自訂設定的子租用戶都將繼承此變更。

   警告！
   停用固定儲存空間不會立即生效。在 14 天的寬限期內，固定儲存空間仍處於作用中狀態，而且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，將永久刪除固定儲存空間內的所有備份。

3. 按一下 **[停用]**，確認您的選擇。

在客戶租用戶中

1. 以系統管理員身分，登入管理入口網站，然後移至 **[用戶端]**。
2. 若要為客戶租用戶編輯設定，請按一下其名稱。
3. 在導覽功能表中，移至 **[設定]** > **[安全性]**。
4. 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，固定儲存空間仍處於作用中狀態，而且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，將永久刪除固定儲存空間內的所有備份。

5. 按一下 **[停用]**，確認您的選擇。

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

異地備援儲存空間

異地備援儲存會將資料以非同步方式複製到在地理上遠離主要位置的次要位置，藉此確保資料的持久性。透過異地備援，即使主要位置無法使用，您的資料也可供存取。

啟用和停用異地備援儲存空間

必要條件

- 請確認異地備援儲存空間可用於您的雲端基礎架構。
- 只有系統管理員可以啟用或停用異地備援儲存空間。請確認您擁有系統管理員權限。

若要為現有的租用戶啟用異地備援儲存空間

1. 在管理入口網站中，前往 **[用戶端]**。
2. 瀏覽到您要為其啟用異地備援的租用戶。

   注意事項
   若要為多個租用戶啟用異地備援，請參閱 "為多個現有的租用戶啟用服務" (第 35 頁)。

3. 按一下 **[編輯]** 以變更設定。
4. 在 **[雲端資源]** 底下，選擇所需儲存空間名稱的 **[異地備援]** 核取方塊。
5. 按一下 **[儲存]**。
   租用戶隨即啟用異地備援。客戶系統管理員可以在 Cyber Protect 主控台中停用異地備援。

若要為現有的租用戶停用異地備援儲存空間

1. 在管理入口網站中，前往 **[用戶端]**。
2. 瀏覽到您要為其停用異地備援的租用戶。
3. 按一下 **[編輯]** 以變更設定。
4. 在 **[雲端資源]** 底下，清除所需儲存空間名稱的 **[異地備援]** 核取方塊。

5. 按一下 **[儲存]**。

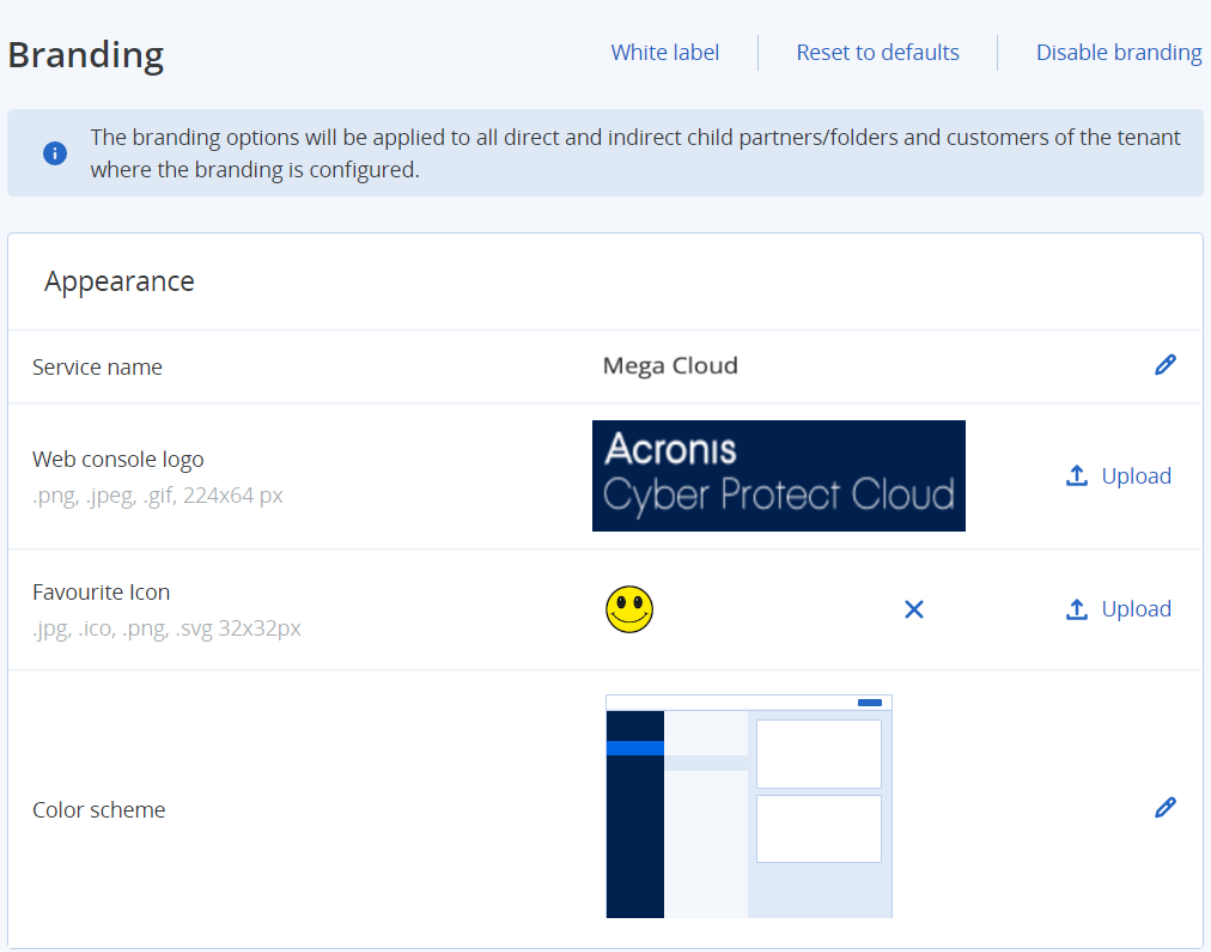
警告！
異地備援隨即遭到停用。複寫的資料將在一天內遭到刪除。

限制

- 目前複寫資料的次要位置僅適用於美國和加拿大。
- 如需使用異地備援時災難復原服務限制的相關資訊，請參閱「災難復原」文件。

設定商標和白色標籤服務

[設定] > **[商標]** 區段可讓合作夥伴系統管理員自訂管理入口網站和 **Cyber Protection** 服務的使用者介面，以移除與更高層級合作夥伴的所有關聯。



商標可在合作夥伴和資料夾層級上設定。商標會套用到所有直接和間接的子合作夥伴/資料夾，以及設定商標所在租用戶的客戶。

其他服務會在其服務主控台中提供個別的商標功能。如需詳細資訊，請參閱對應服務的使用指南。

商標項目

外觀

- **服務名稱**。此名稱會用在管理入口網站和雲端服務所傳送的所有電子郵件訊息中 (帳戶啟用訊息、服務通知電子郵件訊息)、第一次登入後的 **[歡迎]** 畫面上，以及作為管理入口網站瀏覽器索引標籤名稱。
- **[Web 主控台標誌]**。標誌會顯示在管理入口網站和服務。按一下 **[上傳]** 來上傳影像檔案。
- **[最愛圖示]** [僅在設定自訂 URL 時可用]。最愛圖示會顯示在瀏覽器索引標籤的頁面標題旁邊。按一下 **[上傳]** 來上傳影像檔案。
- **色彩配置**。色彩配置會定義所有使用者介面元素所使用的色彩組合。

注意事項
按一下 **[在新的索引標籤中預覽配置]** 可預覽子租用戶所看到的介面。在您按一下 **[選擇色彩配置]** 面板上的 **[完成]** 之前，將不會套用商標。

代理程式和安裝程式商標

您可以針對 Windows 和 macOS，自訂代理程式安裝檔案和系統匣監視器的商標。

注意事項
若要啟用此商標功能，您必須將 Cyber Protection 代理程式更新到 15.0.28816 (發行版本 22.01) 版或更新版本。

- **代理程式安裝程式檔案名稱**。在受保護的工作負載上下載的安裝檔案的名稱。
- **代理程式安裝程式標誌**。在代理程式安裝期間，顯示在安裝程式精靈中的標誌。按一下 **[上傳]** 來上傳影像檔案。
- **代理程式名稱**。在代理程式安裝期間，顯示在安裝程式精靈中的名稱。
- **系統匣監視器名稱**。顯示在系統匣監視器視窗頂端的名稱。

說明文件和支援

- **首頁 URL**。當使用者按一下 **[關於]** 面板上的公司名稱時，會開啟此頁面。
- **支援 URL**。當使用者按一下 **[關於]** 面板上或管理入口網站所傳送的電子郵件訊息中的 **[聯絡客戶服務支援]** 連結時，會開啟此頁面。
- **支援電話**。此電話號碼會顯示在 **[關於]** 面板上。
- **知識庫 URL**。當使用者按一下錯誤訊息中的 **[知識庫]** 連結時，會開啟此頁面。
- **管理入口網站系統管理員指南**。當使用者按一下管理入口網站使用者介面右上角的問號圖示，然後按一下 **[關於]** > **[系統管理員指南]** 時，會開啟此頁面。
- **管理入口網站系統管理員說明**。當使用者按一下管理入口網站使用者介面右上角的問號圖示，然後按一下 **[說明]** 時，會開啟此頁面。

Cyber Protect 雲端服務 URL

您可從自訂網域提供 Cyber Protect 雲端服務。首次設定自訂 URL，按一下 **[設定]**，或按一下 **[重新設定]** 以變更現有 URL。若要使用預設 URL (https://cloud.acronis.com)，按一下 **重設為預設值**。有關自訂 URL 的詳細資訊，請參閱設定自訂 Web 介面 URL。

法律文件設定

- **最終使用者授權合約 (EULA) URL**。當使用者在 **[關於]** 面板上、在第一次登入後的 **[歡迎]** 畫面上，以及在 上傳要求登陸頁面上，按一下 **[最終使用者授權合約]** 連結時，會開啟此頁面。
- **平台條款 URL**。當合作夥伴系統管理員在 **[關於]** 面板上或在第一次登入後的 **[歡迎]** 畫面上，按一下 **[平台條款]** 連結時，會開啟此頁面。
- **隱私權聲明 URL**。當使用者在第一次登入後的 **[歡迎]** 畫面上，以及在 上傳要求登陸頁面上，按一下 **[隱私權聲明]** 連結時，會開啟此頁面。

重要事項
如果您不希望文件出現在 [歡迎] 畫面上，請不要輸入該文件的 URL。

注意事項
如需有關 File Sync & Share 上傳要求的詳細資訊，請參閱《Cyber Files Cloud 使用指南》。

向上銷售

- **購買 URL**。當使用者按一下 **[立即購買]** 以升級至 Cyber Protection 服務的更進階版本時，會開啟此頁面。如需有關追加銷售案例的詳細資訊，請參閱「設定適用於客戶的追加銷售案例」。

行動應用程式

- **App Store**。當使用者在 **Cyber Protection** 服務中按一下 **[新增]** > **[iOS]** 時，會開啟此頁面。
- **Google Play**。當使用者在 服務中按一下 **[新增]** > **[Android]** 時，會開啟此頁面。

電子郵件伺服器設定

您可以指定一個自訂電子郵件伺服器，用來從管理入口網站和服務傳送電子郵件通知。若要指定自訂電子郵件伺服器，請按一下 **[自訂]**，然後指定下列設定：

- 在 **[寄件者]** 中，輸入會顯示在電子郵件通知的 **[寄件者]** 欄位中的名稱。
- 在 **[SMTP]** 中，輸入外送郵件伺服器 (SMTP) 的名稱。
- 在 **[連接埠]** 中，輸入外送郵件伺服器的連接埠。連接埠預設為 25。
- 在 **[加密]** 中，選擇使用 SSL 或 TLS 加密。選擇 **[無]** 以停用加密。
- 在 **[使用者名稱]** 和 **[密碼]** 中，指定將用於傳送訊息的帳戶認證。

設定商標

1. 登入管理入口網站。
2. 瀏覽到您要設定商標的租用戶。
3. 請按一下**[設定]** > **[商標]**。
4. [如果還未啟用商標] 按一下 **[啟用商標]**。
5. 設定上述的商標項目。

還原預設商標設定

您可以將所有商標項目重設為其預設值。

1. 登入管理入口網站。
2. 瀏覽到您要重設商標的租用戶。
3. 請按一下**[設定]** > **[商標]**。
4. 按一下右上方的 **[還原至預設值]**。

停用商標

您可以停用您帳戶及所有子租用戶的商標。

1. 登入管理入口網站。
2. 瀏覽到您要停用商標的租用戶。
3. 請按一下**[設定]** > **[商標]**。
4. 按一下右上方的 **[停用商標]**。

白色標籤服務

您可以針對所有子合作夥伴和客戶，控制 Cyber Protection 代理程式 (Windows 版、macOS 版和 Linux 版)、Cyber Protection 監視器 (Windows 版、macOS 版和 Linux 版) 與 Connect 用戶端 將是有商標的還是白色標籤的。如果您啟用白色標籤服務，則代理程式、Connect 用戶端 與系統匣監視器將是白色標籤的。此設定也會影響安裝程式和 Cyber Protection 監視器中所使用的名稱和標誌。

套用白色標籤服務

1. 登入管理入口網站。
2. 瀏覽到您要套用白色標籤服務的租用戶。
3. 請按一下**[設定]** > **[商標]**。
4. 在視窗的上端，按一下 **[白色標籤]** 可清除所有商標項目，但不包括 **[服務名稱]**、**[最終使用者授權合約 (EULA) URL]**、**[管理入口網站系統管理員指南]**、**[管理入口網站系統管理員說明]**，以及 **[電子郵件伺服器設定]**。

設定自訂網頁介面 URL

注意事項
與預設 URL 相比，自訂 URL 會指向不同的 IP 位址。設定防火牆原則時請記住這一點。

若要設定網路安全雲端服務的網頁介面 URL

1. 在管理入口網站，按一下 **[設定]** > **[品牌化]**。
2. 在 **[Cyber Protect 雲端服務 URL]** 區段：
   - 首次設定自訂 URL，按一下 **[設定]**。
   - 按一下 **[重新設定]** 以變更現有的自訂 URL。
3. 在 **[網域設定]** 步驟，準備您的網域和 CNAME 記錄。
   要使用自定義 URL，您必須具有網域名稱和設定為指向您的帳戶所在的資料中心的 CNAME 記錄。CNAME 記錄的設定由您的 DNS 註冊商完成，最多可能需要 48 小時才能傳播。
   若要尋找資料中心的網域名稱並要求設定 CNAME 記錄，請參閱 商標 Web 主控台 URL (58275) 文章。
4. 在 **[檢查您的 URL]** 步驟，確認您的自訂 URL 是否能夠存取，以及您的 CNAME 記錄設定正確。若要這麼做，請輸入主要 URL 名稱，然後按一下 **檢查**。如果您使用萬用字元 SSL 憑證，您最多可以新增 10 個替代網域名稱。如果您使用「讓我們加密」憑證，替代網域名稱將被忽略。
5. 在 **[SSL 憑證]** 步驟，您可執行下列其中一項作業：
   - 建立「讓我們加密」憑證。為此，按一下 **[帶有「讓我們加密」的免費 SSL 憑證]**。此選項使用第三方實體所核發的「Let's Encrypt」憑證。對於使用這些免費憑證而導致的任何問題，服務提供者概不負責。有關「讓我們加密」術語的更多資訊，請參閱 https://letsencrypt.org/repository/。
   - 上傳您的萬用字元憑證。若要這麼做，請按一下 **上傳萬用字元憑證**，然後提供萬用字元憑證和私密金鑰。

     注意事項
     出現憑證驗證錯誤時可能會有以下錯誤訊息："無法驗證憑證：x509：憑證已由未知授權簽署"。這通常代表缺少部分中間憑證。使用憑證鏈解析器修正您的憑證，並上傳完整憑證鏈。
6. 按一下 **提交** 以套用變更。

將自訂 URL 重設為預設值

1. 在管理入口網站，按一下 **[設定]** > **[品牌化]**。
2. 在 **[Acronis Cyber Protect Cloud 服務的 URL]** 區段，按一下 **[重設為預設值]** 來使用預設網址 (https://cloud.acronis.com)。

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]**。

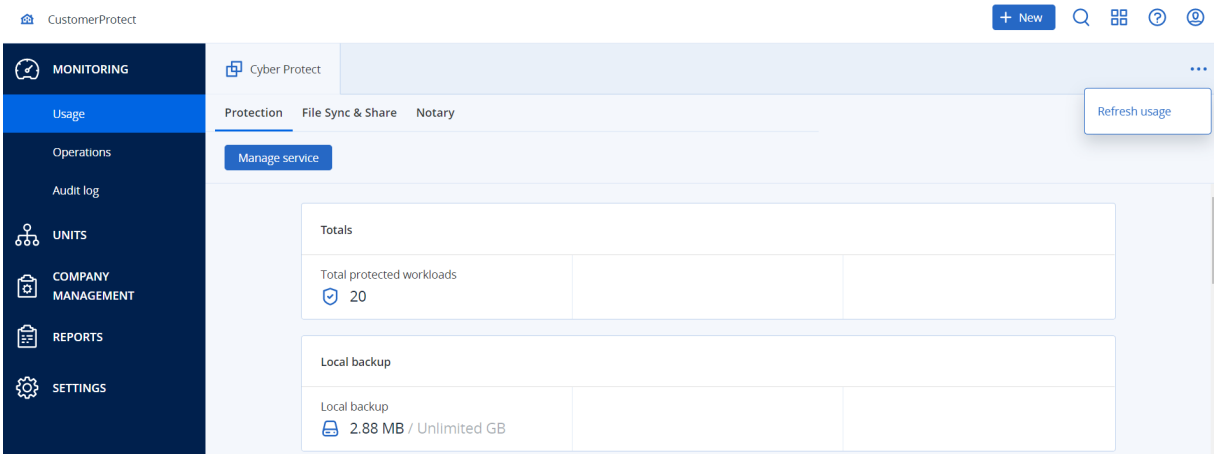
用量

[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。

要重新整理索引標籤上顯示的使用狀況資料，請按一下螢幕右上角的省略符號，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。



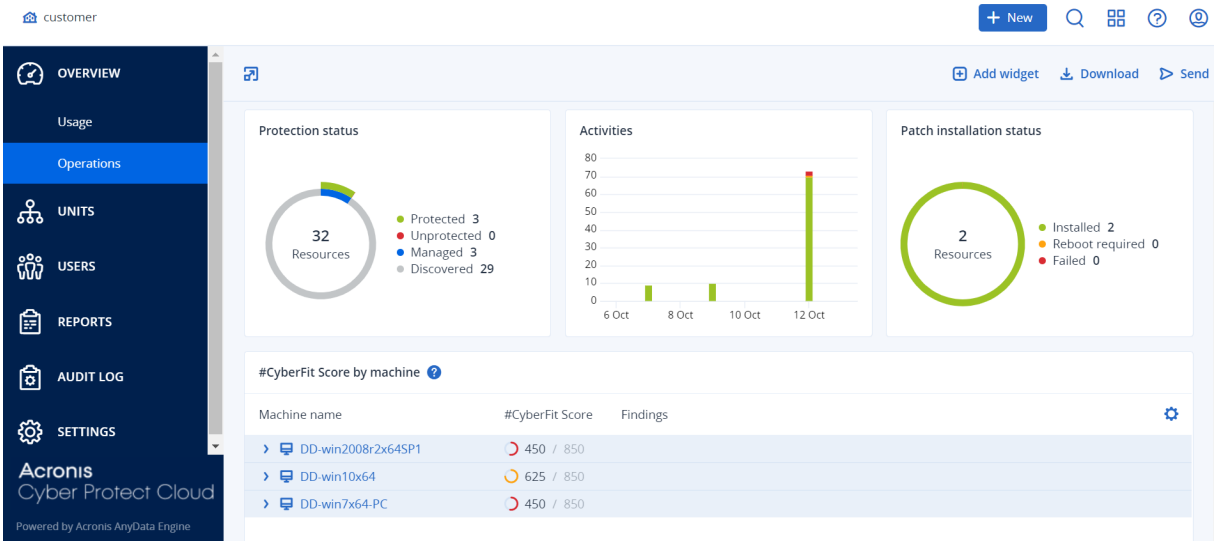
維運資訊

[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。針對其他服務的動態小工具將在未來版本中提供。

根據預設，會顯示您正在操作之租用戶的資料。您可以透過編輯動態小工具，為每個動態小工具個別變更顯示的租用戶。也會顯示關於所選租用戶的直接子客戶租用戶的彙總資訊，包括位於資料夾中的資訊。儀表板不顯示有關子合作夥伴及其子租用戶的資訊；您必須向下鑽研特定合作夥伴才能檢視其儀表板。不過，如果您將子合作夥伴租用戶轉換為資料夾租用戶，關於此租用戶之子客戶的資訊將會顯示在父租用戶的儀表板上。

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，或透過電子郵件將它傳送到任何地址 (包括外部收件者)。

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。您可以為不同租用戶新增相同類型的多個桌面小工具,或具有不同篩選的多個桌面小工具。



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、變更時間期間、選取要顯示資料的租用戶,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動態小工具,請在選取動態小工具時按一下齒輪圖示。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

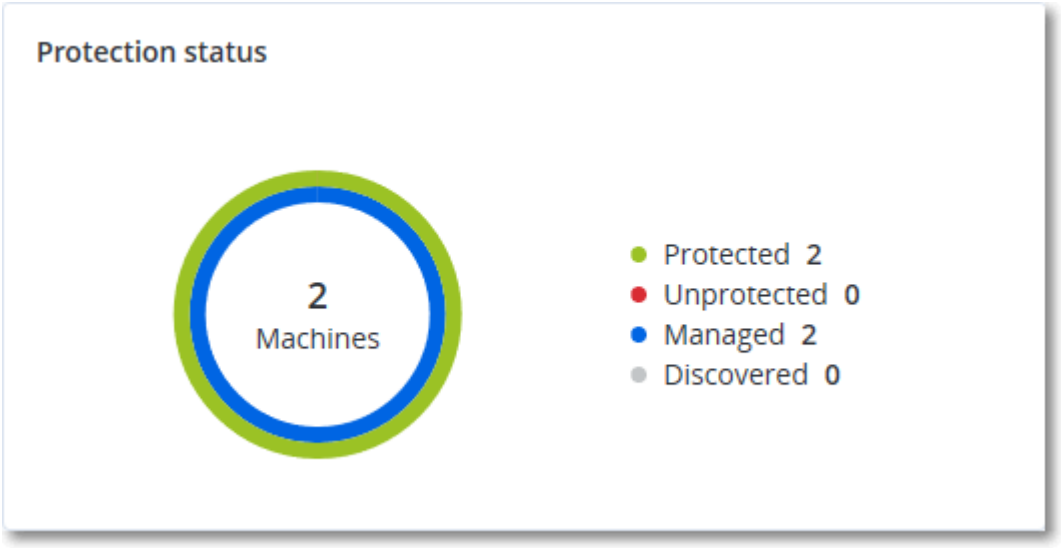
保護狀態

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。
- **已發現** – 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。



探索到的電腦

此桌面小工具會顯示在指定的時間範圍內發現之電腦的清單。

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

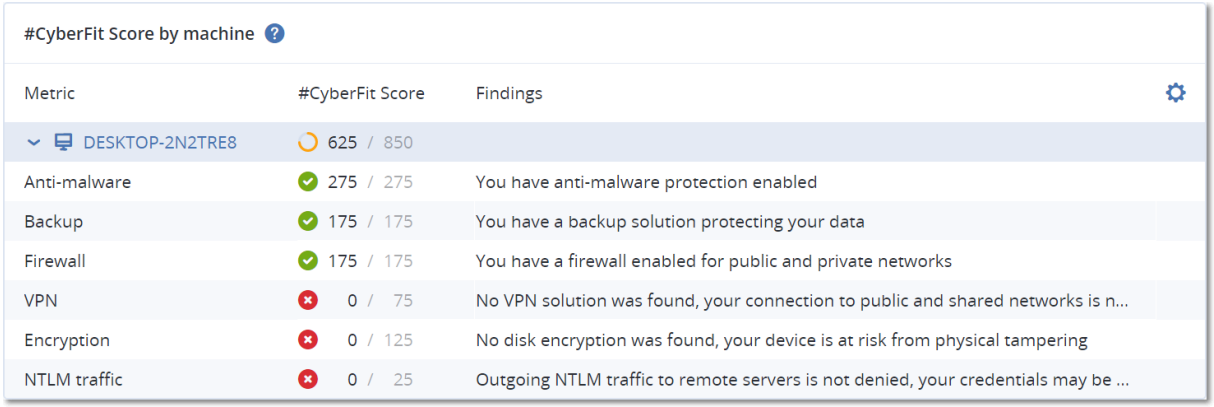
依電腦分類的 #CyberFit 分數

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」。



端點偵測與回應 (EDR) 桌面小工具

重要事項
這是優先體驗版本的 EDR 文件。部分功能和描述可能不完整。

端點偵測與回應 (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

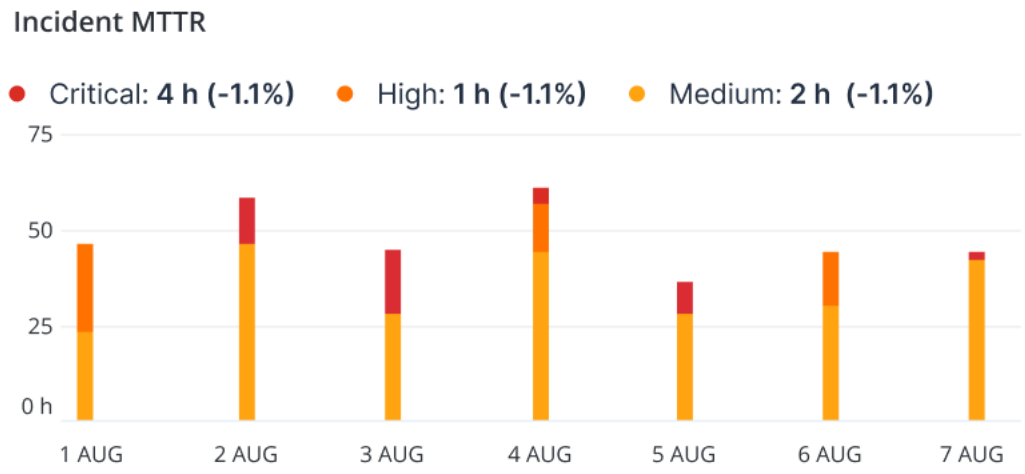
此桌面小工具會顯示包含最多事件的前五個工作負載 (按一下 **[全部顯示]** 可重新導向至根據桌面小工具設定篩選的事件清單)。

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。

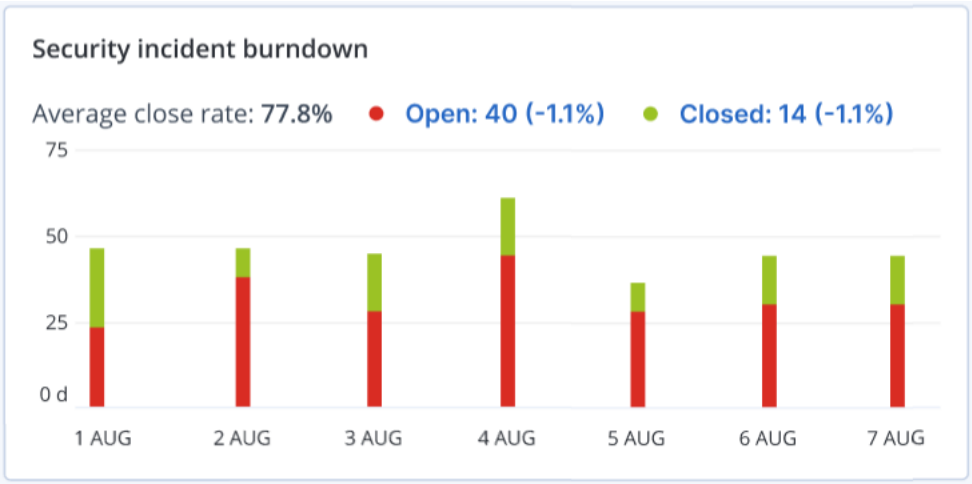


安全性事件待執行工作

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。

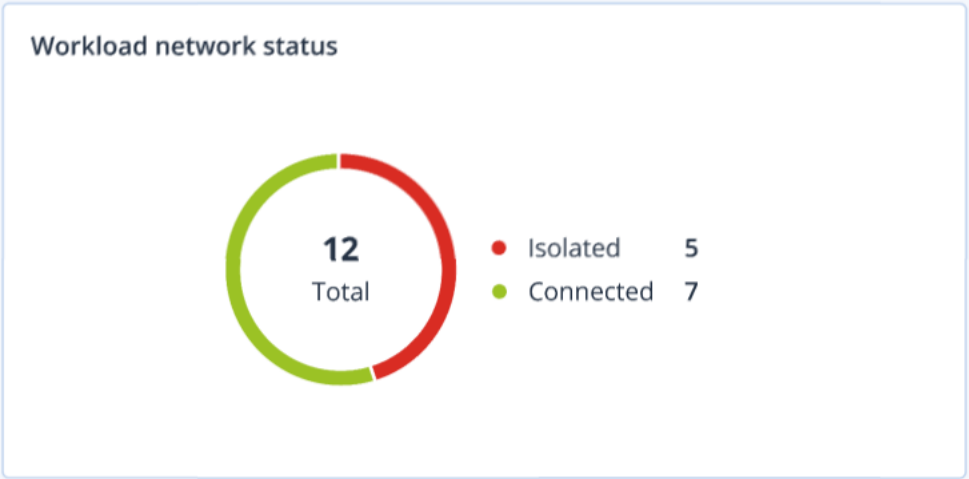
顯示在括號中的 % 值表示與前一段時間相比增加或減少。



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。

磁碟健全狀況以下列其中一種狀態表示：

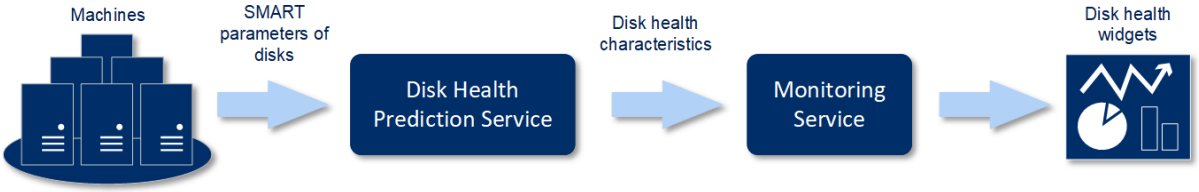
- **正常**
  磁碟健全狀況介於 70% 到 100% 之間。
- **警告**
  磁碟健全狀況介於 30% 到 70% 之間。
- **重大**
  磁碟健全狀況介於 0% 到 30% 之間。
- **正在計算磁碟資料**
  目前的磁碟狀態和預測正在計算中。

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。

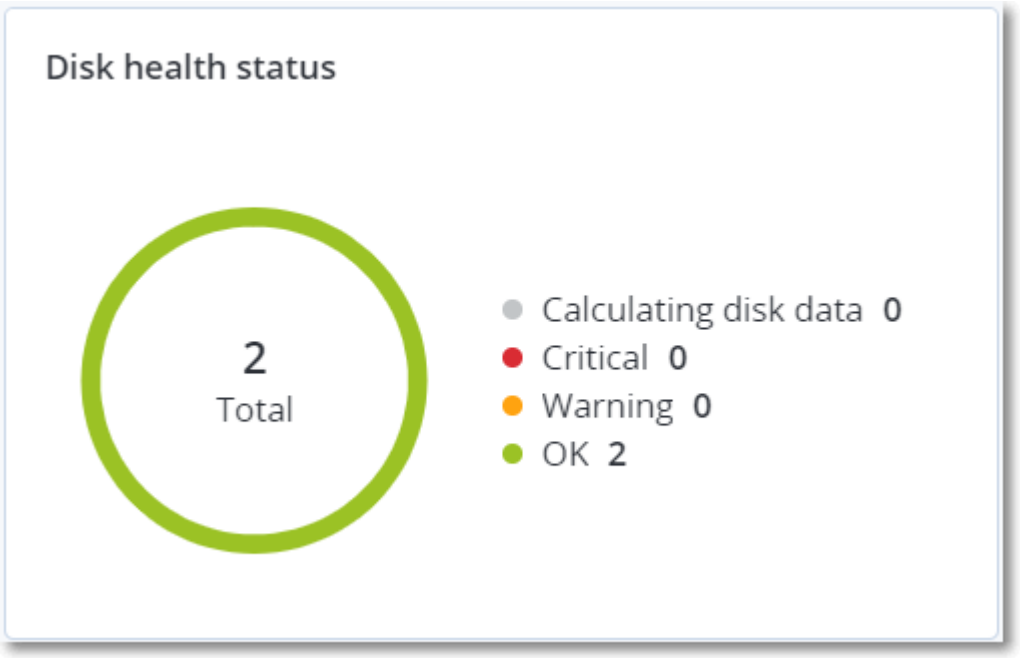
- **磁碟健全狀況概觀**是一個樹狀圖桌面小工具，其中包含可以透過查找切換的兩個詳細資料層級。
  - 電腦層級
    針對選取的客戶電腦，顯示磁碟健全狀況狀態的摘要資訊。只有最嚴重的磁碟狀態才會顯示。

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 <磁碟名稱> 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 <磁碟名稱> 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檢查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。

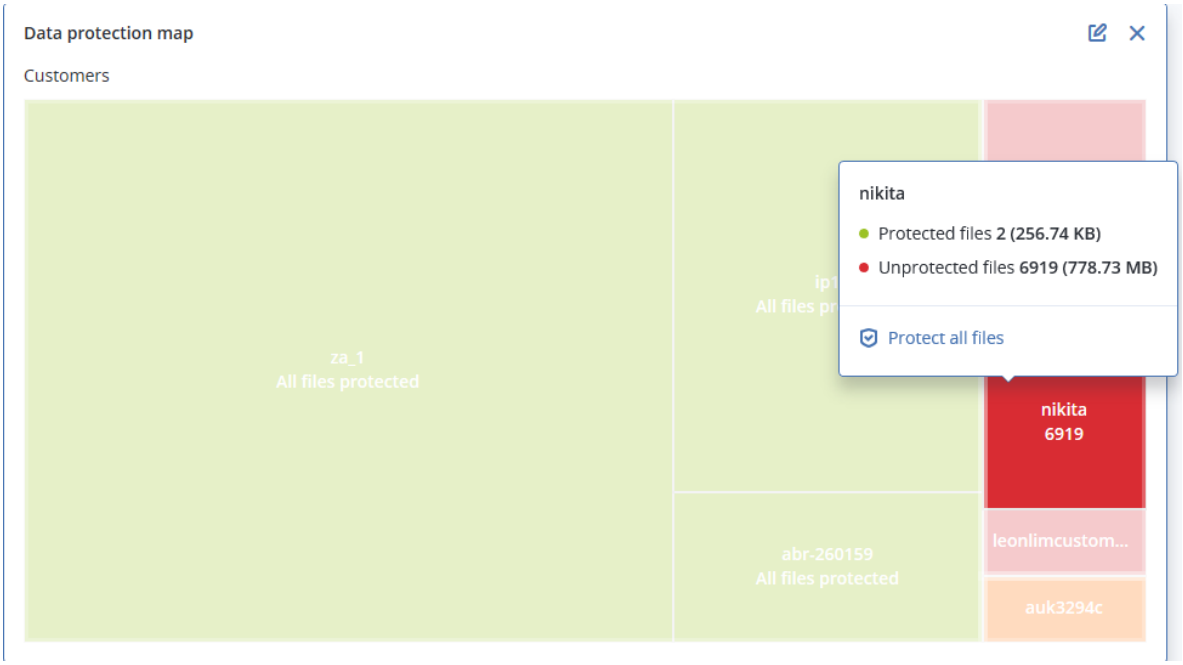
每個區塊大小取決於客戶/電腦所屬所有重要檔案的總數/大小總計。

檔案可以擁有以下保護狀態之一：

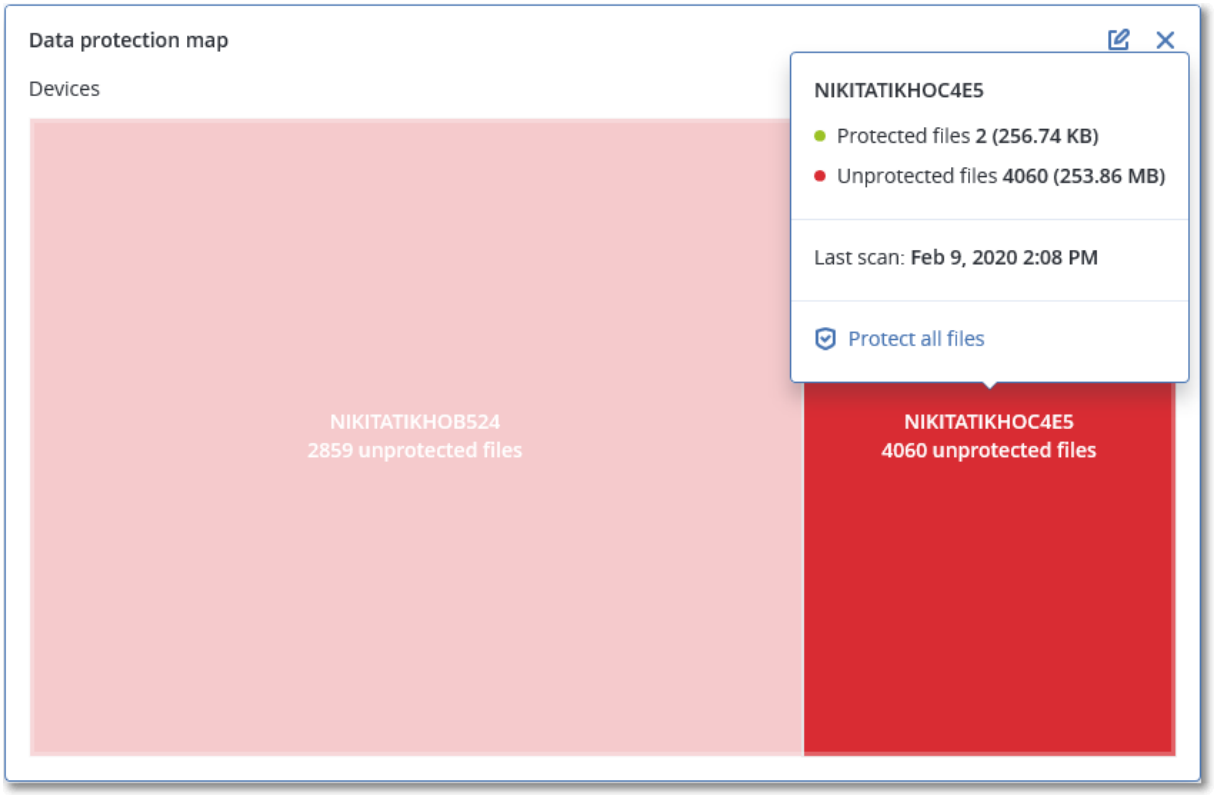
- **重大** – 有 51-100% 具有您指定之副檔名的未受保護檔案未針對所選客戶租用戶/電腦/位置進行備份。
- **低** – 有 21-50% 具有您指定之副檔名的未受保護檔案未針對所選客戶租用戶/電腦/位置進行備份。
- **中** – 有 1-20% 具有您指定之副檔名的未受保護檔案未針對所選客戶租用戶/電腦/位置進行備份。
- **高** – 具有您指定之副檔名的所有檔案都針對所選客戶租用戶/電腦/位置受到保護 (備份)。

資料保護檢查的結果可以在資料保護圖桌面小工具 (包含兩個詳細資料層級的樹狀圖桌面小工具，可以透過查找切換) 的儀表板上找到：

- 客戶租用戶層級 – 針對您已經選擇的每個客戶，顯示重要檔案保護狀態的摘要資訊。



- 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。

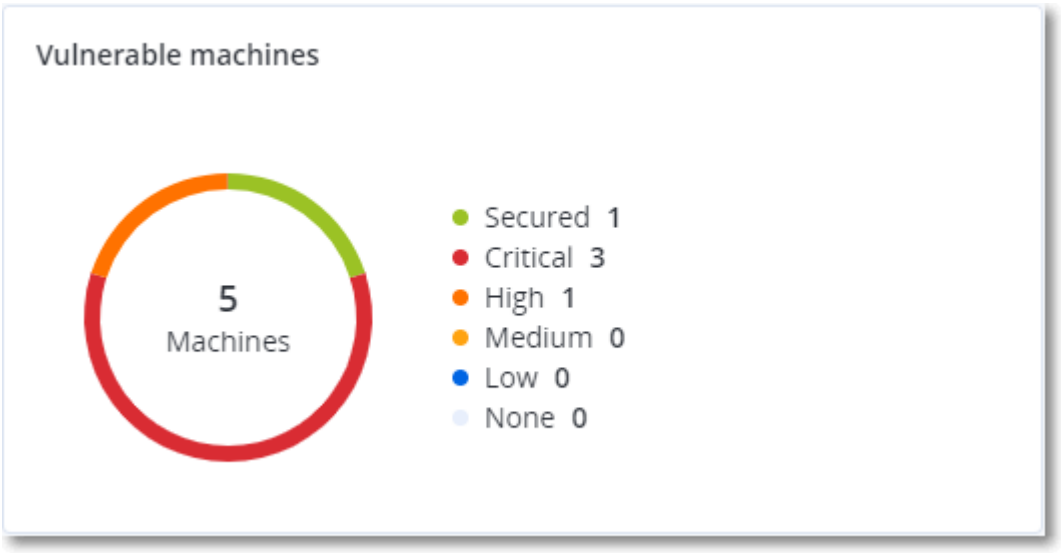
弱點評估桌面小工具

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

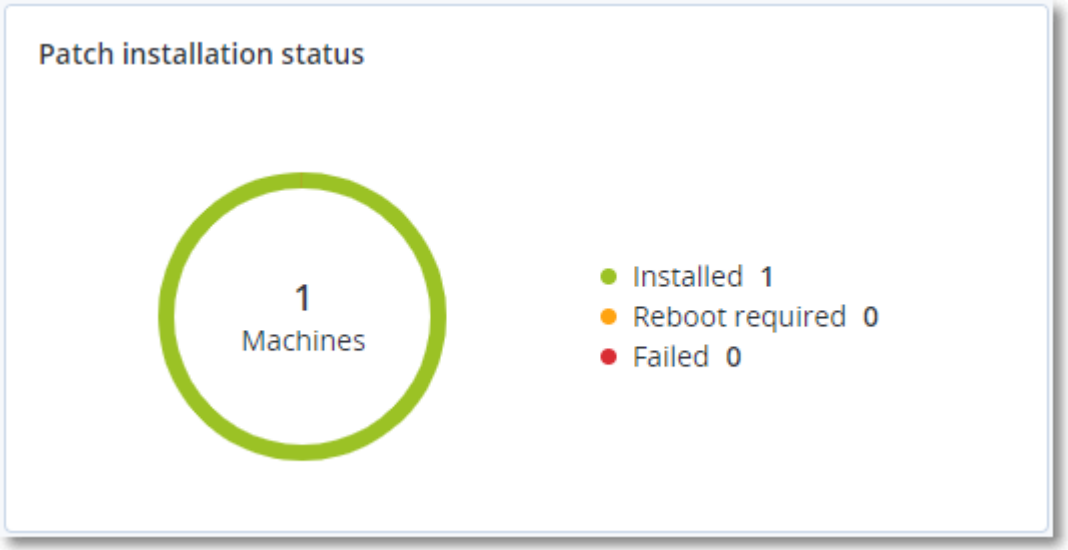
修補程式安裝桌面小工具

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。

Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

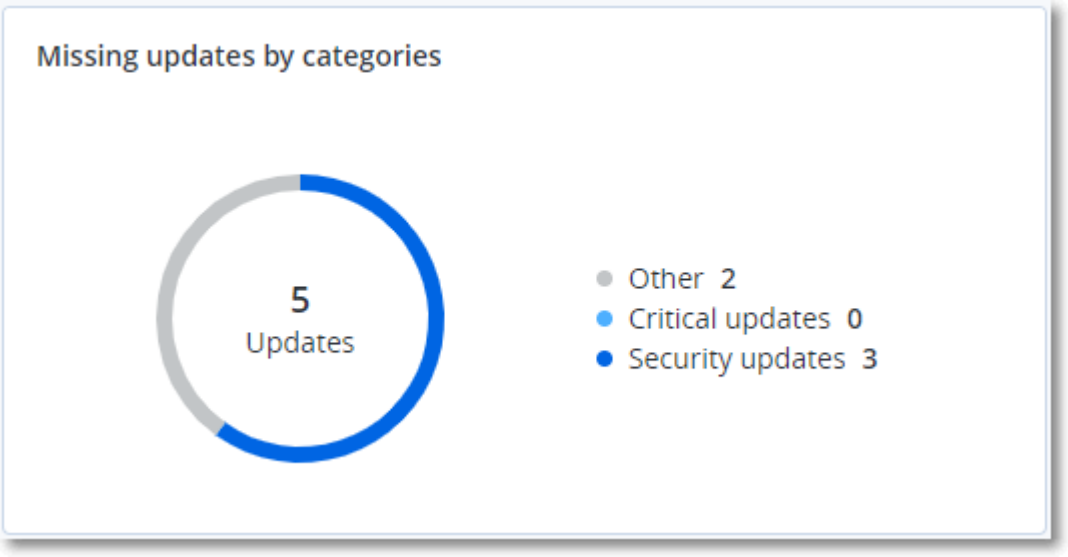
修補程式安裝歷史記錄

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)

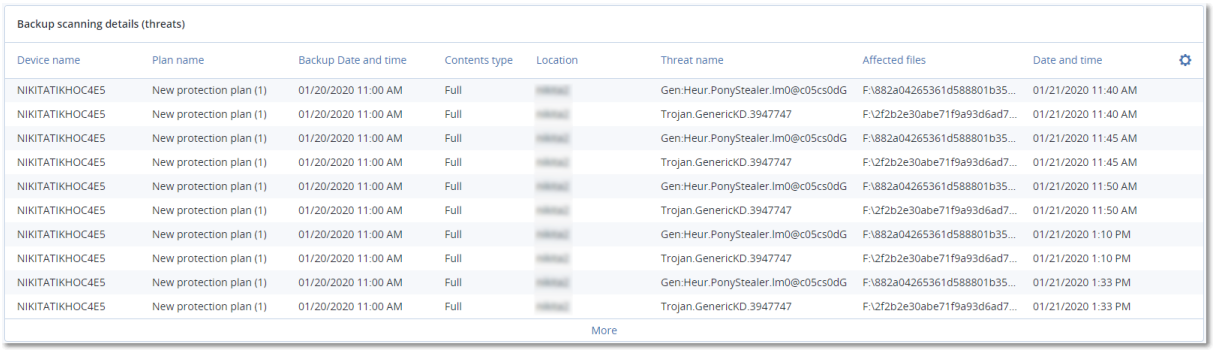
此桌面小工具會依類別顯示遺漏的更新數目。顯示下列類別：

- 安全性更新
- 重大更新
- 其他



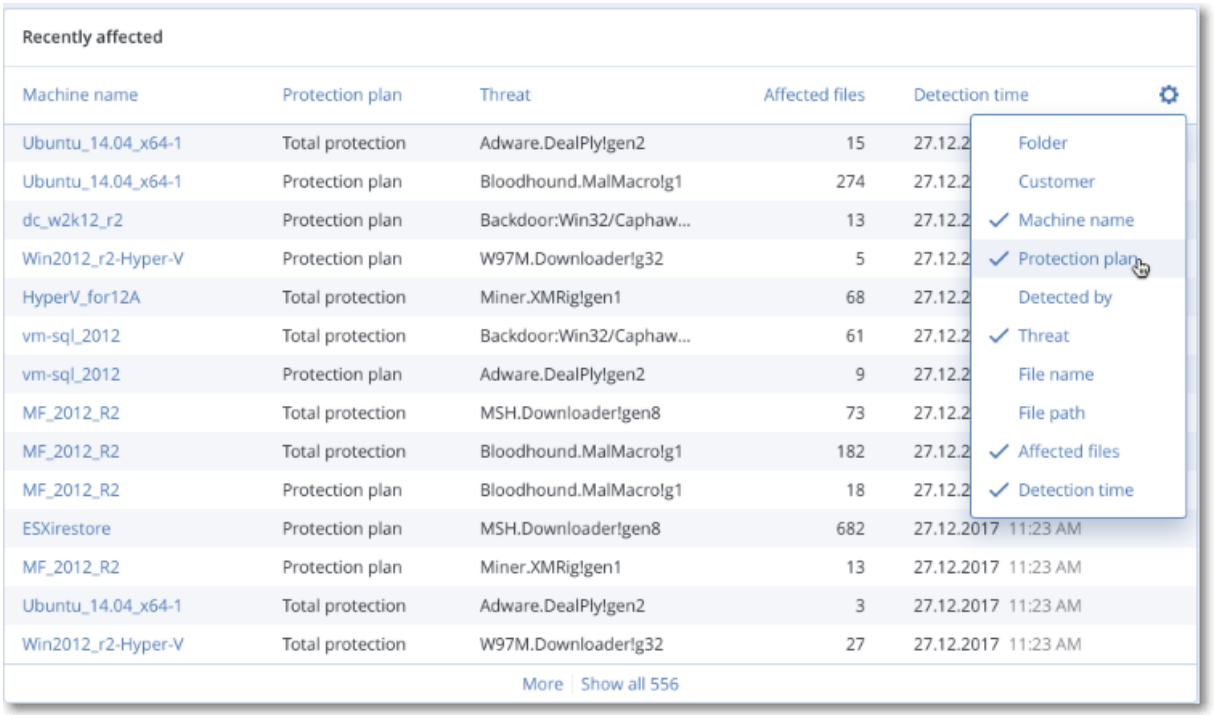
備份掃描詳細資料

此桌面小工具會顯示備份中偵測到之威脅的詳細資訊。



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。

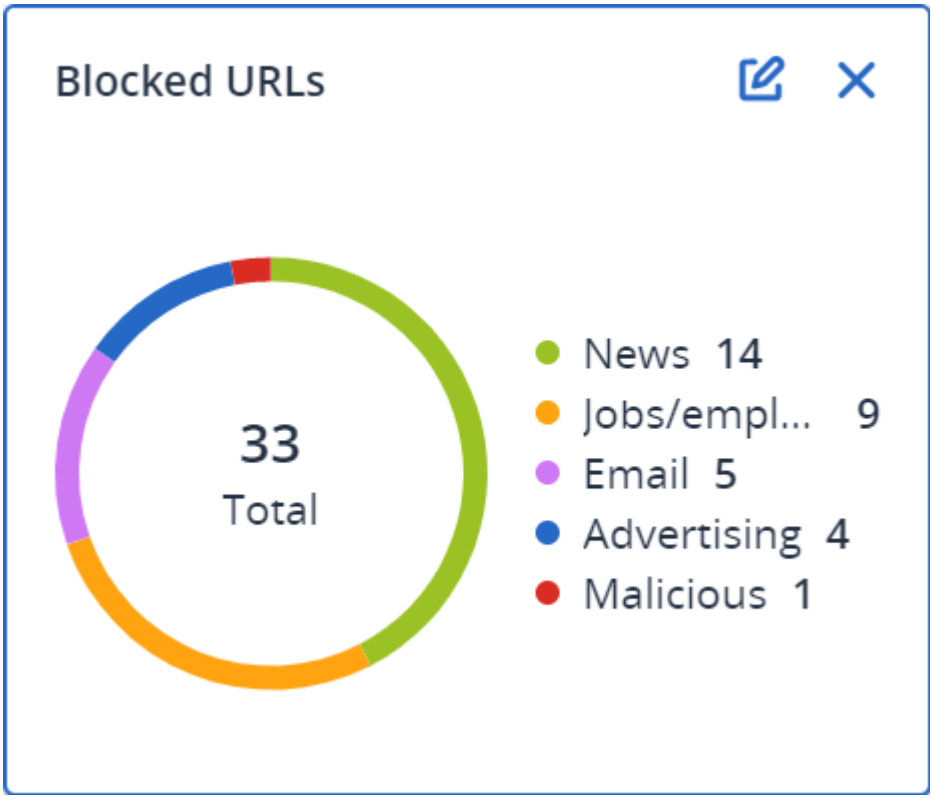
若要下載最近受影響工作負載的資料

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。

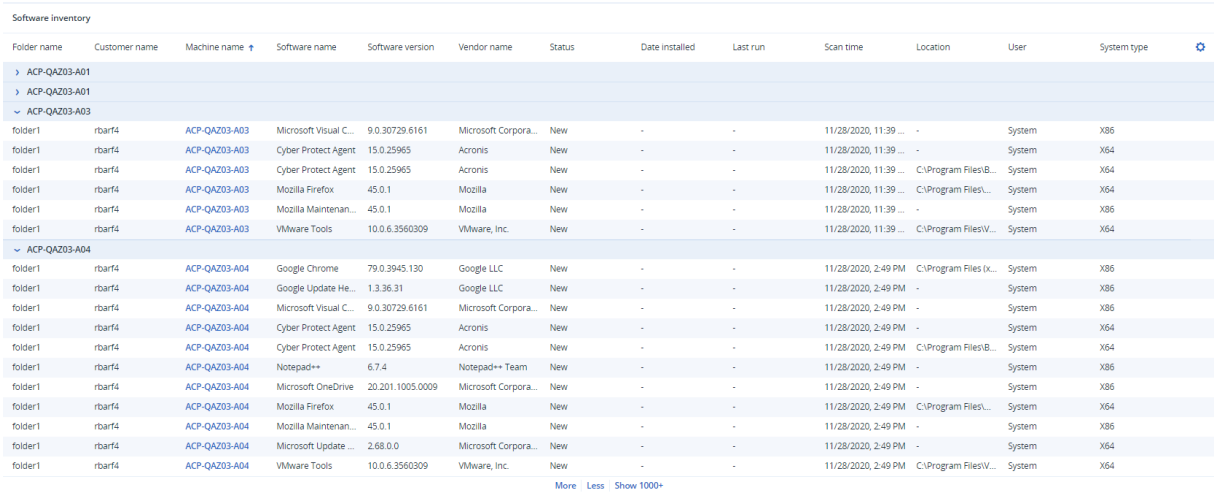
已封鎖的 URL

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

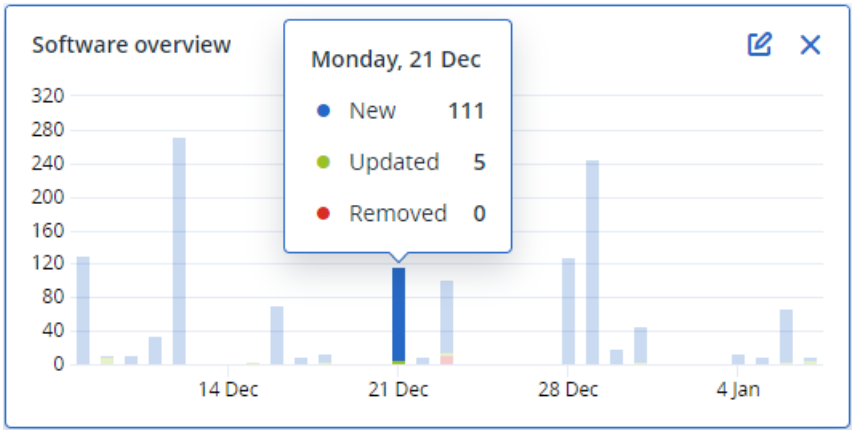
[軟體清查] 表格桌面小工具會顯示安裝在客戶組織中 Windows 和 macOS 裝置上的所有軟體的詳細資訊。


Software inventory

Folder name	Customer name	Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User	System type
ACP-QAZ03-A01												
ACP-QAZ03-A01												
ACP-QAZ03-A03												
folder1	rbarf4	ACP-QAZ03-A03	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	-	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A03	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 11:39 ...	-	System	X86
folder1	rbarf4	ACP-QAZ03-A03	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 11:39 ...	C:\Program Files\V...	System	X64
ACP-QAZ03-A04												
folder1	rbarf4	ACP-QAZ03-A04	Google Chrome	79.0.3945.130	Google LLC	New	-	-	11/28/2020, 2:49 PM	C:\Program Files (x...	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Google Update He...	1.3.36.31	Google LLC	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Visual C...	9.0.30729.6161	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Cyber Protect Agent	15.0.25965	Acronis	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\B...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Notepad++	6.7.4	Notepad++ Team	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft OneDrive	20.201.1005.0009	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Firefox	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\...	System	X64
folder1	rbarf4	ACP-QAZ03-A04	Mozilla Maintenan...	45.0.1	Mozilla	New	-	-	11/28/2020, 2:49 PM	-	System	X86
folder1	rbarf4	ACP-QAZ03-A04	Microsoft Update ...	2.68.0.0	Microsoft Corpora...	New	-	-	11/28/2020, 2:49 PM	-	System	X64
folder1	rbarf4	ACP-QAZ03-A04	VMware Tools	10.0.6.3560309	VMware, Inc.	New	-	-	11/28/2020, 2:49 PM	C:\Program Files\V...	System	X64

More | Less | Show 1000+

[軟體概觀] 桌面小工具會顯示指定的期間 (7 天、30 天或當月)，客戶組織中 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。

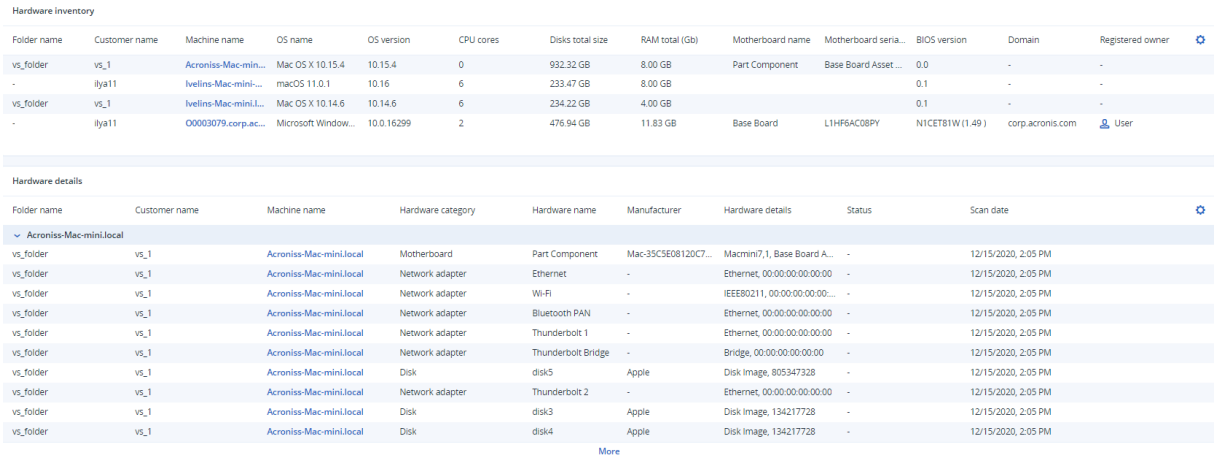
已更新 - 已更新的應用程式的數目。

已移除 - 已移除的應用程式的數目。

當您按一下對應到某個狀態那一列的部分時，就會載入快顯視窗。該視窗會列出在所選日期，其裝置的應用程式處於所選狀態的所有客戶。您可以從清單中選擇一個客戶，按一下 **[前往客戶]**，然後系統會將您重新導向至客戶的 主控台中的 **[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客戶組織中實體與虛擬 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)，客戶組織中實體與虛擬 Windows 和 macOS 裝置上新增、移除和變更的硬體的相關資訊。

Hardware changes

Folder name	Customer name	Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF							
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Windscribe.com, Ethernet...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek Semiconductor C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	Removed	(Standard disk drives), W...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	Removed	Realtek, Ethernet 802.3, C...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	Removed	Samsung, 985D7122, 4.00...	-	12/29/2020 9:35 AM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 8...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	GeForce 940MX	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Microsoft, Ethernet 802.3,...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows P...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor C...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ether...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Network adapter	New	-	Windscribe.com, Ethernet...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), W...	01/04/2021 2:37 PM
-	PK.test.Customer	DESKTOP-0FF9TTF	CPU	New	-	GenuineIntel, Intel64 Fam...	01/04/2021 2:37 PM

More | Less | Show 309

工作階段歷程記錄

該桌面小工具會顯示指定期限內在您用戶端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。

Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

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
- 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租用戶及其子租用戶中的事件。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**
  物件所屬租用戶的名稱。
- **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**
  起始端所屬租用戶的名稱。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。

報告

若要建立有關服務使用狀況和作業的報告，請按一下 **[報告]**。

用量

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。

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。
  使用狀況計量是在每個子租用戶的計費期間內計算的。如果租用戶包含在有不同計費期間的報告內，父租用戶的使用狀況可能與子租用戶使用狀況的總和不同。
- **目前使用狀況分配**
  此報告僅適用於外部佈建系統所管理的父租用戶。當子租用戶的計費期間與父租用戶的計費期間不符時，此報告相當實用。報告中包含父租用戶的目前計費期間內計算之子租用戶的服務使用狀況計量。父租用戶的使用狀況保證等於子租用戶使用狀況的總和。
- **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。
- **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之租用戶的子租用戶的服務使用狀況計量。
- **所有客戶和合作夥伴**
  報告將包含適用於您所操作之租用戶的所有子租用戶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。報告會傳送給在使用者設定中選取 **[已排程的**

使用報告] 核取方塊之租用戶的所有系統管理員。

注意事項
依日期篩選是以事件提交到雲端的時間戳記進行，而非活動開始或完成的時間。因此，如果與伺服器的連線中斷，每日報告可能會包含超過一天的資料。

啟用或停用排程報告

1. 登入管理入口網站。
2. 確認您在適用的最上層租用戶上操作。
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

此報告類型可供隨需產生，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租用戶。
3. 按一下 **[報告]** > **[使用狀況]**。
4. 選擇 **[自訂]** 索引標籤。
5. 在 **[類型]** 中，按照上述方式選擇報告類型。
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 **[詳細程度]** 中，按照上述方式選擇報告範圍。
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]**。

操作報告

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。根據預設，所有桌面小工具都會顯示您正在操作的租用戶的摘要資訊。您可以透過編輯動態小工具為每個動態小工具個別變更此項，或變更報告設定內的所有動態小工具。

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 105 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。
探索到的電腦	顯示組織網路中所有找到的電腦。
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	顯示安裝在客戶組織中 Windows 和 macOS 電腦上的所有軟體的詳細資訊。
硬體清查	顯示適用於客戶組織中實體與虛擬 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用戶端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

若要檢視報告，請按一下其名稱。

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。

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。

   您可以執行以下操作：
   - 重新命名報告。
   - 變更報告內所有桌面小工具的時間範圍。
   - 指定報告收件者以及將報告傳送給他們的時間。可用的格式為 PDF 和 XLSX。

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. 按一下省略符號圖示 (...)，然後按一下 **[刪除]**。
4. 按一下 **[刪除]**，確認您的選擇。

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，然後按一下 **[設定]**。
3. 啟用 **[排程]** 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 1000 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。
4. 按一下 **[儲存]**。

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，然後按一下 **[下載]**。
3. 選擇報告格式。

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，然後按一下 **[傳送]**。
3. 指定收件者的電子郵件地址。
4. 選擇報告格式。
5. 按一下 **[傳送]**。

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。

要傾印報告資料

您可以使用此選項，在不篩選的情況下，將自訂期間的所有資料匯出至 CSV 檔案，並將該 CSV 檔案傳送給電子郵件收件者。

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，客戶環境及其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區段，其中會顯示與用戶端對下列雲端服務的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、資料洩漏防禦、Notary、災難復原，以及 Files Sync & Share。

有數種方式可以自訂報告。

- 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，並將其傳送給客戶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。

合作夥伴系統管理員可以產生執行摘要報告，並僅將其傳送給直接客戶。若是擁有子合作夥伴的更複雜租用戶階層，子合作夥伴將必須產生報告。

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，如果客戶的 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。

桌面小工具	描述
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。 **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** - 已受到災難復原保護的伺服器總數。 **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。 選擇相關的客戶;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 (針對所選客戶)。
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]**。

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	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。

桌面小工具	描述
碼掃描	**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。
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

桌面小工具	描述
	• 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。

桌面小工具	描述
	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)。

災難復原桌面小工具

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
災難復原統計資料	此桌面小工具會針對指定的日期範圍，顯示災難復原主要效能指標。 **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。
已測試的災難復原伺服器	此桌面小工具會顯示已受到災難復原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，受災難復原保護的伺服器數目 (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，受災難復原保護的所有伺服器中，受災難復原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，受災難復原保護的所有伺服器中，受災難復原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，災難復原儲存空間的大小 (GB)。亦即，雲端伺服器備份大小的加總。
已受到災難復原保護的伺服	此桌面小工具會顯示已受到災難復原保護的伺服器以及未受保護的伺服器的相關資訊。

桌面小工具	描述
器	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，受災難復原保護的伺服器數目 (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。

桌面小工具	描述
	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直接客戶，選擇 **[傳送至所有直接客戶]**。
   - 如果您希望將報告傳送給特定客戶
     a. 清除 **[傳送至所有直接客戶]**。
     b. 按一下 **[選擇聯絡人]**。
     c. 選擇特定客戶。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 102 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 > [概觀] > [維運資訊] (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 > [概觀] > [維運資訊] (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] > [維運資訊] (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] > [維運資訊] (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] > [維運資訊] (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] > [網路保護狀態通知]	• 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
探索到的電腦	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

使用計算程式估算 Cyber Protect Cloud 成本

如果您使用的是試用版的 Cyber Protect Cloud，可以使用計算程式估算您的成本。

注意事項

只有試用版合作夥伴可以從管理入口網站存取 Cyber Protect Cloud 計算程式，試用版合作夥伴的客戶或非試用版合作夥伴則無法存取。

若要使用計算程式估算 Cyber Protect Cloud 成本

1. 按一下管理入口網站左下角的 **[計算每月成本]**。
2. 針對您預計的負載指定以下詳細資料：
   - 依工作負載類型劃分的工作負載數量。例如，指定虛擬機器、工作站、託管伺服器、Google Workplace 授權、行動裝置以及 Microsoft 365 授權的數量。
   - 資料儲存空間的詳細資料，例如資料中心的位置以及儲存數量。
3. [選擇性] 指定您打算使用的進階備份、安全性或管理選項及其各自的工作負載數量。
4. 選擇授權模型：按工作負載或按 GB。

您將會在右側看到估算的每月成本。

若要成為合作夥伴，您可以按一下對應的按鈕、與專員聊天或請求雲端顧問直接與您聯繫，全部都在自計算程式頁面上進行。

您也可以按一下管理入口網站左下角的 **[聯絡銷售人員]**，開始與銷售部門進行通訊。

使用合作夥伴入口網站

合作夥伴入口網站是針對參與 #CyberFit 合作夥伴方案的服務提供者、代理商和經銷商而設計。

您可以透過合作夥伴入口網站存取 內容、工具和訓練。

若要開始使用合作夥伴入口網站

1. 透過下列其中一種方式，存取合作夥伴入口網站：
   - 按一下管理入口網站左下角的 **[成為合作夥伴]**。
   - 瀏覽合作夥伴入口網站的網站。
2. 在合作夥伴方案中登錄您的公司。
3. 透過電子郵件接收存取詳細資料。

合作夥伴入口網站角色

合作夥伴入口網站包括多種角色，可以視需要指派給使用者。

下表描述合作夥伴入口網站中的各個可用角色，以及指派給每個角色的權限：

角色	描述
基本	預設角色已套用到所有使用者。 此角色可授予對合作夥伴入口網站基本功能的存取，包括儀表板、合作夥伴方案、內容中心、訓練和支援。
訓練	擁有此角色的使用者可以存取訓練材料。這些使用者將無法使用合作夥伴入口網站的其他功能。
行銷	此角色可對行銷專員所需的合作夥伴入口網站功能授予存取權，包括儀表板、合作夥伴方案、行銷、內容中心、訓練、支援、資料中心狀態和資料庫管理。
銷售	擁有此角色的使用者可以存取銷售專員所需的合作夥伴入口網站功能，例如儀表板、合作夥伴方案、銷售、內容中心、訓練、支援、資料中心狀態和資料庫管理。
銷售與行銷	此角色可對整合銷售行銷專員所需的合作夥伴入口網站功能授予存取權，包括儀表板、合作夥伴方案、銷售、行銷、內容中心、訓練、支援、資料中心狀態和資料庫管理。
系統管理員	系統管理員可以存取合作夥伴入口網站的所有功能，包括儀表板、合作夥伴方案、銷售、行銷、內容中心、訓練、支援、資料中心狀態和資料庫管理。此外，系統管理員可以管理合作夥伴使用者的權限以及修改公司資訊。

使用供應商入口網站

供應商入口網站 (CyberApp Standard) 是一個平台，可讓第三方軟體供應商將其產品和服務整合到 Cyber Protect Cloud 中。

透過供應商入口網站，您可以：

- 存取 Acronis 沙箱環境以進行開發和測試。
- 將您的解決方案新增到 Acronis 應用程式目錄中。
- 將工作負載、警示、小工具和報告整合到 Cyber Protect Cloud 主控台中。
- 透過業界標準措施確保資料的安全性。

若要開始使用供應商入口網站

1. 在 Acronis 技術生態系統網站上註冊。
2. 啟用您的帳戶。

進階保護套件

除了 保護 服務之外，還可以啟用進階保護套件，但需要額外付費。進階保護套件所提供的獨特功能不會與標準功能集重疊，而且還包含其他進階套件。用戶端可以透過一個、數個或所有進階套件保護其工作負載。進階保護套件適用於 保護 服務的兩種計費模式：按工作負載和按 GB。

The Advanced File Sync & Share features can be enabled with the File Sync & Share service.It is available in both billing modes - Per user and Per gigabyte.

您可以啟用下列進階保護套件：

- 進階備份

  Advanced Backup 套件包含許多不同的授權和配額，可供工作站、伺服器、虛擬機器、Web 託管伺服器、Google Workspace 授權和 Microsoft 365 授權使用。
- 進階管理
- Advanced Security + EDR (端點偵測與回應)
- 進階版資料洩漏防禦
- 進階災難復原
- 進階版 Email Security
- 進階版 File Sync & Share

注意事項
只有在啟用所擴展的功能時，才能使用進階套件。使用者在標準服務功能遭到停用時，無法使用進階功能。例如，如果 保護 功能遭到停用，使用者無法使用進階備份套件的功能。

如果啟用進階保護套件，則其功能會出現在保護計劃中，並以進階功能圖示  標示。當使用者嘗試啟用此功能時，系統會提示他們將收取額外費用。

如果未啟用進階保護套件，但追加銷售已開啟，則進階保護功能會出現在保護計劃中，但無法存取使用。此時會出現一個訊息，提示使用者聯絡系統管理員，以啟用所需的進階功能集。

如果未啟用進階保護套件且追加銷售關閉，客戶將不會在其保護計劃中看到進階功能。

Cyber Protect 服務中隨附的功能和進階套件

當您在 Cyber Protect 中啟用某個服務或功能集時，表示您啟用了預設隨附且可用的數個功能。此外，您也可以啟用進階保護套件。

下列區段包含 Cyber Protect 服務功能和進階套件的高層級概觀。如需產品的完整清單，請參閱 Cyber Protect 授權指南。

保護服務中隨附的功能和進階功能

保護服務中隨附的功能和進階功能

功能群組	隨附的標準功能	進階功能
安全性 + EDR	• #CyberFit Score • 弱點評估 • 反勒索軟體保護：Active Protection • 防毒和防惡意程式保護：雲端特徵比對檔案偵測 (無即時保護，只有排程掃描)* • 防毒和防惡意程式保護：執行前基於 AI 的檔案分析程式、基於行為的 Cyber Engine • Microsoft Defender 管理 *為偵測零時差攻擊，Cyber Protect 使用啟發式掃描規則和演算法尋找惡意命令。	Advanced Security + EDR 套件包括： • 在集中式的 [案件] 頁面中管理案件 • 將案件的範圍和影響視覺化 • 建議和修復步驟 • 使用威脅摘要對您的工作負載檢查公開披露的攻擊 • 儲存安全性事件 180 天 • 受管理的偵測與回應 (MDR) • 包含本機特徵比對偵測的防毒和防惡意程式保護 (含即時保護) • 漏洞利用防禦 • URL 篩選 • 端點防火牆管理 • 鑑識備份、惡意程式碼的掃描備份、安全復原、公司允許名單 • 智慧型保護計劃 (與 CPOC 警示整合) • 惡意程式碼的集中備份掃描 • 遠端抹除 • Microsoft Defender 防毒軟體 • Microsoft Security Essentials 如需如何啟用 Advanced Security + EDR 的相關資訊，請參閱 "啟用進階安全性 + EDR" (第 115 頁)。
資料洩漏防禦	• 裝置控制	• 內容感知透過週邊裝置和網路通訊，防止工作負載導致資料遺失 • 預先組建的自動偵測個人識別資訊 (PII)、受保護的健康資訊 (PHI) 和支付卡行業資料安全標準 (PCI DSS) 資料，以及「標記為機密」類別的文件 • 透過選擇性終端使用者協助，自動建立資料外洩防護原則 • 以自動學習為基礎的原則調整功能，執行調適性資料外洩防護 • 雲端式集中稽核記錄、警示和終端使用者通知
管理	• 工作負載的群組管理 • 保護計劃的集中管理	• 修補程式管理 • 磁碟健全狀況

功能群組	隨附的標準功能	進階功能
	• 硬體清查 • 遠端控制 • 遠端動作 • 每個技術人員的並行連線 • 遠端連線通訊協定：RDP • 四個監視器 • 基於閾值的監控	• 軟體清查 • 故障安全的修補程式 • 網路指令碼撰寫 • 遠端協助 • 檔案傳輸與共用 • 選擇要連線的工作階段 • 以多重檢視觀察工作負載 • 連線模式：控制、僅檢視和窗簾 • 透過快速協助應用程式的連線 • 遠端連線通訊協定：NEAR 與 Apple 畫面共用 • NEAR 連線的工作階段錄製 • 螢幕擷取畫面傳輸 • 工作階段歷程記錄報告 • 24 個監視器 • 基於閾值的監控 • 基於異常的監控
電子郵件安全性	無	適用於 Microsoft 365 和 Gmail 信箱的即時保護： • 反惡意程式碼與反垃圾郵件 • 電子郵件內的 URL 掃描 • DMARC 分析 • 防網路釣魚 • 模擬保護 • 附件掃描 • 消除內容的傷害力並重建 • 信任圖 請參閱設定指南。
Cyber Disaster Recovery Cloud	您可以使用 Disaster Recovery 標準功能，為您的工作負載測試災難復原案例。 注意可用的 Disaster Recovery 標準功能及其限制： • 在隔離的網路環境中測試容錯移轉。每個月限制為 32 個計算點，且同時最多 5 個測試容錯移轉作業。 • 復原伺服器設定：1 個 CPU 和 2 GB RAM、1 個 CPU 和 4 GB RAM，以及 2 個 CPU 和 8 GB RAM。	您可以啟用進階版災難復原套件，並使用完整的災難復原功能保護您的工作負載。 注意可用的 Disaster Recovery 進階功能： • 實際執行容錯移轉 • 在隔離的網路環境中測試容錯移轉。 • 適用於容錯移轉的復原點數目：建立復原伺服器後提供的所有復原點。 • 主要伺服器 • 復原/主要伺服器設定：無限制

功能群組	隨附的標準功能	進階功能
	• 可用於容錯移轉的復原點數目：僅限備份後提供的最後一個復原點。 • 可用的連線模式：僅雲端和點對站台。 • VPN 閘道的可用性：如果 VPN 閘道在上次測試容錯移轉完成後閒置 4 小時，將會暫時暫停，而且將會在您開始測試容錯移轉時，再次進行部署。 • 雲端網路數目：1. • 網際網路存取 • Runbook 的相關作業：建立和編輯。	• 可用的連線模式：僅雲端、點對站台、站台對站台 OpenVPN 以及多站台 IPsec VPN。 • VPN 閘道的可用性：一律可用。 • 雲端網路數目：23. • 公共 IP 位址 • 網際網路存取 • Runbook 的相關作業：建立、編輯和執行。

保護服務中的按用量付費功能和進階功能

保護服務中的按用量付費功能和進階功能

功能群組	按用量付費功能	進階功能
備份	• 檔案備份 • 映像備份 • 應用程式備份 • 網路共用備份 • 備份至雲端儲存空間 • 備份至本機儲存空間 **注意事項** 雲端儲存空間使用量的費用適用。	• 單鍵復原 • 連續資料保護 • Microsoft SQL Server 叢集和 Microsoft Exchange 叢集的備份支援 – Always On 可用性群組 (AAG) 和資料庫可用性群組 (DAG) • MariaDB、MySQL、Oracle DB 和 SAP HANA 的備份支援 • 資料保護圖和合規性報告 • 脫離主機資料處理 • Microsoft 365 與 Google Workspace 工作負載的備份頻率 • 可開機媒體的相關遠端作業 • 直接備份至 Microsoft Azure 公有雲端儲存
File Sync & Share	• 儲存加密檔案的內容 • 跨指定的裝置同步檔案 • 與指定的使用者和系統共用資料夾及檔案	• 公證及電子簽名 • 文件範本* *備份同步及共用檔案
實體資料運送	實體資料運送功能	不適用
Notary	• 檔案公證 • 檔案電子簽署 • 文件範本	不適用

注意事項
如果沒有啟用所擴展的標準保護功能，您就無法啟用進階保護套件。如果您停用某個功能，就會自動停用其進階套件，而且會自動撤銷使用這些進階套件的保護計劃。例如，如果您停用保護功能，就會自動停用其進階套件，而且會撤銷使用這些進階套件的所有計劃。

使用者無法使用沒有標準保護的進階保護套件，但是可以在特定的工作負載上，僅使用隨附的標準保護功能搭配進階套件。在此情況下，系統僅會針對所使用的進階套件收費。

如需計費的相關資訊，請參閱 "Cyber Protect 的計費模式" (第 8 頁)。

進階版資料洩漏防禦

[進階版資料洩漏防禦] 模組會檢查透過本機和網路通道傳輸的資料內容，並套用組織專屬的資料流程原則規則，以防止機密資訊從工作站、伺服器和虛擬機器洩漏。

開始使用 [進階版資料洩漏防禦] 模組之前，請確認您閱讀並瞭解基礎指南中所述之進階版資料洩漏防禦管理的基本概念和邏輯。

您也可以檢閱技術規格文件。

啟用進階版資料洩漏防禦

根據預設，系統已針對新租用戶，在設定中啟用 [進階版資料洩漏防禦]。如果此功能在租用戶建立期間遭到停用，則合作夥伴系統管理員之後可以再啟用。

若要啟用進階版資料洩漏防禦

1. 在 Cyber Protect Cloud 管理主控台中，導覽至 **[用戶端]**。
2. 選擇租用戶以進行編輯。
3. 在 **[選擇服務]** 區段中，捲動至 **[保護]**，然後在您套用的計費模式下，選擇 **[進階版資料洩漏防禦]**。
4. 在 [設定服務] 底下，捲動至 **[進階版資料洩漏防禦]**，然後設定配額。
   根據預設，配額設為無限制。
5. 儲存您的設定。

進階安全性 + EDR

端點偵測與回應 (EDR) 會偵測工作負載上的可疑活動 (包括未引起注意的攻擊)，並產生事件。這些事件會提供每次攻擊的逐步概觀，從而協助您瞭解攻擊是如何發生的以及如何防止它再次發生。由於攻擊的每個階段都有易於瞭解的解釋，因此調查攻擊所花的時間可以減少到幾分鐘。

啟用進階安全性 + EDR

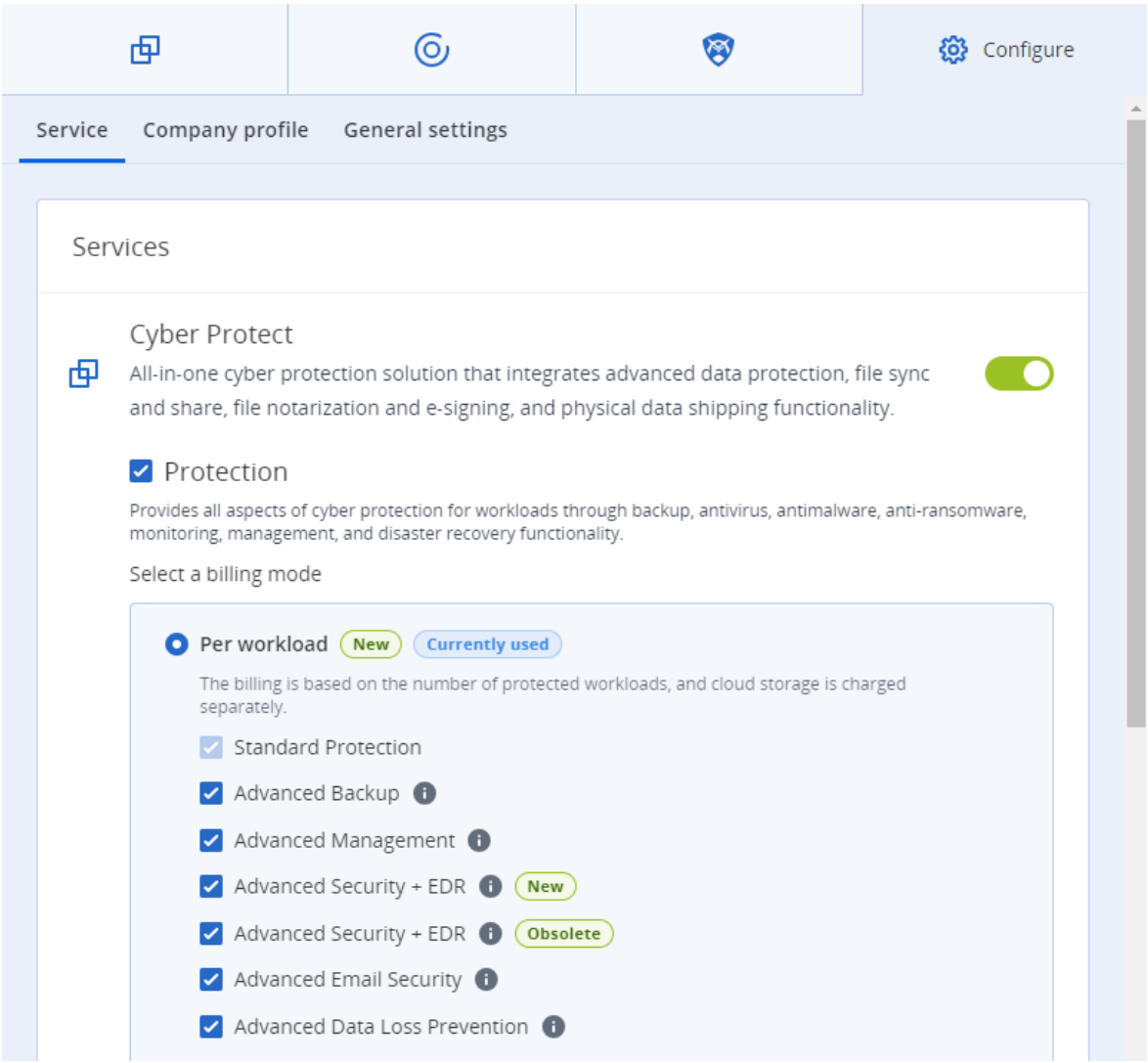
身為合作夥伴系統管理員，您可以啟用 [進階安全性 + EDR] 保護套件，以便在用戶端保護計劃中提供 [端點偵測與回應 (EDR)] 功能。

若要啟用進階安全性 + EDR 套件

1. 登入管理入口網站。

   注意事項
   如果出現提示，請選擇您要在其中套用 [進階安全性 + EDR] 保護套件的用戶端，然後按一下 **[啟用]**。

2. 在左導覽窗格中，按一下 **[用戶端]**。
3. 在 Cyber Protect 底下，按一下 **[防護]** 索引標籤。
   訂閱防護服務的現有用戶端清單隨即顯示。
4. 按一下您要在其中新增 [進階安全性 + EDR] 套件的相關用戶端。
   在 **[設定]** 索引標籤的 **[防護]** 區段下，確認已選擇 **[Advanced Security + EDR]** 核取方塊。



Managed Detection and Response (MDR)

MDR 可為沒有內部安全性專業知識或需要額外協助來調查和回應端點偵測與回應 (EDR) 偵測到的安全性事件的 MSP 提供全天候服務。

MDR 功能是在 Advanced Security + EDR 套件下的管理入口網站中啟用的，而且 MDR 服務是由外部 MDR 廠商所提供。當針對特定客戶啟用 MDR 時，MDR 廠商會針對該客戶所屬保護計劃中啟用 EDR 的工作負載，從 Acronis 接收其 EDR 事件資料。接著，MDR 廠商會執行不同層級的服務，以使用可用的回應動作，對事件進行分類。如需詳細資訊，請參閱 "什麼是受管理的偵測與回應 (MDR)？ "(第 117 頁)

如需有關使用 EDR 的詳細資訊，請參閱端點偵測與回應 (EDR)。

什麼是受管理的偵測與回應 (MDR)?

MDR 是第三方廠商提供的一種服務，其結合來自廠商和 Acronis 的熟練分析師、整合式工具、威脅情報和技術來監控並回應潛在的安全威脅和違規行為。

在管理入口網站中為客戶啟用 MDR 時，Acronis 會將 EDR 事件遙測資料轉送給 MDR 廠商，以便對這些事件進行調查和回應活動。請注意，只有 EDR 未自動緩解的事件才會轉送給 MDR 廠商。

MDR 的重要元件

MDR 由三個主要元件組成：

- 監控
- 隔離
- 回應和修復

監控

MDR 廠商會監控 EDR 偵測到，來自客戶端點的安全性警示和通知。接著，廠商會使用分析、安全性協調和回應，建立這些警示與常見威脅、威脅情報以及第三方威脅情報的關聯，並排定其優先順序。因此，廠商會判斷這些警示或通知是資料外洩還是入侵。

MDR 廠商認為可能構成潛在安全性威脅的任何安全性事件都會升級為面向客戶的安全性事件，並在 Cyber Protect 主控台中提供。廠商會針對威脅嚴重性提供背景資訊以及建議的補救措施 (包括已採取的任何動作)。

隔離

MDR 廠商分析師會利用預先定義的手冊來啟動端點隔離的回應。MDR 廠商的任何回應動作都會反映在相關的安全性事件中。隔離端點的決定取決於來自端點的資料以及來自威脅情報和威脅研究的進一步輸入。

回應和修復

回應和修復活動是在初始監控和隔離活動完成後進行的。在偵測到安全性事件後，MDR 廠商會根據安全性事件啟動回應。回應和修復活動包括：

- 根據提供的資料、情報和建議，指導如何減輕、停止或防止安全性事件。
- 分析和調查安全性事件，以確定入侵的根本原因和程度。
- 執行已核准的工作流程 (如 MDR 廠商的回應手冊中定義) 以隔離工作負載、隔離威脅或完全修復威脅。

- 引用面向客戶的安全性事件、威脅情報和建議，為服務提供者提供更詳細的安全升級。
- 透過各種管道升級事件，包括建立安全性事件、電子郵件通知和電話，上述全部透過客戶提供的聯絡方式進行。
- 與客戶保持溝通管道暢通，直到威脅獲得修補為止，並在出現新資訊時及時提供更新。
- 如果回應動作超出 MDR 服務的範圍，MDR 廠商會提供有關重點領域的建議。這可能包括對其他服務的建議，例如事件回應。

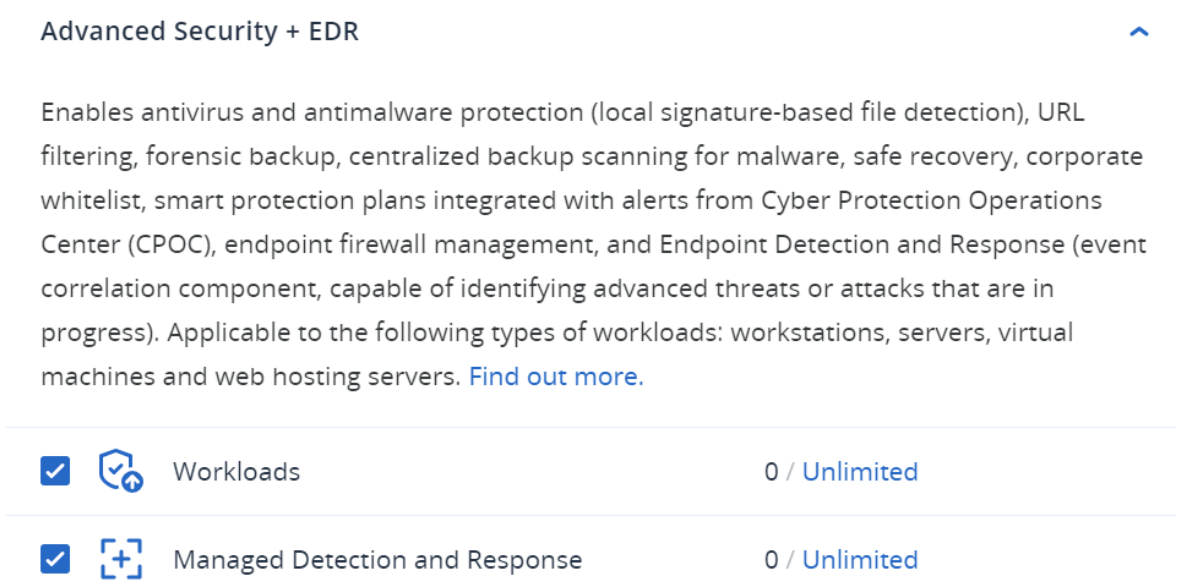
啟用受管理的偵測與回應 (MDR)

您可以執行以下兩個步驟，為所選客戶啟用 MDR：

- 步驟 1：為客戶啟用 MDR 產品項目。
- 步驟 2：設定與 MDR 廠商應用程式的整合。

若要為所選客戶啟用 MDR

1. 在管理入口網站中，前往 **[用戶端]**。
2. 按一下相關客戶旁的省略符號圖示 (...)，然後選擇 **[設定]**。
3. 在 **[保護]** 索引標籤中，按一下 **[編輯]**。
4. 在 **[Advanced Security + EDR]** 區段中，請確認已選擇 **[工作負載]** 和 **[受管理的偵測與回應]** 核取方塊。然後按一下 **[儲存]** 以套用任何變更。

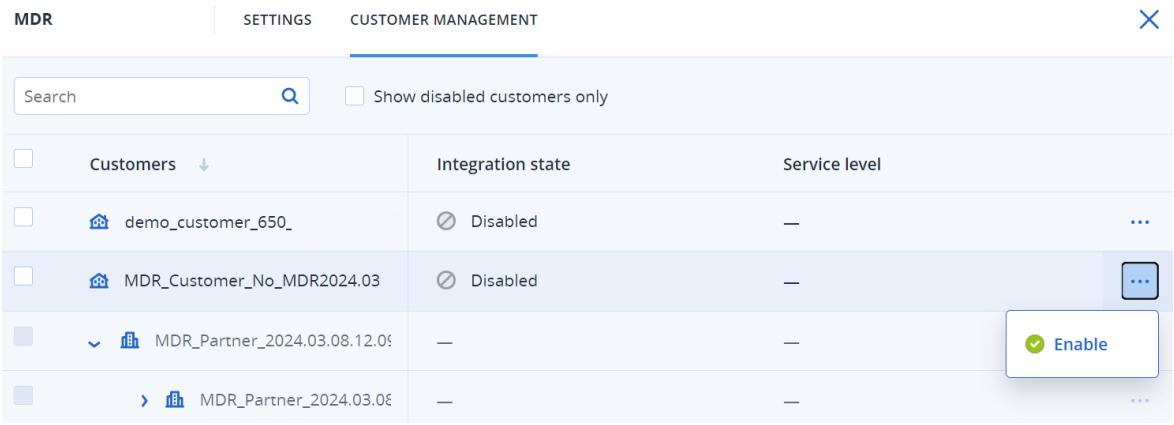


若要設定與 MDR 廠商應用程式的整合

1. 在管理入口網站中，前往 **[整合]**。
2. 使用搜尋列找到 MDR 廠商的應用程式。
3. 在顯示的 MDR 目錄卡片中，按一下 **[設定]**。
4. 在 **[設定]** 索引標籤中，按一下鉛筆圖示，並輸入至少一個合作夥伴聯絡人的聯絡人詳細資料。當偵測到安全性事件時，MDR 廠商將聯絡此聯絡人。請注意，您最多可以新增三個聯絡人的詳細資料。完成後，按一下 **[啟用]**。

偵測到安全性事件時，廠商會致電每個聯絡人六次，然後再轉至下一個聯絡人。通話後，或在沒有聯絡的情況下，廠商會向所有聯絡人傳送電子郵件，概述呈報內容和事件。

5. 在 **[客戶管理]** 索引標籤中，按一下相關客戶最右欄中的省略符號圖示 (...)，然後按一下 **[啟用]**。



若要啟用多個客戶，請選擇相關客戶旁的核取方塊，然後按一下 **[客戶管理]** 索引標籤左上角的 **[啟用]**。

6. 從顯示的對話方塊的 **[服務層級]** 下拉式清單中，選擇要套用到所選客戶的 MDR 服務的層級：
   - **標準**：包括全天候監控客戶端點以擷取攻擊、將由 AI 提供技術支援的事件分類並排定優先順序、遏制並隔離受影響端點的威脅，以及即時掌握主控台內排定優先順序的事件清單。
   - **進階**：除了**標準**中包含的功能外，此層級還可以進行完整修復，包括攻擊復原、安全性漏洞復原和消除。
7. 按一下 **[啟用]** 以完成 MDR 整合。

   如果已啟用 IP 允許名單功能 (請參閱 "限制 Web 介面的存取權" (第 26 頁))，系統會提示您將 MDR 廠商的 IP 新增至允許名單。如此可確保廠商可以監控相關的工作負載。按一下 **[啟用]** 以確認。

   MDR 現已啟用，而且 EDR 安全性事件將轉送給 MDR 廠商以進行調查和回應活動。如需有關 MDR 服務的進一步資訊，請參閱 "什麼是受管理的偵測與回應 (MDR)？" (第 117 頁)

停用受管理的偵測與回應 (MDR)

您可以在產品項目層級停用 MDR。您也可以在 MDR 廠商的整合應用程式中，為個別客戶停用 MDR。

若要停用 MDR 產品項目

1. 在管理入口網站中，前往 **[用戶端]**。
2. 按一下相關客戶旁的省略符號圖示 (...)，然後選擇 **[設定]**。
3. 在 **[保護]** 索引標籤中，按一下 **[編輯]**。
4. 在 **[Advanced Security + EDR]** 區段中，請確認未選擇 **[工作負載]** 和 **[受管理的偵測與回應]** 核取方塊。然後按一下 **[儲存]** 以套用您的變更。

   或者，您可以在 **[設定]** 索引標籤中停用 **[Advanced Security + EDR]** 服務，如此就會自動停用 MDR。

若要在 MDR 廠商的整合應用程式中為個別客戶停用 MDR

1. 在管理入口網站中，前往 **[整合]**。
2. 搜尋相關的 MDR 廠商應用程式。
3. 在顯示的 MDR 目錄卡片中，按一下 **[設定]**。
4. 在 **[客戶管理]** 索引標籤中，按一下相關客戶最右欄中的省略符號圖示 (...)，然後選擇 **[停用]**。
   若要停用多個客戶，請選擇每個客戶左側的核取方塊，然後按一下 **[客戶管理]** 索引標籤左上角的 **[停用]**。

受管理的偵測與回應 (MDR) 中可用的回應動作

MDR 包含許多可以在事件層級套用的回應動作。

回應動作由 MDR 安全分析師執行，他們會透過存取 Cyber Protect 主控台或執行 API 呼叫，套用相關的動作。這些分析師會以 **[安全分析師]** 角色登入 Cyber Protect 主控台。

所有回應動作都記錄在 **[活動]** 清單中。客戶可以檢視已執行的回應動作活動的清單以及這些活動的狀態 (進行中/成功/失敗)。在 **[啟動者]** 欄位中，會顯示啟動動作的使用者 (無論是合作夥伴使用者、客戶使用者還是 MDR 安全分析師)。如需詳細資訊，請參閱如何使用端點偵測與回應 (EDR)。

注意事項
下表列出的回應動作包括對端點偵測與回應 (EDR) 文件中相關章節的引用。

回應動作	其他資訊
變更調查狀態	狀態可以設定為以下任一項： • **正在調查** • **已結束** • **誤報** 如需有關變更調查狀態的詳細資訊，請參閱如何調查網路攻擊鏈中的事件。
網路隔離	MDR 安全分析師可以： • 隔離工作負載 • 取消隔離工作負載 • 檢查隔離狀態 如需有關隔離工作負載的詳細資訊，請參閱管理工作負載的網路隔離。
新增留言	MDR 安全分析師可以透過在事件的網路攻擊鏈中按一下 **[張貼留言]** 來新增對該事件的留言。這些留言會顯示在特定事件的 **[活動]** 索引標籤中。如需詳細資訊，請參閱瞭解為緩解事件所採取的動作。
停止程序/程序樹狀結構	此動作可以套用到整個事件。即使事件的程序已停止，還是可以觸發回應動作。

回應動作	其他資訊
	非同步回應會在處理回應動作後傳送。回應可以是以下其中之一： • 成功：已成功停止所有程序。 • 成功，但有警告：已成功停止部分程序或沒有程序可停止 (或在 MDR 之外停止)。 • 錯誤：未停止任何程序。 如需有關停止程序或程序樹狀結構的詳細資訊，請參閱定義可疑程序的回應動作。
隔離	此動作可以套用到整個事件。即使已隔離檔案或程序，還是可以觸發回應動作。 非同步回應會在處理回應動作後傳送。回應可以是以下其中之一： • 成功：已成功隔離所有檔案和程序。 • 成功，但有警告：已成功隔離部分檔案和程序，或沒有檔案或程序可隔離 (或在 MDR 之外隔離)。 • 錯誤：未隔離任何檔案或程序。 如需有關隔離程序的詳細資訊，請參閱定義可疑程序的回應動作。如需有關隔離檔案的詳細資訊，請參閱定義可疑檔案的回應動作。
刪除檔案	此動作可以套用到整個事件。即使已刪除檔案，還是可以觸發回應動作。 非同步回應會在處理回應動作後傳送。回應可以是以下其中之一： • 成功：已成功刪除所有檔案。 • 成功，但有警告：已成功刪除部分檔案或沒有檔案可刪除 (或在 MDR 之外刪除)。 • 錯誤：未刪除任何檔案。 如需有關刪除檔案的詳細資訊，請參閱定義可疑檔案的回應動作。
重新啟動工作負載	在重新啟動工作負載或立即重新啟動之前，啟用時間間隔的設定。 如需有關重新啟動工作負載的詳細資訊，請參閱重新啟動工作負載。
將 URL、檔案或程序新增至允許名單/封鎖名單	將 URL、檔案或程序新增至預設計劃(目前指派給工作負載的計劃) 上的允許名單/封鎖名單。

回應動作	其他資訊
	非同步回應會在處理回應動作後傳送。回應可以是以下其中之一： • 成功：已成功新增所有 URL、文件和程序。 • 成功，但有警告：已成功新增部分 URL、檔案和程序，有些則未成功 (例如，它們可能已包含在允許名單中)。 • 錯誤：動作失敗。 如需有關將 URL、檔案或程序新增到允許名單和封鎖名單的詳細資訊，請參閱將程序、檔案或網路新增至保護計劃封鎖名單或允許名單。

進階災難復原

您可以啟用進階版災難復原套件，並使用完整的災難復原功能保護您的工作負載。

下列進階版災難復原功能可供使用：

- 實際執行容錯移轉
- 在隔離的網路環境中測試容錯移轉。
- 適用於容錯移轉的復原點數目：建立復原伺服器後提供的所有復原點。
- 主要伺服器
- 復原/主要伺服器設定：無限制
- 可用的連線模式：僅雲端、點對站台、站台對站台 OpenVPN 以及多站台 IPsec VPN。
- VPN 閘道的可用性：一律可用。
- 雲端網路數目：23.
- 公共 IP 位址
- 網際網路存取
- Runbook 的相關作業：建立、編輯和執行。

進階版 Email Security

Advanced Email Security 套件可為 Microsoft 365、Google Workspace 或 Open-Xchange 信箱提供即時保護：

- 反惡意程式碼和防垃圾郵件
- 電子郵件內的 URL 掃描
- DMARC 分析
- 防網路釣魚
- 模擬保護
- 附件掃描

- 消除內容的傷害力並重建
- 信任圖

您也可以啟用 Microsoft 365 協同作業應用程式授權，如此可保護 Microsoft 365 雲端協同作業應用程式免受內容傳播的安全性威脅。這些應用程式包括 OneDrive、SharePoint 和 Teams。

Advanced Email Security 可以按工作負載或按 GB 啟用，而且將影響您的授權模型。

在Advanced Email Security 規格書中深入瞭解Advanced Email Security。

如需設定指示，請參閱採用 Perception Point 技術的Advanced Email Security。

進階備份

您可以啟用進階備份套件，並使用進階備份和復原功能保護您的工作負載。

下列功能可供使用：

- 單鍵復原
- 連續資料保護
- Microsoft SQL Server 叢集和 Microsoft Exchange 叢集的備份支援 – Always On 可用性群組 (AAG) 和資料庫可用性群組 (DAG)
- MariaDB、MySQL、Oracle DB 和 SAP HANA 的備份支援
- 資料保護圖和合規性報告
- 脫離主機資料處理
- Microsoft 365 與 Google Workspace 工作負載的備份頻率
- 可開機媒體的相關遠端作業
- 直接備份至 Microsoft Azure 公有雲端儲存

進階管理

您可以透過進階管理，建置可防止發生大多數問題的快速、主動且反應迅速的管理基礎架構。

進階管理套件包含下列功能：

- **軟體清查** - 查看用戶端所使用軟體的完整清單，並在準備、規劃或追蹤更新時節省時間和精力。
- **自動管理修補程式** - 在弱點遭到利用之前修復。
- **故障安全修補** - 在修補前執行自動備份系統，快速且輕鬆地從故障的修補程式復原工作負載。
- **根據機器學習進行監控和智慧型警示** - 利用預測性監控和警示，緩解操作風險並將監控工作最佳化。
- **現成可用的網路指令碼編寫** - 自動執行並簡化例行工作。
- **磁碟機健康監控** - 使用預測性監控和警示，並主動緩解磁碟機故障所造成的停機時間。
- **遠端桌面與遠端協助** - 存取遠端工作負載並快速解決技術問題。即使在頻寬有限的情況下，也可以透過卓越的效能，節省時間並提供可靠的支援。此功能包含更好的平台覆蓋範圍 (Windows、macOS 和 Linux)，以及工作階段錄製、遠端動作、檔案傳輸、監控、報告並以多重檢視觀察工作負載等擴充功能。

整合

與第三方系統的整合

服務提供者可以將 Cyber Protect Cloud 與第三方系統整合在一起，如下所示：

- 透過在此系統中設定平台擴充功能。

  管理入口網站的 **[整合]** 頁面會列出可用於最常用專業服務自動化 (PSA) 與遠端監控和管理 (RMM) 系統的擴充功能。

  這是建議的整合平台方式。
- 透過建立系統的 API 用戶端，從而使系統能夠存取平台及其服務的應用程式開發介面 (API)。API 用戶端是平台 OAuth 2.0 授權架構的一部分。如需有關 OAuth 2.0 的詳細資訊，請參閱 https://tools.ietf.org/html/rfc6749。

  這是低階的整合平台方式，需要程式設計技巧。當系統沒有平台擴充功能，或系統是針對管理可用擴充功能未涵蓋之平台及其服務的這類情況而自訂，則建議使用這種方式。

設定 Cyber Protect Cloud 的整合

1. 登入管理入口網站。
2. 在主導覽功能表中，前往 **[整合]**。
3. 按一下您想要啟用整合之第三方系統的名稱。
4. 依照畫面上的說明操作。

請尋找有關與第三方系統的可用整合的詳細資訊，包括 https://solutions.acronis.com 上的逐步文件。

管理 API 用戶端

使用其應用程式開發介面 (API) 可以將第三方系統與 Cyber Protect Cloud 整合在一起。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。

什麼是 API 用戶端？

API 用戶端是一個特殊的平台帳戶，旨在代表需要驗證並獲授權存取平台及其服務之 API 中資料的第三方系統。

用戶端的存取限制為租用戶，系統管理員會在其中建立用戶端及其子租用戶。

建立時，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。

用戶端認證由唯一識別碼 (ID) 和密碼值所組成。這些認證不會過期，而且無法用於登入管理入口網站或任何服務主控台。密碼值則可以重設。

您無法為用戶端啟用雙重驗證機制。

一般整合程序

1. 系統管理員會在第三方系統將管理的租用戶中建立一個 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。

   根據此流程，在透過 API 存取租用戶及其服務之前，系統應該先使用授權 API，將已建立之用戶端的認證傳送到平台。此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。接著，系統必須將此權杖新增至所有 API 要求。

   安全性權杖不需要傳遞具有 API 要求的用戶端認證。為提高安全性，權杖將在兩小時後過期。這段時間之後，具有過期權杖的所有 API 要求都將失敗，而且系統將需要向平台要求一個新的權杖。

如需有關使用授權和平台 API 的詳細資訊，請參閱開發人員指南，網址是：https://developer.acronis.com/doc/account-management/v2/guide/index。

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，只能重設。
6. 按一下 **[完成]**。

重設 API 用戶端的密碼值

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]**，確認您的決定。

   系統將會產生一個新密碼值。用戶端 ID 和資料中心 URL 將不會變更。

   指派給此用戶端的所有安全性權杖將會立即變成過期，而且具有這些權杖的 API 要求將會失敗。
6. 複製並儲存用戶端的新密碼值。

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，只能重設。

7. 按一下**[完成]**。

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。

   用戶端的狀態將會變更為 **[已停用]**。

   指派給此用戶端，且具有安全性權杖的 API 要求將會失敗，但是權杖將不會立即變成過期。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用戶端。

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]**。

   用戶端的狀態將會變更為 **[作用中]**。

   如果安全性權杖尚未過期，指派給此用戶端，且具有這些權杖的 API 要求將會成功。

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。

   指派給此用戶端的所有安全性權杖將會立即變成過期，而且具有這些權杖的 API 要求將會失敗。

重要事項

您無法復原已刪除的用戶端。

整合參照

您可以在 [整合目錄] 中找到任何整合的文件。

若要找出所需的文件

1. 請造訪 https://solutions.acronis.com。
2. 選擇您需要的整合，然後按一下 **[深入瞭解]**。
   您將會在頁面頂端找到指南或操作說明文章的連結。

或者，您可以在 https://www.acronis.com/support/documentation/ 的 **[整合參考資料]** 下，找到 Acronis 開發的最新整合文件。

與 VMware Cloud Director 整合

服務提供者可以將 VMware Cloud Director (前身為 VMware vCloud Director) 與 Cyber Protect Cloud 整合在一起，並為其客戶提供適用於其虛擬機器的現成可用的備份解決方案。

整合包括下列步驟：

1. 為 VMware Cloud Director 環境設定 RabbitMQ 訊息代理程式。
   RabbitMQ 提供單一登入 (SSO) 功能，因此您可以使用 VMware Cloud Director 認證登入 Cyber Protect 主控台。
   在 Cyber Protect Cloud 23.05 版 (2023 年 5 月發行) 及較舊版本中，RabbitMQ 也用於將 VMware Cloud Director 環境中的變更同步到 Cyber Protect Cloud。
2. 部署管理代理程式。
   在部署管理代理程式期間，也會安裝 VMware Cloud Director 的外掛程式。此外掛程式會將 Cyber Protection 新增至 VMware Cloud Director 使用者介面。
   管理代理程式會將 VMware Cloud Director 組織對應到 Cyber Protect Cloud 中的客戶租用戶，並將組織系統管理員對應至客戶租用戶系統管理員。如需有關組織的詳細資訊，請參閱 VMware 知識庫中的在 VMware Cloud Director 中建立組織。
   客戶租用戶是在設定 VMware Cloud Director 整合所在合作夥伴租用戶中建立的。這些新的客戶租用戶處於 **[已鎖定]** 模式，而且合作夥伴系統管理員無法在 Cyber Protect Cloud 中加以管理。

   注意事項
   在 VMware Cloud Director 中，只有擁有唯一電子郵件地址的組織系統管理員會對應到 Cyber Protect Cloud。
3. 部署一或多個備份代理程式。
   備份代理程式會針對 VMware Cloud Director 環境中的虛擬機器，提供備份與復原功能。

若要停用 VMware Cloud Director 和 Cyber Protect Cloud 之間的整合，請聯絡技術支援。

限制

- 與 VMware Cloud Director 整合僅適用於 **[由服務提供者管理]** 管理模式下，其父租用戶 (如果有的話) 也使用 **[由服務提供者管理]** 管理模式的合作夥伴租用戶。如需有關租用戶類型及其管理模式的詳細資訊，請參閱 "建立租用戶" (第 31 頁)。

  所有現有的直接合作夥伴都可以設定與 VMware Cloud Director 整合。合作夥伴系統管理員也可以為子租用戶啟用此選項，方法是，建立子合作夥伴租用戶時，選擇 **[合作夥伴擁有的 VMware Cloud Director 基礎架構]** 核取方塊。
- 設定與 VMware Cloud Director 整合所在的合作夥伴租用戶必須停用雙重驗證機制。
- 在多個 VMware Cloud Director 組織中擁有 [組織系統管理員] 角色的系統管理員僅能為 Cyber Protection 中的一個客戶租用戶管理備份和復原。
- Cyber Protect 主控台隨即在新的索引標籤中開啟。

軟體需求

支援的 VMware Cloud Director 版本

- VMware Cloud Director 10.4, 10.5

支援的網頁瀏覽器

- 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。

設定 RabbitMQ 訊息代理程式

此程序依 Cyber Protect Cloud 的版本而定。簡化版本用於 23.06 版 (2023 年 6 月發行) 及更新版本。

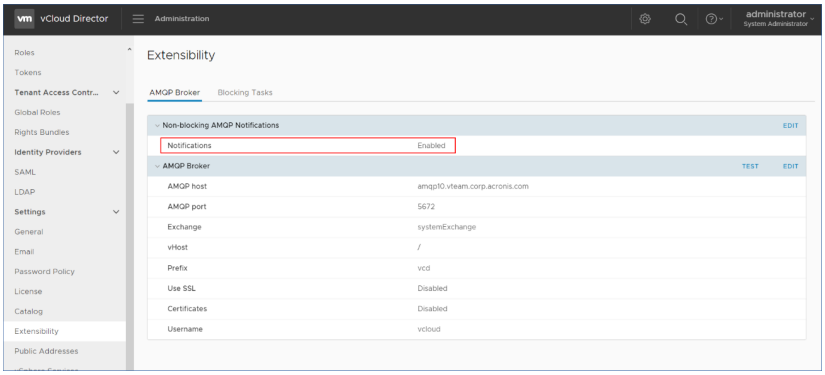
若要設定 RabbitMQ 訊息代理程式

適用於 23.06 版及更新版本

1. 安裝適用於您 VMware Cloud Director 環境的 RabbitMQ AMQP 代理程式。

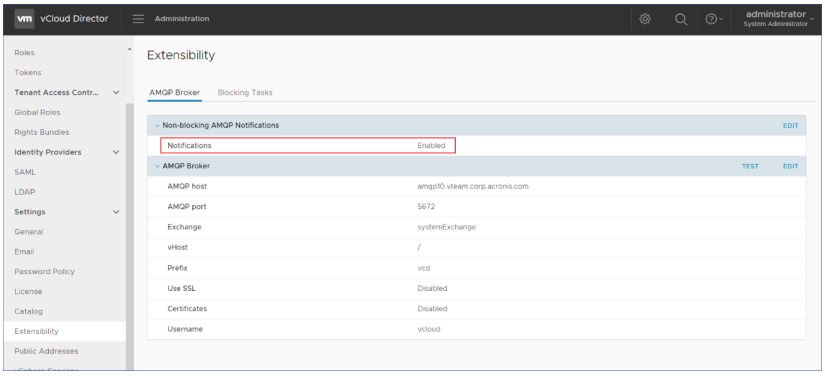
   如需有關如何安裝 RabbitMQ 的詳細資訊，請參閱 VMware 文件：安裝並設定 RabbitMQ AMQP 代理程式。
2. 以系統管理員身分，登入 VMware Cloud Director 提供者入口網站。

3. 移至 **[系統管理]** > **[擴充性]**，然後確認已在 **[非封鎖 AMQP 通知]** 底下啟用 **[通知]**。

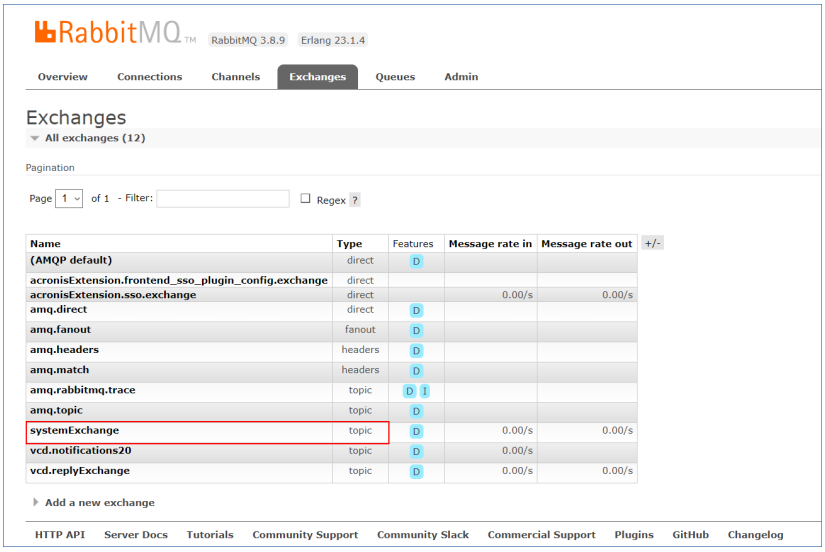


適用於 23.05 版及更新版本

1. 安裝適用於您 VMware Cloud Director 環境的 RabbitMQ AMQP 代理程式。
   如需有關如何安裝 RabbitMQ 的詳細資訊，請參閱 VMware 文件：安裝並設定 RabbitMQ AMQP 代理程式。
2. 以系統管理員身分，登入 VMware Cloud Director 提供者入口網站。
3. 移至 **[系統管理]** > **[擴充性]**，然後確認已在 **[非封鎖 AMQP 通知]** 底下啟用 **[通知]**。



4. 以系統管理員身分，登入 RabbitMQ 管理主控台。
5. 在 **[交換]** 索引標籤上，確認已建立交換 (名稱預設為 **SystemExchange**)，且其類型為**主題**。



安裝並發佈 VMware Cloud Director 的外掛程式

當您安裝管理代理程式時，將自動安裝 VMware Cloud Director 的外掛程式。

但是，您需要將外掛程式手動發佈到將使用 Cyber Protection 的租用戶。

若要發佈 VMware Cloud Director 的外掛程式

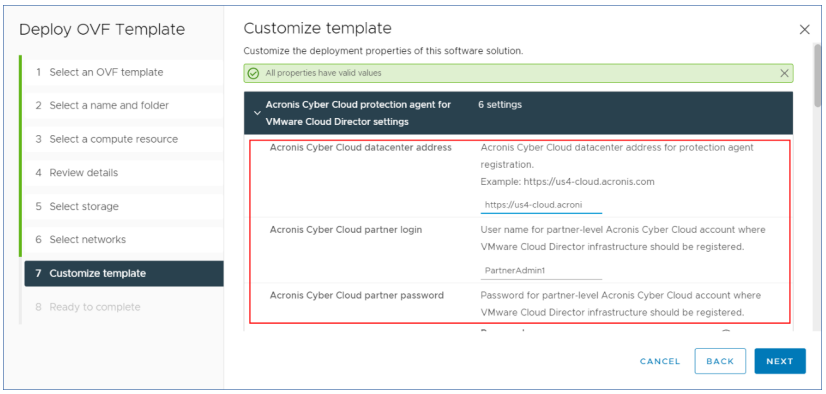
1. 以系統管理員身分，登入 VMware Cloud Director 提供者入口網站。
2. 從導覽功能表中，選擇 **[自訂入口網站]**。
3. 在 **[外掛程式]** 索引標籤上，選擇 **Cyber Protection** 外掛程式，然後按一下 **[發佈]**。
4. 設定發佈範圍：
   a. 在 **[範圍]** 區段中，僅選擇 **[租用戶]** 核取方塊。
   b. 在 **[發佈至]** 區段中，選擇 **[所有租用戶]** 以便為所有現有和之後的租用戶啟用外掛程式，或選擇您想要為其啟用外掛程式的個別租用戶。
5. 按一下 **[儲存]**。
6. 按一下 **[信任]**。

安裝管理代理程式

1. 以合作夥伴系統管理員的身分，登入 Cyber Protect Cloud 管理入口網站。
2. 前往 **[設定]** > **[位置]**，然後按一下 **[新增 VMware Cloud Director]**。
3. 從 **[發行通道]** 下拉式清單中，選擇代理程式的版本。您可以選取下列選項：
   - **目前** – 這是最新版本。
   - **穩定** - 這是先前發行的版本。
4. 按一下 **[管理代理程式]** 連結，並下載 ZIP 檔案。
5. 解壓縮管理代理程式範本檔案 `vCDManagementAgent.ovf` 以及虛擬硬碟檔案 `vCDManagementAgent-disk1.vmdk`。
6. 在 vSphere Client 中，將管理代理程式 OVF 範本部署到 VMware Cloud Director 管理的 vCenter 執行個體底下的 ESXi 主機。

   重要事項
   每個 VMware Cloud Director 環境僅能安裝一個管理代理程式。

7. 在 **[部署 OVF 範本]** 精靈中，進行下列設定以設定管理代理程式：



a. Cyber Protect Cloud 資料中心的 URL。例如，`https://us5-cloud.example.com`。

b. 合作夥伴系統管理員登入和密碼。

c. VMware Cloud Director 環境中，虛擬機器備份儲存空間的 ID。此備份儲存空間可以是僅合作夥伴擁有的。如需有關儲存空間的詳細資訊，請參閱 "管理位置和儲存空間" (第 60 頁)。

   若要檢查 ID，請在管理入口網站中，前往 **[設定]** > **[位置]**，然後選擇所需的儲存空間。您可以在 URL 中的 **uuid=** 部分後面看到其 ID。

d. Cyber Protect Cloud 計費模式：**[按 GB]** 或 **[按工作負載]**。

   注意事項
   所選計費模式適用於將建立的所有新客戶租用戶。

e. VMware Cloud Director 參數：基礎架構位址、系統管理員登入和密碼。

f. RabbitMQ 參數：系統管理員登入和密碼。

g. 具有代理程式的虛擬裝置上，root 使用者的密碼。

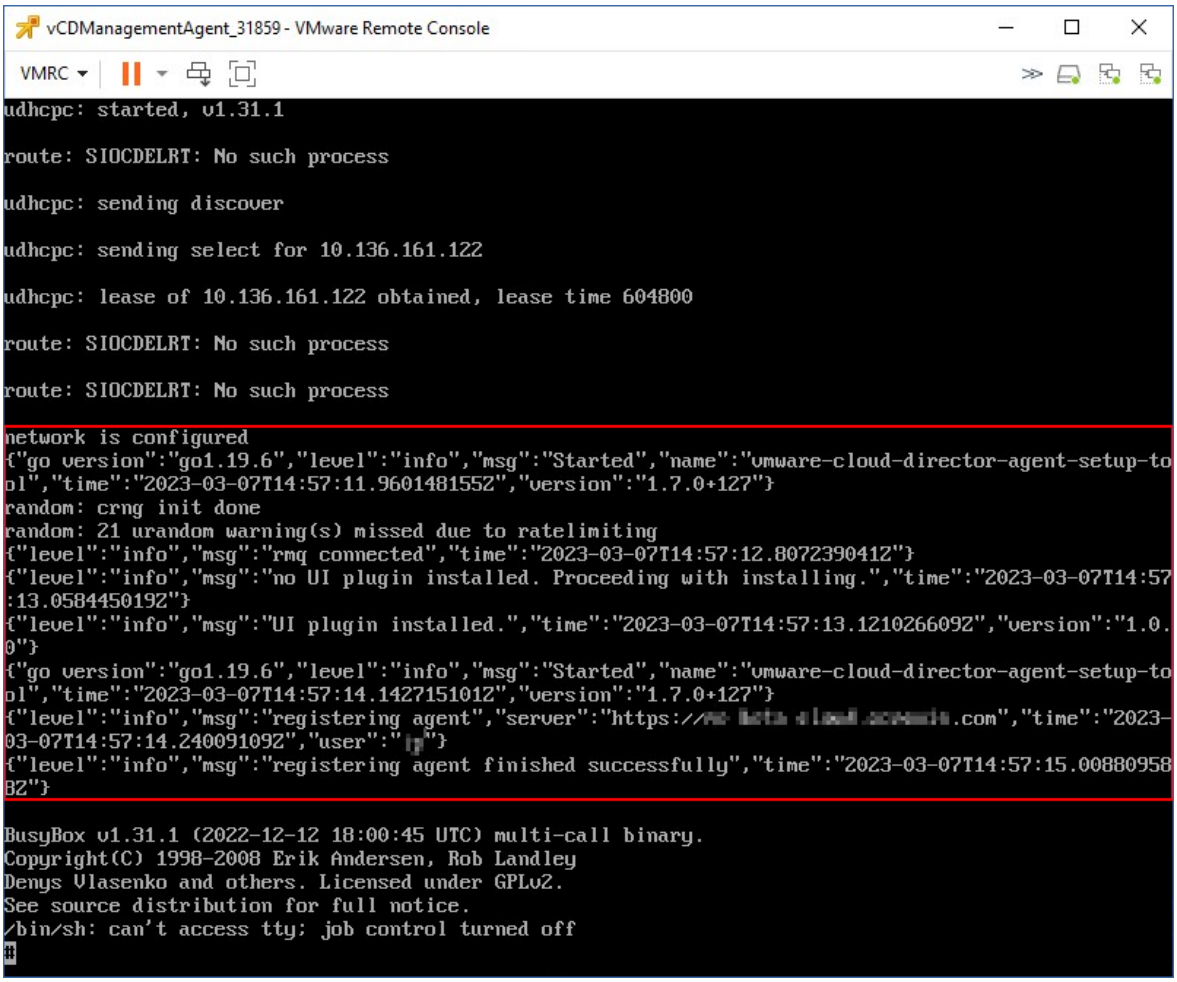
h. 網路參數：IP 位址、子網路遮罩、預設閘道、DNS、DNS 尾碼。

   預設只會啟用一個網路介面。若要啟用另一個網路介面，請選擇 **[啟用 eth1]** 旁的核取方塊。

   注意事項
   請確認您的網路設定允許管理代理程式存取 VMware Cloud Director 環境和您的 Cyber Protect Cloud 資料中心。

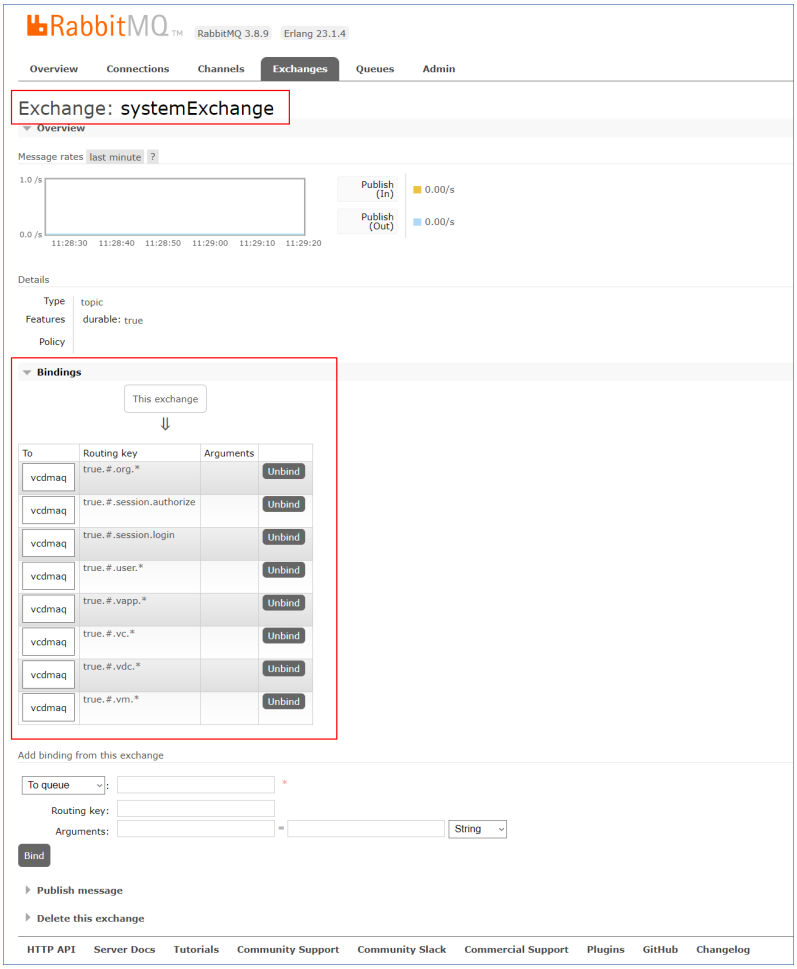
您也可以在初始部署之後，設定管理代理程式設定。在 vSphere Client 中，關閉裝有管理代理程式的虛擬機器，然後按一下 **[設定]** > **[設定]** > **[vApp 選項]**。套用所需的設定，然後開啟裝有管理代理程式的虛擬機器。

8. [選用] 在 vSphere Client 中，開啟裝有管理代理程式的虛擬機器的主控台，然後驗證您的設定。



9. 驗證 RabbitMQ 連線。
   a. 以系統管理員身分，登入 RabbitMQ 管理主控台。
   b. 在 **[交換]** 索引標籤中，選擇您在 RabbitMQ 安裝期間設定的交換。根據預設，其名稱為 **systemExchange**。

c. 驗證與 **vcdmaq** 佇列的繫結。



安裝備份代理程式

1. 以合作夥伴系統管理員的身分，登入管理入口網站。
2. 前往 **[設定]** > **[位置]**，然後按一下 **[新增 VMware Cloud Director]**。
3. 從 **[發行通道]** 下拉式清單中，選擇代理程式的版本。您可以選取下列選項：
   - **目前** – 這是最新版本。
   - **穩定** - 這是先前發行的版本。
4. 按一下 **[備份代理程式]** 連結，並下載 ZIP 檔案。
5. 解壓縮備份代理程式範本檔案 `vCDCyberProtectAgent.ovf` 以及虛擬硬碟檔案 `vCDCyberProtectAgent-disk1.vmdk`。
6. 在 vSphere Client 中，將備份代理程式範本部署到所需的 ESXi 主機。

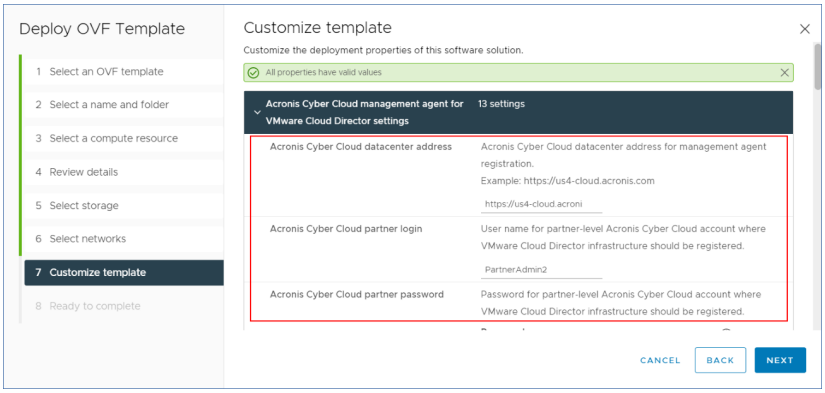
   每個主機至少需要一個備份代理程式。根據預設，備份代理程式獲指派 8 GB 的 RAM 和 2 個 CPU，而且可以同時處理最多 5 個備份或復原工作。

   若要處理更多工作或分配備份和復原流量，請將其他代理程式部署到相同的主機。或者，為避免與記憶體不足相關的失敗，建議您將 16 GB 的 RAM 和 4 個 vCPU 指派到現有的代理程式。

注意事項

在未安裝備份代理程式的 ESXi 主機上備份虛擬機器將會失敗，並出現「工作逾時已過期」錯誤。

7. 在 **[部署 OVF 範本]** 精靈中，進行下列設定以設定備份代理程式：



a. Cyber Protect Cloud 資料中心的 URL。例如，`https://us5-cloud.example.com`。

b. 合作夥伴系統管理員登入和密碼。

c. VMware vCenter 參數：伺服器位址、登入和密碼。

代理程式將使用這些認證連線到 vCenter Server。建議您使用已獲指派 **[系統管理員]** 角色的帳戶。否則，請在 vCenter Server 上提供具備所需權限的帳戶。

d. 具有代理程式的虛擬裝置上，root 使用者的密碼。

e. 網路參數：IP 位址、子網路遮罩、預設閘道、DNS、DNS 尾碼。

預設只會啟用一個網路介面。若要啟用另一個網路介面，請選擇 **[啟用 eth1]** 旁的核取方塊。

注意事項

確認您的網路設定將允許備份代理程式存取 vCenter Server 和您的 Cyber Protect Cloud 資料中心。

f. 下載限制：下載速率上限 (Kbps)，可定義復原作業期間的備份存檔讀取速度。預設值為 0 - 無限制。

g. 上傳限制：上傳速率上限 (Kbps)，可定義備份作業期間的備份存檔寫入速度。預設值為 0 - 無限制。

您也可以在初始部署之後，設定備份代理程式設定參數。在 vSphere Client 中，關閉裝有備份代理程式的虛擬機器，然後按一下 **[設定]** > **[設定]** > **[vApp 選項]**。套用所需的設定，然後開啟裝有備份代理程式的虛擬機器。

8. 在 vSphere Client 中，請確認已為裝有備份代理程式的虛擬機器啟用 **[主機]** 和 **[Storage vMotion]**。

更新代理程式

若要更新管理代理程式

1. 以合作夥伴系統管理員的身分，登入 Cyber Protect Cloud 管理入口網站。
2. 前往 **[設定]** > **[位置]**，然後按一下 **[新增 VMware Cloud Director]**。

3. 按一下 **[管理代理程式]** 連結，然後下載包含最新代理程式的 ZIP 檔案。
4. 解壓縮管理代理程式範本檔案 `vCDManagementAgent.ovf` 以及虛擬硬碟檔案 `vCDManagementAgent-disk1.vmdk`。
5. 在 vSphere Client 中，關閉裝有最新管理代理程式的虛擬機器。
6. 使用最新的 `vCDManagementAgent.ovf` 和 `vCDManagementAgent-disk1.vmdk` 檔案，部署裝有新管理代理程式的虛擬機器。
7. 使用與舊管理代理程式中的相同設定，設定該管理代理程式。
8. [選用] 刪除裝有舊管理代理程式的虛擬機器。

重要事項
每個 VMware Cloud Director 環境必須只能有一個作用中的管理代理程式。

若要更新備份代理程式

1. 以合作夥伴系統管理員的身分，登入 Cyber Protect Cloud 管理入口網站。
2. 前往 **[設定]** > **[位置]**，然後按一下 **[新增 VMware Cloud Director]**。
3. 按一下 **[備份代理程式]** 連結，並下載包含最新代理程式的 ZIP 檔案。
4. 解壓縮管理代理程式範本檔案 `vCDCyberProtectAgent.ovf` 以及虛擬硬碟檔案 `vCDCyberProtectAgent-disk1.vmdk`。
5. 在 vSphere Client 中，關閉裝有最新備份代理程式的虛擬機器。
   目前可能正在執行的所有備份與復原工作都將失敗。若要檢查是否有任何工作正在執行中，請在 vSphere Client 中，開啟裝有備份代理程式的虛擬機器的主控台，然後執行下列命令：`ps | grep esx_worker`。請確認沒有作用中的 `esx_worker` 處理程序。
6. 使用最新的 `vCDCyberProtectAgent.ovf` 和 `vCDCyberProtectAgent-disk1.vmdk` 檔案，部署裝有新備份代理程式的虛擬機器。
7. 使用與舊備份代理程式中的相同設定，設定該備份代理程式。
8. [選用] 刪除裝有舊備份代理程式的虛擬機器。

建立備份系統管理員

組織系統管理員可以將備份管理委派給專門指派的備份系統管理員。

若要建立備份系統管理員

1. 在 VMware Cloud Director 租用戶入口網站中，按一下 **[管理]** > **[角色]** > **[新增]**。
2. 在 **[新增角色]** 視窗中，指定新角色的名稱和描述。
3. 向下捲動權限清單，然後在 **[其他]** 底下，選擇 **[自助 VM 備份操作員]**。

注意事項
在您安裝 VMware Cloud Director 的外掛程式之後，**[自助 VM 備份操作員]** 權限將變成可用。如需有關操作方式的詳細資訊，請參閱 "安裝並發佈 VMware Cloud Director 的外掛程式" (第 130 頁)。

4. 在 VMware Cloud Director 租用戶入口網站中，按一下 **[使用者]**。

5. 選擇使用者，然後按一下 **[編輯]**。
6. 為此使用者指派您建立的新角色。

結果，所選使用者將能夠管理此組織中的虛擬機器備份。

注意事項
VMware Cloud Director 環境的系統管理員可以在啟用 **[自助 VM 備份操作員]** 權限的情況下定義全域角色，然後將此角色發佈到租用戶。因此，組織系統管理員僅需要將角色指派給使用者。

系統報告、記錄檔和組態檔

基於疑難排解用途，您可能需要使用 sysinfo 工具建立系統報告，或檢查裝有代理程式的虛擬機器上的記錄檔和組態檔。

您可以透過在 vSphere Client 中開啟其主控台，直接存取虛擬機器，或透過 SSH 用戶端，從遠端存取。若要透過 SSH 用戶端存取虛擬機器，首先，您必須建立與此機器的 SSH 連線。

若要啟用與虛擬機器的 SSH 連線

1. 在 vSphere Client 中，開啟裝有代理程式的虛擬機器的主控台。
2. 在命令提示字元下，執行下列命令：`/bin/sshd` 以啟動 SSH 精靈。

結果，您可以使用 SSH 用戶端 (例如 WinSCP)，連線到此虛擬機器。

若要執行 sysinfo 工具

1. 存取裝有代理程式的虛擬機器。
   - 若要直接存取該虛擬機器，請在 vSphere Client 中，開啟虛擬機器的主控台。
   - 若要從遠端存取該虛擬機器，請透過 SSH 用戶端連線到虛擬機器。
     使用下列預設登入：密碼組合：`root`：`root`。
2. 瀏覽至 `/bin` 目錄，然後執行 `sysinfo` 工具。

   ```
   # cd /bin/
   # ./sysinfo
   ```

   結果，系統報告檔案將會儲存到預設目錄：`/var/lib/Acronis/sysinfo`。
   您可以在執行 `sysinfo` 工具時使用 `--target_dir` 選項，以指令其他目錄。

   ```
   ./sysinfo --target_dir path/to/report/dir
   ```

3. 使用 SSH 用戶端下載所產生的系統報告。

若要存取記錄檔或組態檔

1. 透過 SSH 用戶端連線到虛擬機器。
   使用下列預設登入：密碼組合：`root`：`root`。
2. 下載所需的檔案。
   您可以在下列位置找到記錄檔：

- 備份代理程式：/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log
- 管理代理程式：/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log

您可以在下列位置找到組態檔：

- 備份代理程式：/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml
- 管理代理程式：/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml

存取 Cyber Protect 主控台

下列系統管理員可以在 VMware Cloud Director 組織中管理虛擬機器的備份：

- 組織系統管理員
- 專門指派的備份系統管理員
  如需有關建立此種系統管理員的詳細資訊，請參閱 "建立備份系統管理員"(第 135 頁)。

系統管理員可以在 租用戶入口網站的導覽功能表中按一下 **[資安防護]**，以存取自訂的 Cyber Protect 主控台。

注意事項
單一登入僅適用於組織系統管理員，且不支援使用 VMware Cloud Director 租用戶入口網站的系統管理員。

在 Cyber Protect 主控台中，系統管理員僅能存取自己的 VMware Cloud Director 組織元素：虛擬資料中心、vApp 和個別的虛擬機器。他們可以管理 VMware Cloud Director 組織資源的備份和復原。

合作夥伴系統管理員可以存取其客戶租用戶的 Cyber Protect 主控台，而且可以代表他們管理備份和復原。

執行備份和復原

建立保護計劃

若要設定備份設定，您必須建立保護計劃。

您可以將保護計劃套用至多部電腦。此外，您可以對相同的電腦套用多個保護計劃。

限制

- 僅支援備份整部電腦。您無法備份個別磁碟或磁碟區。
- 不支援檔案篩選 (包含/排除)。
- 雲端儲存空間是唯一可用的備份位置。儲存空間是在管理代理程式設定中設定的，使用者無法在保護計劃中變更。
- 不支援動態群組。
- 支援下列備份配置：**[一律增量 (單一檔案)]**、**[一律完整備份]** 和 **[每週完整備份，每日增量備份]**。
- 支援僅在備份後清理。

若要建立保護計劃

1. 在 Cyber Protect 主控台中，移至 **[裝置]** > **[VMware Cloud Director]**。
2. 選擇您要保護的電腦，然後按一下 **[保護]**。
3. [如果已套用計劃] 按一下 **[新增計劃]**。
4. 按一下 **[建立計劃]**。
5. 在 **[加密]** 中，設定加密設定。
6. [選用] 若要重新命名保護計劃，請按一下鉛筆圖示，然後輸入新名稱。
7. [選用] 若要變更備份配置或排程，按一下 **[排程]**，然後進行設定。
8. [選用] 若要變更保留規則，按一下 **[保留的數量]**，然後進行設定。
9. [選用] 若要變更備份選項，按一下 **[備份選項]**，然後進行設定。
10. 按一下**[套用]**。

復原電腦

您可以將備份復原到原始虛擬機器或新虛擬機器。

限制

- 不支援檔案層級的復原。
- 您可以將備份復原到 VMware Cloud Director 10.4 和更新版本中的新虛擬機器。
  若要將備份復原到新的虛擬機器，備份必須由代理程式 24.02 版或更高版本建立。您可以在 `ProductVersion.conf` 檔案中檢查代理程式版本，該檔案位於已安裝代理程式的虛擬機器的 `/etc` 目錄中。
- 將備份復原到新機器後，新機器將顯示在 **[裝置]** > **[VMware Cloud Director]** > [組織] > 虛擬資料中心 >**[獨立 VM]** 中。您無法選擇特定的 vApp 作為復原目標。

若要復原電腦

到原始機器

1. 在 Cyber Protect 主控台中，透過以下其中一種方式選擇復原點：
   - 移至 **[裝置]** > **[VMware Cloud Director]**，選擇備份機器，按一下 **[復原]**，然後選擇復原點。
   - 移至 **[裝置]** > **[VMware Cloud Director]**，選擇備份存檔，按一下 **[顯示備份]**，然後選擇復原點。
2. 按一下 **[復原機器]**。
3. 按一下 **[開始復原]**。

到新機器

1. 在 Cyber Protect 主控台中，透過以下其中一種方式選擇復原點：
   - 移至 **[裝置]** > **[VMware Cloud Director]**，選擇備份機器，按一下 **[復原]**，然後選擇復原點。
   - 移至 **[裝置]** > **[VMware Cloud Director]**，選擇備份存檔，按一下 **[顯示備份]**，然後選擇復原點。
2. 按一下 **[復原機器]**。
3. 按一下 **[目標機器]**，然後選擇 **[新機器]**。
4. 為新電腦選擇虛擬資料中心。

5. 指定新機器的名稱。

   依預設，建議使用原始機器的名稱。
6. 按一下 **[確定]**。
7. [選用] 按一下 **[VM 設定]** 以變更新機器的以下任何設定，然後按一下 **[確定]**：
   - RAM 大小
   - 虛擬處理器數量
   - 每個插槽的核心數
   - 儲存空間設定檔
   - 網路介面卡和指派的網路
8. [選用] 按一下 **[磁碟對應]** 以變更磁碟對應或磁碟的儲存設定檔，然後按一下 **[確定]**。
9. 按一下 **[開始復原]**。

移除與 VMware Cloud Director 的整合

還原設定並從 Cyber Protect Cloud 解除登錄 VMware Cloud Director 執行個體是一個複雜的程序。如需協助，請聯絡您的支援代表。

索引

若

計

重

限

修

套

弱

根

停

商

啟

執

變