Cyber Protect Cloud

23.02

合作伙伴管理员指南

修改：2023/2/28

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，例如高级备份、高级安全性等。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 103 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 6 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 8 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 • 高级安全性 - 2/10 • 高级备份工作站 - 1/10 • 高级管理 - 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:三个工作负载使用高级管理包的功能、两个工作负载使用高级安全包的功能,以及一个工作负载使用高级备份包的功能。

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 • 高级备份工作站 - 2/42 • 高级安全性 - 13/42 • 高级管理 - 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服务中控台中的安装程序可用性?

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 6 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 53 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 7 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 12 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。	本地存储将不可用作客户租户内备份的目标。
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进行数据源(包括 Microsoft 365 和 Google Workspace) 的备份和恢复。
所有灾难恢复产品项目	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。

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**。

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**

  此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。

  Microsoft 365 席位的许可取决于为 Cyber Protection 选择的计费模式。

  在**按工作负载**计费模式下，**Microsoft 365 席位**配额按唯一用户进行计算。唯一用户是具有以下至少一项产品/服务的用户：

  - 受保护的邮箱
  - 受保护的 OneDrive
  - 有权访问至少一项受保护的公司级资源：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。

  注意

  不会向没有受保护的个人邮箱或 OneDrive 且只能访问共享资源（共享邮箱、SharePoint 站点和 Microsoft Teams）的受阻止 Microsoft 365 用户收取费用。

  受阻止用户是没有有效登录名且无法访问 Microsoft 365 服务的用户。要了解如何阻止 Microsoft 365 组织中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 16 页）。

  以下 Microsoft 365 席位不会收费，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

有关“按 GB”计费模式的许可选项的详细信息，请参阅 Cyber Protect 云：Microsoft 365（按 GB 许可）。

有关“按工作负载”计费模式的许可选项的详细信息，请参阅 Cyber Protect 云：Microsoft 365 许可和定价变更。

- **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 SharePoint Online**

  此配额由服务提供商应用于整个公司。此配额可启用或禁用保护 SharePoint Online 站点的功能，以及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 备份所占据的存储空间量。

- **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。

- **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。

只要向用户的邮箱或 OneDrive 应用至少一个保护计划，Microsoft 365 席位就被视为受保护。只要向用户的邮箱或 Google Drive 应用至少一个保护计划，Google Workspace 席位就被视为受保护。

当超出许多席位的超额时，公司管理员无法将保护计划应用于更多席位。

存储的配额

- **本地备份**

  本地备份配额可限制使用云基础架构创建的本地备份的总大小。不能为此配额设置超额。

- **云资源**

  云资源配额结合了备份存储的配额和灾难恢复的配额。备份存储空间配额限制了位于云存储中备份的总大小。当超出备份存储空间配额超额时，备份失败。

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。

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，则可以在服务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）。

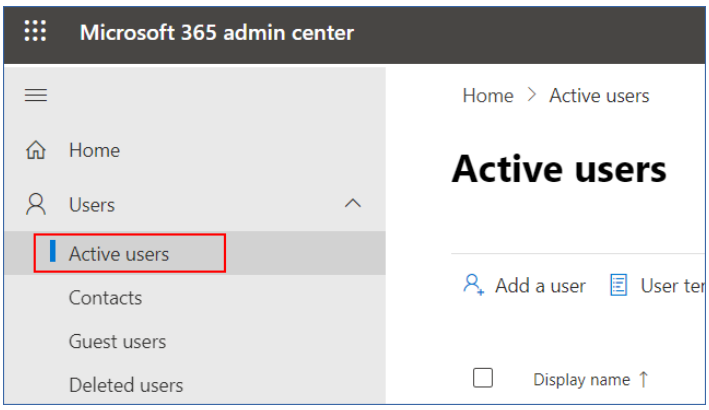
首先，系统会检查是否有已分配的**虚拟机**配额。如果找不到，系统会自动尝试获取**工作站**配额。如果还是找不到，系统不会自动获取其他配额。如果您具有足够贵于**虚拟机**配额的配额并且该配额适用于虚拟机，则可以登录到服务中控台，然后手动指派**服务器**配额。

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。

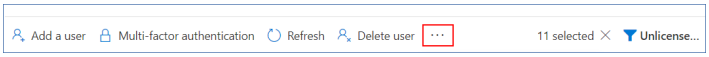
防止未经许可的用户登录

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**。

灾难恢复配额

注意
灾难恢复产品项目仅通过灾难恢复附加组件提供。

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冷存储大小。此存储会从创建恢复服务器时就开始计算，无论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仅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。
  当配额禁用后，服务器在服务中控台中可见，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**
  该配额定义可以访问此服务的用户数量。
  管理员帐户不再作为此配额的一部分计数。
- **云存储**
  这是用于存储用户文件的云存储。该配额在云存储中为租户定义分配空间。

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**
  公证存储是存储已公证文件、已签名文件和正在进行公证或签名的文件的云存储。此配额定义这些文件可以占用的最大空间。
  要减少此配额的使用，您可以从公证存储中删除已公证或已签名的文件。
- **公证**
  此配额定义可通过公证服务公证的文件的最大数量。文件一旦上传到公证存储且其公证状态变为进行中，即视为已公证。
  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**
  此配额定义可通过公证服务签名的文件的最大数量。文件一旦发送进行签名即被视为已签名。

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。
- 将向运行桌面 Windows 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。如果**虚拟机**配额不可用，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 Protection 服务中控台中，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**更改许可证**窗口中，选择所需的服务配额或**无配额**，然后单击**更改**。

更改一组计算机的服务配额

1. 在 Cyber Protection 服务中控台中，转到**设备**。
2. 选择多台计算机，然后单击**指派配额**。
3. 在**更改许可证**窗口中，选择所需的服务配额或**无配额**，然后单击**更改**。

代理程序安装程序依赖于产品项目

视允许的产品项目而定，相应的代理程序安装程序将在服务中控台的**添加设备**部分中可用。在下表中，可以查看代理程序安装程序及其在服务中控台中的可用性，具体取决于启用的产品项目。

启用的产品项目 代理程序安装程序	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
工作站 - 适用于 Windows 的代理程序		+	+					+
工作站 - 适用于 Mac OS 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			+					

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 Microsoft 365 的代理程序				+				
适用于 Google Workspace 的代理程序					+			
适用于 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 21 页）。

密码要求

用户帐户的密码长度必须至少为 9 个字符。还会检查密码的复杂性，并分为以下类别之一：

- 弱
- 中
- 强

不会保存弱密码，即使它可能包含 9 个或更多字符也是如此。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。

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

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. 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。

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**公司管理 > 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 Protection 中控台

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

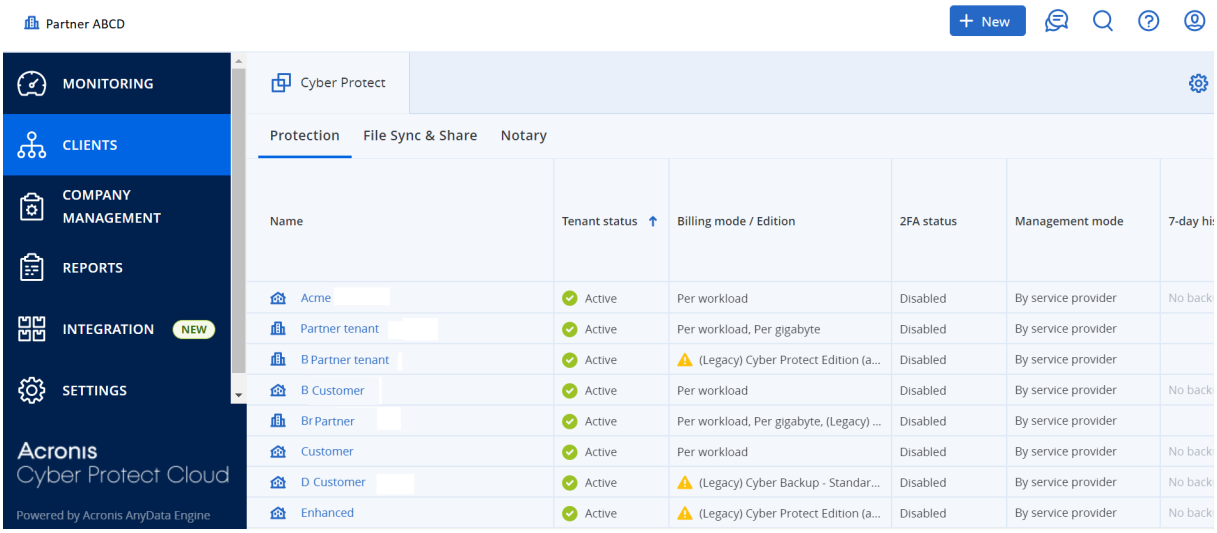
   或者，在**客户端**下，选择一个客户，然后单击**管理服务**。

因此，系统会将您重定向到 Cyber Protection 中控台。

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**选项卡仅显示您当前正在操作的租户的直接子租户。
- **公司管理**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。
- 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。

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。

此限制同样适用于通过 API 访问管理门户。

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。

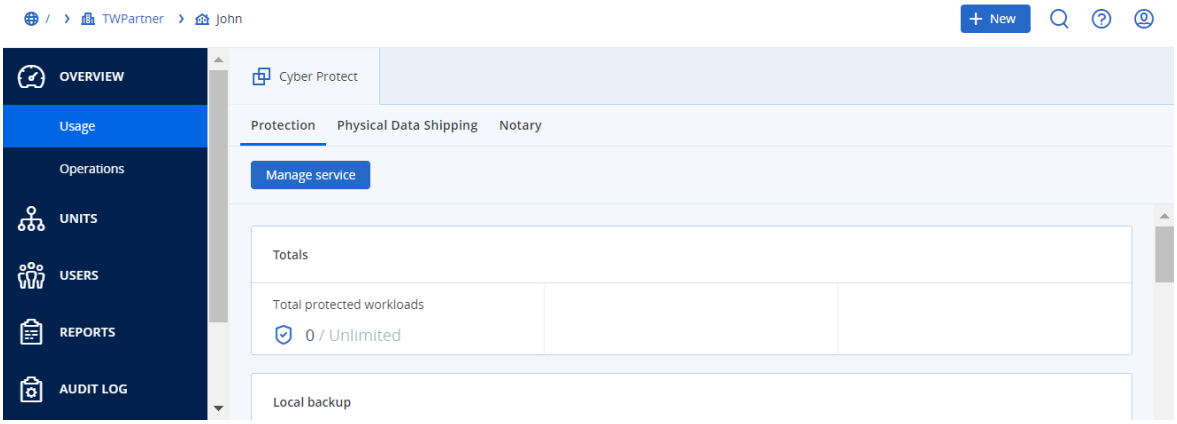
访问服务

“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。

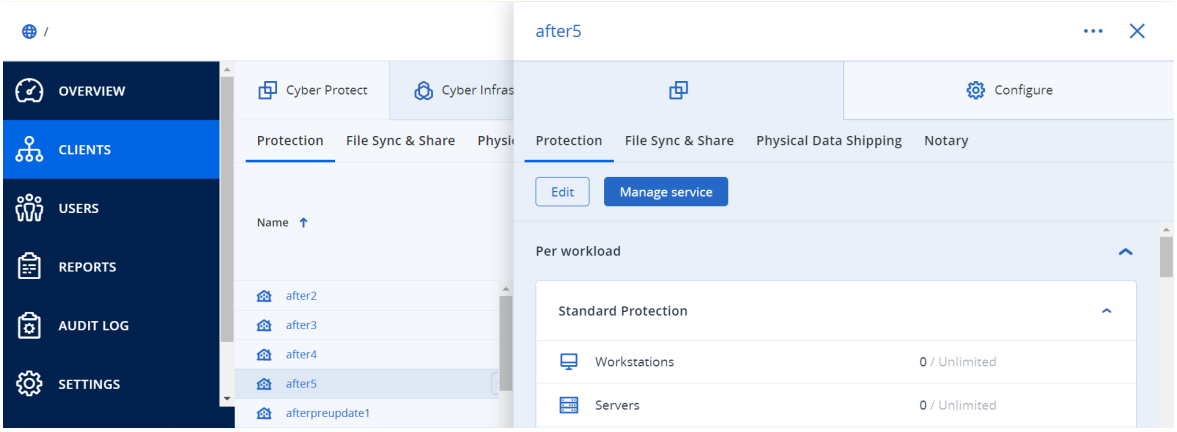


“客户端”选项卡

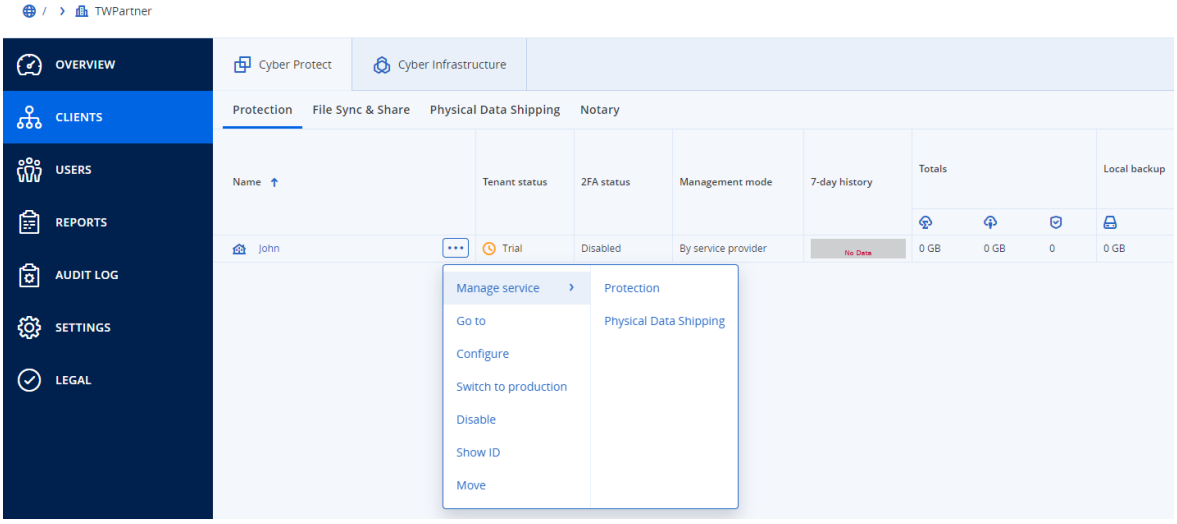
客户选项卡显示您正在操作的租户的子租户，并允许您在这些子租户内访问服务。

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	说明
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。

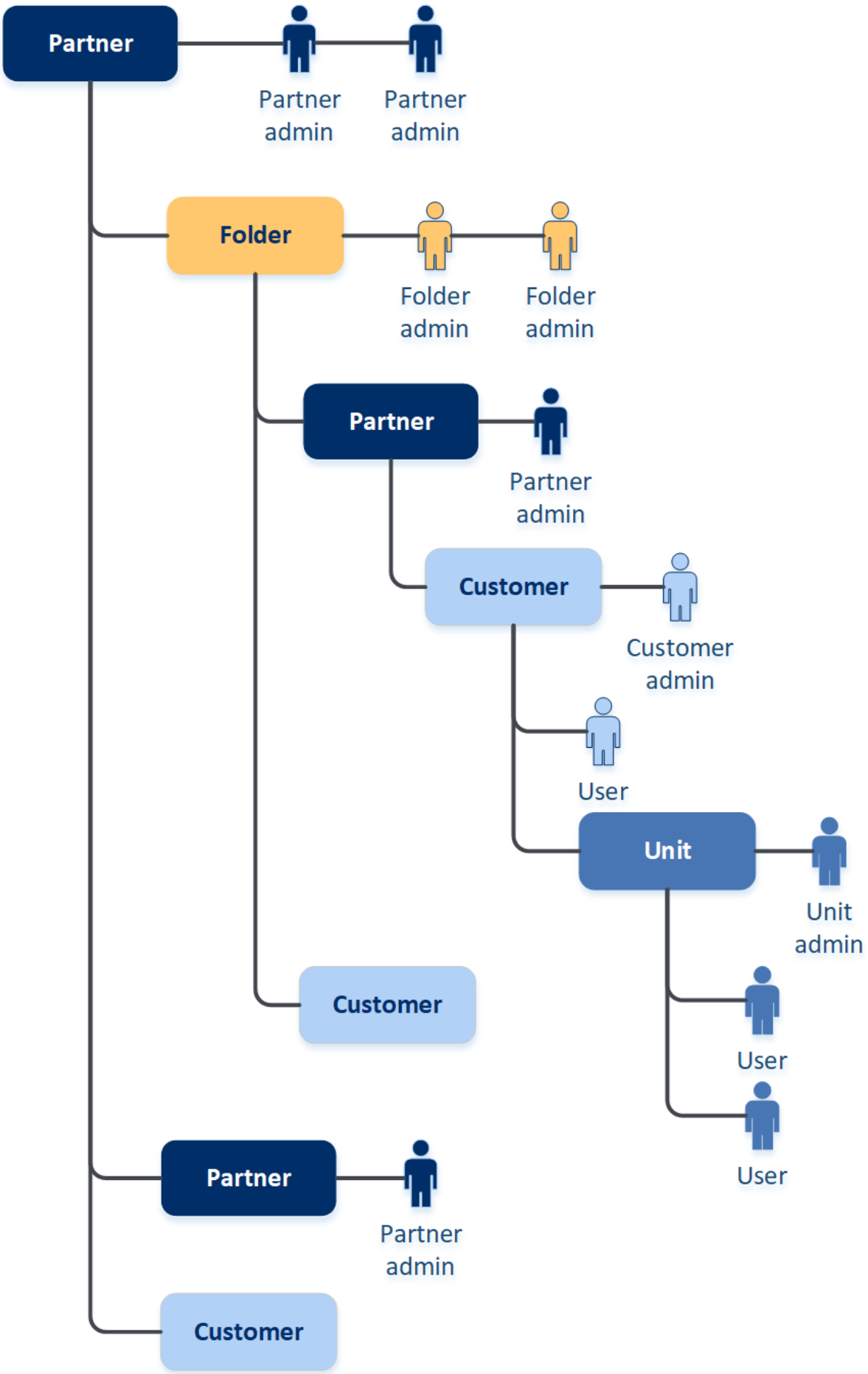
每个帐户都属于某个租户。租户是专用于合作伙伴或客户的管理门户资源（例如用户帐户和子租户）和服务产品（已启用的服务和服务中的产品项目）的一部分。租户层次结构应与服务用户和提供商之间的客户/供应商关系相匹配。

- **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

*需要执行这些操作的合作伙伴管理员可以为其自己创建客户管理员或用户帐户。

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。
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. [仅当创建客户租户时] 在**模式**中，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不包含试用模式租户的使用情况数据。

重要事项

如果您在月中将模式从试用切换为生产，则整个月都会包含在每月服务使用情况报告中。因此，我们建议您在某月的第一天切换模式。当租户保持处于试用模式一整个月时，该模式会自动切换为生产模式。

有两种可能的场景会自动将租户的试用模式切换为生产模式：

- 在月中，在这种情况下，**下一个**整月也会包含在每月服务使用情况报告中。
- [建议选项] 在一个月的第一天，仅会计算当月。

7. 在**管理模式**中，选择以下一种模式来管理对租户的访问权限：
   - **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、服务、备份和其他资源）。
   - **由服务提供商托管** - 此模式授予父租户的管理员对该租户的完全访问权限：修改属性；管理租户、用户和服务；访问备份和其他资源。

   如果管理模式是**自助服务**，则只有您创建的租户的管理员才能更改该管理模式。为此，该已创建租户的管理员可以转到**设置** > **安全**，然后设置支持访问开关。

   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**中，启用或禁用租户的双重身份验证。

   如果启用，则将要求此租户的所有用户都为其帐户设置双重身份验证，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“增强的安全性”模式下创建客户租户时] 在**安全性**中，选中**增强的安全性模式**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 "增强的安全性模式"（第 30 页）。

重要事项

在创建租户后不能禁用“增强的安全性”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. 输入管理员帐户的登录名和电子邮件地址。其余字段是可选字段，但提供更多沟通渠道，以防我们需要联系管理员。
   b. 选择一种语言。

      如果不选择语言，则默认使用英语。
   c. 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 30 页）。

增强的安全性模式

增强的安全模式为具有增加的安全需求的客户提供特殊设置。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。

仅当创建新的客户租户时，合作伙伴管理员才可以启用增强的安全模式，并且以后不能禁用此模式。无法为已存在的租户启用增强的安全模式。

在增强的安全模式下，在客户租户中创建的所有备份及其单位都自动使用 AES 算法和 256 位密钥加密。用户仅可以在受保护的设备上设置其加密密码，不能在保护计划中设置加密密码。

云服务不能访问加密密码。由于此局限性，在增强的安全模式下，以下功能不可用于租户：

- 通过服务中控台恢复
- 通过服务中控台在文件级别浏览备份
- 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

限制

- 增强的安全模式仅与代理程序兼容，其版本为 15.0.26390 或更高。
- 增加的安全模式不可用于运行 Red Hat Enterprise Linux 4.x 或 5.x 及其衍生产品的设备。

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 32 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。

     对于高级灾难恢复，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 31 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。

   注意
   可以禁用与高级保护功能相关的产品项目，但当用户在保护计划中启用高级功能时，将会自动启用这些产品项目。

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。

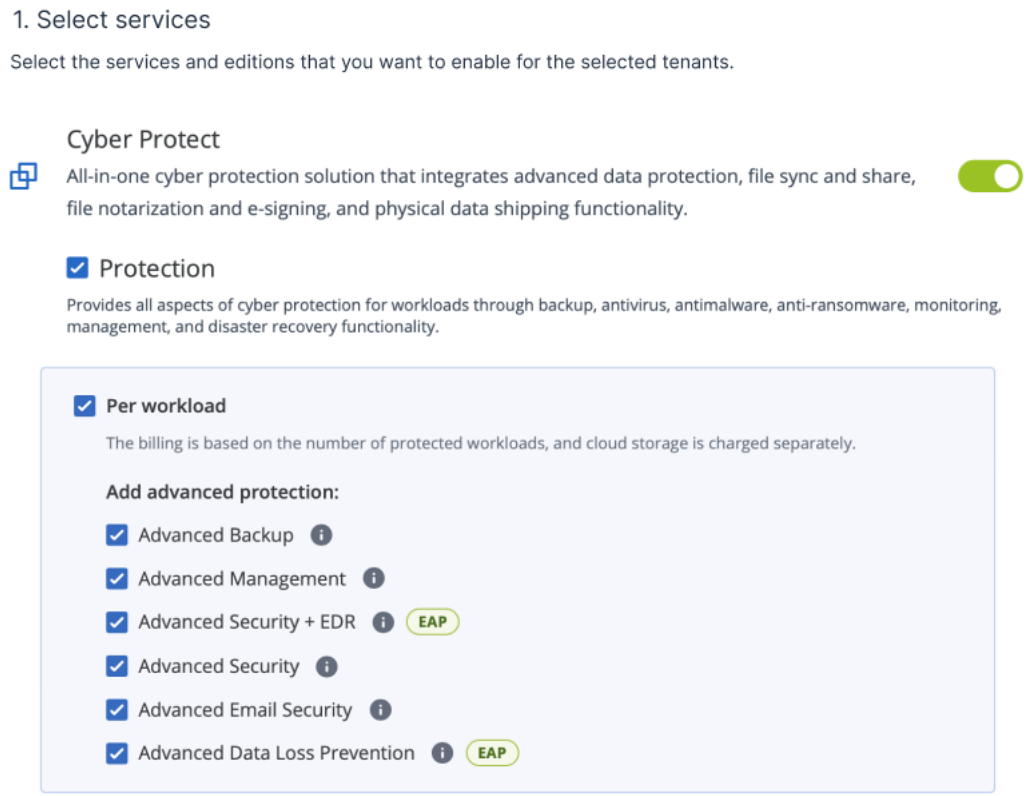
为多个现有租户启用服务

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

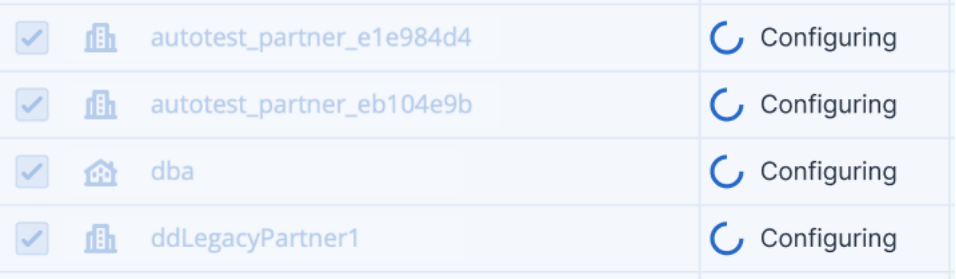
1. 在管理门户中，转到**客户端**。
2. 在右上角，单击**配置服务**。
3. 通过选中租户名称旁边的复选框，来选择要启用服务的每个租户，然后单击**下一步**。
4. 在**选择服务**部分中，选择要应用于所有选定租户的相关服务，然后单击**下一步**。



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。

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**公司管理** > **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。

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**公司管理** > **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，请在 中联系客户经理。
- 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。

如果对租户的访问受到限制，父租户管理员只能修改租户属性。他们完全看不到帐户和子租户。

防止更高级别的管理员访问您的租户

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

结果，父租户的管理员将拥有对您租户受限制的访问权限。他们将仅可修改租户属性，但不能访问或管理内部的任何内容(例如，租户、用户、服务、备份和其他资源)。

如果**支持访问**开关已启用，那么父租户的管理员将拥有对您租户的完全访问权限。他们将能够执行以下操作：修改属性；管理租户、用户和服务；访问备份和其他资源。

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。

重要事项
删除租户是不可逆的！

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。

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/候选者/单位管理员帐户 — 将服务管理委派给访问权限严格限制在相应客户/候选者/单位的其他人员。
- 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 23 页)。
3. 在右上角，依次单击**新建** > **用户**。
   或者转至**公司管理** > **用户**，并单击 **+ 新建**。
4. 为帐户指定以下联系信息：
   - **登录**

     重要事项
     每个帐户都必须有一个唯一的登录名。

- **电子邮件**

  重要事项
  如果用户是在 File Sync & Share 服务中注册的，请提供用于 File Sync & Share 注册的电子邮件地址。
  请注意，每个客户用户帐户都必须有唯一的电子邮件地址。

- **名字**
- **姓氏**
- [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**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，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，用户将拥有您在所选服务中选择的角色。
7. 单击**创建**。

新创建的用户帐户即会显示在**公司管理**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**公司管理** > **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*（即不需要双重身份验证的帐户）。

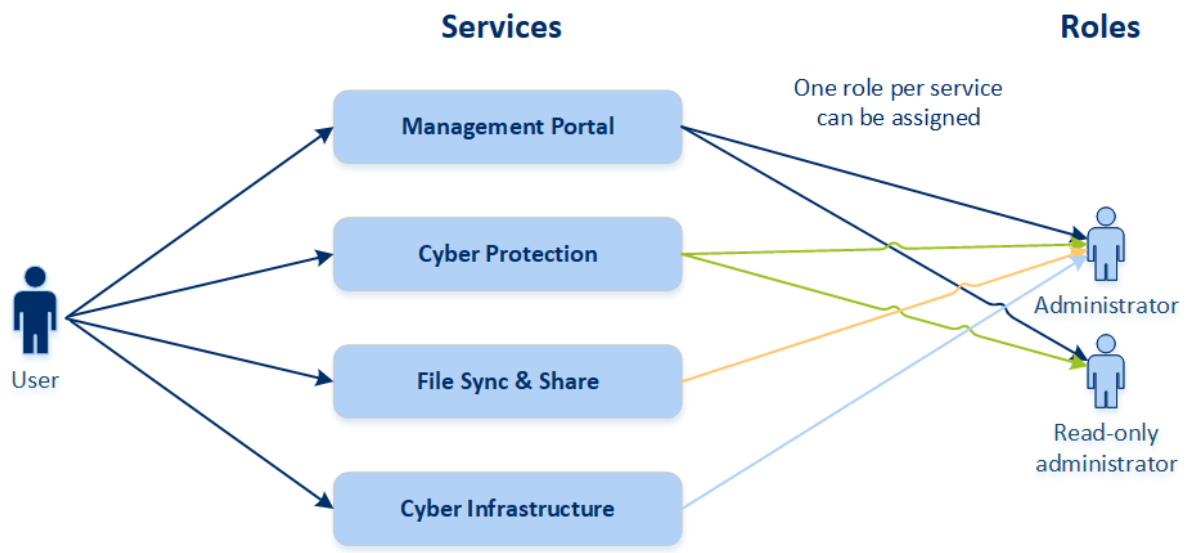
将用户帐户转换为服务帐户类型

1. 在管理门户中，转到**公司管理** > **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。

服务	角色	说明
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 Cyber Protection 服务的灾难恢复附加组件，则此角色还可授予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	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。此类用户可以在“只读”模式下访问组织中其他用户的数据。

	合作伙伴级别	
	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。此类用户可以在只读模式下访问组织中其他用户的数据。
	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。此类用户可以在只读模式下访问组织中其他用户的数据。
Cyber Protection	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 Cyber Protection 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高级管理包的租户。
	管理员	使用此角色可配置和管理您客户的 Cyber Protection。 该角色是配置和管理“灾难恢复”功能及公司白名单所必需的。
	只读管理员	该角色将提供对 Cyber Protection 服务的所有对象的“只读”访问权限。此类用户可以在只读模式下访问组织中其他用户的数据。 只读管理员无法配置和管理“灾难恢复”功能或公司允许列表。
	还原操作者	该角色提供对 Microsoft 365 和 Google Workspace 组织备份的访问并允许其恢复，同时限制对敏感内容的访问。
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。

只读管理员角色

具有此角色的帐户对 Cyber Protection Web 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。

“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。

- 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。

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。

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

还原操作者角色

此角色仅在 Cyber Protection 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。
- 浏览并刷新备份列表。
- 浏览备份而不访问其内容。还原操作者可以查看已备份文件的名称以及已备份电子邮件的主题和发件人。
- 搜索备份（不支持全文搜索）。
- 将云到云备份恢复到原始 Microsoft 365 或 Google Workspace 组织中的原始位置。

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。
- 在将备份恢复到自定义位置时，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	创建 编辑 更改状态 运行	创建 编辑 更改状态 运行

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

要更改用户的通知设置，请导航到**公司管理** > **用户**。选择要配置通知的用户，然后单击**设置**部分中的铅笔图标。如果为创建用户的租户启用了 Cyber Protection 服务，则可以使用以下通知设置：

- **配额过度使用通知**(默认已启用)
  已超出配额的相关通知。
- **预定的使用情况报告**(默认已启用)
  在每个月的第一天发送的使用情况报告。
- **URL 品牌推广通知**(默认已禁用)
  关于用于 Cyber Protect 云服务的自定义 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。
- **失败通知**、**警告通知**和**成功通知**(默认禁用)
  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。
- **活动警告的每日概述**(默认启用)

每日概述是根据生成概述时服务中控台中存在的活动警告列表生成的。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。如果当前没有活动警告，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**(默认情况下禁用)

  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。

- **恢复通知**(默认已禁用)

  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：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。

- **数据丢失防护通知**(默认已禁用)

  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。

- **安全性事件通知**(默认已禁用)

  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**。对于终端检测和响应 (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**(默认已禁用)

  有关灾难恢复基础架构出现问题时的通知：灾难恢复基础架构不可用或 VPN 隧道不可用时。

所有通知都发送到用户的电子邮件地址。

用户角色收到的通知

Cyber Protection 发送的通知取决于用户角色。

通知类型\用户角色	用户	客户管理员
自己设备的通知	是	是
组织中所有设备的通知	不适用	是(**安全事件通知**除外)
Microsoft 365、Google Workspace 和其他基于云的备份的通知	不适用	是

通知类型\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。

要启用已禁用的用户帐户，请在用户列表中选择它，然后依次单击省略号图标 > **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。

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。

重要事项
删除用户帐户是不可逆的！

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：

- 将删除该用户帐户。
- 将删除属于该用户帐户的所有数据。
- 将注销与该用户帐户关联的所有计算机。

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。

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 TOTP 机密信息，并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 TOTP 机密信息，使用支持在云中备份代码的应用程序)。如果丢失第二重身份验证设备，您需要 TOTP 机密信息来重置双重身份验证。

6. 系统会在身份验证应用程序中生成一次性 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"屏幕上输入 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。

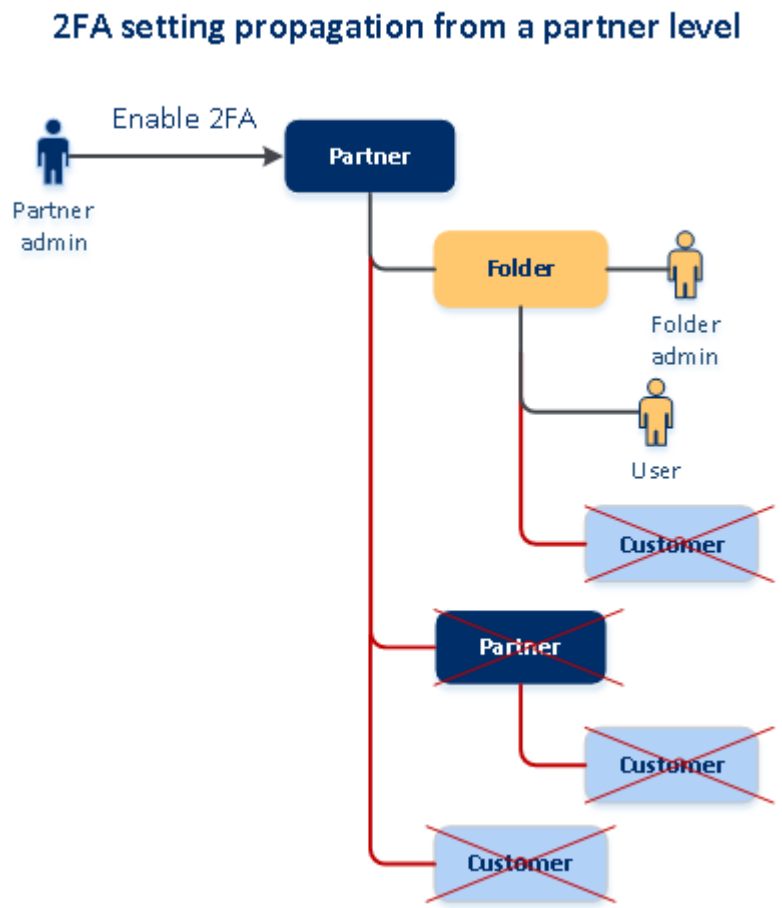
租户级别的双重身份验证设置传播

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：

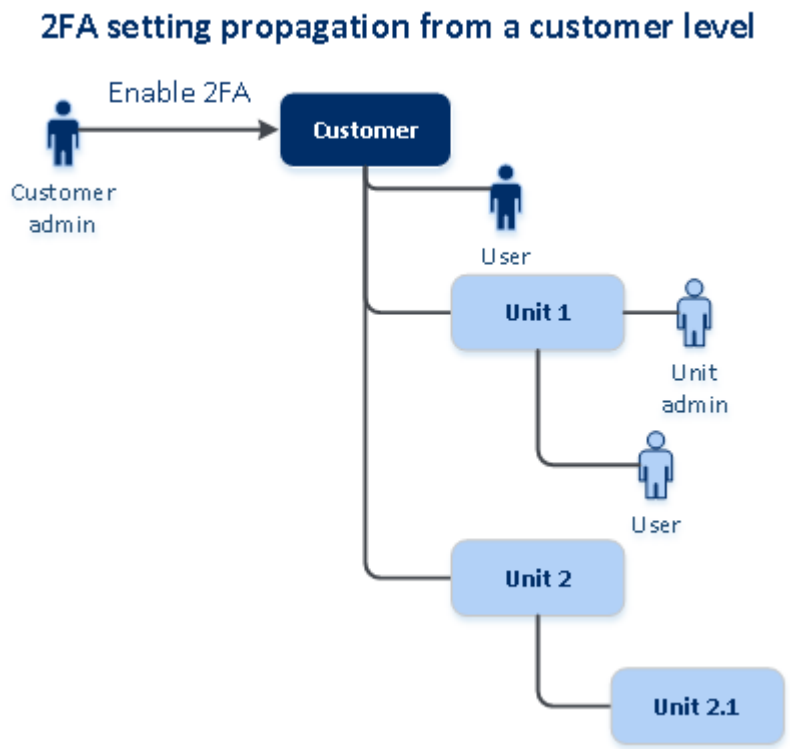
- 为您自己的组织。
- 为您的子租户(仅在该子租户中启用**支持访问**选项时)。

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

作为管理员,可以为贵组织启用双重身份验证。

为租户启用双重身份验证

1. 在管理门户中,转到**设置** > **安全**。
2. 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**公司管理** > **用户**选项卡,然后检查**双重身份验证状态**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。

禁用租户的双重身份验证

1. 在管理门户中,转到**设置** > **安全**。
2. 要禁用双重身份验证,请关闭开关,然后单击**禁用**。
3. [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。

结果,系统会为您的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**公司管理** > **用户**选项卡上,将隐藏**双重身份验证状态**列。

管理用户的双重身份验证

可以在管理门户的**公司管理** > **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**公司管理** > **用户**下,可以查看组织中所有用户的列表。**双重身份验证状态**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**公司管理** > **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**公司管理** > **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**公司管理** > **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**公司管理** > **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。

Cyber Protection 有多个旧版本，所有这些版本在功能和价格方面都不尽相同。您可能想要为使用基本版本的现有客户推销更昂贵的版本(具有更高级功能)。

可以启用或禁用每个客户的追加销售功能。默认情况下，追加销售选项处于禁用状态。如果为客户启用追加销售，那么客户会看到他们在购买推销版本后才可用的额外功能。此额外功能标有标签，

这些标签显示推销版本的名称或图标并全部以橙色亮显。这些追加销售点将向客户显示，以鼓动他们购买更昂贵的版本。在单击这些追加销售点时，客户会看到一个对话框，其中建议他们购买更昂贵的版本来启用所需功能。

操作项取决于客户用户的类型。可以使用平台 API 配置用户类型(买方或非买方)；有关详细信息，请参阅 API 文档。有关向客户显示的操作项的详细信息，请参阅下表：

客户租户中的用户类型	操作项
管理员；买方	**立即购买**按钮显示在用户界面中。*
管理员；非买方	消息“请与您的合作伙伴联系以升级版本”显示在用户界面中。
用户；买方	消息“请与您的合作伙伴联系以升级版本”显示在用户界面中。
用户；非买方	消息“请与您的合作伙伴联系以升级版本”显示在用户界面中。

* 可以在**设置** > **品牌**中配置**立即购买**按钮的链接，该链接会将客户重定向到网站以购买更高级版本。在**追加销售**部分中，可以指定**购买 URL**。品牌设置将应用于租户(品牌配置于其中)的所有直接和间接子合作伙伴/文件夹和客户。

为客户启用或禁用追加销售功能

1. 在管理门户中，转到**客户端**。
2. 选择客户、转到右窗格，然后单击**配置**选项卡。
3. 在**追加销售**部分中，执行以下操作：
   - 启用**推销更多高级版**，以为客户打开追加销售方案。
   - 禁用**推销更多高级版**，以为客户关闭追加销售方案。

向客户显示的追加销售点

漏洞列表

在服务中控台中，可以在**软件管理** > **漏洞**中找到漏洞列表。当用户单击针迹图标时，将打开版本推销对话框，提示用户购买更昂贵的版本。

创建或编辑保护计划

在服务中控台中，可以在**计划** > **保护**中找到此内容。单击**创建计划**。Cyber Backup 版本仅启用了**备份**和**漏洞**模块；其余模块仅在 Cyber Protect 版本中可用。客户可以在购买 Cyber Protect 版本之一后启用所有模块。

自动发现向导

在服务中控台中，可以在**设备** > **所有设备**中找到该向导。客户应通过以下方法来启动“自动发现”向导：单击**添加**、转到**多个设备**部分，然后单击**仅限 Windows**。计算机自动发现方法仅在高级版中可用。

设备列表中的操作

在服务中控台中，可以在**设备** > **所有设备**中找到该列表。客户应选择相应计算机，然后两个附加选项将显示在左窗格中：

- **通过 HTML5 客户端连接**
- **修补**

仅当客户购买的版本比现有版本更昂贵时，这些选项才可用。

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。

有关使用存储进行的操作的更多信息，请参阅"管理存储"。

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。

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。

如果存储已指定给任何客户租户，则在删除该存储之前，必须禁用将该存储用于所有客户租户的服务。

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。

配置不可变存储

可以在合作伙伴级别和客户级别配置不可变存储。

对于合作伙伴租户，无法选择不可变存储模式。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。

对于客户租户，不可变存储在以下模式下可用：

- **监管模式**
  在此模式下，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。
- **合规模式**
  选择此模式后，无法禁用不可变存储，也无法再更改其模式或保留期。

当没有自定义设置应用到子租户时，子租户会继承父租户的设置。

只有为管理员帐户所属的租户启用了双重身份验证，才能配置不可变存储设置。

不可变存储中已删除的备份仍会使用存储空间并相应收费。

注意
从 21.12 版开始，默认会为新合作伙伴租户启用保留期为 14 天的不可变存储。对于现有租户，需要手动启用不可变存储。

为合作伙伴租户启用不可变存储

1. 以管理员身份登录到管理门户，然后转到**设置** > **安全**。
2. 启用**不可变存储**开关。
3. 在 14 天到 999 天的范围内指定保留期。
   默认的保留期为 14 天。较长的保留期可能会导致存储使用量增加。
4. 单击**保存**。

为合作伙伴租户禁用不可变存储

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。

   警告！
   此更改将由所有不使用不可变存储的自定义设置的子租户继承。将永久删除所有已删除的备份。删除新备份也将是永久删除。

3. 单击**禁用**来确认选择。

为客户租户启用不可变存储

1. 以管理员身份登录到管理门户，然后转到**客户**。
2. 要编辑客户租户的设置，请单击其名称。
3. 在导航菜单中，转到**设置** > **安全**。
4. 启用**不可变存储**开关。
5. 在 14 天到 999 天的范围内指定保留期。
   默认的保留期为 14 天。较长的保留期可能会导致存储使用量增加。
6. 选择不可变存储模式。

   警告！
   选择**合规模式**是不可逆的。再也无法禁用不可变存储，也无法更改其模式或保留期。

7. 单击**保存**。

为客户租户禁用不可变存储

1. 以管理员身份登录到管理门户，然后转到**客户**。
2. 要编辑客户租户的设置，请单击其名称。
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！
   如果禁用不可变存储，则将永久擦除所有删除的备份。删除新备份也将是永久删除。

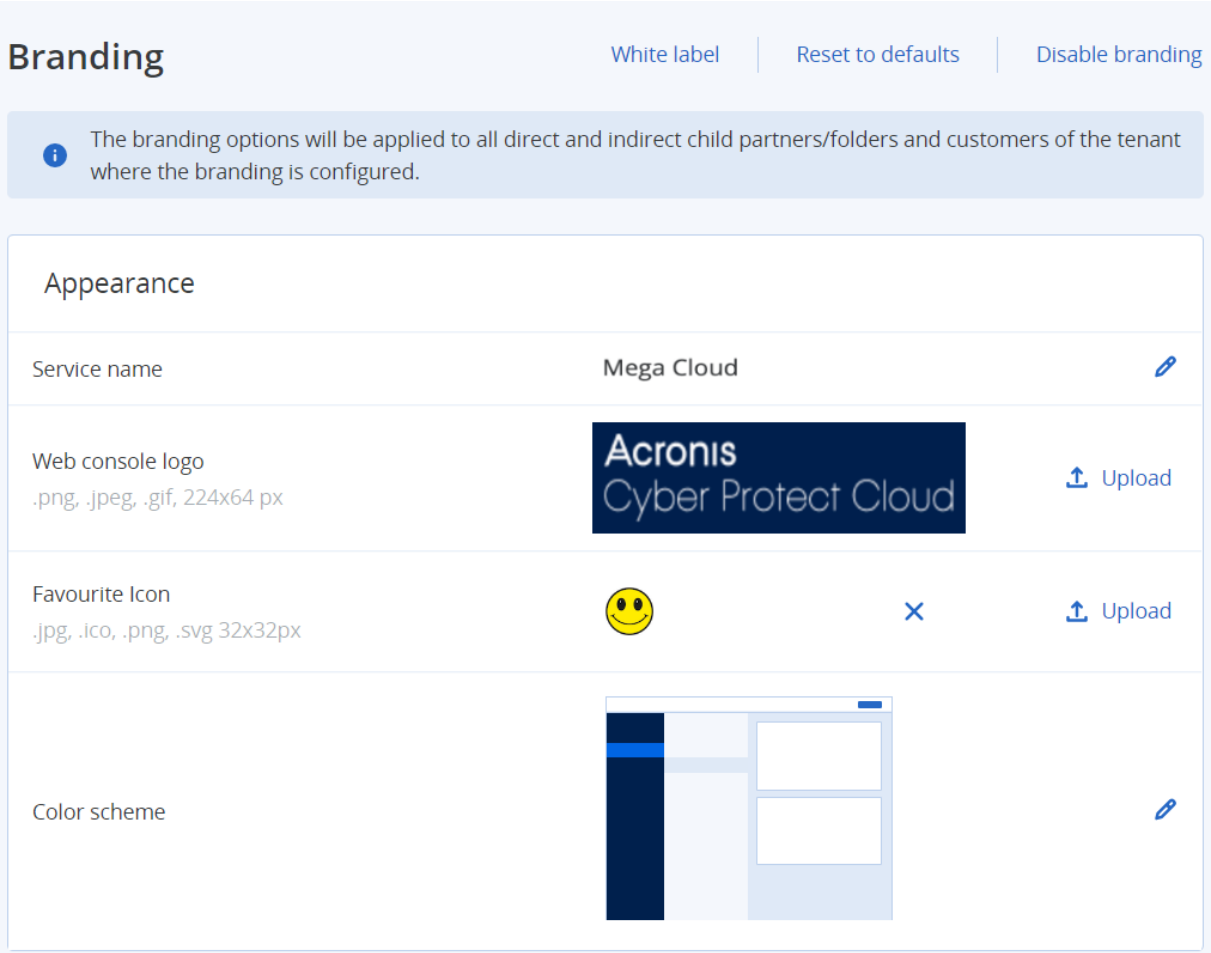
5. 单击**禁用**来确认选择。

限制

- 不可变存储适用于使用 Acronis Cyber Infrastructure 4.7.1 或更高版本的 Acronis 托管和合作伙伴托管的存储。
  不可变存储要求为 Acronis Cyber Infrastructure 中的 Backup Gateway 服务打开 TCP 端口 40440。在 4.7.1 及更高版本中，TCP 端口 40440 会为**备份 (ABGW) 公共**流量类型自动打开。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。

配置品牌和白标

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



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 服务中依次单击**添加** > **iOS** 时，将打开此页面。
- **Google Play**。当用户在 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）和 Cyber Protection 监视器（适用于 Windows、macOS 和 Linux）进行品牌化或白标。如果启用白标，将对代理程序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 监视器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。

   要找到您数据中心的域名并请求配置您的 CNAME 记录，请参阅品牌 Web 中控台 URL (58275) 一文。
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。

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)。

自动更新代理程序

Cyber Protect 有三类代理程序可以安装在受保护的计算机上：适用于 Windows 的代理程序、适用于 Linux 的代理程序和适用于 Mac 的代理程序。

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。

为了便于管理多个工作负载，可以为所有计算机上的所有代理程序配置(和禁用)无人值守的自动更新。

重要事项
当前，仅已启用 保护 的合作伙伴和客户有权访问代理程序更新管理功能。

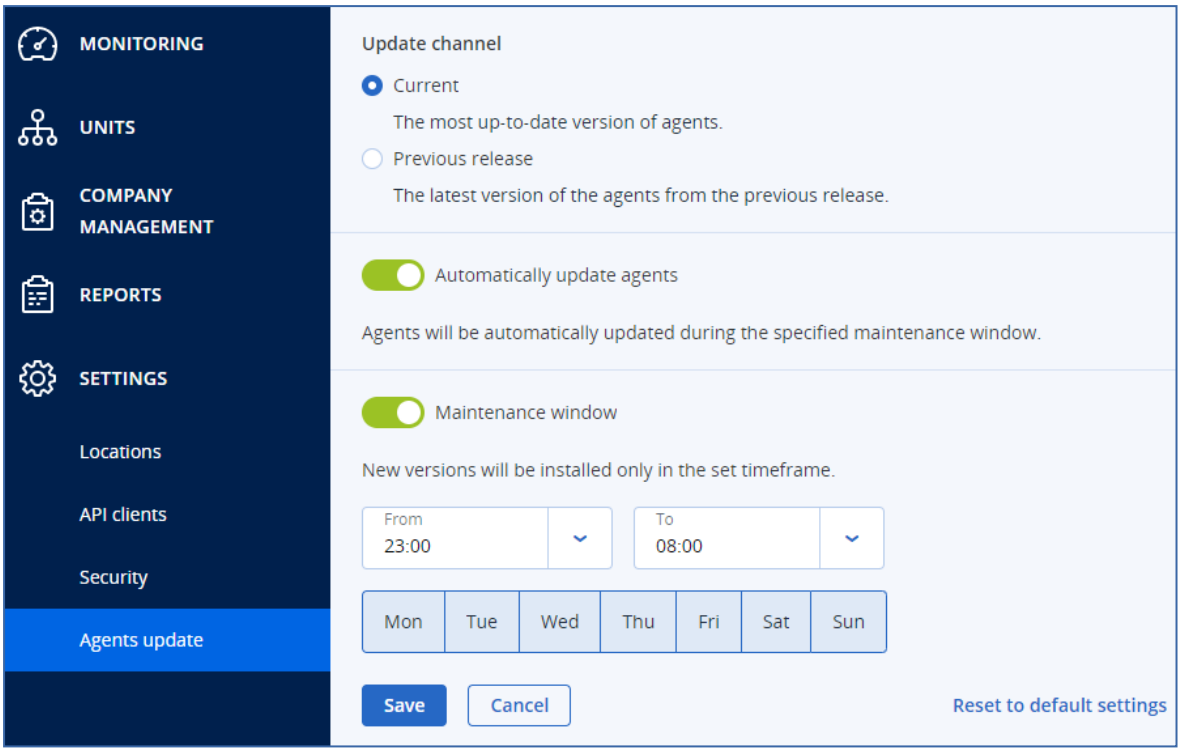
注意
要管理个别计算机上的代理程序并自定义自动更新设置，请参阅更新代理程序上的 Cyber Protect 用户指南部分。

自动更新代理程序

注意
自动更新适用于 File Sync & Share 的代理程序的设置由未启用保护的合作伙伴和客户继承。

从管理门户的初始页面设置代理程序的自动更新

1. 选择**设置 > 代理程序更新**。



2. 选择要检测自动更新的版本:**当前**或**以前版本**。
   (默认为**当前**。)
3. 打开**自动更新代理程序**。
   (默认为**打开**。)
4. 设置维护时间范围。
   (默认为 23:00 至 08:00。)

注意
尽管代理程序更新过程旨在快速无缝,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. [可选] 选择要执行自动更新的特定日期。
6. 选择**保存**。

注意
自动更新仅适用于:

- Cyber Protect 代理程序版本 15.0.26986(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。

监视代理程序更新

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。

要监视代理程序更新，请参阅 Cyber Protect 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**监视**。

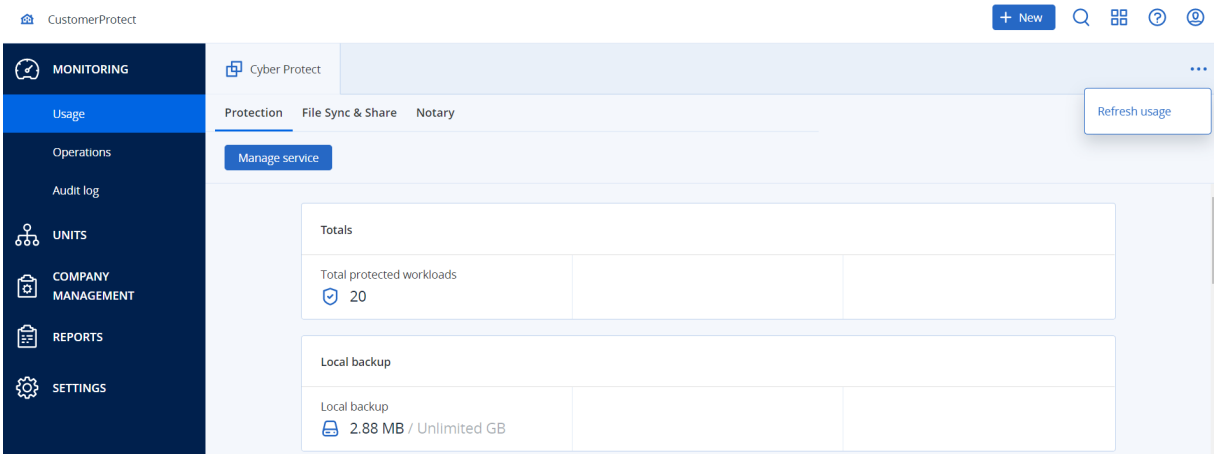
使用情况

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。

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，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。



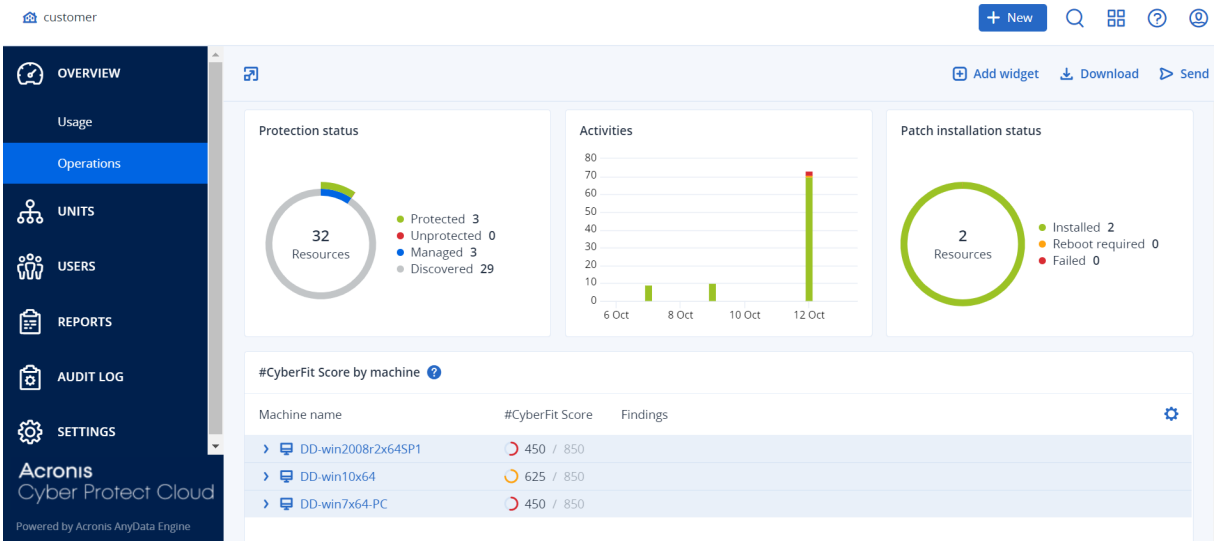
操作

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

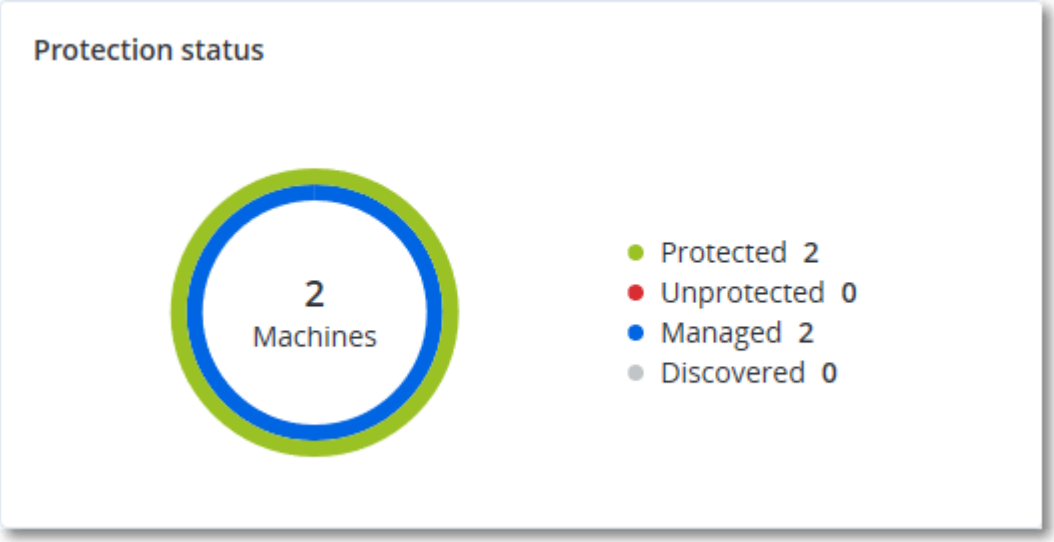
该小部件显示所有计算机的当前保护状态。

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。



发现的计算机

该小部件显示在指定时间范围内发现的计算机列表。

Discovered machines

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

#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 ...

端点检测和响应 (EDR) 小组件

重要事项
这是抢先体验版的 EDR 文档。某些功能和描述可能并不完整。

终端检测和响应 (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

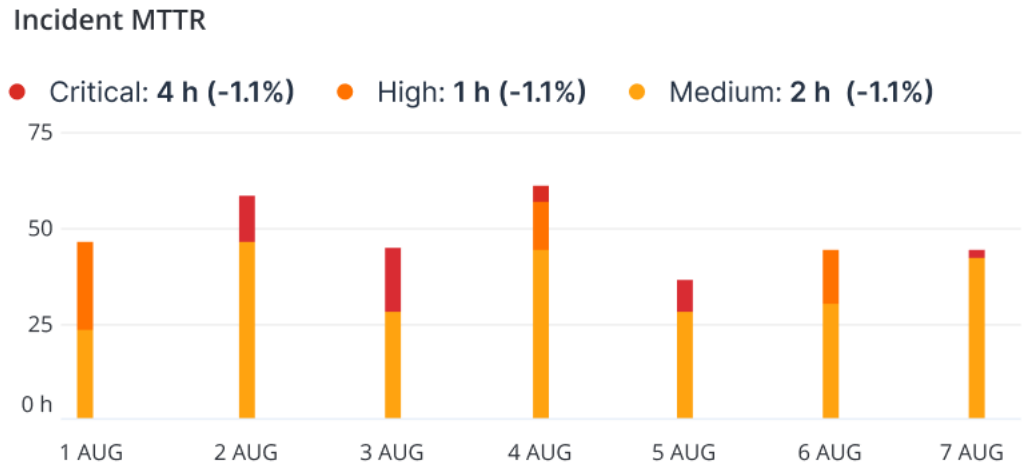
此小组件显示具有最多事件的前五个工作负载(单击**全部显示**以重定向到事件列表，这可根据小组件设置进行过滤)。

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。

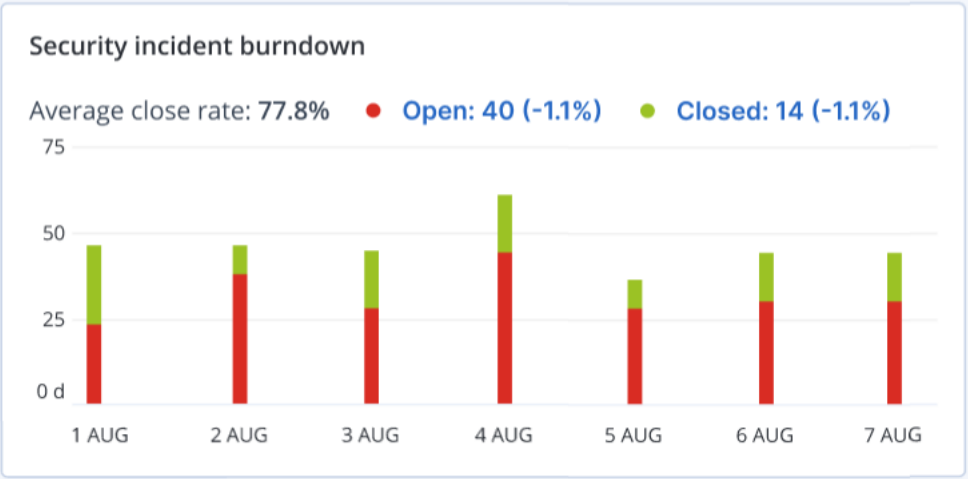


安全性事件刻录

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)。

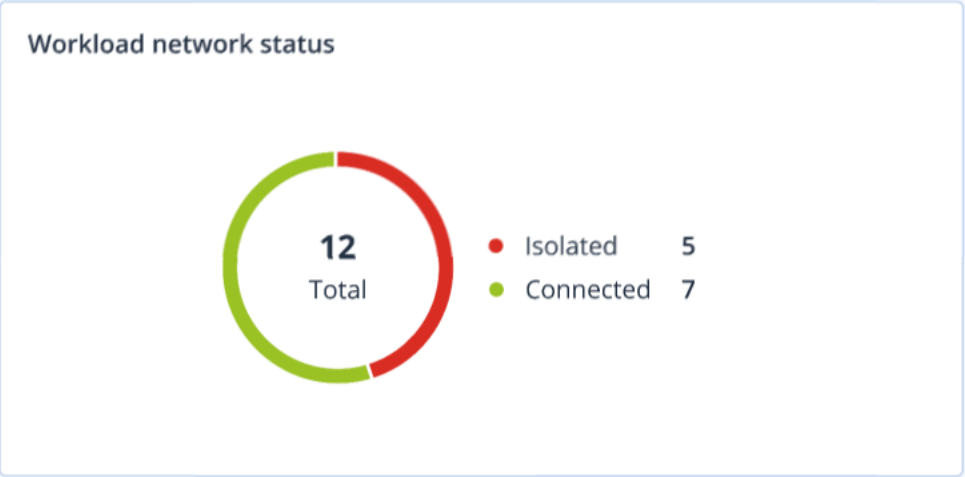
在括号中显示的 % 值表示与以前时间段比较的上升或下降。



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。

- 在 NVMe 驱动器上，仅对于通过 Windows API 传输 SMART 数据的驱动器支持磁盘运行状况监控。对于需要直接从驱动器读取 SMART 数据的 NVMe 驱动器，磁盘运行状况监控不受支持。

磁盘运行状况可以表示为以下状态之一：

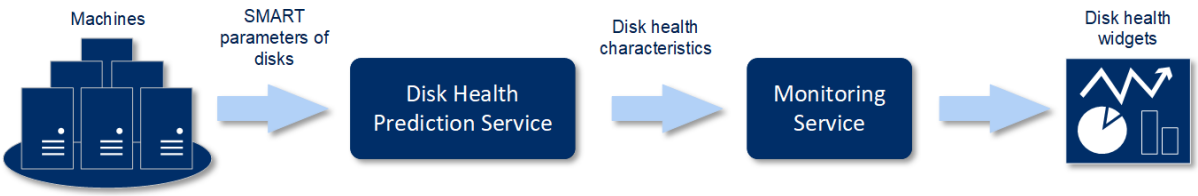
- **正常**
  磁盘运行状况为 70% 和 100% 之间。
- **警告**
  磁盘运行状况为 30% 和 70% 之间。
- **严重**
  磁盘运行状况为 0% 和 30% 之间。
- **计算磁盘数据**
  正在计算当前磁盘状态和预测。

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. 监视服务接收这些特征，然后在服务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

磁盘运行状况监控的结果显示在服务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

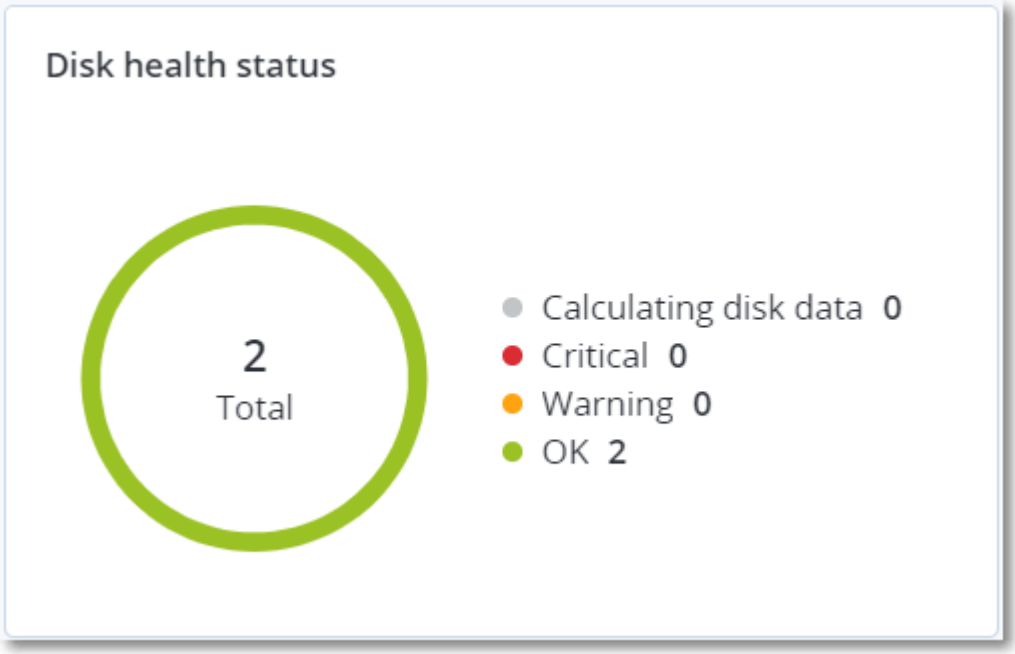
    显示有关每个选定客户计算机的磁盘运行状况状态的概要信息。仅显示最严重的磁盘状态。将光标悬停在特定块上时，其他状态会显示在工具提示中。计算机块的大小取决于该计算机所有磁盘的总大小。计算机块的颜色取决于找到的最严重磁盘状态。

  - 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	说明
磁盘可能发生故障	警告	(30 – 70)	此计算机上的 <磁盘名称> 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	重大	(0 – 30)	此计算机上的 <磁盘名称> 磁盘处于严重状态，很可能即将发生故障。目前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。

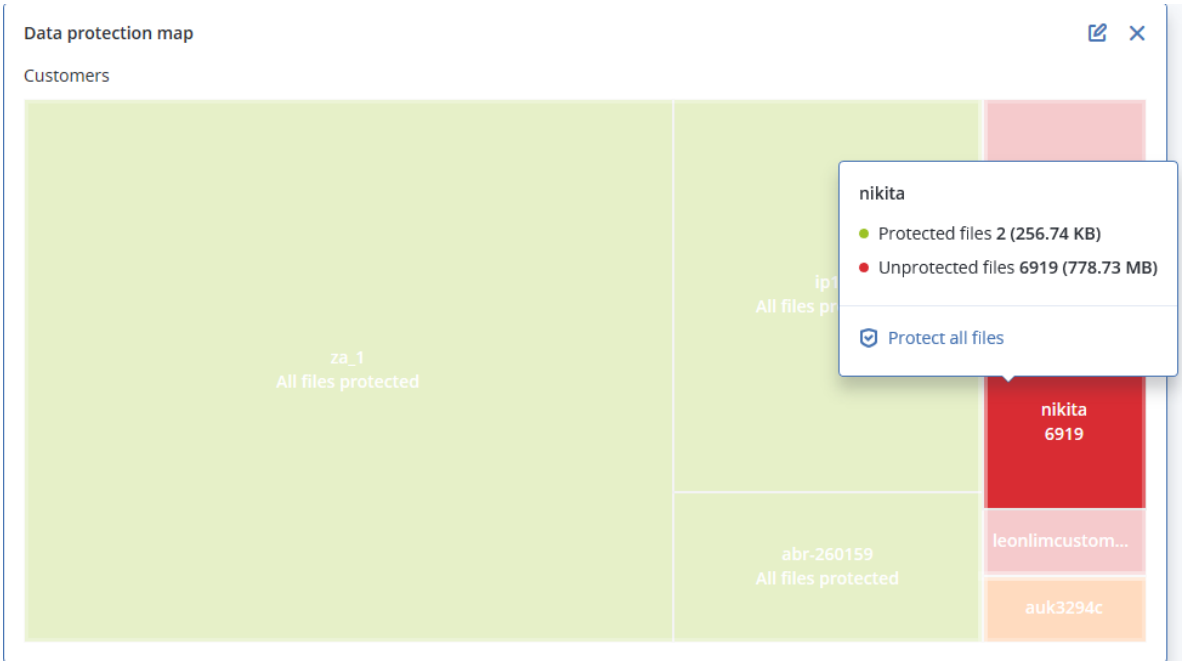
每个块的大小取决于属于客户/计算机的所有重要文件的总数/大小。

文件可以具有以下保护状态之一：

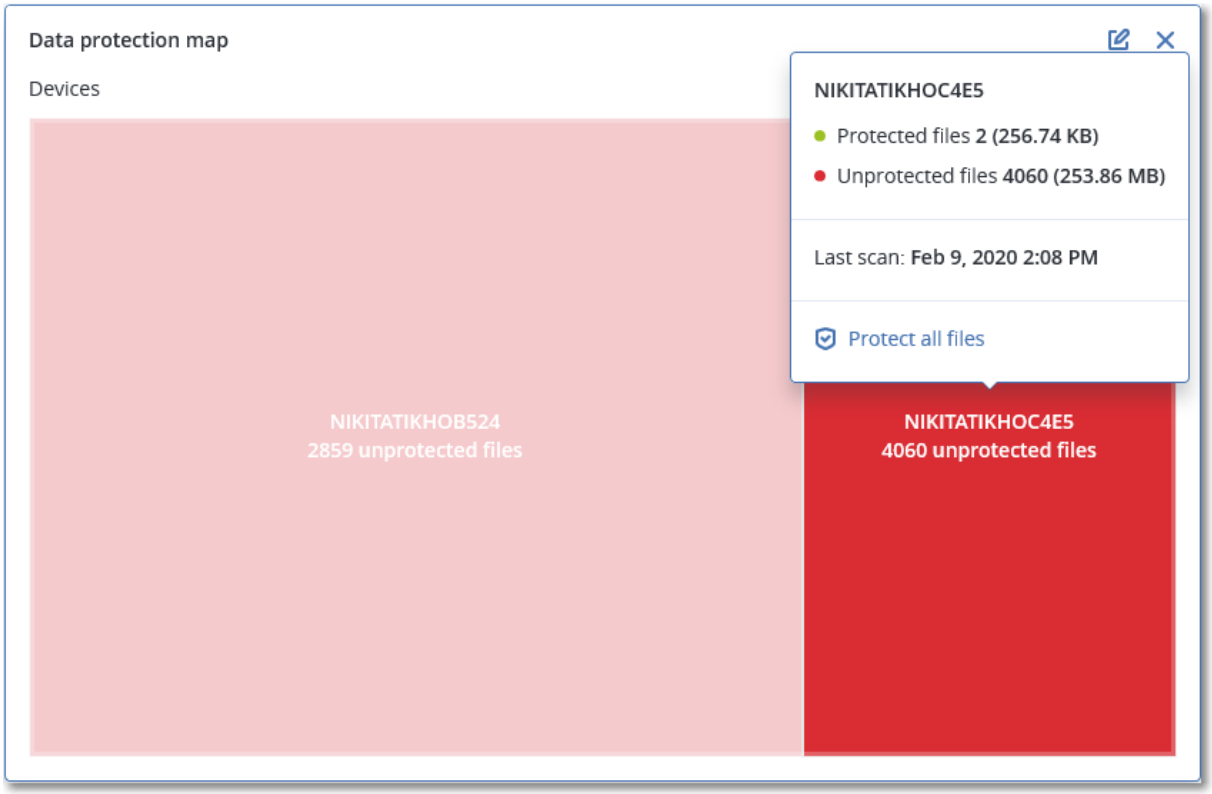
- **严重** - 有 51-100% 的不受保护文件（具有您指定的扩展名）未针对选定客户租户/计算机/位置进行备份。
- **低** - 有 21-50% 的不受保护文件（具有您指定的扩展名）未针对选定客户租户/计算机/位置进行备份。
- **中** - 有 1-20% 的不受保护文件（具有您指定的扩展名）未针对选定客户租户/计算机/位置进行备份。
- **高** - 所有具有您指定扩展名的文件都已针对选定客户租户/计算机/位置进行了保护（备份）。

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。

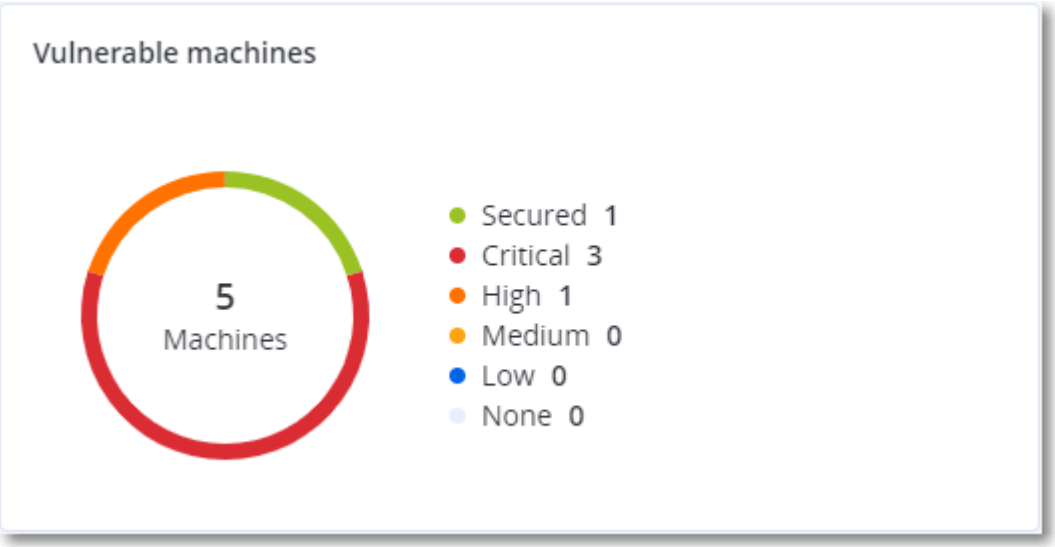
漏洞评估小部件

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

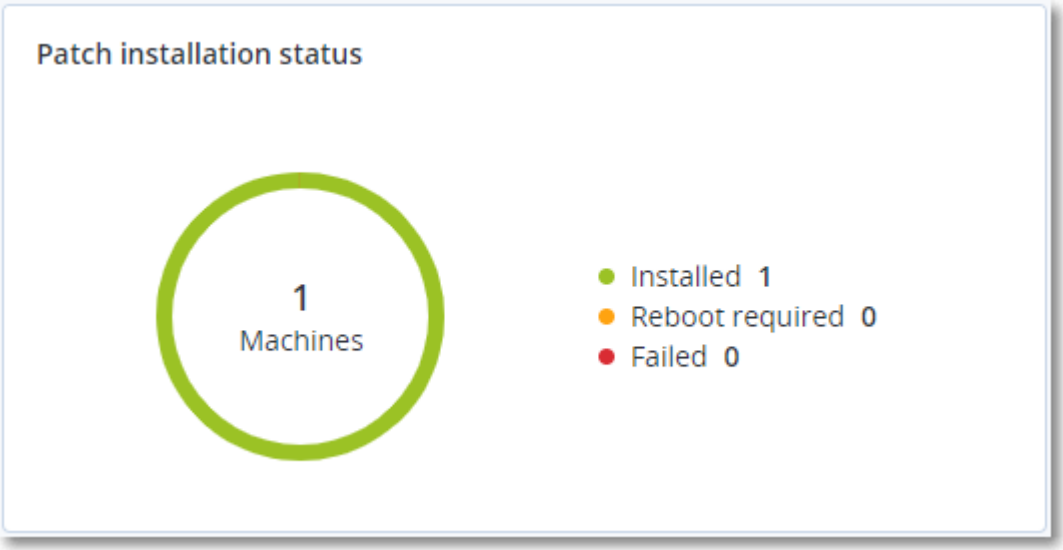
修补程序安装小部件

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

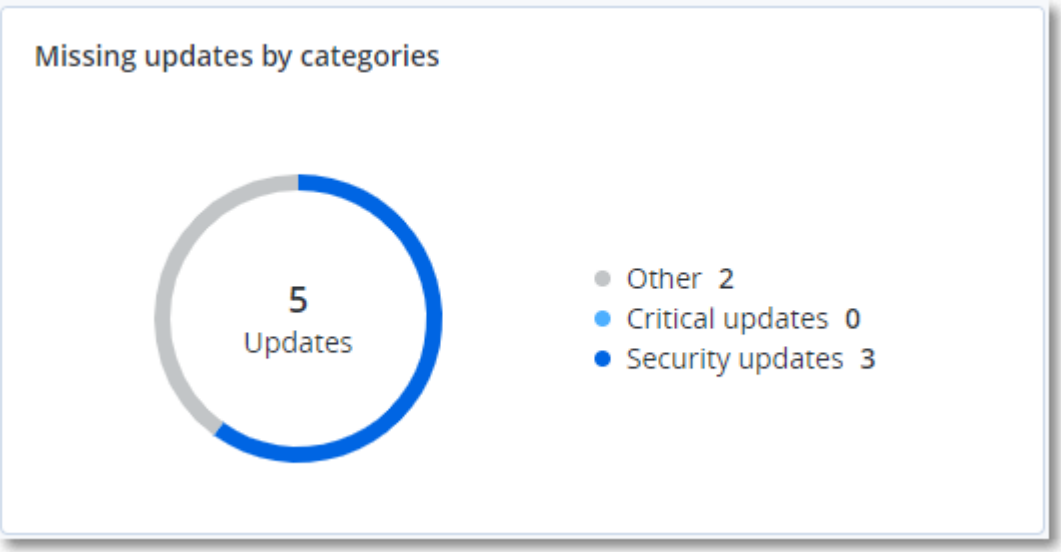
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical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

Backup scanning details (threats)

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

More

最近受影响

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。

Recently affected

Machine name	Protection plan	Threat	Affected files	Detection time
Ubuntu_14.04_x64-1	Total protection	Adware.DealPly!gen2	15	27.12.2
Ubuntu_14.04_x64-1	Protection plan	Bloodhound.MalMacro!g1	274	27.12.2
dc_w2k12_r2	Protection plan	Backdoor:Win32/Caphaw...	13	27.12.2
Win2012_r2-Hyper-V	Protection plan	W97M.Downloader!g32	5	27.12.2
HyperV_for12A	Total protection	Miner.XMRig!gen1	68	27.12.2
vm-sql_2012	Total protection	Backdoor:Win32/Caphaw...	61	27.12.2
vm-sql_2012	Protection plan	Adware.DealPly!gen2	9	27.12.2
MF_2012_R2	Total protection	MSH.Downloader!gen8	73	27.12.2
MF_2012_R2	Total protection	Bloodhound.MalMacro!g1	182	27.12.2
MF_2012_R2	Protection plan	Bloodhound.MalMacro!g1	18	27.12.2
ESXirestore	Protection plan	MSH.Downloader!gen8	682	27.12.2017 11:23 AM
MF_2012_R2	Protection plan	Miner.XMRig!gen1	13	27.12.2017 11:23 AM
Ubuntu_14.04_x64-1	Total protection	Adware.DealPly!gen2	3	27.12.2017 11:23 AM
Win2012_r2-Hyper-V	Total protection	W97M.Downloader!g32	27	27.12.2017 11:23 AM

More | Show all 556

- Folder
- Customer
- ✓ Machine name
- ✓ Protection plan
- Detected by
- ✓ Threat
- File name
- File path
- ✓ Affected files
- ✓ Detection time

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。

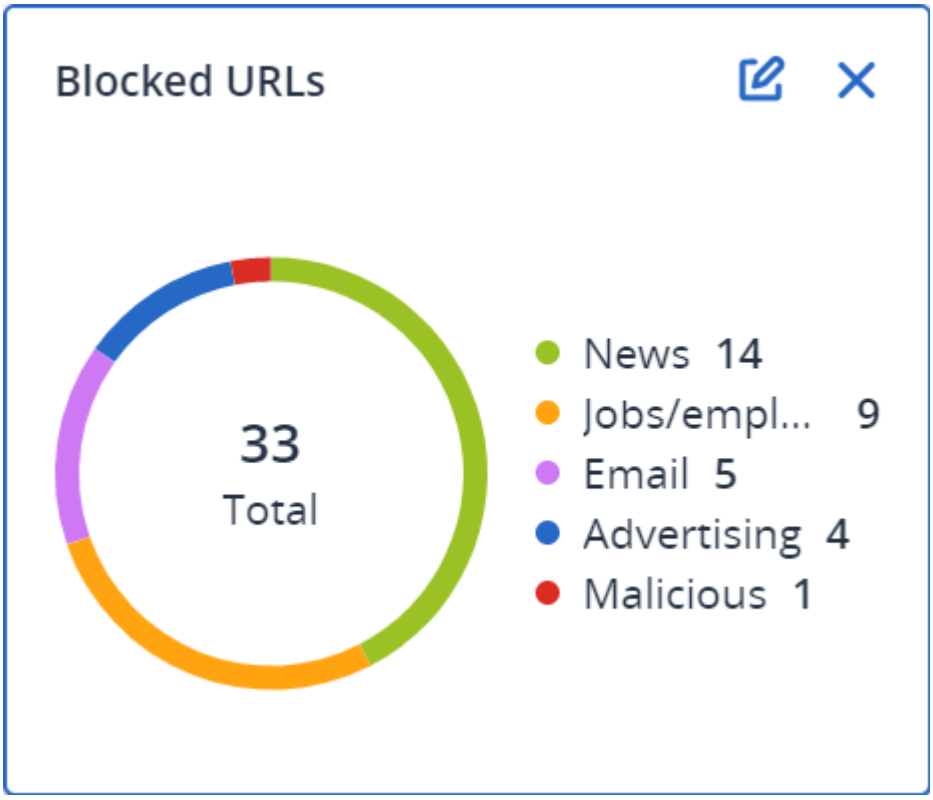
下载最近受影响工作负载的数据

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

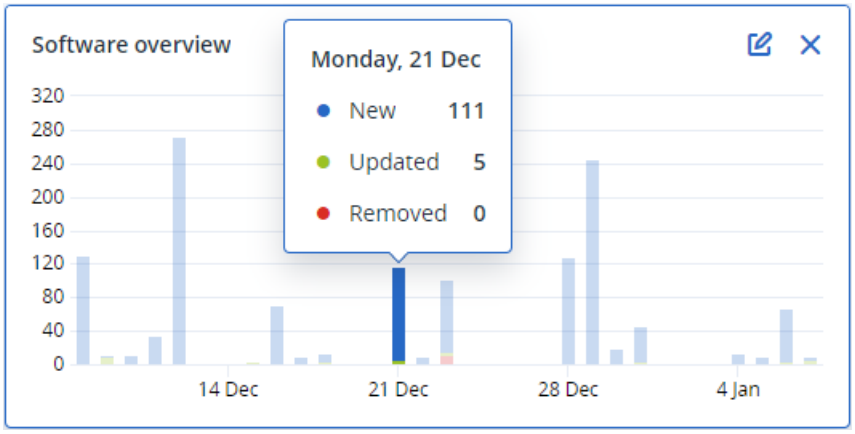
软件清查表小组件会显示有关客户组织中 Windows 和 macOS 设备上安装的所有软件的详细信息。

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。

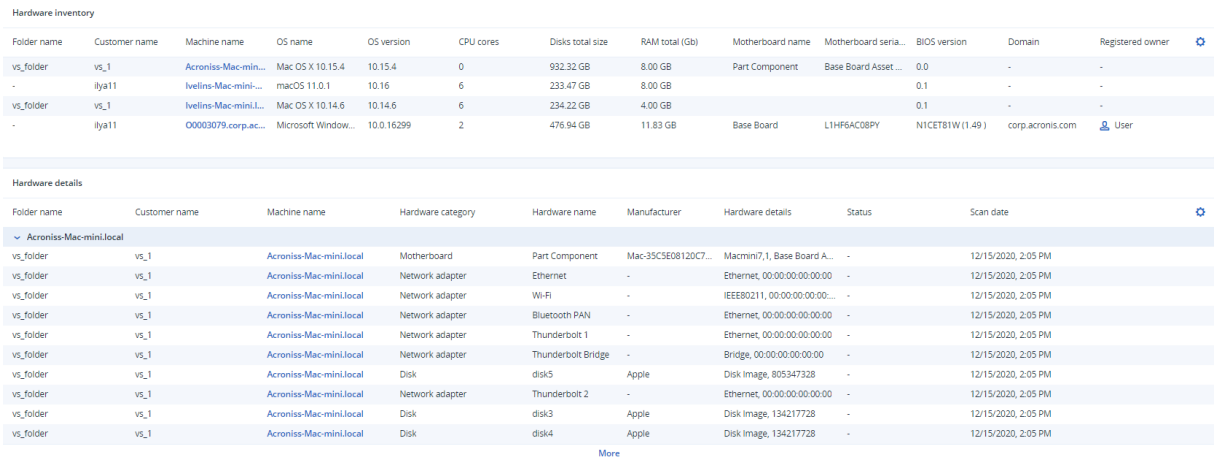
已更新 - 已更新应用程序的数量。

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服务中控台中的**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。



Hardware inventory

Folder name	Customer name	Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner
vs_folder	vs_1	Acroniss-Mac-min...	Mac OS X 10.15.4	10.15.4	0	932.32 GB	8.00 GB	Part Component	Base Board Asset ...	0.0	-	-
-	ilya11	Ivelins-Mac-mini-...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-
vs_folder	vs_1	Ivelins-Mac-mini.l...	Mac OS X 10.14.6	10.14.6	6	234.22 GB	4.00 GB			0.1	-	-
-	ilya11	O0003079.corp.ac...	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User

Hardware details

Folder name	Customer name	Machine name	Hardware category	Hardware name	Manufacturer	Hardware details	Status	Scan date
Acroniss-Mac-mini.local								
vs_folder	vs_1	Acroniss-Mac-mini.local	Motherboard	Part Component	Mac-35C5E08120C7...	Macmini7,1, Base Board A...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Ethernet	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Wi-Fi	-	IEEE80211, 00:00:00:00:00:...	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Bluetooth PAN	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 1	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt Bridge	-	Bridge, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk5	Apple	Disk Image, 805347328	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Network adapter	Thunderbolt 2	-	Ethernet, 00:00:00:00:00:00	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk3	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM
vs_folder	vs_1	Acroniss-Mac-mini.local	Disk	disk4	Apple	Disk Image, 134217728	-	12/15/2020, 2:05 PM

More

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

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

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。

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。
- **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。

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

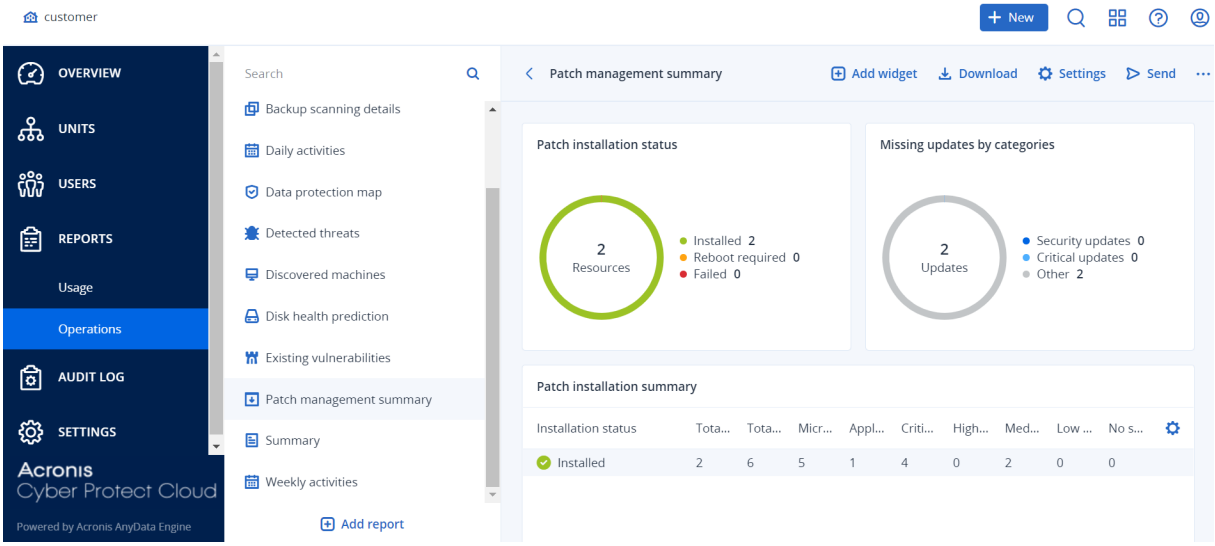
关于操作的报告可以包括任何一组**操作**仪表板小部件。默认情况下，所有小组件都会显示您正在其中进行操作的租户的概要信息。可以通过编辑小部件来为每个小组件或报告设置中的所有小部件分别更改租户。

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 99 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。

可以下载有关操作的报告，也可以通过电子邮件以 Excel (XLSX) 或 PDF 格式发送该报告。



默认报告如下所示：

报告名称	说明
#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。
发现的计算机	显示在组织网络中发现的所有计算机。
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。

要查看报告，请单击其名称。

要通过报告访问操作，请单击报告行上的垂直省略号图标。可从报告中访问相同的操作。

添加报告

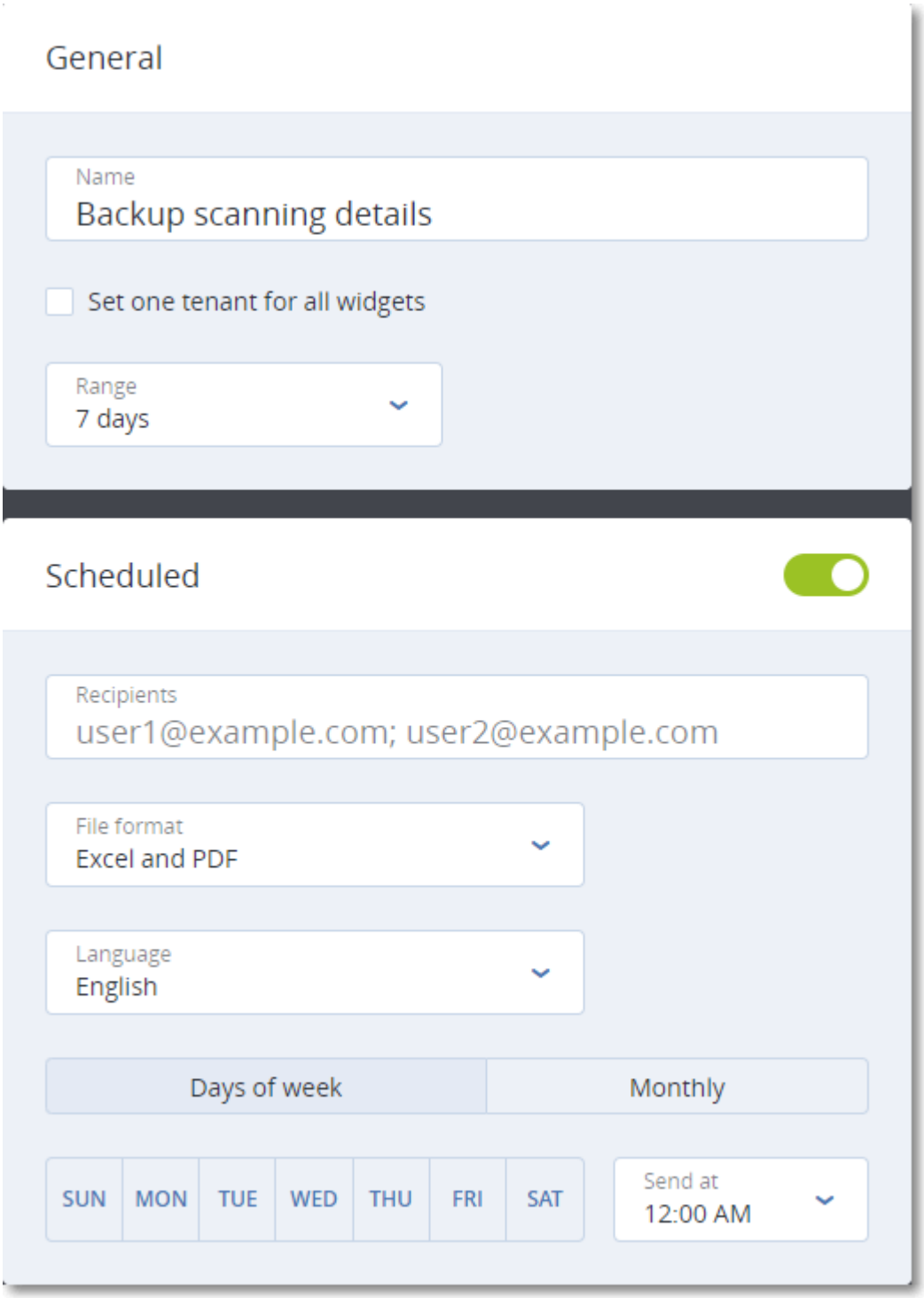
1. 单击**添加报告**。
2. 请执行以下任一操作：
   - 要添加预定义的报告，请单击其名称。
   - 要添加自定义报告，请单击**自定义**，单击报告名称（默认分配的名称，如 **自定义(1)**），然后将小部件添加到报告。
3. [可选] 拖放小部件即可重新排列它们。
4. [可选] 按照下面的描述编辑报告。

编辑报告设置

要编辑报告，请单击其名称，然后单击**设置**。编辑报告时，您可以：

- 重命名报告
- 为报告中包含的所有小部件更改显示的租户

  如果您有子租户，那么**为所有小组件设置一个租户**选项将可供您使用。通过此选项，可以按选定租户过滤报告的所有小组件中的数据。如果未选择此选项，那么小组件将显示当前租户的所有子租户的数据。
- 为报告中包含的所有小部件更改时间范围
- 预定通过电子邮件以 PDF 或/和 Excel 格式发送报告。



预定报告

1. 单击报告名称，然后单击**设置**。
2. 启用**预定**开关。
3. 指定收件人的电子邮件地址。
4. 选择报告格式：PDF、Excel 或两者。

5. 选择发送报告的日期和时间。
6. 单击右上角的**保存**。

导出和导入报告结构

可以将报告结构(一组小组件和报告设置)导出和导入到一个 JSON 文件。这对将报告结构从一个租户复制到另一个租户可能很有用。

要导出报告结构,请单击报告名称、单击右上角的垂直省略号图标,然后单击**导出**。

要导入报告结构,请单击**添加报告**,然后单击**导入**。

下载报告

可以下载报告,单击**下载**,然后选择所需格式:

- Excel 和 PDF
- Excel
- PDF

转储报告数据

可以通过电子邮件发送 CSV 文件中的报告数据转储。转储包括自定义时间范围内的所有报告数据(未筛选)。CSV 报告中的时间戳为 UTC 格式,而 Excel 和 PDF 报告中的时间戳为当前系统时区。

软件随时生成数据转储。如果您指定一长段时间,则此操作可能需要很长时间。

转储报告数据

1. 单击报告名称。
2. 单击右上角的垂直省略号图标,然后单击**转储数据**。
3. 指定收件人的电子邮件地址。
4. 在**时间范围**中,指定时间范围。
5. 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、灾难恢复,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	说明
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 • 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	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。

小部件	说明
安全保护摘要	**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** - 受灾难恢复保护的服务器总数。 **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**。
云工作负载保护状态	**云工作负载保护状态** 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

小部件	说明
	• 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 • 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。

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	说明
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	说明
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 • 漏洞防御 • 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	说明
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	说明
	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	说明
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)。

灾难恢复小组件

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	说明
灾难恢复统计信息	小组件显示指定日期范围内的灾难恢复关键性能指标。 **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)。

小部件	说明
	已使用的总计算点 - 指定时间范围内使用的计算点的总数。
灾难恢复服务器已测试	小组件显示有关受灾难恢复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** - 在报告生成时受灾难恢复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** - 在所有受灾难恢复保护的服务器中,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灾难恢复保护的服务器数。 **未测试** - 在所有受灾难恢复保护的服务器中,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灾难恢复保护的服务器数。 小组件还显示在报告生成时,灾难恢复存储(以 GB 为单位)的大小。它是云服务器的备份大小的总和。
受灾难恢复保护的服务器	小组件显示有关受灾难恢复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,受灾难恢复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	说明
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	说明
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	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

小部件	说明
文档	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 96 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 > 概述 > 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 > 概述 > 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	• 报告生成的时间是浏览器运行时所在计算机的时区。

(小部件)	• 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 > 活动警告的每日概述	• 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
发现的计算机	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

审核日志

若要查看审核日志，请单击**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
- 在 Cyber Protection 服务中控台中由用户执行的使用云到云资源进行的操作
- 用户在 Cyber Protection 服务中控台中执行的网络脚本操作
- 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。

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”。

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

可以启用以下高级保护包：

- 高级备份
- 高级管理
- 高级安全性
- 高级安全性 + EDR
- 高级数据丢失防护
- 高级灾难恢复
- 高级电子邮件安全性
- 高级 File Sync & Share

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，则用户无法使用高级备份包的功能。

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。功能名称旁边会显示以下图标。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
安全	• #CyberFit Score • 漏洞评估 • 反勒索软件保护：Active Protection • 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。	There are two available advanced protection packs:**Advanced Security** and **Advanced Security + EDR**. 高级安全性包包括： • 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) • 漏洞防御 • 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 “高级安全 + EDR”保护包包括所有上述功能，以及用于识别高级威胁或正在进行的攻击的以下端点检测和响应功能： • 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 有关启用“高级安全 + EDR”的信息，请参阅 "启用“高级安全 + EDR”"(第 107 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 • 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

功能组	包含的标准功能	高级功能
管理	• 工作负载的组管理 • 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	• 修补程序管理 • 磁盘运行状况 • 软件库存记录 • 文件安全修补 • 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、观察和隔离 • 通过“Quick Assist”应用程序连接 • 远程连接协议：NEAR 和屏幕共享 • NEAR 连接的会话记录 • 屏幕截图传输 • 会话历史记录报告
电子邮件安全	无	为您的 Microsoft 365 和 Gmail 邮箱提供实时保护： • 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。
Cyber Disaster Recovery Cloud	可以使用灾难恢复标准功能来为您的工作负载测试灾难恢复方案。 请注意可用的灾难恢复标准功能及其限制： • 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”。	可以启用高级灾难恢复包，并使用完整的灾难恢复功能保护工作负载。 请注意可用的灾难恢复高级功能： • 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。

功能组	包含的标准功能	高级功能
	• 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。	• 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。	• Microsoft SQL Server 和 Microsoft Exchange 群集 • Oracle 数据库 • SAP HANA • 数据保护示意图 • 连续数据保护 • 脱离主机数据处理计划 • 备份的公证 • Microsoft 365 席位 • Google Workspace 席位
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 7 页）。

高级数据丢失防护

高级数据丢失防护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。

在开始使用高级数据丢失防护模块之前，请确认您已阅读并理解基础指南中所述的高级数据丢失防护管理的基本概念和逻辑。

您可能还想要查看技术规范文档。

启用高级数据丢失防护

默认情况下，高级数据丢失防护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。

启用高级数据丢失防护

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**高级数据丢失防护**。
4. 在配置服务下，滚动到**高级数据丢失防护**，然后配置配额。
   默认情况下，配额设置为无限制。
5. 保存设置。

高级安全性 + EDR

端点检测和响应 (EDR) 会检测工作负载上的可疑活动(包括未注意到的攻击)，并生成事件。这些事件提供了每次攻击的分步概述，可帮助您了解攻击是如何发生的以及如何防止它再次发生。通过轻松了解攻击中每个阶段的说明，调查攻击所花费的时间可以减少到几分钟。

启用“高级安全 + EDR”

作为合作伙伴管理员，您可以启用“高级安全 + EDR”保护包，以在客户端保护计划中提供端点检测和响应 (EDR) 功能。

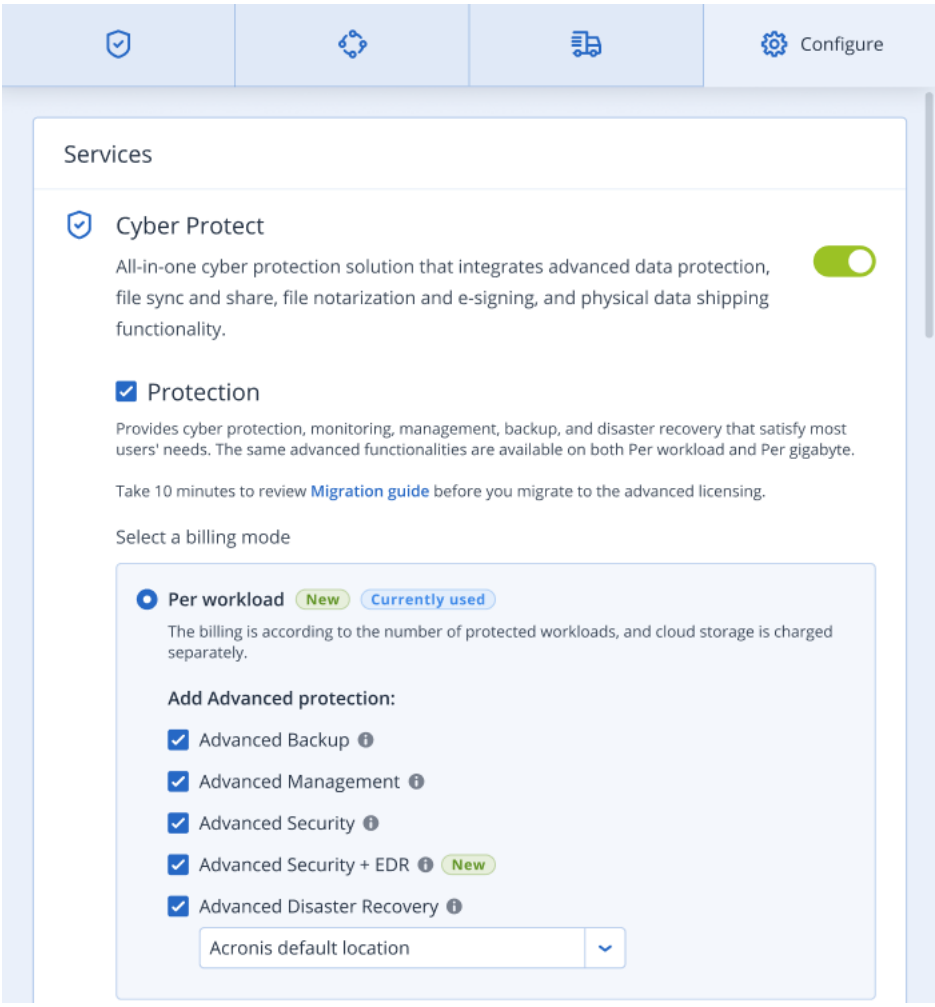
启用“高级安全 + EDR”包

1. 登录管理门户。

   注意
   如果出现提示，请选择要应用“高级安全 + EDR”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“网络安全保护”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“高级安全 + EDR”包的相关客户端。

在**配置**选项卡中的“保护”部分下，确保选中**高级安全 + EDR** 复选框。



高级灾难恢复

可以启用高级灾难恢复包，并使用完整的灾难恢复功能保护工作负载。

提供以下高级灾难恢复功能：

- 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。

高级电子邮件安全性

高级电子邮件安全包会为您的 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

在高级电子邮件安全产品彩页中，了解有关高级电子邮件安全的详细信息。

有关配置说明，请参阅带有感知点的高级电子邮件安全。

集成

与第三方系统的集成

服务提供商可以将 Cyber Protect Cloud 与第三方系统集成，如下所示：

- 通过在此系统中设置平台扩展。

  管理门户的**集成**页面中列出可用于最受欢迎的专业服务自动化 (PSA) 和远程监视与管理 (RMM) 系统的扩展。

  这是集成平台的建议方法。
- 通过为系统创建 API 客户端，从而使系统能够访问平台及其服务的应用程序编程接口 (API)。API 客户端是平台的 OAuth 2.0 授权框架的一部分。有关 OAuth 2.0 的详细信息，请参阅 https://tools.ietf.org/html/rfc6749。

  这是一种集成平台的底层方法，需要编程技能。建议您在以下情况下选择使用它：系统没有平台扩展，或者管理可用扩展未涵盖的平台及其服务的情况下自定义系统。

设置 Cyber Protect Cloud 的集成

1. 请登录管理门户。
2. 转到主导航菜单中的**集成**。
3. 单击要与之集成的第三方系统名称。
4. 按照屏幕上的说明操作。

有关与第三方系统的可用集成的详细信息（包括分步文档），请访问 https://solutions.acronis.com。

管理 API 客户端

第三方系统可以通过使用 Cyber Protect Cloud 的应用程序编程接口 (API) 来与其集成。可以通过 API 客户端（即平台的 OAuth 2.0 授权框架的组成部分）访问这些 API。

什么是 API 客户端？

API 客户端是一个特殊平台帐户，旨在表示需要验证并被授权访问平台及其服务的 API 中的数据的第三方系统。

客户端的访问仅限于租户（其中管理员创建客户端及其子租户）。

创建客户端时，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。

客户端凭据由唯一标识符 (ID) 和密码值组成。凭据不会过期，并且不能用于登录到管理门户或任何服务中控台。可以重置密码值。

无法为客户端启用双重身份验证。

典型集成过程

1. 管理员在第三方系统将管理的租户中创建 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。

   根据此流，在通过 API 访问租户及其服务之前，系统应先使用授权 API 将创建的客户端的凭据发送到平台。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。接着，系统必须将此标记添加到所有 API 请求。

   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，该标记会于两小时后过期。在此时间过后，所有带有过期标记的 API 请求都将失败，系统将需要从平台请求新的标记。

有关使用授权和平台 API 的详细信息，请参阅开发者指南，网址：https://developer.acronis.com/doc/account-management/v2/guide/index。

创建 API 客户端

1. 登录管理门户。
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 - 只可进行重置。

6. 单击**完成**。

重置 API 客户端的密码值

1. 登录管理门户。
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**下一步**确认您的决定。

   将生成一个新的密码值。客户端 ID 和数据中心 URL 不会改变。

   指派给该客户端的所有安全标记将立即过期，并且使用这些标记的 API 请求将失败。
6. 复制并保存客户端的新密码值。

   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 - 只可进行重置。

7. 单击**完成**。

禁用 API 客户端

1. 登录管理门户。
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。

   客户端的状态将更改为**已禁用**。

   使用指派给此客户端的安全标记的 API 请求将失败，但是标记不会立即过期。禁用客户端并不会影响标记的过期时间。

   将随时可以重新启用客户端。

启用已禁用的 API 客户端

1. 登录管理门户。
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**。

   客户端的状态将更改为**活动**。

   如果这些标记尚未过期，则使用指派给此客户端的安全标记的 API 请求将成功。

删除 API 客户端

1. 登录管理门户。
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。

   指派给该客户端的所有安全标记将立即过期，并且使用这些标记的 API 请求将失败。

   重要事项

   无法恢复已删除的客户端。

集成参考

下表列出了与第三方实现的集成，并提供了相应文档的链接。

集成名称	联机查看	打开 PDF
Autotask PSA	https://www.acronis.com/support/documentation/AutotaskPSA/	https://dl.acronis.com/u/pdf/AutotaskPSA_Integration_quickstartguide_en-US.pdf

集成名称	联机查看	打开 PDF
CloudBlue Commerce	https://www.acronis.com/support/documentation/CloudBlueCommerce/	https://dl.acronis.com/u/pdf/CloudBlue_Commerce_Integration_Guide_en-US.pdf
CloudBlue PSA	https://www.acronis.com/support/documentation/CloudBluePSA/	https://dl.acronis.com/u/pdf/CloudBluePSAIntegration_quickstartguide_en-US.pdf
ConnectWise Automate	https://www.acronis.com/support/documentation/ConnectWiseAutomate/	https://dl.acronis.com/u/pdf/AcronisConnectWiseAutomatePlugin_userguide_en-US.pdf
ConnectWise Command	https://www.acronis.com/support/documentation/ConnectWiseCommand/	https://dl.acronis.com/u/pdf/ConnectWiseCommandIntegration_quickstartguide_en-US.pdf
ConnectWise Control	https://www.acronis.com/support/documentation/ConnectWiseControl/	https://dl.acronis.com/u/pdf/ConnectWiseControl_integration_en-US.pdf
ConnectWise Manage	https://www.acronis.com/support/documentation/ConnectWiseManage/	https://dl.acronis.com/u/pdf/ConnectWiseManageIntegration_quickstartguide_en-US.pdf
Datto RMM	https://www.acronis.com/support/documentation/DattoRMM/	https://dl.acronis.com/u/pdf/DattoRMMIntegration_quickstartguide_en-US.pdf
Jamf Pro	https://www.acronis.com/support/documentation/JamfPro/	https://dl.acronis.com/u/pdf/JamfProIntegration_quickstartguide_en-US.pdf
Kaseya BMS	https://www.acronis.com/support/documentation/KaseyaBMS/	https://dl.acronis.com/u/pdf/AcronisKaseyaBMSPlugin_userguide_en-US.pdf
Kaseya VSA	https://www.acronis.com/support/documentation/KaseyaVSA/	https://download.acronis.com/pdf/AcronisKaseyaVSAPlugin_userguide_en-US.pdf
Matrix 42	https://www.acronis.com/support/documentation/Matrix42/	https://dl.acronis.com/u/pdf/Matrix42Integration_quickstartguide_en-US.pdf
Microsoft Intune	https://www.acronis.com/support/documentation/MicrosoftIntune/	https://dl.acronis.com/u/pdf/MicrosoftIntuneIntegration_quickstartguide_en-US.pdf
N-able N-central	https://www.acronis.com/support/documentation/NableNcentral/	https://dl.acronis.com/u/pdf/N-able_N-central_Integration_Guide_en-US.pdf
N-able	https://www.acronis.com/en-	https://dl.acronis.com/u/pdf/N-ableN-

集成名称	联机查看	打开 PDF
N-sight RMM	us/support/documentation/NableNsightRMM/	sightRMMIntegration_quickstartguide_en-US.pdf
Ninja One	https://www.acronis.com/support/documentation/NinjaOne/	https://dl.acronis.com/u/pdf/NinjaOneIntegration_quickstartguide_en-US.pdf
Omnivoice	https://www.acronis.com/support/documentation/Omnivoice/	https://dl.acronis.com/u/pdf/OmnivoiceIntegration_quickstartguide_en-US.pdf
Plesk	https://www.acronis.com/support/documentation/Plesk/	https://dl.acronis.com/u/pdf/Acronis_Backup_extension_for_Plesk_en-US.pdf
PRTG	https://www.acronis.com/support/documentation/PRTG/	https://dl.acronis.com/u/pdf/AcronisPRTGPlugin_userguide_en-US.pdf
Service Now	https://www.acronis.com/support/documentation/ServiceNow/	https://dl.acronis.com/u/pdf/ServiceNow_Integration_quickstartguide_en-US.pdf
Splashtop	https://www.acronis.com/support/documentation/Splashtop/	https://dl.acronis.com/u/pdf/Splashtop_Integration_quickstartguide_en-US.pdf
Tigerpaw One	https://www.acronis.com/en-us/support/documentation/TigerpawOne/	https://dl.acronis.com/u/pdf/TigerpawOneIntegration_quickstartguide_en-US.pdf
WHM & cPanel	https://www.acronis.com/en-us/support/documentation/WHMCPanel/	https://www.acronis.com/en-us/support/documentation/WHMCPanel/
WHMCS	https://www.acronis.com/en-us/support/documentation/WHMCS/	https://dl.acronis.com/u/pdf/WHMCS_Integration_Manual_en-US.pdf

与 VMware Cloud Director 集成

服务提供商可以将 VMware Cloud Director(以前称为 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 允许将 VMware Cloud Director 环境中的更改同步到 Cyber Protect Cloud。
2. 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。
3. 部署管理代理程序。

   管理代理程序会自动将 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。

4. 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 28 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。
- 必须为合作伙伴租户（其中已配置与 VMware Cloud Director 集成）禁用双重身份验证。
- 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 Protection Web 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 10.0, 10.1, 10.2, 10.3, 10.4, 10.4.1

支持的 Web 浏览器

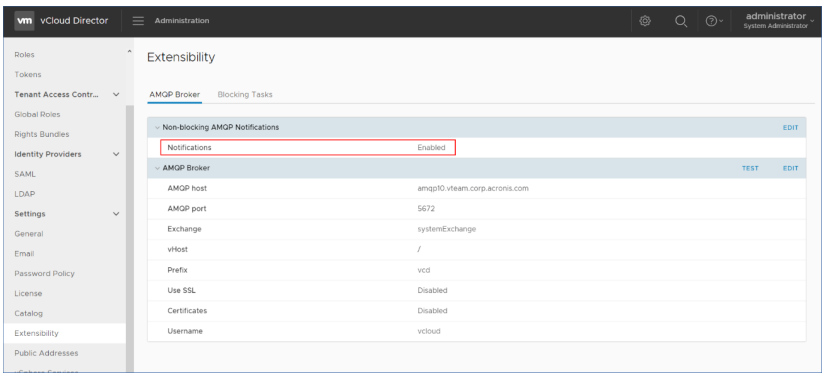
- Google Chrome 29 或更高版本
- Mozilla Firefox 23 或更高版本
- Opera 16 或更高版本
- Microsoft Edge 25 或更高版本
- 在 macOS 和 iOS 操作系统中运行的 Safari 8 或更高版本

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。

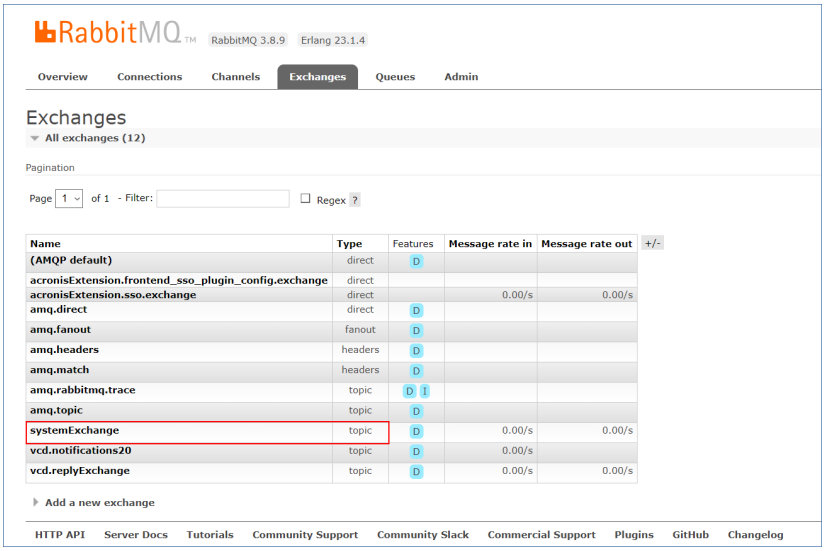
配置 RabbitMQ 消息代理

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**。



安装适用于 VMware Cloud Director 的插件

1. 单击以下链接以下载 **vCDPlugin.zip** 文件：https://dl.managed-protection.com/u/vCD/vCDPlugin.zip。
2. 以系统管理员身份登录到 VMware Cloud Director 提供商门户。
3. 在导航菜单中，选择**自定义门户**。
4. 在**管理插件**选项卡上，单击**上传**。

   将打开**上传插件**向导。
5. 单击**选择插件文件**，然后选择 **vCDPlugin.zip** 文件。
6. 单击**下一步**。
7. 配置范围和发布：
   a. 在**目标范围**部分中，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。

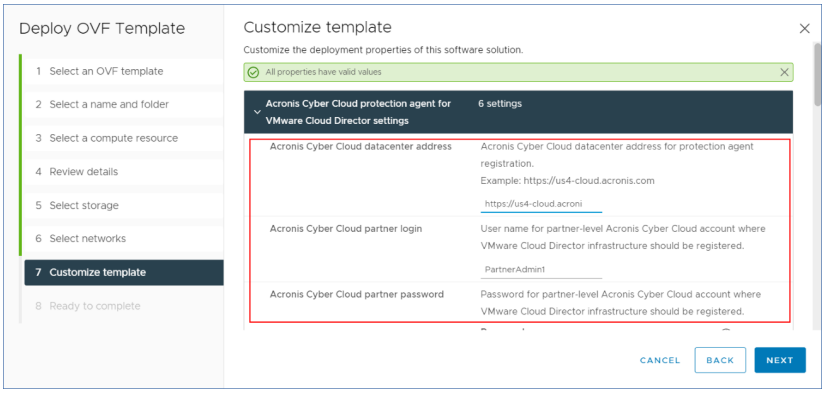
8. 单击**下一步**。
9. 查看设置，然后单击**完成**。

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. 单击**管理代理程序**链接，然后下载 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，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。

6. 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。
   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 55 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**。

      注意
      所选计费模式会应用于将创建的所有新客户租户。

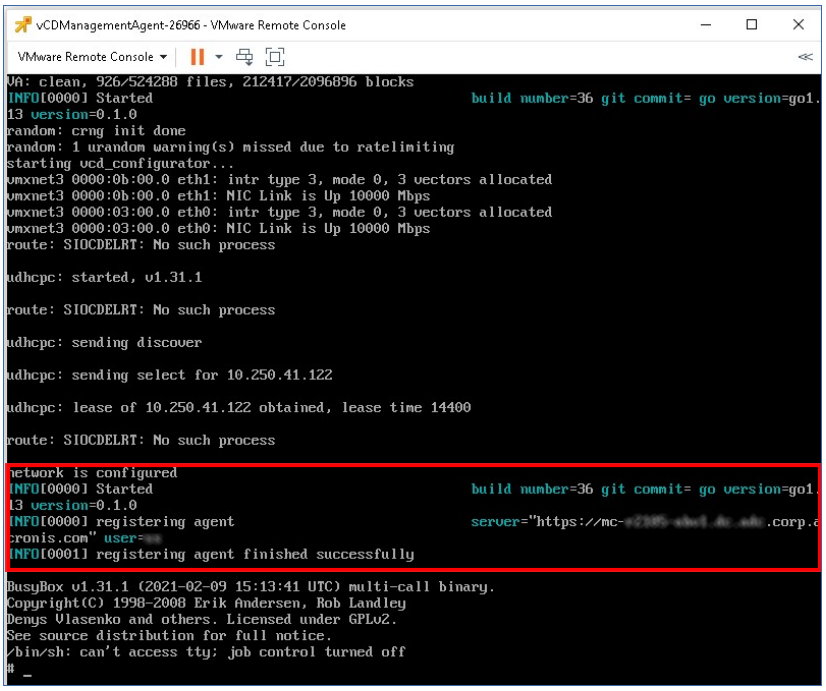
   e. VMware Cloud Director 参数：基础架构地址、系统管理员登录名和密码。
   f. RabbitMQ 参数：服务器地址、端口、虚拟主机名、管理员登录名和密码。
   g. 网络参数：IP 地址、子网掩码、默认网关、DNS、DNS 后缀。
      默认情况下，仅启用一个网络接口。要启用第二个网络接口，请选中**启用 eth1** 旁边的复选框。

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。

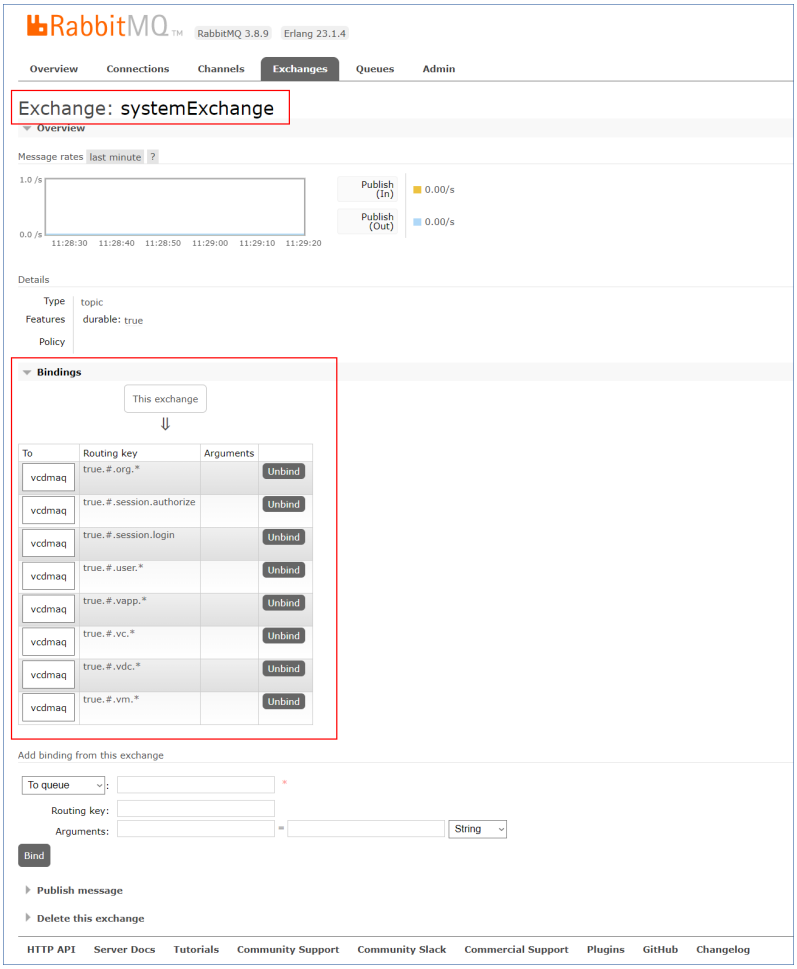
还可以在初始部署后配置管理代理程序设置。在 vSphere Client 中，关闭具有管理代理程序的虚拟机，然后依次单击**配置** > **设置** > **vApp 选项**。应用所需设置，然后打开具有管理代理程序的虚拟机。

7. [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。



8. 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。



安装备份代理程序

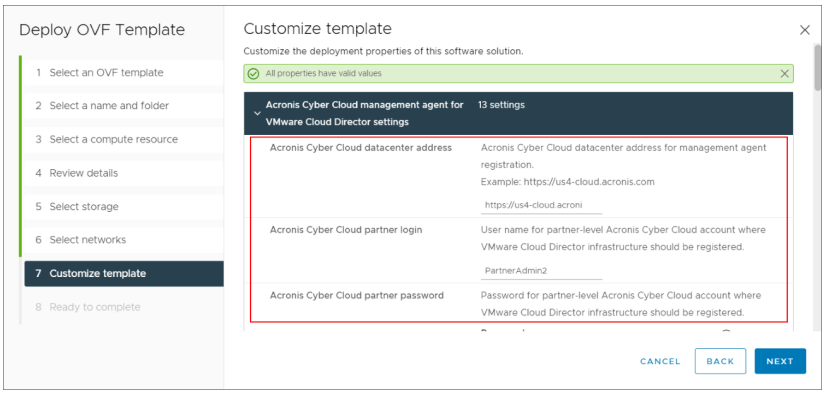
1. 以合作伙伴管理员身份登录到管理门户。
2. 转到**设置** > **位置**，然后单击**添加 VMware Cloud Director**。
3. 单击**备份代理程序**链接，然后下载 ZIP 文件。
4. 提取备份代理程序模板文件 `vCDCyberProtectAgent.ovf` 和虚拟硬盘文件 `vCDCyberProtectAgent-disk1.vmdk`。
5. 在 vSphere Client 中，将备份代理程序模板部署到所需的 ESXi 主机。

   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 10 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。

   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。

6. 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。

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. 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。

e. 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。

f. 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。

7. 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**。

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。

访问 Cyber Protection Web 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 122 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 Protection Web 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 Protection Web 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 Protection Web 中控台，并可以代表他们管理备份和恢复。

限制

在即将发布的 Cyber Protect Cloud 版本中，限制列表可能会发生变化。

备份

- 仅支持备份整个计算机。文件过滤器或者选择磁盘或卷不可用。
- 仅支持云存储作为备份位置。存储在管理代理程序设置中进行配置，用户无法在保护计划中更改它。
- 动态组不受支持。
- 支持以下备份方案：**始终增量（单个文件）**、**始终完整备份**和**每周完整备份，每日增量备份**。
- 仅支持备份后清理。

恢复

- 仅支持恢复到原始虚拟机。原始虚拟机必须存在于 VMware Cloud Director 环境中。
- 不支持文件级恢复。

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 "安装适用于 VMware Cloud Director 的插件"（第 116 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

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。

隐私设置

隐私设置可帮助您表明是否同意收集、使用和披露您的个人信息。

根据您使用 Cyber Protect 所做的国家/地区和为您提供服务的 Cyber Protect Cloud 数据中心，在首次启动推出 Cyber Protect 时，系统可能会要求您确认是否同意在 Cyber Protect 中使用 Google Analytics。

Google Analytics 通过收集匿名数据，帮助我们更好地了解用户行为并改善 Cyber Protect 中的用户体验。

如果您在 Cyber Protect 界面中没有看到 Google Analytics 同意和菜单，则表示您所在的国家/地区未使用 Google Analytics。

如果在首次启动 Cyber Protect 时启用或拒绝启用 Google Analytics，可以在以后随时改变您的决定。

启用或禁用 Google Analytics

1. 在 Cyber Protect 中控台中，单击右上角的帐户图标。
2. 选择**我的隐私设置**。
3. 在 **Google Analytics 数据收集**部分中，单击以下按钮之一：
   - **打开** - 启用 Google Analytics
   - **关闭** - 禁用 Google Analytics

索引

在

增

支

执

重

转

追

自

租

最