Device Control Plus
快速用户手册

ME 产品部
2023-09-05

本文档旨在帮助用户快速熟悉产品的使用方法。

目录

1. 简介

对于任何可移动设备（例如 USB），数据盗窃都是一个步骤：插入接口。Device Control Plus 是一个全面的数据泄漏防护解决方案，可控制阻止和监视 USB 和外围设备，以防止他人未经授权访问敏感数据，能够对内置和外部进行详细的扫描和监视集中管理网络中所有端点上的设备。

直接跟踪网络中各种类型的内部和外围设备，可以将这些设备分类为信任和不信任，并关联策略以防止未经授权的访问，Device Control Plus 可以从单个控制台进行所有操作。这个消除了使用多个软件应用程序的需要，从而启用端到端设备控制和信息安全功能。

Device Control Plus 可帮助您：

- 快速检测多达 18 种类型的内置设备和外围设备
- 将设备分类为受信任和不信任
- 自助服务门户，用于临时访问请求
- 未经授权接入的设备引发提示警报
- 文件访问控制（授予以下级别的访问权限：设备和用户）
- 文件跟踪（跟踪从中交换的信息设备/系统并根据文件大小，扩展名等设置适当的数据传输条件）
- 基于角色的策略管理自定义组，操作简便且提升效率
- 直观的仪表板，可对网络进行汇总分析
- 执行报告详细展示终端和设备状态

2. 系统安装

1. 访问以下链接下载安装包
https://www.manageengine.com/device-control//download_confirm.html

服务器硬件要求：

Device Control Plus 服务器的硬件要求：

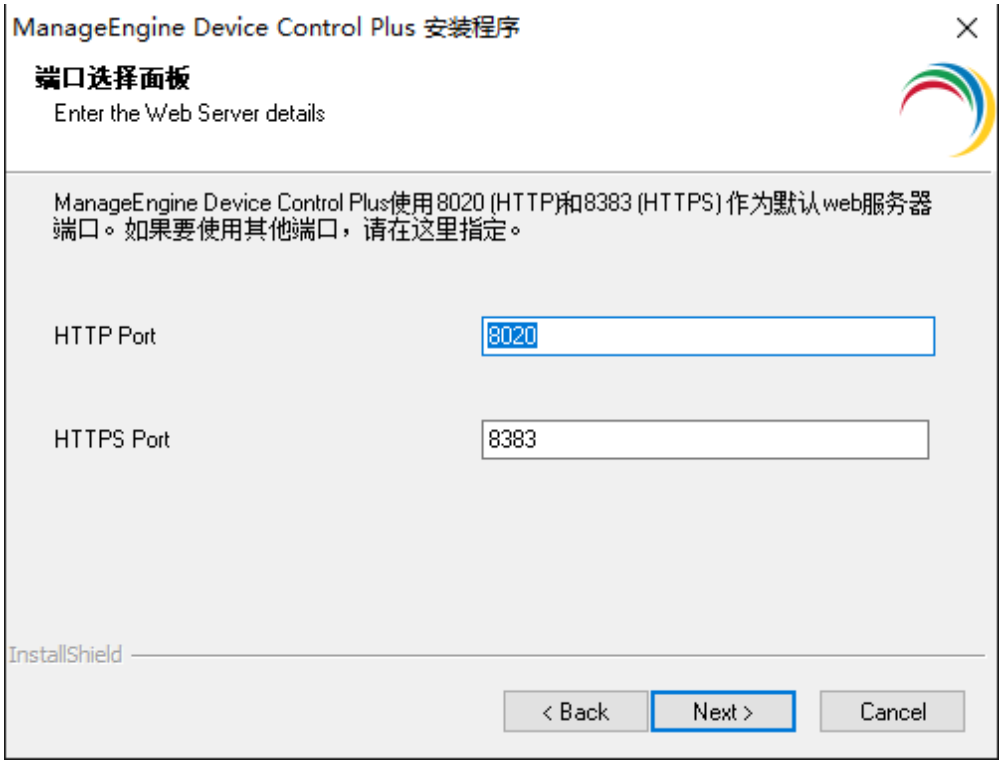
设备数量	处理器	内存	磁盘空间
1-250	Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache	2GB	5GB
251-500	Intel Core i3 (2 core/4 thread) 2.4 Ghz 3 MB cache	4GB	10GB
501-1000	Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MB cache	4GB	20GB
1001-3000	Intel Core i5 (4 core/4 thread) 2.3 GHz. 6 MB cache	8GB	30GB
3001-5000	Intel Core i7 (6 core/12 thread) 3.2 GHz. 12 MB cache	8GB	40GB
5001-10000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 20 MB cache	16GB	60GB
10000-20000	Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 40 MB cache	32GB	120GB

2. 在安装包下载完成后，关闭杀毒软件，用户可以手动双击安装包进入安装向导，根据向导中的提示进行安装操作。

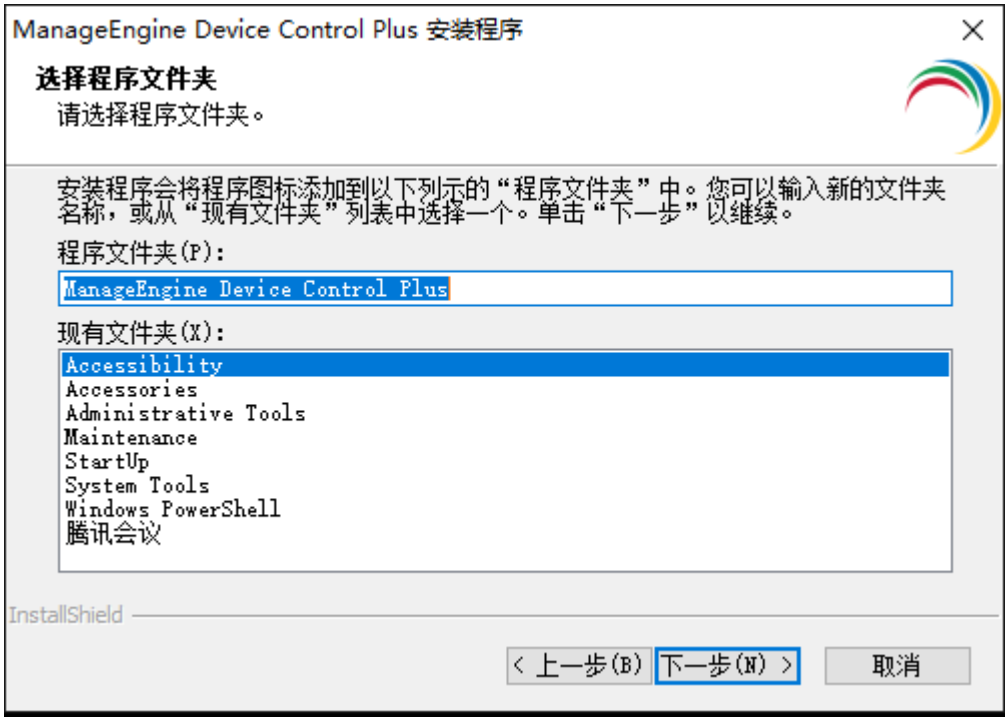

ManageEngine Device Control Plus 安装程序
欢迎使用 ManageEngine Device Control Plus InstallShield Wizard
InstallShield(R) Wizard 将在计算机中安装 ManageEngine Device Control Plus。若要继续，请单击“下一步”。
< 上一步(B)
下一步(N) >
取消


ManageEngine Device Control Plus 安装程序
许可证协议
请仔细阅读下面的许可证协议。
按 PAGE DOWN 键以查看协议的剩余部分。
TERMS OF SALE FOR MANAGEENGINE SOFTWARE PRODUCTS
1. Your Acceptance of the Terms of Sale
Thank you for visiting the Zoho Corporation Private Limited ("we" or "Zoho") website, www.manageengine.com (the "Website"). This document ("Terms of Sale") is a legal agreement between you or the entity that you represent ("you") and Zoho, and governs your download and purchase of ManageEngine software products from the Website.
PLEASE NOTE THAT YOUR USE OF THE WEBSITE TO DOWNLOAD A SOFTWARE PRODUCT CONSTITUTES ACCEPTANCE OF THE TERMS OF SALE, AND TERMS AND CONDITIONS OF THE END USER LICENSE AGREEMENT PROVIDED BELOW. IF YOU DO
是否接受上述许可证协议中的全部条款？如果选择“否”，则安装程序将关闭。要安装 ManageEngine Device Control Plus，必须接受本协议。
打印(P)
InstallShield
< 上一步(B)
是(Y)
否(N)

3. 选择访问端口号：



4. 选择程序菜单文件夹。



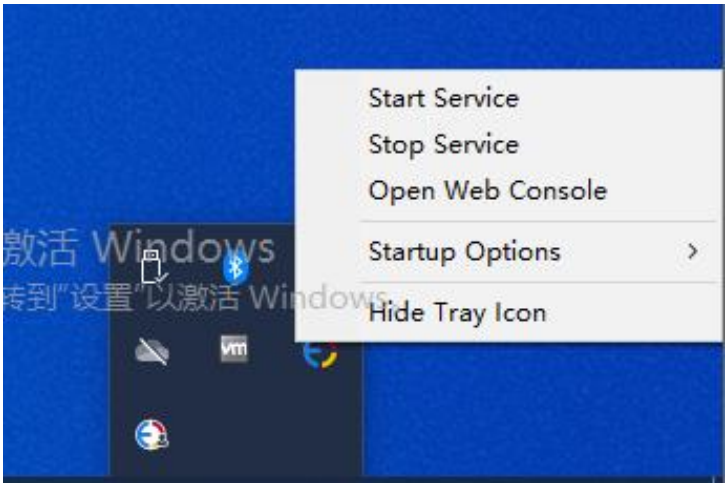
5. 完成以上操作之后，Device Control Plus 开始安装。完成后显示:

6. 选择“是的，启动 Device Control Plus”即可自动启动该系统。点击完成即可结束安装。

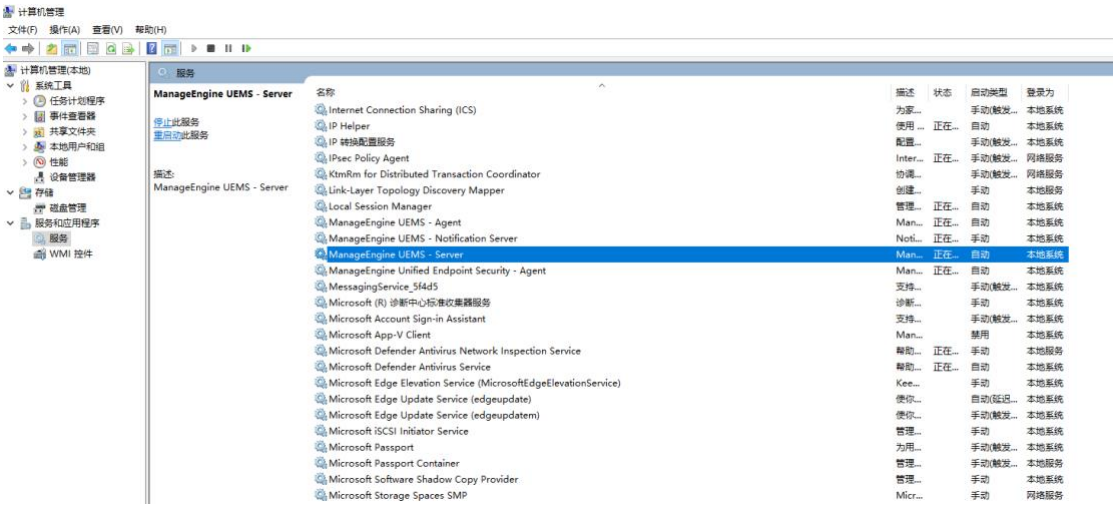
2.1 启动 Device Control Plus

Device Control Plus 可以通过如下方式启动：

- 方式一：桌面图标启动：双击桌面上的“Start Service”图标启动；



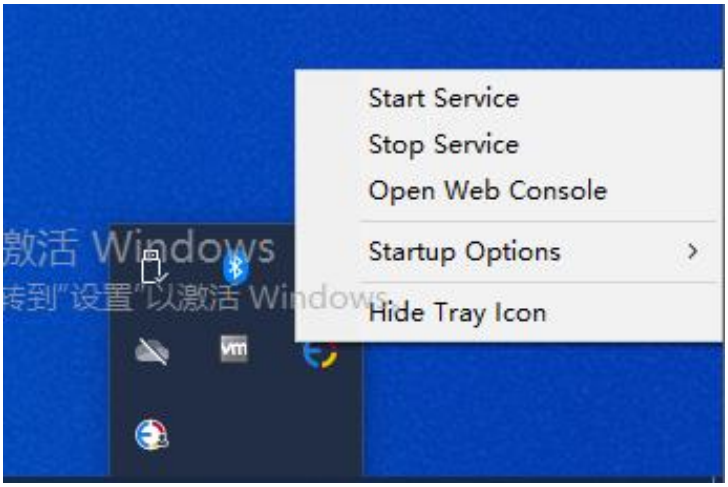
- 方式二：服务启动：打开 windows 的服务，在服务列表中找到 ManageEngine UEMS - Server 服务，打开其属性并点击‘启动’；



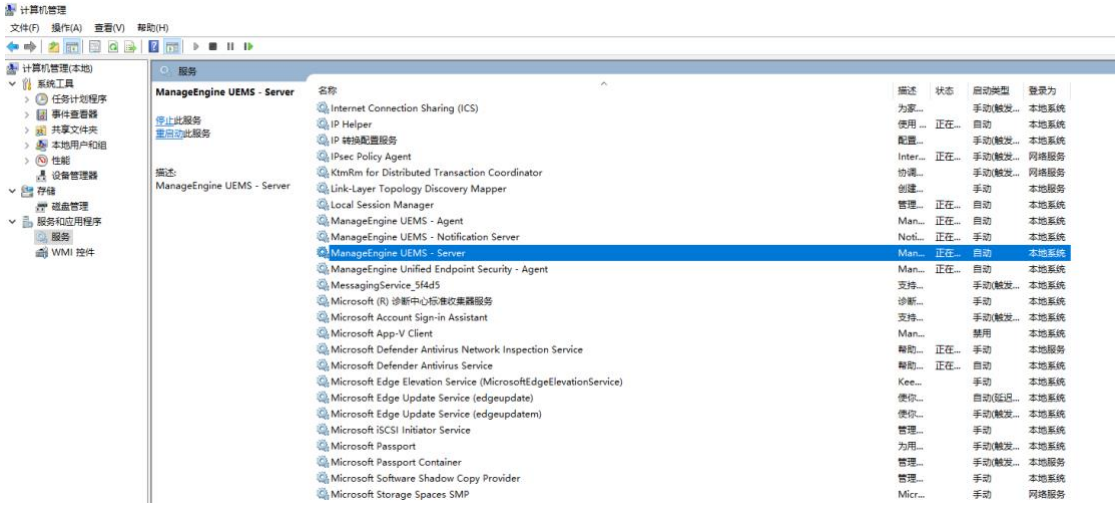
2.2 关闭 Device Control Plus

Device Control Plus 可以通过如下方式关闭：

- 方式一：右击系统托盘中的 Device Control Plus 图标，在弹出的选项中选择“Stop Service”



- 方式二：打开 windows 系统的服务列表，关闭 Manage EngineUEMS - Server 的服务；



2.3 登录 Device Control Plus

在启动完成后用户便可以访问客户端登录 Device Control Plus。Device Control Plus 基于 B/S 架构开发，所以支持基于 WEB 页面的访问，所以用户可以打开浏览器，在地址栏中输入：

http://server:port

来访问 Device Control Plus 的客户端，其中链接中的“server”是指 Device Control Plus 所安装的服务器的 DNS 名称或者 IP 地址，端口就是在安装的过程中配置的 web 端口，例如 Device Control Plus 服务器的 DNS 名称叫 Device Control Plus， web 端口使用的是 8020，那么我们可以通过访问

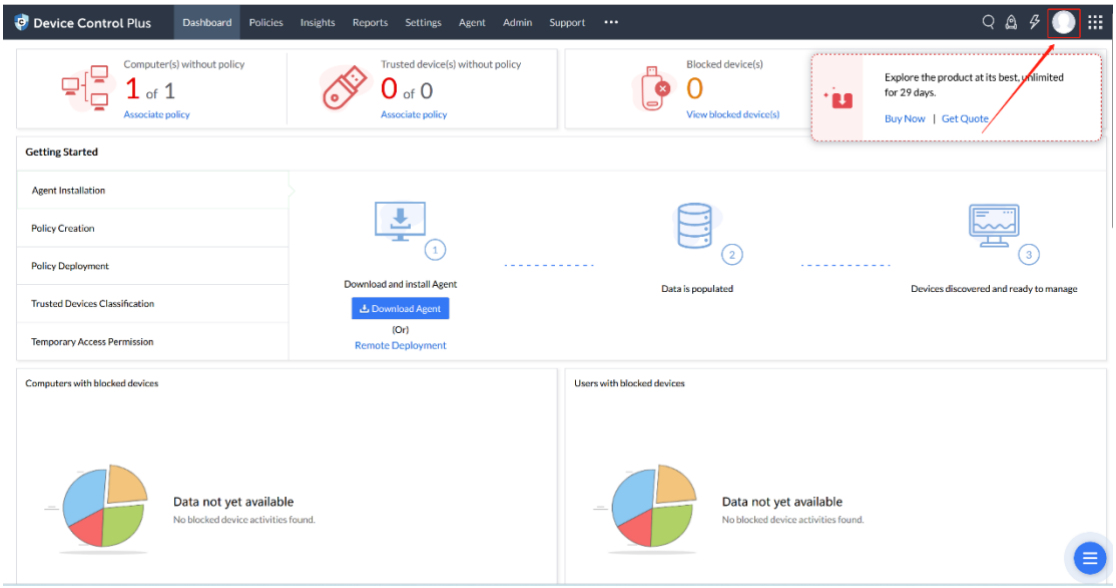
http://192.168.1.12:8020

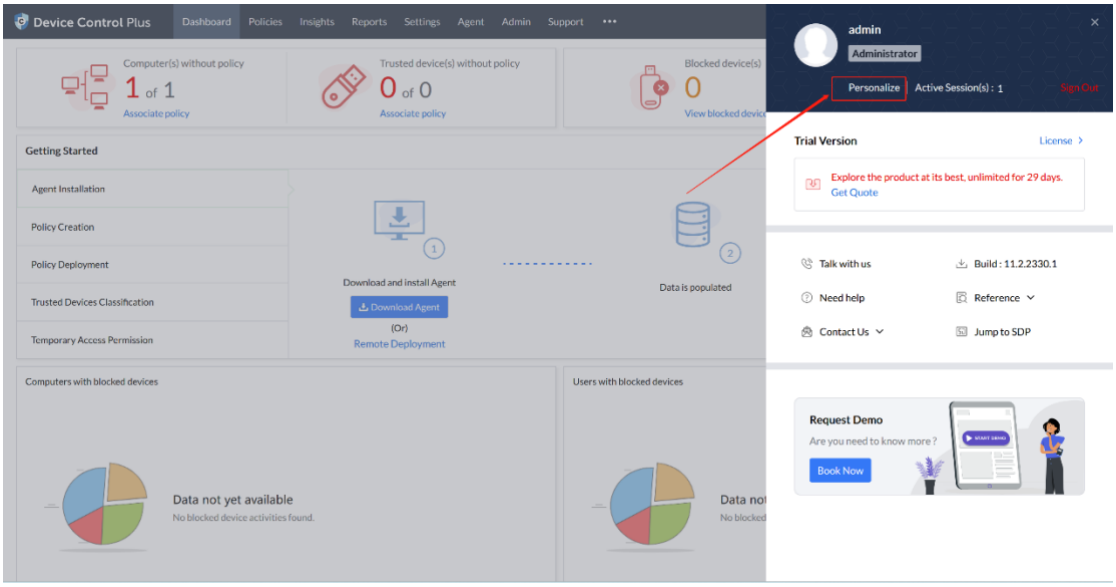
来访问 Device Control Plus 的客户端。当然，如果用户在 Device Control Plus 服务器上访问 Device Control Plus 的客户端，可以使用:

http://localhost:8020

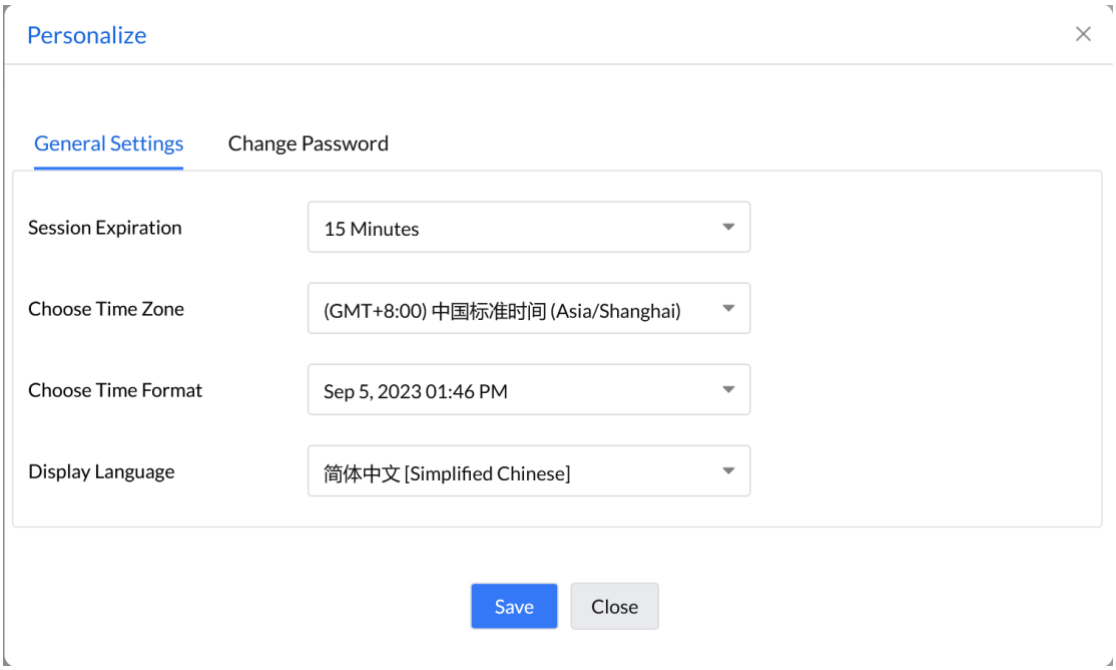
来进行访问。系统默认账号为 admin/admin。

1) 点击右上角用户图像，Personalize





2) Display Language 选择简体中文。Save>Refresh，界面切换为中文。



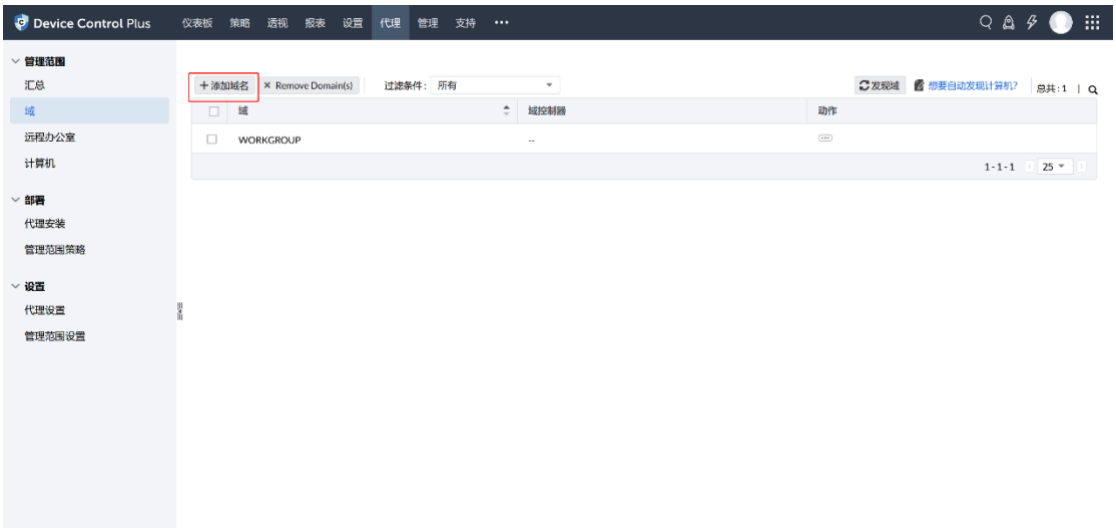
3. 添加计算机

Device Control Plus 系统通过代理的方式与客户机通信，将计算机添加到系统时，客户机同时安装代理。

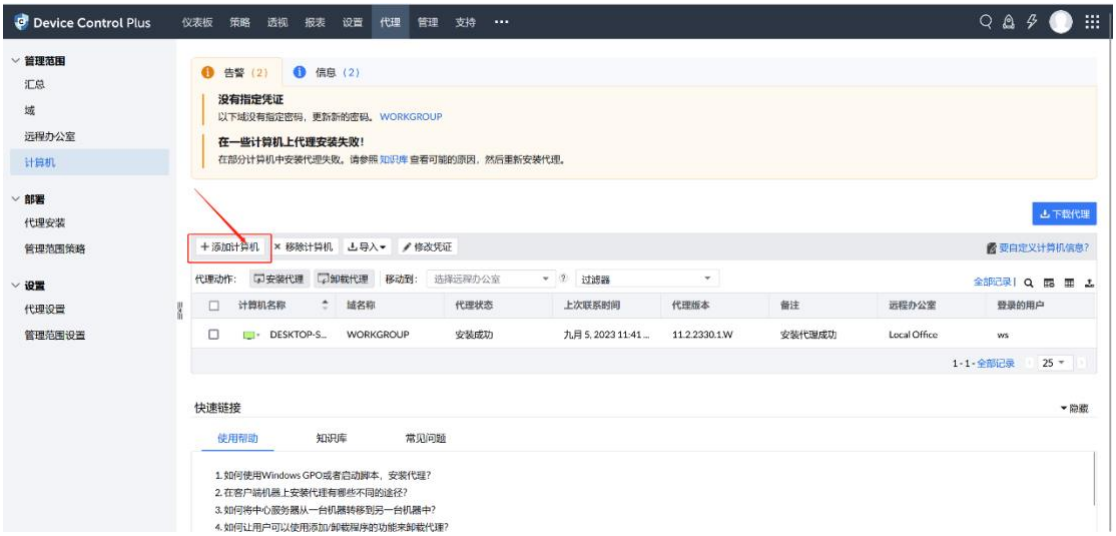
3.1 添加 Windows 计算机

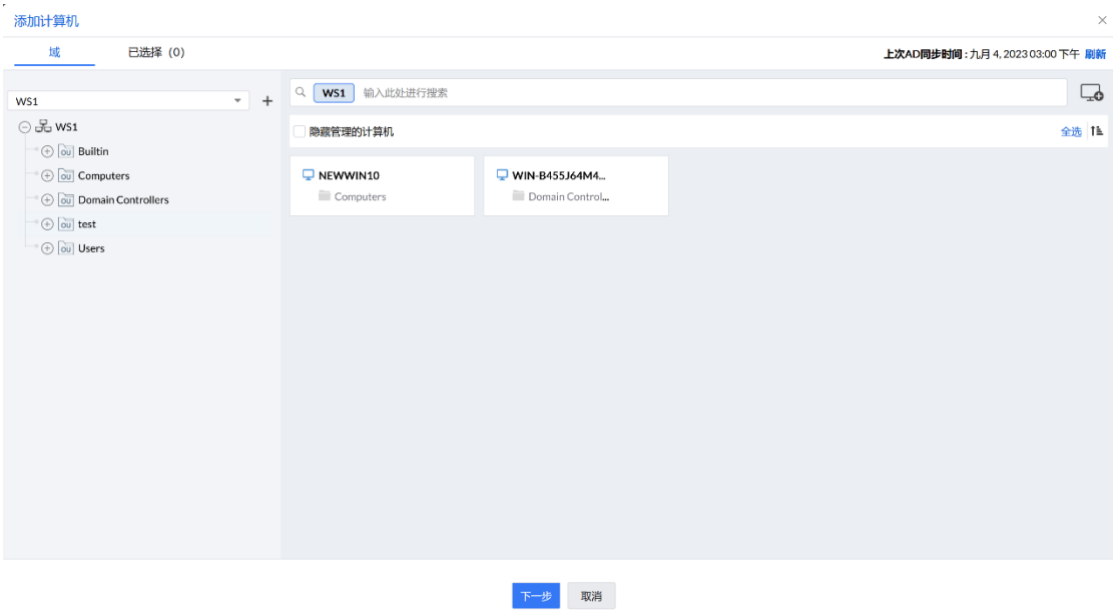
➢ 有 AD 域/工作组环境

管理员登录系统后，打开“代理 – 域”，选择计算机，点击添加计算机，添加 AD 域/工作组，将域/工作组信息填写完成后，点击选择计算机，将客户机添加入系统中，并安装代理。



添加域/工作组信息后，在计算机页面即可直接选择计算机自动安装代理

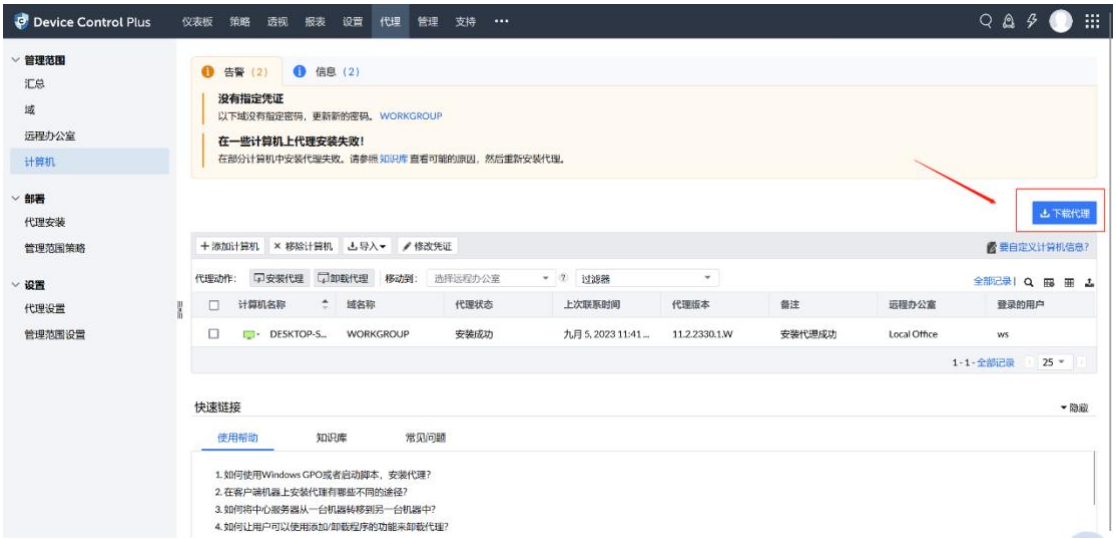


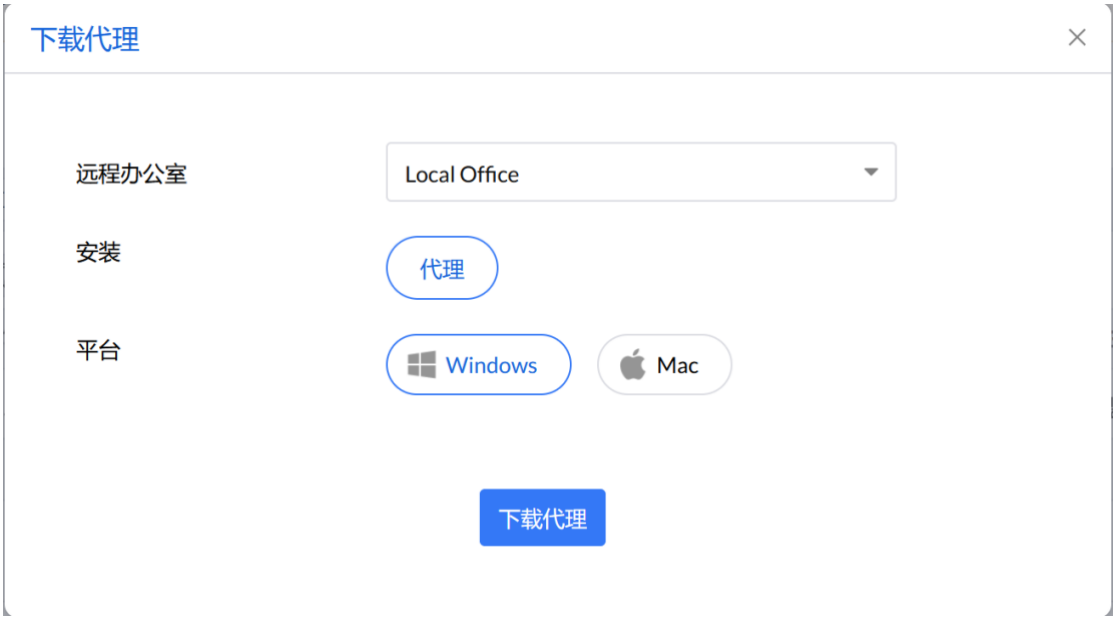


➢ 无 AD 域/工作组环境

管理员登录系统后，在页面导航中选择“代理”，选择计算机，点击下载代理，选择 Windows 本地代理（或某个远程办公室代理）。将下载的文件拷贝到客户机，运行并安装。

成功安装代理后，Windows 计算机将列在 Endpoint Central Web 控制台的代理-计算机页面中



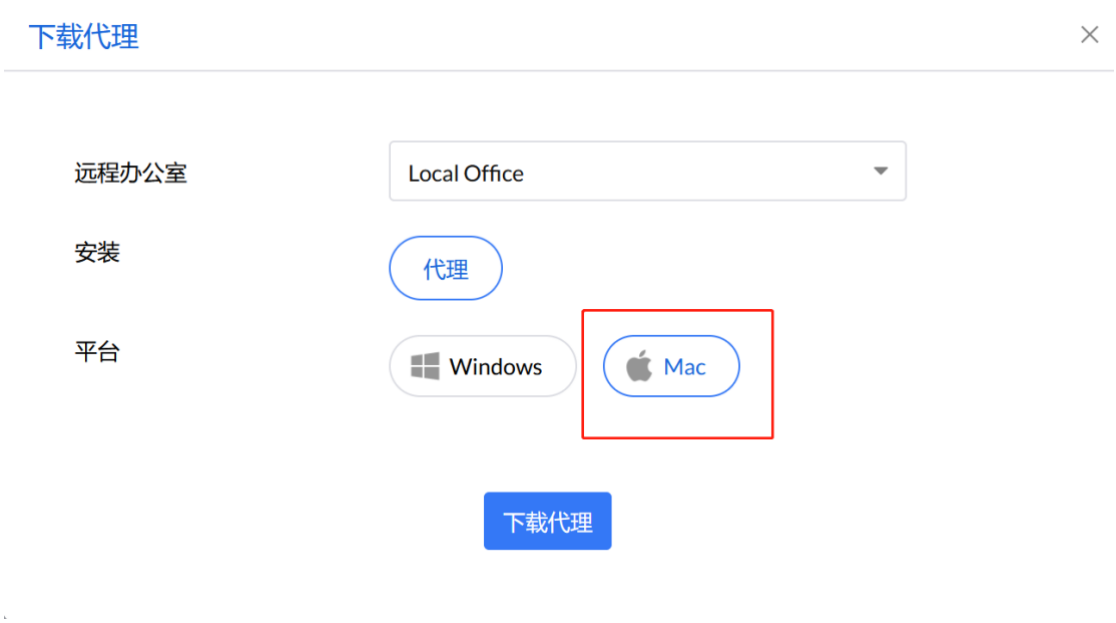


安装成功后，计算机自动加入 Device Control Plus。

3.2 安装 MAC 代理

管理员登录系统后，在页面导航中选择“代理”，选择计算机，点击下载代理，选择 MAC 本地代理（或某个远程办公室代理）。将下载的文件拷贝到客户机

在 Mac 计算机上以管理员身份登录计算机，解压缩下载的文件，运行 pkg 文件安装。更多信息可以查看该压缩包中的说明文档



4. 策略设置

设备控制主要是管理连接到计算机的外部设备。比如是否允许某个 USB 设备的连接。或者临时给某个设备访问权限

4.1 工作流程

1）这里设置具体的外部设备管理策略以及把策略部署到目标机器。通常来说，其工作流程是：

1.代理发现设备

2.管理员设置信任的设备列表

3.管理员创建策略来执行“允许”或“禁止”操作。

4.把策略部署到被管计算机。

5.被管计算机上的代理执行策略。

2）往往有些非可信设备需要临时能被使用，那么就要用到“临时访问”。临时访问可以是管理员主动添加；也可以是用户从代理发起的访问请求，其流程为：

1.用户从代理发起临时访问请求

2.服务器将请求通知给管理员

3.管理员审批

4.代理根据管理员的审批来允许和阻止对设备的访问。

5.以下是对策略和临时访问的详细操作说明。

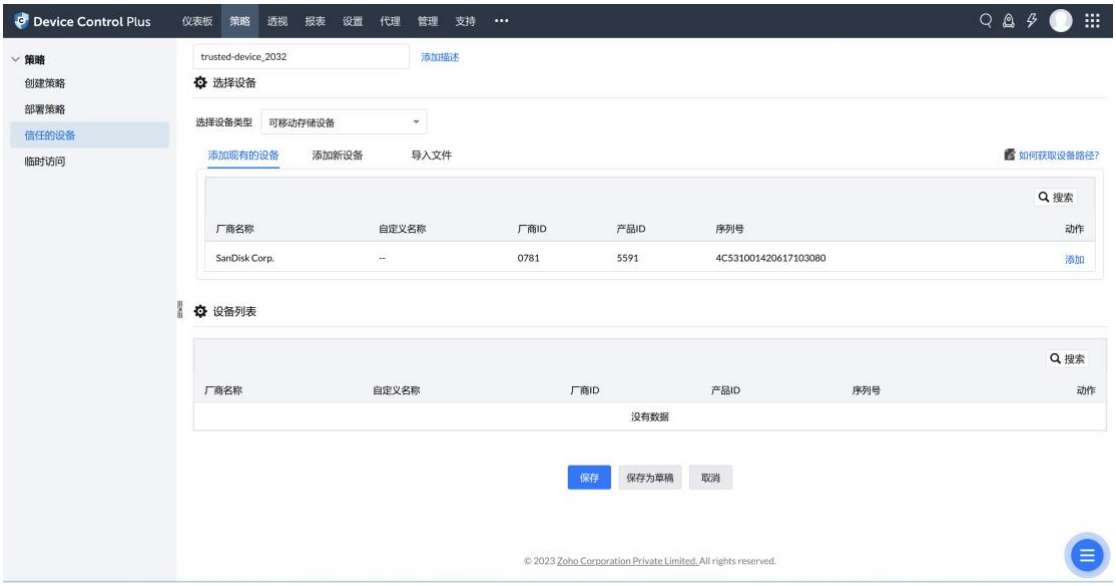
4.2 信任的设备

这里是创建可信的设备列表。可信设备列表用于后面的策略中使用。

登录 Endpoint Central 的 Web 控制台，点击“策略 – 信任的设备”，点击添加新列表或者修改已有列表。选择“设备类型”。具体的设备添加有三种方式

4.2.1 添加现有设备

现有的设备是代理程序从当前管理的计算机中扫描到的设备。点击某个设备后的“添加”链接来添加到列表中。

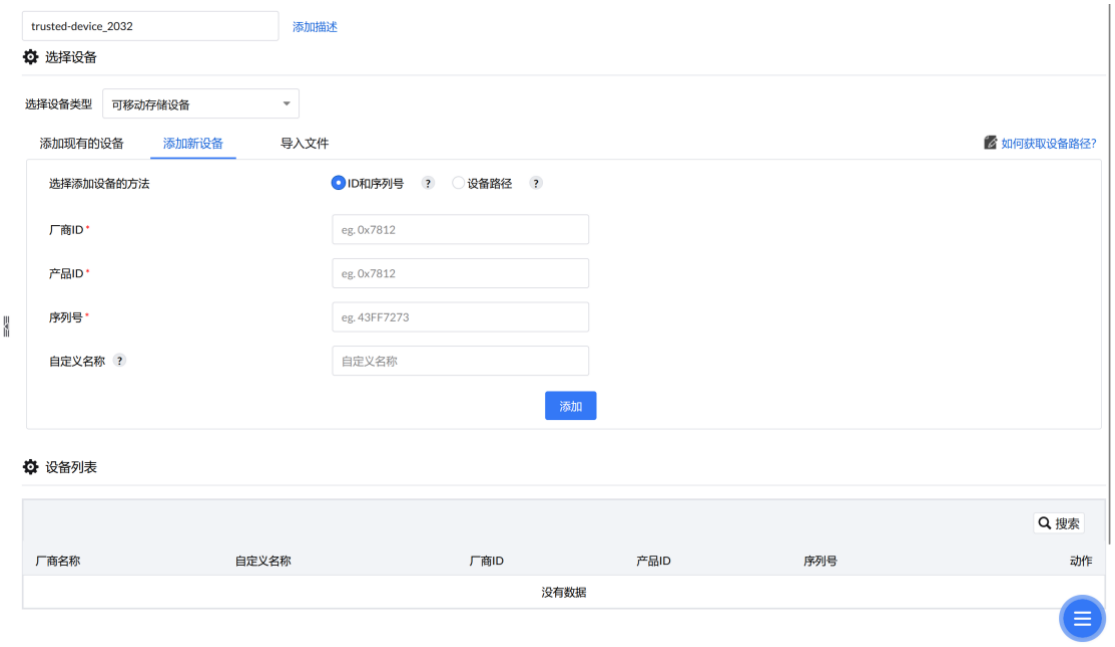


4.2.2 添加新设备

添加新设备是要手动输入设备信息。可以输入“厂商 ID 和序列号”；或者输入“设备路径”。

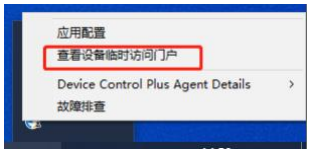
1.“厂商 ID 和序列号”：

说明：下图中的“序列号”可以使用通配符*，来批量设置设备。

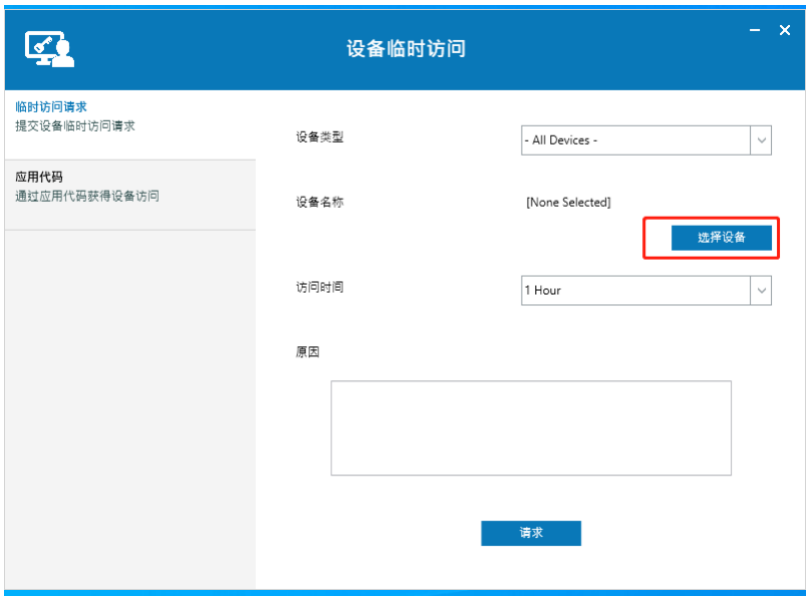


如何获取设备的“厂商 ID”、“产品 ID”和“序列号”？

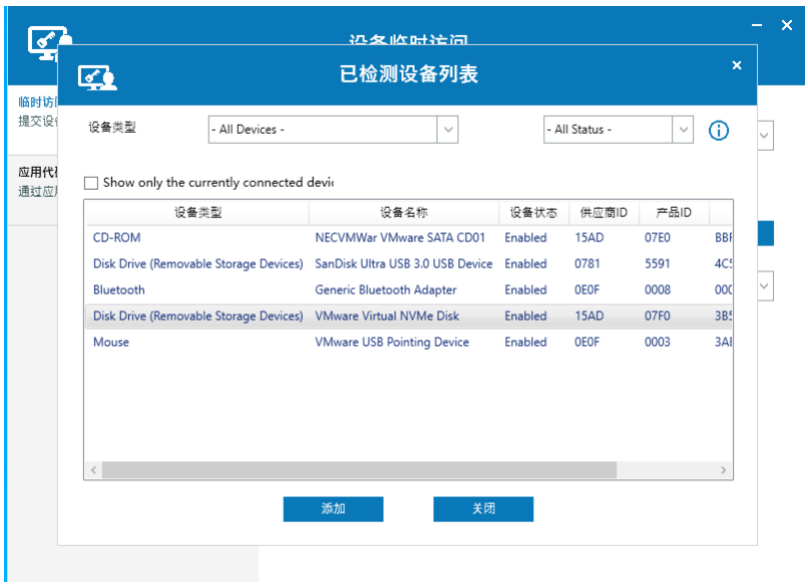
在一个被管计算机上，点击代理托盘图标菜单中的“查看设备临时访问门户”



在打开的窗口中点击“选择设备”

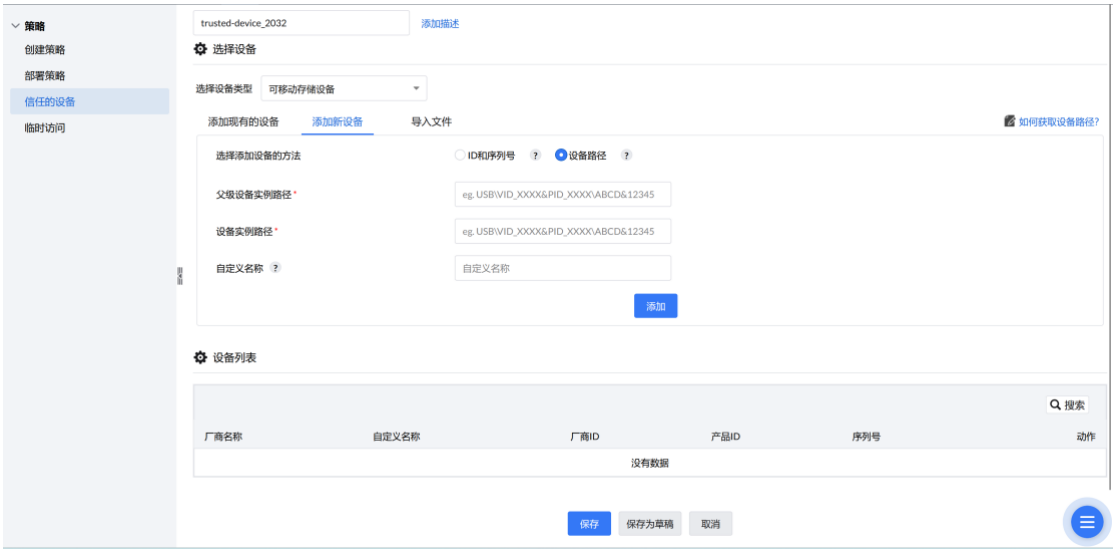


可以找到这个设备的所有信息



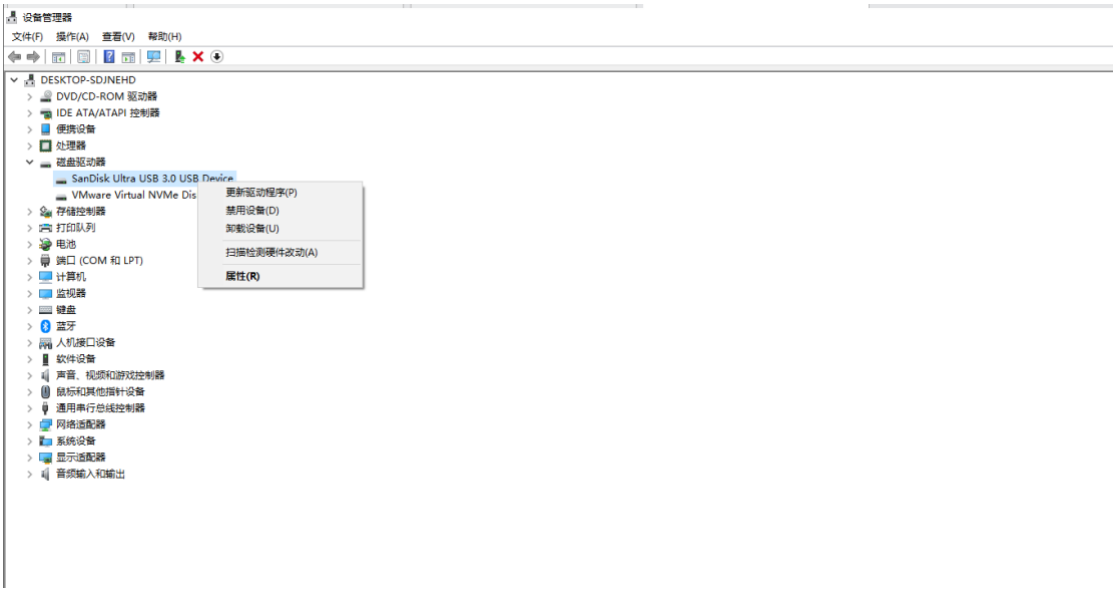
2.“设备路径”：

如果添加新设备的时候选择了“设备路径”，如下图

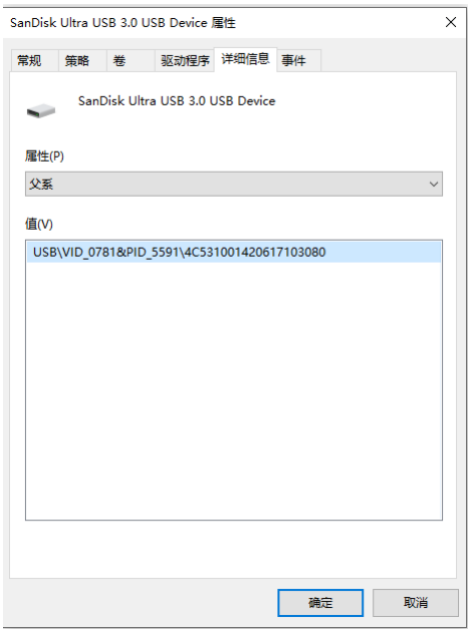


需要输入“父级设备实例路径”和“设备实例路径”。

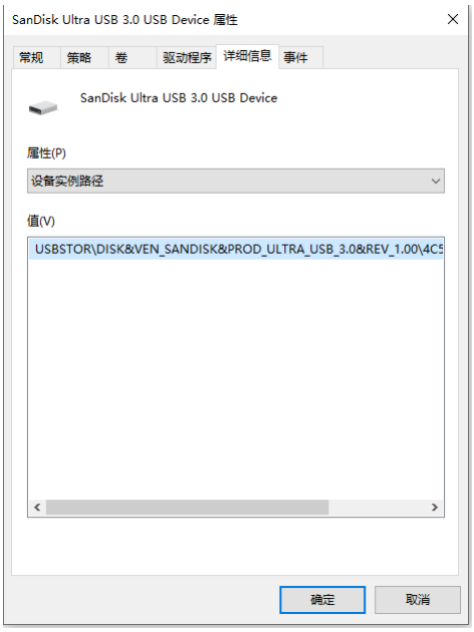
在连接该设备的计算机上，打开“设备管理器”，找到这个设备，右键菜单中点击“属性”



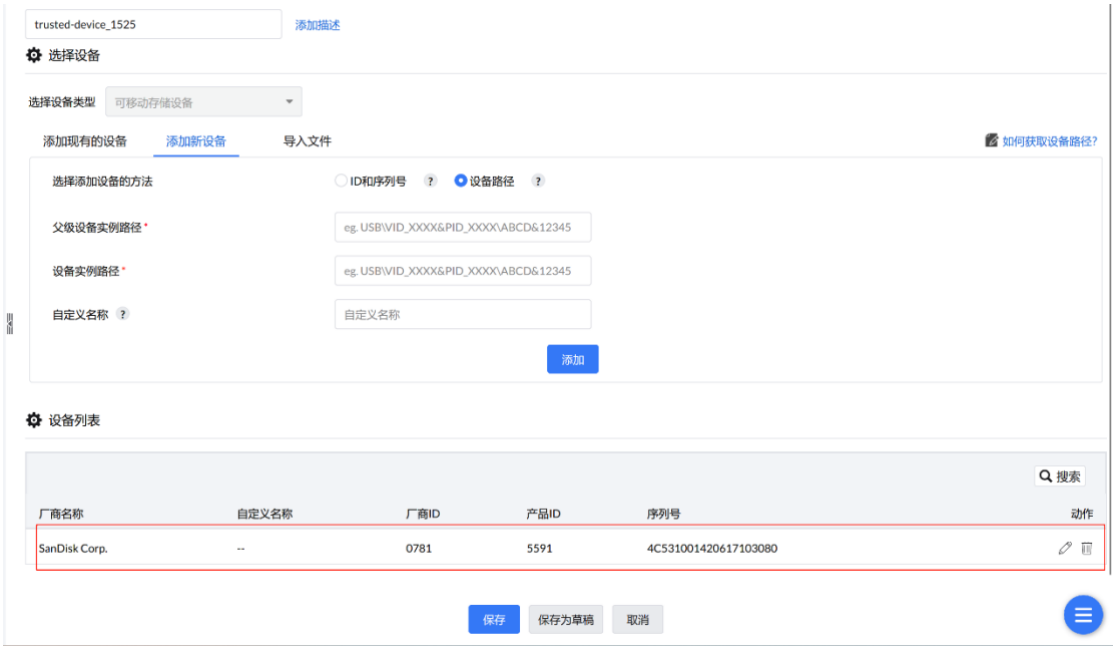
在打开的属性窗口中，点击“详细信息”，在属性中找到“父系”，复制属性值，填写到“父级设备实例路径”字段。



在属性中找到“设备实例路径”，复制属性值，填写到“设备实例路径”字段。



当点击“添加”按钮时，这个设备就会添加到下面的设备列表中。同时，可以看到这个设备的“厂商 ID”、“产品 ID”、“序列号”



4.2.3 从文件导入

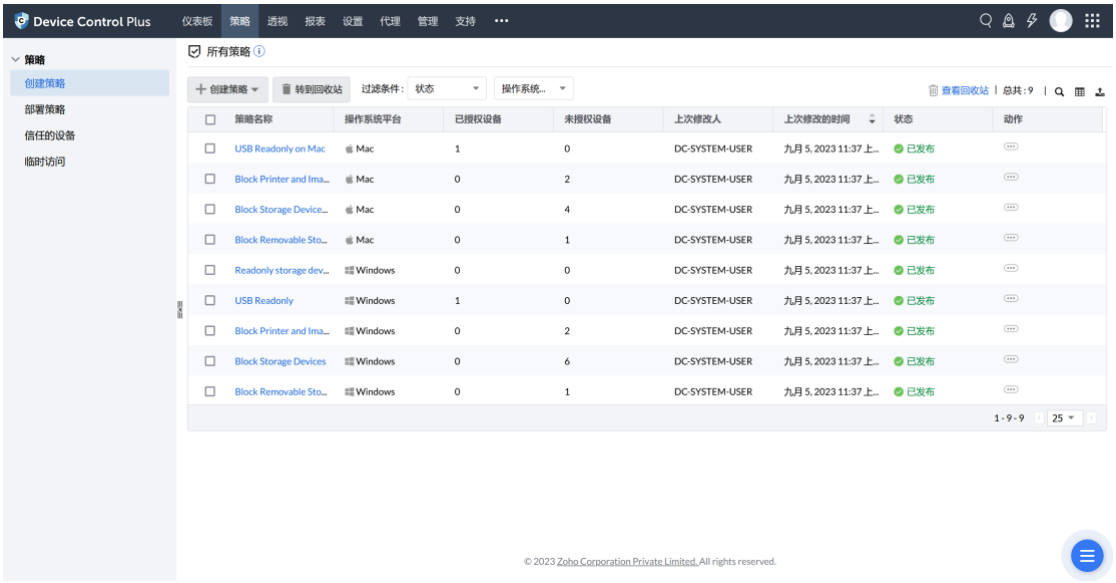
如果要批量添加设备，可以使用 csv 文件。下载示例文件，把你的设备信息添加进来。然后上传这个文件来批量导入设备。

注意：有了信任的设备列表（不是必须的），就可以创建策略了。

4.3 创建/部署策略

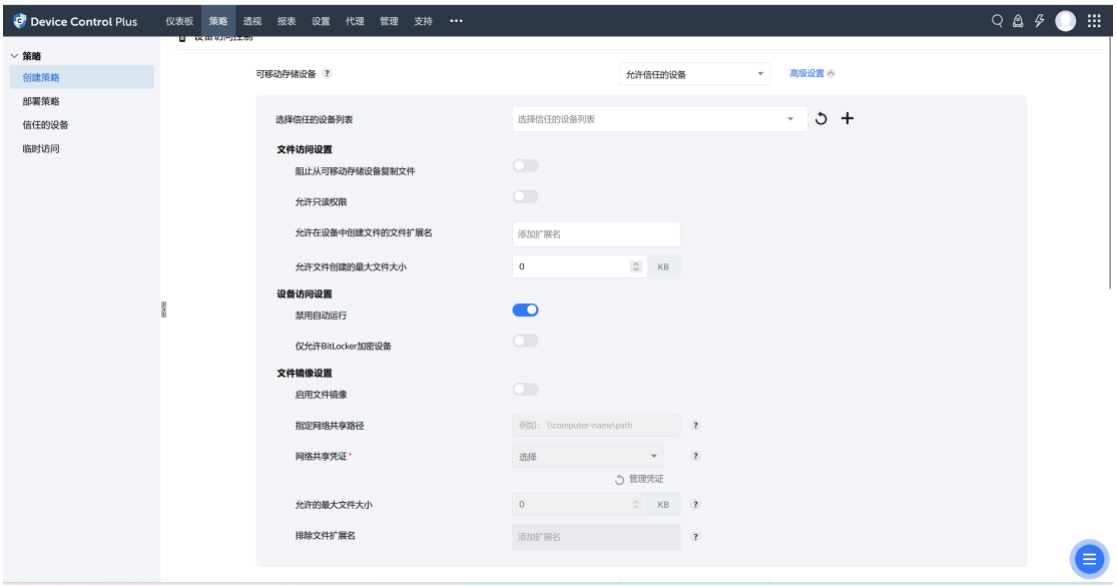
4.3.1 创建策略

点击 “策略” - “创建策略” 。在这里可以创建或修改策略



一个策略包括“设备访问控制”、“设备审计设置“和“告警设置”等部分。

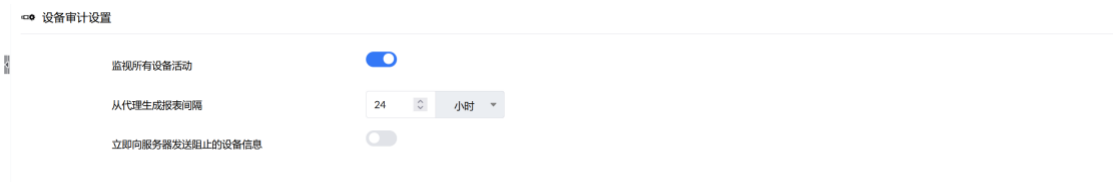
1) 设备访问控制：选择要配置的设备类型，然后选择控制方式：“无更改”、“允许”、“允许信任的设备”、“阻止”。当选择不同方式的时候，点击后面的“高级设置”进行详细的设置。



“可移动存储设备”的高级设置中选项最多。可以设置文件访问、设备访问和文件镜像（当文件传输时，复制一份该文件到某个位置）。

2) 设备审计设置：

这里设置审计数据上传的时间间隔。

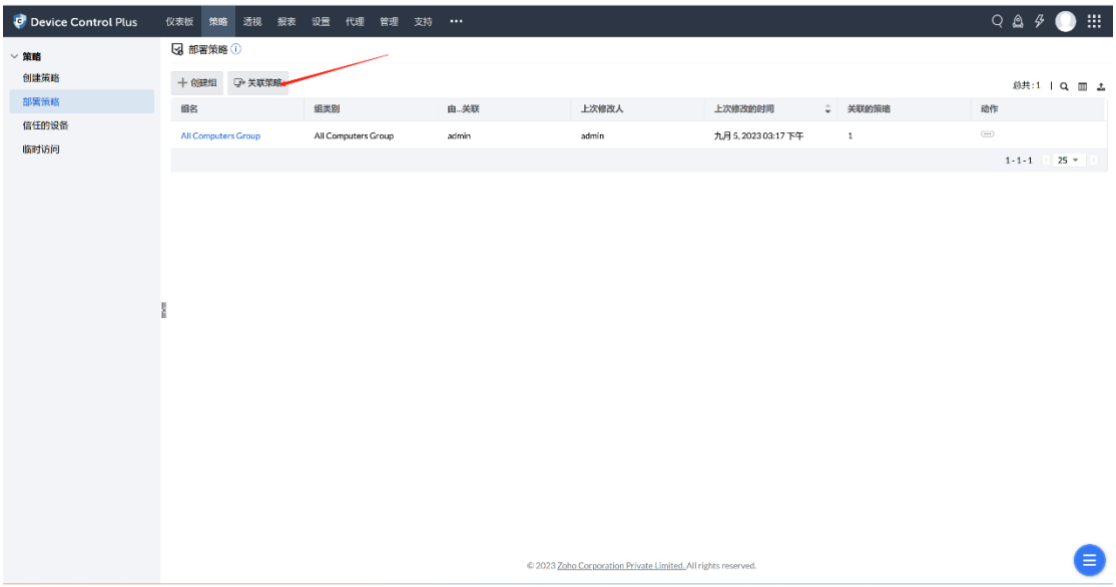


3) 告警设置：配置告警信息。

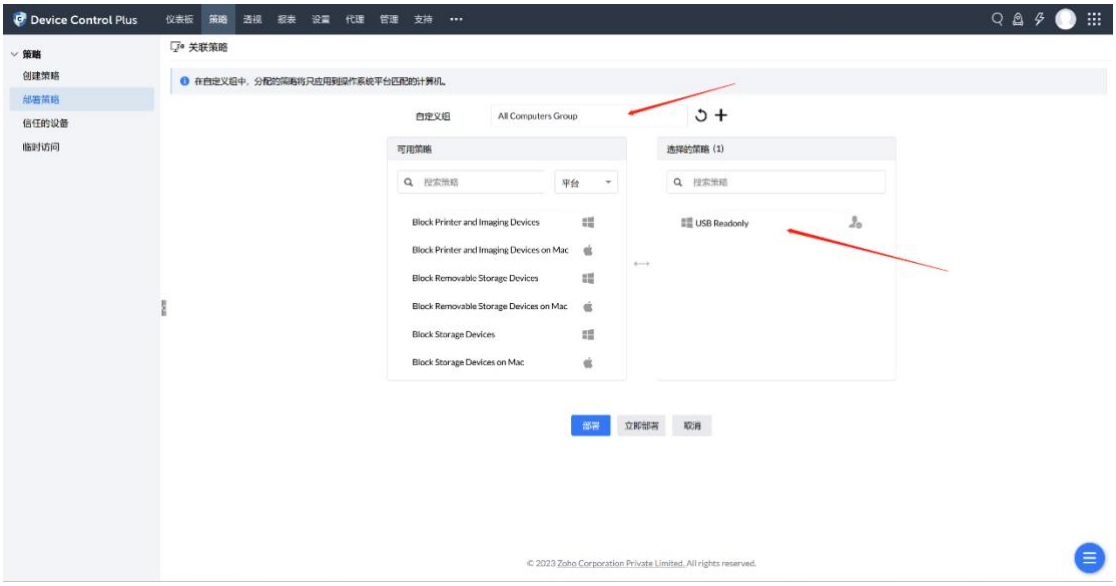
4.3.2 部署策略

部署策略是把上一步创建的策略部署到目标对象（计算机组）。

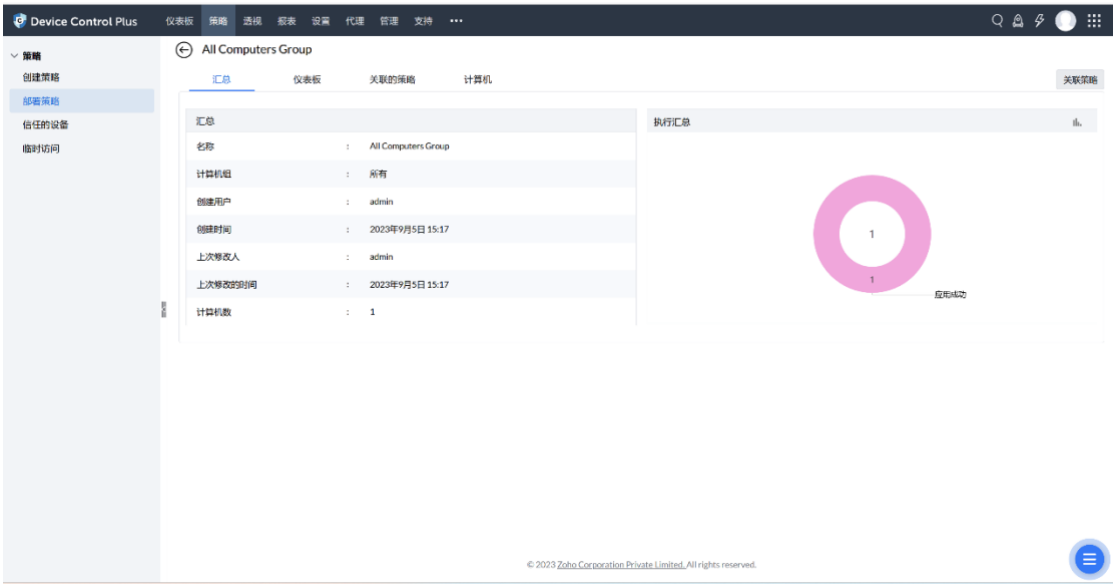
在 DeviceControl Plus 控制台中点击“策略 – 部署策略”，点击“关联策略”按钮。



选择/创建计算机组，然后选择需要的策略。最后点击“部署”按钮。



点击部署的策略，查看部署状态及详细信息。

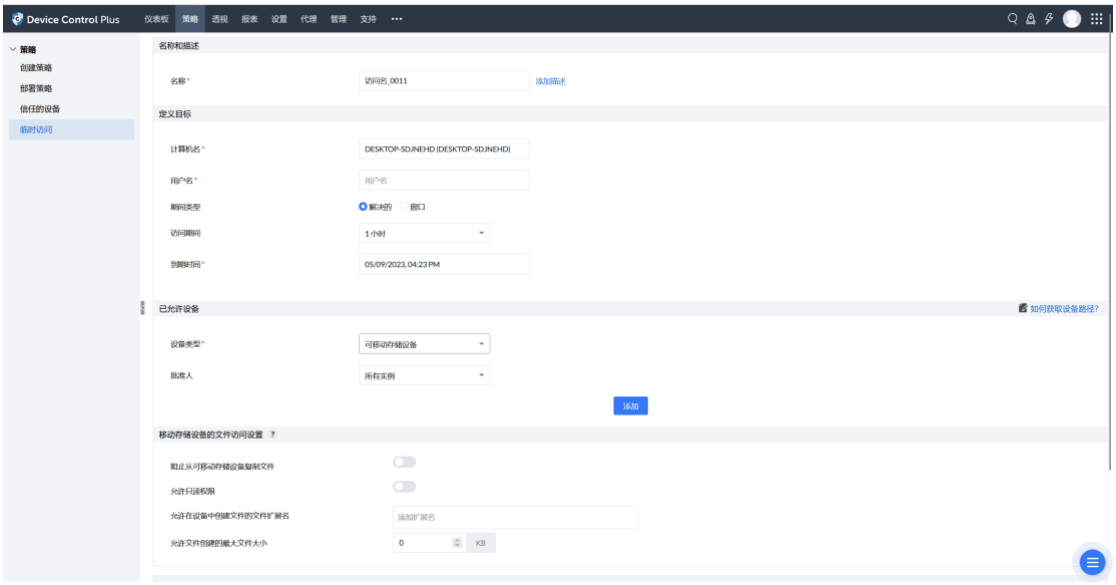


4.4 临时访问

4.4.1 管理员添加临时访问策略

登录 Web 客户端，点击“策略 – 临时访问”，点击“创建”按钮来添加临时访问策略。

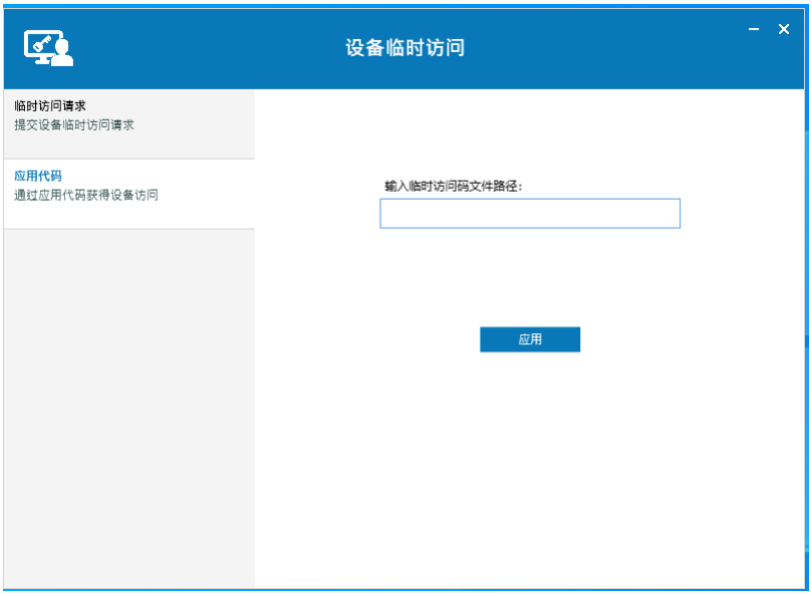
在策略中设置目标计算机、允许的设备、文件访问权限。



当临时访问策略创建成功后，管理员可以选择“部署（在 90 分钟刷新周期时部署）”、“立即部署”或“生成代码”。生成代码可以把临时访问代码通过邮件或下载后发送给用户。用户在客户端导入访问代码。

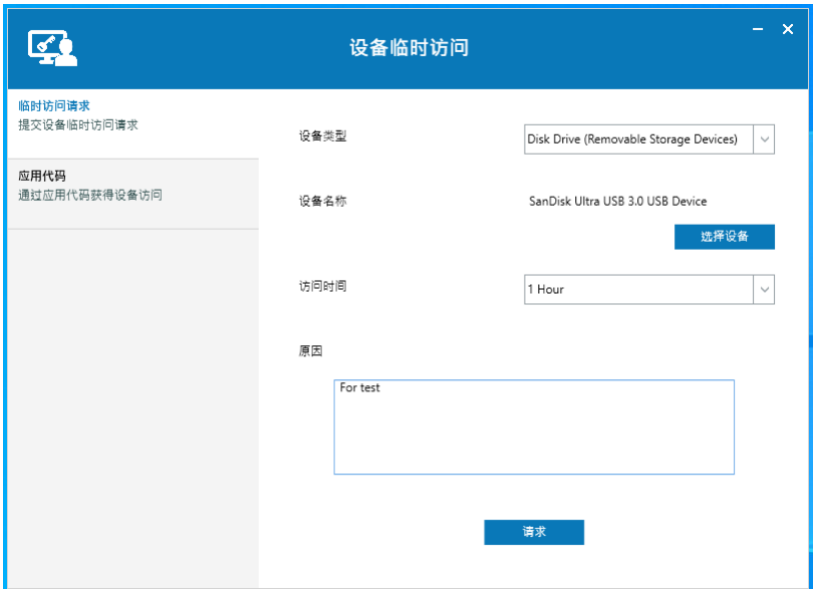
注意：如何导入代码：

在控制台下载代码或邮件收到代码后，将代码拷贝到目标机器，在目标机器右键点击代理图标->运行设备临时访问门户，点击应用代码，输入代码路径位置，点击应用即可

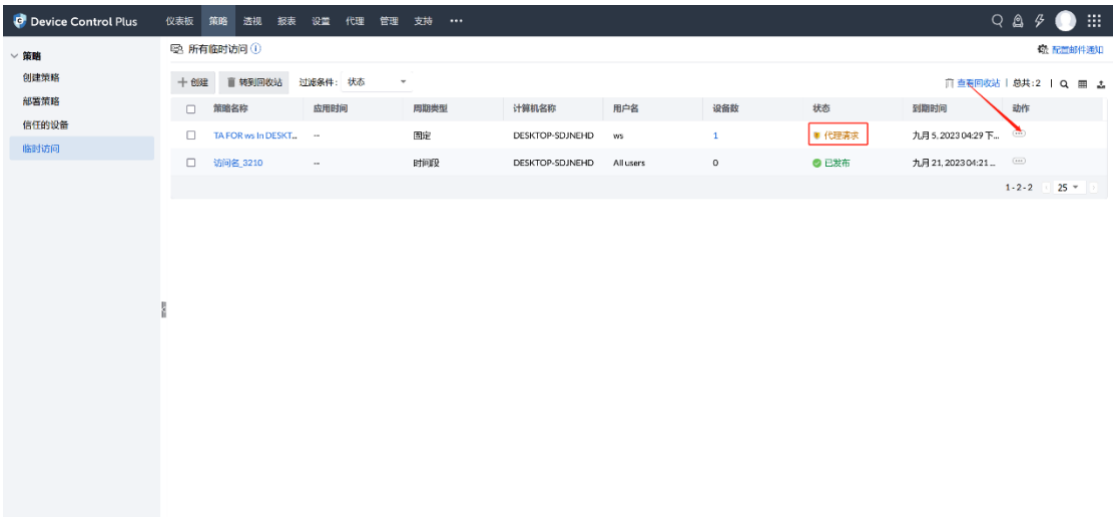


4.4.2 用户申请

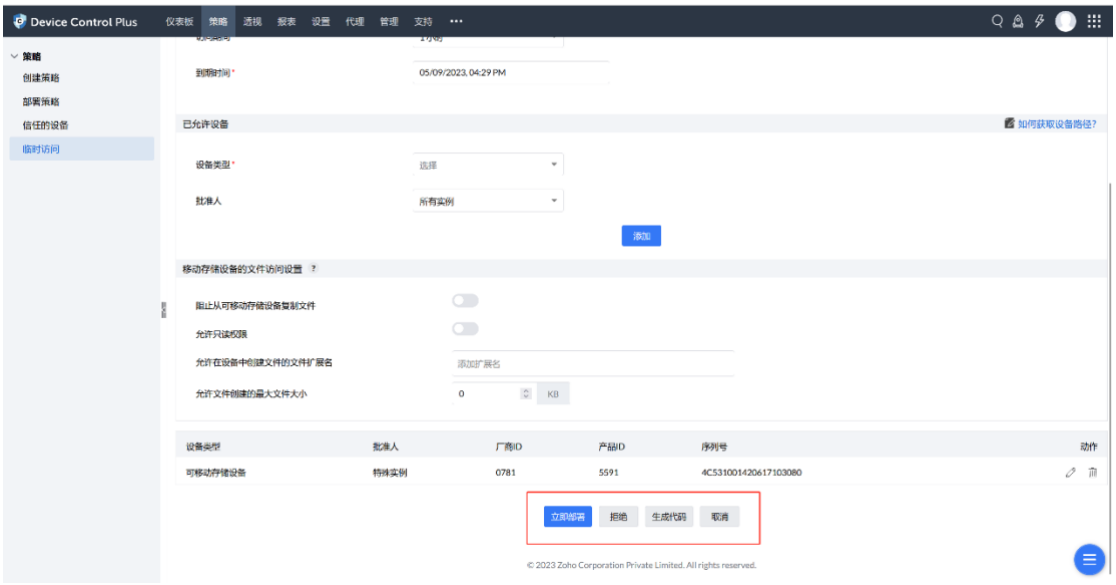
用户在其计算机上，点击代理托盘图标菜单中的“查看设备临时访问门户”，点击“临时访问请求”，选择设备类型，点击“选择设备”按钮来选择要访问的设备。输入原因，点击“请求”按钮。



临时访问请求发送到中心服务器，管理员可以在“临时访问”列表中找到用户发起的请求，点击“动作”按钮 – 选择“修改”，



管理员可以选择“部署（在 90 分钟刷新周期时部署）”、“立即部署”或“生成代码”。生成代码可以把临时访问代码通过邮件或下载后发送给用户。用户在客户端导入访问代码。

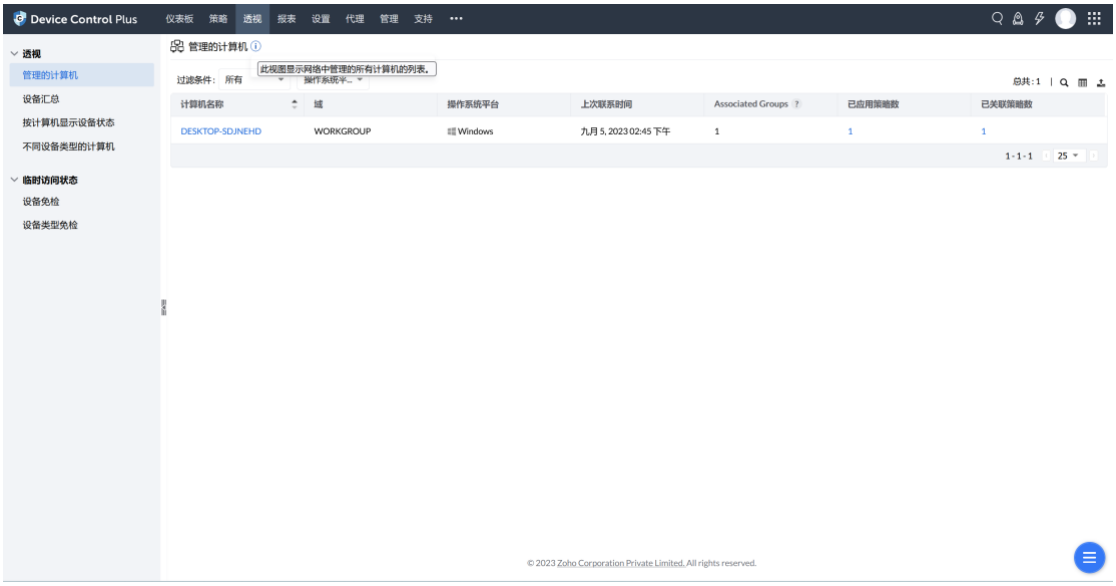


5. 透视

透视页签帮助管理员从设备和计算机的不同角度来管理外部设备和临时访问。

在透视中提示以下几种视图：

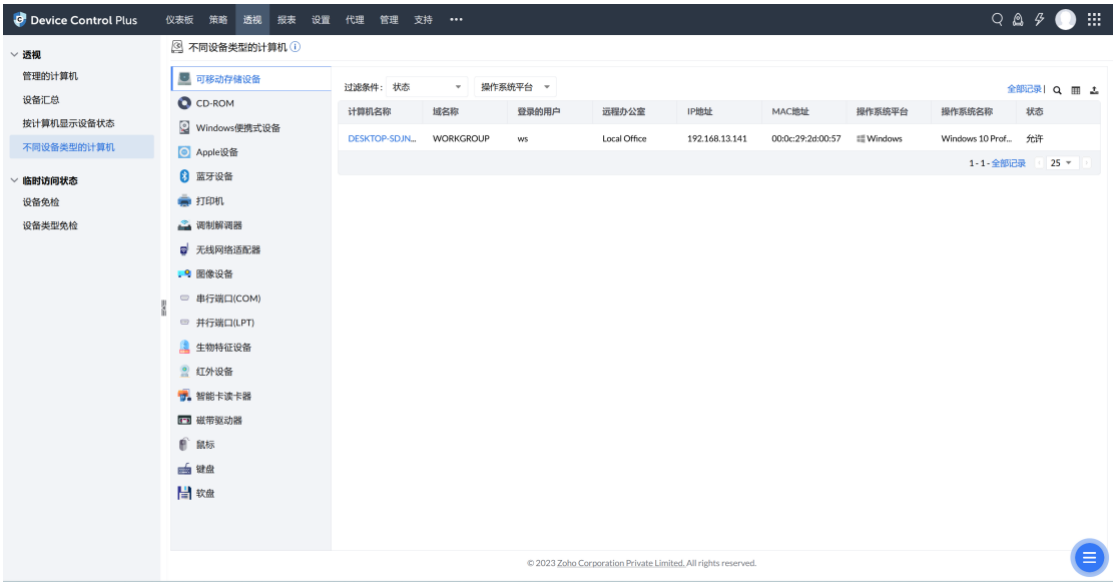
1）管理的计算机



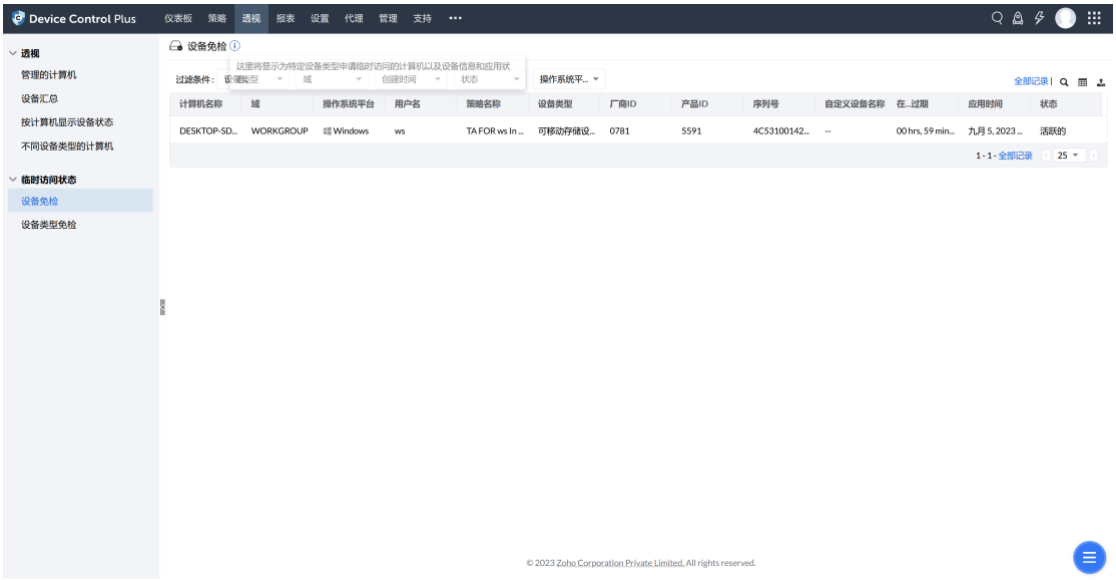
2）设备汇总

3）按计算机显示设备状态

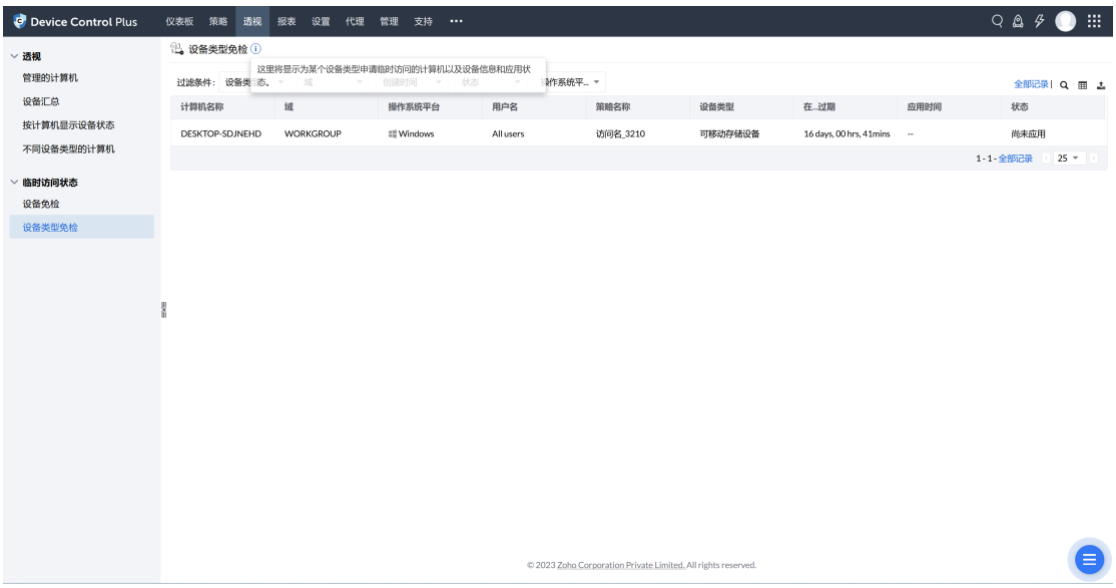
4）不同设备类型的计算机



4） 设备免检


Device Control Plus
仪表板 策略 透视 报表 设置 代理 管理 支持
透视
管理的计算机
设备汇总
按计算机显示设备状态
不同设备类型的计算机
临时访问状态
设备免检
设备类型免检
设备免检
这里将显示为特定设备类型申请临时访问的计算机以及设备信息和应用状
过滤条件：
操作系统平...
全部记录
计算机名称 域 操作系统平台 用户名 策略名称 设备类型 厂商ID 产品ID 序列号 自定义设备名称 在...过期 应用时间 状态
DESKTOP-SD... WORKGROUP Windows ws TA FOR ws In ... 可移动存储设... 0781 5591 4C53100142... -- 00 hrs, 59 min... 九月 5, 2023 ... 活跃的
1 - 1 - 全部记录 25
© 2023 Zoho Corporation Private Limited. All rights reserved.

5) 设备类型免检


Device Control Plus
仪表板 策略 透视 报表 设置 代理 管理 支持
透视
管理的计算机
设备汇总
按计算机显示设备状态
不同设备类型的计算机
临时访问状态
设备免检
设备类型免检
设备类型免检
这里将显示为某个设备类型申请临时访问的计算机以及设备信息和应用状
过滤条件：
操作系统平...
全部记录
计算机名称 域 操作系统平台 用户名 策略名称 设备类型 在...过期 应用时间 状态
DESKTOP-SDJNEHD WORKGROUP Windows All users 访问名_3210 可移动存储设备 16 days, 00 hrs, 41mins -- 尚未应用
1 - 1 - 全部记录 25
© 2023 Zoho Corporation Private Limited. All rights reserved.

产品文档

关于更详细的说明可参见产品官网：

https://www.manageengine.cn/device-control

在线演示：https://www.manageengine.com/device-control/request-demo.html

联系电话：4006608680

技术支持：support@manageengine.cn