管理门户

25.04

合作伙伴管理员指南

修改：2025/5/6

目录

关于本文档

本文档面向想要使用 Cyber Protect Cloud 向客户提供服务的合作伙伴管理员。

本文档介绍如何使用管理门户来设置和管理 Cyber Protect Cloud 中提供的服务。

关于 Cyber Protect

Cyber Protect 是一个云平台，允许服务提供商、经销商和代理商向其合作伙伴和客户提供数据保护服务。

这些服务在合作伙伴级别乃至客户公司级别和最终用户级别上提供。

服务管理通过称为**服务中控台**的 Web 应用程序提供。租户和用户帐户管理通过称为**管理门户**的 Web 应用程序提供。

管理门户使管理员能够：

- 监控服务的使用情况和访问服务中控台
- 管理租户
- 管理用户帐户
- 为租户配置服务和配额
- 管理存储
- 管理品牌
- 生成关于服务使用情况的报告

Cyber Protect 服务

本部分介绍于 2021 年 3 月引入的功能集(包含新的计费模式)。在 Cyber Protect 产品彩页中，详细了解新计费模式的优势。

以下服务和功能集在 Cyber Protect Cloud 中可用：

- **Cyber Protect**
  - **保护** - 具有包含在基本产品中的安全性和管理功能的完全网络安全保护，以及灾难恢复、备份和恢复、自动化和作为即付即用功能提供的电子邮件安全性。可以使用高级保护包来扩展此功能，但需要另外付费。
    高级保护包是独特功能集，可解决特定功能方面的较复杂情况，例如 Advanced Backup、Advanced Security + XDR 等。高级包扩展了标准 Cyber Protect 服务中可用的功能。
    有关高级保护包的更多信息，请参阅 "高级保护包"(第 128 页)。
  - **File Sync & Share** - 一种随时随地通过任何设备安全共享公司内容的解决方案。
  - **物理数据装运** - 一种通过将数据发送到硬盘驱动器上的云数据中心来帮助您节省时间和网络流量的解决方案。
  - **公证** - 一种基于区块链的解决方案，可确保共享内容的真实性。
- **Cyber 基础架构 SPLA**

在管理门户中，可以选择将向您租户提供的服务和功能集。按创建租户中所述调配或编辑租户后，请为每个租户完成配置。

Cyber Protect 的计费模式

计费模式是一种用于对服务及其功能的使用进行记账和计费的方案。计费模式确定哪些单位将用作定价计算的基础。计费模式可以由合作伙伴在客户级别设置。

许可引擎会根据保护计划中请求的功能自动获取产品项目。用户可以通过自定义其保护计划，来优化保护级别和成本。

注意
每个客户租户只能使用一种计费模式。

保护 组件的计费模式

保护 有两种计费模式：

- 每工作负载
- 每 GB

两种计费模式的功能集是相同的。

在这两种计费模式中，保护服务均包含涵盖大多数网络安全风险的标准保护功能。用户无需另外付费即可使用它们。将对使用包含的功能进行记账，但不会收费。如需所包含计费产品项目的完整列表，请参阅 "Cyber Protect 服务"（第 7 页）。

尽管为客户启用了高级包，但仅客户在保护计划中开始使用该包的功能后，才会开始计费。当在保护计划中应用了高级功能时，许可引擎会自动为保护的工作负载指派所需的许可证。

当不再使用高级功能时，许可证会被吊销并停止计费。许可引擎会自动指派反映功能实际使用情况的许可证。

只能为标准 Cyber Protect 服务功能指派许可证。高级功能是根据使用情况计费的，并且其许可证无法手动修改。许可引擎会自动指派和取消指派这些许可证。可以手动更改工作负载的许可证类型，但当用户修改了该工作负载的保护计划时，将会重新指派许可证类型。

注意
启用高级保护功能后，将不会开始对其进行计费。仅当客户在保护计划中开始使用高级功能后，才会开始计费。启用的功能集将会记账并包含在使用情况报告中，但不会对它们进行计费，除非使用了其功能。

File Sync & Share 的计费模式

File Sync & Share 有以下计费模式：

- 每用户
- 每 GB

还可以应用旧版 File Sync & Share 的计费规则。

注意

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.

物理数据装运的计费

物理数据装运的计费遵循即付即用模式。

公证的计费

公证的计费遵循即付即用模式。

使用旧版的计费模式

如果还没有迁移到当前计费模式，可以在一种计费模式下使用这些产品项目来替换旧版本。许可引擎会自动优化已指派给客户的许可证，以最大程度地减少计费金额。

注意

不能将各版本与计费模式混合使用。

从旧版本切换到当前许可模式

可以通过编辑租户的个人资料并为他们选择产品项目，来为这些租户手动切换产品项目。有关切换过程的详细信息，请参阅 "在版本和计费模式之间切换"(第 9 页) 。

要将多个客户的各版本切换到计费模式，请参阅多个客户的批量版本切换 (67942)。

在版本和计费模式之间切换

在管理门户中，可以修改租户帐户，以在计费模式之间(从“按工作负载”到“按 GB”，反之亦然) 以及旧版本和计费模式之间切换产品项目。

有关批量切换租户的信息，请参阅多个客户的批量版本切换 (67942)。

切换过程包括以下步骤。

1. 将新的产品项目调配给客户租户(启用产品项目和配额设置) ，以匹配原始产品项目中可用的功能。
2. 取消指派未使用的产品项目，并根据保护计划中所使用的功能将这些产品项目指派给工作负载(使用核对) 。

下表阐述了两个方向下的过程。

	切换方向	
	版本 > 计费模式	**计费模式 > 计费模式**
产	启用产品项目以实现源版本中可用的功能。	将启用相同的产品项目集。

	切换方向	
	版本 > 计费模式	**计费模式 > 计费模式**
品项目切换		
配额切换	配额将从源产品项目复制到目标产品项目。源标准 → 目标标准产品源标准 → 目标包。 **注意** 如果从带有子版本的版本(例如,“Cyber Protect (按工作负载)”) 进行切换,将会汇总配额。	配额将从源产品项目复制到目标产品项目。
使用切换	根据已指派给工作负载的保护计划中所请求的功能,将向这些工作负载重新指派产品项目。	

示例:将 Cyber Protect 高级版切换为按工作负载计费

在此方案中,客户租户在 8 个工作站上使用 Cyber Protect 高级版,并将配额设置为 10 个工作负载。3 个工作站在其保护计划中使用的是软件清查和修补程序管理、2 个工作站在其保护计划中启用了 URL 过滤,其中一台计算机使用的是连续数据保护。下表阐述了相应版本到新产品项目的转换。

源产品项目 - 使用/配额	目标产品项目 - 使用/配额
Cyber Protect Advanced Workstation 8/10	• 工作站 - 8/10 • Advanced Security + XDR - 2/10 • Advanced Backup 工作站 - 1/10 • Advanced Management (RMM) - 3/10

切换过程中执行了以下步骤:

1. 涵盖源版本中可用功能的产品项目已自动启用。
2. 配额已复制到新产品项目上。
3. 使用情况已根据保护计划中的实际使用情况进行了调整:三个工作负载使用 Advanced Management (RMM) 包的功能、两个工作负载使用 Advanced Security + XDR 包的功能,以及一个工作负载使用 Advanced Backup 包的功能。

示例:Cyber Protect 按工作负载版本切换为按工作负载计费

在此示例中,客户在工作负载上指派多个版本。每个工作负载只能指派一个版本或一种计费模式。

源产品项目 - 使用/配额	目标产品项目 - 使用/配额
Cyber Protect Essentials Workstation - 6/12	• 工作站 - 14/42 • Advanced Backup 工作站 - 2/42 • Advanced Security + XDR - 13/42 • Advanced Management (RMM) - 5/42
Cyber Protect Standard Workstation - 5/10	
Cyber Protect Advanced Workstation - 2/10	
Cyber Backup Standard Workstation - 1/10	

切换过程中执行了以下步骤：

1. 涵盖所有源版本中可用功能的提供项已自动启用。使用计费模式时，可以根据需要将多个产品项目指派给工作负载。
2. 配额已汇总并复制。
3. 使用情况已根据保护计划进行了调整。

更改合作伙伴租户的计费模式

更改合作伙伴租户的计费模式

1. 在管理门户中，转到**客户端**。
2. 选择要更改计费模式的合作伙伴租户、单击省略号图标 ，然后单击**配置**。
3. 在**Cyber Protect**选项卡上，选择要更改计费模式的服务，然后单击**编辑**。
4. 选择所需的计费模式，并根据需要启用或禁用可用的产品项目。
5. 单击**保存**。

更改客户租户的计费模式

可以按以下方法操作来更改客户租户的计费：

- 通过启用或禁用产品项目，编辑原始计费模式。
- 切换到全新的计费模式。

有关如何编辑可用的产品项目的详细信息，请参阅启用或禁用产品项目。

切换客户租户的计费模式

1. 在管理门户中，转到**客户端**。
2. 选择要更改其版本的客户租户、单击省略号图标 ，然后单击**配置**。
3. 在**配置**选项卡上的**服务**下，选择新的计费模式。
   将弹出一个对话框，以通知您对新计费模式更改的结果。
4. 输入您的用户名以确认选择。

注意
该更改可能需要 10 分钟才能完成。

产品项目和配额管理

本节介绍以下内容:

- 什么是服务和产品项目?
- 如何启用或禁用产品项目?
- 什么是计费模式?
- 什么是高级保护包?
- 什么是旧版本和子版本?
- 什么是软配额和硬配额?
- 何时可以超出硬配额?
- 什么是备份配额转换?
- 产品项目可用性如何影响 Cyber Protect 中控台中的工作负载类型可用性?

服务和产品项目

服务

云服务是由合作伙伴或最终客户的私有云托管的一组功能。通常,服务以订购许可或即付即用的方式出售。

Cyber Protect 服务集成有网络安全、数据保护和管理,以保护您的端点、系统和数据免受网络安全威胁。Cyber Protect 服务包含多个组件:保护、File Sync & Share、公证和物理数据装运。通过使用高级保护包,可以使用高级功能扩展其中的某些组件。有关包含的功能和高级功能的详细信息,请参阅 "Cyber Protect 服务"(第 7 页)。

提供项

产品项目是按特定工作负载类型或功能(例如,存储、灾难恢复基础架构等) 分组的一组服务功能。通过启用特定产品项目,即可确定可以保护的工作负载类型、可以保护的工作负载数量(通过设置配额) 以及将向合作伙伴、客户及其最终用户提供的保护级别(通过启用或禁用高级保护包) 。

除非配置追加销售方案,否则会对客户和用户隐藏未启用的功能。有关追加销售方案的详细信息,请参阅 "为客户配置追加销售方案"(第 67 页)。

功能使用情况是从服务中收集的,并反映在产品项目中,这些内容会用于报告和进一步计费。

计费模式和版本

使用旧版时,可以为每个工作负载启用一个产品项目。使用计费模式时,将拆分功能,因此可以为每个工作负载启用多个产品项目(服务功能和高级包) ,以便更好地满足客户的需求,并仅针对客户实际使用的功能应用更精确的计费。

有关 Cyber Protect 的计费模式的详细信息,请参阅 "Cyber Protect 的计费模式"(第 8 页)。

可以使用计费模式或版本，来配置可供租户使用的服务。可以为每个客户租户选择一种计费模式或一个版本。因此，要为不同的服务功能应用不同的计费模式，您需要为客户创建多个租户。例如，如果客户想要将 Microsoft 365 邮箱置于“按 GB”计费模式下，并将 Teams 置于“按工作负载”计费模式下，则必须为此客户创建两个不同的客户租户。

要在产品项目中限制使用服务，可以为该产品项目定义配额。请参阅 "软配额和硬配额"(第 14 页)。

启用或禁用产品项目

可以按创建租户中所述，启用给定版本或计费模式下可用的所有产品项目。

注意
禁用服务的所有产品项目不会自动禁用该服务。

下表列出了禁用产品项目的一些限制。

产品项目	禁用	结果
备份存储	当使用量为零时可以禁用。	云存储将不可用作客户租户内备份的目标。
本地备份	当使用量为零时可以禁用。	本地存储将无法作为客户租户内备份的目标。禁用本地备份配额将禁用备份到本地磁盘、网络共享和公共云(如与 S3 兼容的云、Azure、AWS、Wasabi 和 Impossible Cloud) 。
数据源(包括 Microsoft 365 和 Google Workspace) *	当使用量为零时可以禁用。	将无法在客户租户内保护已禁用的数据源(包括 Microsoft 365 和 Google Workspace) ，如下所示：
所有Disaster Recovery产品项目	当使用量大于零时可以禁用。	有关详细信息，请参阅“软配额和硬配额”。
所有公证产品项目	当使用量为零时可以禁用。	公证服务将在客户租户中不可用。
所有File Sync & Share产品项目	无法单独启用或禁用产品项目。	File Sync & Share服务将在客户租户中不可用。
所有物理数据装运产品项目	当使用量为零时可以禁用。	物理数据装运服务将在客户租户中不可用。

对于使用量大于零时无法禁用的产品项目，可以手动删除使用量，然后禁用相应产品项目。

* 与可以在 Cyber Protect 中控台中添加的工作负载有关的产品项目。有关详细信息，请参阅 "工作负载依赖于产品项目"(第 23 页)。下表汇总了一个产品项目、一组产品项目或一个高级包在管理门户中未启用的情况下，哪些工作负载类型将不可用。

如果禁用这些产品项目或高级包	您将无法添加这些类型的工作负载
以下组合： • Microsoft 365 席位 • Microsoft 365 SharePoint online • Microsoft 365 Teams	Microsoft 365 企业
以下组合： • Google Workspace • Google Workspace Shared Drive	Google Workspace
以下组合： • 服务器 • 虚拟机	• Microsoft SQL Server • Microsoft Exchange Server • Microsoft Active Directory
以下产品项目： • NAS	Synology
以下产品项目： • 手机	• iOS 设备 • Android 设备
以下高级包： • Advanced Backup	Oracle 数据库
以下组合： • 电子邮件存档席位 • 存档存储	邮件服务器

软配额和硬配额

配额让您可以限制租户使用服务的能力。要设置配额，请在**客户端**选项卡上选择客户端，选择“服务”选项卡，然后单击**编辑**。

当超出配额时，将向用户的电子邮件地址发送一条通知。如果未设置配额超额，系统会将该配额视为**“软配额”**。这意味着将不会对使用 Cyber Protection 服务施加限制。

如果指定配额超额，那么系统将该配额视为**“硬配额”**。**超额**允许用户超出指定值的配额。当超出超额时，系统会对使用服务施加限制。

示例

软配额：您已将工作站的配额设置为 20。当客户的受保护工作站数量达到 20 个时，客户会收到电子邮件通知，但 Cyber Protection 服务仍然可用。

硬配额:如果已将工作站的配额设置为 20,且超额为 5,则当受保护的工作站数量达到 20 个时,客户会收到电子邮件通知;而当数量达到 25 个时,将禁用 Cyber Protection 服务。

当达到硬配额时,服务会受到限制(无法保护另一个工作负载或使用更多存储空间)。当超出硬配额时,将向用户的电子邮件地址发送通知。

可以定义配额的级别

可以基于下表所列的级别设置配额。

租户/用户	软配额(仅限配额)	硬配额(配额和超额)
合作伙伴	是	否
文件夹:	是	否
客户	是	是
单元	否	否
用户	是	是

可以基于合作伙伴和文件夹级别设置软配额。无法基于单位级别设置配额。可以基于客户和用户级别设置硬配额。

基于用户级别设置的硬配额总量不能超过相关客户的硬配额。

设置软配额和硬配额

为客户端设置配额

1. 在管理门户中,转到**客户端**。
2. 选择要为其设置配额的客户端。
3. 选择**保护**选项卡,然后单击**编辑**。
4. 选择要设置的配额类型。例如,选择**工作站**或**服务器**。
5. 单击右侧的**无限制**链接,以打开**配额编辑**窗口。
   - 如果要向客户端通知配额,但不希望限制客户端使用服务的能力,请在**软配额**字段中设置配额值。

     客户端将在达到配额后收到电子邮件通知,但 Cyber Protection 服务仍会可用。
   - 如果要限制客户端使用服务的能力,请选择**硬配额**,然后在**硬配额**下面的字段中设置配额值。

     客户端将在达到配额后收到电子邮件通知,并且 Cyber Protection 服务会禁用。
6. 在**配额编辑**窗口中,单击**完成**,然后单击**保存**。

重要事项

产品 UI 中显示的存储使用值为二进制字节单位 – 以 Mib、Gib 和 Tib 为单位 – 尽管标签分别显示为 MB、GB 和 TB。例如,如果实际使用量为 3105886629888 字节,则 UI 中显示的值将正确显示为 2.82,但标签显示为 TB 而非 TiB。

备份配额

可指定云存储空间配额、本地备份的配额以及允许用户保护的最大计算机/设备/网站数量。以下配额可用。

设备的配额

- **工作站**
- **服务器**
- **虚拟机**
- **移动设备**
- **Web 托管服务器**(基于 Linux 的物理或虚拟服务器，运行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板)
- **网站**

只要向计算机/设备/网站应用至少一个保护计划，相应计算机/设备/网站就被视为受到保护。移动设备在第一次备份后进入受保护状态。

当超出许多设备的超额时，用户无法将保护计划应用于更多设备。

云数据源的配额

- **Microsoft 365 席位**

  服务提供商会将此配额应用于整个公司。公司管理员可以在管理门户中查看配额及其使用情况。超出硬配额后，无法将备份计划应用于新席位。

  此配额的计费取决于 Cyber Protection 的所选计费模式。

  - 在**每 GB** 计费模式下，计费仅基于存储使用量，不会计算席位。
  - 在**按工作负载**计费模式下，计费基于受保护的 Microsoft 365 席位的数量。仅对未受保护的席位计费存储使用情况。

    下表总结了**按工作负载**计费模式。

	备份位置	
	Acronis 托管存储* 合作伙伴托管存储	**Microsoft Azure 存储 Google 存储**
受保护的席位	该计费基于受保护的席位数量进行计算。 受保护席位的备份使用的存储空间不会计费。	受保护的许可和已使用的存储空间都会计费。
未受保护的许可	未受保护的许可证不会计费。 将对未受保护座席的备份使用的存储空间计费。	未受保护的许可证不会计费。 将对未受保护座席的备份使用的存储空间计费。

* 适用于 Acronis Storage 的合理使用策略。条款和条件可在 https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage 查看。

当 Microsoft 365 用户具有以下任一条件时，将视为该席位受保护：

- 应用备份计划的邮箱
- 应用了备份计划的 OneDrive
- 有权访问受保护的公司级资源，如 Microsoft 365 SharePoint Online 站点或 Microsoft 365 Teams。

  要了解如何检查 Microsoft 365 SharePoint 或 Teams 站点的成员数量，请参阅此知识库文章。

以下情况下，座席会变为未受保护状态：

- 已撤销用户对受保护的公司级资源（如 Microsoft 365 SharePoint Online 站点或 Microsoft 365 Teams）的访问权限。
- 已从用户的邮箱或 OneDrive 撤销所有备份计划。
- Microsoft 365 组织中的用户已删除。

以下 Microsoft 365 组元不会收费，并且不需要每个席位一个许可证：

- 共享邮箱
- 空间和设备
- 有权访问备份的 SharePoint 站点和/或 Microsoft Teams 的外部用户。

注意

受到阻止的 Microsoft 365 用户没有受保护的个人邮箱或 OneDrive，只能访问共享资源（共享邮箱、SharePoint 站点和 Microsoft Teams），不收取费用。受到阻止的用户是指没有有效登录且无法访问 Microsoft 365 服务的用户。如需了解如何阻止 Microsoft 365 组织中的所有未经许可的用户，请参阅 "防止未经许可的 Microsoft 365 用户登录"（第 20 页）。

重要事项

本地代理程序和云代理程序消耗不同的配额。如果使用上述两个代理程序备份相同的工作负载，您将支付两次费用。例如：

- 如果使用本地代理程序备份 120 个用户的邮箱，并使用云代理程序备份相同用户的 OneDrive 文件，您将为 240 个 Microsoft 365 席位支付费用。
- 如果使用本地代理程序备份 120 个用户的邮箱，还使用云代理程序备份相同邮箱，您将为 240 个 Microsoft 365 席位支付费用。

若要查看有关 Microsoft 365 席位许可的常见问题，请参阅Cyber Protect Cloud: Microsoft 365 每 GB 许可和Cyber Protect Cloud：Microsoft 365 许可和定价变化。

- **Microsoft 365 SharePoint Online**

  此配额由服务提供商应用于整个公司。此配额启用对 SharePoint Online 站点的保护，并会设置可以保护的站点集合和组站点的最大数量。

  公司管理员可以在管理门户中查看配额。他们还可以在使用情况报告中查看配额以及 SharePoint Online 备份所使用的存储空间量。
- **Microsoft 365 Teams**

  此配额由服务提供商应用于整个公司。此配额启用或禁用保护 Microsoft 365 Teams 的功能，并设置可以保护的最大团队数量。要保护一个团队，无论其成员或渠道有多少，都需要一个配额。公司管理员可以在管理门户中查看配额和使用情况。
- **Microsoft 365 邮件存档席位**

Microsoft 365 电子邮件存档席位配额可启用或禁用创建 Microsoft 365 电子邮件服务器存档的功能，并设置可添加到存档的最大邮箱数量。

- **电子邮件存档席位(已过时)**

  此配额已被弃用，您无法在管理门户中创建新租户时启用此配额。

  对于现有租户，您只能禁用已启用的配额，但无法重新启用。

  重要事项

  创建新客户租户时，请使用 **Microsoft 365 存档席位**配额。

  对于现有客户，**电子邮件存档席位(已过时)**配额将自动替换为 **Microsoft 365 存档席位**配额。**电子邮件存档席位(已过时)**下的任何现有用量将转移到 **Microsoft 365 存档席位**。

  Google Workspace 席位

  此配额由服务提供商应用于整个公司。可以允许该公司保护 **Gmail** 邮箱(包括日历和联系人)、**Google Drive** 文件或两者。公司管理员可以在管理门户中查看配额和使用情况。

  如果向用户的邮箱或 Google Drive 应用至少一个备份计划，Google Workspace 席位就被视为受保护。

  超出硬配额后，公司管理员无法将备份计划应用于新的许可证。

- **Google Workspace Shared Drive**

  此配额由服务提供商应用于整个公司。此配额启用或禁用保护 Google Workspace Shared Drive 的功能。如果启用了该配额，即可保护任意数量的 Shared Drive。公司管理员在管理门户中无法查看配额，但可以在"使用报告"中查看 Shared Drive 备份所占据的存储空间量。

  此外，仅有至少一个 Google Workspace 席位配额的客户才能备份 Google Workspace Shared Drive。此配额仅经过验证，不会被占用。

存储的配额

重要事项

产品 UI 中显示的存储使用值为二进制字节单位 – 以 Mib、Gib 和 Tib 为单位 – 尽管标签分别显示为 MB、GB 和 TB。例如，如果实际使用量为 3105886629888 字节，则 UI 中显示的值将正确显示为 2.82，但标签显示为 TB 而非 TiB。

- **云资源**
  - **备份存储**
    - **备份存储**

      此配额限制位于云存储中的备份的总大小。当备份存储硬配额超出时，备份操作将不会启动。

      在**按工作负载**计费模式下，此配额仅适用于与 Microsoft 365 和 Google Workspace 不同的工作负载的备份。

      Microsoft 365 和 Google Workspace 工作负载的备份存储空间是无限的*。如果从工作负载中删除了席位配额(例如 **Microsoft 365 席位** 或 **Google Workspace 席位**)，则备份存储空间仍然是无限的，但其使用量将会收费。

在**每 GB** 计费模式中，此配额适用于所有备份，包括 Microsoft 365 和 Google Workspace 工作负载的备份。

* 适用于 Acronis Storage 的合理使用策略。条款和条件可在 https://www.acronis.com/company/licensing/#cyber-cloud-fair-usage 查看。

  - **存档存储**

    此配额限制云基础架构中电子邮件存档的总大小。

- **Advanced Disaster Recovery**

  本部分包含与灾难恢复相关的配额。

- **本地资源**
  - **本地备份**

    本地备份配额限制备份到本地磁盘、网络共享和公共云(如 S3 兼容、Azure、AWS、Wasabi 和 Impossible Cloud)的总大小。

    - 不能为此配额设置超额。
    - 硬性配额不能用于本地备份。

    注意

    禁用**本地备份**配额将禁用本地备份、备份到网络共享和备份到公共云。

超出备份存储的配额

不能超出备份存储空间配额。保护代理程序的技术配额等于租户的备份配额 + 超额。如果超出了配额，则不能开始备份。如果在备份创建期间达到证书中的配额但未达到超额，则备份将成功完成。如果在备份创建期间达到超额，则备份将失败。

示例：

用户租户有 1 TB 的配额可用空间，为此用户配置的超额为 5 TB。用户开始备份。例如，如果创建的备份大小为 3 TB，该备份将成功完成，因为未超过超额。如果创建的备份大小大于 6 TB，当超过超额时该备份将失败。

重要事项

产品 UI 中显示的存储使用值为二进制字节单位 – 以 Mib、Gib 和 Tib 为单位 – 尽管标签分别显示为 MB、GB 和 TB。例如，如果实际使用量为 3105886629888 字节，则 UI 中显示的值将正确显示为 2.82，但标签显示为 TB 而非 TiB。

备份配额转换

通常，这是获取备份配额和产品项目映射到资源类型的工作方式：系统将可用产品项目与资源类型进行比较，然后获取匹配产品项目的配额。

还可以指派另一个产品项目配额，即使它与资源类型不完全匹配。这称为**备份配额转换**。如果没有匹配的产品项目，系统会尝试为资源类型查找更高价值的合适配额(自动备份配额转换)。如果找不到合适配额，则可以在 Cyber Protect 中控台中手动将服务配额指派给资源类型。

示例

您想要备份虚拟机(工作站，基于代理程序)。

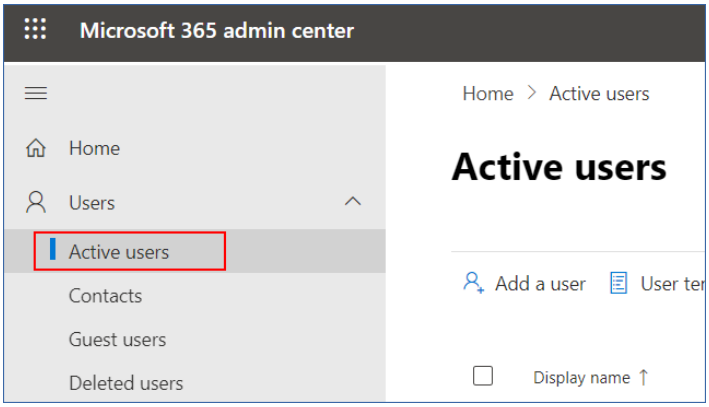
首先，系统会检查是否有已分配的**虚拟机**配额。如果找不到，系统会自动尝试获取**工作站**配额。如果还是找不到，将不会自动获取其他配额。如果您有足够贵于**虚拟机**配额的配额并且该配额适用于虚拟机，则可以登录到 Cyber Protect 中控台，然后手动指派**服务器**配额。

防止未经许可的 Microsoft 365 用户登录

可以通过编辑 Microsoft 365 组织中所有未经许可的用户的登录状态来阻止他们登录。

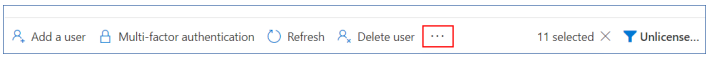
防止未经许可的用户登录

1. 以全局管理员身份登录到 Microsoft 365 管理中心 (https://admin.microsoft.com)。
2. 在导航菜单中，转到**用户** > **活动用户**。



3. 单击**过滤器**，然后单击**未经许可的用户**。

4. 选中用户名旁边的复选框，然后单击省略号 (...) 图标。



5. 在菜单中，选择**编辑登录状态**。
6. 选中**阻止用户登录**复选框，然后单击**保存**。

Disaster Recovery 配额

注意
Disaster Recovery 产品项目仅通过 Disaster Recovery 附加组件提供。

这些配额由服务提供商应用于整个公司。公司管理员可以在管理门户中查看配额和使用情况，但无法为用户设置配额。

- **灾难恢复存储**
  灾难恢复存储会显示受灾难恢复保护的服务器的备份存储大小。使用灾难恢复存储等同于使用受灾难恢复服务器保护的工作负载的备份存储。此存储会从创建恢复服务器时就开始计算，无论该服务器当前是否正在运行。如果达到此配额的超额，将无法创建主服务器和恢复服务器，也无法添加/扩展现有主服务器的磁盘。如果超过此配额的超额，将无法启动故障转移或启动已停止的服务器。正在运行的服务器继续运行。
- **计算点**

此配额可限制计费期内主服务器和恢复服务器使用的 CPU 和 RAM 资源。如果达到此配额的超额，则所有主服务器和恢复服务器都将关机。在下一个计费期开始之前，无法使用这些服务器。默认计费期为一个完整的日历月。

当配额禁用时，无论计费期如何，都无法使用服务器。

- **公共 IP 地址**

  此配额会限制可以分配给主服务器和恢复服务器的公共 IP 地址的数量。如果达到此配额的超额，则无法为更多服务器启用公共 IP 地址。可以通过在服务器设置中取消选中**公共 IP 地址**复选框，来禁止服务器使用公共 IP 地址。之后，可以允许另一台服务器使用公共 IP 地址，这通常不会是同一个 IP 地址。

  当配额禁用时，所有服务器将停止使用公共 IP 地址，从而无法通过 Internet 进行访问。

- **云服务器**

  此配额可限制主服务器和恢复服务器的总数。如果达到此配额的超额，则无法创建主服务器或恢复服务器。

  在配额禁用后，服务器会在 Cyber Protect 中控台中可见，但唯一可进行的操作是**删除**。

- **Internet 访问**

  此配额可启用或禁用主服务器和恢复服务器的 Internet 访问。

  当该配额禁用后，主服务器和恢复服务器将无法与 Internet 建立连接。

File Sync & Share配额

可以为租户定义以下 File Sync & Share 配额：

- **用户**

  这将定义对 File Sync & Share 用户数量的限制。

  注意
  仅用户和用户+管理员用户角色数接近此配额。
  管理员和来宾用户角色不包括在此配额中。

- **云存储**

  这将定义对为租户分配的云存储的限制。

物理数据装运配额

物理数据装运服务配额的使用基于每个驱动器。您可以将多台计算机的初始备份保存在一个硬盘上。

可以为租户定义以下物理数据装运配额：

- **至云**

  允许使用一个硬盘驱动器将初始备份发送到云数据中心。此配额定义要传输到云数据中心的驱动器的最大数量。

公证配额

可以为租户定义以下公证配额：

- **公证存储**
  为已公证文件、已签名文件和正在进行公证或签名的文件定义最大云存储空间。
  要减少此配额的使用，可以从公证存储中删除已公证或已签名的文件。
- **公证**
  定义可以使用公证服务进行公证的文件的最大数量。
  文件一上传到公证存储就视为已公证，并且其公证状态更改为**进行中**。
  如果同一文件进行多次公证，每次公证视为新的公证。
- **电子签名**
  定义数字电子签名的最大数量。

更改计算机的服务配额

计算机的保护级别由应用于它的服务配额定义。服务配额与注册计算机的租户的可用产品项目有关。

首次将保护计划应用于计算机时，将自动指派服务配额。

根据受保护计算机的类型、其操作系统、所需的保护级别和配额可用性，将指派最合适的配额。如果贵组织中没有最合适的配额，则会指派次优配额。例如，如果最合适的配额是 **Web 托管服务器**，但它不可用，则会指派**服务器**配额。

配额指派示例：

- 将向运行 Windows Server 或 Linux 操作系统的物理机指派**服务器**配额。
- 将向运行 Windows 桌面操作系统的物理机指派**工作站**配额。
- 将向运行 Windows 10(已启用 Hyper-V 角色) 的物理机指派**工作站**配额。
- 将向在虚拟桌面基础架构上运行且其保护代理程序安装在来宾操作系统(例如，适用于 Windows 的代理程序) 中的桌面计算机指派**虚拟机**配额。当**虚拟机**配额不可用时，此类计算机还可以使用**工作站**配额。
- 将向在虚拟桌面基础架构上运行并在无代理程序模式(例如，由适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序) 下备份的桌面计算机指派**虚拟机**配额。
- 将向 Hyper-V 或 vSphere 服务器指派**服务器**配额。
- 将向具有 cPanel 或 Plesk 的服务器指派 **Web 托管服务器**配额。如果 Web 托管服务器配额不可用，它还可以使用**虚拟机**或**服务器**配额，具体取决于运行 Web 服务器的计算机类型。
- 应用程序感知备份需要**服务器**配额，即使对于工作站也是如此。

可以稍后手动更改原始指派。例如，要将更高级的保护计划应用于同一台计算机，可能需要升级该计算机的服务配额。如果当前指派的服务配额不支持此保护计划所需的功能，则保护计划将失败。

或者，如果在已指派原始配额后购买了更多适用配额，可以更改服务配额。例如，**工作站**配额已指派给虚拟机。购买**虚拟机**配额后，可以手动将此配额指派给计算机，而不是原来的**工作站**配额。

还可以释放当前指派的服务配额，然后将此配额指派给其他计算机。

可以更改一台计算机的服务配额，也可以更改一组计算机的服务配额。

更改一台计算机的服务配额

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 选择所需计算机，然后单击**详细信息**。
3. 在**服务配额**部分中，单击**更改**。
4. 在**更改配额**窗口中，选择服务配额或**无配额**，然后单击**更改**。

更改一组计算机的服务配额

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 选择多台计算机，然后单击**指派配额**。
3. 在**更改配额**窗口中，选择服务配额或**无配额**，然后单击**更改**。

工作负载依赖于产品项目

根据已启用的产品项目，将在 中控台的**添加设备**窗格中提供不同的工作负载类型。在下表中，您可以看到可用的工作负载类型以及不同的产品项目。

工作负载类型（代理程序安装程序）	已启用的产品项目										
	服务器	工作站	虚拟机	Microsoft 365 席位	Google Workspace 席位	移动设备	Web 托管服务器	网站	NAS	电子邮件存档席位	存档存储
工作站 - 适用于 Windows 的代理程序		+	+					+			
工作站 - 适用于 macOS 的代理程序		+	+					+			
服务器 - 适用于 Windows 的代理程序	+		+				+	+			
服务器 - 适用于 Linux 的代理程序	+		+				+	+			
适用于 Hyper-V 的代理程序			+								

工作负载类型(代理程序安装程序)	已启用的产品项目										
	服务器	工作站	虚拟机	Microsoft 365 席位	Google Workspace 席位	移动设备	Web 托管服务器	网站	NAS	电子邮件存档席位	存档存储
适用于 VMware 的代理程序			+								
适用于 Virtuozzo 的代理程序			+								
适用于 SQL 的代理程序	+		+								
适用于 Exchange 的代理程序	+		+								
适用于 Active Directory 的代理程序	+		+								
适用于 Synology 的代理程序									+		
Microsoft 365 Business 工作负载				+							
Google Workspace 工作负载					+						
邮件服务器										+	+
适用于	+	+	+				+	+			

工作负载类型(代理程序安装程序)	已启用的产品项目										
	服务器	工作站	虚拟机	Microsoft 365 席位	Google Workspace 席位	移动设备	Web 托管服务器	网站	NAS	电子邮件存档席位	存档存储
Windows 的完整安装程序											
移动设备(iOS 和 Android)						+					

使用管理门户

以下步骤将指导您完成管理门户的基本用法。

支持的 Web 浏览器

Web 界面支持以下 Web 浏览器：

- Google Chrome 29 或更高版本
- Mozilla Firefox 23 或更高版本
- Opera 16 或更高版本
- Microsoft Edge 25 或更高版本
- 在 macOS 和 iOS 操作系统中运行的 Safari 8 或更高版本

在其他 Web 浏览器（包括在其他操作系统中运行的 Safari 浏览器），用户界面可能显示错误，或者某些功能可能不可用。

激活管理员帐户

在签署合作伙伴协议后，您将收到包含以下信息的电子邮件：

- **您的登录名。**这是您用于登录的用户名。您的登录名也会显示在帐户激活页面上。
- **激活帐户**按钮。单击该按钮并为您的帐户设置密码。确保密码的长度至少为九个字符。有关密码的详细信息，请参阅 "密码要求"（第 26 页）。

密码要求

在用户注册期间，会检查密码的复杂性，并将其分类为以下某一类别：

- 弱
- 中
- 强

不会保存弱密码，即使它长度够长也是如此。反复出现用户名、登录名、用户电子邮件地址或用户帐户所属租户的名称的密码始终被视为弱密码。最常见的密码也会被视为弱密码。

注意
密码要求可能会发生更改。

要加强密码，请向其中添加更多字符。不强制使用不同类型的字符（例如，数字、大写和小写字母以及特殊字符），但它会生成长度更短的更强密码。

访问管理门户

激活管理员帐户后，您可以使用登录名和设置的密码登录管理门户。

若要首次访问管理门户

1. 转到服务登录页面。
   登录页面的地址已包含在您收到的激活电子邮件中。
2. 键入登录名，然后单击**下一步**。
3. 键入密码，然后单击**下一步**。

> **注意**
> 为了防止 Cyber Protect Cloud 遭受暴力攻击，门户会在 10 次登录尝试失败后将您锁定。锁定时长为 5 分钟。15 分钟过后，系统会重置登录尝试失败次数。

4. 完成加入调查。
   有关加入选项的详细信息，请参阅 "加入调查"(第 27 页)。
5. 使用右侧菜单导航管理门户。

管理门户的超时时长为：活动会话为 24 小时，空闲会话为 1 小时。

部分服务包含从服务中控台切换到管理门户的功能。

加入调查

租户的第一位合作伙伴管理员在首次登录管理门户时，必须完成加入调查。此调查会根据管理员对主要兴趣、商业模式和公司规模的回答动态调整。通过根据企业的需求和兴趣量身定制入职体验，流程变得更加相关和高效。

无法跳过或关闭该调查。所有问题均为强制性问题。

在公司资料向导中配置联系人

可以为您公司配置联系信息。我们会向您提供的联系人发送有关平台中新功能和其他重要变化的更新。

首次登录到管理门户时，公司资料向导会引导您了解有关公司的基本信息以及要提供的联系人。

可以从 Cyber Protect 平台中存在的用户创建联系人，也可以添加无权访问服务的人员的联系信息。

使用公司资料向导配置公司联系人

1. 在**公司信息**中，指定您公司的以下详细信息：
   - **官方(法定)公司名称**
   - **公司法定地址(总部地址)**
     - **国家/地区**
     - **邮政编码**
2. 单击**下一步**。
3. 在**公司联系人**中，出于以下目的配置联系人：
   - **计费联系人** - 将获得有关在平台中报告的使用情况重要变化的更新的联系人。
   - **业务联系人** - 将获得有关平台中与业务相关重要变化的更新的联系人。

- **技术联系人** - 将获得有关平台中技术重要变化的更新的联系人。

可以出于多个目的使用联系人。

选择一个用于创建联系人的选项。

- **从现有用户创建**。从下拉列表中选择一个用户。
- **创建新联系人**。提供以下联系人信息：
  - **名字** - 联系人的名字。此字段为必填项。
  - **姓氏** - 联系人的姓氏。此字段为必填项。
  - **公司邮箱** - 联系人的电子邮件地址。此字段为必填项。
  - **公司电话** - 此字段为可选字段。
  - **职位** - 此字段为可选字段。

4. 如果您还计划将计费联系人用作业务联系人或技术联系人，请在**计费联系人**部分中选择相应的标志：
   - **使用相同的联系人作为业务联系人**
   - **使用相同的联系人作为技术联系人**
5. 单击**完成**。

   结果，将创建联系人。可以在管理中控台的**我的公司 > 公司资料**部分中编辑信息并配置其他联系人，如配置公司联系人中所述。

从管理门户访问 Cyber Protect 中控台

1. 在管理门户中，转到**监控 > 使用情况**。
2. 在 **Cyber Protect** 下，选择**保护**，然后单击**管理服务**。

   或者，在**客户端**下，选择一个客户，然后单击**管理服务**。

因此，系统会将您重定向到 Cyber Protect 中控台。

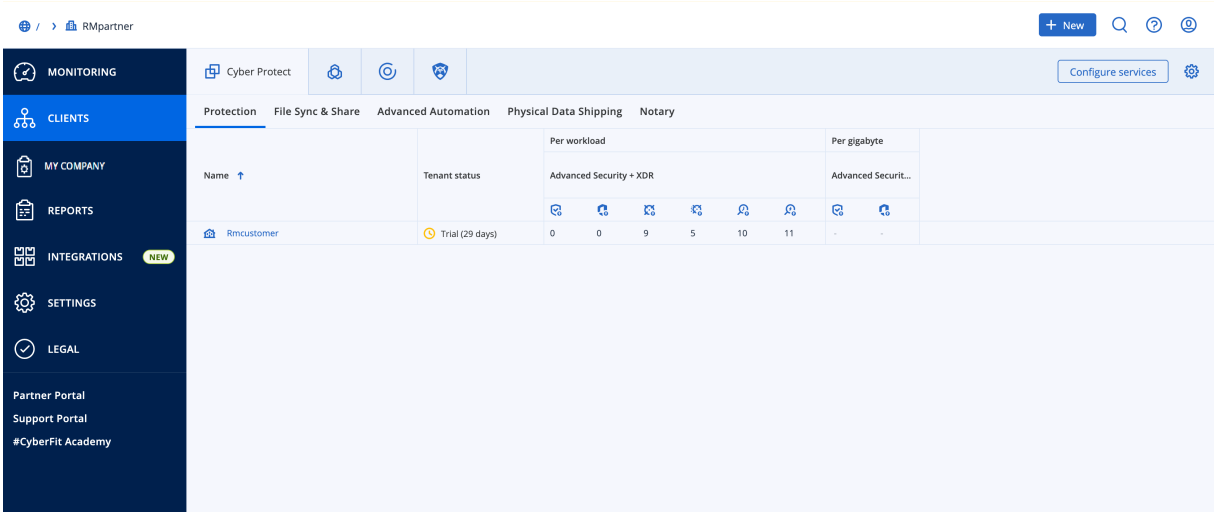
重要事项

如果客户处于**自助服务**管理模式下，则无法为其管理服务。只有客户管理员才能将客户模式更改为**由服务提供商管理**，然后管理服务。

导航管理门户

使用管理门户时，您可以在任何给定时间在租户内进行操作。此租户的名称显示在左上角。

默认情况下，您可用的最高层次结构级别处于选中状态。单击列表中的租户名称，可逐层展开层次结构。若要返回上一级别，请单击左上角的名称。



用户界面的所有部分仅显示和影响您当前正在操作的租户。例如：

- **客户端**选项卡仅显示您当前正在操作的租户的直接子对象。
- **我的公司**选项卡显示您当前正在操作的租户中存在的公司配置文件和用户帐户。
- **监控**选项卡显示当前操作的租户的直接子对象的使用情况和操作信息。

  注意
  此选项卡中可能有其他选项，具体取决于您订阅的服务。

- 使用**新建**按钮，您只能在当前正在操作的租户中创建租户或新的用户帐户。

  注意
  此菜单中可能有其他选项，具体取决于您订阅的服务。

我的收件匣

“我的收件匣”页面旨在简化您在应用程序中的通信。通过本指南，您可以有效地管理自己的消息，保持有序，提高生产力。产品收件匣是您在应用程序中接收和管理通信的集中式枢纽。它可让您了解工作流程中的重要更新、消息和警报。

概述

我的收件匣选项卡上有一个通知计数器，显示未读通知的数量。单击此计数器，即可显示未读通知，方便您跟踪待办事项。此外，每个筛选器(类别、重要性、操作)旁边的计数器显示特定筛选器下可用的通知的数量，帮助您了解每个类别中有多少通知。

您的收件匣中将收到各种通知，每种通知均根据您的帐户设置和上下文设计用于特定目的：功能公告、可用的新培训、活动和网络研讨会邀请、证书到期提醒、促销、维护通知、调查等。

检查您的通知

正在检查您的通知部分

1. 登录到 Cyber Protect Cloud 中控台。
2. 在导航窗格中，选择 **我的收件匣** 菜单项。

搜索“我的收件匣”

若要搜索未读取的邮件

1. 单击 **我的收件匣** 菜单项。
2. 在右上角，切换 **仅显示未读** 开关。

若要在收件匣中搜索重要信息

1. 从 仪表板访问 **我的收件匣**。
2. 在收件匣视图中，定位到顶部的 **搜索** 栏。
3. 输入相关关键字或发件人姓名以筛选邮件。
4. 按 **Enter** 以查看搜索结果。

结果将显示所有符合搜索条件的通知。

管理门户中的新增功能

在发布 Cyber Protect Cloud 的新功能后，您会在登录到管理门户时看到一个弹出窗口，其中简要描述了这些功能。

还可以通过单击主管理门户窗口左下角的**新增功能**链接，来查看新功能的描述。

限制对 Web 界面的访问

管理员可以通过指定允许租户成员登录的 IP 地址列表来限制对 Web 界面的访问。

注意
此限制同样适用于通过 API 访问管理门户。

注意
此限制仅适用于已设置该限制的级别。不适用于子租户的成员。

限制对 Web 界面的访问

1. 登录到管理门户。
2. 导航到您想要限制访问权限的租户。
3. 依次单击**设置** > **安全**。
4. 启用**登录控制**切换。
5. 在**允许的 IP 地址**中，指定允许的 IP 地址。
   您可以输入以下任意参数，由分号分隔：
   - IP 地址，例如：192.0.2.0
   - IP 范围，例如：192.0.2.0-192.0.2.255

- 子网，例如：192.0.2.0/24

6. 单击**保存**。

注意
对于使用 Cyber Infrastructure（混合模型）的服务提供商：

如果在管理门户中的**设置** > **安全**下启用了**登录控制**开关，则将 Cyber Infrastructure 节点的外部公共 IP 地址添加到**允许的 IP 地址**列表中。

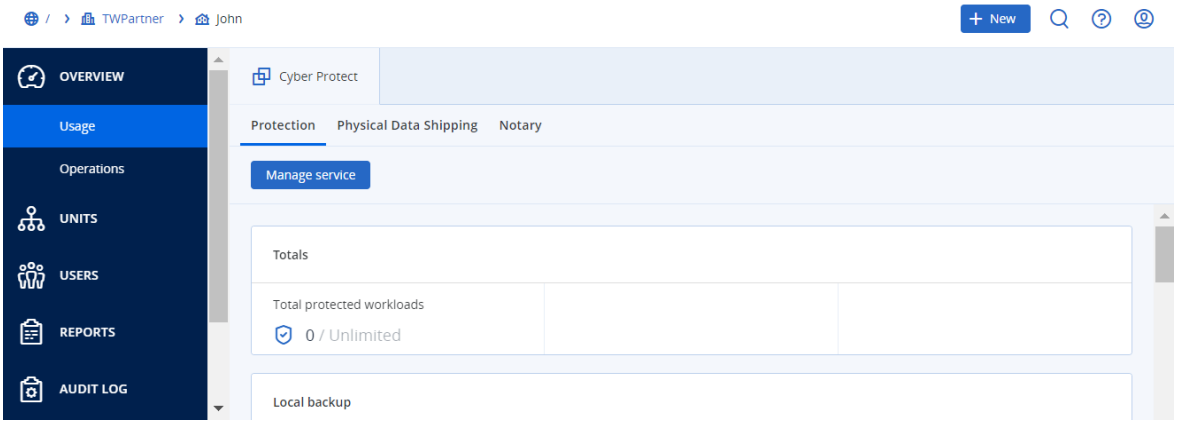
访问服务

“概述”选项卡

概述 > **使用情况**部分提供服务使用情况概述，并允许您在正在操作的租户内访问服务。

使用“概述”选项卡管理租户的服务

1. 导航到租户（要管理其服务），然后依次单击**概述** > **使用情况**。
   请注意，有些服务可以在合作伙伴租户和客户租户级别进行管理，而其他服务只能在客户租户级别进行管理。
2. 单击您要管理的服务的名称，然后单击**管理服务**或**配置服务**。
   有关使用服务的信息，请参阅服务中控台中提供的用户指南。

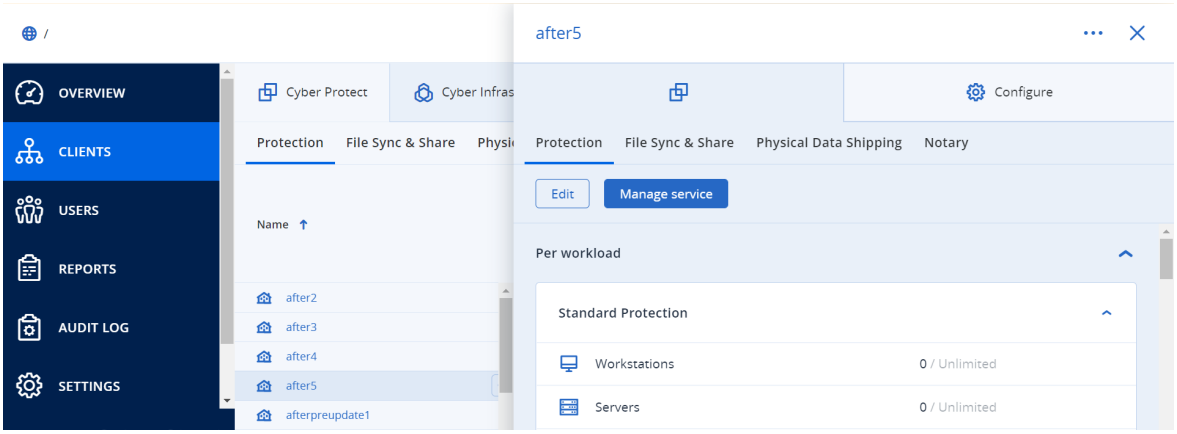


“客户端”选项卡

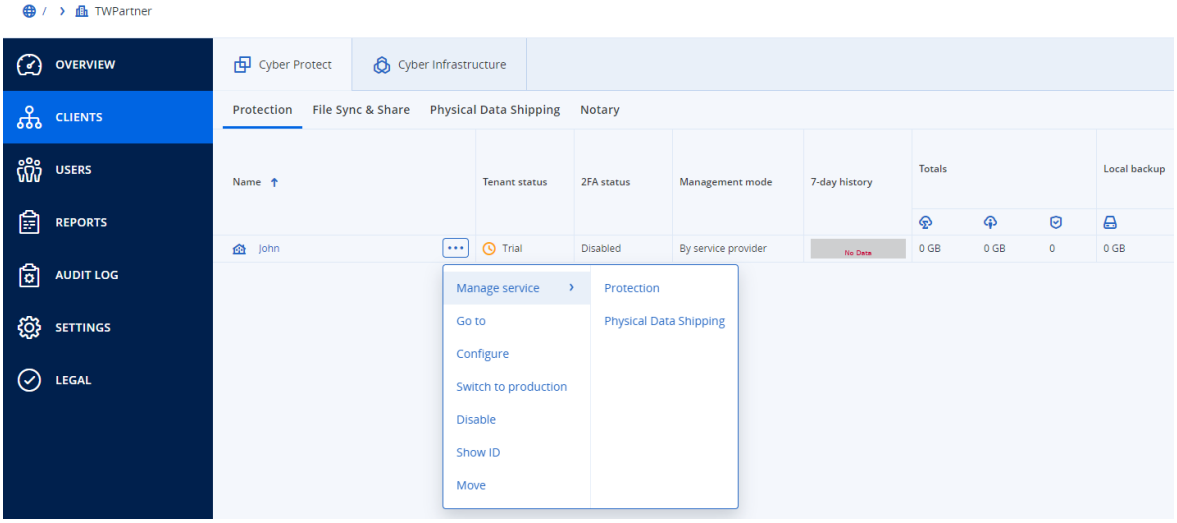
客户选项卡显示您正在操作的租户的子租户，并允许您在这些子租户内访问服务。

使用“客户端”选项卡管理租户的服务

1. 请执行以下任一操作：
   - 单击**客户端**，选择您要管理其服务的租户，单击您要管理的服务的名称或图标，然后单击**管理服务**或**配置服务**。



- 单击**客户端**，单击您要管理其服务的租户名称旁边的省略号图标，单击**管理服务**，然后选择您要管理的服务。



请注意，有些服务可以在合作伙伴租户和客户租户级别进行管理，而其他服务只能在客户租户级别进行管理。

有关使用服务的信息，请参阅服务中控台中提供的用户指南。

7 天历史记录栏

在**客户端**屏幕上，**7 天历史记录**栏会显示每个客户租户过去七天的工作负载备份的状态。该栏分为 168 条彩色线。每条线表示一小时间隔，并显示相应一小时间隔内备份的最差状态。

下表提供了有关每一线条颜色含义的信息。

颜色	描述
红色	一小时内至少有一个备份失败
橙色	一小时内至少有一个备份完成并出现警告，但没有任何备份错误
绿色	一小时内至少有一个备份成功，没有任何备份错误和警告
灰色	一小时内没有备份完成

在收集到相应的统计数据之前，**7 天历史记录**栏会一直显示“无备份”。

对于合作合作租户，**7 天历史记录**栏为空，因为不支持汇总统计数据。

用户帐户和租户

有两种用户帐户类型：管理员帐户和用户帐户。

- **管理员**拥有对管理门户的访问权限。他们在所有服务中都有管理员角色。
- **用户**没有对管理门户的访问权限。他们对服务的访问权限和在服务中的角色都由管理员定义。

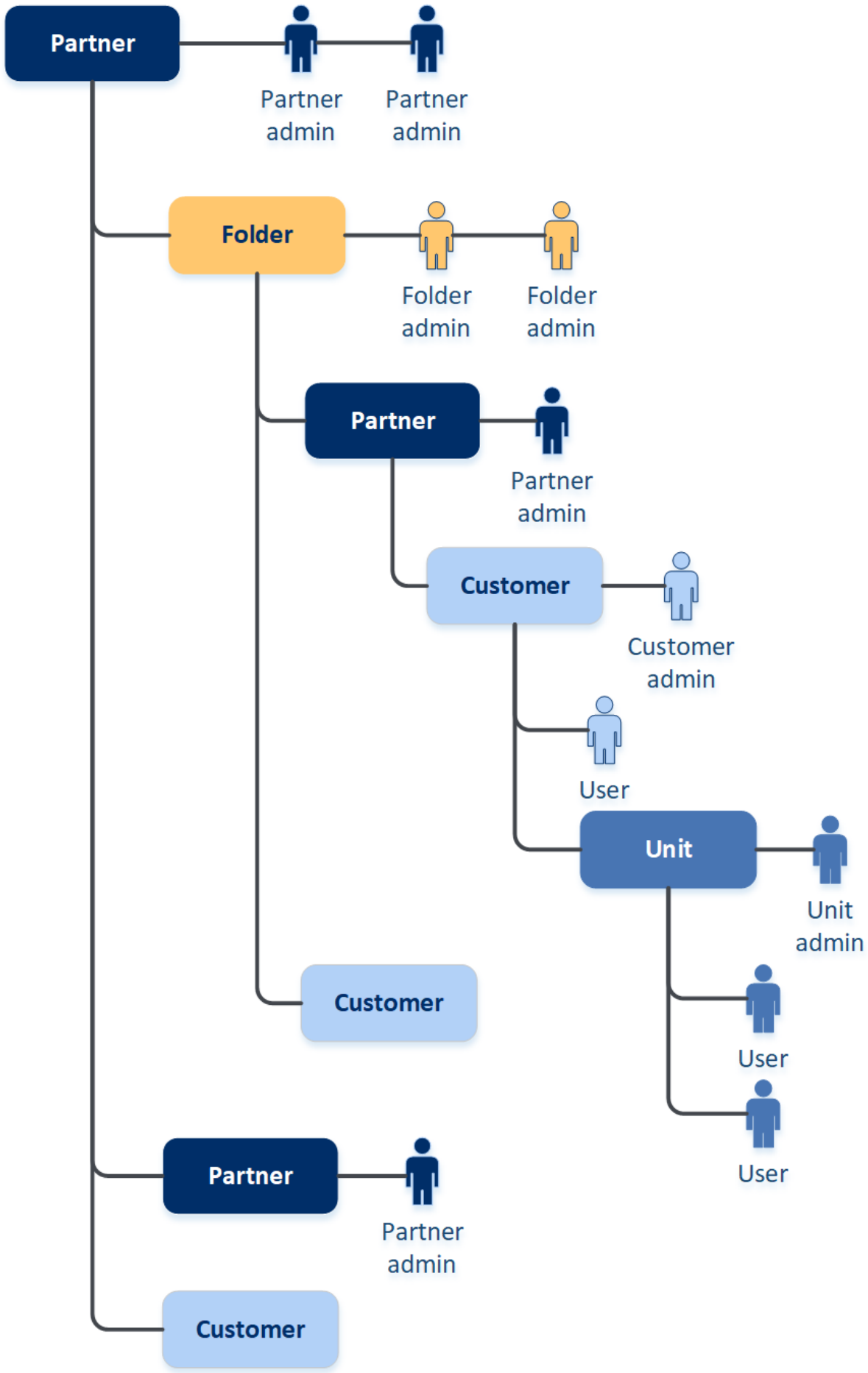
每个帐户都属于某个租户。租户是专用于合作伙伴或客户的管理门户资源（例如用户帐户和子租户）和服务产品（已启用的服务和服务中的产品项目）的一部分。租户层次结构应与服务用户和提供商之间的客户/供应商关系相匹配。

- **合作伙伴**类型的租户通常对应于转售服务的服务提供商。
- **文件夹**类型的租户是辅助租户，通常被合作伙伴管理员用于对合作伙伴和客户进行分组，以配置单独的产品和/或不同的品牌。
- **客户**类型的租户通常对应于使用服务的组织。
- **单位**类型的租户通常对应于组织内的单位或部门。

管理员可以在他们在层次结构中的级别上面或下面创建和管理租户、管理员帐户和用户帐户。

类型为**合作伙伴**的父租户的管理员可以充当类型为**客户**或**合作伙伴**的租户中的低级别管理员，其管理模式为**由服务提供商托管**。因此，该合作伙伴级管理员可以进行以下操作：例如，管理用户帐户和服务，或访问子租户中的备份和其他资源。但是，低级别管理员可以限制更高级别的管理员对其租户的访问。

下图演示合作伙伴、文件夹、客户和单位租户的示例层次结构。


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

下表总结了管理员和用户可以执行的操作。

操作	用户	客户和单元管理员	合作伙伴和文件夹管理员
创建租户	否	是	是
创建帐户	否	是	是
下载和安装软件	是	是	否*
管理服务	是	是	是
创建关于服务使用情况的报告	否	是	是
配置品牌	否	否	是

注意

- 可以从任意类型的租户创建用户，并且用户具有共享的电子邮件地址，只要它是从最高权限到最低权限创建的。例如，合作伙伴租户可以创建一个文件夹、客户和单位租户，而客户租户不能创建文件夹租户。
- 单位管理员无法创建、修改或应用Disaster Recovery保护计划。

管理租户

以下租户在 Cyber Protect 中可用：

- 通常为签署合作伙伴协议的每个合作伙伴创建**合作伙伴**租户。
- 通常创建**文件夹**租户来对合作伙伴和客户进行分组，以配置单独的产品和/或不同的品牌。
- 通常为注册服务的每个组织创建**客户**租户。
- 在客户租户内创建**单位**租户，以将服务扩展到新的组织单元。

创建和配置租户的步骤因您创建的租户而异，但通常该过程包括以下步骤：

1. 创建租户。
2. 为租户选择服务。
3. 为租户配置产品项目。

创建租户

1. 登录管理门户。
2. 导航到要在其中创建租户的租户。
3. 在右上角，单击**新建**，然后根据要创建的租户类型，单击以下选项之一：
   - 通常为签署合作伙伴协议的每个合作伙伴创建**合作伙伴**租户。
   - 通常创建**文件夹**租户来对合作伙伴和客户进行分组，以配置单独的产品和/或不同的品牌。
   - 通常为注册服务的每个组织创建**客户**租户。
   - 在客户租户内创建**单位**租户，以将服务扩展到新的组织单元。

   类型是否可用取决于父租户类型。

4. 在**名称**中，指定新租户的名称。
5. [仅在创建合作伙伴租户时]输入**官方(法定)公司名称**(必填)和 **VAT 编号/TAX ID/公司注册号**(可选)。
6. [仅在创建客户租户时]
   a. 在**运行模式**下，选择该租户是在试用模式下还是生产模式下使用服务。每月服务使用情况报告包含两种模式下租户的使用情况数据。

      重要事项
      试用模式提供 30 天的评估期，期间提供对产品的完全访问权限。请注意，一旦客户切换到生产模式，他们的使用情况将自动包含在最近的计费周期中。
      可以随时切换到生产模式。但是，无法载从生产模式恢复到试用模式。
      如果决定取消某客户的试用，则还必须删除相应的客户租户。否则，30 天试用期满后，客户将自动切换到生产模式，相应的使用量将计入最近的计费周期。有关更多详细信息，请参阅此知识库文章。

   b. 在**高级设置**下，选择租户的管理模式。
      - **由服务提供商托管** - 此模式授予父租户的管理员对该客户的完全访问权限：修改属性；管理租户、用户和服务；访问备份和其他资源。默认会选中此模式。
      - **自助服务** - 此模式限制父租户的管理员对此租户的访问权限：他们仅可修改租户属性，但不能访问或管理内部的任何内容(例如，租户、用户、单元、服务、备份和其他资源)。

        注意
        如果选择**自助服务**，则只有"客户"租户的管理员才能更改管理模式。为此，客户管理员必须导航至**设置** > **安全**，并启用**支持访问**开关。

      可以在**客户端**选项卡中检查为子租户选择的管理模式。
7. [仅创建合作伙伴租户时]在**高级设置**下，选择以下模式之一以管理对租户的访问：
   - **完全访问** – 此模式授予父租户的管理员对租户的完全访问权限：管理合作伙伴的配额、用户和属性，访问合作伙伴的客户，并获取合作伙伴及其客户的使用情况报告。默认会选择此模式。
   - **受限访问** – 此模式限制父租户的管理员访问此合作伙伴租户：他们只能修改租户属性和配额，并获取合作伙伴的使用情况报告，但无法访问或管理内部任何内容(例如租户、用户、服务、备份和合作伙伴下的其他资源)，并且不会获取合作伙伴的客户的使用情况报告。

     注意
     若选择**有限访问**，则只有租户的管理员才能更改管理模式。若要执行此操作，管理员必须导航至**设置** > **安全**，并启用**支持访问**开关。

   可以在**客户端**选项卡中检查为子租户选择的管理模式。
8. 在**安全性**中，启用或禁用租户的双重身份验证 (2FA)。
   如果启用 2FA，则将要求此租户的所有用户都为其帐户配置双重身份验证，以提高安全访问。用户必须在其第二重身份验证设备上安装身份验证应用程序，然后使用一次性生成的 TOTP 代码

以及传统的登录名和密码来登录到中控台。有关更多详细信息，请参阅“设置双重身份验证”。要查看客户的双重身份验证状态，请转到**客户端**。

9. [仅当在合规模式下创建客户租户时] 在**安全性**中，选中**合规模式**复选框。
   在此模式下，仅允许加密备份。必须在受保护的设备上设置加密密码，否则创建备份将失败。需要向云服务提供加密密码的所有操作均不可用。有关更多详细信息，请参阅 "合规模式"(第 37 页)。

   重要事项
   在创建租户后不能禁用合规模式。

10. 在**创建管理员**中，配置管理员帐户。

    注意
    对于客户租户和**管理模式**设置为**自助服务**的合作伙伴租户，必须创建管理员。

    a. 输入管理员帐户的电子邮件。此电子邮件地址还将用作登录名。
    b. 如果您喜欢使用不同于电子邮件地址的登录名，请选中**使用不同于电子邮件地址的登录名**复选框，然后输入管理员帐户的登录名和电子邮件地址。
       其余字段是可选字段，但提供了更多沟通渠道，以备我们需要联系管理员时使用。
    c. 选择一种语言。
       如果不选择语言，则默认使用英语。
    d. 指定公司联系人。
       - **计费** - 将获得有关在平台中报告的使用情况重要变化的更新的联系人。
       - **技术** - 将获得有关平台中技术重要变化的更新的联系人。
       - **业务** - 将获得有关平台中与业务相关重要变化的更新的联系人。
         可以为一个用户指派多个公司联系人。

11. 在**语言**中，更改将在此租户中使用的通知、报告和软件的默认语言。
12. 请执行以下任一操作：
    - 要结束租户创建，请单击**保存并关闭**。在这种情况下，将为租户启用所有服务。保护 服务的计费模式将设置为按工作负载。
    - 要为租户选择服务，请单击**下一步**。请参阅 "为租户选择服务"(第 38 页)。

合规模式

合规模式是专为有更高安全要求的客户端而设计的。此模式对所有备份要求强制加密，仅允许本地设置加密密码。

在合规模式下，在客户租户中创建的所有备份及其单位都会自动使用 AES 算法和 256 位密钥进行加密。用户只能在受保护的设备上设置加密密码，不能在保护计划中设置加密密码。

重要事项
仅当创建新的客户租户时，合作伙伴管理员才可以启用合规模式，并且以后不能禁用此模式。无法为已存在的租户启用合规模式。

限制

- 合规模式仅与 15.0.26390 或更高版本的代理程序兼容。
- 合规模式不适用于运行 Red Hat Enterprise Linux 4.x 或 5.x 及其衍生产品的设备。
- 云服务不能访问加密密码。由于此限制，在合规模式下，某些功能不适用于租户。

不支持的功能

在合规模式下，以下功能不适用于租户：

- 通过 Cyber Protect 中控台恢复
- 通过 Cyber Protect 中控台在文件级别上浏览备份
- 访问 Web 恢复中控台
- 云到云备份
- 网站备份
- 应用程序备份
- 移动设备的备份
- 备份的反恶意软件扫描
- 安全恢复
- 公司白名单的自动创建
- 数据保护地图
- 灾难恢复
- 与不可用功能相关的报告和仪表板

为租户选择服务

默认情况下，创建新租户时，将会启用所有服务。可以选择将向租户及其子租户内的用户提供的服务。

还可以通过一键操作来为多个现有租户选择并启用服务。有关详细信息，请参阅 "为多个现有租户启用服务"(第 39 页)。

此步骤不适用于单位租户。

为租户选择服务

1. 在“创建/编辑租户”对话框的**选择服务**部分中，选择计费模式或版本。
   - 选择**按工作负载**或**按 GB** 计费模式，然后清除要禁用的租户服务的复选框。
     这两种计费模式的服务集都是相同的。
     对于 Advanced Disaster Recovery，如果已在您帐户下注册了自己的灾难恢复位置，则可以从下拉列表中选择灾难恢复的位置。
   - 要使用旧版本，请选中**旧版**单选按钮，然后从下拉列表中选择一个版本。

   已禁用的服务将对租户及其子租户内的用户隐藏。

2. 请执行以下任一操作：
   - 要结束租户创建，请单击**保存并关闭**。在这种情况下，将为无配额限制的租户启用选定服务的所有产品项目。
   - 要为租户配置产品项目，请单击**下一步**。请参阅 "为租户配置产品项目"(第 39 页)。

为租户配置产品项目

创建新租户时，将为选定服务启用所有产品项目。可以选择将向租户及其子租户内的用户提供的产品项目，并为它们设置配额。

此步骤不适用于单位租户。

为租户配置产品项目

1. 在“创建/编辑租户”对话框的**配置服务**部分中的每个服务选项卡下，清除要禁用的产品项目的复选框。
   与已禁用的产品项目相对应的功能不会提供给租户及其子租户内的用户。
2. 对于某些服务，可以选择将提供给新租户的存储。存储按位置分组。您可以从将提供给租户的位置和存储列表中进行选择。
   - 创建合作伙伴/文件夹租户时，可以为每个服务选择多个位置和存储。
   - 创建客户租户时，必须选择一个位置，然后在此位置中为每个服务选择一个存储。可以稍后更改向客户指派的存储，但前提是其使用量为 0 GB - 即在客户开始使用存储之前或客户从该存储中删除所有备份之后。有关存储空间使用情况的信息不会实时更新。请给予多达 24 小时的时间供信息进行更新。

   有关存储的详细信息，请参阅“管理位置和存储”。
3. 要为某个项目指定配额，请单击相应产品项目旁边的**无限制**链接。
   这些配额是“灵活的”。如果超出其中任意值，将向租户管理员和父租户的管理员发送电子邮件通知。不会对使用服务施加限制。对于合作伙伴租户，由于在创建合作伙伴租户时无法设置超额，因此预计产品项目使用情况可能会超过配额。
4. [仅当创建客户租户时] 指定配额超额。
   超额允许客户租户超出指定值的配额。当超出超额时，将限制使用相应的服务。
5. 单击**保存并关闭**。

新建的租户会显示在管理中控台的**客户**选项卡中。

如果要编辑租户设置或更改管理员，请在**客户**选项卡上选择租户，然后单击要编辑部分中的铅笔图标。

为多个现有租户启用服务

可以为多个租户(一个会话中最多 100 个租户) 批量启用服务、版本、包和产品项目。

此过程适用于子根、合作伙伴、文件夹和客户租户。可以同时选择这些不同类型的租户。

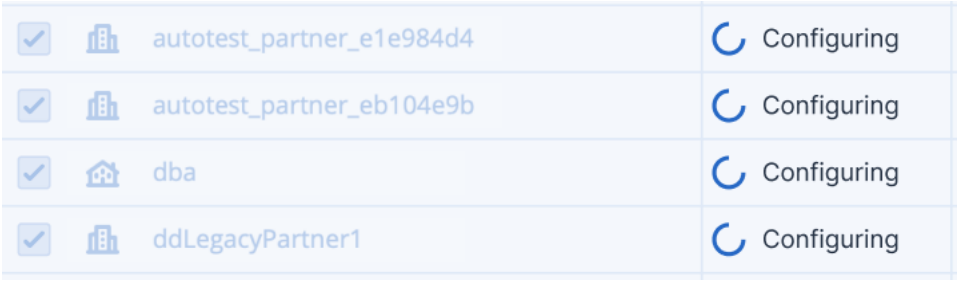
为多个租户启用服务

1. 在“管理”门户中，转到**客户端**。
2. 在右上角，单击**配置服务**。

3. 通过选中租户名称旁边的复选框，来选择要启用服务的每个租户，然后单击**下一步**。
4. 在**选择服务**部分中，选择要应用于所有选定租户的相关服务，然后单击**下一步**。

注意
无法在此屏幕中禁用以前启用的服务。开始此过程之前选择的所有服务、版本和产品项目将保持处于启用状态。

5. 在**配置服务**部分中，选择要为选定租户启用的服务功能和产品项目，然后单击**下一步**。
6. 在**概要**部分中，查看将应用于选定租户的更改。
   可以单击**全部展开**，以查看所有租户将应用的选定服务和产品项目。或者，可以展开每个租户以查看特定于该租户的选定服务和产品项目。
7. 单击**应用更改**。当为每个租户配置服务时，相应租户处于禁用状态，并且**租户状态**列指示当前正在配置服务和产品项目，如下所示。



8. 当服务和产品项目的配置成功应用于选定租户时，将显示一条确认消息。
   如果由于某种原因而无法将服务和产品项目应用于租户，则**租户状态**列会显示**未应用**。单击**重试**，以查看选定租户的配置。

启用维护通知

作为合作伙伴用户，可以允许子租户（合作伙伴和客户）直接从 Cyber Protect 数据中心接收维护通知电子邮件，并在管理门户内接收产品内维护通知。这将帮助您减少与维护相关的支持来电的数量。

注意
- 维护通知电子邮件由数据中心标记品牌。这些通知不支持自定义品牌。
- 不支持 VMware Cloud Director 用户的维护通知。

为子合作伙伴或客户启用维护通知

1. 以合作伙伴用户身份登录到管理门户，单击**客户端**，然后单击要为其启用维护通知的合作伙伴或客户租户的名称。
2. 单击**配置**。
3. 在**常规设置**选项卡上，找到**维护通知**选项并启用它。
   如果您没有看到**维护通知**选项，请联系服务提供商。

注意
维护通知已启用，但在选定租户为其用户启用通知或进一步将此选项传播给子合作伙伴或客户以为其用户启用通知之前，不会发送维护通知。

为用户启用维护通知

1. 以合作伙伴用户或公司管理员身份登录到管理门户。
   作为合作伙伴，可以访问由您管理的所有租户的用户。
2. 导航到**我的公司** > **用户**，然后单击要为其启用维护通知的用户的名称。
3. 在**服务**选项卡上的**设置**部分中，单击铅笔以编辑选项。
4. 选中**维护通知**复选框，然后单击**完成**。

选定用户将收到有关数据中心即将进行的维护活动的电子邮件通知。

启用有关已发现设备的通知

您可以为分配有以下角色的合作伙伴和客户用户帐户启用有关新发现设备的通知：

- 管理门户的管理员。
- 保护 中控台的管理员或网络管理员。

在这种情况下，系统将在每周一和周四发送电子邮件通知，其中包括以下信息：

- 对于客户管理员：上次检查后按设备类型分组的新发现的设备数量。
- 对于合作伙伴管理员：每位客户的新发现设备数。

若要启用已发现设备的通知

1. 以合作伙伴用户或公司管理员身份登录到管理门户。
2. 导航到**公司管理** > **用户**，然后单击要为其启用通知的用户的名称。
3. 在**服务**选项卡上的**设置**部分中，单击铅笔图标。
4. 选择**有关新发现设备的通知**，然后单击**完成**。

所选用户将收到有关在其公司网络中新发现的设备的电子邮件通知。

配置自我管理的客户资料

作为合作伙伴，可以为您管理的租户配置自我管理的客户资料。此选项允许您控制租户资料和联系信息对每个客户的可见性。

配置自我管理的客户资料

1. 在管理门户中，转到**客户端**。
2. 选择要为其配置自我管理的客户资料的客户端。
3. 选择**配置**选项卡，然后选择**常规设置**选项卡。
4. 启用或禁用**启用自我管理的客户资料**开关。

在启用自我管理的客户资料后，此客户端会在导航菜单中显示**公司资料**部分，并在用户创建向导中显示与联系人相关的字段(**公司电话**、**公司联系人**和**职位**)。

在启用自我管理的客户资料后，此客户端会在导航菜单中显示**公司资料**部分，并在用户创建向导中显示与联系人相关的字段(公司电话、公司联系人和职位)。

配置公司联系人

作为合作伙伴，您可以为贵公司和您管理的租户配置联系信息。我们会向此列表中的联系人发送有关平台中新功能和其他重要变化的更新。

可以添加多个联系人并指派公司联系人，具体取决于用户角色。可以从 Cyber Protect 平台中存在的用户创建联系人，也可以添加无权访问服务的人员的联系信息。

为公司配置联系人

1. 在管理中控台中，转到**我的公司** > **公司资料**。
2. 在**联系人**部分，单击 **+**。
3. 选择一个用于创建联系人的选项。
   - **从现有用户创建**
     - 从下拉列表中选择一个用户。
     - 选择公司联系人。
       - **计费** - 将获得有关在平台中报告的使用情况重要变化的更新的联系人。
       - **技术** - 将获得有关平台中技术重要变化的更新的联系人。
       - **业务** - 将获得有关平台中与业务相关重要变化的更新的联系人。

         可以为一个用户指派多个公司联系人。

       如果从公司资料的联系人列表中删除与某个用户关联的联系人，将不会删除该用户。系统会为该用户取消指派所有公司联系人，因此他们将不会再出现在**用户**列表的**公司联系人**列中。

       如果要更改与用户关联的联系人的电子邮件地址，系统会要求验证新定义的地址。将向该地址发送一封电子邮件，用户需要确认这一更改。
   - **创建新联系人**
     - 提供联系信息。
       - **名字** - 联系人的名字。此字段为必填项。
       - **姓氏** - 联系人的姓氏。此字段为必填项。
       - **公司邮箱** - 联系人的电子邮件地址。此字段为必填项。
       - **公司电话** - 此字段为可选字段。
       - **职位** - 此字段为可选字段。
     - 选择**公司联系人**。
       - **计费** - 将获得有关在平台中报告的使用情况重要变化的更新的联系人。
       - **技术** - 将获得有关平台中技术重要变化的更新的联系人。
       - **业务** - 将获得有关平台中与业务相关重要变化的更新的联系人。

         可以为一个用户指派多个公司联系人。
4. 单击**添加**。

为租户配置联系人

注意
如果修改子租户的联系信息，则所做的更改会对租户可见。

1. 在管理门户中，转到**客户端**。
2. 单击租户，然后单击**配置**。
3. 在**联系人**部分，单击 **+**。
4. 选择一个用于创建联系人的选项。
   - **从现有用户创建**
     - 从下拉列表中选择一个用户。
     - 选择公司联系人。
       - **计费** - 将获得有关在平台中报告的使用情况重要变化的更新的联系人。
       - **技术** - 将获得有关平台中技术重要变化的更新的联系人。
       - **业务** - 将获得有关平台中与业务相关重要变化的更新的联系人。

         可以为一个用户指派多个公司联系人。

       如果从公司资料的联系人列表中删除与某个用户关联的联系人，将不会删除该用户。系统会为该用户取消指派所有公司联系人，因此他们将不会再出现在**用户**列表的**公司联系人**列中。

       如果要更改与用户关联的联系人的电子邮件地址，系统会要求验证新定义的地址。将向该地址发送一封电子邮件，用户需要确认这一更改。
   - **创建新联系人**
     - 提供联系信息。
       - **名字** - 联系人的名字。此字段为必填项。
       - **姓氏** - 联系人的姓氏。此字段为必填项。
       - **公司邮箱** - 联系人的电子邮件地址。此字段为必填项。
       - **公司电话** - 此字段为可选字段。
       - **职位** - 此字段为可选字段。
     - 选择**公司联系人**。
       - **计费** - 将获得有关在平台中报告的使用情况重要变化的更新的联系人。
       - **技术** - 将获得有关平台中技术重要变化的更新的联系人。
       - **业务** - 将获得有关平台中与业务相关重要变化的更新的联系人。

         可以为一个用户指派多个公司联系人。
5. 单击**添加**。

刷新租户的使用情况数据

默认情况下，使用情况数据以固定时间间隔刷新。可以手动刷新租户的使用情况数据。

1. 在管理中控台中，转至**客户端**。
2. 单击租户，然后单击租户行中的省略号。

3. 选择**刷新使用情况**。

> **注意**
> 获取数据可能最多需要 10 分钟。

4. 重新加载页面以查看更新的数据。

禁用和启用租户

您可能需要暂时禁用租户。例如，如果租户有使用服务的欠款未付。

禁用租户

1. 在管理门户中，转到**客户端**。
2. 选择要禁用的租户，然后单击省略号图标 > **禁用**。
3. 单击**禁用**来确认操作。

结果：

- 租户及其所有子租户都将被禁用，他们的服务也将停用。
- 租户及其子租户的计费将继续，因为他们的数据将保留并存储在 Cyber Protect Cloud 中。
- 租户及其子租户中的所有 API 客户端都将被禁用，并且使用这些客户端的所有集成也都将停止工作。

要启用租户，请在客户端列表中选择它，然后依次单击省略号图标 > **启用**。

将一个租户移到另一个租户中

管理门户使您能够将租户从一个父租户移到另一个父租户中。如果要将客户从一个合作伙伴转移给另一个合作伙伴，或者如果您创建了一个文件夹租户来组织客户并想要将其中一部分客户移到新建的文件夹租户中，这可能很有用。

可以移动的租户类型

租户类型	可以移动	目标租户
合作伙伴	是	合作伙伴或文件夹
文件夹:	是	合作伙伴或文件夹
客户	是	合作伙伴或文件夹
单元	否	无

要求和限制

- 仅当目标父租户具有与原始父租户相同或更大的服务和产品项目集时，才能移动租户。
- 移动客户租户时，原始父租户中指派给客户租户的所有存储必须存在于目标父租户中。这是必需的，因为与客户服务相关的数据无法从一个存储移到另一个存储中。
- 在由服务提供商管理的客户租户中，可能有服务提供商级别的计划应用于客户工作负载(例如，脚本计划)。

  移动此类客户租户时，服务提供商的计划将从客户工作负载中撤消，并且与这些计划相关的所有服务都将停止为该客户工作。
- 可以在合作伙伴帐户层次结构中移动租户。还可以将一些客户租户移动到合作伙伴帐户层次结构之外的目标租户。要了解该操作是否可行，请联系您的客户经理。
- 只有管理员(例如，管理门户中的管理员或公司管理员)才能将租户移动到不同的父租户。

如何移动租户

1. 登录管理门户。
2. 查找并复制要将租户移动到的目标合作伙伴或文件夹租户的**内部 ID**。请执行以下操作：
   a. 在**客户**选项卡上，选择要将租户移动至的目标租户。
   b. 在“租户属性”面板上，单击垂直省略号图标，然后单击**显示 ID**。
   c. 复制**内部 ID** 字段中显示的文本字符串，然后单击**取消**。
3. 选择要移动的租户，然后将其移动到目标合作伙伴/文件夹。请执行以下操作：
   a. 在**客户**选项卡上，选择要移动的租户。
   b. 在“租户属性”面板上，单击垂直省略号图标，然后单击**移动**。
   c. 粘贴目标租户的内部标识符，然后单击**移动**。

该操作会立即开始，最多需要 10 分钟。

如果要移动的租户有子租户(例如，它是包含客户租户的合作伙伴或文件夹租户)，则整个租户子树会移动到目标租户。

将合作伙伴租户转换为文件夹租户，反之亦然

您可以通过管理门户将合作伙伴租户转换为文件夹租户。

如果您已将合作伙伴租户用于分组，并且现在想要正确组织租户基础架构，这可能很有用。如果您想要操作仪表板包含关于租户的汇总信息，这也很有用。

您还可以将文件夹租户转换为合作伙伴租户。

注意
此转换为安全操作，不会影响租户内的用户和任何服务相关数据。

转换租户的步骤

1. 登录管理门户。
2. 在**客户**选项卡上，选择要转换的租户。

3. 请执行以下任一操作：
   - 单击租户名称旁边的省略号图标。
   - 选择租户，然后单击“租户属性”面板上的省略号图标。
4. 单击**转换为文件夹**或**转换为合作伙伴**。
5. 确认您的决定。

限制对您的租户的访问

客户级别和更高级别的管理员可以限制更高级别的管理员对其租户的访问权限。

如果对租户的访问不受限制，父租户的管理员则将可以完全访问您的租户。他们将能够执行以下操作：

- 修改租户的属性
- 管理租户、用户和服务以供您的租户使用
- 访问租户中的备份和其他资源
- 获取租户、子租户和所有客户的使用情况报告。

如果对租户的访问受限，则父租户的管理员可以执行以下操作：

- 修改租户的属性
- 获取租户、子租户和所有客户的使用情况报告。

限制高级管理员对您的租户的访问

1. 登录到管理门户。
2. 转到**设置** > **安全**。
3. 禁用**支持访问**切换。

删除租户

您可能想要删除某个租户，以便释放其使用的资源。使用情况统计数据将在删除后的一天之内进行更新。对于大型租户，可能需要花费更长的时间。

在删除某个租户之前，需要先禁用它。有关如何执行此操作的详细信息，请参阅禁用和启用租户。

注意
虽然 Cyber Protect 提供了恢复租户的机会，但请注意，File Sync & Share 服务不支持恢复。

删除租户

1. 在管理门户中，转到**客户端**。
2. 选择要删除的已禁用租户，然后依次单击省略号图标 > **删除**。
3. 要确认操作，请输入登录名，然后单击**删除**。

结果：

- 将删除租户及其子租户。
- 将停用租户及其子租户内已启用的所有服务。
- 将删除租户及其子租户内的所有用户。
- 将注销租户及其子租户中的所有计算机。
- 将删除租户及其子租户中与服务有关的所有数据(例如，备份和同步文件)。
- 将删除租户及其子租户中的所有 API 客户端，并且使用这些客户端的所有集成也都将停止工作。
- 您将看到**租户状态**为**已删除**。当您将鼠标悬停在**已删除**状态上时，将看到删除租户的日期。

注意
您仍可以在此删除日期后的 30 天内恢复所有相关数据和设置。

恢复租户

如果租户被意外删除，Cyber Protect 允许 30 天内恢复租户。

例如，在以下情况下，您可能需要恢复租户：

- 合作伙伴意外删除了他的租户。
- 合作伙伴开发团队在测试其集成时，意外删除了一部分租户层次结构甚至整个租户层次结构。
- 合作伙伴集成意外取消调配应用程序，而不是切换到新版本，您需要恢复数据。
- 合作伙伴在切换到新许可时意外禁用了应用程序，您需要恢复已禁用应用程序中的数据。

恢复租户

1. 在管理门户中，转到**客户端**。
2. 在 **Cyber Protect** 选项卡上，找到要恢复的租户。其状态显示为**已删除**。
3. 将光标悬停在租户上方，然后单击省略号图标 。
4. 单击**恢复**。
   您将看到一个确认窗口，其中提示租户将恢复到删除前的状态，它将默认处于禁用状态。
5. [可选] 如果需要启用租户，请选中**我要启用租户**复选框。稍后可以随时启用租户。
6. 单击**恢复**。

结果：

- 将恢复租户及其子租户。
- 将重新启动租户及其子租户内已启用的所有服务。

注意
File Sync & Share 服务不支持恢复。

- 将恢复租户及其子租户内的所有用户。
- 将重新注册租户及其子租户中的所有计算机。
- 将恢复租户及其子租户中所有与服务有关的数据(例如，备份)。

- 将恢复租户及其子租户内的所有 API 客户端，使用这些客户端的所有集成都将重新开始工作。
- 您将看到**租户状态**为**活动**（如果已启用租户）或**已禁用**（如果尚未启用租户）。

管理用户

合作伙伴管理员、客户管理员和单位管理员可以在其可访问的租户下配置和管理用户帐户。

创建用户帐户

在以下情况下，您可能想创建其他帐户：

- 合作伙伴/文件夹管理员帐户 — 与其他人共享服务管理职责。
- 客户/潜在客户 - 将服务管理委派给访问权限严格限制在相应客户/潜在客户的其他人员
- 客户或单位租户中的用户帐户 — 使用户只能访问服务子集。

请注意，现有帐户无法在租户间移动。首先，您需要创建一个租户，然后用帐户填充。

创建用户帐户

1. 登录管理门户。
2. 导航到要在其中创建用户帐户的租户。请参阅 "导航管理门户"（第 28 页）。
3. 在右上角，依次单击**新建** > **用户**。
   或者，转到**我的公司** > **用户**，并单击 **+ 新建**。
4. 为帐户指定以下联系信息：
   - **电子邮件** - 此电子邮件地址还将用作登录名。。如果您喜欢使用不同于电子邮件地址的登录名，请选中**使用不同于电子邮件地址的登录名**复选框，然后输入**登录名**和**电子邮件**。

     重要事项
     每个帐户都必须有一个唯一的登录名。

   - **名** - 创建用户帐户和在文件夹中创建用户时，此字段为必填字段。
   - **姓** - 创建用户帐户和在文件夹中创建用户时，此字段为必填字段。
   - [可选] **公司电话**

     注意
     仅当父合作伙伴为客户租户启用了启用自我管理的客户资料选项时，才会在用户创建向导中显示**公司电话**、**职位**和**公司联系人**等字段。否则，这些字段不会显示。

   - [可选] **职位**
   - 在**语言**字段中，更改将用于此帐户的通知、报告和软件的默认语言。
5. [可选] 指定公司联系人。
   - **计费** - 将获得有关在平台中报告的使用情况重要变化的更新的联系人。
   - **技术** - 将获得有关平台中技术重要变化的更新的联系人。
   - **业务** - 将获得有关平台中与业务相关重要变化的更新的联系人。
     可以为一个用户指派多个公司联系人。

可以在**用户**列表的**公司联系人**列中查看为用户指派的公司联系人，并根据需要编辑用户帐户以更改公司联系人。

6. [在合作伙伴/文件夹租户中创建帐户时不可用]选择用户将有权访问的服务以及每个服务中的角色。

   服务是否可用取决于为在其中创建用户帐户的租户启用的服务。

   - 如果选中**公司管理员**复选框，用户将有权访问管理门户以及当前为租户启用的所有服务中的管理员角色。用户还将拥有将来为租户启用的所有服务中的管理员角色。
   - 如果选中**单位管理员**复选框，则用户将拥有对管理门户的访问权限，但可能有也可能没有服务管理员角色，具体取决于服务。
   - 否则，用户将具有您在为该用户启用的服务中对其指派的角色。

7. 单击**创建**。

新创建的用户帐户即会显示在**我的公司**下的**用户**选项卡中。

如果要编辑用户设置或为用户指定通知设置和配额(不适用于合作伙伴/文件夹管理员)，请在**用户**选项卡上选择用户，然后单击要编辑部分中的铅笔图标。

重置用户的密码

1. 在管理门户中，转到**我的公司** > **用户**。
2. 选择要重置其密码的用户，然后依次单击省略号图标 > **重置密码**。
3. 单击**重置**来确认操作。

现在，用户可以按照接收到的电子邮件中的指示进行操作，来完成重置过程。

对于不支持双重身份验证的服务(例如，在 Cyber Infrastructure 中注册)，可能需要将用户帐户转换为服务帐户。该账户不需要双重身份验证。

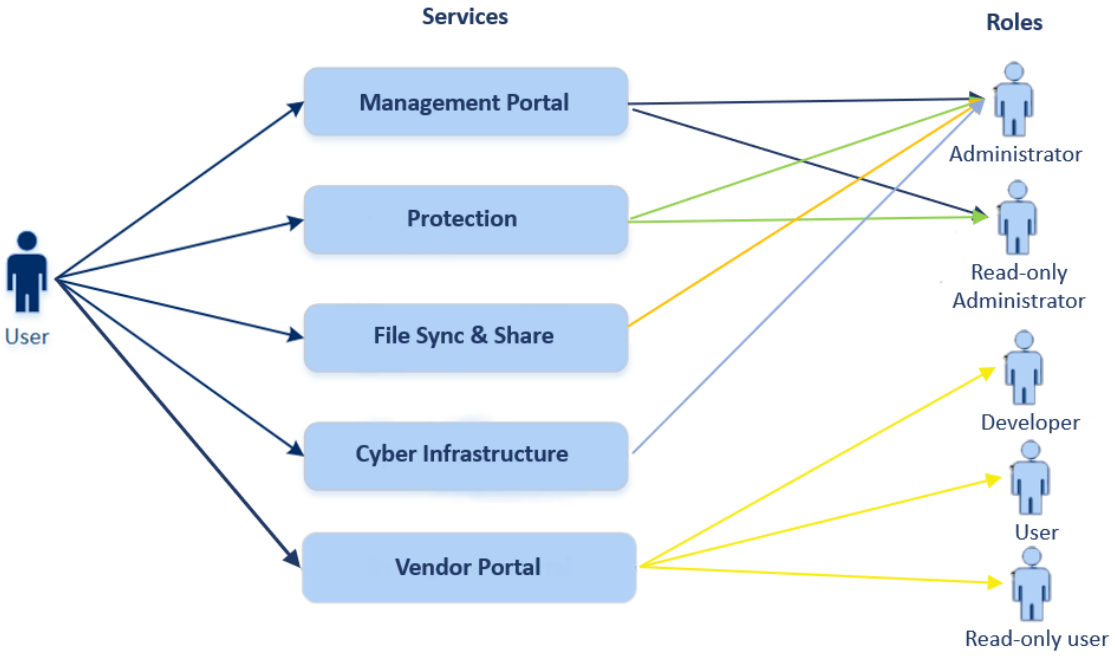
若要将用户帐户转换为服务帐户

1. 在管理门户中，转到**我的公司** > **用户**。
2. 选择要将其帐户转换为服务帐户类型的用户，然后依次单击省略号图标 > **标记为服务帐户**。
3. 在确认窗口中，输入双重身份验证代码并确认操作。

该帐户现在可用于不支持双重身份验证的服务。

每个服务可用的用户角色

一个用户可以有多个角色，但每个服务只能有一个角色。



对于每个服务，可以定义将分配给用户的角色。

注意
可用服务由您的服务提供商配置。

服务	角色	描述
不适用	公司管理员	此角色授予所有服务的完全管理员权限。 此角色授予对公司允许列表的访问权限。如果已为公司启用保护服务的Disaster Recovery附加组件，则此角色还可授予对灾难恢复功能的访问权限。
	单位管理员 单位级别	此角色授予单位中所有适用服务的最高权限。此角色不提供对灾难恢复功能的访问权限。
管理门户	管理员	此角色可以授予对管理门户的访问权限，其中管理员可以管理整个组织内的用户。
	只读管理员 合作伙伴级别	该角色提供对合作伙伴的管理门户和该合作伙伴所有客户的管理门户中所有对象的“只读”访问。请参阅 "只读管理员角色"(第 52 页)。
	只读管理员 客户级别	该角色提供对整个公司的管理门户中所有对象的“只读”访问。请参阅 "只读管理员角色"(第 52 页)。
	只读管理员 单位级别	该角色提供对公司单位和子单位的管理门户中所有对象的“只读”访问。请参阅 "只读管理员角色"(第 52 页)。

供应商门户	开发人员	此角色提供对供应商门户的完全访问权限。开发者可以创建和管理 CyberApp、CyberApp Descriptions 和 CyberApp Versions。他们还可以提交部署请求并监控 CyberApp 指标。
	用户	此角色允许用户创建、管理、并请求 CyberApp Descriptions 的批准。
	只读用户	此角色提供对供应商门户的只读访问权限。
保护	管理员	使用此角色可配置和管理您客户的保护服务。 此角色适用于： • 配置和管理Disaster Recovery功能。 • 配置和管理公司白名单。 • 执行设备的自动发现。 • 使用 DeployPilot 执行与软件部署相关的所有操作(与软件部署计划、软件存储库、软件包的操作以及执行快速部署操作)。
	网络管理员	除了“管理员”角色权限之外，此角色还支持配置和管理保护服务以及批准“网络安全脚本”中的操作。 “网络安全管理员”角色仅适用于启用了 Advanced Management (RMM) 包的租户。
	只读管理员	该角色将提供对保护服务的所有对象的“只读”访问权限。请参阅 "只读管理员角色"(第 52 页)。
	用户	此角色支持使用保护服务，但没有管理权限。为诸如 Endpoint Detection and Response 的功能提供访问权限，但指派了此角色的用户不能访问组织中其他用户的数据。
	还原操作者	适用于 Microsoft 365 和 Google Workspace 组织，该角色提供对备份的访问权限并允许恢复备份，同时限制对备份中敏感内容的访问。请参阅"还原操作者角色"(第 53 页)。
	安全分析师	只能在启用了 Advanced Security + EDR 或 Advanced Security + XDR 包的客户租户中指派此角色。它提供对网络安全保护中控台的访问，并使用户能够管理 EDR 事件并执行响应操作。
File Sync & Share	管理员	使用此角色可配置和管理您用户的“File Sync & Share”。
Cyber Infrastructure	管理员	使用此角色可配置和管理您用户的 Cyber Infrastructure。
合作伙伴门户	有许多角色可以指派给合作伙伴门户的用户。有关更多信息，请参见"合作伙伴门户角色"(第 178 页)。	
公证	管理员	使用此角色可配置和管理您用户的公证。
	用户	此角色支持使用“公证”服务，但没有管理权限。此类用户无法访问组织中其他用户的数据。

注意
供应商门户网站适用于 2023 年 10 月 4 日之后在 Acronis 技术生态系统网站上注册的技术合作伙伴。
如果您希望构建与 集成，并需要访问供应商门户和专用沙盒，请参阅集成章节这些说明进行操作。

与帐户和角色有关的任何更改会显示在**活动**选项卡上，并带有以下详细信息：

- 更改内容
- 更改者
- 更改的日期和时间

只读管理员角色

有此角色的帐户对 Cyber Protect 中控台拥有“只读”访问权限，可以执行以下操作：

- 收集诊断数据，如系统报告。
- 查看备份的恢复点，但无法深入了解备份内容，也无法查看文件、文件夹或电子邮件。
- 当启用 Advanced Security + XDR 后，只读管理员可以访问 EDR 事件屏幕中的响应操作选项卡，但无法执行任何操作。
- 在只读模式下访问组织中其他用户的数据。

“只读”管理员无法执行以下操作：

- 启动或停止任何任务。
  例如，只读管理员无法启动恢复，也无法停止正在运行的备份。
- 配置和管理 “Disaster Recovery” 功能或公司白名单，并且对软件部署计划、软件存储库和软件包具有只读访问权限。
- 访问源计算机或目标计算机上的文件系统。
  例如，只读管理员无法查看已备份计算机上的文件、文件夹或电子邮件。
- 更改任何设置。
  例如，只读管理员无法创建保护计划，也无法更改保护计划的任何设置。
- 创建、更新或删除任何数据。
  例如，只读管理员无法删除备份。

  注意
  在管理门户中，只读管理员可以启动新子租户的创建并配置其所有属性以供演示，但无法保存。

- 保存对脚本计划、监控计划或代理程序计划的任何更改。

除了保护计划的默认设置之外，所有只读管理员无法访问的 UI 对象都处于隐藏状态。这些设置将显示，但**保存**按钮处于不活动状态。

还原操作者角色

注意
此角色仅在保护服务中可用，并且仅限于 Microsoft 365 和 Google Workspace 备份。

还原操作者可以执行以下操作：

- 查看警报和活动。
- 查看并刷新备份列表。
- 查看恢复点列表。
- 浏览备份而不访问其内容。

  注意
  恢复操作员能够看到已备份文件的名称以及已备份邮件的收件人和发件人。

- 搜索备份(不支持全文搜索)。
- 仅恢复云到云备份至其在原始 Microsoft 365 或 Google Workspace 组织内的原始位置。

还原操作者无法执行以下操作：

- 删除警报。
- 添加或删除 Microsoft 365 或 Google Workspace 组织。
- 添加、删除或重命名备份位置。
- 删除或重命名备份。
- 在恢复备份时，可以创建、删除或重命名文件夹。
- 应用备份计划或运行备份。
- 访问已备份文件或已备份电子邮件的内容。
- 下载已备份文件或电子邮件附件。
- 将备份的云资源(例如电子邮件或日历项目)作为电子邮件发送。
- 查看或恢复 Microsoft 365 Teams 会话。
- 将云到云备份恢复到非原始位置，例如其他邮箱、OneDrive、Google Drive 或 Microsoft 365 Team。

用户角色和网络安全脚本权限

脚本和脚本计划的可用操作取决于脚本状态和您的用户角色。

管理员可以管理他们自己的租户及其子租户中的对象。他们无法查看或访问上级管理级别的对象(如果有)。

下级管理员对上级管理员应用于其工作负载的脚本计划仅有“只读”访问权限。

以下角色提供与网络安全脚本相关的权限：

- **公司管理员**
  此角色授予所有服务中的完全管理员权限。对于网络安全脚本，它授予与“网络安全管理员”角色相同的权限。
- **网络管理员**
  此角色授予完全权限，包括批准可以在租户中使用的脚本以及可以运行状态为**正在测试**的脚本。
- **管理员**
  此角色授予部分权限，可以运行批准的脚本以及创建和运行使用批准的脚本的脚本计划。
- **只读管理员**
  此角色授予有限权限，可以查看租户中使用的脚本和保护计划。
- **用户**
  此角色授予部分权限，可以运行批准的脚本以及创建和运行使用批准的脚本的脚本计划，但仅限于用户自己的计算机上。

下表汇总了所有可用操作，具体取决于脚本状态和用户角色。

角色	对象	脚本状态		
		方案	正在测试	已批准
网络管理员 **公司管理员**	脚本计划	编辑(从计划中删除草稿脚本) 删除 废除 禁用 停止	创建 编辑 应用 启用 运行 删除 废除 禁用 停止	创建 编辑 应用 启用 运行 删除 废除 禁用 停止
	脚本	创建 编辑 更改状态 克隆 删除 取消正在运行	创建 编辑 更改状态 运行 克隆 删除 取消正在运行	创建 编辑 更改状态 运行 克隆 删除 取消正在运行
管理员	脚本计划	查看	查看	创建

用户(针对他们自己的工作负载)		编辑 废除 禁用 停止	取消运行	编辑 应用 启用 运行 删除 废除 禁用 停止
	脚本	创建 编辑 克隆 删除 取消正在运行	查看 克隆 取消正在运行	运行 克隆 取消正在运行
只读管理员	脚本计划	查看	查看	查看
	脚本	查看	查看	查看

更改用户的通知设置

如果为创建用户的租户启用了 Cyber Protection 服务，则可以配置用户将通过电子邮件接收哪些通知。

若要为用户配置通知

1. 导航至**我的公司** > **用户**。
2. 单击要配置通知的用户，然后在**服务**选项卡的**电子邮件通知**部分中，单击铅笔图标。
3. 选择要启用的电子邮件通知的复选框。

通知	描述
维护通知	在 Cyber Protect 数据中心通知合作伙伴用户、子租户(合作伙伴和客户)以及个人用户即将进行的维护活动。合作伙伴用户可以为其子租户启用这些通知，合作伙伴用户或公司管理员也可以为其组织内的个人用户启用这些通知。
配额超限使用通知	已超出配额的相关通知。
预定使用	在每个月的第一天发送的使用情况报告。

通知	描述
情况报告	
URL 品牌推广通知	关于用于 Cyber Protect Cloud 服务的自定义 URL 的证书即将到期的通知。通知将在证书到期前的 30 天、15 天、7 天、3 天和 1 天发送给选定租户的所有管理员。
倒数计时至生产切换通知	在试用版到期前 10 天和到期前 3 天发送的有关客户试用版到期的通知。
生产模式激活通知	有关生产模式激活的通知。
失败通知	每个设备的保护计划执行结果和灾难恢复操作结果的相关通知。
警告通知	每个设备的保护计划执行结果和灾难恢复操作结果的相关通知。
成功通知	每个设备的保护计划执行结果和灾难恢复操作结果的相关通知。
活动警报的每日概述	每日概述是根据生成概述时 Cyber Protect 中控台中存在的活动警报列表生成的。该概述每天于 UTC 时间 10:00 和 23:59 之间生成并发送一次。生成并发送报告的具体时间取决于数据中心中的工作负载。如果当时没有活动警报，则不会发送概述。概述不包括不再有效的过去警告的信息。例如，如果用户发现失败的备份并清除警告，或者备份在生成概述之前重试并成功，则该警告将不再存在并且概述将不包括该警告。
设备控制通知	尝试使用保护计划(已启用设备控制模块)所限制的外围设备和端口的相关通知。
有关新发现设备的通知	有关新发现设备的通知。每周一和周四会发送这些通知。
恢复通知	针对以下资源的恢复操作的相关通知：用户电子邮件和整个邮箱、公用文件夹，OneDrive/GoogleDrive：整个 OneDrive 和文件或文件夹、SharePoint 文件，Teams：

通知	描述
	频道、整个团队、电子邮件和团队站点。 在这些通知的上下文中，以下操作将视为恢复操作：作为电子邮件发送、下载或启动恢复操作。
数据丢失预防通知	有关数据丢失防护警报的通知与此用户在网络上的活动有关。
安全事件通知	有关访问时、执行时和按需扫描期间检测到的恶意软件以及来自行为引擎和 URL 过滤引擎的检测的通知。 有两个选项可供选择：**已缓解**和**未缓解**。Endpoint Detection and Response (EDR) 事件警报、来自威胁源的 EDR 警报以及个别警报（未对其启用 EDR 的工作负载），这些选项是相关的。 在创建 EDR 警报后，将向相关用户发送一封电子邮件。如果事件的威胁状态发生变化，将发送一封新的电子邮件。该电子邮件中包含操作按钮，使用户能够查看事件的详细信息（如果事件已缓解），或调查和修复事件（如果事件未缓解）。
基础架构通知	有关Disaster Recovery基础架构出现问题时的通知：Disaster Recovery基础架构不可用或 VPN 隧道不可用时。

注意

VMware Cloud Director 用户可以收到以下通知：配额超限使用通知、计划使用情况报告（如果为组织配置了此类报告）和有关活动警报的每日摘要。

默认通知设置会根据设备类型和用户角色启用

默认启用或禁用的通知取决于通知类型和用户角色。

通知类型\用户角色	合作伙伴、文件夹管理员	客户、单位管理员（自助服务）	客户、单位管理员（由服务提供商管理）
维护通知	是 （默认对直接合作伙伴的用户启用，对非直接合作伙伴禁用）	否	否
配额过度使用通知	是	是	否
预定使用情况报告通知	是	是	否
URL 品牌推广通知	否	否	否
失败通知	否	否	否
警告通知	否	否	否

成功通知	否	否	否
活动警告的每日概述	否	是	否
设备控制通知	否	否	否
恢复通知	否	否	否
数据丢失预防通知	否	否	否
安全事件通知:已缓解	否	否	否
安全事件通知:未缓解	否	否	否
基础架构通知	否	否	否

按设备类型和用户角色默认启用通知

设备类型\用户角色	用户	客户和单元管理员	合作伙伴和文件夹管理员
自己设备的通知	是	是	不适用*
子租户的所有设备的通知	不适用	是	是
Microsoft 365、Google Workspace 和其他基于云的备份的通知	不适用	是	是

* 合作伙伴管理员无法注册自己的设备，但可以创建自己的客户管理员帐户并使用这些帐户添加自己的设备。请参阅用户帐户和租户。

禁用和启用用户帐户

您可能需要禁用某个用户帐户，以临时限制其对云平台的访问。

禁用用户帐户

1. 在管理门户中，转到**用户**。
2. 选择要禁用的用户帐户，然后依次单击省略号图标 > **禁用**。
3. 单击**禁用**来确认操作。

结果，该用户将无法使用云平台或接收任何通知。

注意
与禁用用户关联的所有设备将不再受到保护，因为不会对它们应用配额。要继续保护这些设备，请将它们重新分配给活动用户。

启用一个禁用的用户账户

1. 在管理门户中，转到**用户**。
2. 在用户列表中选择已禁用的用户，然后单击省略号图标  >**启用**。

删除用户帐户

您可能需要永久删除某个用户帐户，以释放其使用的资源（例如，存储空间或许可）。使用情况统计数据将在删除后的一天之内进行更新。对于带有大量数据的帐户，可能需要花费更长的时间。

注意
删除用户后，您可以重复使用已删除用户的登录。

在删除某个用户帐户之前，需要先禁用它。有关如何执行此操作的详细信息，请参阅禁用和启用用户帐户。

删除用户帐户

1. 在管理门户中，转到**用户**。
2. 选择已禁用的用户帐户，然后依次单击省略号图标 > **删除**。
3. 要确认操作，请输入登录名，然后单击**删除**。

结果：

- 将禁用为此帐户配置的所有通知。
- 将删除属于该用户帐户的所有数据。
- 管理员无法访问管理门户。
- 将删除与此用户关联的工作负载的所有备份。
- 将注销与该用户帐户关联的所有计算机。
- 将从与此用户关联的所有工作负载中撤消所有保护计划。
- 将删除属于此用户的所有 File Sync & Share 数据（例如，文件和文件夹）。
- 将删除属于此用户的公正数据（例如，公证文件、电子签名的文件）。
- 您将看到用户**状态**为**已删除**。将光标悬停在**已删除**状态的上方时，您将看到删除用户的日期，以及仍可以在此删除日期后的 30 天内恢复所有相关用户数据和设置的注释。

恢复用户帐户

由于可能会意外删除用户帐户，因此 Cyber Protection 让您有机会恢复用户帐户。

例如，在以下情况下，您可能需要恢复用户帐户：公司管理员已删除从公司离职的用户，但您仍需要在该用户下注册的所有资源。

恢复用户帐户

1. 在管理门户中，转到**我的公司** > **用户**。
2. 在**用户**选项卡上，找到要恢复的用户帐户。其状态显示为**已删除**。

3. 将光标悬停在用户帐户上方，然后单击省略号图标 。
4. 单击**恢复**。
   您将看到一个确认窗口，其中提示用户帐户将恢复到删除前的状态，它将默认处于禁用状态。
5. [可选] 如果需要启用用户帐户，请选中**我要启用用户**复选框。稍后可以随时启用用户帐户。
6. 单击**恢复**。

结果：

- 将恢复该用户帐户。
- 将恢复属于该用户帐户的所有数据。
- 将重新注册与该用户帐户关联的所有计算机。
- 您将看到用户状态为**活动**（如果已启用用户帐户）或**已禁用**（如果尚未启用用户帐户）。

转移用户帐户的所有权

如果您希望保留对受限用户的数据的访问，则可能需要转移用户帐户的所有权。

重要事项
无法重新指派已删除帐户的内容。

要转移用户帐户的所有权，请执行以下操作：

1. 在管理门户中，转到**用户**。
2. 选择要转移其所有权的用户帐户，然后在**一般信息**部分中单击铅笔图标。
3. 将现有电子邮件地址替换为将来帐户所有者的电子邮件地址，然后单击**完成**。
4. 单击**是**来确认操作。
5. 让将来帐户所有者按照发送到其邮箱中的说明来验证其电子邮件地址。
6. 选择要转移其所有权的用户帐户，然后依次单击省略号图标 > **重置密码**。
7. 单击**重置**来确认操作。
8. 让将来帐户所有者按照发送到其电子邮件地址的说明来重置密码。

现在，新的所有者可以访问该帐户。

设置双重身份验证

双重身份验证 (2FA) 是一种多因素身份验证，它通过使用两个不同因素的组合来检查用户身份：

- 用户知道的信息（PIN 或密码）
- 用户拥有的信息（令牌）
- 用户自身的信息（生物识别）

双重身份验证会对您帐户未经授权的访问提供额外保护。

该平台支持**基于时间的一次性密码 (TOTP)** 身份验证。如果在系统中启用了 TOTP 身份验证，那么用户必须输入其传统密码和一次性 TOTP 代码才能访问系统。换句话说，用户提供密码（第一重身

份验证)和 TOTP 代码(第二重身份验证)。在用户第二重身份验证设备上的身份验证应用程序中,系统基于当前时间和平台提供的机密信息(二维码或字母数字代码)来生成 TOTP 代码。

注意
对于生产模式下的合作伙伴租户,默认情况下会启用双因素身份验证,并且无法禁用。

对于客户租户,双因素身份验证是可选的,且可以禁用。

集成使用的合作伙伴管理员帐户必须转换为服务帐户。否则,集成将无法对 Cyber Protect Cloud 进行身份验证。例如,VMware Cloud Director 集成中的管理代理程序和备份代理程序的帐户是集成使用的帐户。有关如何创建服务帐户的详细信息,请参阅 "若要将用户帐户转换为服务帐户"(第 49 页)。

工作方式

1. 您基于贵组织级别启用双重身份验证。
2. 您组织的所有用户都必须在其第二重身份验证设备(手机、笔记本电脑、台式机或平板电脑)上安装身份验证应用程序。此应用程序将用于生成一次性 TOTP 代码。建议的身份验证器:
   - Google Authenticator
     iOS 应用程序版本 (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 应用程序版本 (https://apps.apple.com/app/microsoft-authenticator/id983156458)
     Android 版本 (https://play.google.com/store/apps/details?id=com.azure.authenticator)

   重要事项
   用户必须确保已安装身份验证应用程序的设备上的时间正确设置并反映当前实际时间。
3. 您的组织用户必须重新登录系统。
4. 输入登录名和密码后,系统将提示他们为其用户帐户设置双重身份验证。
5. 他们必须使用其身份验证应用程序扫描二维码。如果无法扫描二维码,他们可以使用二维码下方显示的 32 位代码,然后在身份验证应用程序中手动添加它。

   重要事项
   强烈建议您保存它(打印二维码、写下临时一次性密码 (TOTP) 机密信息、使用支持在云中备份代码的应用程序)。如果第二重身份验证设备丢失,您需要使用临时一次性密码 (TOTP) 来重置双重身份验证。
6. 将在身份验证应用程序中生成临时一次性密码 (TOTP) 代码。它会每隔 30 秒自动重新生成。
7. 用户在输入其密码后,必须在**设置双重身份验证**窗口上输入 TOTP 代码。
8. 结果,将为用户设置双重身份验证。

现在，当用户登录系统时，系统会要求他们提供登录名和密码，以及在身份验证应用程序中生成的一次性 TOTP 代码。用户可以在登录系统后将浏览器标记为受信任，则后续通过此浏览器登录时不会要求输入 TOTP 代码。

在新设备上恢复双重身份验证

如果您可以访问以前设置的移动身份验证应用程序：

1. 在新设备上安装身份验证器应用程序。
2. 使用在设备上设置 2FA 时保存的 PDF 文件。此文件包含必须在身份验证器应用程序中输入的 32 位代码，才能将该身份验证器应用程序重新链接到您的 Acronis 帐户。

   重要事项
   如果代码正确但不起作用，请确保在身份验证器移动应用程序中同步时间。

3. 如果您在设置过程中并未保存 PDF 文件：

a. *单击**重置 2FA**，并输入在以前设置的移动身份验证器应用程序中显示的一次性密码。*
b. 按照屏幕上的说明操作。

如果您无法访问以前设置的移动身份验证器应用程序：

1. 拿取一个新的移动设备。
2. 使用存储的 PDF 文件来链接新设备（默认文件名为 `cyberprotect-2fa-backupcode.pdf`）。
3. 通过备份恢复对您帐户的访问权限。确保您的移动应用程序支持备份。
4. 从该应用程序支持的另一个移动设备，使用同一帐户打开该应用程序。

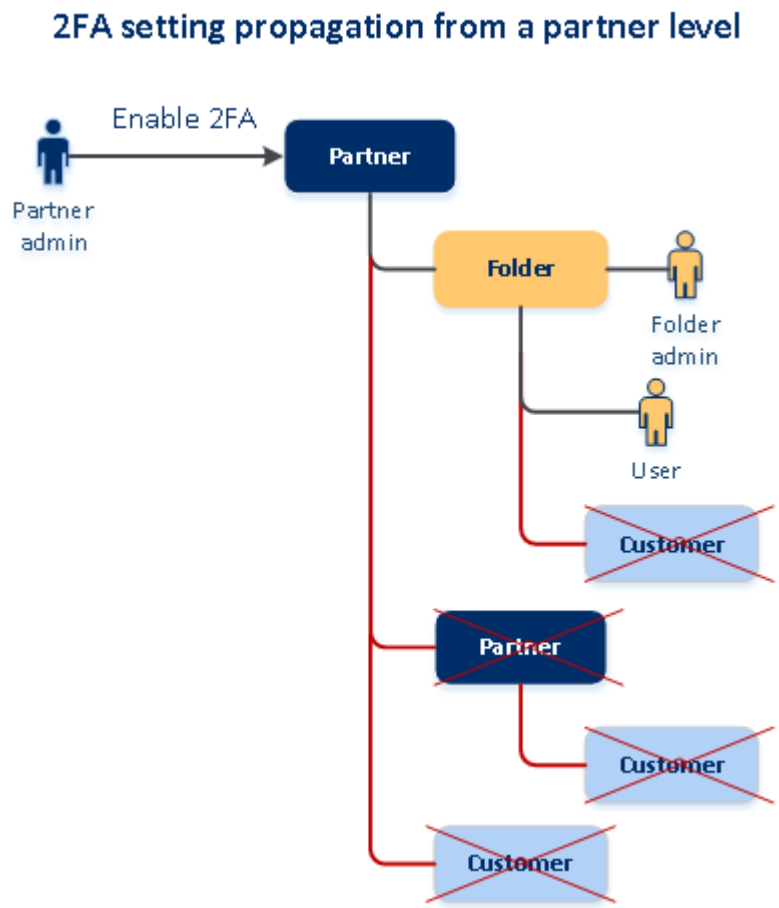
租户级别的双重身份验证设置传播

双重身份验证基于**组织**级别设置。可以启用或禁用双重身份验证：

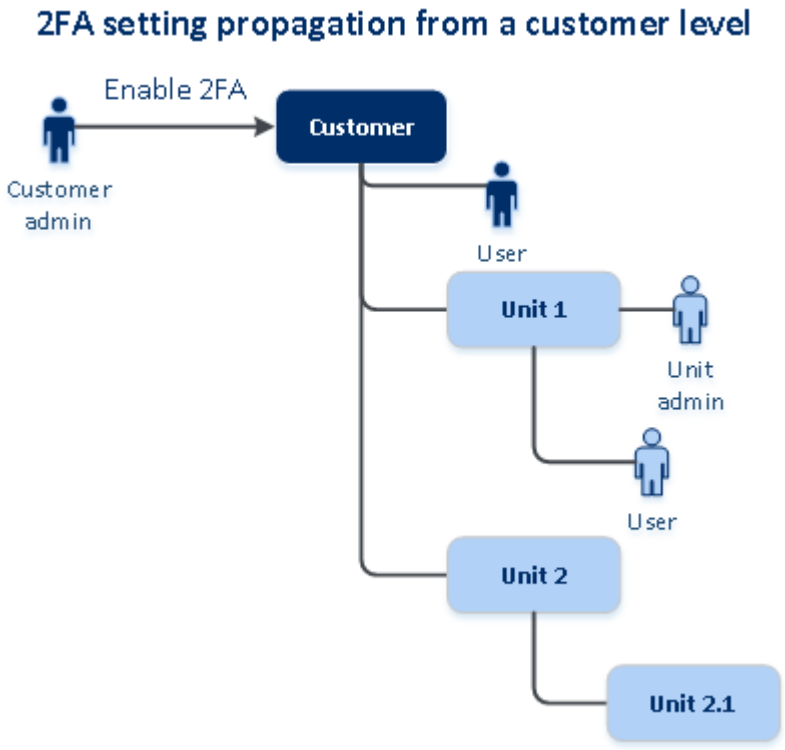
- 为您自己的组织。
- 为您的子租户（仅在该子租户中启用**支持访问**选项时）。

双重身份验证设置会在租户级别传播，如下所示：

- 文件夹自动继承其合作伙伴组织的双重身份验证设置。在以下方案中，红线意味着无法传播双重身份验证设置。



- 单位自动继承其客户组织的双重身份验证设置。



注意

1. 可以为您的子组织启用或禁用双重身份验证(仅在该子组织中启用**支持访问**选项时)。
2. 可以管理子组织的用户的双重身份验证设置(仅在该子组织中启用**支持访问**选项时)。
3. 无法基于文件夹或单位级别设置双重身份验证。
4. 即使您的父组织未启用此设置,您也可以配置双重身份验证设置。

为租户设置双重身份验证

从 24.09 版本开始,默认情况下,生产模式下的所有合作伙伴租户(直接和间接)都启用了双因素身份验证 (2FA),且无法禁用。

试用合作伙伴的帐户只有在切换到生产模式时,2FA 才会自动启用。

对于服务帐户(已禁用双因素身份验证的用户)的支持将继续。合作伙伴管理员仍可通过将用户转换为服务帐户来临时禁用用户的双因素身份验证。现有服务帐户不受影响,这对于使用基本身份验证的自定义集成非常重要,因为它与双因素身份验证不兼容。此类集成的建议解决方案是将其迁移到 API 客户端。

对于"客户"租户,不会强制执行 2AF,但我们强烈建议他们为其组织启用双因素身份验证。作为合作伙伴管理员,您可以扮演"客户"管理员并为您管理的客户启用 2AF。

若要启用双重身份验证

所需角色:合作伙伴管理员

1. 请登录管理门户。
2. 导航至**客户**并选择要启用双因素身份验证的客户租户。
3. 转到**设置** > **安全**。
4. 滑动**双重身份验证**开关,然后单击**启用**。

现在,组织中的所有用户都必须为其帐户设置双重身份验证。当他们下次尝试登录或其当前会话到期时,系统会提示他们执行此操作。

开关下的进度栏显示有多少用户已为其帐户设置了双重身份验证。要检查哪些用户已配置其帐户,请导航到**我的公司** > **用户**选项卡,然后检查**2FA 状态**列。尚未为其帐户配置双重身份验证的用户的 2FA 状态为**需要设置**。

在成功配置双重身份验证后,用户每次登录到服务中控台时都需要输入其登录名、密码和 TOTP 代码。

若要禁用双重身份验证

所需角色:合作伙伴管理员

1. 请登录管理门户。
2. 导航至**客户**并选择要禁用双因素身份验证的客户租户。
3. 转到**设置** > **安全**。
4. 要禁用双重身份验证,请关闭开关,然后单击**禁用**。

5. [如果组织中至少有一个用户配置了双重身份验证]输入在移动设备上的身份验证应用程序中生成的 TOTP 代码。

由此，系统会为组织禁用双重身份验证、删除所有机密信息以及忘记所有受信任的浏览器。所有用户将仅使用其登录名和密码登录系统。在**我的公司** > **用户**选项卡上，将隐藏 **2FA 状态**列。

管理用户的双重身份验证

可以在管理门户的**我的公司** > **用户**选项卡下，监视所有用户的双重身份验证设置并重置设置。

监控

在管理门户的**我的公司** > **用户**下，可以查看组织中所有用户的列表。**2FA 状态**指示是否已为用户设置了双重身份验证配置。

为用户重置双重身份验证

1. 在管理门户中，转到**我的公司** > **用户**。
2. 在**用户**选项卡上，查找要更改设置的用户，然后单击省略号图标。
3. 单击**重置双重身份验证**。
4. 输入在第二重身份验证设备上的身份验证应用程序中生成的 TOTP 代码，然后单击**重置**。

结果，用户将可以再次设置双重身份验证。

为用户重置受信任的浏览器

1. 在管理门户中，转到**我的公司** > **用户**。
2. 在**用户**选项卡上，查找要更改设置的用户，然后单击省略号图标。
3. 单击**重置所有受信任的浏览器**。
4. 输入在第二重身份验证设备上的身份验证应用程序中生成的 TOTP 代码，然后单击**重置**。

已为其重置所有受信任的浏览器的用户在下次登录时将需要提供 TOTP 代码。

用户可以重置所有受信任的浏览器，以及自行重置双重身份验证设置。可以在他们登录系统后执行这一操作，方法是单击相应链接并输入 TOTP 代码确认操作。

为用户禁用双重身份验证

不建议您禁用双重身份验证，因为这可能会导致破坏租户安全性。

此外，还可以为某个用户禁用双重身份验证，并为租户的所有其他用户保留双重身份验证。这是一个针对以下情况的解决方法：当在租户内启用双重身份验证时，其中云集成已配置且该集成允许通过用户帐户（登录密码）访问平台。为了能够继续使用集成，临时解决方案是：可以将用户转换为不适用双重身份验证的服务帐户。

重要事项
不建议将普通用户切换为服务用户来禁用双重身份验证，因为这会给租户安全性带来风险。

为在不禁用双重身份验证的情况下使用云集成的租户建议的安全解决方案是：创建 API 客户端并将您的云集成配置为供它们使用。

1. 在管理门户中，转到**我的公司 > 用户**。
2. 在**用户**选项卡上，查找要更改设置的用户，然后单击省略号图标。
3. 单击**标记为服务帐户**。结果，用户处于称为**服务帐户**的特殊双重身份验证状态。
4. [如果租户中至少有一个用户配置了双重身份验证] 输入在第二重身份验证设备上的身份验证应用程序中生成的 TOTP 代码以确认禁用。

为用户启用双重身份验证

可能需要为之前已禁用双重身份验证的特定用户重新启用它。

1. 在管理门户中，转到**我的公司 > 用户**。
2. 在**用户**选项卡上，查找要更改设置的用户，然后单击省略号图标。
3. 单击**标记为常规帐户**。结果，用户将需要设置双重身份验证，或在进入系统时提供 TOTP 代码。

在第二重身份验证设备丢失的情况下重置双重身份验证

要在第二重身份验证设备丢失的情况下重置对您帐户的访问权限，请按照以下建议的方法之一操作：

- 从备份恢复您的 TOTP 机密信息（二维码或字母数字代码）。
  使用另一台第二重身份验证设备，并将保存的 TOTP 机密信息添加到该设备上安装的身份验证应用程序中。
- 请求管理员为您重置双重身份验证设置。

蛮力防护

蛮力攻击是如下一种攻击：入侵者尝试获取系统的访问权限时会提交许多密码，希望能够正确猜测到一个密码。

平台的蛮力防护机制基于设备 Cookie。

系统会预定义平台中所使用的蛮力防护的设置：

参数	输入密码	输入 TOTP 代码
尝试限制	10	5
尝试限制时长（超时后会重置该限制）	15 分钟（900 秒）	15 分钟（900 秒）
锁定发生时间	尝试限制 + 1（第 11 次尝试）	尝试限制
锁定时长	5 分钟（300 秒）	5 分钟（300 秒）

如果已启用双重身份验证，则只有在使用这两个因素（密码和 TOTP 代码）成功进行身份验证后，才会向客户端（浏览器）发布设备 Cookie。

对于受信任的浏览器，则在仅使用一个因素（密码）成功进行身份验证后发布设备 Cookie。

TOTP 代码输入尝试基于用户（而非设备）记录。这意味着，即使某个用户尝试使用不同设备输入 TOTP 代码，他们仍会遭阻止。

为客户配置追加销售方案

追加销售是一种邀请您的客户购买其他功能的技术。

您可能想要为使用标准版 Cyber Protect 功能的现有客户推销更高级的功能。

您可以按客户启用或禁用升级销售功能。默认情况下，升级销售选项已启用。您的客户将看到不可用的附加功能，直到客户购买为止。此附加功能标有绿色高亮显示的推广的高级包的名称或图标。当客户单击升级销售点时，将显示对话框，建议客户启用所需的高级包。如果客户单击**启用所需的高级包**链接，则会打开确认对话框。如果客户单击**启用**按钮并且购买 URL 在合作伙伴级别上已配置，则会将客户重定向到该 URL。

若要配置购买链接

您可以配置 **启用** 按钮的链接，以便将客户重定向到您的网站以购买高级服务。

1. 在“管理”门户的导航菜单中，选择 **设置** > **品牌**。
2. 在**追加销售**部分，编辑 **Buy URL** 字符串的值。

注意
可以在合作伙伴和文件夹级别上配置品牌。品牌应用于租户（品牌配置于其中）的所有直接和间接子合作伙伴/文件夹以及客户。

若要为客户禁用追加销售功能

1. 在管理门户中，转到**客户端**。
2. 选择客户，转到右窗格，单击**配置**选项卡，然后单击**常规设置**。
3. 在 **追加销售** 部分，禁用“**推广高级保护选项**”以关闭所选客户的追加销售方案。

向客户显示的追加销售点

白名单

白名单菜单已添加到 **保护** > **防恶意软件**下。

当某公司具有可能被防病毒解决方案识别和检测为“误报”的公司特定的应用程序时，将受信任的应用程序手动添加到白名单也可能会很耗时。白名单可以自动化将此类应用程序添加到允许列表的过程。“防病毒和防恶意软件保护”模块会扫描备份并分析扫描的数据，以将此类应用程序加入允许列表并防止出现误报检测。

此追加销售点推广 Advanced Security 包。

创建或编辑保护计划

在客户创建或编辑保护计划时，向客户展示以下各包的各种高级功能。

- Advanced Backup
- Advanced Management (RMM)
- Advanced Data Loss Prevention
- 防病毒和防恶意软件保护
- Advanced Security + XDR

数据丢失预防

数据丢失预防追加销售点位于 Cyber Protection 中控台的 **保护**菜单项下。

此追加销售点关于推广“Advanced Data Loss Prevention”包。

管理位置和存储

设置 > **位置**部分中显示云存储和灾难恢复基础架构，可以使用这些基础架构来为合作伙伴和客户提供 **Cyber Protection** 和 **File Sync & Share** 服务。

在将来的版本中，为其他服务配置的存储将显示在**位置**部分。

位置

位置是一个容器，它使您可以方便地对云存储和灾难恢复基础架构进行分组。它可以代表您所选择的任何内容，如特定的数据中心或基础架构组件的地理位置。

您可以创建任意数量的位置，并使用备份存储、灾难恢复基础架构和**File Sync & Share**存储填充它们。一个位置可以包含多个云存储，但仅可包含一个灾难恢复基础架构。

有关存储操作的信息，请参阅 "管理存储"(第 69 页)。

为合作伙伴和客户选择位置和存储

创建合作伙伴/文件夹租户时，您可以选择多个位置以及在这些位置中为每个服务选择多个在新租户中可用的存储。

创建客户租户时，必须选择一个位置，然后在此位置中为每个服务选择一个存储。可以稍后更改向客户指派的存储，但前提是其使用量为 0 GB - 即在客户开始使用存储之前或客户从该存储中删除所有备份之后。

在**客户**选项卡上选择某个租户后，有关指派给该客户租户的存储的信息将显示在“租户详细信息”面板中。有关存储空间使用情况的信息不会实时更新。请给予多达 24 小时的时间供信息进行更新。

有关地理冗余的信息，请参阅 "地理冗余存储"(第 74 页)。

与位置有关的操作

若要创建新位置，请单击**添加位置**，然后指定位置名称。

若要将存储或灾难恢复基础架构移动到其他位置，请选择存储或基础架构，单击**位置**字段中的铅笔图标，然后选择目标位置。

若要重命名位置，请单击位置名称旁边的省略号图标，单击**重命名**，然后指定新的位置名称。

若要删除位置，请单击位置名称旁边的省略号图标，单击**删除**，然后确认您的决定。仅可删除空位置。

管理存储

添加新存储

- **Cyber Protection** 服务：
  - 默认情况下，备份存储位于 数据中心中。
  - 如果上级管理员为合作伙伴租户启用了**合作伙伴拥有的备份存储**产品项目，则合作伙伴管理员可以通过使用 Cyber Infrastructure 软件来组织合作伙伴自己数据中心中的存储。单击**位置**部分的**添加备份存储**，可查找有关在您自己的数据中心中组织备份存储的信息。
  - 如果上级管理员为合作伙伴租户启用了**合作伙伴拥有的灾难恢复基础架构**产品项目，则合作伙伴管理员可以组织合作伙伴自己的数据中心中的灾难恢复基础架构。有关如何添加灾难恢复基础架构的信息，请联系技术支持。

注意
无法对 数据中心所使用的公共云对象存储(例如 Amazon S3、Microsoft Azure、Google Cloud Storage 和 Wasabi)进行备份验证。
可以对 合租伙伴所使用的公共云对象存储进行备份验证。但是，不建议启用它，因为验证操作会增加这些公共对象存储的流出流量，并可能会导致产生大量费用。

- 有关如何添加将由其他服务使用的存储的信息，请联系技术支持。

删除存储

可以删除由您或您的子租户添加的存储。

如果已将存储指派给任何客户租户，则必须在删除存储之前，为所有客户租户禁用使用存储的服务。当存储的使用量为零时，可以删除存储。

删除存储

1. 登录管理门户。
2. 导航到租户(已将存储添加到其中)。
3. 依次单击**设置** > **位置**。
4. 选择要删除的存储。
5. 在"存储属性"面板上，单击省略号图标，然后单击**删除存储**。
6. 确认您的决定。

不可变存储

不可变存储是一种数据存储类型，可在定义的时间段内防止备份被更改、修改或删除。它可确保数据保持安全和防篡改，提供了一层额外的保护，可防止未经授权或意外修改或勒索软件攻击。不可变存储可用于所有存储在支持的云存储实例中的云备份。请参阅 "支持的存储和代理程序"(第 70 页)。

通过使用不可变存储，可以在指定的保留期内访问已删除的备份。可以从这些备份中恢复内容，但不能更改、移动或删除这些备份。在保留期结束后，将永久删除已删除的备份。

不可变存储包含以下备份：

- 手动删除的备份。
- 根据保护计划中**保留时间**部分或清理计划中**保留规则**部分中的设置自动删除的备份。

不可变存储中已删除的备份仍会使用存储空间并收取相应费用。

已删除的租户无需支付任何存储费用，包括不可变存储。

不可变存储模式

对于合作伙伴租户，无法选择不可变存储模式。合作伙伴可以禁用或重新启用另一个合作伙伴或客户租户的不可变存储，并设置保留期。

客户管理员可以禁用和重新启用不可变存储，并更改其模式和保留期。

不可变存储在以下模式下可用：

- **监管模式**
  您可以禁用并重新启用不可变存储。您可以更改保留期限或切换到合规模式。

  注意
  从 2024 年 9 月开始，默认情况下，对于所有合作伙伴和客户租户，所有 Acronis 托管的存储中启用了保留期为 14 天的不可变存储治理模式。有关详细信息，请参阅 此 KB 文章。

- **合规模式**

  警告！
  选择合规模式是不可逆的。

  您无法禁用不可变存储。您无法更改保留期限，也无法切换回监管模式。

支持的存储和代理程序

- 仅云存储支持不可变存储。
  - 不可变存储适用于使用 4.7.1 或更高 Cyber Infrastructure 版本的 Acronis 托管和合作伙伴托管云存储。
  - 所有具有 Cyber Infrastructure Backup 网关的存储均受支持。例如， Cyber Infrastructure 存储、Amazon S3 和 EC2 存储以及 Microsoft Azure 存储。

  - 不可变存储要求在 Cyber Infrastructure 中为备份网关服务打开 TCP 端口 40440。在版本 4.7.1 及更高版本中，使用**备份 (ABGW) 公共**流量类型自动打开 TCP 端口 40440。有关流量类型的详细信息，请参阅Acronis Cyber Infrastructure 文档。
- 不可变存储需要版本为 21.12(内部版本 15.0.28532) 或更高版本的保护代理程序。
- 仅支持 TIBX(版本 12) 备份。

配置不可变存储

2024 年 9 月之后，默认情况下，对于所有合作伙伴和客户租户，将启用治理模式下的不可变存储，保留期为 14 天。

注意
为了允许访问已删除的备份，应该启用备份存储上的 40440 端口以接收传入的连接。

若要配置不可变存储

在合作伙伴租户中

1. 以管理员身份登录到管理门户，然后转到**设置** > **安全**。
2. 请验证**不可变存储**开关是否打开。
3. 在 14 天到 3650 天的范围内指定保留期。
   默认的保留期为 14 天。较长的保留期会导致存储使用量增加。
4. 单击**保存**。

在客户租户中

1. 以管理员身份登录到管理门户，然后转到**客户**。
2. 若要编辑客户租户的设置，请单击租户名称。
3. 在导航菜单中，转到**设置** > **安全**。
4. 请验证**不可变存储**开关是否打开。
5. 在 14 天到 3650 天的范围内指定保留期。
   默认的保留期为 14 天。较长的保留期会导致存储使用量增加。
6. 选择不可变存储模式，如果出现提示，请确认您的选择。
   - **监管模式**
     此模式可确保勒索软件或恶意操作者无法篡改或删除备份数据，因为所有已删除的备份都将在不可变存储中保留您指定的保留期。此外，它还可确保备份数据的完整性，这对于灾难恢复至关重要。
     在此模式中，您可以禁用并重新启用不可变存储、更改保留期限或切换到合规模式。
   - **合规模式**
     除了监管模式的优点外，合规模式还有助于组织满足数据保留和安全的法规要求，因为它可以防止数据篡改。

警告！
选择合规模式是不可逆的。选择此模式后，您无法禁用不可变存储、更改保留期或切换回监管模式。

7. 单击**保存**。
8. 若要将现有存档添加到不可变存储中，请通过手动或预定运行相应的保护计划，在该存档中创建新的备份。

警告！
如果在将存档添加到不可变存储之前删除备份，备份将被永久删除。

禁用不可变存储

在合作伙伴租户中

1. 以管理员身份登录到管理门户，然后转到**设置** > **安全**。
2. 禁用**不可变存储**开关。

重要事项
此更改仅将继承给默认未启用不可变存储且客户级别的不可变存储设置未更改的子租户。
从 24.09 版本开始，不可变存储默认在客户租户中启用。若要按数据中心检查启用状态，请参阅此知识库文章。在合作伙伴级别禁用不可变存储不会影响这些租户。若要禁用不可变存储，请转到客户租户。

警告！
禁用不可变存储不会立即生效。在 14 天(336 小时)的宽限期内，您可以根据原始保留期访问已删除的备份。
宽限期结束时，所有AMS中的备份将被永久删除。例如，如果您在 10 月 1 日上午 10:00 禁用 AMS，则在 10 月 15 日上午 10:00 仍在 AMS 中的所有备份将被永久删除。

3. 单击**禁用**来确认选择。

在客户租户中

1. 以管理员身份登录到管理门户，然后转到**客户**。
2. 若要编辑客户租户的设置，请单击租户名称。
3. 在导航菜单中，转到**设置** > **安全**。
4. 禁用**不可变存储**开关。

注意
只能在监管模式下禁用不可变存储。

警告！
禁用不可变存储不会立即生效。在 14 天(336 小时)的宽限期内，您可以根据原始保留期访问已删除的备份。
宽限期结束时，所有AMS中的备份将被永久删除。例如，如果您在 10 月 1 日上午 10:00 禁用 AMS，则在 10 月 15 日上午 10:00 仍在 AMS 中的所有备份将被永久删除。

5. 单击**禁用**来确认选择。

查看不可变存储使用情况

您可以在 Cyber Protect 中控台或在管理门户中生成的**当前使用情况**报告中查看不可变存储占用的空间。

限制

- 报告的值包括存储中所有已删除备份的总大小和备份存档的元数据。元数据可达到报告的值的 10%。
- 该值显示生成报告前 24 小时的使用情况。
- 如果实际使用量小于 0.01 GB，则会显示为 0.0 GB。

查看不可变存储使用情况

在 Cyber Protect 中控台中

1. 登录到 Cyber Protect 中控台。
2. 转到 **备份存储** > **备份**，然后选择支持不可变存储的云存储位置。
3. 检查**不可变存储和元数据**列。

在当前使用情况报告中

1. 以管理员身份登录到管理门户。
2. 转到 **报告** > **使用情况**。
3. 选择 **即时**。
4. 选择 **当前使用情况**，然后单击**生成并发送**。
   将以 CSV 和 HTML 格式的报告发送到您的电子邮件地址。
   HTML 文件包含在 ZIP 存档中。
5. 在报告中，勾选**指标名称**列。
   您可以在 **云存储 - 不可变**行中查看不可变存储使用情况。

不可变存储的计费示例

下面的示例显示了一个已删除的备份，该备份转到保留期为 14 天(这是默认保留期)的不可变存储。在此期间，已删除的备份会占用存储空间。在保留期结束后，将永久删除已删除的备份，存储使用量会降低。每个月都会相应地收取存储使用费。

日期	备份	存储使用情况	计费
4 月 1 日	备份 A (10 GB) 已创建 备份 B (1 GB) 已创建	10 GB + 1 GB = 11 GB	
4 月 20 日	备份 B 已删除，转到不可变存储 (保留期为 14 天)	10 GB + 1 GB = 11 GB	
4 月 30 日			4 月份计费的存储使用量为 11 GB
5 月 4 日	备份 B 已因其保留期结束而永久删除	11 GB - 1 GB = 10 GB	
5 月 31 日			5 月份计费的存储使用量为 10 GB

地理冗余存储

使用地理冗余存储，备份数据会异步复制到与主要备份位置相距较远的复制位置。因此，即使主要位置不可用，数据仍然持久且具有可访问性。

复制的数据会占用与原始数据相同的存储空间。

限制

- 并非所有数据中心均可使用地理冗余存储。
- 仅支持云存储的地理冗余。它不支持第三方存储，例如合作伙伴托管存储或公共云存储。
- 复制数据的位置取决于您的数据中心。有关详细信息，请参阅此知识库文章。
- 使用"Disaster Recovery"的地理冗余存储时，还存在其他限制。
  有关更多信息，请参阅Cyber Protect Cloud文档。

调配地理冗余存储

在管理门户中为客户租户调配后，地理冗余存储才会在客户租户中可用。

若要调配地理冗余存储

1. 以管理员身份登录到管理门户。
2. 在**客户端**中，单击租户名称旁边的省略号按钮 (...)> **配置**。
3. 在**保护**选项卡中，单击**编辑**。
4. 在 **云资源**下，找到要启用地理冗余的存储。
5. 在**地理冗余**旁边，单击 **启用**。
6. 单击**保存**。

由此，地理冗余云存储在此客户租户中可用，但它不会自动启用。若要使用地理冗余存储，请在 Cyber Protect 中控台中启用它。请参阅 "启用地理冗余存储"(第 75 页)。

有关在多个租户中调配地理冗余存储的更多信息，请参阅 "为多个现有租户启用服务"(第 39 页)。

启用地理冗余存储

先决条件

- 已将支持地理冗余的存储指派给客户租户。请参阅 "为合作伙伴和客户选择位置和存储"(第 68 页) 。
- 在管理门户中为客户租户调配地理冗余存储。请参阅 "调配地理冗余存储"(第 74 页) 。
  如果指派了不兼容的存储(例如合作伙伴托管的存储) , 则无法调配地理冗余存储。

您可以在 Cyber Protect 中控台的主屏幕或 **设置** 选项卡上启用地理冗余存储。两种程序的结果相同。

若要启用地理冗余存储

在主屏幕上

1. 以管理员身份登录 Cyber Protect 中控台。
   在 Cyber Protect 中控台顶部会出现警告消息。
2. 在警告消息中, 单击**启用地理冗余云存储**。
3. 若要表示您已了解复制位置和费用, 请勾选复选框。
4. 若要确认您的选择, 请单击**启用**。

由此, 地理冗余存储已启用, 并且会将备份数据复制到复制位置。

在设置选项卡上

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转至**设置>系统设置**。
3. 折叠默认备份选项列表, 然后单击**地理冗余云存储**。
4. 启用**地理冗余云存储**开关。
5. 单击**保存**。
6. 若要表示您已了解复制位置和费用, 请勾选复选框。
7. 若要确认您的选择, 请单击**启用**。

由此, 地理冗余存储已启用, 并且会将备份数据复制到复制位置。

仅用地理冗余存储

您可以从 Cyber Protect 中控台禁用地理冗余存储, 或者在管理门户中取消配置。

若要禁用地理冗余存储

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转至**设置>系统设置**。
3. 折叠默认备份选项列表, 然后单击**地理冗余云存储**。
4. 禁用**地理冗余云存储**开关。
5. 单击**保存**。
6. 若要确认您的选择, 键入**禁用**, 然后单击**禁用**。

由此，已禁用地理冗余存储。复制的数据将在一天内删除。

若要撤销地理冗余存储

1. 以管理员身份登录到管理门户。
2. 在**客户端**中，单击客户租户名称旁边的省略号按钮 (...) > **配置**。
3. 在**保护**选项卡中，单击**编辑**。
4. 在**云资源**下，清除存储名称下的**地理冗余**复选框。
5. 单击**保存**。

由此，客户租户的地理冗余存储已禁用，无法在 Cyber Protect 中控台中启用。复制的数据将在一天内删除。

查看地理复制状态

地理复制状态显示是否会将来自主备份位置的数据复制到复制位置。

可能出现以下状态：

- **已同步** – 数据已复制到复制位置。
- **正在同步** - 数据正在复制到复制位置。此操作的持续时间取决于数据的大小。
- **挂起** - 数据复制已暂时暂停。
- **已禁用** - 数据复制已禁用。

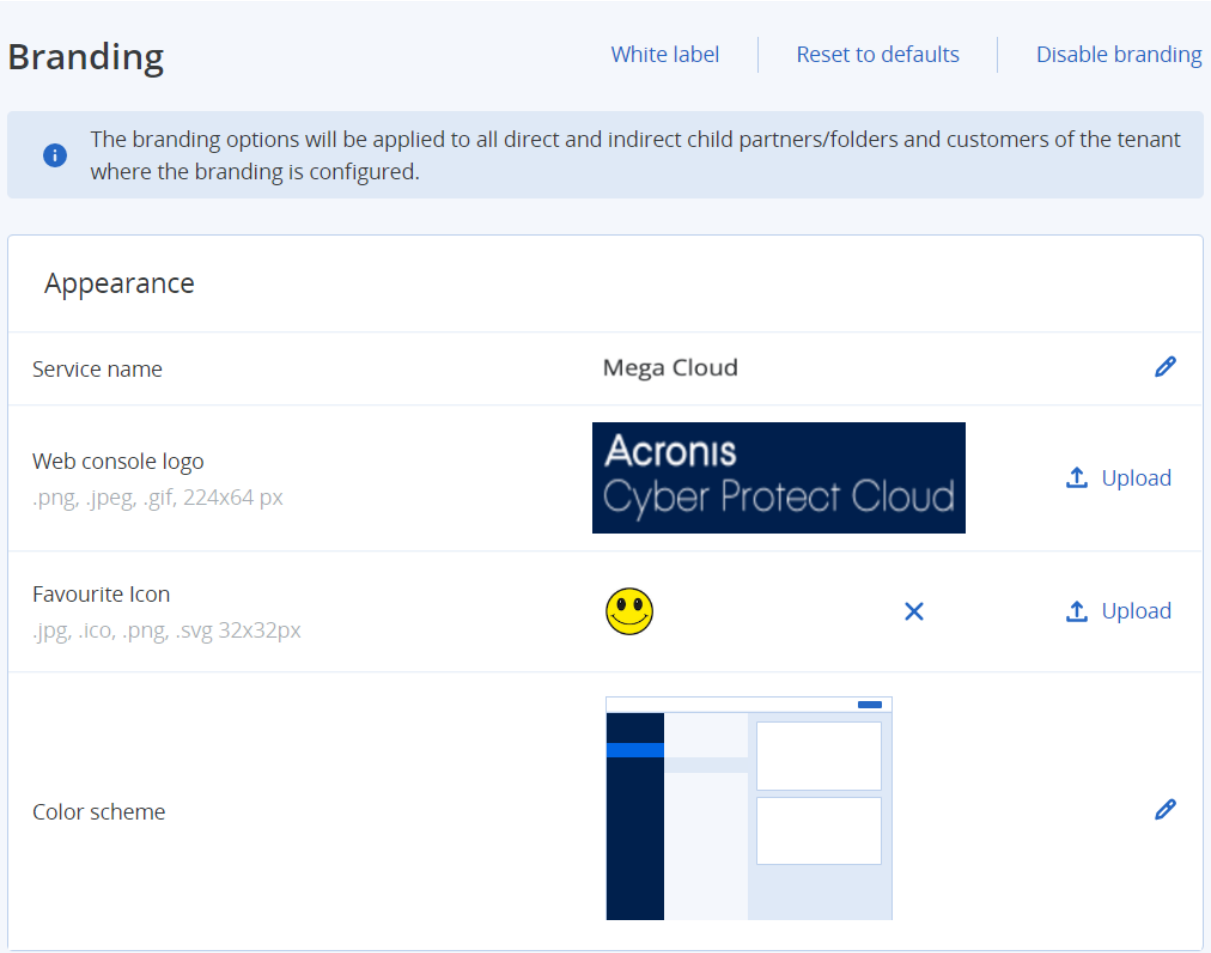
若要检查复制状态

1. 登录到 Cyber Protect 中控台。
2. 在**备份存储**选项卡上，选择备份位置，然后选择备份存档。
3. 单击**详细信息**，然后检查**地理复制状态**部分中的状态。

配置品牌和白标

通过**设置** > **品牌**部分，合作伙伴管理员可以为子租户自定义管理门户的用户界面和 **Cyber Protection** 服务，以移除与更高级别合作伙伴的任何关联。

注意
品牌设置将应用于您的所有子租户（直接和间接）。您自己租户的品牌设置由您的服务提供商配置。



可以在合作伙伴和文件夹级别上配置品牌。品牌应用于租户(品牌配置于其中)的所有直接和间接子合作伙伴/文件夹以及客户。

其他服务会在其服务中控台中提供单独的品牌功能。有关详细信息,请参阅相应服务的用户指南。

品牌项目

外观

- **服务名称**。此名称用于管理门户和云服务发送的所有电子邮件消息(帐户激活消息、服务通知电子邮件消息)、首次登录后的**欢迎**屏幕,以及作为管理门户浏览器选项卡名称。
- **Web 中控台徽标**。徽标显示在管理门户和服务中。单击**上传**以上传图像文件。
- **网站图标** [仅在配置了自定义 URL 时可用]。网站图标会显示在浏览器选项卡中的页面标题旁边。单击**上传**以上传图像文件。
- **颜色方案**。颜色方案定义用于所有用户界面元素的颜色组合。

注意
单击**在新选项卡中预览方案**,可预览将呈现给子租户的界面外观。只有在**选择颜色方案**面板上单击**完成**后,才会应用品牌。

代理程序和安装程序品牌

可以为 Windows 和 macOS 自定义代理程序安装文件和任务栏监视器的品牌。

注意
要启用此品牌功能，必须将 Cyber Protection 代理程序更新到版本 15.0.28816(发行版 22.01) 或更高版本。

- **代理程序安装程序文件名**。在受保护工作负载上下载的安装文件的名称。
- **代理程序安装程序徽标**。代理程序安装期间，在“安装”向导中显示的徽标。单击**上传**以上传图像文件。
- **代理程序名称**。代理程序安装期间，在“安装”向导中显示的名称。
- **任务栏监视器名称**。在任务栏监视器窗口顶部显示的名称。

文档和支持

- **主页 URL**。当用户单击**关于**面板上的公司名称时，将打开此页面。
- **支持 URL**。当用户单击**关于**面板上或管理门户发送的电子邮件中的**联系支持人员**链接时，将打开此页面。
- **支持电话**。电话号码显示在**关于**面板中。
- **知识库 URL**。当用户单击错误消息中的**知识库**链接时，将打开此页面。
- **管理门户管理员指南**。当用户单击管理门户用户界面右上角的问号图标时，此页面即会打开，然后依次单击**关于** > **管理员指南**。
- **管理门户管理员帮助**。当用户单击管理门户用户界面右上角的问号图标时，此页面即会打开，然后单击**帮助**。

Cyber Protect Cloud 服务的 URL

可以从您的自定义域中提供 Cyber Protect Cloud 服务。单击**配置**以首次设置自定义 URL，或单击**重新配置**以更改现有 URL。要使用默认 URL (https://cloud.acronis.com)，请单击**重置为默认值**。有关自定义 URL 的详细信息，请参阅“配置自定义 Web 界面 URL”。

法律文档设置

- **最终用户许可协议 (EULA) URL**。当用户单击**关于**面板、首次登录后出现的**欢迎**屏幕和 File Sync & Share 上传请求登录页面上的**最终用户许可协议**链接时，将打开此页面。
- **平台条款 URL**。当合作伙伴管理员首次登录后，在**关于**面板上或在**欢迎**屏幕上单击**平台条款**链接时，将打开此页面。
- **隐私声明 URL**。当用户单击首次登录后出现的**欢迎**屏幕和 File Sync & Share 上传请求登录页面上的**隐私声明**链接时，将打开此页面。

重要事项
如果您不希望文档显示在欢迎屏幕上，则请勿输入该文档的 URL。

注意
有关 File Sync & Share 上传请求的详细信息，请参阅 Cyber Files Cloud 用户指南。

追加销售

- **购买 URL**。当用户单击**立即购买**以升级到 Cyber Protection 服务的更高级版本时，将打开此页面。有关追加销售方案的详细信息，请参阅“为客户配置追加销售方案”。

移动应用程序

- **应用程序商店**。当用户在 **Cyber Protection** 服务中依次单击**添加** > **iOS** 时，将打开此页面。
- **Google Play**。当用户在 **Cyber Protection** 服务中依次单击**添加** > **Android** 时，将打开此页面。

电子邮件服务器设置

您可以指定将用于从管理门户和服务发送电子邮件通知的自定义电子邮件服务器。若要指定自定义电子邮件服务器，请单击**自定义**，然后指定以下设置：

- 在**发件人**中，输入要在电子邮件通知的**发件人**字段中显示的姓名。
- 在 **SMTP** 中，输入发送邮件服务器 (SMTP) 的名称。
- 在**端口**中，输入发送邮件服务器的端口。默认情况下，端口设为 25。
- 在**加密**中，选择是使用 SSL 还是 TLS 加密。选择**无**以禁用加密。
- 在**用户名**和**密码**中，指定将用于发送邮件的帐户的凭据。

配置品牌

1. 登录管理门户。
2. 导航到要在其中配置品牌的租户。
3. 依次单击**设置** > **品牌**。
4. [如果品牌尚未启用] 单击**启用品牌**。
5. 配置上述的品牌项目。

恢复默认品牌设置

可以将所有品牌项目重置为其默认值。

1. 登录管理门户。
2. 导航到要在其中重置品牌的租户。
3. 依次单击**设置** > **品牌**。
4. 在右上角，单击**恢复为默认值**。

禁用品牌

可以为您的帐户和所有子租户禁用品牌。

1. 登录管理门户。
2. 导航到要在其中禁用品牌的租户。
3. 依次单击**设置** > **品牌**。
4. 在右上角，单击**禁用品牌**。

白标

可以控制是否要为所有子合作伙伴和客户对 Cyber Protection 代理程序(适用于 Windows、macOS 和 Linux)、Cyber Protection Monitor(适用于 Windows、macOS 和 Linux)和 Connect Client 进行品牌化或白标。如果启用白标，将对代理程序、Connect Client 和任务栏监视器进行白标。此设置还会影响安装程序和 Cyber Protection Monitor 中所使用的名称和徽标。

应用白标

1. 登录管理门户。
2. 导航到要在其中应用白标的租户。
3. 依次单击**设置** > **品牌**。
4. 在窗口的上端，单击**白标**以清除所有品牌项目(**服务名称**、**最终用户许可协议 (EULA) URL**、**管理门户管理员指南**、**管理门户管理员帮助**和**电子邮件服务器设置**除外)。

配置自定义 Web 界面 URL

注意
与默认 URL 相比，自定义 URL 会指向不同的 IP 地址。配置防火墙策略时请记住这一点。

为 Cyber Protect Cloud 服务配置 Web 界面 URL

1. 在管理门户中，依次单击**设置** > **品牌**。
2. 在 **Cyber Protect Cloud 服务的 URL** 部分中：
   - 单击**配置**以首次设置自定义 URL。
   - 单击**重新配置**以更改现有自定义 URL。
3. 在**域设置**步骤中，准备您的域和 CNAME 记录。

   要使用自定义 URL，您必须有活动域名和配置为指向您的帐户所在数据中心的 CNAME 记录。CNAME 记录的配置由您的 DNS 注册商完成，并且最长可能需要 48 小时才能传播。

   若要找到您的数据中心的域名并请求 CNAME 记录的配置，请参阅文章 Acronis Cyber Protect Cloud：如何定义 CNAME 记录。
4. 在**检查您的 URL** 步骤中，验证您的自定义 URL 是否可访问，并且您的 CNAME 记录是否已正确配置。为此，请输入主 URL 名称并单击**检查**。如果使用通配符 SSL 证书，则最多可以添加十个替代域名。如果使用“Let's Encrypt”证书，则会忽略替代域名。
5. 在 **SSL 证书**步骤中，可以执行以下任一操作：
   - 创建“Let's Encrypt”证书。为此，请单击**带有“Let's Encrypt”的免费 SSL 证书**。此选项使用第三方实体颁发的“Let's Encrypt”证书。对于因使用这些免费证书而导致出现的任何问题，服务提供商概不负责。有关“Let's Encrypt”条款的详细信息，请参阅

https://letsencrypt.org/repository/。

- 上传您的通配符证书。为此，请单击**上传通配符证书**，然后提供通配符证书和私钥。

  注意
  证书验证错误可能会出现，其中错误消息为："无法验证证书：x509：证书由未知颁发机构签名"。通常，这意味着缺少一些中间证书。使用证书链解析程序来修复证书的结构并上传完整的证书链。

6. 单击**提交**以应用更改。

将自定义 URL 重置为默认值

1. 在管理门户中，依次单击**设置** > **品牌**。
2. 在 **Acronis Cyber Protect Cloud 服务的 URL** 部分中，单击**重置为默认值**以使用默认 URL (https://cloud.acronis.com)。

配置 Cyber Protection 代理程序的更新

重要事项
如果已启用 保护 服务，则可访问代理程序更新管理功能。

此过程适用于以下 Cyber Protection 代理程序的更新：适用于 Windows 的代理程序、适用于 Linux 的代理程序、适用于 Mac 的代理程序和适用于 File Sync & Share 的 Cyber Files Cloud 代理程序。

Cyber Files Cloud 有适用于 File Sync & Share 的 Windows 版和 MacOS 版桌面代理程序，可用于同步计算机和用户的 File Sync & Share 云存储区域之间的文件和文件夹，以促进离线工作以及 WFH (在家办公) 和 BYOD(自带设备办公) 工作实践。

若要便于管理多个工作负载，可以为所有计算机或单个计算机上的所有代理程序配置无人值守的手动或自动更新。

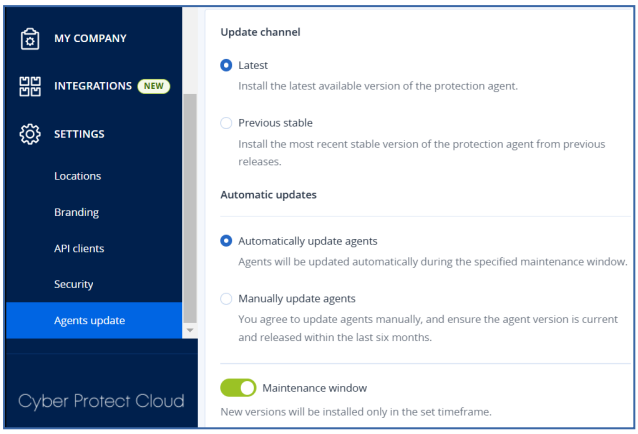
注意
若要从 Cyber Protect 中控台管理单个计算机上的代理程序，请参阅Cyber Protect 用户指南中的更新代理程序部分。

自动更新

注意
未启用保护服务的合作伙伴和客户将继承其服务提供商为 File Sync & Share 提供的代理程序自动更新设置。

若要配置管理门户中管代理程序自动更新的默认设置

1. 选择**设置** > **代理程序更新**。



2. 在**更新通道**下，选择用于自动更新的版本。

选项	描述
最新(默认选中)	安装可用的最新版本的 Cyber Protection 代理程序。
之前的稳定版本	从先前的版本中安装 Cyber Protection 代理程序的最新稳定版本。

3. 请验证选项 **自动更新代理程序** 是否已打开。

注意
仅以下代理程序可使用自动更新：
- Cyber Protect 代理程序版本 26986(于 2021 年 5 月发布)或更高版本。
- 适用于 File Sync & Share 的桌面代理程序，版本 15.0.30370 或更高版本。

较旧的代理程序必须手动更新到最新版本，然后自动更新才能生效。

4. [可选] 设置维护窗口。
默认窗口为每日从安装代理程序的计算机的 23:00 到 08:00。

注意
尽管代理程序更新过程快速无缝，但我们建议选择对用户干扰最小的时间范围，因为用户无法阻止或推迟自动更新。

5. 单击**保存**。

手动更新

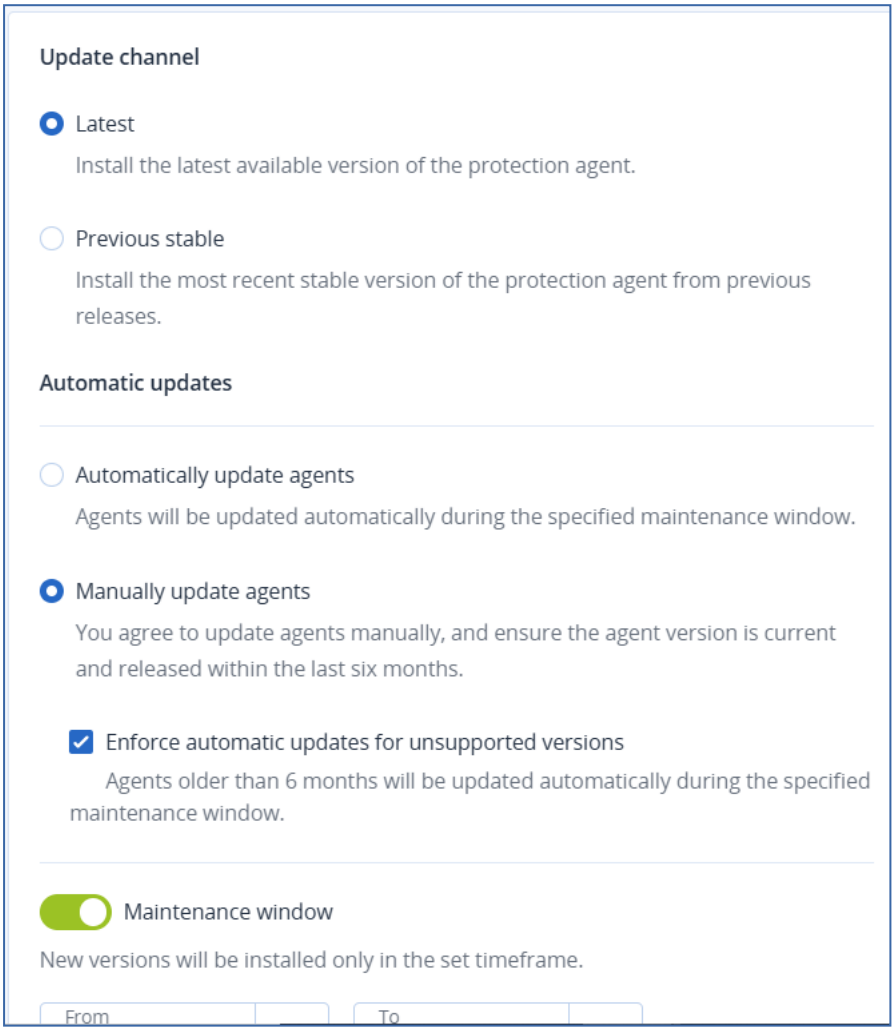
重要事项
我们强烈建议您为代理程序启用自动更新。定期更新可确保使您的代理程序保持最新状态，提供改进性能、修复错误，以及增强保护和安全性功能。

若要在管理门户中配置管理代理程序手动更新的默认设置

1. 转到 **设置** > **代理程序更新**。
2. 在**更新通道**下，选择用于自动更新的版本。

选项	描述
最新(默认选中)	安装可用的最新版本的 Cyber Protection 代理程序。
之前的稳定版本	从先前的版本中安装 Cyber Protection 代理程序的最新稳定版本。

3. 选择**手动更新代理程序**。



4. [可选]为了防止安全风险、确保访问最新功能并尽量减少因代理程序过时而导致的技术问题，请为超过 6 个月的代理程序启用自动更新。
   a. 选择**强制不支持的版本进行自动更新**。

   重要事项
   如果在 C25.02 版本发布之前未启用代理程序的自动更新，则此选项将自动为您环境中的所有租户启用。

   b. [可选]设置维护窗口。
   默认维护窗口为每日从安装代理程序的计算机的 23:00 到 08:00。

注意
尽管代理程序更新过程快速无缝，但我们建议选择对用户干扰最小的时间范围，因为用户无法阻止或推迟自动更新。

5. 单击**保存**。

监控代理程序更新

重要事项
代理程序更新只能由已启用保护模块的合作伙伴和客户的管理员监视。

若要监视代理程序更新，请参阅用户指南的警报和活动部分。

监控

要访问有关服务使用情况和操作的信息，请单击**监控**。

使用情况

使用情况选项卡提供服务使用情况概述并允许您在正在操作的租户内访问服务。

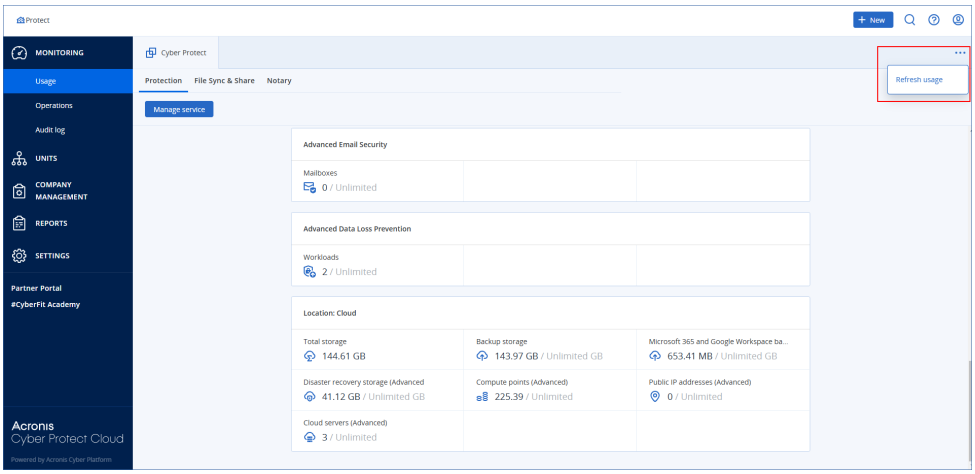
使用情况数据包括标准功能和高级功能。

重要事项
产品 UI 中显示的存储使用值为二进制字节单位 – 以 Mib、Gib 和 Tib 为单位 – 尽管标签分别显示为 MB、GB 和 TB。例如，如果实际使用量为 3105886629888 字节，则 UI 中显示的值将正确显示为 2.82，但标签显示为 TB 而非 TiB。

Microsoft 365 和 Google Workspace 工作负载的存储使用情况将单独从一般备份存储中报告，并显示在 **Microsoft 365 和 Google Workspace 备份**部分下。

要刷新选项卡上显示的使用情况数据，请单击屏幕右上角的省略号图标(...)，然后选择**刷新使用情况**。

注意
获取数据可能最多需要 10 分钟。重新加载页面以查看更新的数据。



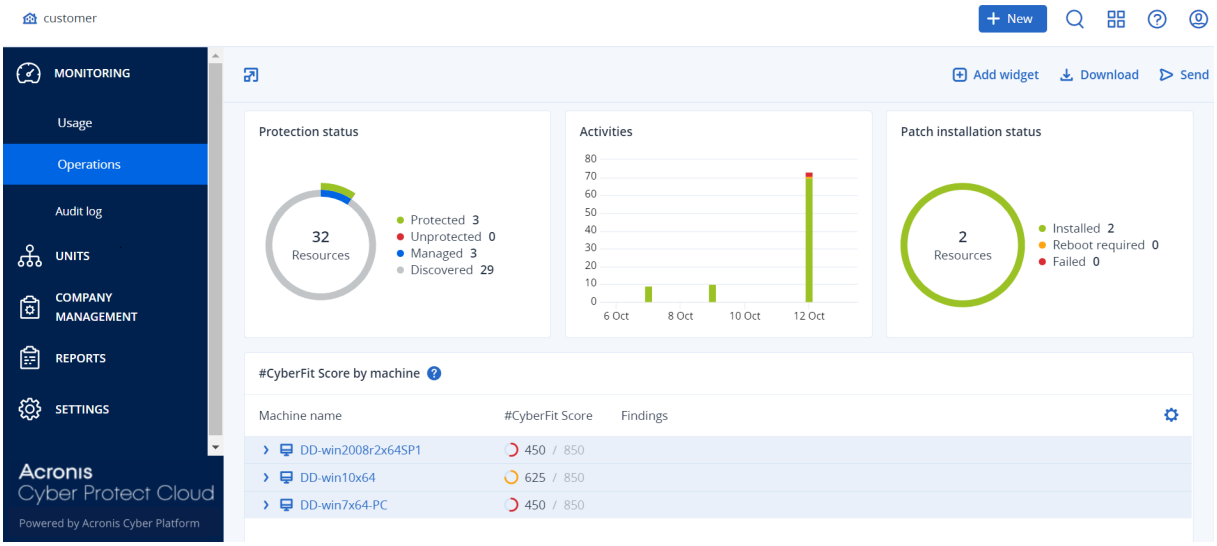
操作

操作仪表板提供了若干可自定义的小组件，这些小组件会提供与 Cyber Protection 服务相关操作的概述。会在将来的版本中提供适用于其他服务的小部件。

默认情况下，会为您正在其中进行操作的租户显示数据。可以通过编辑小部件来单独更改每个小部件显示的租户。还显示了关于所选租户的直接子客户租户的汇总信息，包括位于文件夹中的信息。仪表板不显示关于子合作伙伴及其子租户的信息，您必须深入展开到特定合作伙伴才能查看其仪表板。但如果将子合作伙伴租户转换为文件夹租户，则关于此租户的子客户的信息将出现在父租户的仪表板上。

小组件每两分钟更新一次。小部件具有可单击元素，可让您调查和解决问题。可以用 .pdf 或/和 .xlsx 格式下载仪表板的当前状态或通过电子邮件将其发送到任何地址(包括外部收件人)。

可以从各种小部件中进行选择，这些小部件以表格、饼图、条形图、列表和树形图的形式显示。可以为不同租户或使用的不同过滤器添加多个类型相同的小组件。



在仪表板上重新排列小部件的步骤

通过单击小部件名称即可对其进行拖放。

编辑小部件的步骤

单击小部件名称旁边的铅笔图标。编辑小部件可对其重命名、更改时间范围、选择要为其显示数据的租户以及设置过滤器。

添加小部件的步骤

单击**添加小部件**，然后执行以下任一操作：

- 单击要添加的小部件。将使用默认设置添加小部件。
- 要在添加小部件之前对其编辑，请在选中小部件时单击齿轮图标。在完成编辑小部件后，单击**完成**。

删除小部件的步骤

单击小部件名称旁边的 X 符号。

保护状态

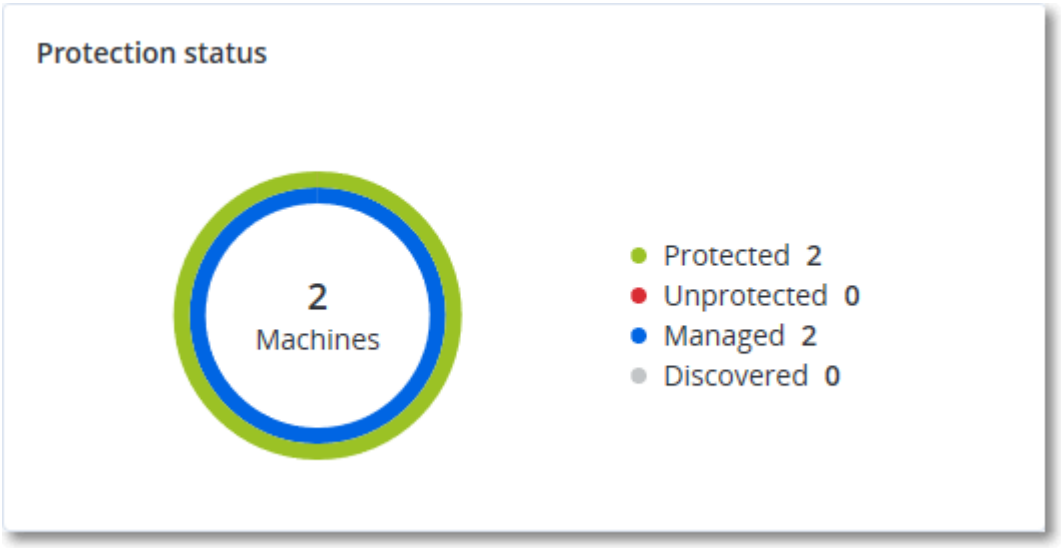
保护状态

该小部件显示所有计算机的当前保护状态。

计算机可以为下列状态之一：

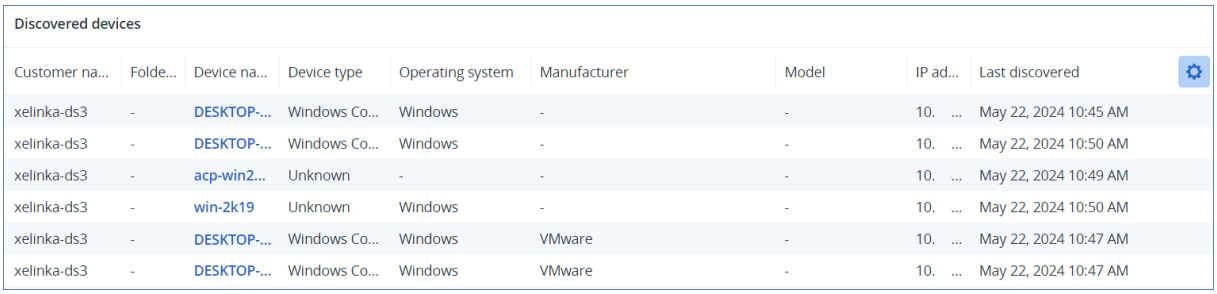
- **受保护** - 计算机已应用保护计划。
- **不受保护** - 计算机未应用保护计划。这包括未应用保护计划的已发现计算机和受控计算机。
- **受控** - 计算机已安装保护代理程序。
- **已发现** - 计算机未安装保护代理程序。

如果单击相应计算机状态，系统会将您重定向到具有此状态的计算机列表，以获取更多详细信息。



已发现的设备

此小组件显示有关在客户端网络中发现的设备的详细信息。设备信息包括设备类型、制造商、操作系统、IP 地址、MAC 地址、发现日期等。


Discovered devices

Customer na...	Folde...	Device na...	Device type	Operating system	Manufacturer	Model	IP ad...	Last discovered
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	-	-	10. ...	May 22, 2024 10:45 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	-	-	10. ...	May 22, 2024 10:50 AM
xelinka-ds3	-	acp-win2...	Unknown	-	-	-	10. ...	May 22, 2024 10:49 AM
xelinka-ds3	-	win-2k19	Unknown	Windows	-	-	10. ...	May 22, 2024 10:50 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	VMware	-	10. ...	May 22, 2024 10:47 AM
xelinka-ds3	-	DESKTOP-...	Windows Co...	Windows	VMware	-	10. ...	May 22, 2024 10:47 AM

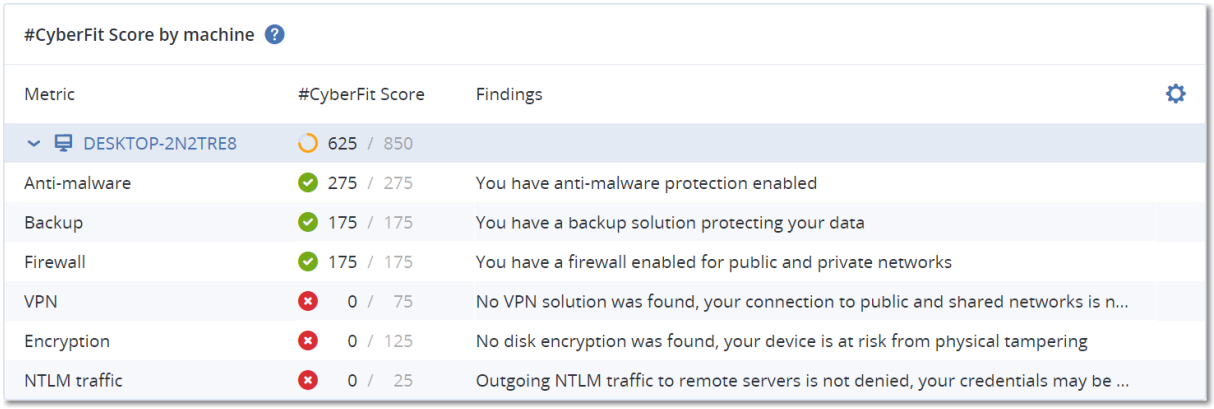
#CyberFit 分数(按计算机)

此小组件显示每台计算机的 #CyberFit 总分、其复合分数以及每个评估指标的发现:

- 反恶意软件
- 备份
- 防火墙
- VPN
- 加密
- NTLM 流量

要提高每个指标的分数,可以查看报告中提供的建议。

有关 #CyberFit 分数的更多详细信息,请参阅"计算机的 #CyberFit 分数"。


#CyberFit Score by machine

Metric	#CyberFit Score	Findings
DESKTOP-2N2TRE8	625 / 850	
Anti-malware	275 / 275	You have anti-malware protection enabled
Backup	175 / 175	You have a backup solution protecting your data
Firewall	175 / 175	You have a firewall enabled for public and private networks
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...

Endpoint Detection and Response (EDR) 小组件

Endpoint Detection and Response (EDR) 包括大量小组件,可以从**操作**仪表板访问它们。

可用小组件有:

- 每个工作负载的主要事件分发
- 事件 MTTR
- 安全性事件刻录
- 工作负载网络状态

每个工作负载的主要事件分发

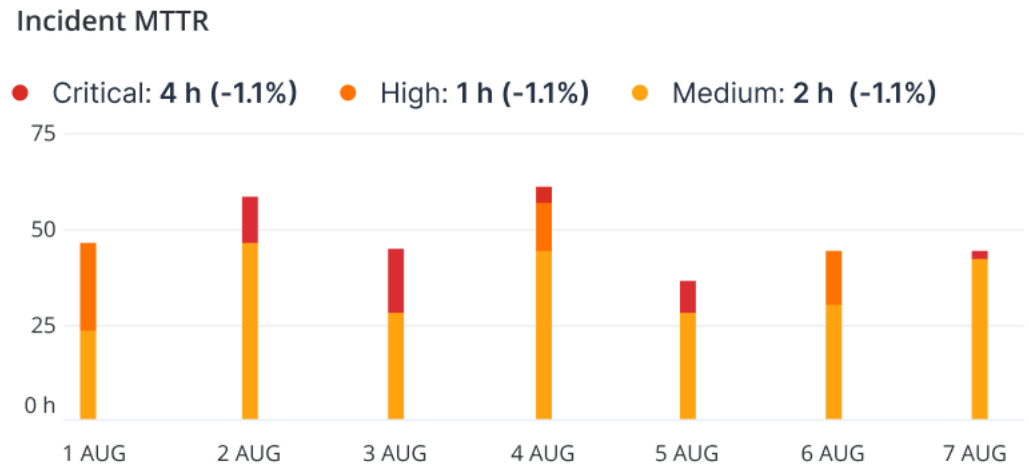
此小组件显示具有最多事件的前五个工作负载(单击**全部显示**以重定向到事件列表,这可根据小组件设置进行过滤)。

将鼠标悬停在工作负载行上以查看事件的当前调查状态明细;调查状态有**未启动**、**正在调查**、**已关闭**和**误报**。然后单击想要进一步分析的工作负载,并在显示的弹出窗口中选择相关客户;事件列表将根据小组件设置进行刷新。

事件 MTTR

此小组件显示用于安全性事件的平均解决时间。它指示调查和解决事件的快速程度。

单击某个列以根据严重性(**严重**、**高**和**中**)查看事件明细,并可查看解决不同严重性级别花费多少时间的指示。在括号中显示的 % 值表示与以前时间段比较的上升或下降。

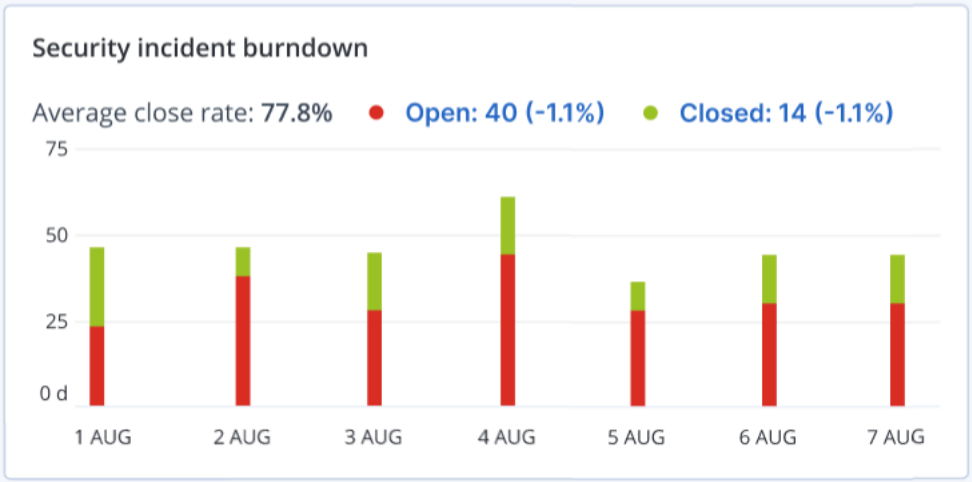


安全性事件刻录

此小组件显示关闭事件中的效率;针对一段时间的关闭事件的数量测量打开事件数。

将鼠标悬停在某列上可以查看在选定日发生的关闭和打开事件的明细。如果单击“打开”值，将显示一个弹出窗口，可以在其中选择相关租户；为选定的租户显示过滤后的事件列表，以显示当前打开的事件（**正在调查**或**未启动**状态）。如果单击“已关闭”值，将为选定的租户显示事件列表，并经过过滤以显示不再打开的事件（**已关闭**或**误报**状态）。

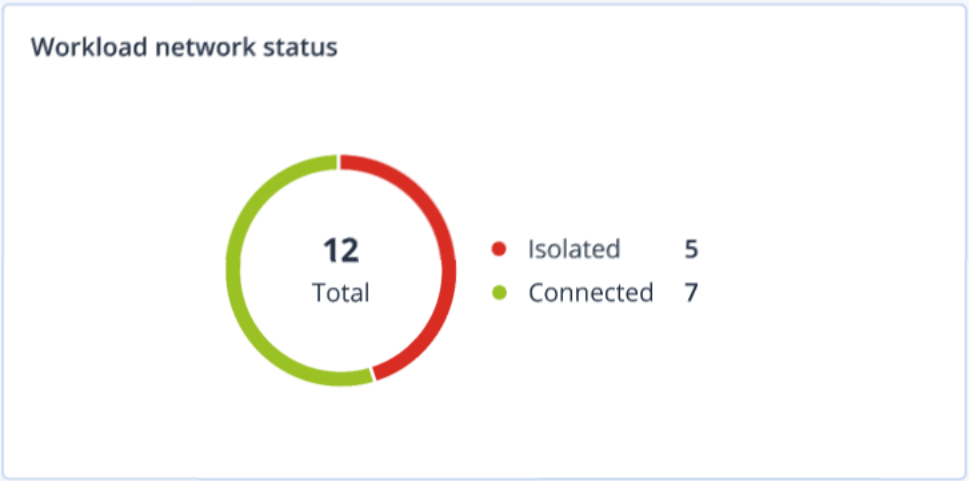
在括号中显示的 % 值表示与以前时间段比较的上升或下降。



工作负载网络状态

此小组件显示工作负载的当前网络状态，并指示隔离和连接了多少工作负载。

单击“已隔离”值，将显示一个弹出窗口，可以在其中选择相关租户。显示的工作负载视图经过过滤以显示隔离的工作负载。单击“已连接”值以查看过滤了代理程序列表的工作负载，以显示连接的工作负载（对于选定的租户）。



磁盘运行状况监控

磁盘运行状况监控提供有关当前磁盘状态及其预测的信息，这样您可以防止可能与磁盘故障相关的数据丢失。HDD 和 SSD 磁盘均受支持。

限制

- 仅对于运行 Windows 的计算机支持磁盘运行状况预测。
- 只可以监控物理计算机的磁盘。虚拟机的磁盘无法进行监控并且不会显示在磁盘运行状况小部件中。
- 不支持 RAID 配置。磁盘运行状况小组件不包括任何有关 RAID 已实现的计算机的信息。
- 不支持 NVMe SSD。
- 不支持外部存储设备。

磁盘运行状况可以表示为以下状态之一：

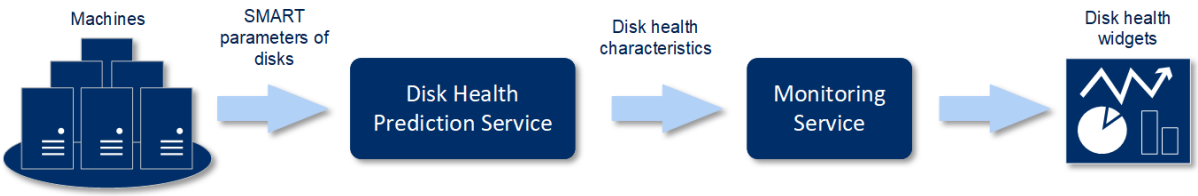
- **正常**
  磁盘运行状况为 70% 和 100% 之间。
- **警告**
  磁盘运行状况为 30% 和 70% 之间。
- **严重**
  磁盘运行状况为 0% 和 30% 之间。
- **计算磁盘数据**
  正在计算当前磁盘状态和预测。

工作方式

“磁盘运行状况预测服务”使用基于人工智能的预测模型。

1. 保护代理程序会收集磁盘的 SMART 参数，并将此数据传递给“磁盘运行状况预测服务”：
   - SMART 5 - 重新分配的扇区数。
   - SMART 9 - 开机时间。
   - SMART 187 - 报告的无法修正错误。
   - SMART 188 - 命令超时。
   - SMART 197 - 当前待处理的扇区数。
   - SMART 198 - 无法修正的脱机扇区数。
   - SMART 200 - 写入错误率。
2. “磁盘运行状况预测服务”会处理收到的 SMART 参数、进行预测，然后提供以下磁盘运行状况特征：
   - 磁盘运行状况当前状态：正常、警告、严重。
   - 磁盘运行状况预测：负面、稳定、正面。
   - 磁盘运行状况预测概率（百分比形式）。

   预测期为一个月。
3. 监视服务会收到这些特征，然后在 Cyber Protect 中控台的磁盘运行状况小组件中显示相关信息。



磁盘运行状况小部件

磁盘运行状况监视的结果显示在 Cyber Protect 中控台中可用的以下小组件中。

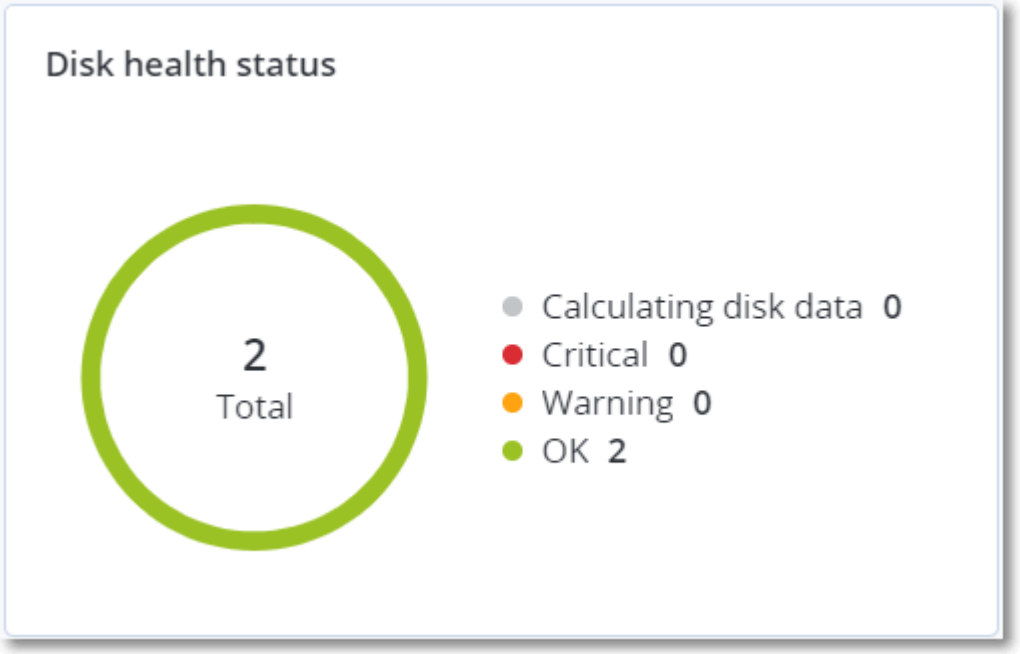
- **磁盘运行状况概述**是一个树形图小部件，具有可以通过向下钻取来切换的两个级别的详细信息。
  - 计算机级别
    显示有关每个选定客户计算机的磁盘运行状况状态的概要信息。仅显示最严重的磁盘状态。将光标悬停在特定块上时，其他状态会显示在工具提示中。计算机块的大小取决于该计算机所有磁盘的总大小。计算机块的颜色取决于找到的最严重磁盘状态。

  - 磁盘级别
    显示选定计算机的所有磁盘的当前磁盘运行状况状态。每个磁盘块显示以下任一磁盘运行状

况预测及其可能性(百分比):

- 将降级
- 将保持稳定
- 将得到改进

- **磁盘运行状况状态**是一个饼图小部件,显示每个状态的磁盘数量。



磁盘运行状况状态警告

磁盘运行状况检查每 30 分钟运行一次，同时每天生成一次相应警告。当磁盘运行状况从**警告**更改为**严重**时，始终会生成警报。

警告名称	严重性	磁盘运行状况状态	描述
磁盘可能发生故障	警告	(30 – 70)	此计算机上的 <disk name> 磁盘将来可能会发生故障。尽快运行该磁盘的完整映像备份、替换该磁盘，然后将映像恢复到新磁盘。
磁盘即将发生故障	严重	(0 – 30)	此计算机上的 <disk name> 磁盘处于严重状态，很可能即将发生故障。此时，不建议对该磁盘进行映像备份，因为增加的压力可能会导致磁盘发生故障。立即备份该磁盘上最重要的文件并替换该磁盘。

数据保护地图

数据保护地图功能允许您检查所有对您重要的数据，并在树形图可伸缩视图中获取有关所有重要文件的数量、大小、位置、保护状态的详细信息。

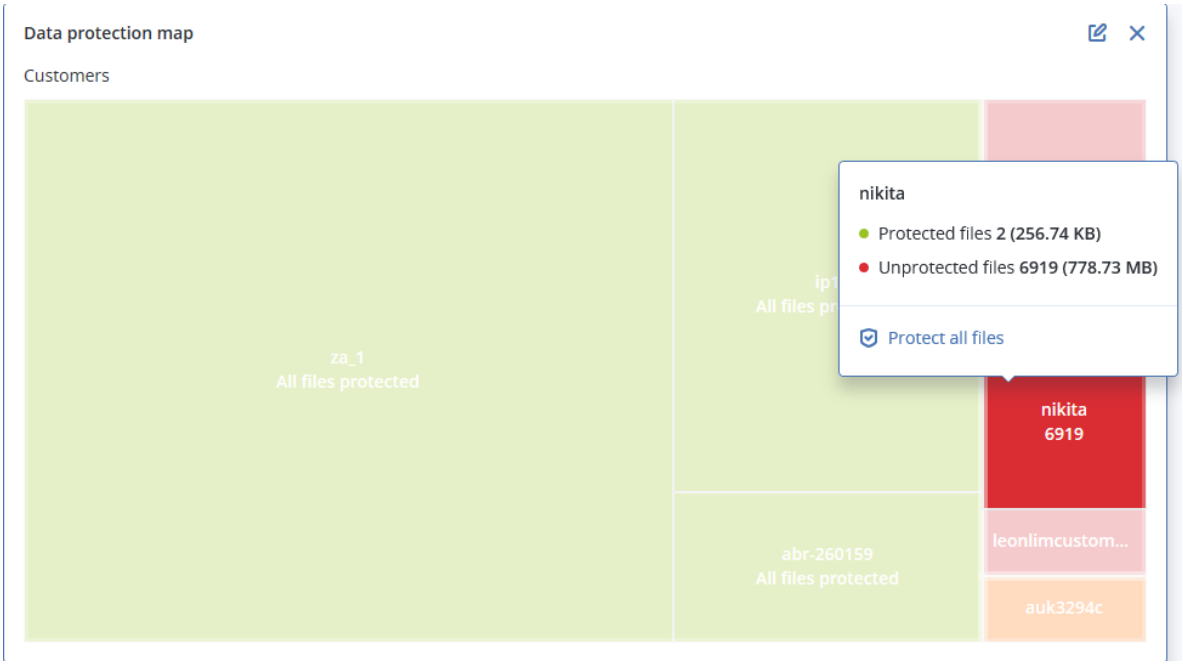
每个块的大小取决于属于客户/计算机的所有重要文件的总数/大小。

文件可以具有以下保护状态之一：

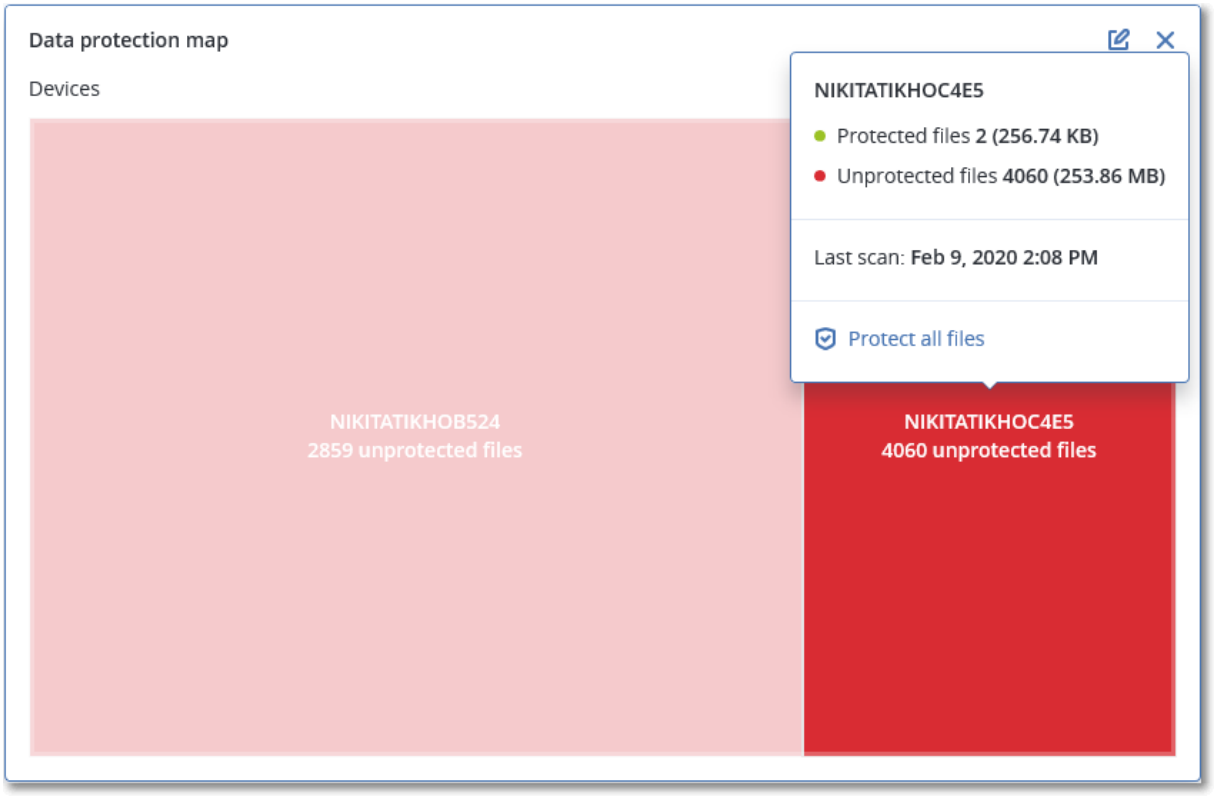
- **严重** - 有 51-100% 的不受保护文件(具有您指定的扩展名)未针对选定客户租户/计算机/位置进行备份。
- **低** - 有 21-50% 的不受保护文件(具有您指定的扩展名)未针对选定客户租户/计算机/位置进行备份。
- **中** - 有 1-20% 的不受保护文件(具有您指定的扩展名)未针对选定客户租户/计算机/位置进行备份。
- **高** - 所有具有您指定扩展名的文件都已针对选定客户租户/计算机/位置进行了保护(备份)。

数据保护检查的结果可以在“数据保护地图”小部件(一个树形图小部件，具有可以通过向下钻取来切换的两个级别的详细信息)的仪表板上找到：

- 客户租户级别 - 显示有关每个选定客户的重要文件保护状态的概要信息。



- 计算机级别 - 显示有关选定客户的每台计算机的重要文件保护状态的信息。



要保护不受保护的文件，请将光标悬停在相应块上，然后单击**保护所有文件**。在该对话框窗口中，可以找到有关不受保护文件数量及其位置的信息。要保护它们，请单击**保护所有文件**。

还可以下载 CSV 格式的详细报告。

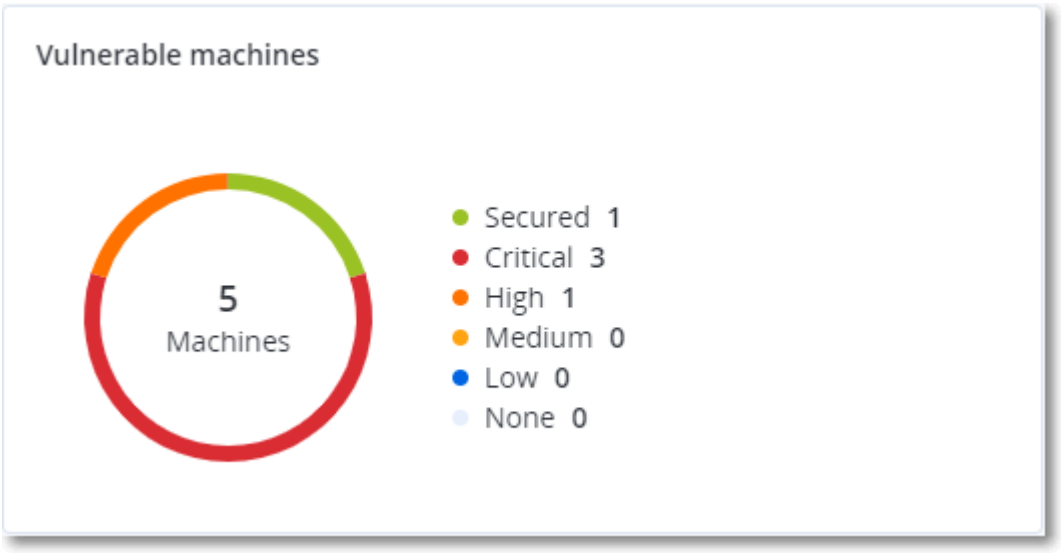
漏洞评估小部件

易受攻击的计算机

该小部件按漏洞严重程度显示易受攻击的计算机。

根据通用漏洞评分系统 (CVSS) v3.0, 发现的漏洞可能具有以下严重级别之一:

- 已保护:未发现任何漏洞
- 严重:9.0 - 10.0 CVSS
- 高:7.0 - 8.9 CVSS
- 中:4.0 - 6.9 CVSS
- 低:0.1 - 3.9 CVSS
- 无:0.0 CVSS



现有漏洞

该小部件显示计算机上当前存在的漏洞。在**现有漏洞**小组件中, 有两列显示时间戳:

- **第一次检测** - 在计算机上最初检测到漏洞的日期和时间。
- **上次检测** - 在计算机上上次检测到漏洞的日期和时间。

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

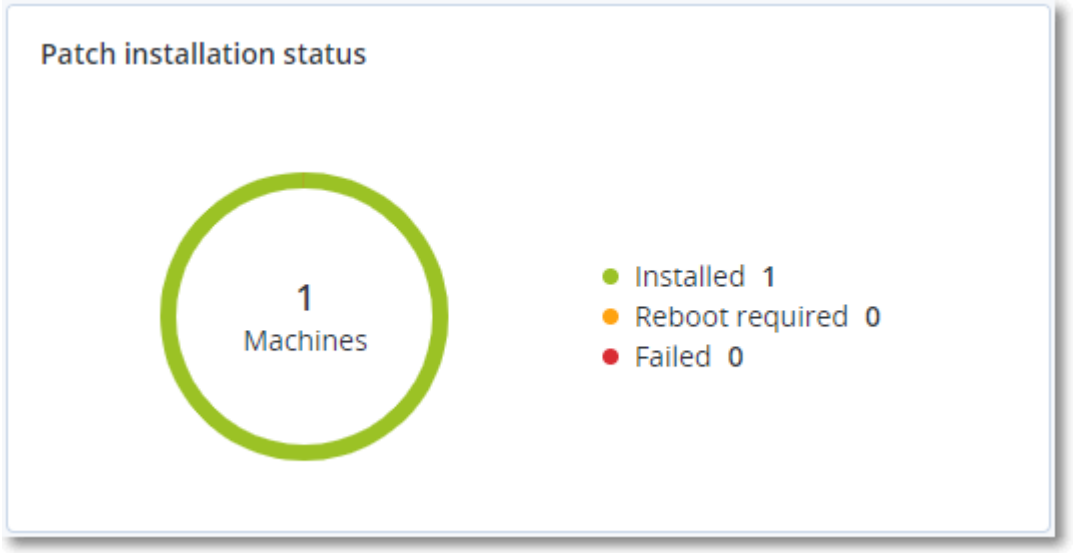
修补程序安装小部件

具有四个与修补程序管理功能相关的小部件。

修补程序安装状态

该小部件显示按修补程序安装状态分组的计算机数量。

- **已安装** - 所有可用修补程序都已安装在计算机上
- **需要重新启动** - 安装修补程序后，计算机需要重新启动
- **失败** - 修补程序无法安装在计算机上



修补程序安装摘要

该小部件按修补程序安装状态显示计算机上修补程序的摘要。

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

修补程序安装历史记录

该小部件显示有关计算机上修补程序的详细信息。

Patch installation history

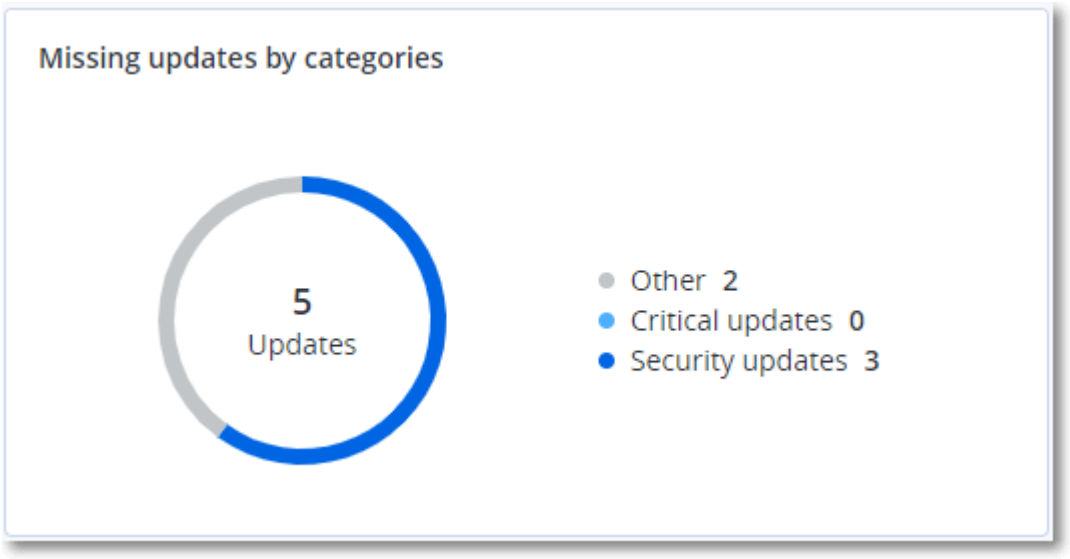
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

More

按类别划分的缺少更新

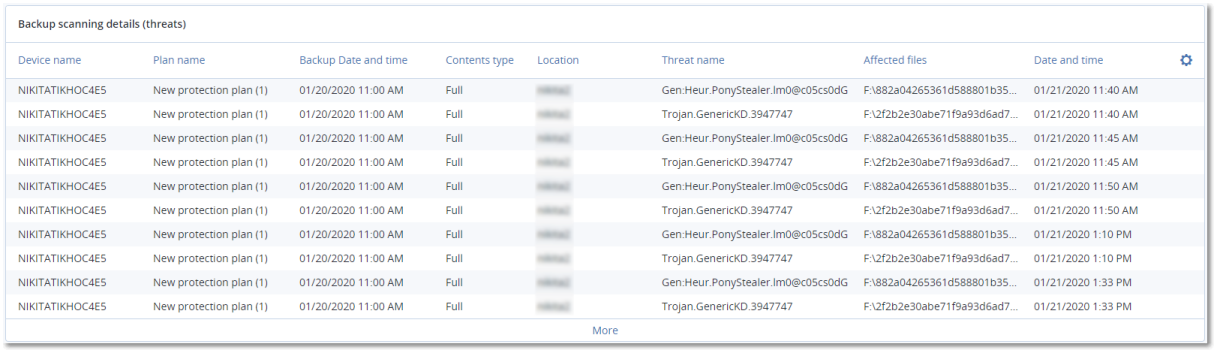
该小部件显示每个类别缺少的更新数量。显示以下类别：

- 安全更新
- 重要更新
- 其他



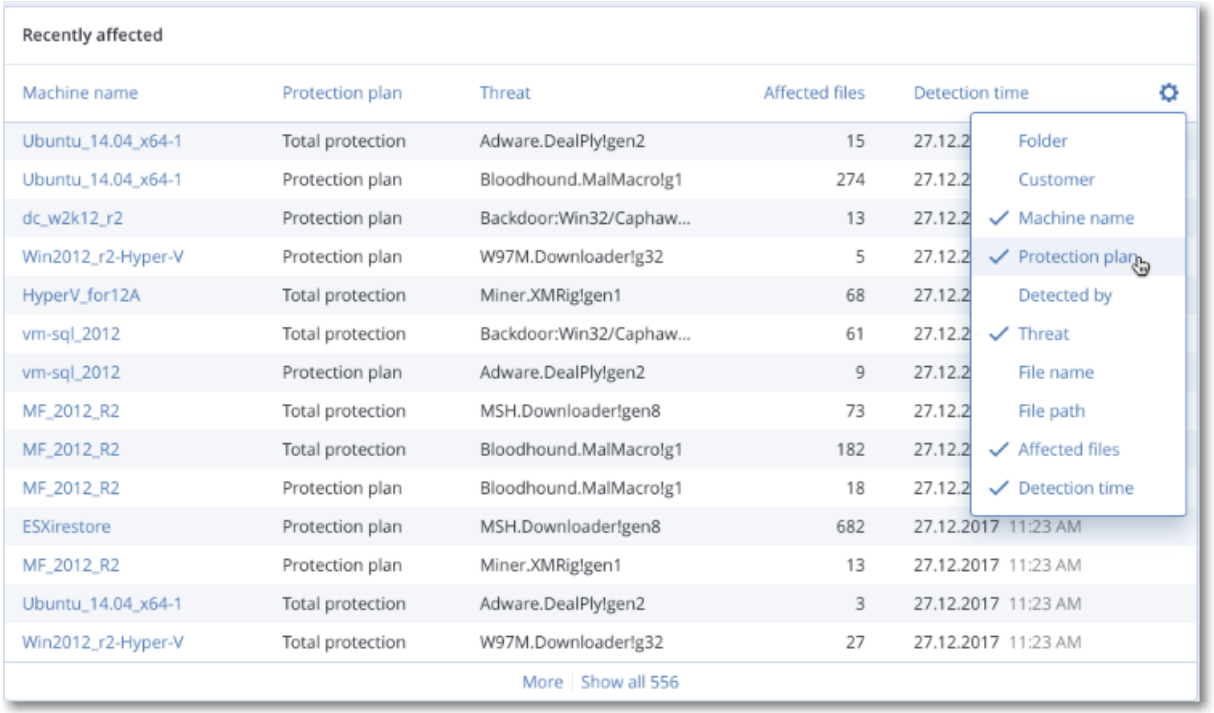
备份扫描详细信息

该小部件显示有关备份中检测到威胁的详细信息。



最近受影响

该小组件会显示有关受病毒、恶意软件和勒索软件等威胁影响的工作负载的详细信息。可以找到有关检测到的威胁、检测到威胁的时间以及受影响的文件数量的信息。



下载最近受影响工作负载的数据

可以下载最近受影响工作负载的数据、生成 CSV 文件，然后将其发送给指定的收件人。

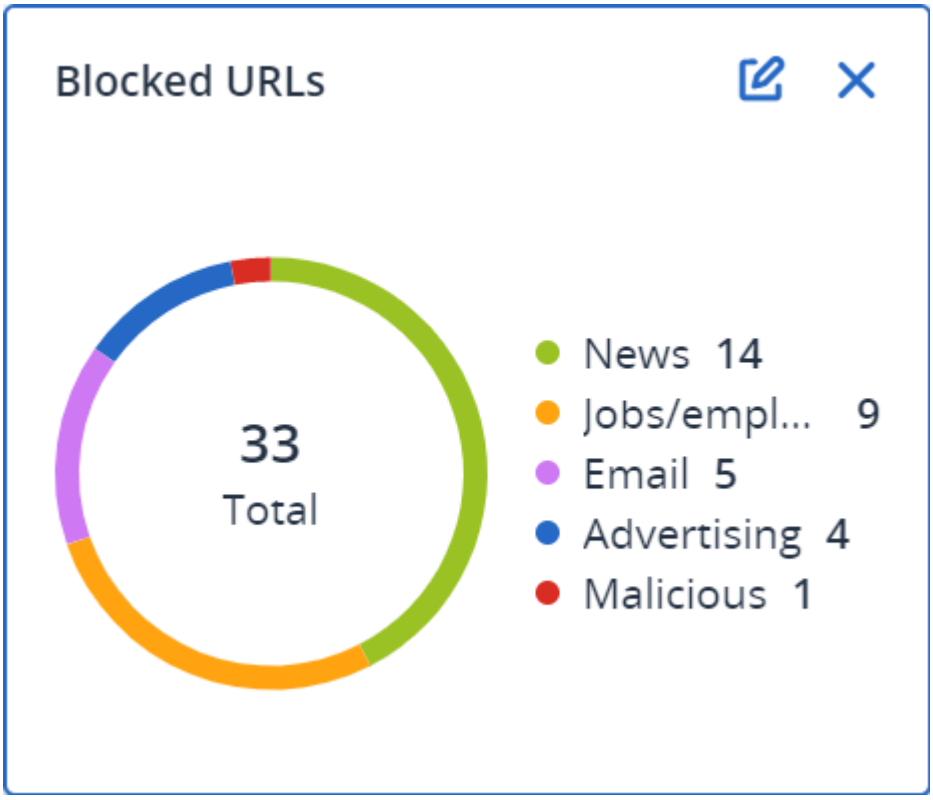
下载最近受影响工作负载的数据

1. 在**最近受影响**小组件中，单击**下载数据**。
2. 在**时间段**字段中，输入要下载数据的天数。可以输入的最大天数为 200。
3. 在**收件人**字段中，输入将接收电子邮件(内含下载 CSV 文件的链接)的所有人员的电子邮件地址。
4. 单击**下载**。

   系统开始生成 CSV 文件，其中包含指定的时间段内受影响工作负载的数据。CSV 文件准备完成后，系统会向收件人发送一封电子邮件。然后，每个收件人都可以下载该 CSV 文件。

已阻止 URL

小组件会按类别显示被阻止的 URL 的统计信息。有关 URL 过滤和类别的详细信息，请参阅“网络安全保护用户指南”。



软件清查小组件

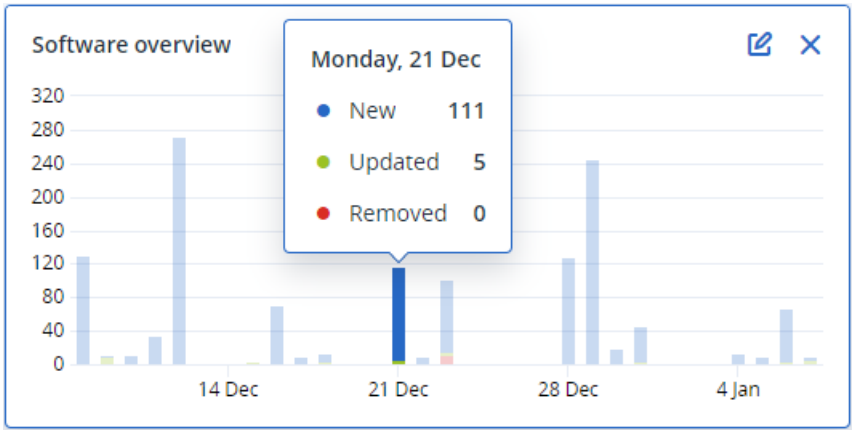
软件清查表小组件会显示有关客户组织中 Windows 和 macOS 设备上安装的所有软件的详细信息。

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+

软件概述小组件会显示特定时段(7 天、30 天或当月)内客户端组织中 Windows 和 macOS 设备上新的、已更新和已删除应用程序的数量。



将光标悬停在图表上的某一栏上时，将显示带有以下信息的工具提示：

新的 - 新安装应用程序的数量。

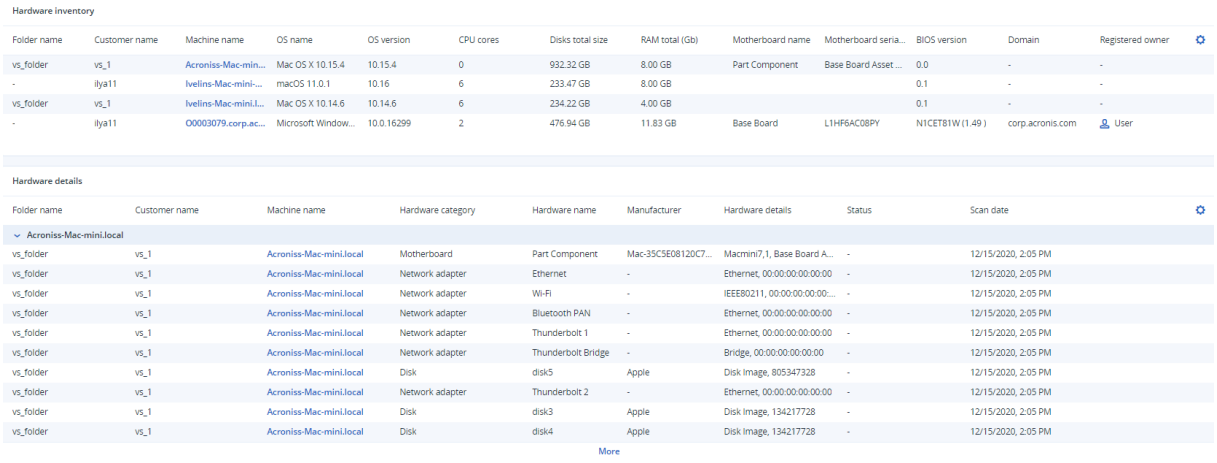
已更新 - 已更新应用程序的数量。

已删除 - 已删除应用程序的数量。

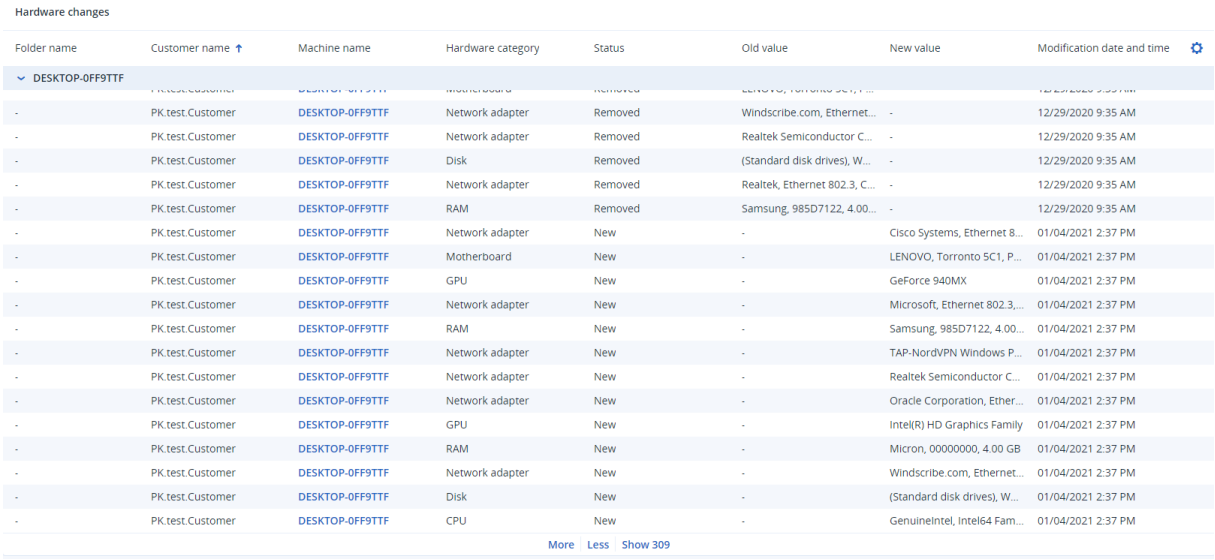
单击栏上与特定状态相对应的部分时，将加载一个弹出窗口。它会列出符合以下条件的所有客户：其设备上的应用程序在选定日期处于选定状态。可以从该列表中选择一个客户、单击**转到客户**，然后系统会将您重定向到客户的 中控台中的**软件管理** -> **软件清查**页面。将针对相应日期和状态过滤该页面中的信息。

硬件清查小组件

硬件清查和**硬件详细信息**表小组件会显示有关您客户端的组织中物理和虚拟 Windows 及 macOS 设备上安装的所有硬件的信息。



硬件更改表小组件会显示有关特定时段(7 天、30 天或当月)内您客户端的组织中物理和虚拟 Windows 及 macOS 设备上已添加、已删除和已更改硬件的信息。

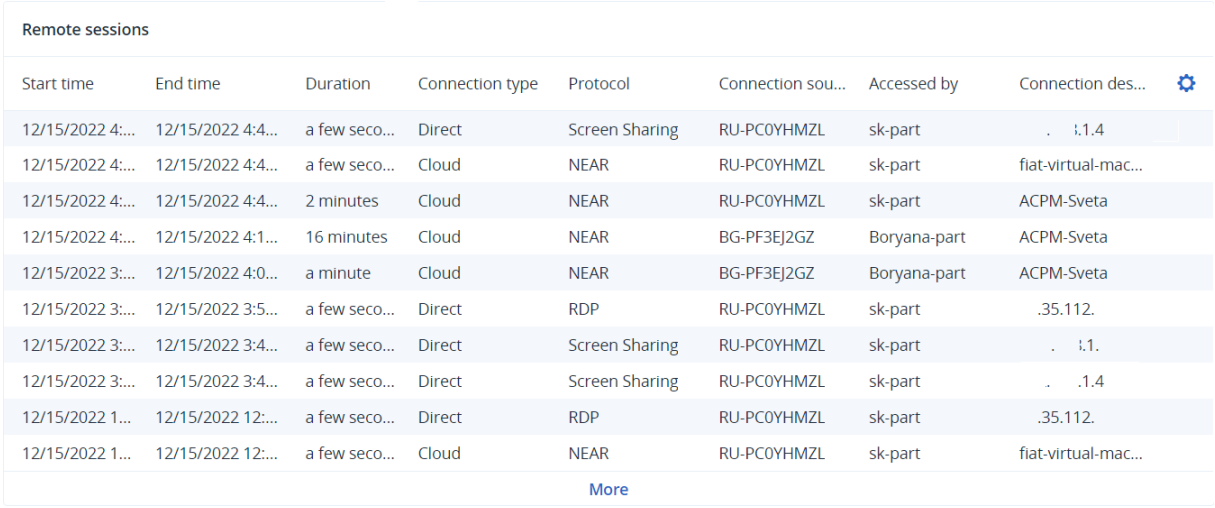

Hardware changes

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

会话历史记录

该小组件会显示指定时间段内在客户组织中进行的远程桌面和文件传输会话的详细信息。

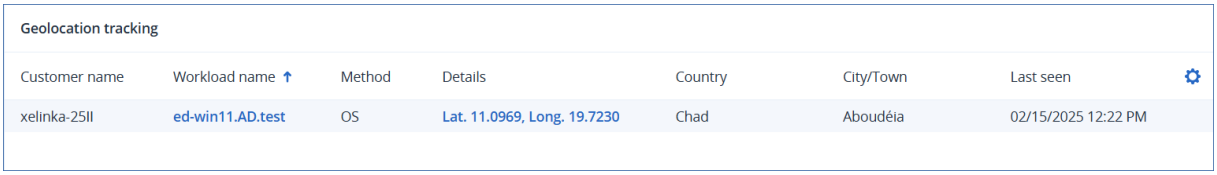

Remote sessions

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

地理位置追踪小组件

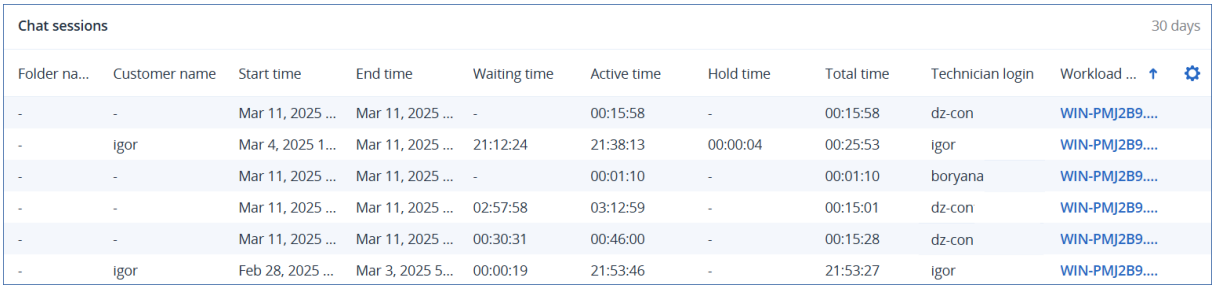
在**地理位置追踪**小组件中，您可以查看有关客户组织中工作负载位置的详细信息，例如国家/地区、城市、坐标、上次查看时间和地理位置追踪方法。


Geolocation tracking

Customer name	Workload name	Method	Details	Country	City/Town	Last seen
xelinka-25ll	ed-win11.AD.test	OS	Lat. 11.0969, Long. 19.7230	Chad	Aboudéia	02/15/2025 12:22 PM

聊天会话小组件

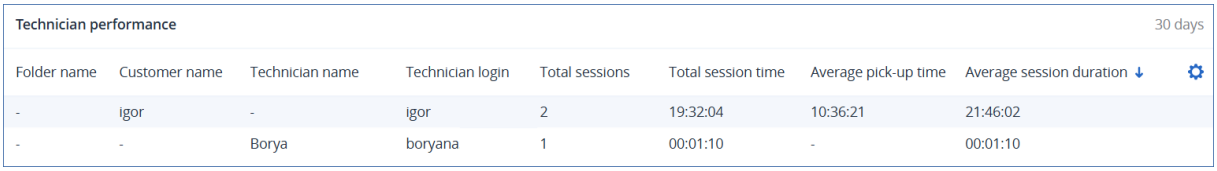
在**聊天会话**小组件中，您可以查看客户的组织中指定时间段内远程聊天会话的详细信息。


Chat sessions 30 days

Folder na...	Customer name	Start time	End time	Waiting time	Active time	Hold time	Total time	Technician login	Workload ...
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:15:58	-	00:15:58	dz-con	WIN-PMJ2B9....
-	igor	Mar 4, 2025 1...	Mar 11, 2025 ...	21:12:24	21:38:13	00:00:04	00:25:53	igor	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	-	00:01:10	-	00:01:10	boryana	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	02:57:58	03:12:59	-	00:15:01	dz-con	WIN-PMJ2B9....
-	-	Mar 11, 2025 ...	Mar 11, 2025 ...	00:30:31	00:46:00	-	00:15:28	dz-con	WIN-PMJ2B9....
-	igor	Feb 28, 2025 ...	Mar 3, 2025 5...	00:00:19	21:53:46	-	21:53:27	igor	WIN-PMJ2B9....

技术人员绩效小组件

在**技术人员绩效**小组件中，您可以查看指定时间段内您客户组织中每位技术人员绩效的详细信息。


Technician performance 30 days

Folder name	Customer name	Technician name	Technician login	Total sessions	Total session time	Average pick-up time	Average session duration
-	igor	-	igor	2	19:32:04	10:36:21	21:46:02
-	-	Borya	boryana	1	00:01:10	-	00:01:10

审核日志

审核日志可提供以下事件的序时记录：

- 用户在管理门户中执行的操作
- 用户在 Cyber Protect 中控台中对云到云资源执行的操作
- 用户在 Cyber Protect 中控台中执行的网络安全脚本操作
- 与电子邮件存档相关的操作
- 有关已达到的配额和配额使用情况的系统消息

该日志显示当前在运转的租户及其子租户中的事件。单击某个事件即可查看有关详细信息。

审核日志存储在数据中心中，其可用性并不会受最终用户计算机上问题的影响。

该日志会每日清除。事件会在 180 天后删除。

审核日志字段

对于每个事件，该日志会显示：

- **事件**

  事件的简短描述。例如，**租户已创建**、**租户已删除**、**用户已创建**、**用户已删除**、**配额已达到**、**备份内容已浏览**、**脚本已更改**。
- **严重性**

  可以为以下选项之一：
  - **错误**

    指示错误。
  - **警告**

    指示潜在的不良操作。例如，**租户已删除**、**用户已删除**、**配额已达到**。

  - **注意**

    指示可能需要注意的事件。例如，**租户已更新**、**用户已更新**。
  - **信息**

    指示中性的信息更改或操作。例如，**租户已创建**、**用户已创建**、**配额已更新**、**脚本计划已删除**。
- **日期**

  事件发生时的日期和时间。
- **对象名称**

  操作执行的目标对象。例如，**用户已更新**事件的对象是其属性已更改的用户。对于与配额有关的事件，配额即是对象。
- **租户**

  目标所属租户的名称。
- **发起程序**

  发起事件的用户的登录名。对于上级管理员发起的系统消息和事件，发起程序显示为**系统**。
- **发起程序的租户**

  发起程序所属租户的名称。对于上级管理员发起的系统消息和事件，该字段为空。
- **方法**

  显示事件是通过 web 界面还是 API 触发。
- **IP**

  触发事件的计算机的 IP 地址。

筛选和搜索

可以按类型、严重性或日期过滤事件。还可以按其名称、对象、租户、发起程序和发起程序的租户搜索事件。

正在收集 Cyber Protection 代理程序的性能数据

对于环境中受保护的 Windows 计算机，您可以手动收集性能日志，或者在系统性能低于出厂定义的阈值时启用自动收集诊断数据。请参阅 "ETL 数据收集的性能阈值"(第 105 页)。

收集的日志在发送给供应商进行分析之前会进行匿名处理。以下数据将从所有日志、消息、警报和错误消息中删除：

- 用户帐户
- 公司名称
- 受保护工作负载的名称

作为合作伙伴管理员，您可以为子租户中随机选择的代理程序或您管理的组织中的特定代理程序启用日志的自动收集。

作为公司管理员，您可以启用随机选择代理程序或组织中特定代理程序的日志自动收集。

注意

- 在适用于 Windows 的 Cyber Protection 代理程序 24.4.37758 版或更高版本上支持对单个工作负载的自动数据收集。
- 租户级别的性能数据收集在适用于 Windows 的 Cyber Protection 代理程序版本 25.03.XXXXX 或更高版本上受支持。

为了确保我们的支持建议信息充分，我们从环境中大约 10% 的代理程序中收集数据进行分析。

这不会覆盖单个工作负载上的设置。例如，如果在特定工作负载上禁用自动数据收集，则该工作负载将不包含在批量数据收集中。

多个代理程序的自动收集

若要启用租户中多个代理程序的性能数据自动收集

所需角色：合作伙伴管理员，客户管理员

1. 在 Cyber Protect Cloud 中控台中，转到**设置** > **代理程序**。
2. 在右侧的**操作**菜单中，单击**编辑性能监视器设置**。
3. 在**性能监视器**部分，启用切换 **自动收集和上传性能日志**。

自动收集的数据存储在受保护计算机的本地磁盘上，存储在 `C:\ProgramData\Acronis\ETLTool\ETL\` 文件夹中，经过匿名处理后发送给服务提供商进行分析。

注意

将 ETL 日志发送到云的限制为每 24 小时 3 次。

单个代理程序的自动更新

若要启用特定代理程序的性能数据自动收集

1. 在 Cyber Protect Cloud 中控台的公司级别中，导航到 **设置** > **代理程序**。
2. 在**代理程序**列表中，找到要启用性能监视器的代理程序。
3. 在右侧的 **操作** 菜单中，单击**详细信息**。
4. 向下滚动到**性能监视器**部分，然后启用**允许此代理程序自动收集性能日志**切换开关。

自动收集的数据存储在受保护计算机的本地磁盘上，位于文件夹 `C:\ProgramData\Acronis\ETLTool\ETL\` 中。

手动收集

若要手动收集性能数据

您可以按需收集性能数据。在这种情况下，无需启用性能监视器和自动收集性能数据。

1. 以管理员用户身份登录到受保护的计算机。
2. 在命令提示符下，运行以下命令之一：
   - `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o`
     ETL 跟踪的收集将一直运行，直到按下键盘上的 S 键，或者直到达到 3600 秒的最大时间限制。

- `"C:\Program Files\Common Files\Acronis\ETLTool\etl-tool.exe" -o -i X`
  其中 X 是以秒为单位的数据收集时间限制，最大值为 3600。您可以随时按键盘上的 S 键来停止收集。

手动收集的数据存储在受保护计算机的本地磁盘上，位于文件夹 `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\` 中

若要收集性能日志

1. 以管理员用户身份登录到受保护的计算机。
2. 定位所需的数据：
   - 自动收集的性能数据位于文件夹 `C:\ProgramData\Acronis\ETLTool\ETL\` 中
   - 按需收集的性能数据位于文件夹 `C:\ProgramData\Acronis\ETLTool\OnDemandCollect\ETL\` 中

ETL 跟踪也包含在 `sysinfo` 包中。

ETL 数据收集的性能阈值

您可以在环境中为受保护的 Windows 计算机启用性能数据的自动收集。监控在每个代理程序的 Cyber Protect Cloud 中控台中进行配置，并在系统性能低于预定义的阈值时启用诊断数据的自动收集。

当超出其中一个阈值时，自动数据收集将开始。

ETL 数据收集的默认阈值

下表描述了触发 ETL 数据自动收集的阈值。

参数	描述	默认值
"process-memory-consumption"	内存过度使用的阈值	
"allocated-memory-percent"		15
"minimum-allocated-memory-duration-seconds"		10
"allocated-memory-free-limit-seconds"		300
"process-disk-io"	磁盘 I/O 高用量阈值	
"maximum-operations-number"		10000
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-file-io"	文件 I/O 高用量阈值	
"maximum-operations-number"		30000

参数	描述	默认值
"maximum-transferred-bytes"		100000000
"estimation-period-seconds"		5
"process-cpu-usage"	高 CPU 消耗的阈值	
"cpu-percent"		15
"estimation-period-seconds"		10
"acronis-component-thresholds"	保护代理程序组件的性能	
"behavioral-engine"	行为引擎的阈值	
"average-system-utilization-percent"		50
"be-stats-event-number"		10
"avc-scan"	防病毒和防恶意软件保护组件的阈值	
"average-scan-duration-seconds"	最大平均扫描持续时间	3
"estimation-period-seconds"		10
"maximum-scan-duration-seconds"	单次扫描的最长持续时间	5

报告

要创建关于服务使用情况和操作的报告，请单击**报告**。

使用情况报告

使用情况报告提供有关使用服务的历史数据。使用情况报告会以 CSV 和 HTML 格式提供。

重要事项

产品 UI 中显示的存储使用值为二进制字节单位 – 以 Mib、Gib 和 Tib 为单位 – 尽管标签分别显示为 MB、GB 和 TB。例如，如果实际使用量为 3105886629888 字节，则 UI 中显示的值将正确显示为 2.82，但标签显示为 TB 而非 TiB。

报告类型

您可以选择以下报告类型之一：

- **当前使用情况**

  报告包含当前服务使用情况指标。

  使用情况指标在每个子租户的计费期内计算。如果报告中包含的租户具有不同的计费期，父租户的使用情况可能与子租户的使用情况之和不同。
- **当前使用情况分配**

  此报告仅对由外部调配系统管理的合作伙伴租户可用。在子租户的计费期与父租户的计费期不匹配时，此报告将发挥作用。报告包含在父租户当前计费期内计算的子租户的服务使用情况指标。确保父租户使用情况等于子租户使用情况之和。
- **一段时间的汇总**

  报告包含指定时间段结束时的服务使用情况指标，以及指定时间段开始和结束时指标的差异。

  注意

  仅在单位和客户租户级别报告本地存储使用数据。用户不会在摘要报告中收到有关本地存储使用情况的信息。
- **以天为单位的时间段**

  报告包含指定时间段内每天的服务使用情况指标及其变化。

报告范围

可以从以下值选择报告范围：

- **直接客户和合作伙伴**

  此报告将仅包含您正在操作的租户的直接子租户的服务使用情况指标。
- **所有客户和合作伙伴**

  此报告将包含您正在操作的租户的所有子租户的服务使用情况指标。
- **所有客户和合作伙伴(包括用户详细信息)**

  此报告将包含您正在操作的租户的所有子租户以及租户中所有用户的服务使用情况指标。

使用情况为零的指标

通过显示有关使用情况非零的指标的信息并隐藏有关使用情况为零的指标的信息，即可减少报告中的行数。

配置预定使用情况报告

预定报告涵盖上一个完整日历月的服务使用情况指标。报告在每个月第一天的 UTC 时间 23:59:59 生成，并在当月第二天发送。报告发送至租户的所有管理员，这些管理员已在用户设置中选中**预定使用情况报告**复选框。

注意

在事件已提交到云后，“按日期过滤”是根据时间戳进行的，而不是根据活动开始或完成的时间进行的。因此，如果与服务器的连接中断，则每日报告可能包含多天的数据。

启用或禁用预定报告

1. 请登录管理门户。
2. 请确保在提供给您的最上面的租户中进行操作。
3. 单击**报告** > **使用情况**。
4. 单击**预定**。
5. 选择或清除**发送每月总结报告**复选框。
6. 在**详细程度**中，选择报告范围。
7. [可选] 如果要从报告中排除使用情况为零的指标，请选择**隐藏使用情况为零的指标**。

配置自定义使用情况报告

此类型的报告可以按需生成，无法预定。报告将发送到您的电子邮件地址。

生成自定义报告

1. 请登录管理门户。
2. 导航到要为其创建报告的租户。
3. 单击**报告** > **使用情况**。
4. 选择**自定义**选项卡。
5. 在**类型**中，选择报告类型，如上所述。
6. [对**当前使用情况**报告类型不可用] 在**期间**中，选择报告期间：
   - **当前日历月**
   - **上一日历月**
   - **自定义**
7. [对**当前使用情况**报告类型不可用] 如果您要指定自定义报告期间，请选择开始和结束日期。否则，请跳过此步骤。
8. 在**详细程度**中，选择报告范围，如上所述。
9. [可选] 如果要从报告中排除使用情况为零的指标，请选择**隐藏使用情况为零的指标**。
10. 若要生成报告，请单击**生成并发送**。

操作报告

关于操作的报告可以包括任何一组**操作**仪表板小部件。默认情况下，所有小组件都会显示您正在其中进行操作的租户的概要信息。可以通过编辑小部件来为每个小组件或报告设置中的所有小部件分别更改租户。

根据小组件类型，报告包括时间范围内的数据或者浏览或报告生成时的数据。请参阅 "根据小组件类型报告的数据"(第 122 页)。

所有历史小组件都会显示同一时间范围内的数据。可以在报告设置中更改此范围。

可以使用默认报告，也可以创建自定义报告。

可以下载报告，也可以通过电子邮件以 XLSX (Excel) 或 PDF 格式发送该报告。

默认报告如下所示：

报告名称	描述
#CyberFit 分数(按计算机)	根据对每台计算机的安全指标和配置的评估，显示 #CyberFit 分数和改进建议。
警告	显示某一指定时间段内发生的警告。
备份扫描详细信息	显示有关备份中检测到威胁的详细信息。
每日活动	显示有关某一指定时间段内已执行活动的概要信息。
数据保护地图	显示有关计算机上所有重要文件的数量、大小、位置、保护状态的详细信息。
检测到威胁	按受阻止威胁的数量显示受影响计算机的详细信息，以及运行状况良好和易受攻击的计算机的详细信息。
已发现的设备	显示在客户端网络中发现的所有设备。
磁盘运行状况预测	显示 HDD/SSD 故障发生时间预测和当前磁盘状态。
现有漏洞	显示您组织中操作系统和应用程序的现有漏洞。该报告还会显示您网络中受影响计算机的每个列出产品的详细信息。
修补程序管理摘要	显示缺少的修补程序、已安装的修补程序和适用的修补程序的数量。可以深入了解报告以获取缺少/已安装修补程序的信息以及所有系统的详细信息。
概要	显示有关某一指定时间段内受保护设备的概要信息。
每周活动	显示有关某一指定时间段内已执行活动的概要信息。
软件库存记录	显示有关客户组织中 Windows 和 macOS 计算机上安装的所有软件的详细信息。
硬件清查	显示有关您客户端的组织中物理和虚拟 Windows 及 macOS 计算机上可用的所有硬件的详细信息。
远程会话	显示指定时间段内在客户组织中进行的远程桌面和文件传输会话的详细信息。

对报告的操作

添加

添加新报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在可用报告列表下，单击**添加报告**。
3. [添加预定义报告] 单击预定义报告的名称。
4. [添加自定义报告] 单击**自定义**，然后为报告添加小组件。
5. [可选] 拖放小组件，可重新排列它们。

查看

若要查看报告

- 要查看报告，请单击其名称。

编辑

若要编辑报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要编辑的报告。
3. 在屏幕的右上角，单击**设置**。
4. 编辑报告，然后单击**保存**。

删除

删除报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要删除的报告。
3. 在屏幕的右上角，单击省略号图标 (...)，然后单击 **删除报告**。
4. 在确认窗口中，单击**删除**。

预定

若要安排报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要预定的报告。
3. 在屏幕的右上角，单击**设置**。
4. 在 **已预订** 旁边，启用开关。
   - 指定收件人的电子邮件地址。
   - 选择报告的格式。

     - **注意**
       可以在 PDF 文件中导出多达 1,000 个项目，在 XLSX 文件中导出多达 10,000 个项目。PDF 和 XLSX 文件中的时间戳使用计算机的本地时间。

   - 选择报告的语言。
   - 配置预定。
5. 单击**保存**。

下载

下载报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择报告。
3. 请在屏幕的右上角单击**下载**。
4. 选择报告的格式。

因此，所选格式的文件将下载到您的计算机。

如果您选择了 **Excel 和 PDF**，则会将 ZIP 文件下载到您的计算机。

发送

发送报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择报告。
3. 在屏幕的右上角，单击**发送**。
4. 指定收件人的电子邮件地址。
5. 选择报告的格式。
6. 单击**发送**。

导出结构

导出报告结构

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择报告。
3. 在屏幕的右上角，单击省略号图标 (...)，然后单击 **导出**。

因此，报告结构将作为 JSON 文件保存在计算机上。

转储数据

转储报告数据

您可以将自定义期间的所有数据导出到 CSV 文件，而无需对其进行筛选，并将 CSV 文件发送至电子邮件收件人。CSV 文件仅包含报告中包含的小组件的数据。

注意
可以在一个 CSV 文件中导出多达 150,000 个项目。CSV 文件中的时间戳使用协调世界时 (UTC)。

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要转储其数据的报告。
3. 在屏幕的右上角，单击省略号图标 (...)，然后单击 **转储数据**。
4. 指定收件人的电子邮件地址。
5. 在**时间范围**中，指定要转储数据的自定义时间段。

   注意
   准备较长时间段的 CSV 文件需要花费更多时间。

6. 单击**发送**。

执行摘要

执行摘要报告提供指定时间范围内客户环境及其受保护设备的保护状态的概述。

执行摘要报告包括带有动态小组件的各部分，这些小组件可以显示与以下云服务的客户端使用相关的主要性能指标：备份、反恶意软件保护、漏洞评估、修补程序管理、数据丢失预防、公证、Disaster Recovery，以及 Files Sync & Share。

可以通过几种方式自定义报告。

- 添加或删除各部分。
- 更改各部分的顺序。
- 重命名各部分。
- 将小组件从一个部分移动到另一个部分。
- 更改每个部分中小组件的顺序。
- 添加或删除小组件。
- 自定义小组件。

可以生成 PDF 和 Excel 格式的执行摘要报告，并将其发送给利益相关方或客户的组织的所有者，这样他们可以轻松查看所提供服务的技术和商业价值。

合作伙伴管理员可以生成执行摘要报告并将其仅发送给直接客户。如果有更复杂的租户层次结构具有子合作伙伴，则子合作伙伴必须生成报告。

执行摘要小组件

可以从执行摘要报告中添加或删除部分和小组件，从而控制报告中包含哪些信息。

工作负载概述小组件

下表提供了有关**工作负载概述**部分中小组件的更多信息。

小部件	描述
云工作负载保护状态	此小组件显示生成报告时按类型划分的受保护和不受保护的云工作负载的数量。受保护的云工作负载是应用了至少一个备份计划的工作负载。不受保护的云工作负载是没有应用备份计划的工作负载。以下云工作负载类型显示在图表中(以从 A 到 Z 的字母顺序)： • Google Workspace Drive • Google Workspace Gmail • Google Workspace Shared Drive • 托管的 Exchange 邮箱 • Microsoft 365 邮箱 • Microsoft 365 OneDrive • Microsoft 365 SharePoint Online • Microsoft Teams • 网站 对于某些工作负载类型，使用以下工作负载组： • Microsoft 365：用户、组、公用文件夹、Teams 和站点集合

小部件	描述
	• Google Workspace：用户和共享驱动器 • 托管的 Exchange：用户 如果一个工作负载组中有 10 000 多个工作负载，则小组件不会显示相应工作负载的任何数据。 例如，如果客户有一个包含 10 000 个邮箱的 Microsoft 365 帐户以及面向 500 名用户的 OneDrive 服务，则它们全都属于“用户”工作负载组。这些工作负载的总数是 10 500，超过了工作负载组 10 000 的限制。因此，小组件将隐藏相应的工作负载类型：Microsoft 365 邮箱和 Microsoft 365 OneDrive。
网络安全保护摘要	小组件显示指定时间范围内网络安全保护性能的关键指标。 **已备份数据** - 云和本地存储中创建的存档的总大小。 **缓解的威胁** - 所有设备中阻止的恶意软件总数。 **阻止的恶意 URL** - 所有设备上阻止的 URL 总数。 **已修补的漏洞** - 在所有设备上通过软件修补程序安装修复的漏洞总数。 **安装的修补程序** - 所有设备上安装的修补程序总数。 **DR 保护的服务器** - 受Disaster Recovery保护的服务器总数。 **File Sync & Share 用户** - 使用 Cyber Files 的最终和来宾用户总数。 **公证的文件** - 公证的文件总数。 **电子签名的文档** - 电子签名的文档总数。 **已阻止的外围设备** - 已阻止的外围设备的总数。
工作负载网络状态	此小组件指示隔离和连接了多少工作负载(工作负载的正常状态)。 选择相关的客户，显示的工作负载视图经过过滤以显示隔离的工作负载。单击“已连接”值以查看过滤了代理程序列表的工作负载，以显示连接的工作负载(对于选定的客户)。
工作负载保护状态	小组件显示生成报告时按类型划分的受保护和不受保护的工作负载。受保护的工作负载是应用了至少一个防护或备份计划的工作负载。不受保护的工作负载是没有应用保护或备份计划的工作负载。下列工作负载算在内： **服务器** - 物理服务器和域控制器服务器。 **工作站** - 物理工作站。 **虚拟机** - 基于代理程序和无代理程序的虚拟机。 **Web 托管服务器** - 具有安装的 cPanel 或 Plesk 的虚拟或物理服务器。 **移动设备** - 物理移动设备。 一个工作负载可以属于多个类别。例如，Web 托管服务器计入两个类别 - **服务器**和 **Web 托管服务器**。

小部件	描述
已发现的设备	该小组件显示在指定时间段内在您的客户的网络中发现的设备的以下信息： **客户名称** **文件夹名称** **设备名称** **设备类型** **操作系统** **制造商** **型号** **IP 地址** 您可以编辑小组件，并通过租户、组织单元、设备类型、发现类型、首次发现日期、上次发现日期、IP 地址、MAC 地址和发现类型来筛选显示的信息。

反恶意软件保护小组件

下表提供了有关**威胁防御**部分中小组件的更多信息。

小部件	描述
文件的反恶意软件扫描	小组件显示指定日期范围内，设备的按需反恶意软件扫描结果。 **文件** - 已扫描文件的总数 **干净** - 干净文件的总数 **检测到，已隔离** - 已隔离的被感染文件的总数 **检测到，未隔离** - 未隔离的被感染文件的总数 **受保护的设备** - 应用了反恶意软件保护策略的设备的总数 **注册设备的总数** - 报告生成时注册设备的总数
备份的反恶意软件扫描	小组件使用以下指标，显示指定日期范围内备份的反恶意软件扫描结果： • 扫描的恢复点的总数 • 干净恢复点的数量 • 具有不受支持分区的干净恢复点的数量 • 被感染的恢复点的数量。此指标包括具有不受支持分区的被感染恢复点的数量。
阻止的 URL	在指定日期范围内，小组件显示按网站类别分组的阻止的 URL 数。 小组件列出了具有阻止的 URL 最大数的七个网站类别，把其余的网站类别都归入**其他**。 有关网站类别的更多信息，请参阅 Cyber Protection 中的 URL 过滤主题。

小部件	描述
安全性事件刻录	此小组件显示选定公司的关闭事件中的效率;针对一段时间的关闭事件的数量测量打开事件数。 将鼠标悬停在某列上可以查看在选定日发生的关闭和打开事件的明细。在括号中显示的 % 值表示与以前时间段比较的上升或下降。
事件 MTTR	此小组件显示用于安全性事件的平均解决时间。它指示调查和解决事件的快速程度。 单击某个列以根据严重性(**严重**、**高**和**中**)查看事件明细,并可查看解决不同严重性级别花费多少时间的指示。在括号中显示的 % 值表示与以前时间段比较的上升或下降。
威胁状态	此小组件显示公司工作负载的当前威胁状态(不管工作负载数),并突出显示当前未迁移并需要调查的事件数量。小组件还指示已迁移的事件数(由系统手动和/或自动)。
保护技术检测到的威胁	在指定日期范围内,小组件显示按以下保护技术分组的检测到的威胁数: • 反恶意软件扫描 • 行为引擎 • 加密挖矿防护 • 漏洞利用预防 • 勒索软件主动防护 • 实时保护 • URL 过滤

备份小组件

下表提供了有关**备份**部分中小组件的更多信息。

小部件	描述
备份的工作负载	小组件按备份状态显示已注册工作负载的总数。 **已备份** - 在报告日期范围内,已备份(至少执行了一次成功的备份)的工作负载数。 **未备份** - 在报告日期范围内,未备份(未执行成功的备份)的工作负载数。
磁盘运行状况(按物理设备)	小组件基于物理设备磁盘的运行状况状态,显示物理设备的汇总运行状况状态。 **正常** - 此磁盘运行状况状态与值 [70-100] 相关。当该设备的所有磁盘的状态都是**正常**时,该设备的状态为**正常**。 **警告** - 此磁盘运行状况状态与值 [30-70] 相关。当至少一个磁盘的状态为**警告**时,以及当没有磁盘的状态为**错误**时,设备的状态为**警告**。 **错误** - 此磁盘运行状况状态与值 [0-30] 相关。当至少一个磁盘的状态为**错误**时,设备的状态为**错误**。

小部件	描述
	正在计算磁盘数据 - 当设备的磁盘状态是尚未计算时，该设备的状态是**正在计算磁盘数据**。
备份存储使用情况	在指定的时间范围内，小组件显示云和本地存储中备份的总数和总大小。

漏洞评估和修补程序管理小组件

下表提供了有关**漏洞评估和修补程序管理**部分中小组件的更多信息。

小部件	描述
已修补的漏洞	小组件显示指定日期范围内的漏洞评估性能结果。 **总数** - 已修补的漏洞总数。 **Microsoft 软件漏洞** - 所有 Windows 设备上已修复的 Microsoft 漏洞总数。 **Windows 第三方软件漏洞** - 所有 Windows 设备上已修复的 Windows 第三方漏洞总数。 **扫描的工作负载** - 在指定日期范围内至少成功扫描漏洞一次的设备总数。
已安装的修补程序	小组件显示指定日期范围内的修补程序管理性能结果。 **已安装** - 成功安装在所有设备上的修补程序总数。 **Microsoft 软件修补程序** - 已安装在所有 Windows 设备上的 Microsoft 软件修补程序总数。 **Windows 第三方软件修补程序** - 已安装在所有 Windows 设备上的 Windows 第三方软件修补程序总数。 **修补的工作负载** - 成功修补的设备总数(在指定日期范围内至少成功安装了一个修补程序)。

软件小组件

下表提供了有关**软件**部分中小组件的更多信息。

小部件	描述
安装状态	此小组件按状态显示在你的客户管理的设备上已安装的活动总数。单击圆环图的某个部分，将重定向到**活动**页面，该页面仅显示具有相应状态的活动，按时间顺序排列。
卸载状态	此小组件按状态显示从你的客户管理的设备上卸载的活动总数。单击圆环图的某个部分，将重定向到**活动**页面，该页面仅显示具有相应状态的活动，按时间顺序排列。
软件安装历史记录	此小组件提供你的客户管理的设备上远程软件安装的详细状态信息。单击**安装状态**列中的状态，将重定向到**活动**页面，该页面将按时间顺序显示具有相应状态的活动。

小部件	描述
软件卸载历史记录	该小组件提供你的客户管理的设备上远程软件卸载的详细状态信息。单击**卸载状态**列中的状态，将重定向到**活动**页面，该页面将按时间顺序显示具有相应状态的活动。

Disaster Recovery 小组件

下表提供了有关**灾难恢复**部分中小组件的更多信息。

小部件	描述
Disaster Recovery 统计信息	小组件显示指定日期范围内的Disaster Recovery 关键性能指标。 **生产故障转移** - 指定时间范围内生产故障转移操作的数量。 **测试故障转移** - 指定时间范围内执行的测试故障转移操作的总数。 **主服务器** - 在报告生成时的主服务器总数。 **恢复服务器** - 在报告生成时的恢复服务器总数。 **公共 IP** - 公共 IP 地址的总数(在报告生成时)。 **已使用的总计算点** - 指定时间范围内使用的计算点的总数。
Disaster Recovery 服务器已测试	小组件显示有关受Disaster Recovery 保护并经过测试故障转移测试的服务器的信息。 小组件显示以下指标： **服务器受保护** - 在报告生成时受Disaster Recovery 保护的服务器的数量(至少有一台恢复服务器的服务器)。 **已测试** - 在所有受Disaster Recovery 保护的服务器中，在选定的时间范围内使用测试故障转移对其进行了测试的Disaster Recovery 保护的服务器数。 **未测试** - 在所有受Disaster Recovery 保护的服务器中，在选定的时间范围内未使用测试故障转移对其进行测试的Disaster Recovery 保护的服务器数。 小组件还显示在报告生成时，Disaster Recovery 存储(以 GB 为单位)的大小。它是云服务器的备份大小的总和。
受Disaster Recovery 保护的服务器	小组件显示有关受Disaster Recovery 保护的服务器和不受保护的服务器的信息。 小组件显示以下指标： 在报告生成时客户租户中注册的服务器总数。 **受保护** - 在报告生成时所有注册的服务器中，受Disaster Recovery 保护的服务器的数量(至少有一台恢复服务器和完整的服务器备份)。 **不受保护** - 在报告生成时所有注册的服务器中，不受保护的服务器总数。

数据丢失预防小组件

以下主题提供了有关**数据丢失预防**部分中已阻止外围设备的详细信息。

小组件显示阻止的设备总数以及指定日期范围内按设备类型的阻止的设备总数。

- 可移动存储
- 加密的可移动设备
- 打印机
- 剪贴板 - 包括剪贴板和屏幕截图捕获设备类型。
- 移动设备
- 蓝牙
- 光盘驱动器
- 软盘驱动器
- USB - 包括 USB 端口和重定向的 USB 端口设备类型。
- FireWire
- 已映射的驱动器
- 重定向的剪贴板 - 包括重定向的剪贴板传入和重定向的剪贴板传出设备类型.

小组件显示具有已阻止设备的最高数量的前七大设备类型，并将其余设备类型归入**其他**设备类型。

File Sync & Share 小组件

下表提供了有关 **File Sync & Share** 部分中小组件的更多信息。

小部件	描述
File Sync & Share 统计信息	小组件显示以下指标： **已使用的云存储总量** - 所有用户的总存储使用量。 **最终用户** - 最终用户的总数。 **每个最终用户使用的平均存储** - 每个最终用户的平均存储使用量。 **来宾用户** - 来宾用户的总数。
File Sync & Share 存储使用量 (按最终用户)	小组件显示具有在以下范围内存储使用量的 File Sync & Share 最终用户的总数： • 0 - 1 GB • 1 - 5 GB • 5 - 10 GB • 10 - 50 GB • 50 - 100 GB • 100 – 500 GB • 500 - 1 TB • 1 TB 以上

公证小组件

下表提供了有关**公证**部分中小组件的更多信息。

小部件	描述
网络安全公证统计信息	小组件显示以下公证指标： **已使用的公证云存储** - 用于"公证"服务的存储的总大小。 **公证的文件** - 公证的文件总数。 **电子签名的文档** - 电子签名的文档和电子签名的文件的总数。
最终用户的公证文件	显示所有最终用户的公证文件的总数。根据用户所有的公证文件数对用户分组。 • 最多 10 个文件 • 11 - 100 个文件 • 101 - 500 个文件 • 501 - 1000 个文件 • 1000 多个文件
最终用户的电子签名文档	小组件显示所有最终用户的电子签名的文档和电子签名的文件的总数。根据用户所有的电子签名的文档和文件数对用户分组。 • 最多 10 个文件 • 11 - 100 个文件 • 101 - 500 个文件 • 501 - 1000 个文件 • 1000 多个文件

配置执行摘要报告的设置

可以更新在创建执行摘要报告时配置的报告设置。

更新执行摘要报告的设置

1. 在管理中控台中，转至**报告** > **执行摘要**。
2. 单击要更新的执行摘要报告的名称。
3. 单击**设置**。
4. 根据需要更改字段的值。
5. 单击**保存**。

创建执行摘要报告

您可以创建执行摘要报告、预览其内容、配置报告的收件人，以及预定自动发送报告的时间。

创建执行摘要报告的步骤

1. 在管理中控台中，转至**报告** > **执行摘要**。
2. 单击**创建执行摘要报告**。
3. 在**报告名称**中，键入报告的名称。
4. 选择报告的收件人。
   - 如果要将报告发送给所有直接客户，则选择**发送给所有直接客户**。
   - 如果要将报告发送给特定客户
     a. 清除**发送给所有直接客户**。
     b. 单击**选择联系人**。
     c. 选择特定客户。可以使用“搜索”轻松查找特定联系人。
     d. 单击**选择**。
5. 选择范围：**30 天**或**本月**
6. 选择文件格式：**PDF**、**Excel** 或 **Excel 和 PDF**。
7. 配置预定设置。
   - 如果要将报告按特定日期和时间发送给收件人：
     a. 启用**预定**选项。
     b. 单击**日**字段，清除“最后一天”字段，然后单击想要设置的日期。
     c. 在**时间**字段中，输入想要设置的小时。
     d. 单击**应用**。
   - 如果想要创建报告而不将其发送给收件人，则禁用**预定**选项。
8. 单击**保存**。

自定义执行摘要报告

可以确定哪些信息要包含在执行摘要报告中。可以添加或删除各部分、添加或删除小组件、重命名各部分、自定义小组件以及拖放小组件和各部分来更改信息在报告中的显示顺序。

要添加部分

1. 依次单击**添加项目** > **添加部分**。
2. 在**添加部分**窗口中，键入部分名称或使用默认部分名称。
3. 单击**添加到报告**。

重命名部分

1. 在要重命名的部分中，单击**编辑**。
2. 在**编辑部分**窗口中，键入新名称。
3. 单击**保存**。

删除部分

1. 在要删除的部分中，单击**删除部分**。
2. 在**删除部分**确认窗口中，单击**删除**。

使用默认设置添加小组件到部分

1. 在要添加小组件的部分中，单击**添加小组件**。
2. 在**添加小组件**窗口中，单击要添加的小组件。

添加自定义小组件到部分

1. 在要添加小组件的部分中，单击**添加小组件**。
2. 在**添加小组件**窗口中，找到要添加的小组件，然后单击**自定义**。
3. 根据需要配置字段。
4. 单击**添加小组件**。

使用默认设置添加小组件到报告

1. 依次单击**添加项目 > 添加小组件**。
2. 在**添加小组件**窗口中，单击要添加的小组件。

添加自定义小组件到报告

1. 单击**添加小组件**。
2. 在**添加小组件**窗口中，找到要添加的小组件，然后单击**自定义**。
3. 根据需要配置字段。
4. 单击**添加小组件**。

重置小组件的默认设置的步骤

1. 在要自定义的小组件中，单击**编辑**。
2. 单击**重置为默认值**。
3. 单击**完成**。

自定义小组件的步骤

1. 在要自定义的小组件中，单击**编辑**。
2. 必要时编辑字段。
3. 单击**完成**。

发送执行摘要报告

可以按需发送执行摘要报告。在这种情况下，**预定**设置将被忽略，并且立即发送报告。当发送报告时，系统使用在**设置**中配置的“收件人”、“范围”和“文件格式”值。可以在发送报告前手动更改这些设置。有关详细信息，请参阅 "配置执行摘要报告的设置"(第 119 页)。

发送执行摘要报告的步骤

1. 在管理门户中，转至**报告 > 执行摘要**。
2. 单击要发送的执行摘要报告的名称。
3. 单击**立即发送**。

   系统将执行摘要报告发送给选定的收件人。

报告中的时区

报告中使用的时区取决于报告类型。下表包含供您参考的信息。

报告位置和类型	报告中使用的时区
管理门户> 监视 > 操作 (小部件)	报告生成的时间是浏览器运行时所在计算机的时区。
管理门户> 监视 > 操作 (导出为 PDF 或 xslx)	• 导出的报告的时间戳是在用于导出报告的计算机所在的时区中。 • 报告中显示的活动的时区为 UTC。
管理门户> 报告 > 使用情况 > 预定的报告	• 报告于每个月第一天的 UTC 时间 23:59:59 生成。 • 报告于当月的第二天发送。
管理门户> 报告 > 使用情况 > 自定义报告	报告的时区和日期为 UTC。
管理门户> 报告 > 操作 (小部件)	• 报告生成的时间是浏览器运行时所在计算机的时区。 • 报告中显示的活动的时区为 UTC。
管理门户> 报告 > 操作 (导出为 PDF 或 xslx)	• 导出的报告的时间戳是在用于导出报告的计算机所在的时区中。 • 报告中显示的活动的时区为 UTC。
管理门户> 报告 > 操作 (预定交付)	• 报告交付的时区为 UTC。 • 报告中显示的活动的时区为 UTC。
管理门户> 用户 > 活动警报的每日概述	• 该报告每天于 UTC 时间 10:00 和 23:59 之间发送一次。发送报告的具体时间取决于数据中心中的工作负载。 • 报告中显示的活动的时区为 UTC。
管理门户> 用户 > 网络安全保护状态通知	• 活动完成后将发送此报告。 **注意** 视数据中心中的工作负载而定，某些报告可能会延后发送。 • 报告中的活动的时区为 UTC。

根据小组件类型报告的数据

根据它们所显示的数据范围，仪表板上的小组件分为两类：

- 在浏览或报告生成时显示实际数据的小组件。
- 显示历史数据的小组件。

在报告设置中配置日期范围以转储特定时间段的数据时，所选时间范围将仅适用于显示历史数据的小组件。对于浏览时显示实际数据的小组件，时间范围参数不适用。

下表列出了可用的小组件及其数据范围。

小组件名称	小组件和报告中显示的数据
#CyberFit 分数(按计算机)	实际
5 个最新警告	实际
活动警告详细信息	实际
活动警告摘要	实际
活动	历史
活动列表	历史
警告历史记录	历史
备份的反恶意软件扫描	历史
文件的反恶意软件扫描	历史
备份扫描详细信息(威胁)	历史
备份状态	历史 - 在**运行总计**和**成功运行次数**列中 实际 - 在其他所有列中
备份存储使用情况	历史
已阻止的外围设备	历史
已阻止 URL	实际
云应用程序	实际
云工作负载保护状态	实际
Cyber protection	实际
网络安全保护摘要	历史
数据保护地图	历史
设备	实际
灾难恢复服务器已测试	历史
灾难恢复统计信息	历史
已发现的设备	实际
磁盘运行状况概述	实际
磁盘运行状况状态	实际
磁盘运行状况(按物理设备)	实际
最终用户的电子签名文档	实际

现有漏洞	历史
File Sync & Share 统计信息	实际
File Sync & Share 存储使用情况(按最终用户)	实际
硬件更改	历史
硬件详细信息	实际
硬件清查	实际
历史警告摘要	历史
位置汇总	实际
按类别划分的缺少更新	实际
未保护	实际
最终用户的公证文件	实际
公证统计信息	实际
修补程序安装历史记录	历史
修补程序安装状态	历史
修补程序安装摘要	历史
已修补的漏洞	历史
已安装的修补程序	历史
保护状态	实际
最近受影响	历史
远程会话	历史
安全性事件刻录	历史
安全性事件 MTTR	历史
受灾难恢复保护的服务器	实际
软件库存记录	实际
软件概述	历史
威胁状态	实际
保护技术检测到的威胁	历史
每个工作负载的主要事件分发	实际
易受攻击的计算机	实际

工作负载网络状态	实际
备份的工作负载	历史
工作负载保护状态	实际

使用计算器估算 Cyber Protect Cloud 成本

如果您正在使用 Cyber Protect Cloud 的试用版，则可以使用计算器估算您的成本。

注意
Cyber Protect Cloud 计算器只能由试用合作伙伴从管理门户访问，而其客户或非试用合作伙伴则无法访问。

使用计算器估算 Cyber Protect Cloud 成本

1. 单击管理门户左下角的**计算每月成本**。
2. 为计划的负载指定以下详细信息：
   - 按工作负载类型划分的工作负载数。例如，指定虚拟机、工作站、托管服务器、Google Workplace 席位、移动设备和 Microsoft 365 席位的数量。
   - 数据存储的详细信息，例如数据中心的位置和存储量。
3. [可选] 指定计划使用的 Advanced Backup、安全或管理选项，以及每个选项的工作负载数。
4. 选择许可模式：按工作负载或按 GB。

您将在右侧看到每月的估算成本。

可以通过单击相应按钮、与专家交谈或请求云顾问直接联系您来成为合作伙伴 - 一切操作源于计算器页面。

还可以通过单击管理门户左下角的**联系销售**，来发起与销售部门的沟通。

Copilot

Copilot 是产品中的 AI 聊天助手。Copilot 使用官方 Cyber Protect Cloud 文档和许可指南作为源，并生成答案以协助您并引导您完成以下任务：

- 了解产品的工作原理。
- 了解许可主题。
- 了解如何配置租户。
- 了解如何配置服务。
- 以最小成本即可开始使用产品。
- 快速获取您对如何使用功能的问题的答案。

如果 Copilot 无法回答您的问题，它可以将聊天转接给实时专家或提交工单（如果当前暂无专家可提供服务）。

您不仅可以用英语与在专家聊天，还可以用您的母语与其聊天。Copilot 将自动翻译所有非英语消息，以便您可以用母语与专家交流。

您可以取消固定聊天窗口，并将其移至应用程序窗口内的任何位置。因此，您可以调整聊天的位置，以便在最方便的位置进行聊天。

使用 Copilot

Copilot 可向您提供有关产品和许可模式的信息，并协助您完成常见的配置任务。当您需要更专业的协助时，Copilot 可将您与实时专家进行连线。如果当前没有专家可以提供服务，Copilot 可为您创建工单。专家将尽快就此工单与您联系。

您可以对与 Copilot 的聊天进行评分并留下反馈。

开始聊天

若要开始与 Copilot 的聊天

1. 单击 **Copilot**。
2. 在打开的聊天窗口中，请执行以下操作之一：
   - 若要获取有关预定义常见主题或问题的信息，请单击它。
   - 若要获取有关其他主题的信息或其他问题的答案，请在消息字段中键入信息，然后按 Enter 键或单击箭头图标。
3. 重复步骤 2，直到获得必要的信息。
4. [可选] 若要复制 Copilot 的回复，请单击回复下方的复制图标。
   文本已复制到计算机的剪贴板。

与实时专家交谈

若要开始与实时专家聊天

1. 单击 **Copilot**。
2. 打开新的或现有的聊天。
3. 要求 Copilot 为您连接到实时专家。
4. 与专家聊天。

> **注意**
> 如果专家关闭聊天，聊天窗口中将显示反馈表单。

对响应进行评分

您可以在聊天中对 Copilot 的响应进行评分。

若要对响应进行评分

1. 单击 **Copilot**。
2. 在打开的聊天窗口中，请执行以下操作之一：

- 若要获取有关预定义常见主题或问题的信息，请单击它。
- 若要获取有关其他主题的信息或其他问题的答案，请在消息字段中键入信息，然后按 Enter 键或单击箭头图标。

3. 若要对 Copilot 的响应进行评分，请执行以下操作之一：
   - 如果该响应有帮助，请单击其下方的“喜欢”图标。
   - 如果该响应没有帮助，请单击其下方的“不喜欢”图标。

对聊天进行评分

退出时，您可以对包含 Copilot 响应的聊天进行评分。

若要对聊天进行评分

1. 在活动聊天窗口中，单击 **X** 图标。
   反馈表单将会打开。
2. 对您的聊天体验进行评分(1-差，5-好)。
3. 在文本字段中输入您的反馈。

   注意
   此步骤对于分数 1-4 是强制性的，但您可以跳过分数 5。

4. 单击**发送反馈**。
   聊天窗口将关闭。

退出聊天

退出与 Copilot 的聊天时，聊天记录不会被删除。系统会询问您对体验的评分。

若要退出聊天

1. 在活动聊天窗口中，单击 **X** 图标。
   反馈窗口将打开。您可以发送反馈或跳过此步骤。
2. [可选] 如果您不想发送反馈，请单击 **跳过**。
   聊天窗口将关闭。在您删除聊天之前，您可以从聊天列表访问聊天。如果您未发送反馈，则每次关闭聊天时也会显示该表单。

管理聊天

您可以查看与 Copilot 的聊天会话列表，并删除不再需要的聊天会话。

查看聊天列表并删除聊天

1. 单击 **Copilot**。
2. 单击三层图标，以查看聊天列表。
3. 将鼠标悬停在要删除的聊天上，然后单击垃圾桶图标。

高级保护包

除了 保护 服务之外，还可以启用高级保护包，但需要另外付费。高级保护包提供的独特功能不会与标准功能集和其他高级包重叠。客户端可以使用一个、多个或所有高级包来保护其工作负载。高级保护包可用于 保护 服务的两种计费模式 -“按工作负载”和“按 GB”。

Advanced File Sync & Share 功能可以通过 File Sync & Share 服务启用。在这两种记账方式(按用户和按流量) 下都可用。

可以启用以下高级保护包：

- Advanced Backup
  Advanced Backup 包中包含许多针对工作站、服务器、虚拟机、网络托管服务器、Google Workspace 席位和 Microsoft 365 席位的单独许可证和配额。
- Advanced Management (RMM)
- Advanced Security + XDR (Extended Detection and Response)
- Advanced Data Loss Prevention
- Advanced Disaster Recovery
- Advanced Email Security
- Advanced File Sync & Share
- 高级安全意识培训
  让个人了解有关信息安全风险和威胁的知识，培训他们识别模拟网络钓鱼电子邮件，并为他们提供保护自己和组织免受网络攻击所需的知识和技能。

注意
仅当高级包扩展的功能启用时，才可以使用该高级包。标准服务功能禁用后，用户就无法使用高级功能。例如，如果禁用 保护 功能，则用户无法使用 Advanced Backup 包的功能。

如果启用了高级保护包，则其功能会显示在保护计划中，并标有高级功能图标 。当用户尝试启用该功能时，系统会提示用户需要另外计费。

如果高级保护包未启用，但追加销售已打开，则高级保护功能会显示在保护计划中，但无法访问使用。将显示一条消息，以提示用户与管理员联系来启用所需的高级功能集。

如果高级保护包未启用且追加销售已关闭，客户不会在其保护计划中看到高级功能。

Cyber Protect 服务中包含的功能和高级包

在 Cyber Protect 中启用服务或功能集时，将启用默认包含且可用的许多功能。此外，还可以启用高级保护包。

以下部分包含 Cyber Protect 服务功能和高级包的高级概述。有关产品的完整列表，请参阅 Cyber Protect 许可指南。

“保护”服务中包含的高级功能

“保护”服务中包含的高级功能

功能组	包含的标准功能	高级功能
Security + XDR	• #CyberFit Score • 漏洞评估 • 防病毒和反恶意软件保护:基于云签名的文件检测(无实时保护,仅计划扫描)* • 防病毒和反恶意软件保护:预执行基于人工智能 (AI) 的文件分析器,基于行为的网络安全引擎 • Microsoft Defender 管理 *为了检测零日攻击,Cyber Protect 会使用启发式扫描规则和算法来查找恶意命令。	Advanced Security + XDR 包包括 XDR、Endpoint Detection and Response (EDR) 以及托管检测和响应 (MDR): • 与第三方解决方案集成,包括 Advanced Email Security、Microsoft 365 协作应用程序以及 Microsoft Entra ID • 在集中式事件页面中管理事件 • 可视化事件的范围和影响 • 建议和补救措施 • 使用威胁源检查对您工作负载的公开披露的攻击 • 将安全事件存储 180 天 • 托管检测和响应 (MDR) • 反勒索软件保护:Active Protection • 基于本地签名检测的防病毒和反恶意软件保护(有实时保护) • 漏洞利用预防 • URL 过滤 • 终端防火墙管理 • 取证备份、扫描备份以查找恶意软件、安全恢复、企业允许列表 • 智能保护计划(与 CPOC 警报集成) • 集中式备份扫描恶意软件 • 远程擦除 • Microsoft Defender Antivirus • Microsoft Security Essentials • Microsoft 365 邮箱恶意软件备份扫描 有关如何启用“Advanced Security + EDR”的信息,请参阅 "启用 “Advanced Security + XDR”"(第 133 页)。
数据丢失预防	• 设备控制	• 内容感知预防工作负载通过外围设备和网络通信丢失数据 • 预建自动检测个人身份信息 (PII)、受保护的运行状况信息 (PHI) 和支付卡行业数据安全标准 (PCI DSS) 数据以及“标记为机密”类别中的文档

功能组	包含的标准功能	高级功能
		• 通过可选的最终用户帮助自动创建数据丢失预防策略 • 通过基于学习的自动策略调整实现自适应数据丢失预防 • 基于云的集中式审核日志记录、警报和最终用户通知
管理	对于终端： • 群组管理 • 保护计划的集中式管理 • 硬件清查 • 远程控制 • 远程操作 • 每个技术人员的并发连接 • 远程连接协议：RDP • 四个监视器 • 基于阈值的监视 • 显示最后登录的用户 • 适用于 Windows 和 macOS 的漏洞评估 对于 Microsoft 365 席位： • 使用最佳实践基线、用户管理和用户上线审核 Microsoft 365 安全态势	Advanced Management (RMM) 包包含以下功能： 对于终端： • 修补程序管理 • 磁盘运行状况 • 软件库存记录 • Windows 操作系统的第三方产品漏洞评估 • 故障安全修补 • 网络安全脚本 • 远程协助 • 文件传输和共享 • 选择要连接的会话 • 在多视图中观察工作负载 • 连接模式：控制、仅查看和隔离 • 通过“Quick Assist”应用程序连接 • 远程连接协议：NEAR 和 Apple 屏幕共享 • NEAR 连接的会话记录 • 屏幕截图传输 • 会话历史记录报告 • 24 个监视器 • 基于阈值的监视 • 基于异常的监视 • 使用 DeployPilot 远程部署软件 • 第三方 Windows 应用程序的漏洞评估 • 地理位置追踪 • Helpdesk 聊天 对于 Microsoft 365 席位： • 基线偏差的自动和手动修复，以及移除用户
电子邮件安全	无	为您的 Microsoft 365 和 Gmail 邮箱提供实时保护：

功能组	包含的标准功能	高级功能
		• 反恶意软件和反垃圾邮件 • 电子邮件中 URL 扫描 • DMARC 分析 • 防网络钓鱼 • 假冒保护 • 附件扫描 • 内容拆解与重建 • 信任图 请参阅配置指南。
安全意识培训		• 安全意识培训 • 合规性培训 • 网络钓鱼模拟 • 策略确认管理
Cyber Disaster Recovery Cloud	可以使用Disaster Recovery标准功能来为您的工作负载测试Disaster Recovery方案。 请注意可用的Disaster Recovery标准功能及其限制： • 在隔离的网络环境中测试故障转移。每月限制为 32 个计算点，并且最多可以同时进行 5 个测试故障转移操作。 • 恢复服务器配置：1 个 CPU 和 2 GB RAM，1 个 CPU 和 4 GB RAM，2 个 CPU 和 8 GB RAM。 • 可用于故障转移的恢复点数量：仅备份后立即可用的最后一个恢复点。 • 可用连接模式："仅云"和"点到站点"。 • VPN 网关的可用性：如果 VPN 网关在上次测试故障转移完成之后的 4 个小时内处于不活动状态，则该 VPN 网关将暂时停用，并会在您启动测试故障转移时再次部署。 • 云网络的数量：1. • Internet 访问 • 使用 Runbook 进行的操作：创建和编辑。	可以启用 Advanced Disaster Recovery 包，并使用完整的Disaster Recovery功能保护工作负载。 请注意可用的Disaster Recovery高级功能： • 生产故障转移 • 在隔离的网络环境中测试故障转移。 • 可用于故障转移的恢复点数量：创建恢复服务器后可用的所有恢复点。 • 主服务器 • 恢复/主服务器配置：无限制 • 可用连接模式：仅云、点到站点、站点到站点 Open VPN 和多站点 IPsec VPN。 • VPN 网关的可用性：始终可用。 • 云网络的数量：23. • 公共 IP 地址 • Internet 访问 • 使用 Runbook 进行的操作：创建、编辑和执行。

即付即用和保护服务中的高级功能

即付即用和保护服务中的高级功能

功能组	即用即付功能	高级功能
备份	• 文件备份 • 映像备份 • 应用程序备份 • 网络共享备份 • 备份到云存储 • 备份到本地存储 **注意** 云存储使用费适当。	• 单击恢复 • 连续数据保护 • Microsoft SQL Server 集群和 Microsoft Exchange 集群的备份支持 - Always On 可用性组 (AAG) 和数据库可用性组 (DAG) • MariaDB、MySQL、Oracle DB 和 SAP HANA 的备份支持 • 数据保护地图和合规性报告 • 脱离主机数据处理 • Microsoft 365 和 Google Workspace 工作负载的备份频率 • 通过可启动媒体进行的远程操作 • 直接备份至 Microsoft Azure、Amazon S3 和 Wasabi 公共云存储
File Sync & Share	• 存储基于文件的加密内容 • 跨指定设备同步文件 • 与指定用户和系统共享文件夹和文件	• 公证和电子签名 • 文档模板* *备份同步和共享文件
物理数据装运	物理数据装运功能	N/A
公证	• 文件公证 • 文件电子签名 • 文档模板	N/A

注意
在不启用高级保护包扩展的标准保护功能的情况下，就无法启用高级保护包。如果禁用某个功能，则其高级包会自动禁用，并且使用高级包的保护计划也会自动吊销。例如，如果禁用保护功能，则其高级包会自动禁用，并且使用高级包的所有计划也会吊销。

用户不能在没有标准保护的情况下使用高级保护包，而只能针对特定工作负载将标准保护的随附功能与高级包一起使用。在这种情况下，将仅对工作负载使用的高级包收费。

有关计费的信息，请参阅 "Cyber Protect 的计费模式"(第 8 页)。

Advanced Data Loss Prevention

Advanced Data Loss Prevention 模块通过检查经由本地和网络通道传输的数据内容并应用特定于组织的数据流策略规则，从而防止泄露工作站、服务器和虚拟机的敏感信息。

在开始使用 Advanced Data Loss Prevention 模块之前，请确认您已阅读并理解基础指南中所述的 Advanced Data Loss Prevention 管理的基本概念和逻辑。

您可能还想要查看技术规范文档。

启用 Advanced Data Loss Prevention

默认情况下，Advanced Data Loss Prevention 在新租户的配置中处于启用状态。如果该功能在租户创建过程中被禁用，则合作伙伴管理员可以稍后启用它。

启用 Advanced Data Loss Prevention

1. 在 Cyber Protect Cloud 管理中控台中，导航到**客户端**。
2. 选择要编辑的租户。
3. 在**选择服务**部分中，滚动到**保护**，然后在应用的计费模式下选择**Advanced Data Loss Prevention**。
4. 在配置服务下，滚动到**Advanced Data Loss Prevention**，然后配置配额。
   默认情况下，配额设置为无限制。
5. 保存设置。

Advanced Security + XDR

Advanced Security + XDR(Extended Detection and Response) 包提供了完整、本机集成、高效的解决方案，专为 MSP 而构建。

使用 Advanced Security + XDR 来：

- 通过覆盖终端、电子邮件、Microsoft Entra ID 和 Microsoft 365 应用程序 (SharePoint、OneDrive、Teams) 的广泛可见性，扩展对易受攻击面的客户端环境的保护，确保对复杂的威胁形势的防范。
- 本地集成网络安全、数据保护和终端管理。XDR 旨在保护易受攻击的面，从而实现无与伦比的业务连续性。
- 提高效率，轻松启动、管理、扩展和交付安全服务。此外，XDR 还包括基于 AI 的事件分析和一键响应，为了便于调查，所有服务均使用单一代理程序和中控台，以及可自定义的平台，用于将其他工具集成到您的技术堆栈中。

请注意，Advanced Security + XDR 包由Extended Detection and Response (XDR) 、Endpoint Detection and Response (EDR)和"托管的检测及响应 (MDR)"(第 141 页) 并持续保护您的工作负载免受所有恶意软件威胁。

启用 “Advanced Security + XDR”

作为合作伙伴管理员，您可以启用 “Advanced Security + XDR” 保护包，以在客户端保护计划中提供 Extended Detection and Response (XDR) 功能。

注意
还需要在要保护的所有工作负载的保护计划中启用 Endpoint Detection and Response (EDR)。有关详细信息，请参阅启用 EDR。

启用 "Advanced Security + XDR" 包

1. 登录管理门户。

   注意
   如果出现提示，请选择要应用 "Advanced Security + XDR" 保护包的客户端，然后单击**启用**。

2. 在左侧导航窗格中，单击**"客户端"**。
3. 在"Cyber Protect" 下，单击**保护**选项卡。
   已订阅保护服务的现有客户端列表即会显示。
4. 单击要添加 "Advanced Security + XDR" 包的相关客户端。
   在**配置**选项卡中的**保护**部分下，确保选中 **Advanced Security + XDR** 复选框。

将 Advanced Security + XDR 与第三方平台集成

Advanced Security + XDR 支持以下集成：

- Perception Point
- Microsoft Entra ID
- Microsoft 365 服务

要访问您的集成，请在管理门户中转到**集成**。

注意
此功能仅适用于指派有管理员角色的用户。

与 Perception Point 集成

本主题介绍如何将 Perception Point 与 Advanced Security + XDR 集成。

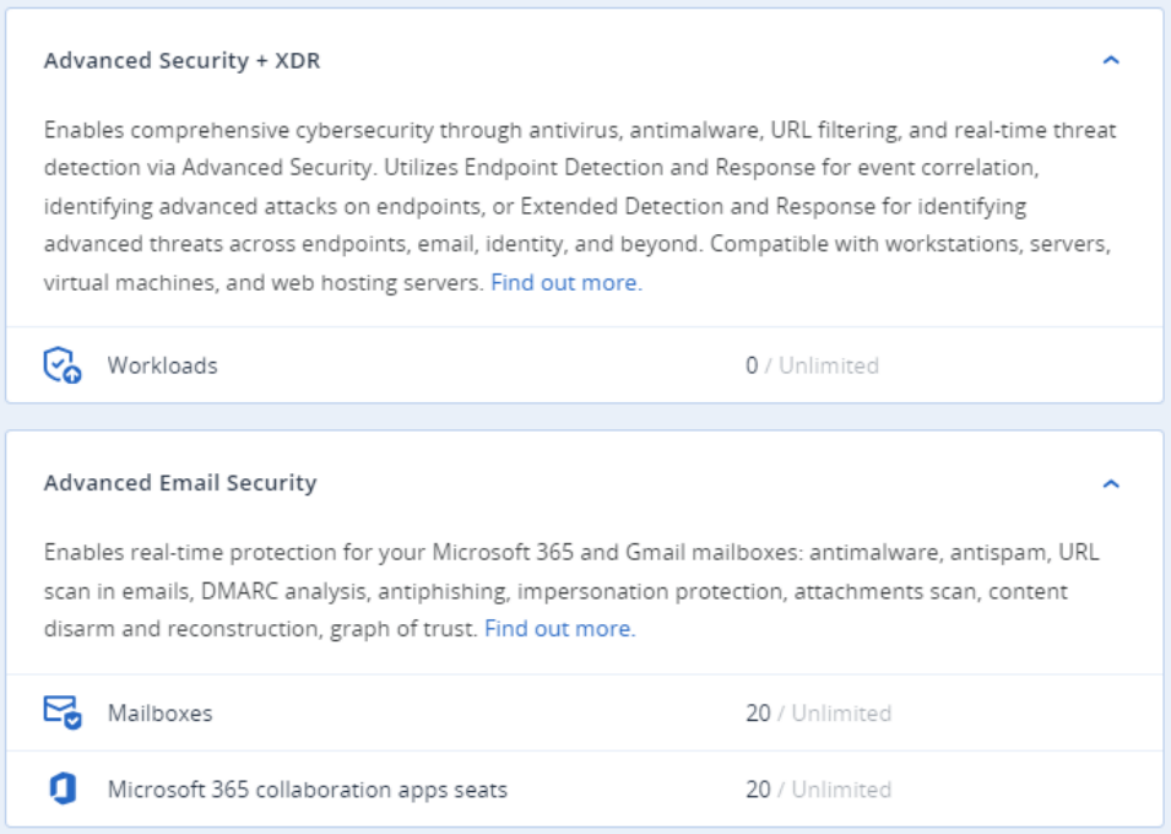
通过此集成，您可以为使用 Microsoft 365 进行电子邮件安全和协作应用的客户提供 Extended Detection and Response (XDR) 解决方案。XDR 集成通过 Perception Point 丰富了现有 Endpoint Detection and Response (EDR) 解决方案的功能。

将 Perception Point 与 Advanced Security + XDR 集成的三个主要步骤如下：

1. 启用所需的高级保护包。
2. 在 Perception Point，配置电子邮件安全和/或协作应用程序通道并提取 API 密钥。
3. 为客户启用 Perception Point XDR 集成。

若要启用所需的高级保护包

1. 在管理门户中，访问您想要为其激活集成的相关客户。
2. 启用 Advanced Security + XDR 和 Advanced Email Security 包。有关详细信息，请参阅 "高级保护包"(第 128 页)。

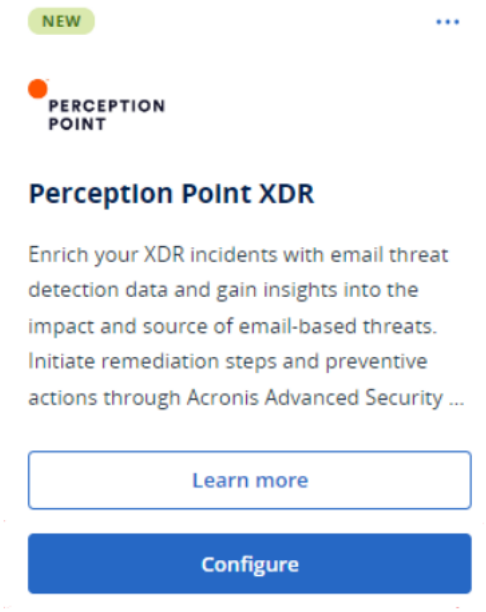


在 Perception Point 中配置电子邮件安全和/或协作应用程序通道并提取 API 密钥

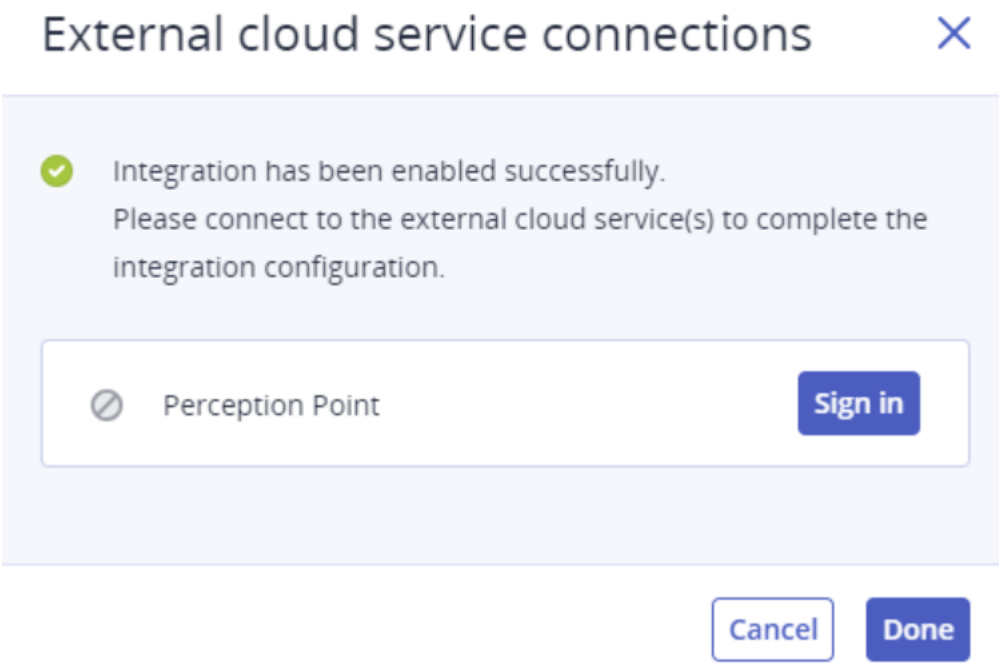
1. 在管理门户中，访问要为其激活集成的相关客户，然后单击**管理服务**以打开 Cyber Protect 中控台。
2. 转到 **电子邮件安全**，然后单击 **转到电子邮件安全中控台** 以打开 Perception Point。
3. 在 Perception Point 中创建相关的电子邮件安全和/或协作应用程序通道。有关详细信息，请参阅 Perception Point 文档。
4. 在左侧导航菜单中，单击**配置文件**。
5. 在**安全性**部分，单击 API 密钥旁边的复制图标。此密钥用于启用 XDR 集成，如下面的过程所述。

为客户启用 Perception Point XDR 集成

1. 在管理门户中，转到**集成**。
2. 搜索 **Perception Point XDR** 集成，然后在显示的平铺中，单击 **配置**。



3. 单击**客户管理**选项卡，选择要为其启用 XDR 集成的客户，然后单击**启用**。
4. 在显示的对话框中，单击**登录**。



5. 输入在上一步骤中复制的 Perception Point API 密钥，然后单击 **完成**。
6. 若要确保集成正在运行，请验证**启用状态**列显示**已启用**，并且**服务连接**列显示为 **1/1**(连接正在运行) 。

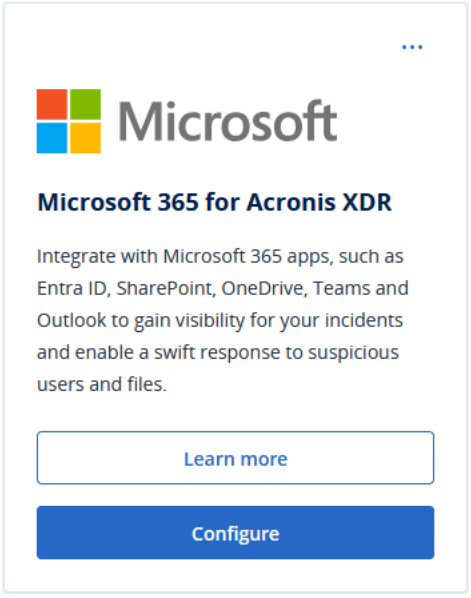
与 Microsoft 365 服务集成

本主题介绍如何将 Microsoft 365 服务与 Advanced Security + XDR 集成。

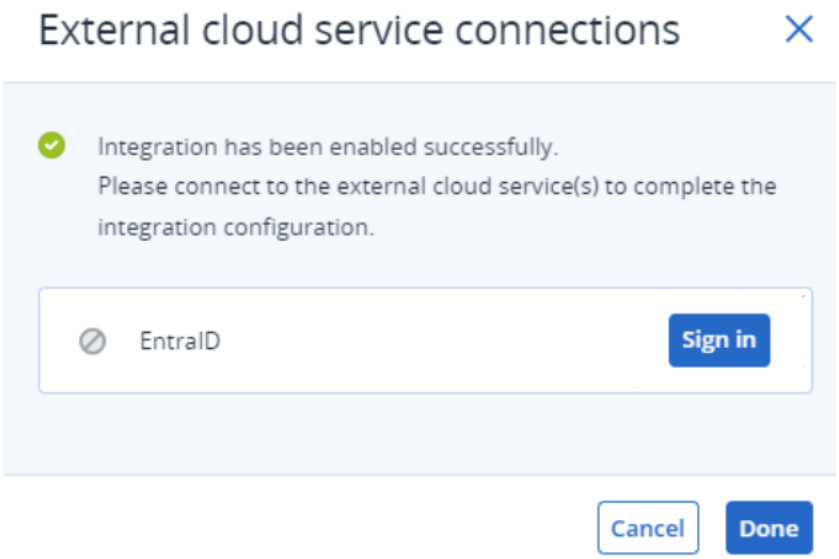
此集成为使用 Microsoft 365 作为其协作应用程序的最终客户的 Endpoint Detection and Response (EDR) 和 Extended Detection and Response (XDR) 事件提供丰富的元数据。此集成还提供有关受事件影响的经过身份验证的用户的详细信息。您还可以执行响应操作，例如阻止或限制用户帐户的访问。

若要与 Microsoft 365 服务集成

1. 转到 Microsoft Azure 门户并以客户租户身份登录。
2. 请按照屏幕上的指示创建新应用程序，并为新应用程序指派必要的角色。有关配置 Microsoft 365 API 访问的更多信息，请参阅此知识库文章。
3. 在管理门户中，验证相关的客户租户是否已启用 Advanced Security + XDR 套餐下的 **Workpack** 选项。
4. 转到**集成**，并搜索 **Microsoft 365 XDR** 集成。
5. 在 **适用于 XDR 的 Microsoft 365** 目录平铺上，单击**配置**，然后单击**启用**。



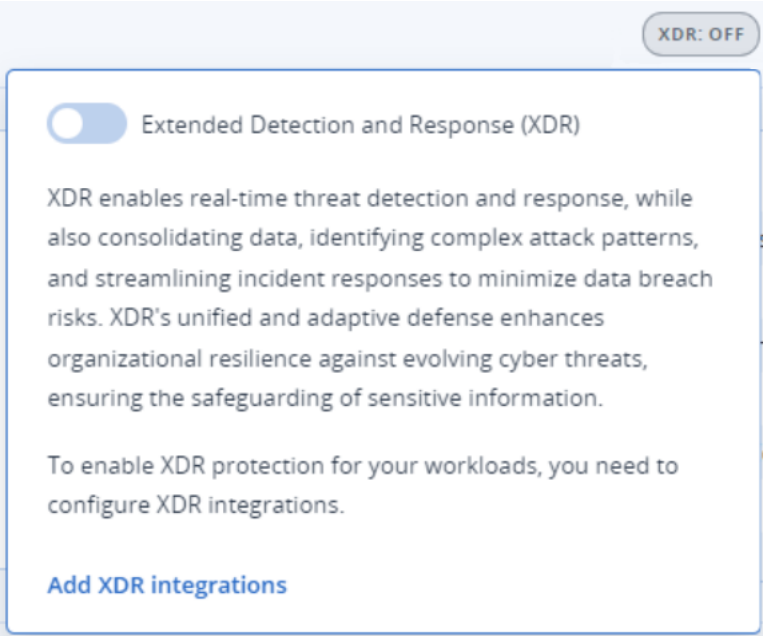
6. 单击**客户管理**选项卡，选择要为其启用集成的客户租户，然后单击**启用**。
7. 定义以下内容：
   - **自定义域**：如果客户在 Microsoft 365 中使用自定义域，请在此处输入。如果未使用自定义域，请将此字段留空。
   - **区域**：从下拉列表中选择 Microsoft 365 租户的相关区域。
8. 单击**启用**。在显示的对话框中，单击**登录**。



9. 输入以下内容：
   - **ID**：您在步骤 2 中创建的应用程序的对象 ID。

     注意
     在 Microsoft 365 中，请确保您通过单击 **应用注册** > **概述** 页中的应用程序名称链接，从 **本地目录中的托管应用程序** 字段复制对象 ID，然后在显示的页面上选择对象 ID。请勿复制显示在主 **应用注册** > **概述** 页上的对象 ID。

   - **Secret**：为应用程序创建的 API 客户端密码。
   - **租户 ID**：Microsoft 365 租户。
10. 单击**登录**，然后单击**完成**。
    为确保连接成功，请验证**服务连接**列显示的是 **1/1**（连接正在运行）。
11. 转到**客户**，选择要为其启用 XDR 的相关客户，然后单击**管理服务**。
    将显示 Cyber Protect 中控台。
12. 转到**保护**，然后单击 **XDR：关闭**。
13. 在显示的弹出窗口中，单击切换开关以启用 XDR。



现在，包括在 Microsoft 365 中注册的工作负载的事件将包含丰富的 XDR 信息和针对该用户的响应操作。

与 Fortinet 集成

本主题介绍如何将 Fortinet 与 Advanced Security + XDR 集成。

此集成通过摄取和相关联来自 Fortinet 安全软件和设备的事件，Endpoint Detection and Response (EDR) 和 Extended Detection and Response (XDR) 事件提供了丰富的元数据。

重要事项
客户必须对相关网络拥有 FortiGate Cloud 服务许可证，以便使集成正常工作。

将 Fortinet 与 Advanced Security + XDR 集成的三个主要步骤如下：

- 启用 “Advanced Security + XDR” 包。
- 配置 Fortinet 与 Acronis 配合使用。
- 在管理门户中启用集成。

若要启用 “Advanced Security + XDR” 包

1. 在管理门户中，访问您想要为其激活集成的相关客户。
2. 请确保已启用 Advanced Security + XDR 包。有关详细信息，请参阅 "高级保护包"(第 128 页)。

若要配置 Fortinet 与 Acronis 配合使用

1. 登录您的 FortiGate 或 FortiGate Cloud 服务帐户。
2. 响应操作以阻止 URL 或 IP 地址：
   - 转到**Security Profiles** > **Web Filter**，并定义名为 **Acronis Web Filter**的筛选器。然后，在 **Static URL Filter** 部分，单击 **URL Filter** 开关以启用它。

- 转到 **Policy & Objects** > **Firewall Policy**，并确保 **Acronis Web Filter**已添加到相关策略(在 **Security Profiles**部分)。

当响应操作被启动时，即使未定义 Web 筛选器和防火墙策略，也会从 Fortinet 接收声誉。添加 Web 筛选器可确保能够阻止 URL 或 IP 地址。

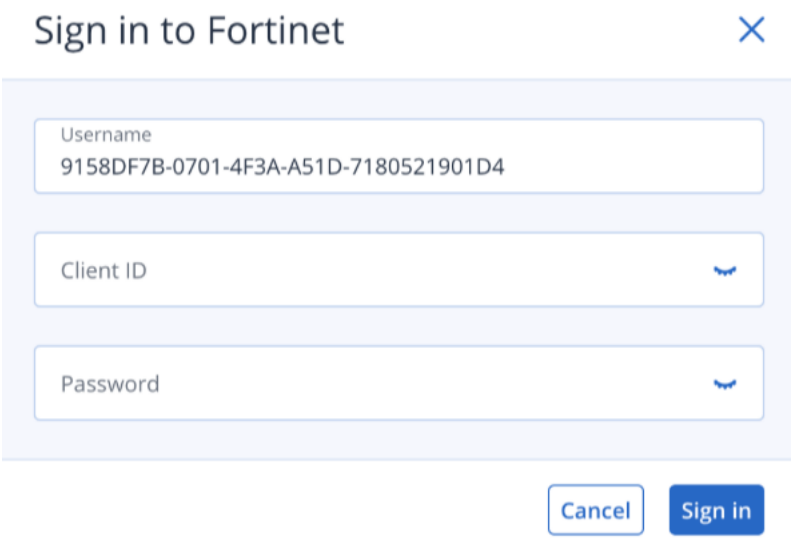
注意
如果未定义或未找到 **Acronis Web Filter**，则 XDR 图中不会显示块响应操作。

3. 若要隔离终端：
   - 转到**Policy & Objects** > **Firewall Policy**，并定义两个用于阻止和接受出站连接(用于 Acronis 域和 IP 地址)的策略。
   - 转到**Policy & Objects** > **Addresses**，在**Address Groups**项卡中，定义以下内容：
     - 自动存储已阻止地址的 **Acronis Isolated Group**。**Acronis Isolated Group** 是**Group**类型，应将其链接到阻止策略。
     - **"Acronis Allowed Hosts"**组是存储允许的地址和域的位置。**"Acronis Allowed Hosts"**是**"Group"**类型，应将其链接到接受传出连接的策略。例如，应将 **"Acronis Isolated Group"**添加到策略的**"Source"**字段，将 **"Acronis Allowed Hosts"**组添加到**"Destination"**字段。

       注意
       Acronis 代理程序正常工作所需的 Acronis 数据中心地址和端口，在此处列出。

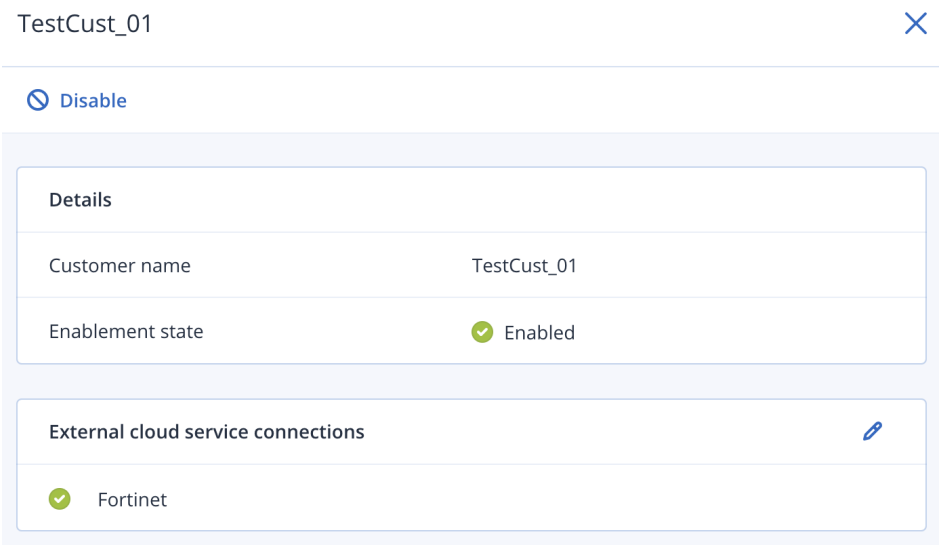
若要为客户启用 Fortinet XDR 集成

1. 在管理门户中，转到**集成**。
2. 搜索 **Fortinet XDR** 集成，然后在显示的平铺中，单击**配置**。
3. 单击**客户管理**选项卡，选择要为其启用 XDR 集成的客户，然后单击**启用**。
4. 在对话框中，输入相关的 Fortinet 用户名、客户端 ID 和密码。



注意
在创建 IAM API 用户并为 FortiGate Cloud 设置管理员权限时生成 Fortinet 凭据。有关详细信息，请参阅 FortiGate Cloud 文档。或者，如果您是 Fortinet 客户并且可以访问其开发网络页面，请参阅 此文档。

5. 单击**登录**。
6. 为确保集成已启动并运行，单击相关客户行，并验证**启用状态**字段是否显示**已启用**。



7. [可选] 若要更新 Fortinet 用户名、客户 ID 和密码，请单击**外部云服务连接**部分中的铅笔图标。

若要禁用 Fortinet XDR 集成

1. 在管理门户中，转到**集成**。
2. 搜索 **Fortinet XDR** 集成，然后在显示的平铺中，单击**配置**。
3. 单击**客户管理**选项卡，选择要为其禁用 XDR 集成的客户，然后单击**禁用**。

托管的检测及响应 (MDR)

MDR 为没有内部安全专业知识或需要额外帮助来调查和响应 Endpoint Detection and Response (EDR) 和 Extended Detection and Response (XDR) 检测到的安全事件的 MSP 提供 24/7 服务。

MDR 功能在 Advanced Security + XDR 包下的管理门户中启用，并且 MDR 服务由外部 MDR 供应商提供。当为特定客户启用 MDR 时，MDR 供应商会从 Acronis 接收属于该客户的保护计划中已启用 EDR 或 XDR 的工作负载的事件数据。然后，MDR 供应商执行不同级别的服务，使用可用的响应操作对事件进行分流。有关更多信息，请参阅 "什么是托管检测和响应 (MDR)？ "(第 142 页)

有关使用 XDR 的更多信息，请参阅 Extended Detection and Response (XDR)。

有关使用 EDR 的更多信息，请参阅 Endpoint Detection and Response (EDR)。

什么是托管检测和响应 (MDR)?

MDR 是第三方供应商提供的一项服务，它结合了来自供应商和 Acronis 的熟练分析师、集成工具、威胁情报和技术来监控和响应潜在的安全威胁和违规行为。

当在管理门户中为客户启用 MDR 时，Acronis 会将事件遥测数据转发给 MDR 供应商，以对这些事件开展调查和响应活动。请注意，只有无法自动缓解的事件才会转发给 MDR 供应商。

MDR 的关键组成部分

MDR 由三个主要部分组成：

- 监控
- 隔离
- 响应和补救

监控

MDR 供应商监控检测到的来自客户终端的安全警报和通知。然后，供应商使用分析、安全编排和响应，将这些警报与常见威胁、威胁情报和第三方威胁情报关联起来并确定优先级。因此，供应商确定警报或通知是违规还是妥协。

MDR 供应商认为可能构成潜在安全威胁的任何安全事件都会升级为面向客户的安全事件，并在 Cyber Protect 中控台中提供。供应商提供有关威胁严重性的背景信息和建议的补救措施(包括已采取的任何措施)。

隔离

MDR 供应商分析师利用预定义的剧本来启动终端隔离响应。MDR 供应商的任何响应操作都会反映在相关安全事件中。隔离终端的决定是通过利用终端的数据以及来自威胁情报和威胁研究的进一步输入来做出的。

响应和补救

响应和补救活动在初始监控和隔离活动完成后进行。当检测到安全事件后，MDR厂商根据安全事件发起响应。响应和补救活动包括：

- 指导如何根据所提供的数据、情报和建议减轻、停止或预防安全事件。
- 分析和调查安全事件，以确定危害的根本原因和程度。
- 执行已批准的工作流程(如 MDR 供应商的响应手册中所定义)以隔离工作负载、隔离威胁或完全补救威胁。
- 引用面向客户的安全事件、威胁情报和建议，为服务提供商提供更详细的安全升级。
- 通过各种渠道升级事件，包括创建安全事件、电子邮件通知和电话，所有这些均通过客户提供的联系方式进行。
- 与客户保持沟通，直到威胁得到不久，并在出现新信息时及时提供更新。
- 如果响应操作超出 MDR 服务范围，MDR 供应商会提供有关重点领域的建议。这可能包括对附加服务的建议，例如事件响应。

启用托管检测和响应 (MDR)

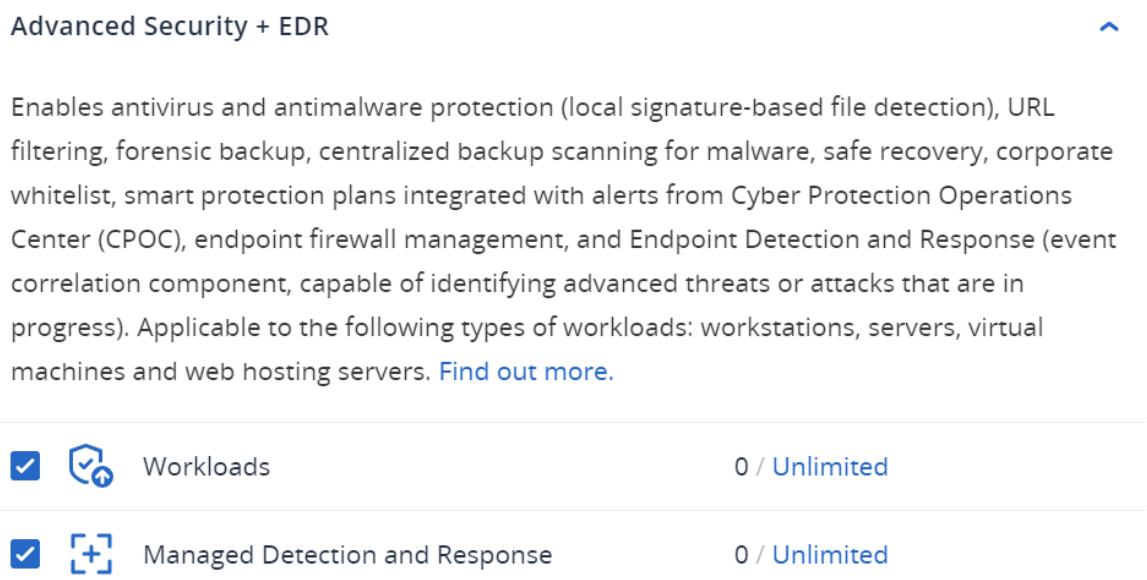
您可以通过执行以下两个步骤为选定的客户启用 MDR:

- 步骤 1:为客户启用 MDR 产品项目。
- 步骤 2:配置与 MDR 供应商应用程序的集成。

注意
自主管理的客户无法启用 MDR。有关配置自主管理客户的更多配置信息,请参阅 "配置自我管理的客户资料"(第 41 页)。

若要为选定的客户启用 MDR

1. 在管理门户中,转到**客户端**。
2. 单击相关客户旁边的省略号图标 (...),然后选择**配置**。
3. 在**"保护"**选项卡中,单击**"编辑"**。
4. 在 **"Advanced Security + EDR"** 部分中,确保选中**"工作负载"**和**"托管检测和响应"**复选框。然后单击**"保存"**以应用任何更改。

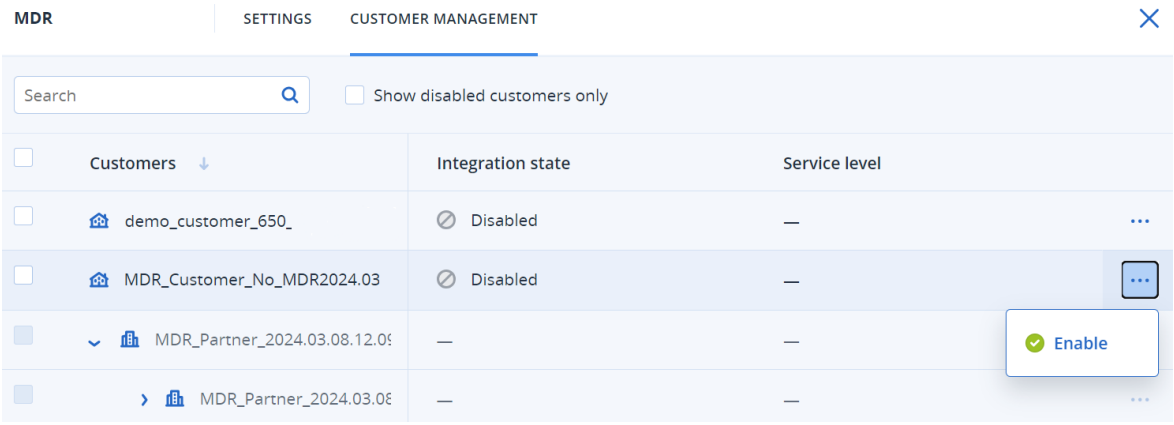


配置与 MDR 供应商的应用程序的集成

1. 在管理门户中,转到**集成**。
2. 使用搜索栏找到 MDR 供应商的应用程序。
3. 在显示的 MDR 目录卡中,单击**"配置"**。
4. 在**"设置"**选项卡中,单击铅笔图标并输入至少一位合作伙伴联系人的详细联系信息。当检测到安全事件时,MDR 供应商将联系此联系人。请注意,您最多可以添加三个联系人的详细信息。完成后,单击**"启用"**。

当检测到安全事件时，供应商会致电每个联系人六次，然后再转至下一个联系人。在接到电话后，或者在没有取得联系的情况下，供应商会向所有联系人发送一封电子邮件，提供升级情况和事件的概述。

5. 在**"客户管理"**选项卡中，单击相关客户最右列中的省略号图标 (...)，然后单击**"启用"**。



若要启用多个客户，请选中相关客户旁边的复选框，然后单击**客户管理**选项卡左上角的**启用**。

6. 从显示对话框的**服务级别**下拉列表中，选择要应用于所选客户的 MDR 服务级别：
   - **标准**：包括对客户端点进行 24/7/365 监控以捕获攻击、AI 驱动的事件分类和优先级、受影响终端的威胁遏制和隔离，以及对事件优先级列表的实时中控台可见性。
   - **高级**：除了**标准**中包含的功能外，此级别还可以实现完整的修复，包括攻击回滚、恢复和消除安全漏洞。
7. 单击**启用**以完成 MDR 集成。

   如果启用了 IP 白名单功能(请参阅"限制对 Web 界面的访问"(第 30 页))，系统会提示您将 MDR 供应商的 IP 添加到允许列表。这确保供应商可以监控相关工作负载。单击**启用**进行确认。

   MDR 现已启用，安全事件将转发给 MDR 供应商以进开展调查和响应活动。有关 MDR 服务的更多信息，请参阅 "什么是托管检测和响应 (MDR)？"(第 142 页)

禁用托管检测和响应 (MDR)

您可以在产品项目级别禁用 MDR。还可以在 MDR 供应商的集成应用程序中为个别客户禁用 MDR。

禁用 MDR 产品项目

1. 在管理门户中，转到**客户端**。
2. 单击相关客户旁边的省略号图标 (...)，然后选择**配置**。
3. 在**"保护"**选项卡中，单击**"编辑"**。
4. 在 **"Advanced Security + EDR"** 部分中，确保未选中**"工作负载"**和**"托管检测和响应"**复选框。然后单击**"保存"**以应用您的更改。

   或者，您可以在**"配置"**选项卡中禁用 **Advanced Security + EDR** 服务，这会自动禁用 MDR。

在 MDR 供应商的集成应用程序中为个别客户禁用 MDR

1. 在管理门户中，转到**集成**。
2. 搜索相关的 MDR 供应商应用程序。
3. 在显示的 MDR 目录卡中，单击**"配置"**。

4. 在**"客户管理"**选项卡中，单击相关客户最右列中的省略号图标 (...)，然后选择**"禁用"**。
   若要禁用多个客户，请选中每个客户左侧的复选框，然后单击**"客户管理"**选项卡左上角的**"禁用"**。

托管检测和响应 (MDR) 中可用的响应操作

MDR 包括许多可在事件级别应用的响应操作。

响应操作由 MDR 安全分析师执行，他们通过访问Cyber Protect中控台或通过运行 API 调用应用相关操作。这些分析师登录Cyber Protect具有**安全分析师**角色的控制台。

所有响应操作都记录在**"活动"**列表中。客户可以查看已执行的响应操作活动的列表以及这些活动的状态(进行中/成功/失败)。在**"发起人"**列中，会显示发起操作的用户，无论是合作伙伴用户、客户用户还是 MDR 安全分析师。

注意
下表中列出的响应操作包括对 Endpoint Detection and Response (EDR) 文档中相关部分的引用。

响应操作	其他信息
更改调查状态	状态可以设置为以下任意一项： • **调查中** • **关闭** • **误报** 有关更改调查状态的更多信息，请参阅如何调查网络杀伤链中的事件。
网络隔离	MDR 安全分析师可以： • 隔离工作负载 • 解除工作负载的隔离 • 检查隔离状态 有关隔离工作负载的更多信息，请参阅管理工作负载的网络隔离。
添加评论	MDR 安全分析师可以通过单击事件的网络杀伤链中的**"发布评论"**来添加对该事件的评论。这些评论将显示在特定事件的**"活动"**选项卡中。有关详细信息，请参阅了解为缓解事件影响而采取的操作。
停止进程/进程树	此操作可以应用于整个事件。即使进程已因事件而停止，也可以触发响应操作。 处理响应操作后发送异步响应。响应可以是以下之一： • 成功：所有进程已成功停止。

响应操作	其他信息
	• 成功但有警告:某些进程已成功停止或没有进程可停止(或在 MDR 之外停止)。 • 错误:没有进程停止。 有关停止进程或进程树的更多信息,请参阅为可疑进程定义响应操作。
隔离	此操作可以应用于整个事件。即使文件或进程已被隔离,也可以触发响应操作。 处理响应操作后发送异步响应。响应可以是以下之一: • 成功:所有文件和进程均已成功隔离。 • 成功但有警告:某些文件和进程已成功隔离,或者没有要隔离的文件或进程(或在 MDR 之外隔离)。 • 错误:没有隔离任何文件或进程。 有关隔离进程的详细信息,请参阅定义可疑进程的响应操作。有关隔离文件的详细信息,请参阅定义可疑文件的响应操作。
删除文件	此操作可以应用于整个事件。即使文件已被删除,也可以触发响应操作。 处理响应操作后发送异步响应。响应可以是以下之一: • 成功:所有文件已成功删除。 • 成功但有警告:某些文件已成功删除或没有可删除的文件(或在 MDR 之外删除)。 • 错误:没有删除任何文件。 有关删除文件的详细信息,请参阅定义可疑文件的响应操作。
重新启动工作负载	启用重新启动工作负载或立即重新启动之前的时间间隔设置。 有关重新启动工作负载的更多信息,请参阅重新启动工作负载。
将 URL、文件或进程添加到白名单/阻止列表	将 URL、文件或进程添加到默认计划(当前指派给工作负载的计划)的白名单/阻止列表中。 处理响应操作后发送异步响应。响应可以是以下之一: • 成功:所有 URL、文件和进程均已成功添

响应操作	其他信息
	加。 • 成功但有警告：有些 URL、文件和进程已成功添加，有些则未成功（例如，它们可能已包含在白名单中）。 • 错误：操作失败。 有关将 URL、文件或进程添加到白名单和阻止列表的详细信息，请参阅将进程、文件或网络添加到保护计划阻止列表或白名单。

Advanced Disaster Recovery

可以启用 Advanced Disaster Recovery 包，并使用完整的Disaster Recovery 功能保护工作负载。

提供以下 Advanced Disaster Recovery 功能：

- 生产故障转移
- 在隔离的网络环境中测试故障转移。
- 可用于故障转移的恢复点数量：创建恢复服务器后可用的所有恢复点。
- 主服务器
- 恢复/主服务器配置：无限制
- 可用连接模式：仅云、点到站点、站点到站点 Open VPN 和多站点 IPsec VPN。
- VPN 网关的可用性：始终可用。
- 云网络的数量：23.
- 公共 IP 地址
- Internet 访问
- 使用 Runbook 进行的操作：创建、编辑和执行。

Advanced Email Security

Advanced Email Security 包会为您的 Microsoft 365、Google Workspace 或 Open-Xchange 邮箱提供实时保护：

- 防恶意软件和防垃圾邮件
- 电子邮件中 URL 扫描
- DMARC 分析
- 防网络钓鱼
- 假冒保护
- 附件扫描
- 内容拆解与重建
- 信任图
- 邮箱所有者可自助释放被隔离的垃圾邮件

还可以启用 Microsoft 365 协作应用程序席位，从而保护 Microsoft 365 云协作应用程序免受内容传播安全威胁。这些应用程序包括 OneDrive、SharePoint 和 Teams。

Advanced Email Security 可以按工作负载或按 GB 启用，这将影响您的许可模式。

在Advanced Email Security 产品彩页中，了解有关 Advanced Email Security 的详细信息。

有关配置说明，请参阅《Advanced Email Security》文档。

Advanced Backup

可以启用 Advanced Backup 包，并使用 Advanced Backup 和恢复功能保护工作负载。

提供以下功能：

- 单击恢复
- 连续数据保护
- Microsoft SQL Server 集群和 Microsoft Exchange 集群的备份支持 - Always On 可用性组 (AAG) 和数据库可用性组 (DAG)
- MariaDB、MySQL、Oracle DB 和 SAP HANA 的备份支持
- 数据保护地图和合规性报告
- 脱离主机数据处理
- Microsoft 365 和 Google Workspace 工作负载的备份频率
- 通过可启动媒体进行的远程操作
- 直接备份至 Microsoft Azure、Amazon S3 和 Wasabi 公共云存储

Advanced Management (RMM)

Advanced Management (RMM) 可以为终端和 Microsoft 365 席位提供高级监视和管理。

- 对于终端，它提供以下内容：
  - **软件盘点** - 查看由客户端使用的完整软件列表，在准备、计划或跟踪更新时节省时间和工作量。
  - **通过使用 DeployPilot 进行软件部署** - 在受控工作负载上远程部署软件。使用软件部署计划来自动执行软件部署过程，并确保在工作负载之间的软件分发是一致的。
  - **自动修补程序管理** - 在漏洞被利用之前修复漏洞。
  - **故障安全修补** - 通过在修补之前执行自动系统备份，可以快速且轻松地从错误的修补程序恢复工作负载。
  - **基于机器学习的监控和智能警报** - 通过可预测的监控和警报，减轻操作风险并优化监控工作。
  - **开箱即用的网络安全脚本** - 自动化和简化日常任务。
  - **驱动器运行状况监控** - 使用可预测的监控和警报并主动减少由驱动器故障引起的停机。
  - **远程桌面和远程协助** - 访问远程工作负载并快速解决技术问题。即使使用有限的带宽，也能节省时间并提供具有出色表现的可靠支持。该功能包括更好的平台覆盖（Windows、macOS 和

Linux)，并扩展了用于会话录制、远程操作、文件传输、监控、报告和以多视图观察工作负载的能力。

- **第三方 Windows 应用程序的漏洞评估** - 通过检测和管理 314 个关键应用程序的漏洞，以 内部维护的数据库支持的方式，增强 Windows 第三方应用程序的安全性。
  第三方 Windows 应用程序的漏洞评估已移至 “Advanced Management (RMM)” 包，可能会产生额外成本。如果要停止保护这些应用程序并禁用该功能，或要在多个现有计划中启用该功能，请参阅 "批量禁用和启用 Windows 第三方应用程序的漏洞评估"(第 149 页)。
- **地理位置磁道** - 查看托管工作负载的实时物理位置。
- **Helpdesk 聊天** - 使用托管的 Windows 和 macOS 工作负载的技术人员与远程用户之间的实时通信工具，以提供更快的问题解决和更好的客户服务。

- 对于 Microsoft 365 许可证，它提供了 Microsoft 365 安全态势的持续审核，包括最佳实践基线和基线偏差的整改。启用 Microsoft 365 管理服务时，有两种产品模式可用：
  - **免费**：可使用最佳实践基线和用户上线审核 Microsoft 365 安全状况。Free 模式可在标准保护功能集中使用。
  - **高级**：包括所有 Free 模式功能，并且还可启用安全态势基线偏差的自动修复和用户移除。

批量禁用和启用 Windows 第三方应用程序的漏洞评估

禁用或启用多个客户租户中具有多个托管工作负载的 Windows 第三方应用程序的漏洞评估可能是一项耗时且繁琐的任务。因此，我们开发了用于批量禁用和启用该功能的工具。有关详细信息，请参阅这些知识库文章：

- 如果您在保护计划中为第三方 Windows 应用程序配置了漏洞评估，但客户在其租户上未启用 Advanced Management (RMM) 包，则使用此实用工具在所有受影响的计划中禁用第三方 Windows 应用程序的漏洞评估，同时保留所有其他漏洞评估组件：https://care.acronis.com/s/article/Acronis-Cyber-Protect-Disabling-Vulnerability-Assessment-of-Third-Party-Windows-Applications-when-Advanced-Management-pack-is-not-enabled-for-the-tenant。
- 如果您需要为第三方 Windows 应用程序启用漏洞评估，以确保在已激活一般漏洞评估策略且已为相应租户启用 Advanced Management (RMM) 包的所有保护计划中保护这些应用程序，请使用此实用工具批量启用子策略：https://care.acronis.com/s/article/Acronis-Cyber-Protect-Enabling-Vulnerability-Assessment-for-Windows-Third-Party-Applications-when-Vulnerability-Assessment-module-is-enabled-in-Protection-plans。

高级安全意识培训

合作伙伴可以为其客户租户启用高级安全意识培训服务，以便其组织中的用户可以从 保护 中控台访问安全意识培训材料。

从 Cyber Protection 云中控台直接访问安全意识培训可促进组织中更多用户的采用和覆盖，有助于客户满足合规性 (PCI、HIPPA、FedRamd、Soc 2)、供应商风险管理、网络安全保险等要求。此外，通过降低人为错误的风险，培训有助于客户提高网络安全。

服务由第三方学习管理系统 Wizer 提供，该系统支持以下功能：

- 多租户：在 Wizer 管理面板中，合作伙伴管理员可以查看所有已注册安全意识培训的客户和直接用户。该平台不支持多级视图，即合作伙伴无法查看子合作伙伴及其子租户。客户管理员只能查看其组织中的用户。
- 租户和管理员用户的自动配置：当首次在 Cyber Protect Cloud 中控台启用服务时，集成会自动为启用集成的管理员在 Wizer 中创建新的租户。然后，管理员将访问 Wizer 管理员面板，手动添加用户或配置 SSO。请参阅 如何添加用户。
- 引人入胜的内容让培训变得有趣
- 易于使用
- 每月订购

请访问 https://www.wizer-training.com/ 了解有关 Wizer 的更多信息。

启用高级安全意识培训服务

安全意识培训作为 Cyber Protect Cloud 中控台中的集成由第三方供应商 Wizer 提供。合作伙伴必须在其自己的租户中启用集成，然后才能为其客户启用服务。

启用服务包括以下高级别步骤。

1. 在“云”管理中控台中，合作伙伴管理员为客户启用“安全意识培训”服务（每个客户一次）。
2. 在 Cyber Protect Cloud 中控台中，管理员在其组织中启用与 Wizer 的集成（每个组织一次）。
3. 管理员用户导航至 Wizer 管理员控制台以将用户添加至培训平台。

注意
服务对于单位管理员和文件夹管理员不可用。

若要为客户租户启用高级安全意识培训服务

所需角色：合作伙伴管理员

1. 在“云管理中控台”中，单击**客户**，然后找到要启用服务的客户。
2. 在上下文菜单中，单击 **配置**。
3. 在服务列表中，**按工作负载**下，选中**高级安全意识培训**复选框。

启用与 Wizer 的组织集成

所需角色：合作伙伴管理员、客户管理员、保护管理员或网络安全管理员。

注意
此初始配置仅会执行一次。

1. 登录到 Cyber Protect Cloud 中控台。
2. 在导航菜单中，单击 **安全意识培训** > **安全意识仪表板**。
3. 单击**启用集成**。
4. 单击**“启用”**以确认。

启用集成后，Wizer 平台将为组织配置一个新的租户。如果您已在 Wizer 中拥有帐户，并且希望使用该帐户而不是新的租户，请联系您的服务提供商。

您可以访问 Wizer 管理面板并手动添加用户，或通过导入 CSV 文件或配置 Active Directory、Octa、Google 或其他身份验证提供程序的 SSO 来添加用户。请参阅 如何添加用户。

集成

本章提供了查找和激活集成所需的信息。

集成提供第三方网络安全保护、终端管理、客户管理、监控、分析等功能，正好与标准 Cyber Protect 中控台产品并列，并通过第三方软件平台提供我们的解决方案。目前有 200 多个集成可自动化日常工作并提高合作伙伴及其客户的工作效率。

集成列在集成目录中。

注意
一些集成需要 API 客户端以访问应用程序编程接口 (API)。

集成目录

集成目录会列出可用的集成：

- 应用程序目录。
  此目录可供公众使用。无法从此目录激活集成。
  如果您的某位客户看到他们想要使用的某个集成，他们应联系您，以便您可以为他们激活该集成。
- 数据中心 (DC) 数据目录。
  这些数据目录是数据中心特定的。可以从这些数据目录激活集成。
  合作伙伴级别的管理门户管理员可以：
  - 查看在数据中心部署的所有集成。
  - 激活数据中心上部署的所有集成，无论是为自己还是为其客户。

  客户级别管理门户管理员可以：
  - 只能查看集成，这些集成是由集成开发人员明确设置为对客户可见的。
  - 只激活那些集成开发人员明确允许客户激活的集成。

  注意
  只有合作伙伴级别的“管理门户”管理员在合作伙伴级别激活了集成后，客户级别的“管理门户”管理员才能激活集成。

目录条目

目录条目由两部分组成：

- 目录卡提供了集成的概述。
- 目录详细信息页面提供更多信息，如完整功能描述、屏幕截图、视频、功能列表、联系人详细信息、集成资源链接等。

打开数据中心集成目录

在数据中心 (DC) 集成目录中，将鼠标悬停在目录卡上以读取简短的产品描述、**配置**按钮和**了解更多**链接：

- **了解详细信息**链接

  每个集成目录条目均具有一个包含集成详细信息的页面，例如，完整的功能描述、屏幕截图、视频、功能列表、联系方式、集成资源链接等。

  单击此链接以打开集成详细信息页面。
- **配置**按钮

  单击此按钮以激活集成。

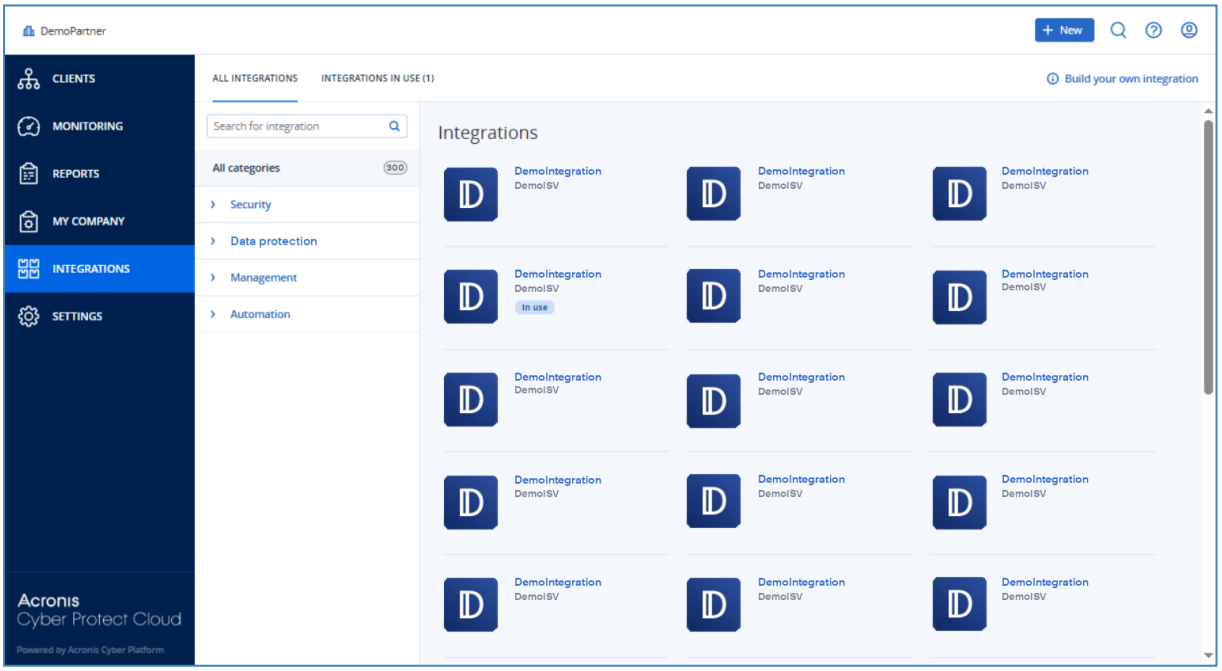
注意

代表非活动集成的目录卡会显示为灰色，并且已禁用。

若要打开您的 DC 集成目录

1. 打开管理门户。
2. 从主菜单中选择 **集成**。

   默认会打开**所有集成**选项卡。这将显示目前在您的 DC 上可用的集成目录卡。
3. [可选] 选择类别并在搜索字段中输入文本，以筛选目录卡。



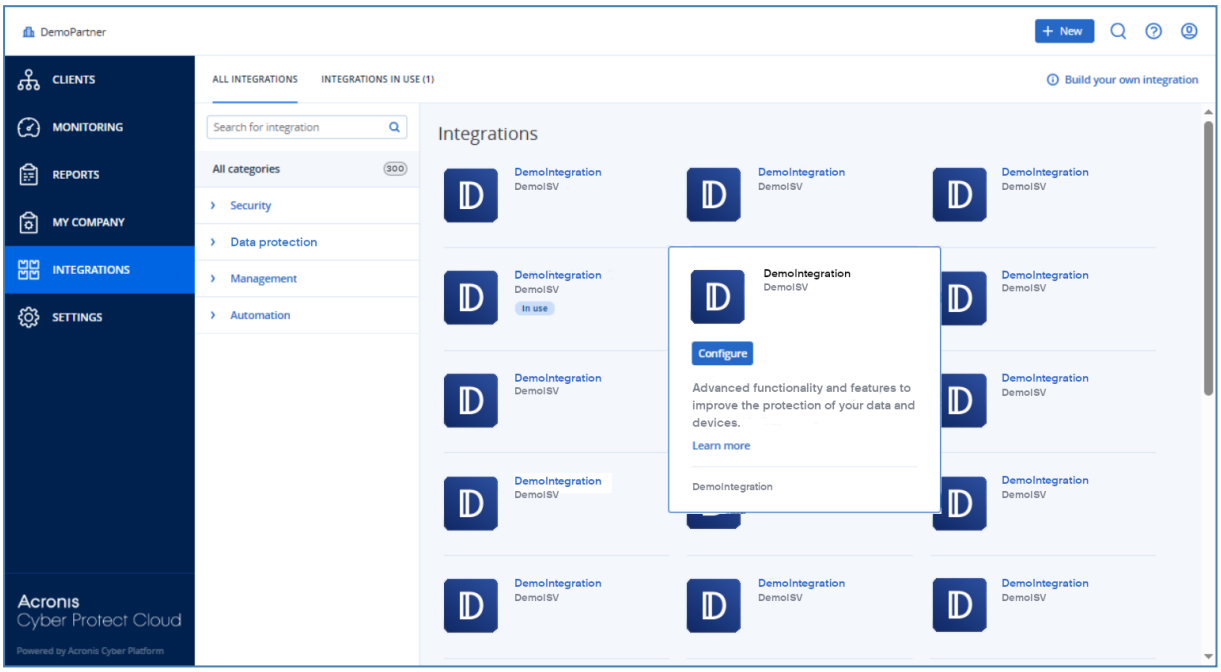
打开集成详细信息页面

打开集成详细信息页面

1. 在数据中心中打开集成目录。
2. 找到集成的目录卡。

3. 将鼠标悬停在该目录卡上。
4. 单击**了解详细信息**。

集成详细信息页面打开。

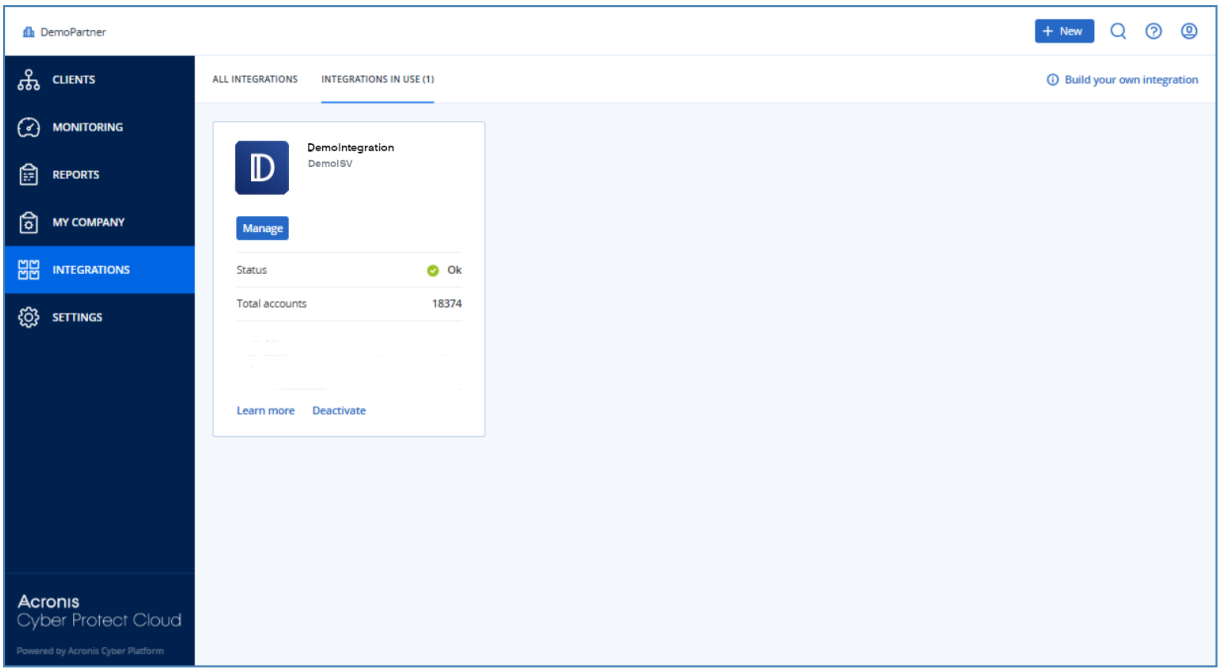


查看已激活的集成

集成目录的**正在使用的集成**选项卡显示您已激活的每个集成的卡片。

查看已激活的集成

1. 在数据中心中打开集成目录。
2. 选择 **正在使用的集成** 选项卡。



正在打开应用程序目录

应用程序目录列出所有 Cyber Protect Cloud 集成。

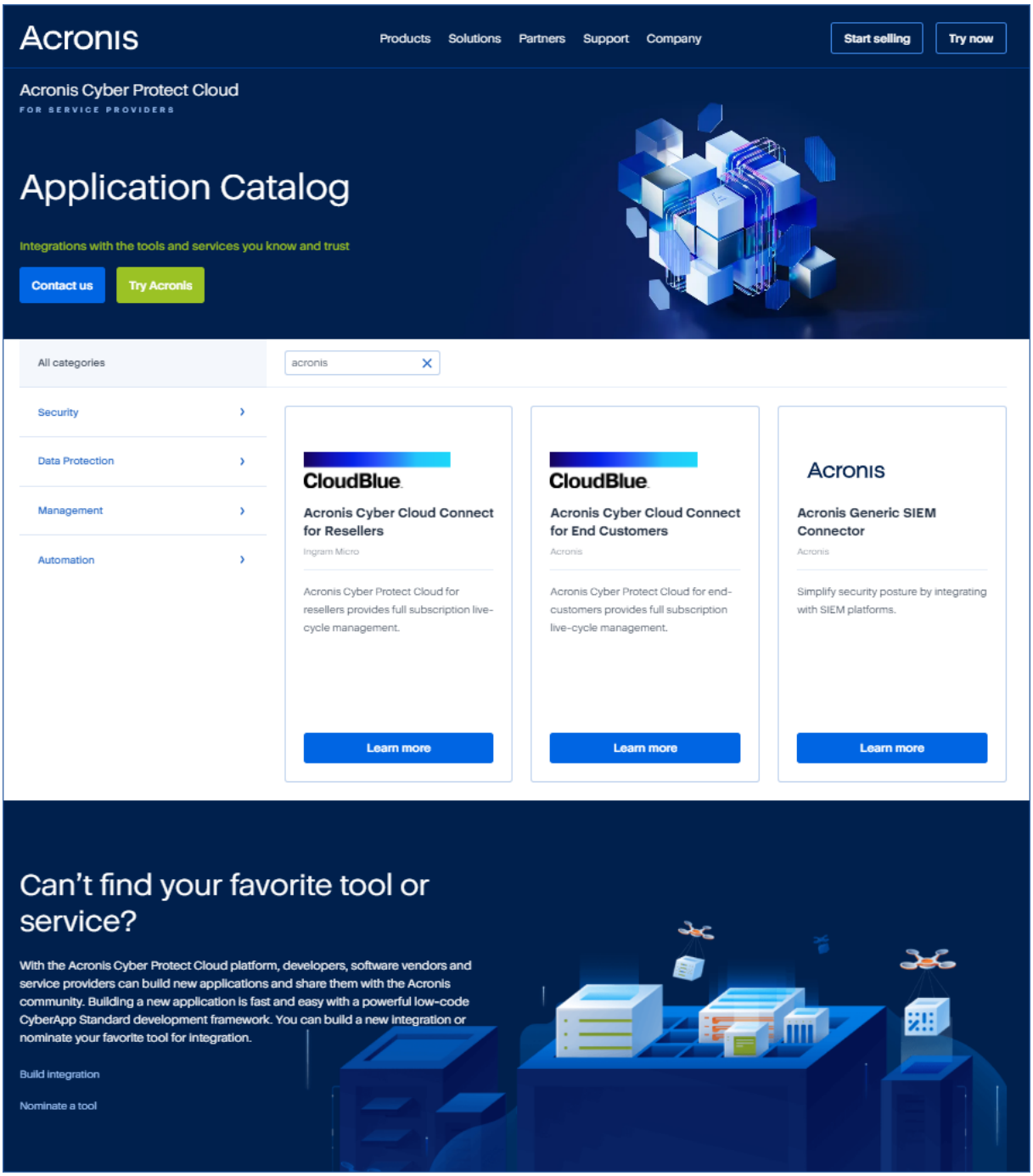
注意

应用程序目录仅供参考:此目录不提供集成启用。

您可以从管理门户上的数据中心集成目录激活集成。

打开应用程序目录

1. 请访问 solutions.acronis.com。
   初始化视图是所有目录卡的网格。
2. [可选]选择类别并在搜索字段中输入文本,以筛选目录卡。



打开集成详细信息页面

每个目录条目还有一个包含HA详细信息的页面，如完整功能描述、屏幕截图、视频、功能列表、联系方式、HA资源链接等。

打开集成详细信息页面

1. 请访问 solutions.acronis.com。
2. 找到您感兴趣的集成的目录卡。
3. 单击目录卡上的**了解详细信息**。

Some features might not be available in your data center yet.

Acronis

Products Solutions Partners Support Company

Start selling Try now

Acronis Cyber Protect Cloud

FOR SERVICE PROVIDERS

Application Catalog

Integrations with the tools and services you know and trust

Contact us Try Acronis

← Back to integrations

Have a question or need help?

Acronis

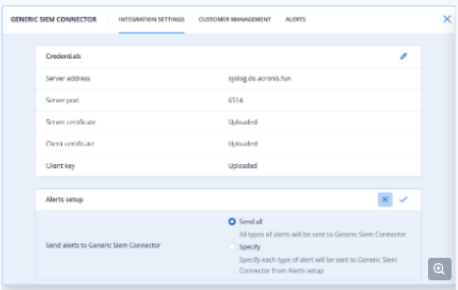
Integration: Acronis Generic SIEM Connector
Category: SIEM
Company: Acronis

Website

Acronis Generic SIEM Connector

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

Integration Overview



Simplify security posture by integrating with SIEM platforms.

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

Features

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

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

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

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

Acronis

Acronis Generic SIEM Connector

Need help or support with an integration?

Contact Support

Can't find your favorite tool or service?

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

Build integration

Nominate a tool

Engage with Acronis

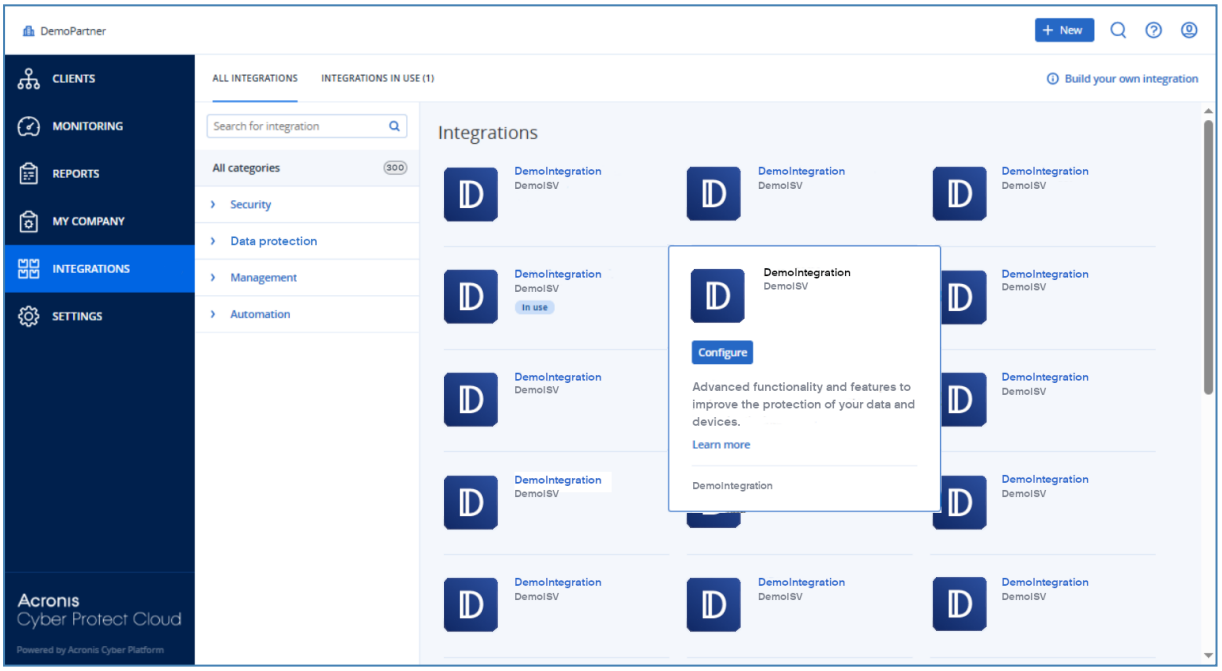
Acronis © 2003–2024 Acronis International GmbH. Legal information | Privacy policy

激活集成

若要激活集成

1. 在数据中心中打开集成目录。
2. 找到要激活的集成的目录卡。

   若要筛选集成：
   - [可选] 选择一种类别。
   - [可选] 在搜索字段中键入字符串。
3. 将鼠标悬停在该目录卡上。
4. 单击**配置**。
5. 按照屏幕上的说明操作。



配置活动集成

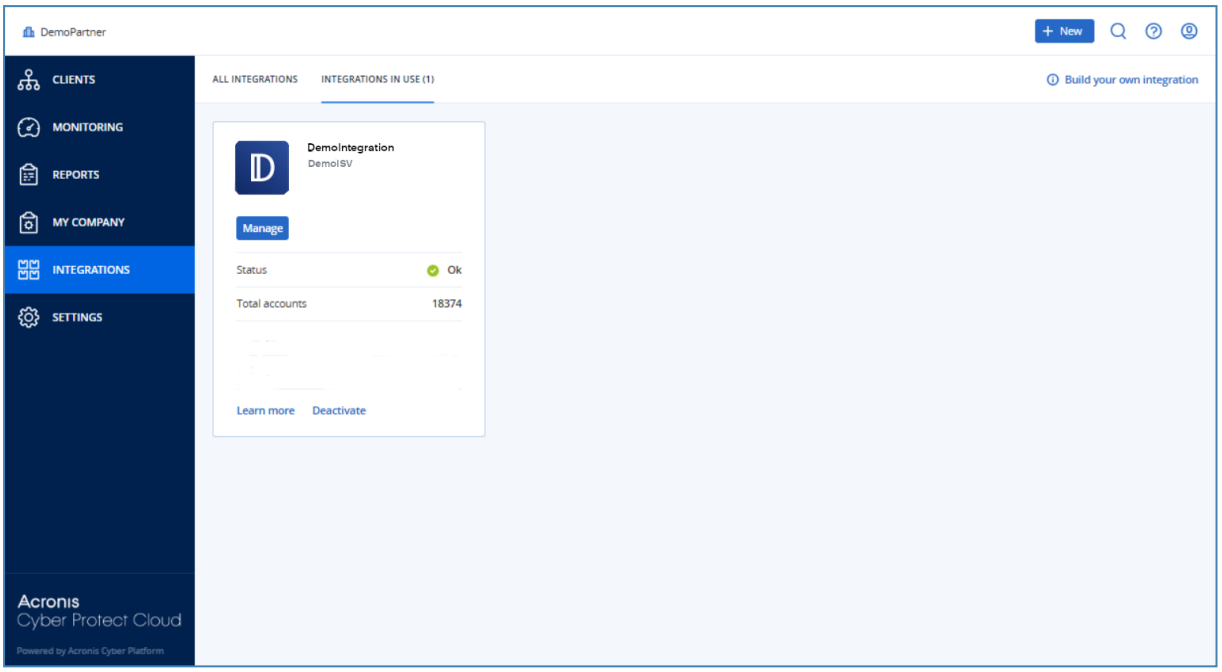
若要配置主动集成

1. 在数据中心中打开集成目录。
2. 选择 **正在使用的集成** 选项卡。
3. 找到要配置的集成的目录位置卡。
4. 单击**管理**。

   打开集成配置屏幕。
5. 请按照屏幕上的说明操作或查阅集成文档。

注意

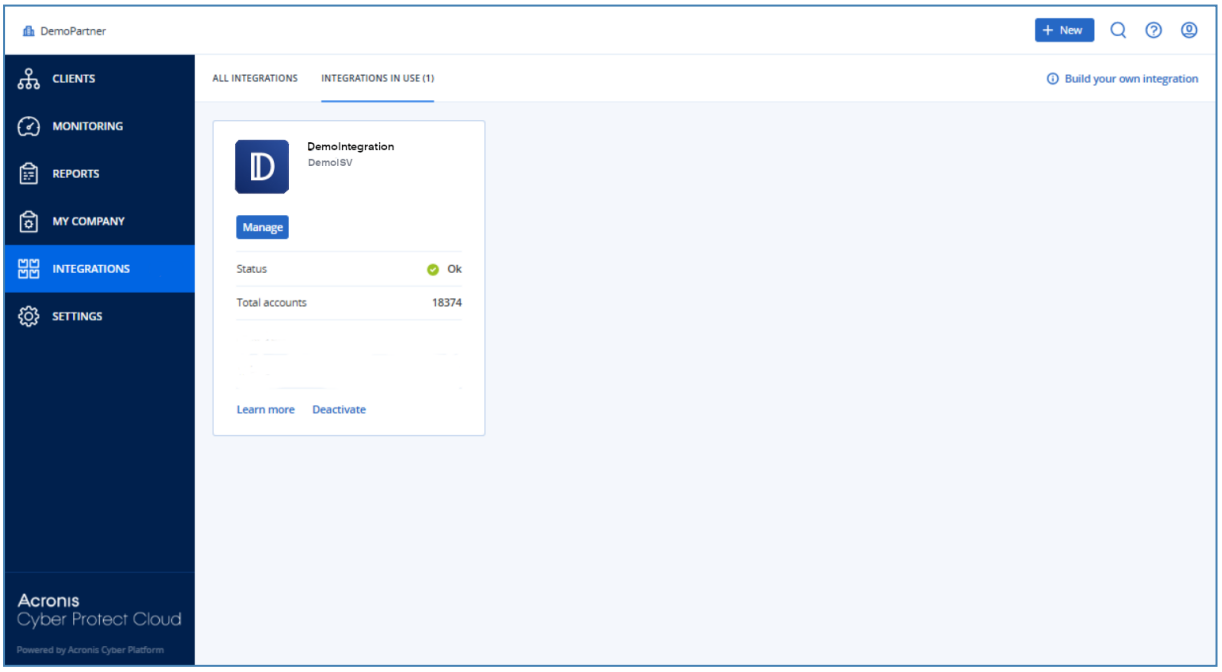
文档通常可在目录详细信息页面中找到。有关详细信息，请参阅 打开集成详细信息页面。



停用活动集成

若要停用集成

1. 在数据中心中打开集成目录。
2. 选择 **正在使用的集成** 选项卡。
3. 找到要禁用的集成的目录位置卡。
4. 单击 **停用**。
5. 单击**删除**。



API 客户端

第三方系统集成可以通过使用的应用程序编程接口 (API)。可以通过 API 客户端(即平台的 OAuth 2.0 授权框架的组成部分)访问 API。

API 客户端是一个特殊的平台帐户,它代表必须进行身份验证和授权才能访问平台数据和服务数据的第三方系统。API 客户端访问受限于创建客户端的管理门户管理员所在的租户和任何子租户。

注意
API 客户端将继承管理员帐户的服务角色,并且以后无法更改这些角色。更改管理员帐户的角色或禁用它并不会影响客户端。

API 客户端凭据

API 客户端凭据由唯一标识符 (ID) 和秘密值组成。这些凭据不会过期,也无法用于登录管理门户或任何其他服务中控台。

注意
无法为客户端启用双重身份验证。

API 客户端流

1. 管理门户管理员创建 API 客户端。
2. 管理员在第三方系统中启用 OAuth 2.0 客户端凭据流。
3. 根据此流,在通过 API 访问租户及其服务之前,系统必须先使用授权 API 发送 API 客户端凭据到平台。
4. 平台生成并发送回安全标记,该标记是指派给此特定客户端的唯一加密字符串。
5. 第三方系统必须将此标记添加到所有 API 请求。

注意
安全标记消除了需要通过 API 请求传递客户端凭据。
为了提高安全性,安全令牌将在两小时后过期。
此后,所有使用过期令牌的 API 请求将失败,系统必须从平台请求新的令牌。

创建 API 客户端

若要创建 API 客户端

1. 登录到管理门户。
2. 依次单击**设置** > **API 客户端** > **创建 API 客户端**。
3. 输入 API 客户端的名称。
4. 单击**下一步**。
   默认情况下,将创建状态为**活动**的 API 客户端。

5. 复制并保存 API 客户端的 ID 和密码值以及数据中心 URL。在第三方系统中启用 OAuth 2.0 客户端凭据流时，将需要使用它们。

   重要事项
   出于安全原因，密码值仅显示一次。如果丢失该值，将无法取回。可进行重置。

6. 单击**完成**。

重置 API 客户端机密值

如果丢失 API 客户端机密值，则可以生成新值。客户端 ID 和数据中心 URL 不会更改。

重要事项
如果重置密钥值，则指派给客户端的所有安全性令牌将立即过期，使用这些令牌的 API 请求将失败。

重置 API 客户端机密值

1. 登录到管理门户。
2. 依次单击**设置** > **API 客户端**。
3. 在列表中查找所需的客户端。
4. 单击 ，然后单击**重置密码**。
5. 单击**继续**以确认您的决定。
6. 复制并保存新的 API 客户端机密值。

   注意
   出于安全原因，密码值仅显示一次。如果丢失该值，将无法取回。可以通过重复这些步骤来进行重置。

7. 单击**完成**。

禁用 API 客户端

您可以禁用 API 客户端。如果这样做，具有指派给客户端的安全性令牌的 API 请求将失败，但是这些令牌不会立即过期。

注意
禁用客户端并不会影响标记的过期时间。

您可以随时重新启用 API 客户端。

若要禁用 API 客户端

1. 登录到管理门户。
2. 依次单击**设置** > **API 客户端**。
3. 在列表中查找所需的客户端。

4. 单击 ，然后单击**禁用**。
5. 确认您的决定。

启用已禁用的 API 客户端

如果启用了先前已禁用的 API 客户端，则**如果这些令牌尚未过期**，指派给客户端的安全性令牌的 API 请求将成功。

若要启用已禁用的 API 客户端

1. 登录到管理门户。
2. 依次单击**设置** > **API 客户端**。
3. 在列表中查找所需的客户端。
4. 单击 ，然后单击**启用**。

   API 客户端的状态将更改为**活动**。

删除 API 客户端

如果删除 API 客户端，则指派给此客户端的所有安全性令牌将立即过期，使用这些令牌的 API 请求将失败。

重要事项
无法恢复已删除的客户端。

若要删除 API 客户端

1. 登录到管理门户。
2. 依次单击**设置** > **API 客户端**。
3. 在列表中查找所需的客户端。
4. 单击 ，然后单击**删除**。
5. 确认您的决定。

创建集成

如果您有数据或服务要与 Cyber Protect Cloud 集成，则可以使用供应商门户创建本机 CyberApp，或使用 API 调用。

CyberApp

供应商门户是一个在线平台，允许第三方软件供应商根据我们的CyberApp标准最佳实践，将产品和服务原生集成到 Cyber Protect Cloud 中。供应商门户集成称为 CyberApp。

注意
有关 CyberApp 和“供应商门户”更多信息，请参阅 《集成指南》。

API 集成

存一整套用于用于集成的 API。

注意

有关 API 的更多信息，请参阅 《集成指南》的平台 API 章节。

将 Cyber Protect Cloud 与 VMware Cloud Director 集成

服务提供商可以将 VMware Cloud Director(旧称 VMware vCloud Director) 与 Cyber Protect Cloud 集成，并为其客户提供开箱即用的虚拟机备份解决方案。

该集成包括以下步骤：

1. 为 VMware Cloud Director 环境配置 RabbitMQ 消息代理。

   RabbitMQ 提供单点登录 (SSO) 功能，以便可以使用 VMware Cloud Director 凭据来登录到 Cyber Protect 中控台。

   在 Cyber Protect Cloud 版本 23.05(已于 2023 年 5 月发布) 及更早版本中，RabbitMQ 还用于将 VMware Cloud Director 环境中的更改同步到 Cyber Protect Cloud。
2. 部署管理代理程序。

   在部署管理代理程序期间，还将安装适用于 VMware Cloud Director 的插件。该插件会将 Cyber Protection 添加到 VMware Cloud Director 用户界面。

   管理代理程序会将 VMware Cloud Director 组织映射到 Cyber Protect Cloud 中的客户租户，并将组织管理员映射到客户租户管理员。有关组织的详细信息，请参阅 VMware 知识库中的在 VMware Cloud Director 中创建组织。

   客户租户是在为其配置了 VMware Cloud Director 集成的合作伙伴租户中创建的。这些新客户租户处于**已锁定**模式下，并且无法由 Cyber Protect Cloud 内的合作伙伴管理员进行管理。

   注意

   仅在 VMware Cloud Director 中具有唯一电子邮件地址的组织管理员才会映射到 Cyber Protect Cloud。
3. 部署一个或多个备份代理程序。

   备份代理程序会为 VMware Cloud Director 环境中的虚拟机提供备份和恢复功能。

要禁用 VMware Cloud Director 和 Cyber Protect Cloud 之间的集成，请联系技术支持。

限制

- 仅在**由服务提供商托管**管理模式下的合作伙伴租户才可以与 VMware Cloud Director 集成，其父租户（如果有）也使用**由服务提供商托管**管理模式。有关租户类型及其管理模式的详细信息，请参阅 "创建租户"（第 35 页）。

  所有现有的直接合作伙伴都可以配置与 VMware Cloud Director 的集成。合作伙伴管理员还可以为子租户启用此选项，方法是在创建子合作伙伴租户时选中**合作伙伴拥有的 VMware Cloud Director 基础架构**复选框。
- 如果为您的租户启用了双因素身份验证，则必须使用标记为服务帐户的合作伙伴管理员帐户。否则，代理程序将无法对 Cyber Protect Cloud 进行身份验证。

  我们建议您为代理程序使用专用帐户。有关如何创建服务帐户的详细信息，请参阅 "若要将用户帐户转换为服务帐户"（第 49 页）。
- 在多个 VMware Cloud Director 组织中具有组织管理员角色的管理员只能为 Cyber Protection 中的一个客户租户管理备份和恢复。
- Cyber Protect 中控台将在新选项卡中打开。

软件要求

支持的 VMware Cloud Director 版本

- VMware Cloud Director 10.4, 10.5

支持的 Web 浏览器

- Google Chrome 29 或更高版本
- Mozilla Firefox 23 或更高版本
- Opera 16 或更高版本
- Microsoft Edge 25 或更高版本
- 在 macOS 和 iOS 操作系统中运行的 Safari 8 或更高版本

在其他 Web 浏览器（包括在其他操作系统中运行的 Safari 浏览器），用户界面可能显示错误，或者某些功能可能不可用。

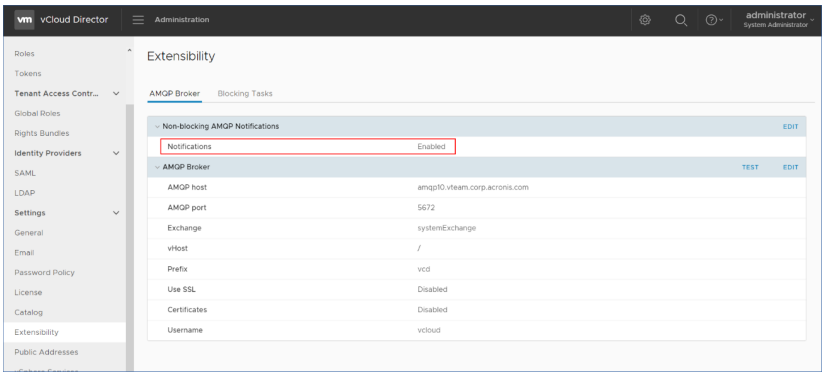
配置 RabbitMQ 消息代理

此过程取决于 Cyber Protect Cloud 的版本。简化过程适用于版本 23.06（已于 2023 年 6 月发布）及更高版本。

配置 RabbitMQ 消息代理

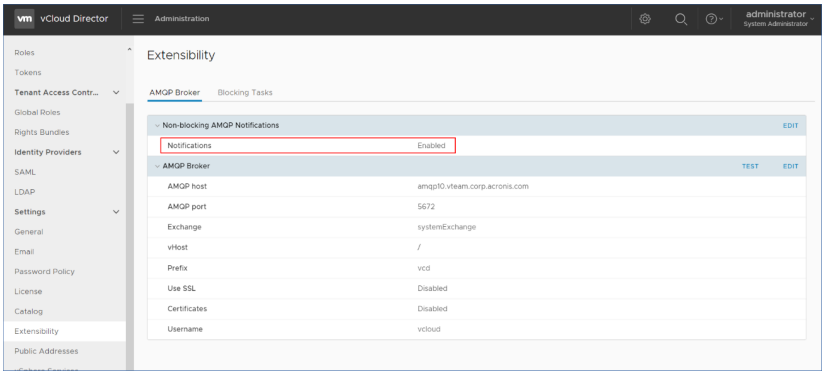
对于版本 23.06 及更高版本

1. 安装适用于您的 VMware Cloud Director 环境的 RabbitMQ AMQP 代理。
   有关如何安装 RabbitMQ 的详细信息，请参阅 VMware 文档：安装和配置 RabbitMQ AMQP 代理。
2. 以系统管理员身份登录到 VMware Cloud Director 提供商门户。
3. 转到**管理** > **可扩展性**，然后在**不阻止 AMQP 通知**下验证**通知**已启用。



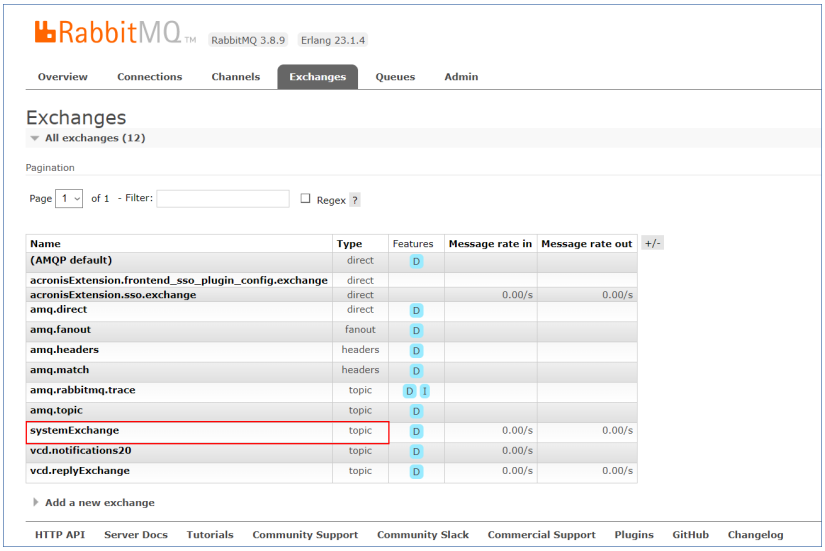
对于版本 23.05 及更早版本

1. 安装适用于您的 VMware Cloud Director 环境的 RabbitMQ AMQP 代理。
   有关如何安装 RabbitMQ 的详细信息，请参阅 VMware 文档：安装和配置 RabbitMQ AMQP 代理。
2. 以系统管理员身份登录到 VMware Cloud Director 提供商门户。
3. 转到**管理** > **可扩展性**，然后在**不阻止 AMQP 通知**下验证**通知**已启用。



4. 以管理员身份登录到 RabbitMQ 管理中控台。
5. 在**交换**选项卡上，验证交换(默认情况下，在名称 **SystemExchange** 下)已创建，并且其类型为

主题。



安装和发布适用于 VMware Cloud Director 的插件

当安装管理代理程序时，将自动安装适用于 VMware Cloud Director 的插件。

但是，需要手动将该插件发布给将使用 Cyber Protection 的租户。

发布适用于 VMware Cloud Director 的插件

1. 以系统管理员身份登录到 VMware Cloud Director 提供商门户。
2. 在导航菜单中，选择**自定义门户**。
3. 在**插件**选项卡上，选择 **Cyber Protection** 插件，然后单击**发布**。
4. 配置发布范围：
   a. 在**范围到**部分，请仅选中**租户**复选框。
   b. 在**发布到**部分中，选择**所有租户**以为所有现有和将来租户启用插件，或选择要为其启用插件的各个租户。
5. 单击**保存**。
6. 单击**信任**。

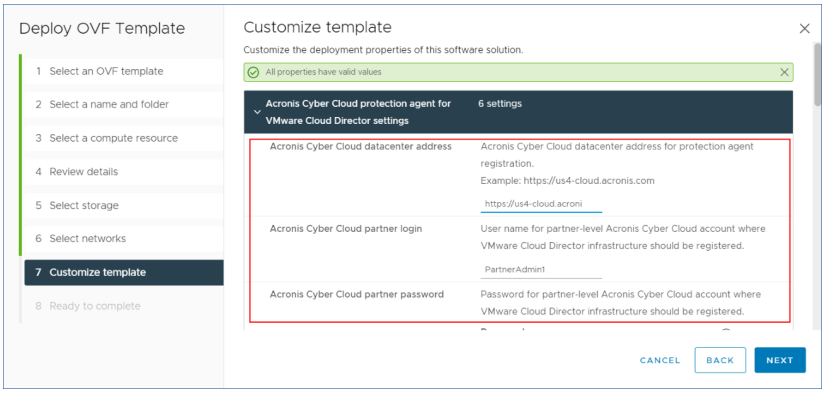
安装管理代理程序

1. 以合作伙伴管理员身份登录到 Cyber Protect Cloud 管理门户。
2. 转到**设置** > **位置**，然后单击**添加 VMware Cloud Director**。
3. 从**发布渠道**下拉列表中，选择代理程序的版本。可使用以下选项：
   - **最新** – 最新可用版本。
   - **上一稳定版** - 从之前的版本中安装保护代理程序的最新稳定版。
4. 单击**管理代理程序**链接，然后下载 ZIP 文件。
5. 提取管理代理程序模板文件 `vCDManagementAgent.ovf` 和虚拟硬盘文件 `vCDManagementAgent-disk1.vmdk`。

6. 在 vSphere Client 中，将管理代理程序 OVF 模板部署到 ESXi 主机中由 VMware Cloud Director 管理的 vCenter 实例下。

   重要事项
   在每个 VMware Cloud Director 环境中，仅安装一个管理代理程序。

7. 在**部署 OVF 模板**向导中，通过设置以下内容来配置管理代理程序：



   a. Cyber Protect Cloud 数据中心的 URL。例如，`https://us5-cloud.example.com`。
   b. 合作伙伴管理员登录名和密码。

      注意
      如果为您的租户启用了双因素身份验证，则必须使用标记为服务帐户的合作伙伴管理员帐户。否则，代理程序将无法对 Cyber Protect Cloud 进行身份验证。
      我们建议您为代理程序使用专用帐户。有关如何创建服务帐户的详细信息，请参阅 "若要将用户帐户转换为服务帐户"(第 49 页)。

   c. VMware Cloud Director 环境中虚拟机的备份存储的 ID。此备份存储只能由合作伙伴拥有。有关存储的更多详细信息，请参阅 "管理位置和存储"(第 68 页)。
      要查看 ID，请在管理门户中转到**设置** > **位置**，然后选择所需存储。可以在 URL 中的 **uuid=** 部分之后看到其 ID。
   d. Cyber Protect Cloud 计费模式：**按 GB** 或**按工作负载**。

      注意
      所选计费模式会应用于将创建的所有新客户租户。

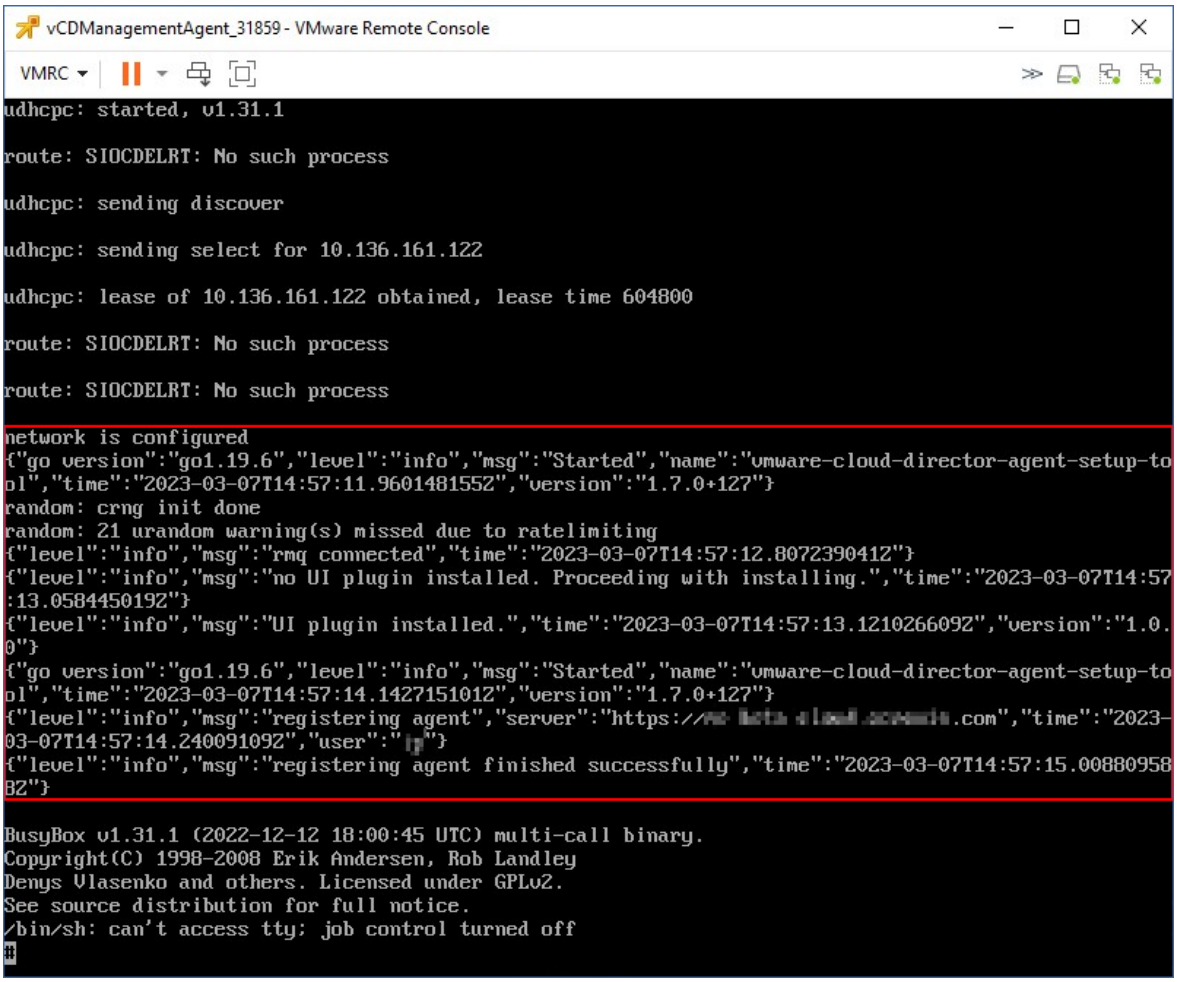
   e. VMware Cloud Director 参数：基础架构地址、系统管理员登录名和密码。
   f. RabbitMQ 参数：管理员登录名和密码。
   g. 代理程序的虚拟机上的 root 用户的密码。
   h. 网络参数：IP 地址、子网掩码、默认网关、DNS、DNS 后缀。
      默认情况下，仅启用一个网络接口。要启用第二个网络接口，请选中**启用 eth1** 旁边的复选框。

注意

确保网络设置允许管理代理程序访问 VMware Cloud Director 环境和您的 Cyber Protect Cloud 数据中心。

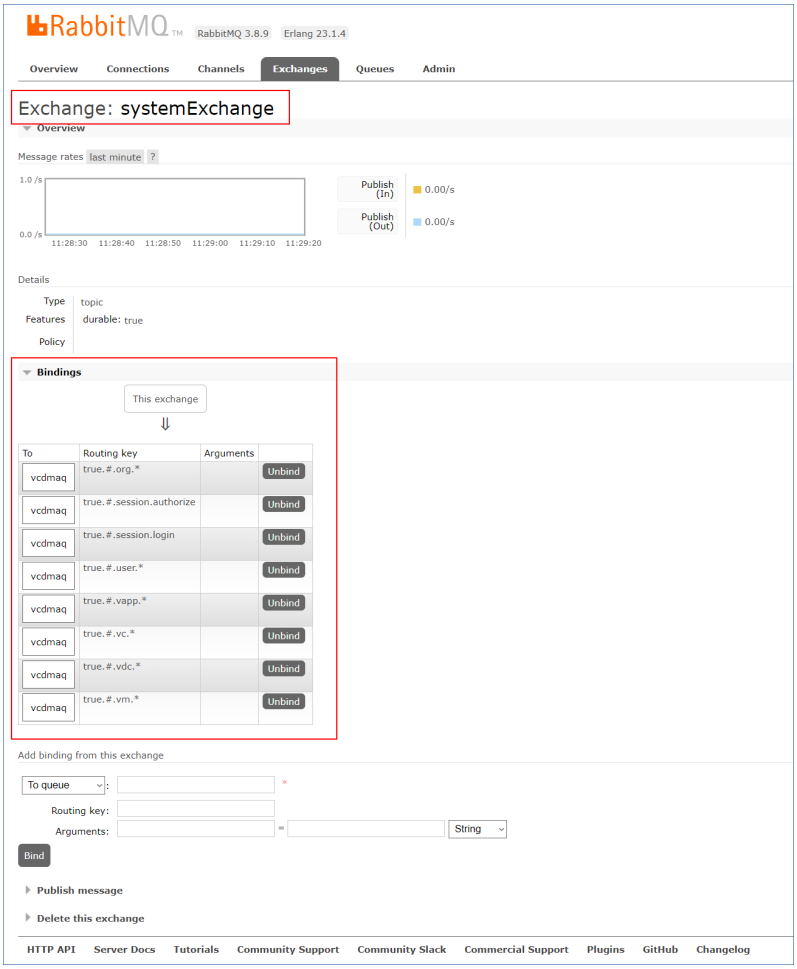
还可以在初始部署后配置管理代理程序设置。在 vSphere Client 中，关闭具有管理代理程序的虚拟机，然后依次单击**配置** > **设置** > **vApp 选项**。应用所需设置，然后打开具有管理代理程序的虚拟机。

8. [可选] 在 vSphere Client 中，打开具有管理代理程序的虚拟机的中控台，然后验证设置。



9. 验证 RabbitMQ 连接。
   a. 以管理员身份登录到 RabbitMQ 管理中控台。
   b. 在**交换**选项卡中，选择您在 RabbitMQ 安装期间设置的交换。默认情况下，其名称为 **systemExchange**。

c. 验证与 **vcdmaq** 队列的绑定。



下一步操作

如果代理程序版本为 24.12.39185 或更高，并且环境为 VMware vSphere 8.x 或更高，则可以启用 FIPS 合规模式。请参阅 "为 VMware 云 Director 启用 FIPS 合规模式"(第 172 页) 。

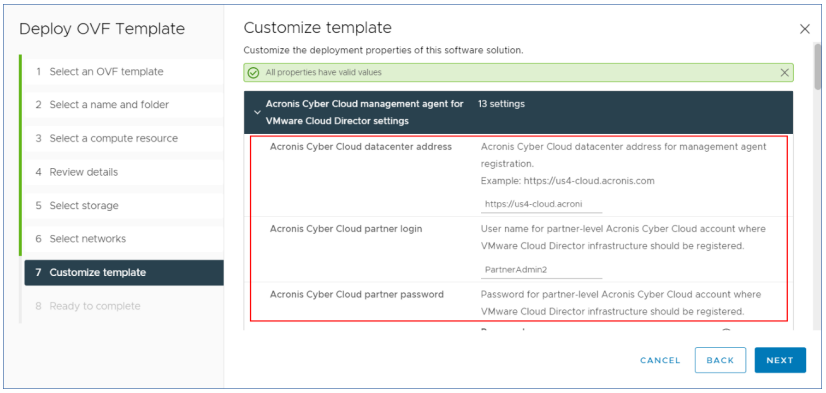
安装备份代理程序

1. 以合作伙伴管理员身份登录到管理门户。
2. 转到**设置** > **位置**，然后单击**添加 VMware Cloud Director**。
3. 从**发布渠道**下拉列表中，选择代理程序的版本。可使用以下选项：
   - **最新** – 最新可用版本。
   - **上一稳定版** - 从之前的版本中安装保护代理程序的最新稳定版。
4. 单击**备份代理程序**链接，然后下载 ZIP 文件。
5. 提取备份代理程序模板文件 `vCDCyberProtectAgent.ovf` 和虚拟硬盘文件 `vCDCyberProtectAgent-disk1.vmdk`。
6. 在 vSphere Client 中，将备份代理程序模板部署到所需的 ESXi 主机。
   每台主机需要至少一个备份代理程序。默认情况下，备份代理程序指派有 8 GB RAM 和 2 个 CPU，可以同时处理最多 5 个备份任务或恢复任务。

要处理更多任务或分发备份和恢复流量，请将其他代理程序部署到同一主机。或者，为了避免出现与内存不足有关的故障，建议您为现有代理程序指派 16 GB RAM 和 4 个 vCPU。

注意
在未安装备份代理程序的 ESXi 主机上备份虚拟机将失败，并显示“任务超时已到期”错误。

7. 在**部署 OVF 模板**向导中，请通过设置以下内容来配置备份代理程序：



a. Cyber Protect Cloud 数据中心的 URL。例如，`https://us5-cloud.example.com`。
b. 合作伙伴管理员登录名和密码。
   如果为您的租户启用了双因素身份验证，则必须使用标记为服务帐户的合作伙伴管理员帐户。否则，代理程序将无法对 Cyber Protect Cloud 进行身份验证。
   我们建议您为代理程序使用专用帐户。有关如何创建服务帐户的详细信息，请参阅 "若要将用户帐户转换为服务帐户"(第 49 页)。
c. VMware vCenter 参数：服务器地址、登录名和密码。
   代理程序将使用这些凭据连接到 vCenter 服务器。建议您使用已指派有**管理员**角色的帐户。否则，提供在 vCenter 服务器上具有必要权限的帐户。
d. 代理程序的虚拟机上的 `root` 用户的密码。
e. 网络参数：IP 地址、子网掩码、默认网关、DNS、DNS 后缀。
   默认情况下，仅启用一个网络接口。要启用第二个网络接口，请选中**启用 eth1** 旁边的复选框。

   注意
   确保您的网络设置将允许备份代理程序访问 vCenter 服务器和您的 Cyber Protect Cloud 数据中心。

f. 下载限制：最大下载速度(以 Kbps 为单位)，定义了恢复操作期间备份存档的读取速度。默认值为 0 - 无限制。
g. 上传限制：最大上传速度(以 Kbps 为单位)，定义了备份操作期间备份存档的写入速度。默认值为 0 - 无限制。

还可以在初始部署后配置备份代理程序设置参数。在 vSphere Client 中，关闭具有备份代理程序的虚拟机，然后依次单击**配置** > **设置** > **vApp 选项**。应用所需设置，然后打开具有备份代理程序的虚拟机。

8. 在 vSphere Client 中，请确保已为具有备份代理程序的虚拟机禁用**主机**和 **Storage vMotion**。

下一步操作

如果代理程序版本为 24.12.39185 或更高，并且环境为 VMware vSphere 8.x 或更高，则可以启用 FIPS 合规模式。请参阅 "为 VMware 云 Director 启用 FIPS 合规模式"(第 172 页) 。

为 VMware 云 Director 启用 FIPS 合规模式

VMware vSphere 8.x 及更高版本中的代理程序版本 24.12.39185 及更高版本可启用 FIPS 兼容模式。在此模式下，备份代理程序使用 FIPS 140-2 合规的加密库进行所有加密操作。有关详细信息，请参阅 FIPS 兼容模式。

重要事项
若要按预期运行，则必须在管理代理程序和备份代理程序上启用 FIPS 模式。

若要为 Cloud Director 实例中的 Cyber Protect 代理程序启用 FIPS 合规模式

1. 在 vSphere Client 中，找到 vCD 管理代理程序虚拟机，打开远程中控台，然后运行以下命令：

   ```
   fips-mode-setup --enable
   ```

2. 返回 vSphere Client，在要启用 FIPS 合规模式的 vCD Cyber Protect 代理虚拟机上，打开远程中控台，然后运行以下命令：

   ```
   fips-mode-setup --enable
   ```

3. 在要启用 FIPS 兼容模式的所有其他 vCD Cyber Protect 代理虚拟机上运行该命令。

更新代理程序

更新管理代理程序

1. 以合作伙伴管理员身份登录到 Cyber Protect Cloud 管理门户。
2. 转到**设置** > **位置**，然后单击**添加 VMware Cloud Director**。
3. 单击**管理代理程序**链接，然后下载具有最新代理程序的 ZIP 文件。
4. 提取管理代理程序模板文件 `vCDManagementAgent.ovf` 和虚拟硬盘文件 `vCDManagementAgent-disk1.vmdk`。
5. 在 vSphere Client 中，关闭具有当前管理代理程序的虚拟机。
6. 使用最新的 `vCDManagementAgent.ovf` 和 `vCDManagementAgent-disk1.vmdk` 文件部署具有新管理代理程序的虚拟机。
7. 使用与旧管理代理程序相同的设置来配置该管理代理程序。
8. [可选] 删除具有旧管理代理程序的虚拟机。

重要事项
每个 VMware Cloud Director 环境必须只有一个活动的管理代理程序。

更新备份代理程序

1. 以合作伙伴管理员身份登录到 Cyber Protect Cloud 管理门户。
2. 转到**设置** > **位置**，然后单击**添加 VMware Cloud Director**。
3. 单击**备份代理程序**链接，然后下载具有最新代理程序的 ZIP 文件。
4. 提取管理代理程序模板文件 `vCDCyberProtectAgent.ovf` 和虚拟硬盘文件 `vCDCyberProtectAgent-disk1.vmdk`。
5. 在 vSphere Client 中，关闭具有当前备份代理程序的虚拟机。
   当前可能正在运行的所有备份和恢复任务都将失败。要检查是否有任何任务正在运行，请在 vSphere Client 中打开具有备份代理程序的虚拟机的中控台，然后运行命令 `ps | grep esx_worker`。确保没有活动的 `esx_worker` 进程。
6. 使用最新的 `vCDCyberProtectAgent.ovf` 和 `vCDCyberProtectAgent-disk1.vmdk` 文件部署具有新备份代理程序的虚拟机。
7. 使用与旧备份代理程序相同的设置来配置该备份代理程序。
8. [可选] 删除具有旧备份代理程序的虚拟机。

创建备份管理员

组织管理员可以将备份管理委托给专门指派的备份管理员。

创建备份管理员

1. 在 VMware Cloud Director 租户门户中，依次单击**管理** > **角色** > **新建**。
2. 在**添加角色**窗口中，为新角色指定名称和描述。
3. 向下滚动权限列表，然后在**其他**下，选择**自助服务 VM 备份操作员**。

注意
在安装适用于 VMware Cloud Director 的插件后，**自助服务 VM 备份操作员**权限将变为可用。有关如何执行此操作的详细信息，请参阅 "安装和发布适用于 VMware Cloud Director 的插件"(第 167 页)。

4. 在 VMware Cloud Director 租户门户中，单击**用户**。
5. 选择一个用户，然后单击**编辑**。
6. 为该用户指派您创建的新角色。

结果，所选用户将能够管理该组织中虚拟机的备份。

注意
VMware Cloud Director 环境的系统管理员可以定义一个已启用**自助服务 VM 备份操作员**权限的全局角色，然后将该角色发布给租户。因此，组织管理员只需将该角色指派给用户。

系统报告、日志文件和配置文件

出于故障排除目的，可能需要使用 sysinfo 工具创建系统报告，或者检查具有代理程序的虚拟机上的日志和配置文件。

可以通过在 vSphere Client 中打开其中控台直接访问虚拟机，也可以通过 SSH 客户端远程访问虚拟机。要通过 SSH 客户端访问虚拟机，首先必须启用与该计算机的 SSH 连接。

启用与虚拟机的 SSH 连接

1. 在 vSphere Client 中，打开具有代理程序的虚拟机的中控台。
2. 在命令提示符处，运行以下命令：/bin/sshd，以启动 SSH daemon。

因此，可以使用 SSH 客户端（例如 WinSCP）连接到此虚拟机。

运行 sysinfo 工具

1. 访问具有代理程序的虚拟机。
   - 要在 vSphere Client 中直接访问虚拟机，请打开该虚拟机的中控台。
   - 要远程访问虚拟机，请通过 SSH 客户端连接到虚拟机。
     使用以下默认的登录名:密码组合：root:root。
2. 导航到 /bin 目录，然后运行 sysinfo 工具。

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

   因此，系统报告文件将保存到默认目录：/var/lib/Acronis/sysinfo。
   可以通过使用 --target_dir 选项运行 sysinfo 工具来指定另一个目录。

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

3. 使用 SSH 客户端下载已生成的系统报告。

访问日志或配置文件

1. 通过 SSH 客户端连接到虚拟机。
   使用以下默认的登录名:密码组合：root:root。
2. 下载所需文件。
   可以在以下位置找到日志文件：
   - 备份代理程序：/opt/acronis/var/log/vmware-cloud-director-backup-service/log.log
   - 管理代理程序：/opt/acronis/var/log/vmware-cloud-director-management-agent/log.log

   可以在以下位置找到配置文件：
   - 备份代理程序：/opt/acronis/etc/vmware-cloud-director-backup-service/config.yml
   - 管理代理程序：/opt/acronis/etc/vmware-cloud-director-management-agent/config.yaml

访问 Cyber Protect 中控台

以下管理员可以管理 VMware Cloud Director 组织中的虚拟机备份：

- 组织管理员
- 专门指派的备份管理员
  有关如何创建此类管理员的详细信息，请参阅 "创建备份管理员"(第 173 页)。

管理员可以通过单击 租户门户的导航菜单中的**网络安全保护**，来访问自定义 Cyber Protect 中控台。

注意
单点登录仅适用于组织管理员，不支持用于使用 VMware Cloud Director 租户门户的系统管理员。

在 Cyber Protect 中控台中，管理员只能访问其自己的 VMware Cloud Director 组织项目：虚拟数据中心、vApp 和各个虚拟机。他们可以管理 VMware Cloud Director 组织资源的备份和恢复。

合作伙伴管理员可以访问其客户租户的 Cyber Protect 中控台，可以代表他们管理备份和恢复。

执行备份和恢复

创建保护计划

若要配置备份设置，则必须创建保护计划。

可以将保护计划应用于多台计算机。此外，还可以对同一台计算机应用多个保护计划。

限制

- 仅支持整个计算机的备份。无法备份单个磁盘或卷。
- 不支持文件筛选器(包含/排除)。
- 云存储是唯一可用的备份位置。存储在管理代理程序设置中配置，用户无法在保护计划中更改它。
- 支持以下备份方案：**始终增量备份(单个文件)**、**始终完整备份**和**每周完整备份，每天增量备份**。
- 仅支持备份后清理。

创建保护计划

1. 在 Cyber Protect 中控台中，转至**设备** > **VMware Cloud Director**。
2. 选择要保护的计算机，然后单击**保护**。
3. [如果已有应用的计划]单击**添加计划**。
4. 单击**创建计划**。
5. 在**加密**中，配置加密设置。
6. [可选]若要重命名保护计划，请单击铅笔图标，然后输入新名称。
7. [可选]若要更改备份方案或计划，请单击**计划**，然后配置设置。
8. [可选]若要更改保留规则，请单击**数量方法**，然后配置设置。
9. [可选]若要更改备份选项，请单击**备份选项**，然后配置设置。
10. 单击**应用**。

恢复计算机

您可以将备份恢复到原始虚拟机或新虚拟机。

限制

- 不支持文件级恢复。
- 您可以在 VMware Cloud Director 10.4 及更高版本中将备份恢复到新的虚拟机。
  若要将备份恢复到新虚拟机，备份必须由版本 24.02 或更高版本的代理程序创建。可以在 `ProductVersion.conf` 文件中检查代理程序版本，该文件位于带有代理程序的虚拟机的 `/etc` 目录中。
- 将备份恢复到新计算机后，新计算机将显示在**设备** > **VMware Cloud Director** > 组织 > 虚拟数据中心 >**独立虚拟机**中。无法选择特定的 vApp 作为恢复目标。

恢复计算机

若要恢复到原计算机

1. 在 Cyber Protect 中控台中，通过以下方式之一选择恢复点：
   - 转至**设备** > **VMware Cloud Director**，选择备份计算机，单击**恢复**，然后选择恢复点。
   - 转至**设备** > **VMware Cloud Director**，选择备份存档，单击**显示备份**，然后选择恢复点。
2. 单击**恢复计算机**。
3. 单击**开始恢复**。

若要恢复到新计算机

1. 在 Cyber Protect 中控台中，通过以下方式之一选择恢复点：
   - 转至**设备** > **VMware Cloud Director**，选择备份计算机，单击**恢复**，然后选择恢复点。
   - 转至**设备** > **VMware Cloud Director**，选择备份存档，单击**显示备份**，然后选择恢复点。
2. 单击**恢复计算机**。
3. 单击**“目标计算机”**，然后选择**“新计算机”**。
4. 为新计算机选择虚拟数据中心。
5. 指定新计算机的名称。
   默认情况下，建议使用原始计算机的名称。
6. 单击**确定**。
7. [可选] 单击**“VM 设置”**以更改新计算机的以下任意设置，然后单击**“确定”**：
   - RAM 大小
   - 虚拟处理器数量
   - 每个插槽的核心数
   - 存储配置文件
   - 网络适配器和分配的网络
8. [可选] 单击**“磁盘映射”**以更改磁盘映射或磁盘的存储配置文件，然后单击**“确定”**。
9. 单击**开始恢复**。

删除与 VMware Cloud Director 的集成

还原配置并从 Cyber Protect Cloud 中注销 VMware Cloud Director 实例是一个复杂的过程.请与支持代表联系以寻求帮助。

使用合作伙伴门户

合作伙伴门户是专为参与 #CyberFit 合作伙伴计划的服务提供商、代理商和经销商设计的。

通过合作伙伴门户，可以访问 内容、工具和培训。

开始使用合作伙伴门户

1. 通过以下方式之一访问合作伙伴门户：
   - 单击管理门户左下角的**成为合伙伙伴**。
   - 访问合作伙伴门户网站。
2. 在合作伙伴计划中注册公司。
3. 通过电子邮件接收访问详细信息。

合作伙伴门户角色

合作伙伴门户包括许多角色，可以根据需要将这些角色指派给您的用户。

下表描述了每个可用角色，以及在合作伙伴门户中指派给每个角色的权限：

角色	描述
基本	应用于所有用户的默认角色。 此角色会授予访问合作伙伴门户的基本功能，包括仪表板，合作伙伴计划，内容中心和培训。
培训	拥有此角色的用户可以访问培训材料。合作伙伴门户的其他功能将对这些用户不可用。
营销	此角色授予营销专家访问合作伙伴门户所需的功能，包括仪表板、合作伙伴计划、营销、内容中心、培训、数据中心状态和数据库管理。
销售人员	拥有此角色的用户可以访问合作伙伴门户网站对销售专家必要的功能，例如仪表板，合作伙伴计划，销售，内容中心，培训，数据中心状态和数据库管理。
销售和营销	此角色授予统一销售和营销专员所需的合作伙伴门户的访问权限，包括仪表板，合作伙伴计划，销售，营销，内容中心，培训，数据中心状态和数据库管理。
管理员	管理员可访问合作伙伴门户网站的所有功能，包括仪表板、合作伙伴计划、销售、营销、内容中心、培训、数据中心状态和数据库管理。此外，管理员还可以管理合作伙伴用户的权限并修改公司信息。

索引