管理门户

24.04

公司管理员指南

修改：2024/5/9

目录

关于本文档

本文档适用于以下情形的客户管理员:要使用云管理门户创建和管理用户帐户、单位、配额;配置和控制访问权限;监控其云组织中的使用情况和操作。

关于管理门户

管理门户是提供数据保护服务的云平台的 Web 界面。

虽然每个服务都有自己的 Web 界面(称为服务中控台),但管理门户使管理员能够控制服务使用情况、创建用户帐户和单位、生成报告等。

帐户和单位

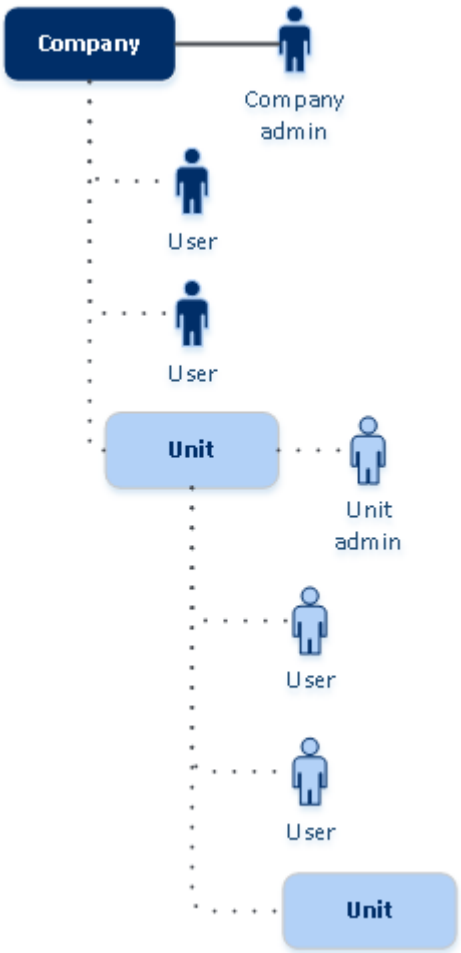
有两种用户帐户类型:管理员帐户和用户帐户。

- **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。

管理员可以创建单位,这些单位通常对应于组织的单位或部门。每个帐户都存在于公司级别或单位中。

管理员可以在他们在层次结构中的级别上面或下面管理单位、管理员帐户和用户帐户。

下图演示三种层次结构级别 - 公司和两个单位。可选的单位和帐户以虚线显示。



下表总结了管理员和用户可以执行的操作。

操作	用户	管理员
创建单位	否	是
创建帐户	否	是
下载和安装软件	是	是
使用服务	是	是
创建关于服务使用情况的报告	否	是

配额管理

配额会限制租户使用服务的能力。

在管理门户中，可以查看由服务提供商分配给贵组织的服务配额，但您无法管理它们。

可以管理您用户的服务配额。

查看组织的配额

在管理门户中，转到**概述** > **使用情况**。您将看到一个仪表板，它会显示为贵组织分配的配额。每个服务的配额都会显示在单独的选项卡上。

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。

重要事项

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

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

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 9 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**

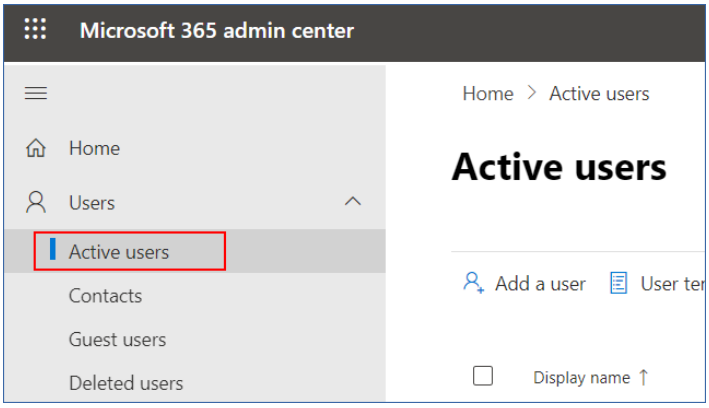
  云资源配额结合了备份存储的配额和灾难恢复的配额。备份存储空间配额限制了位于云存储中备份的总大小。当超出备份存储空间配额超额时，备份失败。

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。

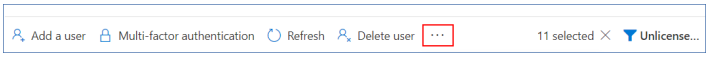
防止未经许可的用户登录

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备份存储大小。使用灾难恢复存储等同于使用受灾难恢复服务器保护的工作负载的备份存储。此存储会从创建恢复服务器时就开始计算，无论该服务器当前是否正在运行。如果达到此配额的超额，将无法创建主服务器和恢复服务器，也无法添加/扩展现有主服务器的磁盘。如果超过此配额的超额，将无法启动故障转移或启动已停止的服务器。正在运行的服务器继续运行。
- **计算点**
  此配额可限制计费期内主服务器和恢复服务器使用的 CPU 和 RAM 资源。如果达到此配额的超额，则所有主服务器和恢复服务器都将关机。在下一个计费期开始之前，无法使用这些服务器。默认计费期为一个完整的日历月。
  当配额禁用时，无论计费期如何，都无法使用服务器。
- **公共 IP 地址**
  此配额会限制可以分配给主服务器和恢复服务器的公共 IP 地址的数量。如果达到此配额的超额，则无法为更多服务器启用公共 IP 地址。可以通过在服务器设置中取消选中**公共 IP 地址**复选框，来禁止服务器使用公共 IP 地址。之后，可以允许另一台服务器使用公共 IP 地址，这通常不会是同一个 IP 地址。
  当配额禁用时，所有服务器将停止使用公共 IP 地址，从而无法通过 Internet 进行访问。
- **云服务器**
  此配额可限制主服务器和恢复服务器的总数。如果达到此配额的超额，则无法创建主服务器或恢复服务器。
  在配额禁用后，服务器会在 Cyber Protect 中控台中可见，但唯一可进行的操作是**删除**。
- **Internet 访问**
  此配额可启用或禁用主服务器和恢复服务器的 Internet 访问。
  当该配额禁用后，主服务器和恢复服务器将无法与 Internet 建立连接。

File Sync & Share配额

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。

- **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。

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。

- **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

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。

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

定义您用户的配额

配额让您可以限制用户使用服务的能力。要为用户设置配额，请在**公司管理**下的**用户**选项卡上选择用户，然后在**配额**部分中单击铅笔图标。

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。当用户的受保护工作站数量达到 20 个时，用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，用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。

备份配额

可以指定备份存储配额，以及允许用户保护的最多计算机/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。

存储的配额

- **备份存储**

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，备份会失败。

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

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

File Sync & Share配额

可以为用户定义以下File Sync & Share配额：

- **个人存储空间**
  为用户的文件定义已分配的云存储空间。

公证配额

可以为用户定义以下公证配额：

- **公证存储**
  为已公证文件、已签名文件和正在进行公证或签名的文件定义最大云存储空间。

要减少此配额的使用，可以从公证存储中删除已公证或已签名的文件。

- **公证**

  定义可以使用公证服务进行公证的文件的最大数量。

  文件一上传到公证存储就视为已公证，并且其公证状态更改为**进行中**。

  如果同一文件进行多次公证，每次公证视为新的公证。

- **电子签名**

  定义数字电子签名的最大数量。

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。

分步说明

以下步骤将指导您完成管理门户的基本用法。它们介绍如何：

- 激活管理员帐户
- 访问管理门户和服务
- 创建单位
- 创建用户帐户

激活管理员帐户

注册服务后，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 14 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。

访问管理门户和服务

1. 转到服务中控台登录页面。
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**。
4. 请执行以下任一操作：
   - 要登录管理门户，请单击**管理门户**。
   - 要登录服务，请单击服务名称。

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。

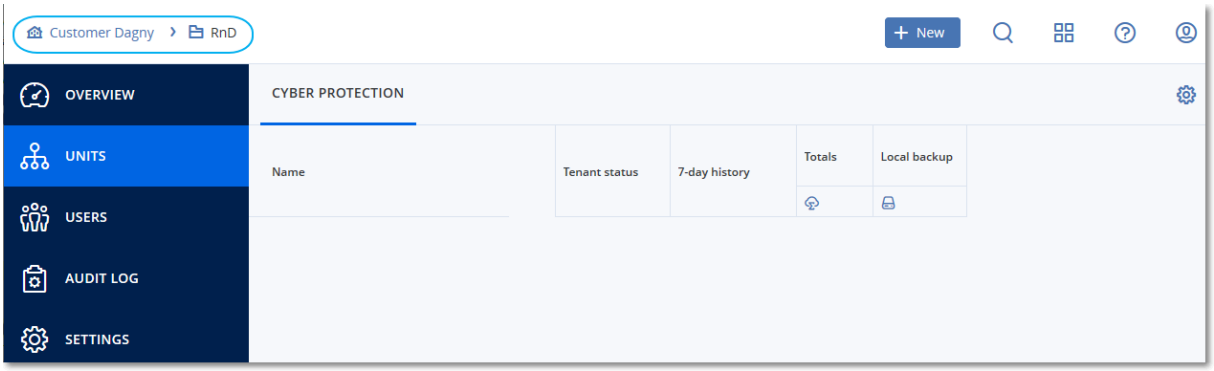
在管理门户和服务中控台之间切换

要在管理门户和服务中控台之间切换，请单击右上角的  图标，然后选择要转到的**管理门户**或服务。

导航管理门户

使用管理门户时，您可以在任何给定时间在公司或单位内进行操作。此消息在左上角显示。

默认情况下，选择向您提供的最高层次结构级别。单击单元名称可以逐层展开层次结构。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公司或单位。例如：

- 使用**新建**按钮，您只能在该公司或单位中创建单位或用户帐户。
- **单位**选项卡仅显示该公司或单位的直接子单位。
- **用户**选项卡仅显示存在于该公司或单位中的用户帐户。

创建单位

如果您不想将帐户组织到单位中，请跳过此步骤。

如果您打算稍后创建单位，请注意现有帐户无法在单位之间或公司与单位之间移动。首先，您需要创建一个单位，然后用帐户填充。

创建单位

1. 请登录管理门户。
2. 导航到要在其中新建单位的单位。
3. 在右上角，依次单击**新建** > **单位**。
4. 在**名称**中，指定新单位的名称。
5. [可选] 在**语言**中，更改将在此单位中使用的通知、报告和软件的默认语言。
6. 请执行以下任一操作：
   - 若要创建单位管理员，请单击**下一步**，然后按照“创建用户帐户”中描述的步骤操作，从第 4 步开始。
   - 若要创建没有管理员的单位，请单击**保存并关闭**。您可以稍后向单位添加管理员和用户。

新建的单位显示在**单位**选项卡中。

如果要编辑单位设置或指定联系信息，请在**单位**选项卡上选择单位，然后单击要编辑部分中的铅笔图标。

创建用户帐户

如果不想创建其他用户帐户，请跳过此步骤。

在以下情况下，您可能想创建其他帐户：

- 公司管理员帐户 — 与其他人共享管理职责。
- 单位管理员帐户 — 将管理委派给访问权限限制在相应单位的其他人员。
- 用户帐户 — 使用户只能访问服务子集。

要创建用户帐户

1. 请登录管理门户。
2. 导航到要在其中创建新用户帐户的单位。
3. 在右上角，依次单击**新建** > **用户**。
4. 为帐户指定以下信息：
   - **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。

   - [可选] **名**
   - [可选] **姓**
   - 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. 选择用户将有权访问的服务和每个服务中的角色。
   - 如果选中**公司管理员**复选框，用户将拥有对管理门户的访问权限和所有服务中的管理员角色。
   - 如果选中**单位管理员**复选框，则用户将拥有对管理门户的访问权限，但可能有也可能没有服务管理员角色，具体取决于服务。
   - 否则，用户将拥有您在所选服务中选择的角色。
6. 单击**创建**。

新建用户帐户显示在**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，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	描述
不适用	公司管理员	此角色授予所有服务的完全管理员权限。 此角色授予对公司允许列表的访问权限。如果已为公司启用 保护 服务的“灾难恢复”功能，则此角色还会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。 例如，此角色为“端点检测和响应”屏幕授予完全权限，包括小组件。
	只读管理员 合作伙伴级别	此角色提供对合作伙伴管理门户中的所有对象以及所有这些合作伙伴的客户的管理门户的只读访问权限。此类用户可以以只读模式访问组织中其他用户的数据。他们能够编辑保护计划，但是他们不能保存对脚本计划，监控计划或代理程序计划的任何更改。
	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	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

	单位级别	据。
保护	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 保护。 例如，该角色是配置和管理“灾难恢复”功能、“端点检测和响应”功能及公司允许列表所必需的。
	只读管理员	该角色将提供对 保护 服务的所有对象的“只读”访问权限。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、“端点检测和响应”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。
	用户	此角色支持使用 保护 服务，但没有管理权限。为诸如“端点检测和响应”的功能提供访问权限，但指派了此角色的用户不能访问组织中其他用户的数据。
File Sync & Share	管理员	此角色支持为用户配置和管理 File Sync & Share。由于此角色不支持访问 功能，因此具有此角色的帐户不会计数为**用户**配额的一部分。
	用户	此角色支持使用 File Sync & Share 服务。用户仅可以访问其自己的和与其分享的数据。
	来宾	当 File Sync & Share 用户与不能使用 File Sync & Share 服务的 Cyber Protect Cloud 用户或不是 Cyber Protect Cloud 用户的人员共享内容时，将创建具有此角色的帐户。 由于“来宾”角色不支持访问 功能，因此“来宾”角色没有同步文件夹、无法使用云存储，并且不会计数为**用户**配额的一部分。“来宾”可以“升级”为“用户”或“管理员”角色。
公证	管理员	使用此角色可配置和管理您用户的公证。
	用户	此角色支持使用“公证”服务，但没有管理权限。此类用户无法访问组织中其他用户的数据。

只读管理员角色

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

- 收集诊断数据，如系统报告。
- 查看备份的恢复点，但无法深入了解备份内容，也无法查看文件、文件夹或电子邮件。

“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。

更改用户的通知设置

若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：

- **维护通知**— 在Cyber Protect数据中心通知合作伙伴用户、子租户（合作伙伴和客户）以及个人用户即将进行的维护活动。合作伙伴用户可以为其子租户启用这些通知，合作伙伴用户或公司管理员也可以为其组织内的个人用户启用这些通知。
- **配额过度使用通知**— 有关超出配额的通知。
- **预定使用情况报告**— 每月第一天发送的使用情况报告。
- **URL 品牌通知** - 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** - 有关保护计划的执行结果和每个设备的灾难恢复操作结果的通知。
- **活动警报每日回顾** - 每日概述是根据生成概述时 Cyber Protect 中控台中存在的活动警报列表生成的。该概述每天于 UTC 时间 10:00 和 23:59 之间生成并发送一次。生成并发送报告的具体时间取决于数据中心中的工作负载。如果当时没有活动警报，则不会发送概述。概述不包括不再有效的过去警告的信息。例如，如果用户发现失败的备份并清除警告，或者备份在生成概述之前重试并成功，则该警告将不再存在并且概述将不包括该警告。
- **设备控制通知** - 关于对使用外围设备和端口的尝试的通知，而这些设备和端口在启用了设备控制模块的情况下受保护计划的限制。
- **恢复通知** - 针对以下资源的恢复操作的相关通知：用户电子邮件和整个邮箱、公用文件夹，OneDrive/GoogleDrive：整个 OneDrive 和文件或文件夹、SharePoint 文件，Teams：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** - 有关数据丢失防护警报的通知与此用户在网络上的活动有关。
- 安全事件通知 - 有关访问时、执行时和按需扫描期间检测到的恶意软件以及来自行为引擎和 URL 过滤引擎的检测的通知。
- 有关访问时、执行时和手动扫描期间检测到的恶意软件以及来自行为引擎的检测的通知。

  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）。
- **基础设施通知** - 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。

根据通知类型和用户角色设置默认通知（启用/禁用）

默认启用或禁用的通知取决于通知类型和用户角色。

通知类型\用户角色	根、子根管理员	合作伙伴、文件夹管理员	客户、单位管理员(自助服务)	客户、单位管理员(由服务提供商管理)
维护通知	否	是 (默认对直接合作伙伴的用户启用,对非直接合作伙伴禁用)	否	否
配额过度使用通知	否	是	是	否
预定使用情况报告通知	否	是	是	否
URL 品牌推广通知	否	否	否	否
失败通知	否	否	否	否
警告通知	否	否	否	否
成功通知	否	否	否	否
活动警告的每日概述	否	否	是	否
设备控制通知	否	否	否	否
恢复通知	否	否	否	否
数据丢失预防通知	否	否	否	否
安全事件通知:已缓解	否	否	否	否
安全事件通知:未缓解	否	否	否	否
基础架构通知	是	否	否	否

根据设备类型和用户角色设置默认通知(启用/禁用)

设备类型\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

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。

删除用户帐户

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

结果：

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

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 32 位代码，然后在身份验证应用程序中手动添加它。

   重要事项
   强烈建议您保存它（打印二维码、写下临时一次性密码 (TOTP) 机密信息、使用支持在云中备份代码的应用程序）。如果第二重身份验证设备丢失，您需要使用临时一次性密码 (TOTP) 来重置双重身份验证。

6. 将在身份验证应用程序中生成临时一次性密码 (TOTP) 代码。它会每隔 30 秒自动重新生成。
7. 用户在输入其密码后，必须在**设置双重身份验证**窗口上输入 TOTP 代码。
8. 结果，将为用户设置双重身份验证。

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

在新设备上恢复双重身份验证

如果您可以访问以前设置的移动身份验证应用程序：

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

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

3. 如果您在设置过程中并未保存 PDF 文件：

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

如果您无法访问以前设置的移动身份验证器应用程序：

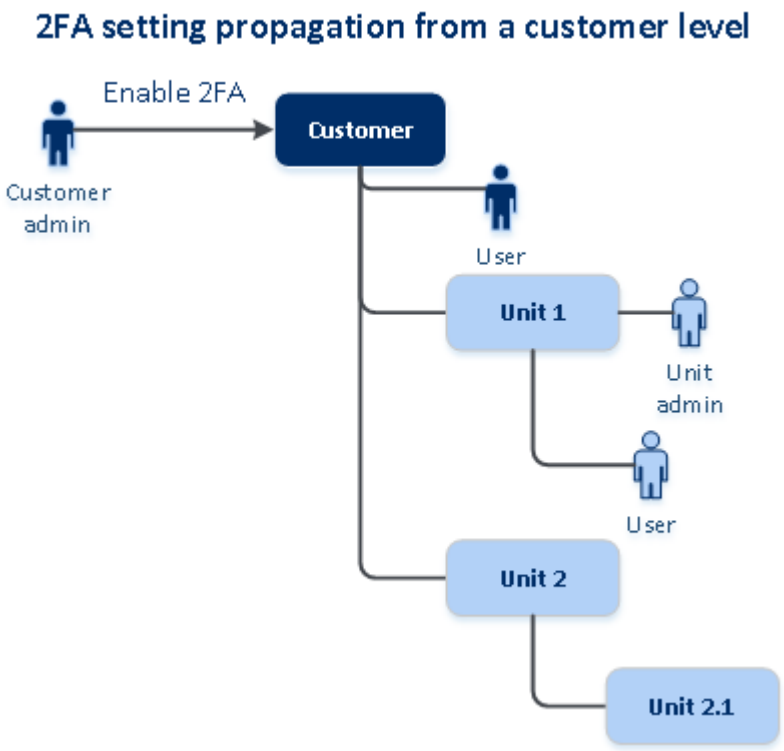
1. 拿取一个新的移动设备。
2. 使用存储的 PDF 文件来链接新设备（默认文件名为 `cyberprotect-2fa-backupcode.pdf`）。
3. 通过备份恢复对您帐户的访问权限。确保您的移动应用程序支持备份。
4. 从该应用程序支持的另一个移动设备，使用同一帐户打开该应用程序。

租户级别的双重身份验证设置传播

双重身份验证基于**组织**级别设置。可以仅为自己的组织设置双重身份验证。

双重身份验证设置会在租户级别传播，如下所示：

- 单位自动继承其客户组织的双重身份验证设置。



注意

1. 无法基于单位级别设置双重身份验证。
2. 可以管理子组织(单位)的用户的双重身份验证。

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。

自动更新代理程序

重要事项
当前，仅当已启用 保护 时，您才有权访问代理程序更新管理功能。

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。

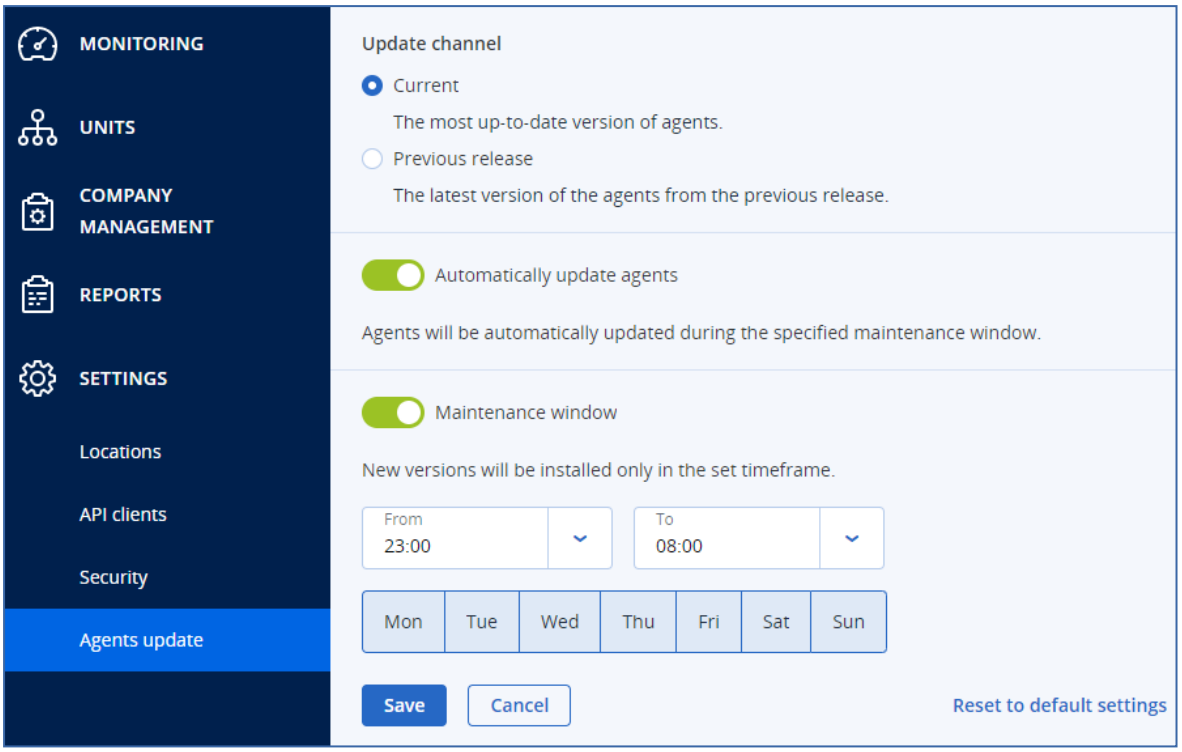
注意
要管理个别计算机上的代理程序并自定义自动更新设置，请参阅更新代理程序上的 Cyber Protect 用户指南部分。

自动更新代理程序

注意
如果未启用保护，则自动更新适用于 File Sync & Share 的代理程序的设置继承自服务提供商。

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
仅当启用保护模块时，才能监视代理程序更新。

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。

配置不可变存储

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

不可变存储包含以下备份：

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

不可变存储中已删除的备份仍会使用存储空间并收取相应费用。

已删除的租户无需支付任何存储费用，包括不可变存储。

对于客户租户，不可变存储在以下模式下可用：

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

  警告！
  选择合规模式是不可逆的。

  您无法禁用不可变存储。您无法更改保留期限，也无法切换回监管模式。

配置不可变存储设置需要在管理员帐户所属的租户中进行双重身份验证。

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

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 3650 天的范围内指定保留期。
   默认的保留期为 14 天。较长的保留期会导致存储使用量增加。
4. 选择不可变存储模式，然后在出现提示时确认您的选择。
5. 单击**保存**。

警告！
选择**合规模式**是不可逆的。在选择此模式后，将不允许禁用不可变存储，也不允许更改其模式或保留期。

6. 要使现有存档能够支持不可变存储，请在该存档中创建一个新备份。
   要创建新备份，请手动或按预定运行保护计划。

警告！
如果在使存档能够支持不可变存储之前删除备份，则将永久删除该备份。

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。

注意
只能在监管模式下禁用不可变存储。

警告！
禁用不可变存储不会立即生效。在 14 天的宽限期内，不可变存储仍处于活动状态，可以根据其原始保留期访问已删除的备份。在宽限期结束后，将永久删除不可变存储中的所有备份。

3. 单击**禁用**来确认选择。

支持的存储和代理程序

- 仅云存储支持不可变存储。
  不可变存储适用于使用 Cyber Infrastructure 4.7.1 或更高版本的 Acronis 托管和合作伙伴托管云存储。
  所有具有 Cyber Infrastructure 备份网关的存储均受支持。例如，Cyber Infrastructure 存储、Amazon S3 和 EC2 存储以及 Microsoft Azure 存储。
  不可变存储要求在 Cyber Infrastructure 中为备份网关服务打开 TCP 端口 40440。在版本 4.7.1 及更高版本中，使用**备份 (ABGW) 公共**流量类型自动打开 TCP 端口 40440。有关流量类型的详细信息，请参阅Acronis Cyber Infrastructure 文档。
- 不可变存储需要版本为 21.12(内部版本 15.0.28532) 或更高版本的保护代理程序。
- 仅支持 TIBX(版本 12) 备份。

监控

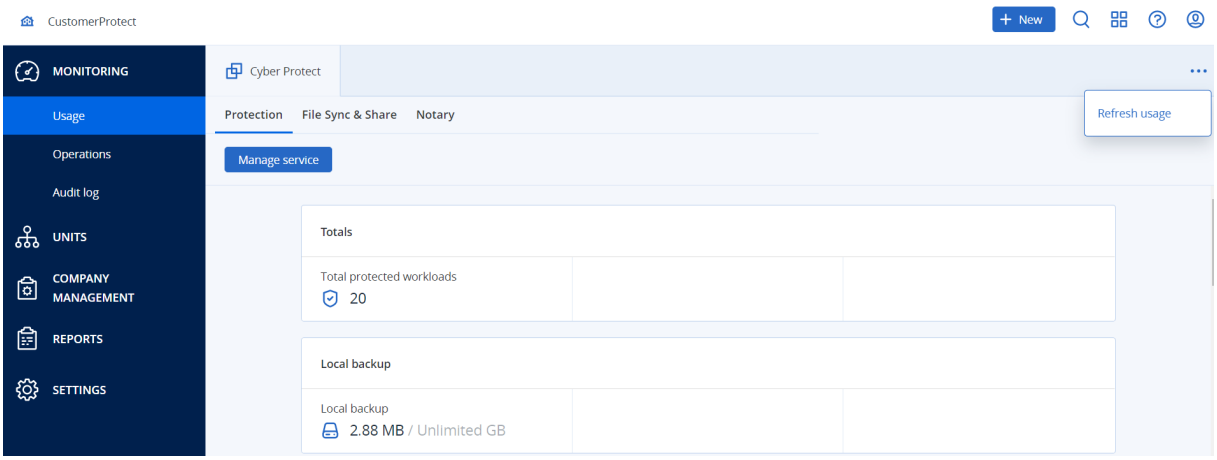
要访问有关服务使用情况和操作的信息，请单击**监控**。

使用情况

使用情况选项卡提供服务使用情况(包括配额，如果有)概述并允许您访问服务中控台。

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。



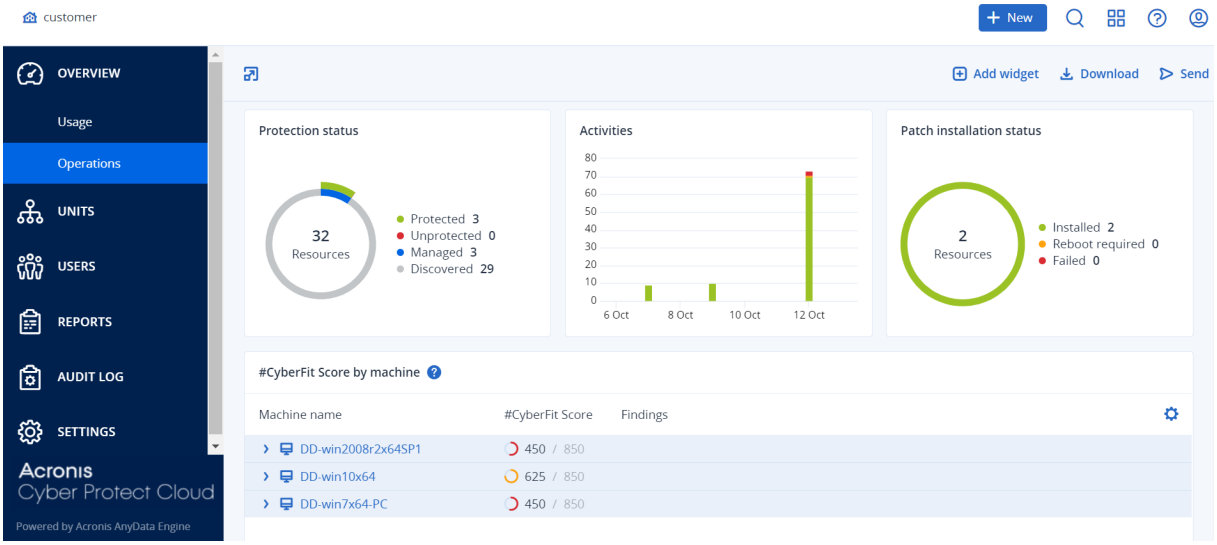
操作仪表板

操作仪表板仅对在公司级别上进行操作的公司管理员可用。

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。

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。可以使用 .pdf 或/和 .xlsx 格式下载仪表板的当前状态或通过电子邮件发送它。

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。可以使用不同过滤器添加相同类型的多个小部件。



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进行编辑，请在选中小部件时单击铅笔图标。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

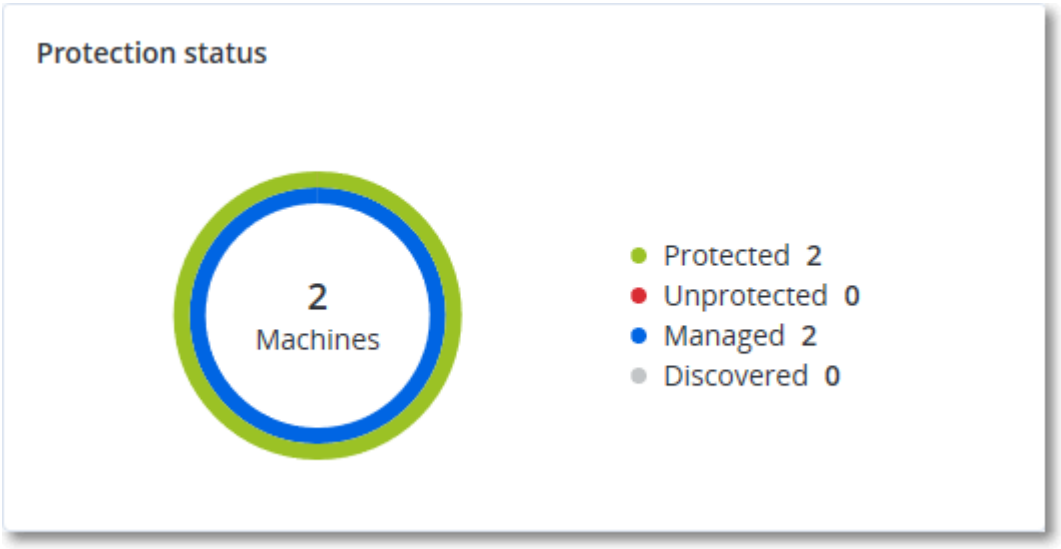
保护状态

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

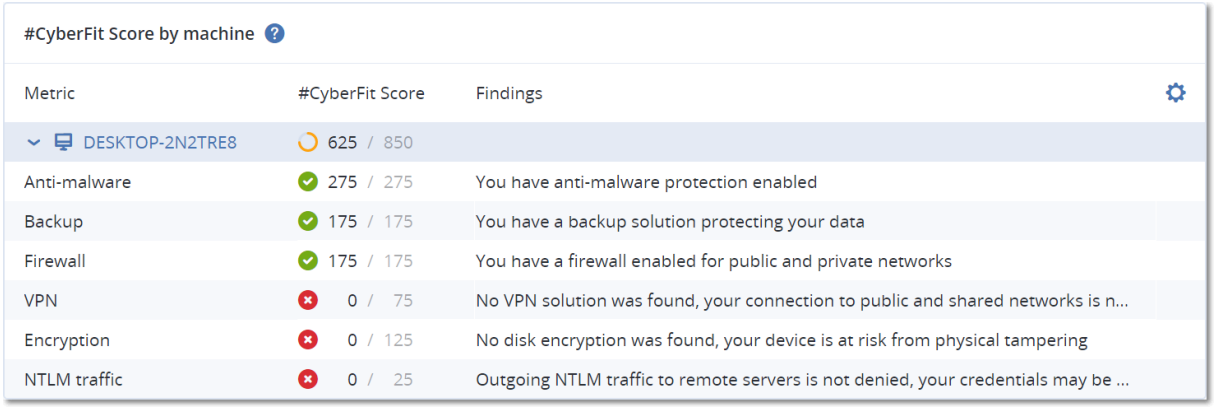
#CyberFit 分数(按计算机)

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”。



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。

端点检测和响应 (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

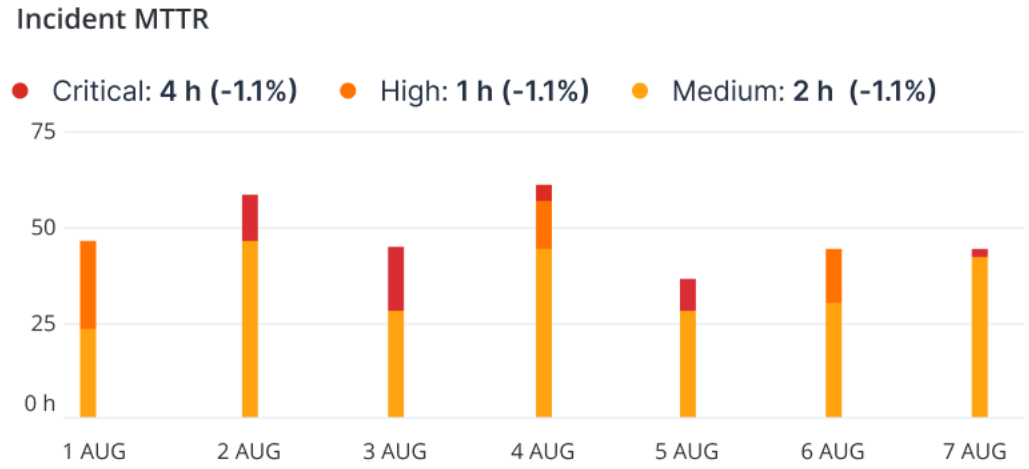
此小组件显示具有最多事件的前五个工作负载(单击**全部显示**以重定向到事件列表，这可根据小组件设置进行过滤)。

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。

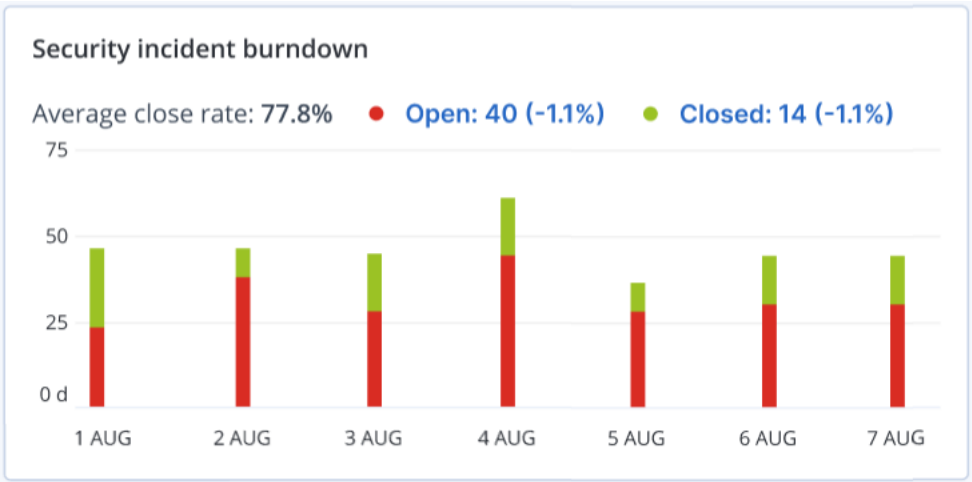


安全性事件刻录

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)。

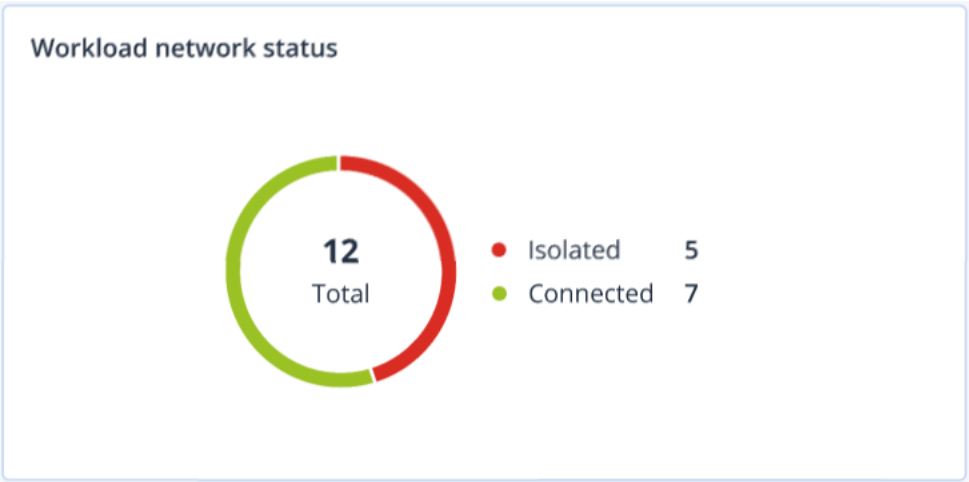
在括号中显示的 % 值表示与以前时间段比较的上升或下降。



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。磁盘运行状况小组件不包括任何有关 RAID 已实现的计算机的信息。
- 不支持 NVMe SSD。

磁盘运行状况可以表示为以下状态之一：

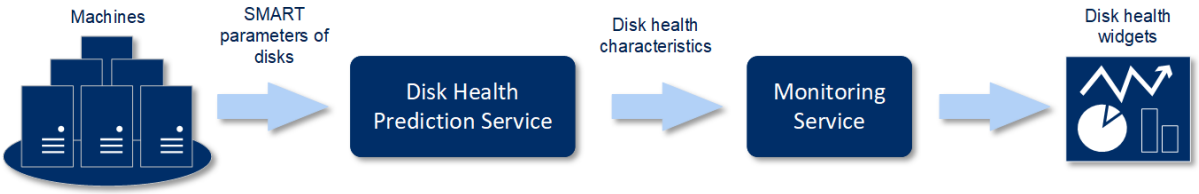
- **正常**
  磁盘运行状况为 70% 和 100% 之间。
- **警告**
  磁盘运行状况为 30% 和 70% 之间。
- **严重**
  磁盘运行状况为 0% 和 30% 之间。
- **计算磁盘数据**
  正在计算当前磁盘状态和预测。

工作方式

“磁盘运行状况预测服务”使用基于人工智能的预测模型。

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

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



磁盘运行状况小部件

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

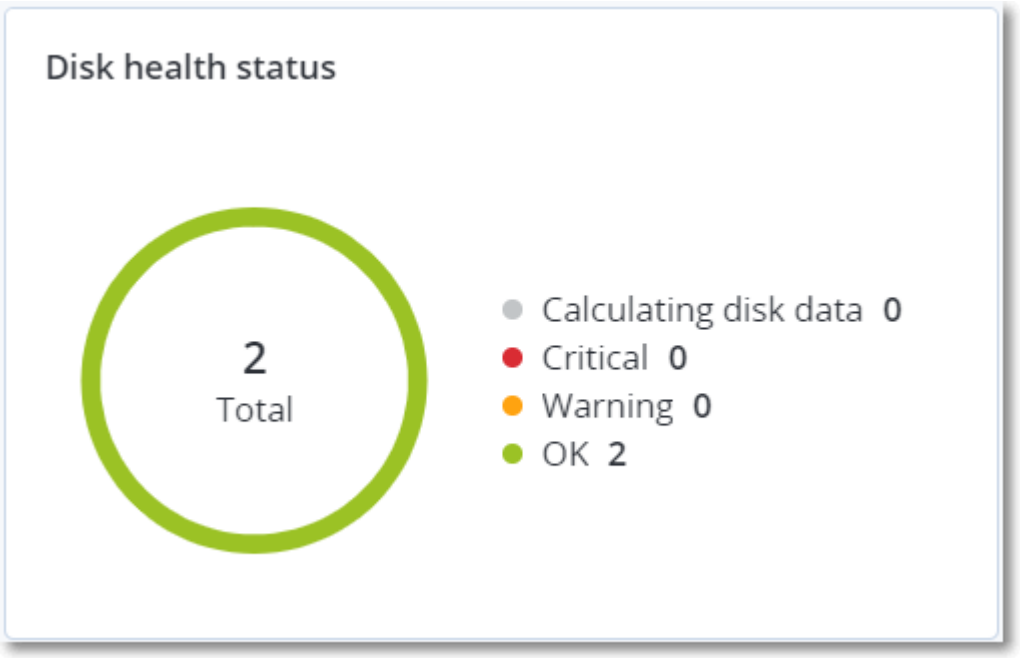
- **磁盘运行状况概述**是一个树形图小部件，具有可以通过向下钻取来切换的两个级别的详细信息。
  - 计算机级别
    显示有关每个选定客户计算机的磁盘运行状况状态的概要信息。仅显示最严重的磁盘状态。

将光标悬停在特定块上时，其他状态会显示在工具提示中。计算机块的大小取决于该计算机所有磁盘的总大小。计算机块的颜色取决于找到的最严重磁盘状态。

- 磁盘级别
  显示选定计算机的所有磁盘的当前磁盘运行状况状态。每个磁盘块显示以下任一磁盘运行状况预测及其可能性(百分比)：
  - 将降级
  - 将保持稳定

- 将得到改进

- **磁盘运行状况状态**是一个饼图小部件，显示每个状态的磁盘数量。



磁盘运行状况状态警告

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

警告名称	严重性	磁盘运行状况状态	描述
磁盘可能发生故障	警告	(30 – 70)	此计算机上的 <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	严重	(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。此时，不建议对该磁盘进行映像备份，因为增加的压力可能会导致磁盘发生故障。立即备份该磁盘上最重要的文件并替换该磁盘。

数据保护地图

数据保护地图功能允许您查找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。

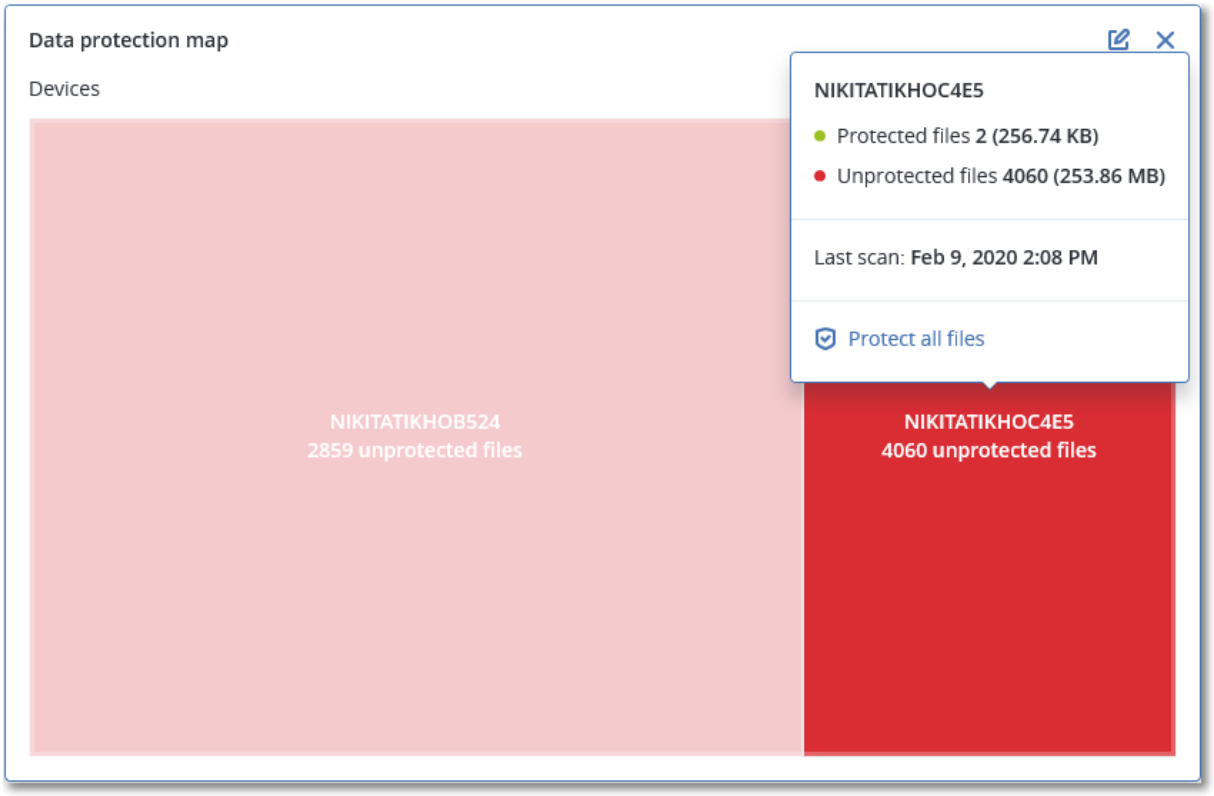
每个块的大小取决于属于客户/计算机的所有重要文件的总数/大小。

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）未针对选定计算机/位置进行备份，并且将不会使用现有备份设置进行备份。
- **低** - 有 21-50% 的不受保护文件（具有您指定的扩展名）未针对选定计算机/位置进行备份，并且将不会使用现有备份设置进行备份。
- **中** - 有 1-20% 的不受保护文件（具有您指定的扩展名）未针对选定计算机/位置进行备份，并且将不会使用现有备份设置进行备份。
- **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，在计算机级别显示详细信息）的仪表板上找到：

- 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。

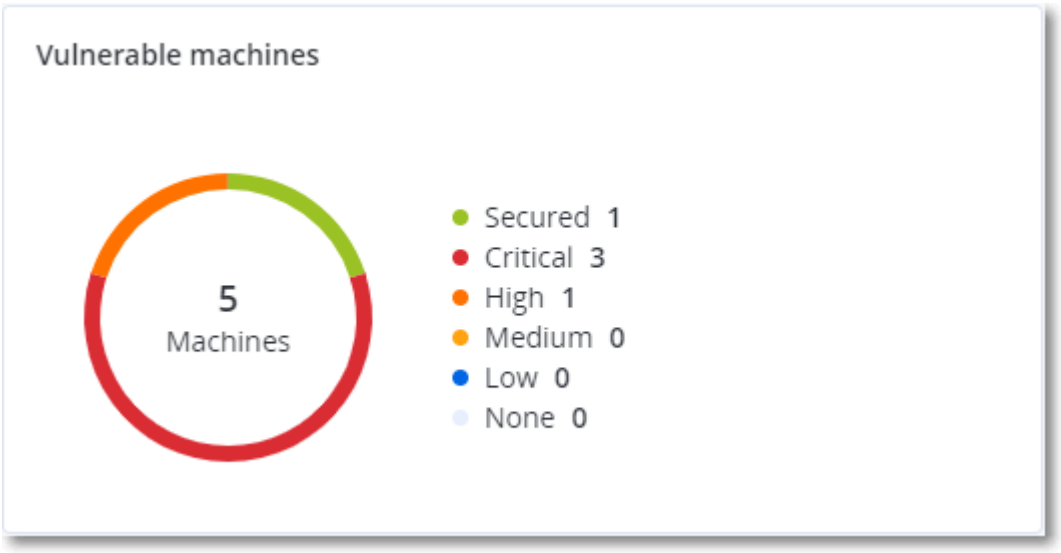
漏洞评估小部件

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：

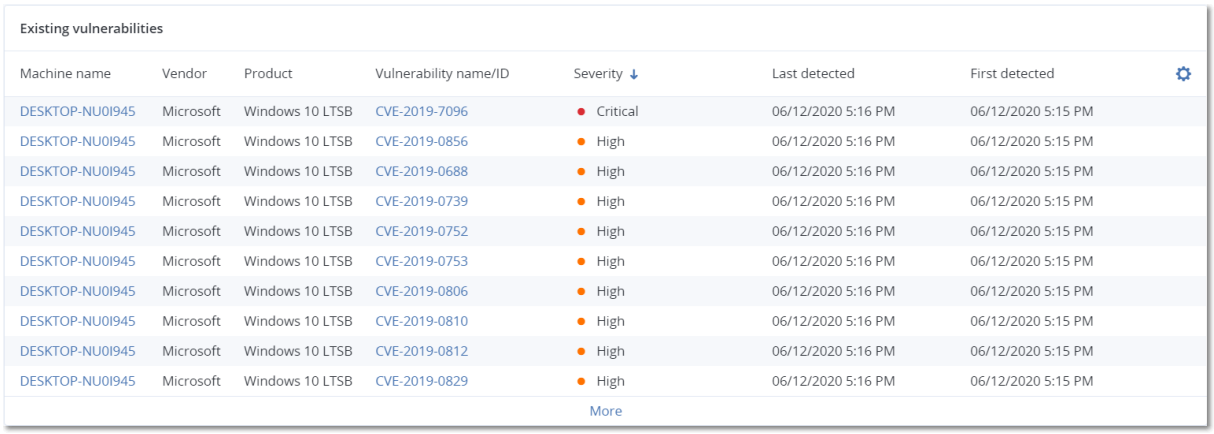
- 已保护：未发现任何漏洞
- 严重：9.0 - 10.0 CVSS
- 高：7.0 - 8.9 CVSS
- 中：4.0 - 6.9 CVSS
- 低：0.1 - 3.9 CVSS
- 无：0.0 CVSS



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。



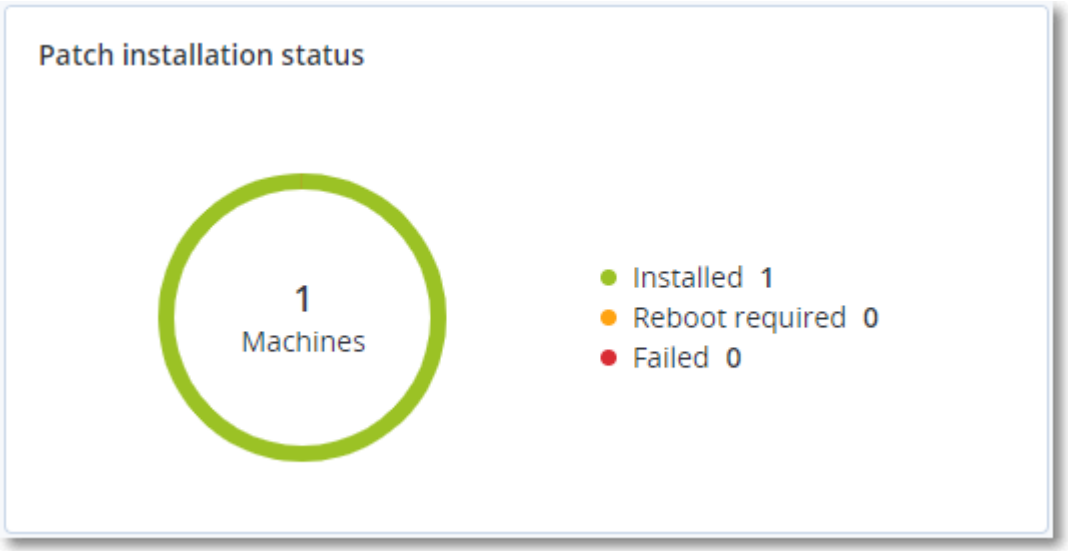
修补程序安装小部件

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

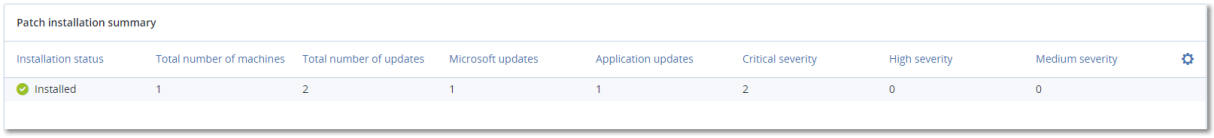
该小部件显示按修补程序安装状态分组的计算机数量。

- **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。



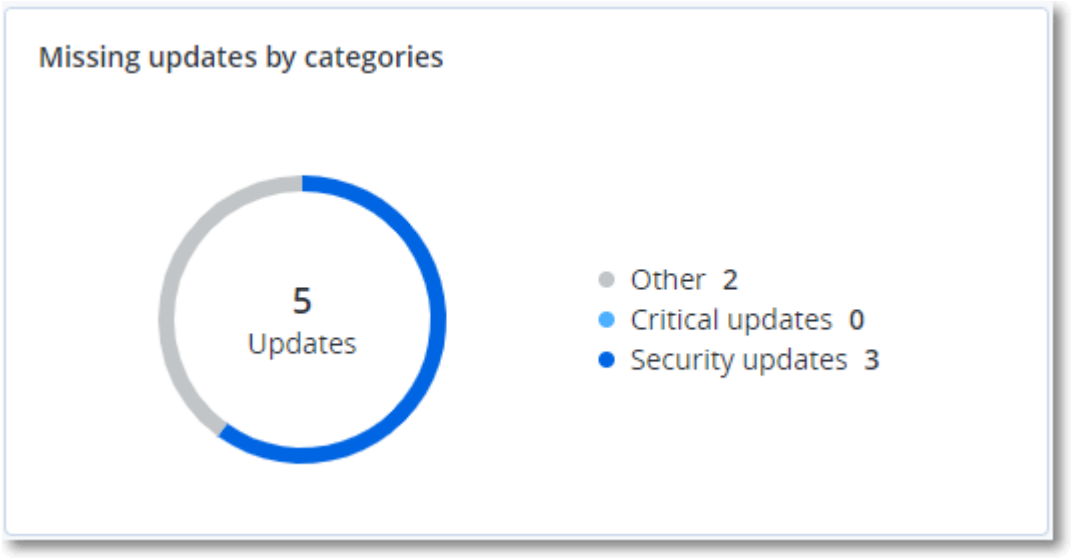
修补程序安装历史记录

该小部件显示有关计算机上修补程序的详细信息。

按类别划分的缺少更新

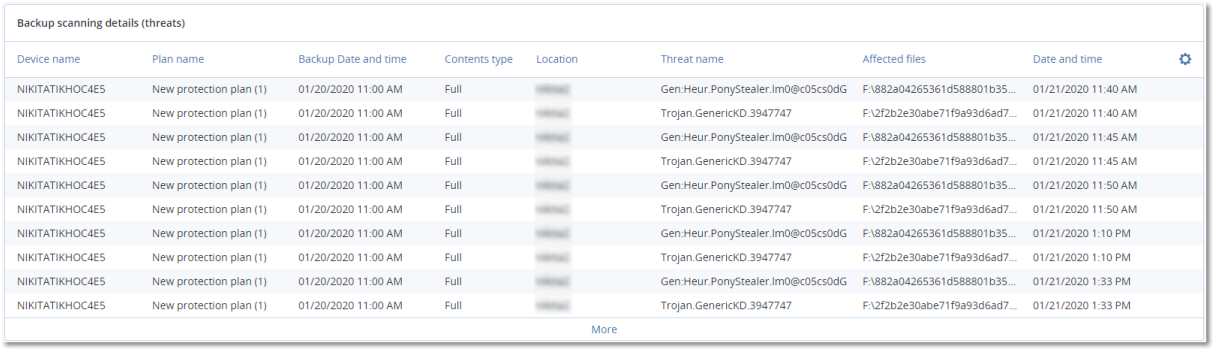
该小部件显示每个类别缺少的更新数量。显示以下类别：

- 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。



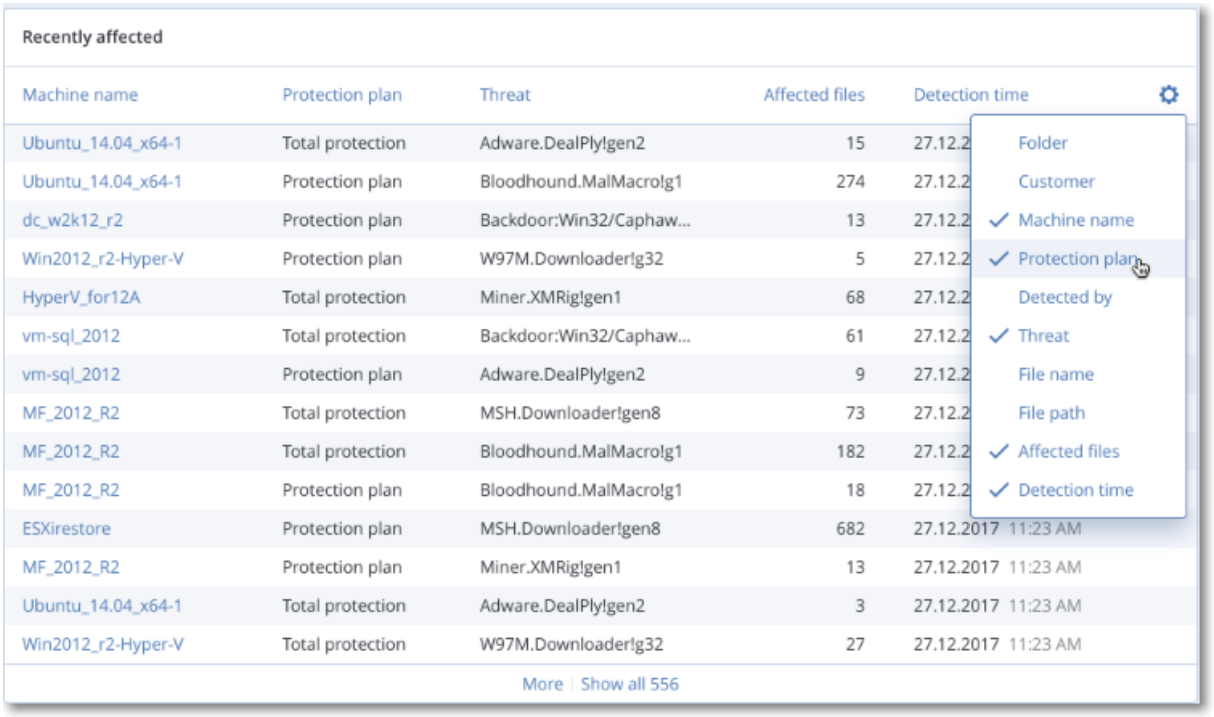
Backup scanning details (threats)

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	[blurred]	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	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	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	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	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	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	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	[blurred]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[blurred]	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	[blurred]	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。



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。

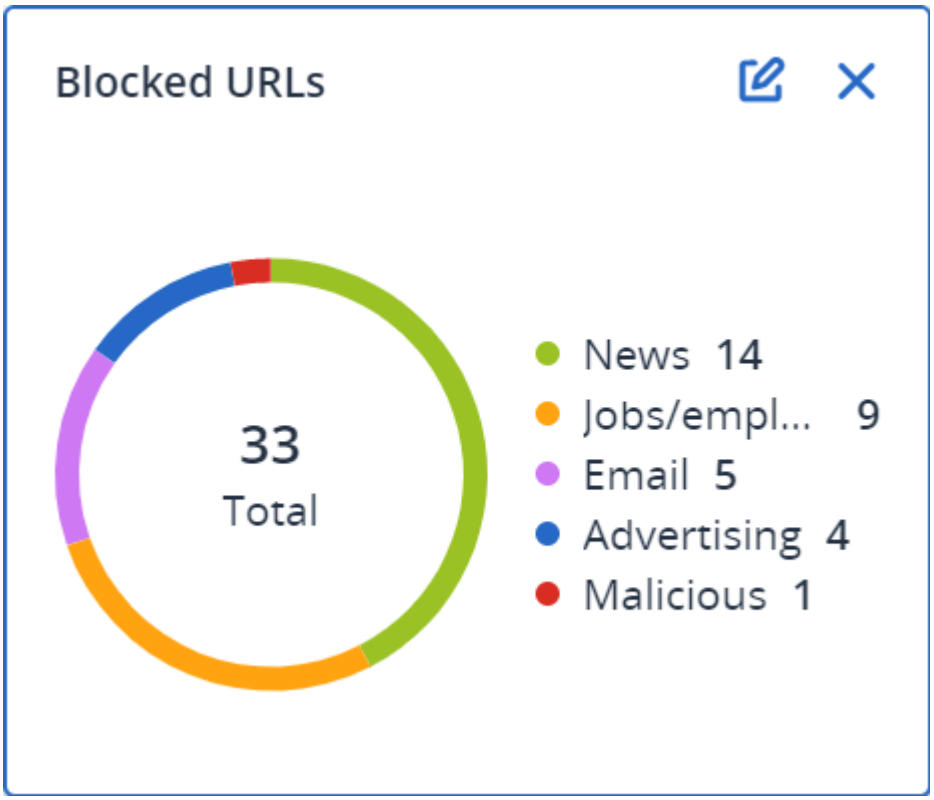
下载最近受影响工作负载的数据

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。

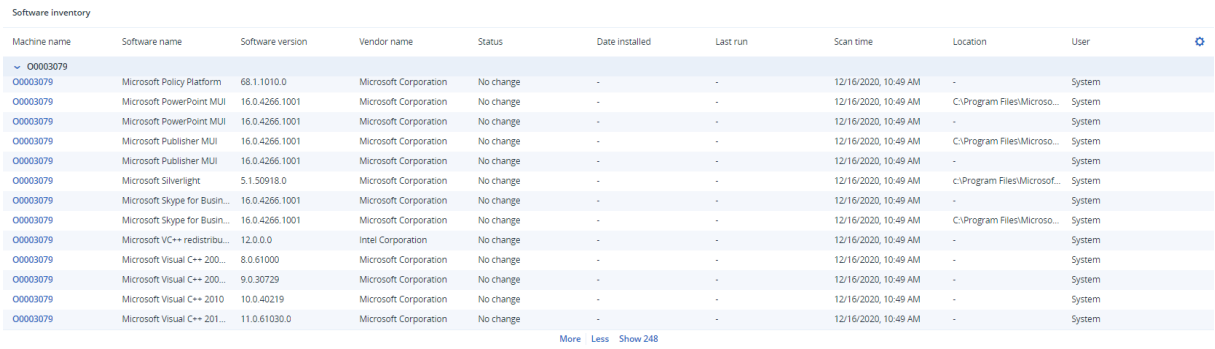
已阻止 URL

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”。

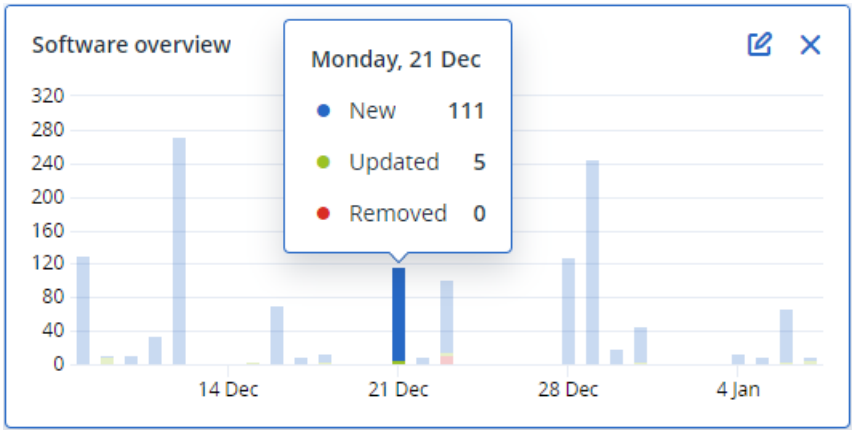


软件清查小组件

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



软件概述小组件会显示特定时段(7 天、30 天或当月)内贵组织中 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。

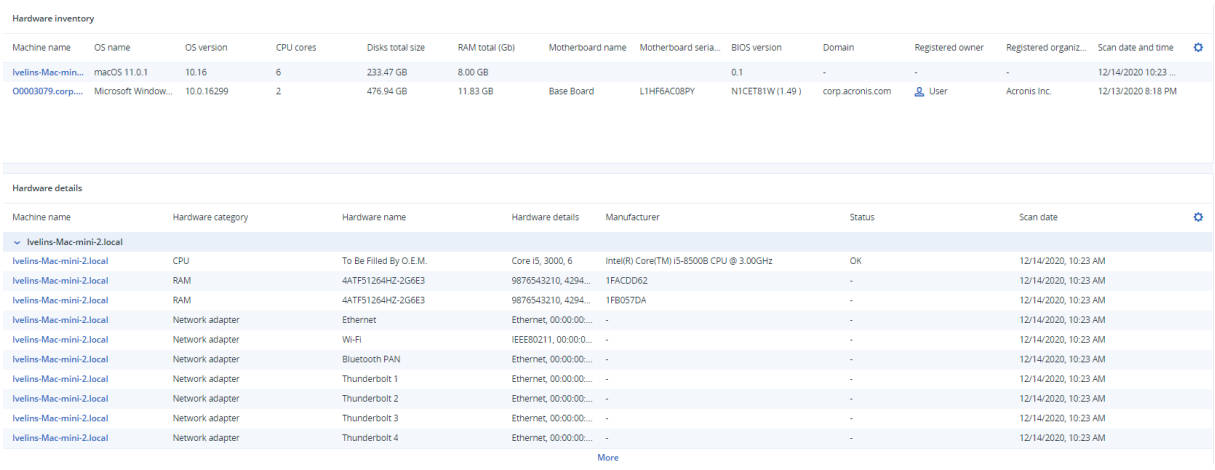
已更新 - 已更新应用程序的数量。

已删除 - 已删除应用程序的数量。

单击栏上特定状态的部分时，系统会将您重定向到**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贵组织中物理和虚拟 Windows 及 macOS 设备上安装的所有硬件的信息。



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

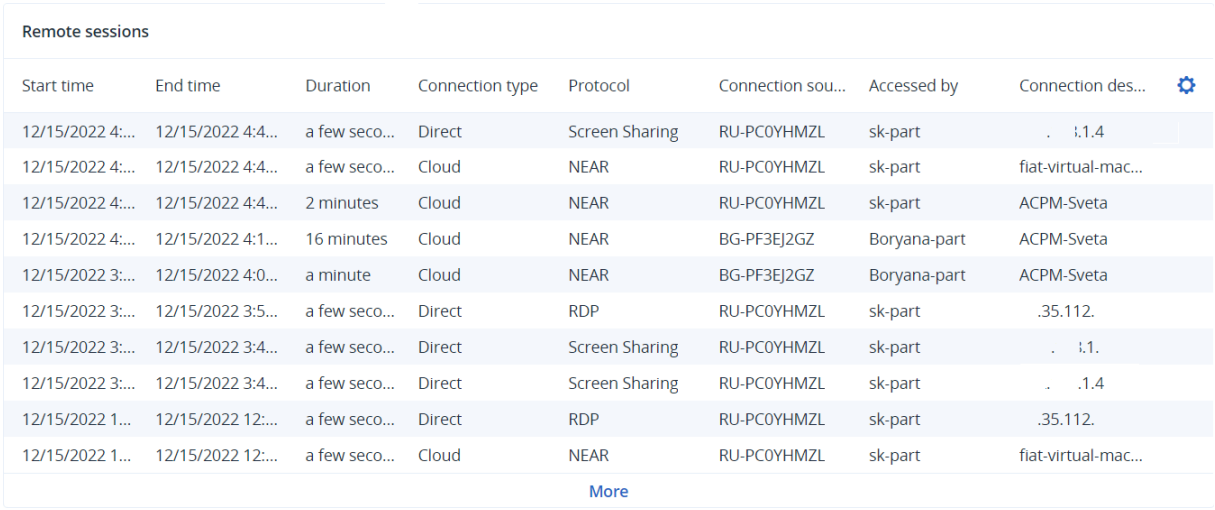
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

会话历史记录

该小组件会显示指定时间段内在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

审核日志

要查看审核日志，请转到**监视** > **审核日志**。

审核日志可提供以下事件的序时记录：

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

该日志显示组织或当前在运转的单位及其子单位中的事件。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**

  目标所属单位的名称。例如，**用户已更新**事件的租户是用户所在的单位。**配额已达到**事件的租户是其配额已达到的用户。
- **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**

  发起程序所属单位的名称。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。

报告

要访问关于服务使用情况和操作的报告，请单击**报告**。

注意
此功能在 Cyber Protection 服务的 Standard 版中不可用。

使用情况报告

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

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。
- **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公司或单位的直接子单位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公司或单位的所有子单位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公司或单位的所有子单位以及单位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。报告发送至公司或单元中的所有管理员，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公司或最上面的单位中进行操作。
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

自定义报告可以按需生成，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. 导航到您想要为其创建报告的单位。
3. 单击**报告** > **使用情况**。
4. 单击**自定义**。
5. 在**类型**中，选择报告类型。
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。
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**。

使用情况报告中的数据

有关使用 Cyber Protection 服务的报告包括公司或单位的以下相关数据：

- 按单位、按用户、按设备类型分类的备份大小。
- 按单位、按用户、按设备类型分类的受保护设备数。
- 按单位、按用户、按设备类型分类的价值。
- 备份的总大小。
- 受保护设备的总数。
- 总价值。

注意

如果 Cyber Protection 服务无法检测到设备类型，则该设备将在报告中显示为**未标明类型**。

操作报告

操作报告仅对在公司级别上进行操作的公司管理员可用。

关于操作的报告可以包括任何一组**操作**仪表板小部件。所有小组件都会显示整个公司的概要信息。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 65 页) 。

所有历史小组件都会显示同一时间范围内的数据。可以在报告设置中更改此范围。

可以使用默认报告，也可以创建自定义报告。

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

默认报告如下所示：

报告名称	描述
#CyberFit 分数(按计算机)	根据对每台计算机的安全指标和配置的评估，显示 #CyberFit 分数和改进建议。
警告	显示某一指定时间段内发生的警告。
备份扫描详细信息	显示有关备份中检测到威胁的详细信息。
每日活动	显示有关某一指定时间段内已执行活动的概要信息。
数据保护地图	显示有关计算机上所有重要文件的数量、大小、位置、保护状态的详细信息。
检测到威胁	按受阻止威胁的数量显示受影响计算机的详细信息，以及运行状况良好和易受攻击的计算机的详细信息。
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	显示有关贵组织中 Windows 和 macOS 计算机上安装的所有软件的详细信息。
硬件清查	显示有关贵组织中物理和虚拟 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组织中进行的远程桌面和文件传输会话的详细信息。

对报告的操作

要查看报告，请单击其名称。

添加新报告

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

若要编辑报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要编辑的报告。
   可以执行以下操作：
   - 重命名报告。
   - 更改报告中所有小组件的时间范围。
   - 指定报告收件人以及将报告发送给他们的时间。可用格式为 PDF 和 XLSX。

删除报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要删除的报告。
3. 单击省略号图标 (...)，然后单击**删除**。
4. 单击**删除**以确认选择。

若要安排报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要预定的报告，然后单击**设置**。
3. 启用**预定**开关。
   - 指定收件人的电子邮件地址。
   - 选择报告的格式。

     注意
     可以在 PDF 文件中导出多达 1000 个项目，在 XLSX 文件中导出多达 10000 个项目。PDF 和 XLSX 文件中的时间戳使用计算机的本地时间。

   - 选择报告的语言。
   - 配置预定。
4. 单击**保存**。

下载报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择报告，然后单击**下载**。
3. 选择报告的格式。

发送报告

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

导出报告结构

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

因此，报告结构将作为 JSON 文件保存在计算机上。

转储报告数据

通过使用此选项，可以将自定义期间未过滤的所有数据导出为 CSV 文件，并将该 CSV 文件发送给电子邮件收件人。

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

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

   注意
   准备较长时间段的 CSV 文件需要花费更多时间。

6. 单击**发送**。

执行摘要

执行摘要报告提供指定时间范围内组织环境和受保护设备的保护状态的概述。

执行摘要报告包括可自定义的部分，带有动态小组件，可以显示与以下云服务的使用情况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、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。

执行摘要小组件

可以从执行摘要报告中添加或删除部分和小组件，从而控制报告中包含哪些信息。

工作负载概述小组件

下表提供了有关**工作负载概述**部分中小组件的更多信息。

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

小部件	描述
	的 OneDrive 服务，则它们全都属于“用户”工作负载组。这些工作负载的总数是 10 500，超过了工作负载组 10 000 的限制。因此，小组件将隐藏相应的工作负载类型：Microsoft 365 邮箱和 Microsoft 365 OneDrive。
网络安全保护摘要	小组件显示指定时间范围内网络安全保护性能的关键指标。 **已备份数据** - 云和本地存储中创建的存档的总大小。 **缓解的威胁** - 所有设备中阻止的恶意软件总数。 **阻止的恶意 URL** - 所有设备上阻止的 URL 总数。 **已修补的漏洞** - 在所有设备上通过软件修补程序安装修复的漏洞总数。 **安装的修补程序** - 所有设备上安装的修补程序总数。 **DR 保护的服务器** - 受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**。

反恶意软件保护小组件

下表提供了有关**威胁防御**部分中小组件的更多信息。

小部件	描述
文件的反恶意软件扫描	小组件显示指定日期范围内，设备的按需反恶意软件扫描结果。 **文件** - 已扫描文件的总数 **干净** - 干净文件的总数 **检测到，已隔离** - 已隔离的被感染文件的总数 **检测到，未隔离** - 未隔离的被感染文件的总数 **受保护的设备** - 应用了反恶意软件保护策略的设备的总数 **注册设备的总数** - 报告生成时注册设备的总数
备份的反恶意软件扫描	小组件使用以下指标，显示指定日期范围内备份的反恶意软件扫描结果： • 扫描的恢复点的总数 • 干净恢复点的数量 • 具有不受支持分区的干净恢复点的数量 • 被感染的恢复点的数量。此指标包括具有不受支持分区的被感染恢复点的数量。
阻止的 URL	在指定日期范围内，小组件显示按网站类别分组的阻止的 URL 数。 小组件列出了具有阻止的 URL 最大数的七个网站类别，把其余的网站类别都归入**其他**。 有关网站类别的更多信息，请参阅 Cyber Protection 中的 URL 过滤主题。
安全性事件刻录	此小组件显示选定公司的关闭事件中的效率；针对一段时间的关闭事件的数量测量打开事件数。 将鼠标悬停在某列上可以查看在选定日发生的关闭和打开事件的明细。在括号中显示的 % 值表示与以前时间段比较的上升或下降。
事件 MTTR	此小组件显示用于安全性事件的平均解决时间。它指示调查和解决事件的快速程度。 单击某个列以根据严重性(**严重**、**高**和**中**)查看事件明细，并可查看解决不同严重性级别花费多少时间的指示。在括号中显示的 % 值表示与以前时间段比较的上升或下降。
威胁状态	此小组件显示公司工作负载的当前威胁状态(不管工作负载数)，并突出显示当前未迁移并需要调查的事件数量。小组件还指示已迁移的事件数(由系统手动和/或自动)。
保护技术检测到的威胁	在指定日期范围内，小组件显示按以下保护技术分组的检测到的威胁数： • 反恶意软件扫描 • 行为引擎 • 加密挖矿防护 • 漏洞利用预防 • 勒索软件主动防护 • 实时保护 • URL 过滤

备份小组件

下表提供了有关**备份**部分中小组件的更多信息。

小部件	描述
备份的工作负载	小组件按备份状态显示已注册工作负载的总数。 **已备份** - 在报告日期范围内，已备份（至少执行了一次成功的备份）的工作负载数。 **未备份** - 在报告日期范围内，未备份（未执行成功的备份）的工作负载数。
磁盘运行状况（按物理设备）	小组件基于物理设备磁盘的运行状况状态，显示物理设备的汇总运行状况状态。 **正常** - 此磁盘运行状况状态与值 [70-100] 相关。当该设备的所有磁盘的状态都是**正常**时，该设备的状态为**正常**。 **警告** - 此磁盘运行状况状态与值 [30-70] 相关。当至少一个磁盘的状态为**警告**时，以及当没有磁盘的状态为**错误**时，设备的状态为**警告**。 **错误** - 此磁盘运行状况状态与值 [0-30] 相关。当至少一个磁盘的状态为**错误**时，设备的状态为**错误**。 **正在计算磁盘数据** - 当设备的磁盘状态是尚未计算时，该设备的状态是**正在计算磁盘数据**。
备份存储使用情况	在指定的时间范围内，小组件显示云和本地存储中备份的总数和总大小。

漏洞评估和修补程序管理小组件

下表提供了有关**漏洞评估和修补程序管理**部分中小组件的更多信息。

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

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

公证小组件

下表提供了有关**公证**部分中小组件的更多信息。

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

配置执行摘要报告的设置

可以更新在创建执行摘要报告时配置的报告设置。

更新执行摘要报告的设置

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

创建执行摘要报告

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

创建执行摘要报告的步骤

1. 在管理中控台中，转至**报告** > **执行摘要**。
2. 单击**创建执行摘要报告**。
3. 在**报告名称**中，键入报告的名称。

4. 选择报告的收件人。
   - 如果要将报告发送给所有联系人和用户，则选择**发送给所有联系人和用户**。
   - 如果要将报告发送给特定联系人和用户
     a. 清除**发送给所有联系人和用户**。
     b. 单击**选择联系人**。
     c. 选择特定联系人和用户。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 62 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 (小部件)	• 报告生成的时间是浏览器运行时所在计算机的时区。 • 报告中显示的活动的时区为 UTC。
管理门户> 报告 > 操作 (导出为 PDF 或 xslx)	• 导出的报告的时间戳是在用于导出报告的计算机所在的时区中。 • 报告中显示的活动的时区为 UTC。
管理门户> 报告 > 操作 (预定交付)	• 报告交付的时区为 UTC。 • 报告中显示的活动的时区为 UTC。
管理门户> 用户 > 活动警告的每日概述	• 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

集成

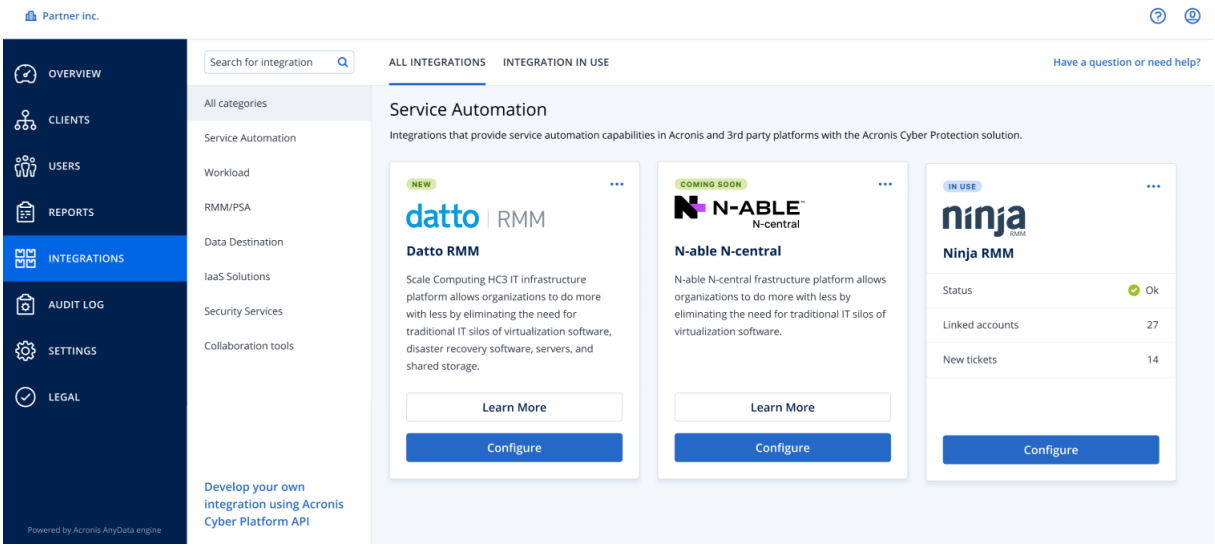
集成目录

此页面用作注册和更新所有集成应用程序的全局位置。
在此处，可以添加新集成或修改现有集成。

注意
只有具有**公司管理员**角色的用户才能更改集成配置。

所有集成

所有集成选项卡会显示所有当前可用的集成列表，并以磁贴形式层叠排列。



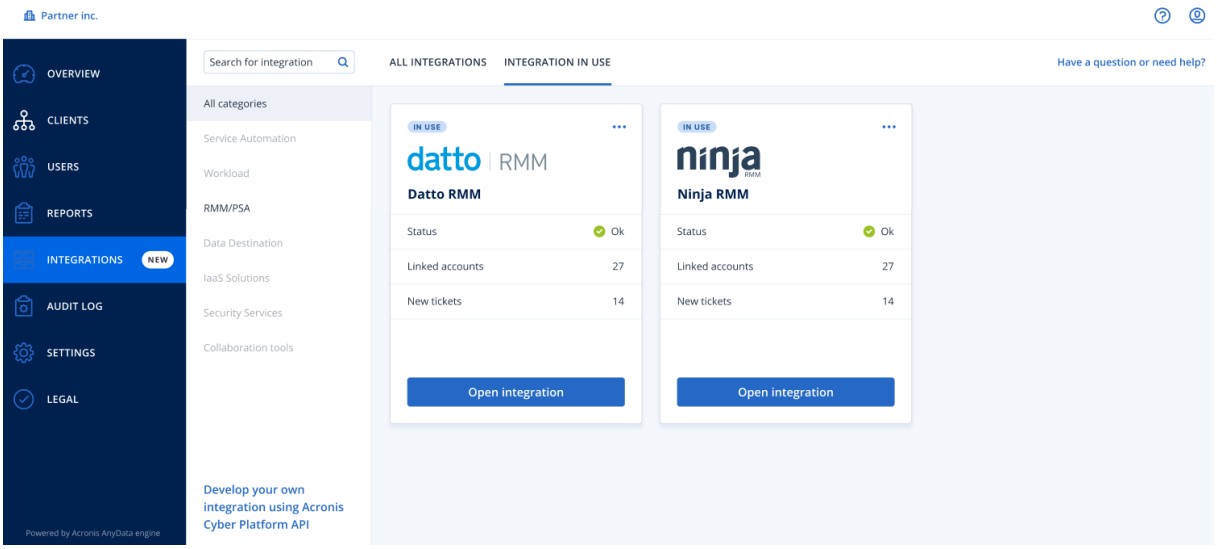
每个磁贴会显示一个简短的产品描述和两个附加选项：

- **了解更多** - 单击此按钮可查看有关特定集成的更多详细信息：
  - **集成功能**
  - **文档链接**
  - **支持联系人**
- **配置** - 使用此选项可编辑一些集成设置。

表示非活动集成的磁贴会灰显并处于禁用状态，并且可能带有**“即将推出”**标签。

集成正在使用

集成正在使用选项卡会显示当前正在使用的所有集成的列表，每个集成都附有一些一般信息。



单击**打开集成**可直接访问对应的应用程序。

在左侧，有一个集成类别列表，其中所有现有应用程序都会分类为某些组，例如服务自动化、工作负载、RMM/PSA 等。单击每个单独的类别会显示属于该特定组的集成。当前查看的类别会亮显。

使用**搜索**选项可查询并查找您选择的集成。

可以按类别和标签过滤集成列表。标签按字母顺序排序。如果未找到任何结果，请扩大搜索范围以包括更多类别。

要禁用应用程序，请单击磁贴右上角的省略号 (...) 图标，然后选择**停用**。

如果您有兴趣开发自己的集成，还可以使用指向 Acronis API 文档的链接。

限制对 Web 界面的访问

您可以限制对 Web 界面的访问，方法是指定允许用户用于登录的 IP 地址列表。

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。不适用于子单位的成员。

限制对 Web 界面的访问

1. 登录管理门户。
2. 导航到您想要限制其访问的单位。
3. 依次单击**设置** > **安全**。
4. 选中**启用登录控制**复选框。
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**。

限制对您公司的访问

公司管理员可以限制更高级别的管理员对公司的访问。

如果对公司的访问受到限制，则更高级别的管理员只能修改公司属性。他们完全看不到用户帐户和子单位。

限制对公司的访问

1. 登录管理门户。
2. 依次单击**设置** > **安全**。
3. 禁用**支持访问**选项。
4. 单击**保存**。

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。

索引