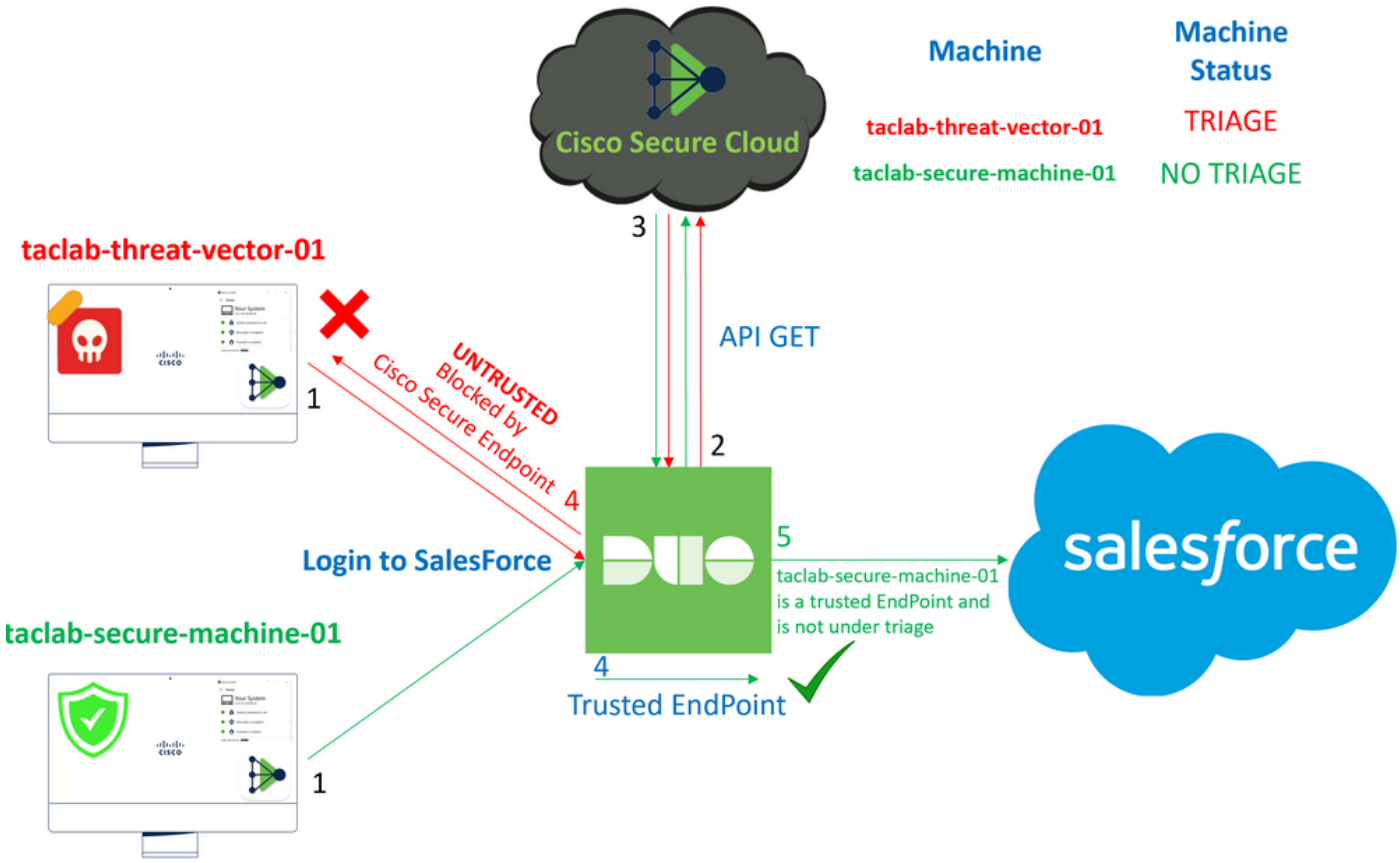
配置Duo和安全终端以响应威胁

目录

简介



本文档介绍如何将Duo Trusted EndPoint与Cisco Secure EndPoint集成。

背景信息

Cisco Secure EndPoint和Duo之间的集成允许针对在受信任的网络设备上检测到的威胁进行有效的协作。这种集成是通过多个设备管理工具来实现的，这些工具可确定每台设备的可靠性。其中一些工具包括：

- Active Directory 域服务
- Active Directory与设备运行状况
- 设备运行状况通用
- Intune with Device Health
- Jamf Pro，带设备健康功能
- LANDESK管理套件
- Mac OS X企业资产管理工具
- 使用设备运行状况进行手动
- Windows企业资产管理工具
- 工作空间ONE与设备运行状况

设备与设备管理工具集成后，可通过以下方式集成思科安全终端和双核： API 如果 Administration Panel.随后，必须在Duo中配置相应的策略，以执行可信设备验证，并检测可能会影响Duo保护的应用程序的被入侵设备。

注意：在本例中，我们使用Active Directory和设备运行状况。

先决条件

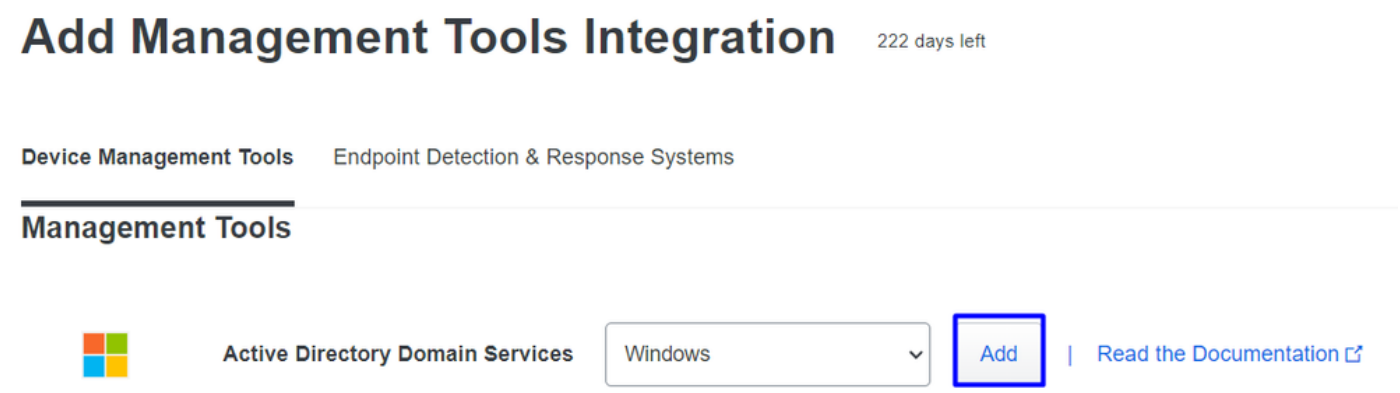
- Active Directory进行集成。
- 要将Duo与受信任终端集成，您的设备必须在Active Directory域中注册。这使得Duo能够安全地验证和授权对网络资源和服务的访问。
- 超乎想象的双人组。

配置和使用案例

配置Duo集成

登录到 **Admin Panel** 并转至：

- **Trusted EndPoints** > **Add Integration**
- 选择 Active Directory Domain Services

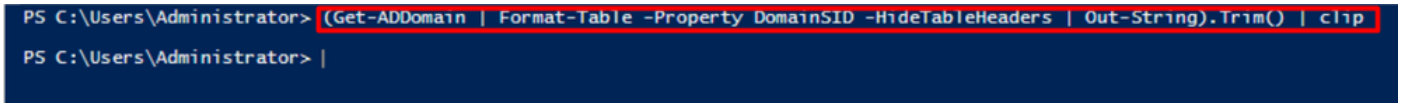


之后，您将重定向以配置 **Active Directory and Device Health.**

请注意，这仅适用于域中的计算机。

转到Active Directory并在PowerShell中运行下一个命令：

```
(Get-ADDomain | Format-Table -Property DomainSID -HideTableHeaders | Out-String).Trim() | clip
```



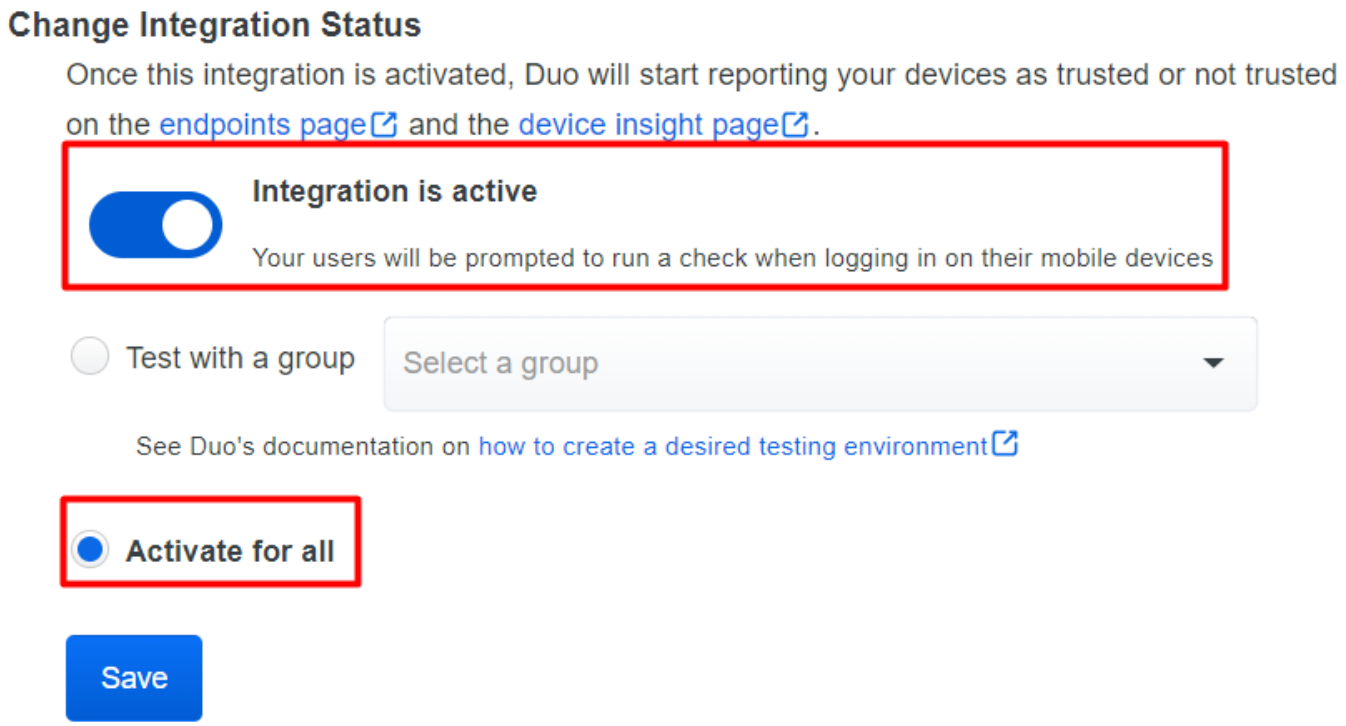
之后，请确保您已将Active Directory的安全标识符复制到剪贴板。

示例

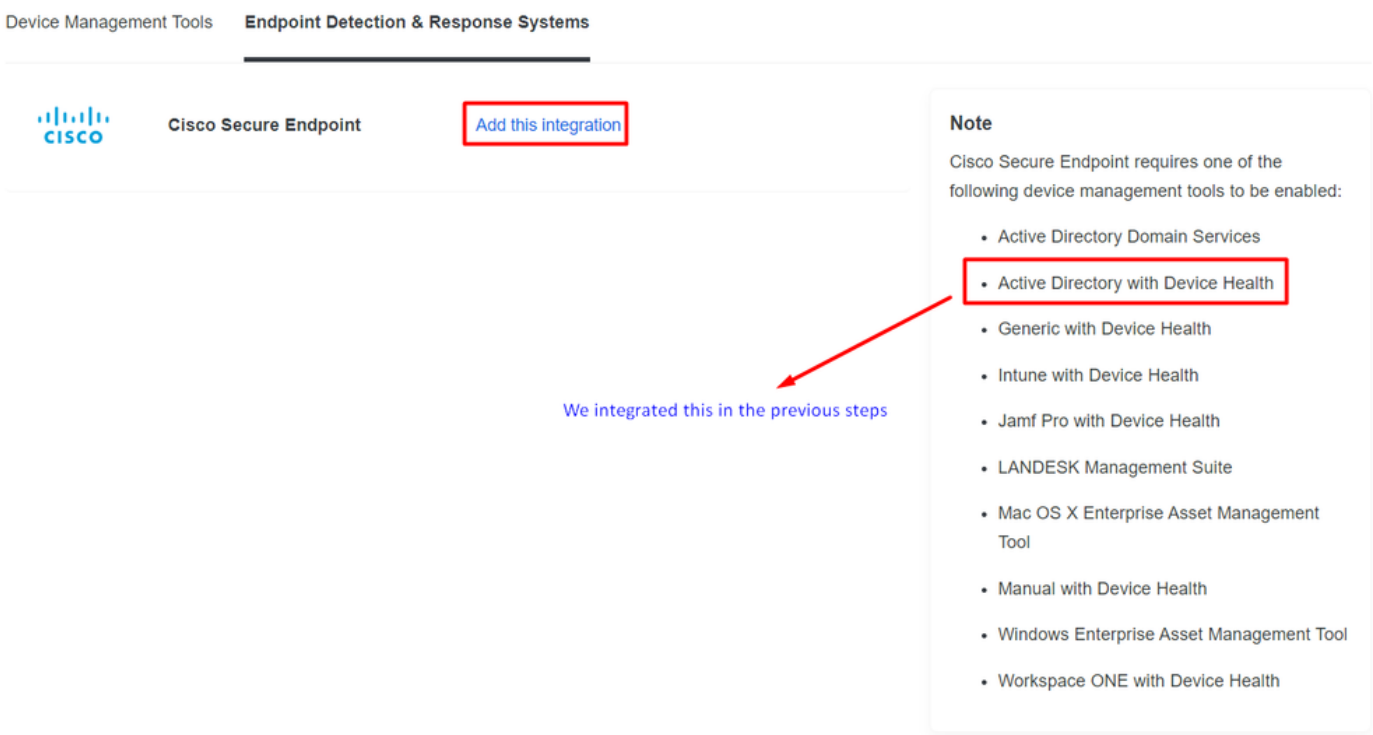
```
S-1-5-21-2952046551-2792955545-1855548404
```

这用于您的Active Directory和设备运行状况集成。

点击 **Save** 并启用集成 Activate for all. 否则，您无法与思科安全终端集成。



转到 Trusted EndPoints > Select Endpoint Detection & Response System > Add this integration.



现在，您处于思科安全终端集成主页上。

Cisco Secure Endpoint

222 days left

1. Generate Cisco Secure Endpoint Credentials

1. Login to the Cisco Secure Endpoint console.
2. Navigate to "Accounts > API Credentials".
3. Click "New API Credentials".
4. Give the credentials a name and make it read-only.
5. Click "Create".
6. Copy the **Client Id** and **API Key** and return to this screen.

---

2. Enter Cisco Secure Endpoint Credentials

Client ID

Enter Client ID from Part 1.

API key

Enter API Key from Part 1.

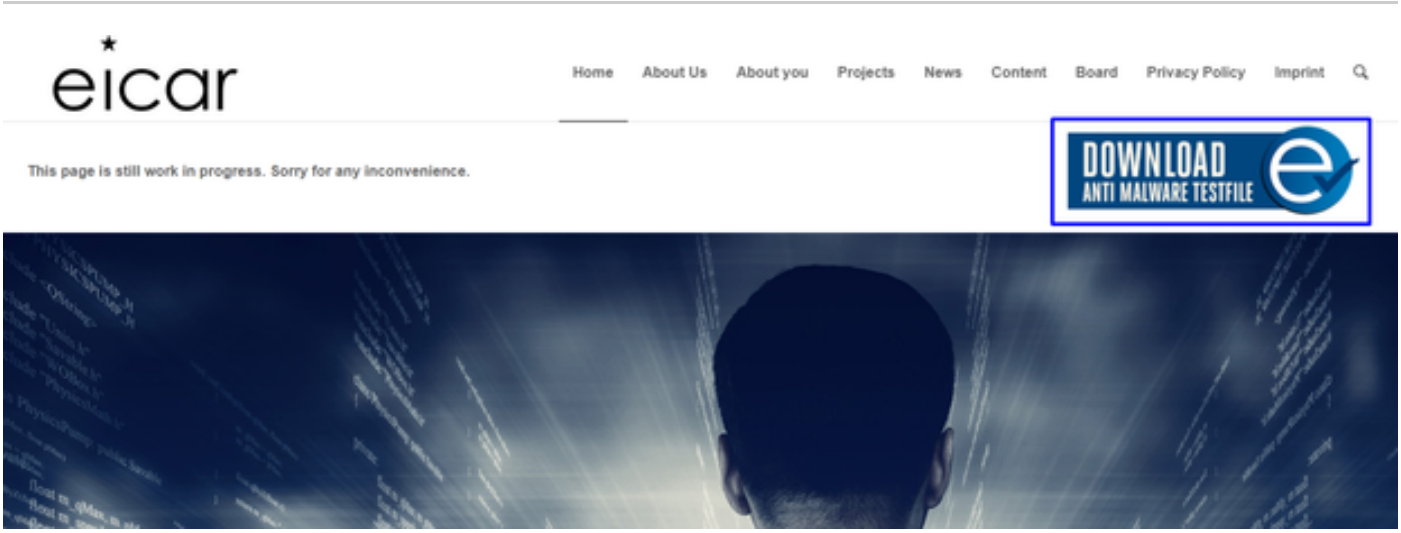
Hostname

https://api.eu.amp.cisco.com/

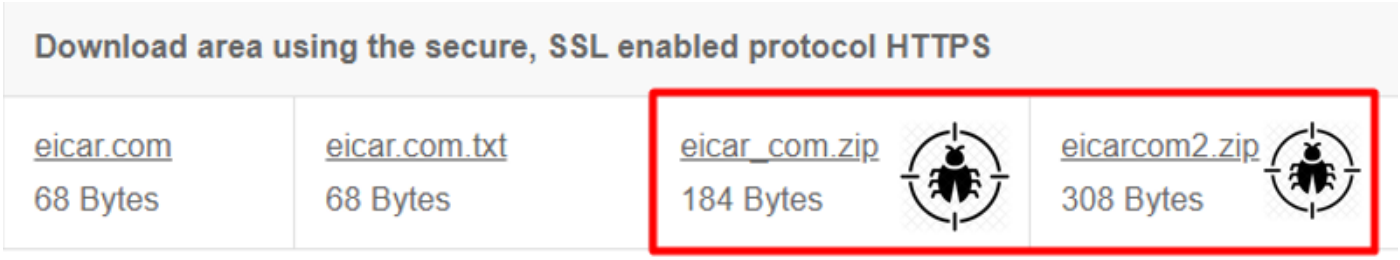
Test Integration

要尝试使用EICAR示例测试该功能，请访问https://www.eicar.org/，并下载恶意示例。

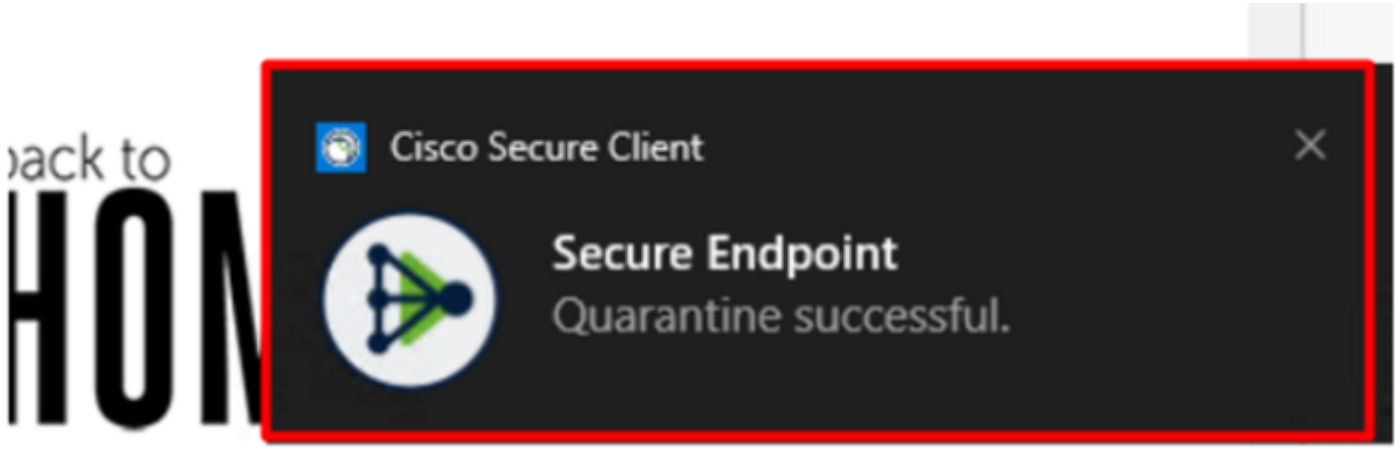
注：不要担心。您可以下载该EICAR测试，它是安全的，并且它只是一个测试文件。



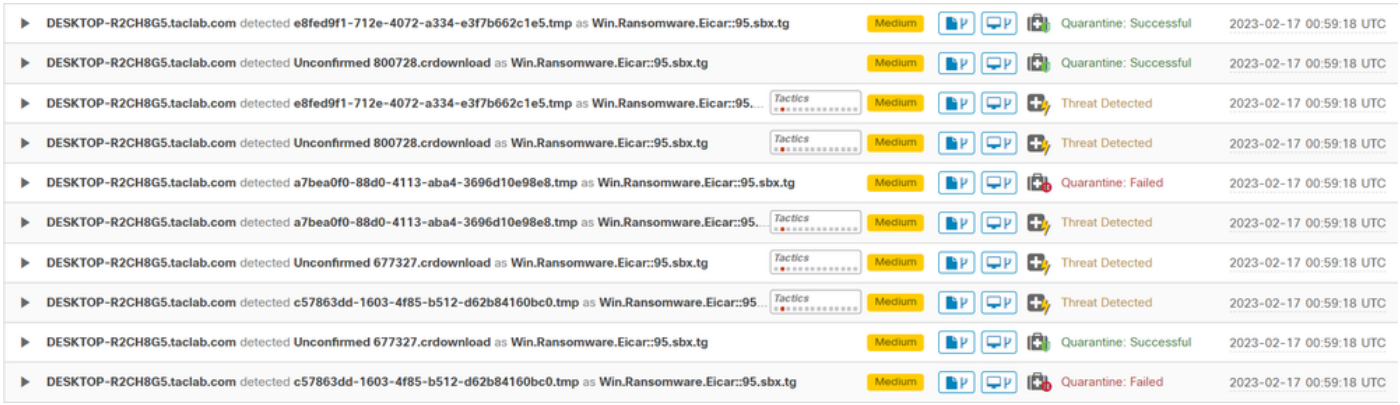
向下滚动并转到部分并下载测试文件。



Cisco Secure EndPoint会检测恶意软件并将其移至隔离区。



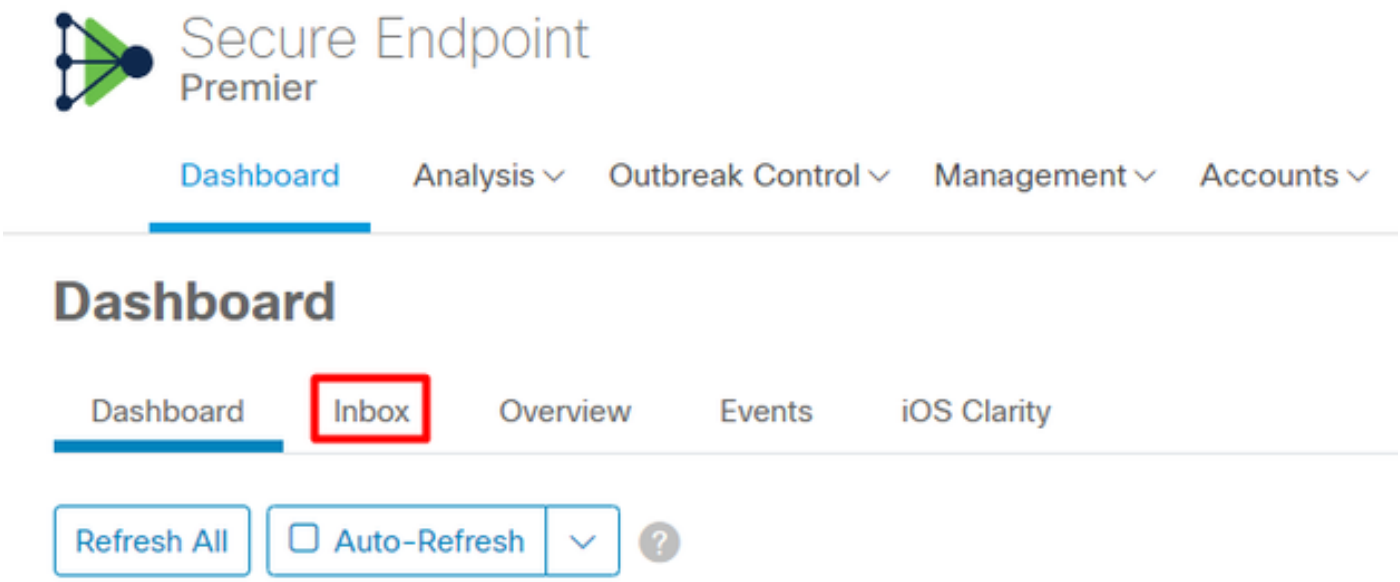
这是更改的方式，如Cisco Secure EndPoint Admin面板所示。



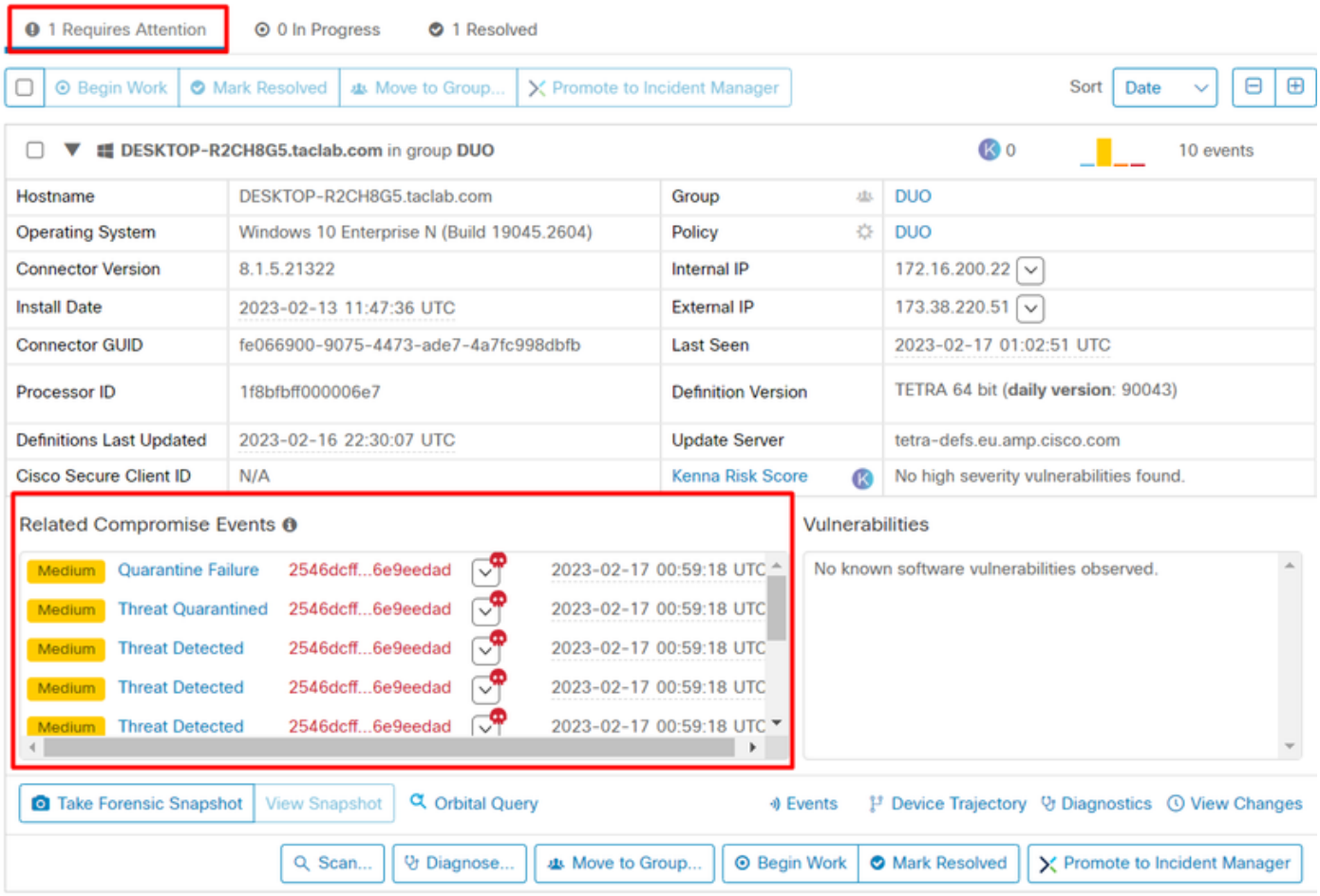
您还检测到计算机中的恶意软件，但这意味着终端将被视为在上的Cisco Secure EndPoint Inbox.

注意：要将终端发送到分类程序，需要多次检测对象或异常行为，以激活某些 Indicators of Compromise 在终端中。

在 Dashboard，在 **Inbox**.

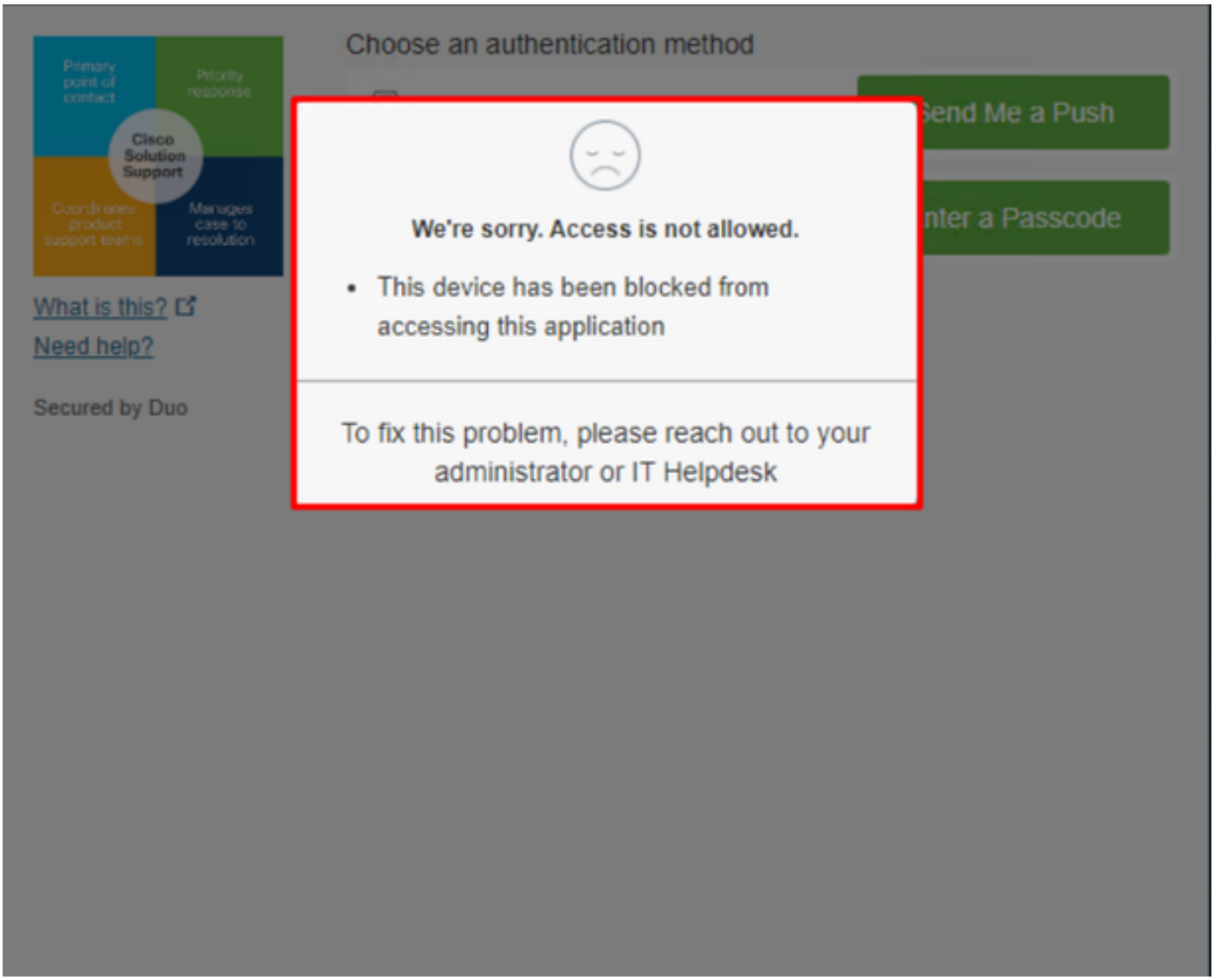


现在，您拥有一台需要关注的机器。

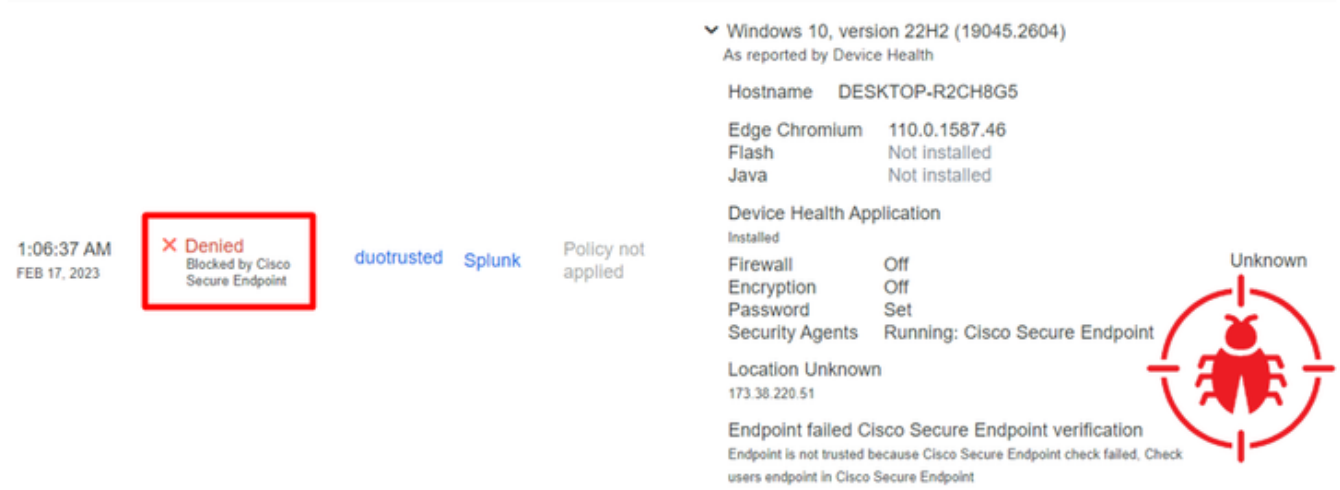


现在，切换到Duo并查看状态。

首先尝试进行身份验证，以查看计算机在下面的Cisco Secure EndPoint上的行为 Require Attention.

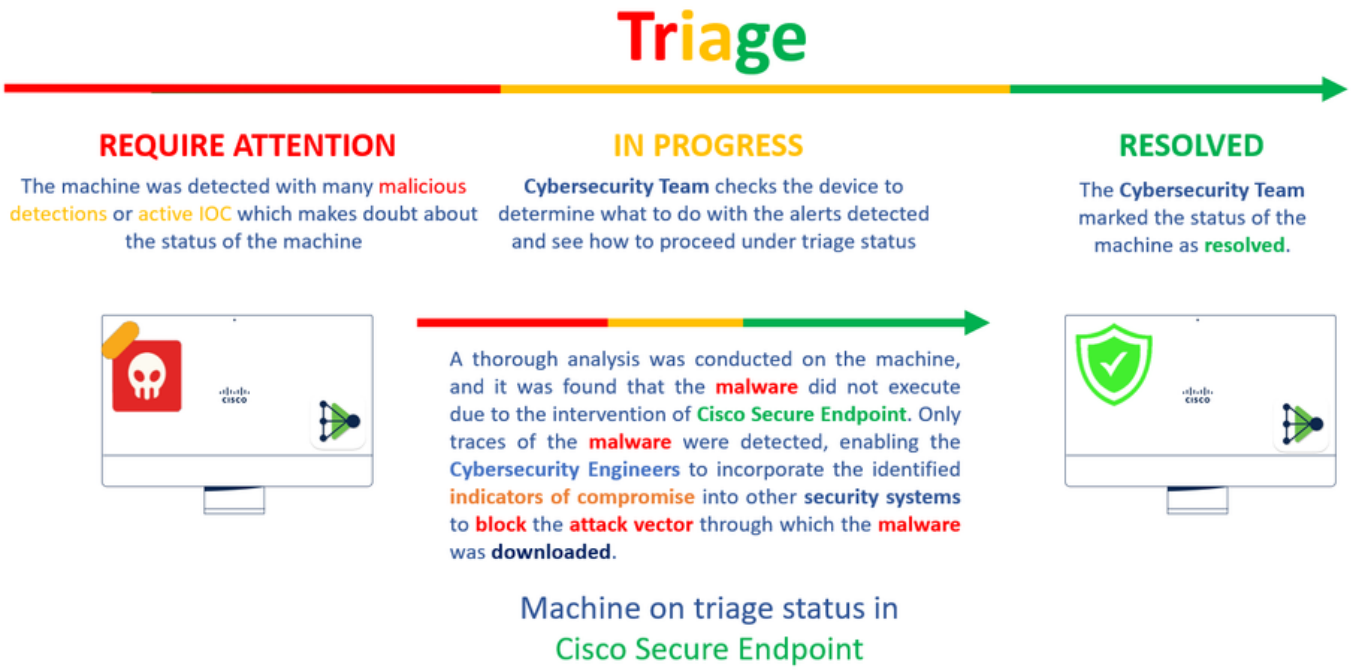


这是它如何在Duo中更改以及身份验证事件下的事件如何显示。



检测到您的计算机不是组织的安全设备。

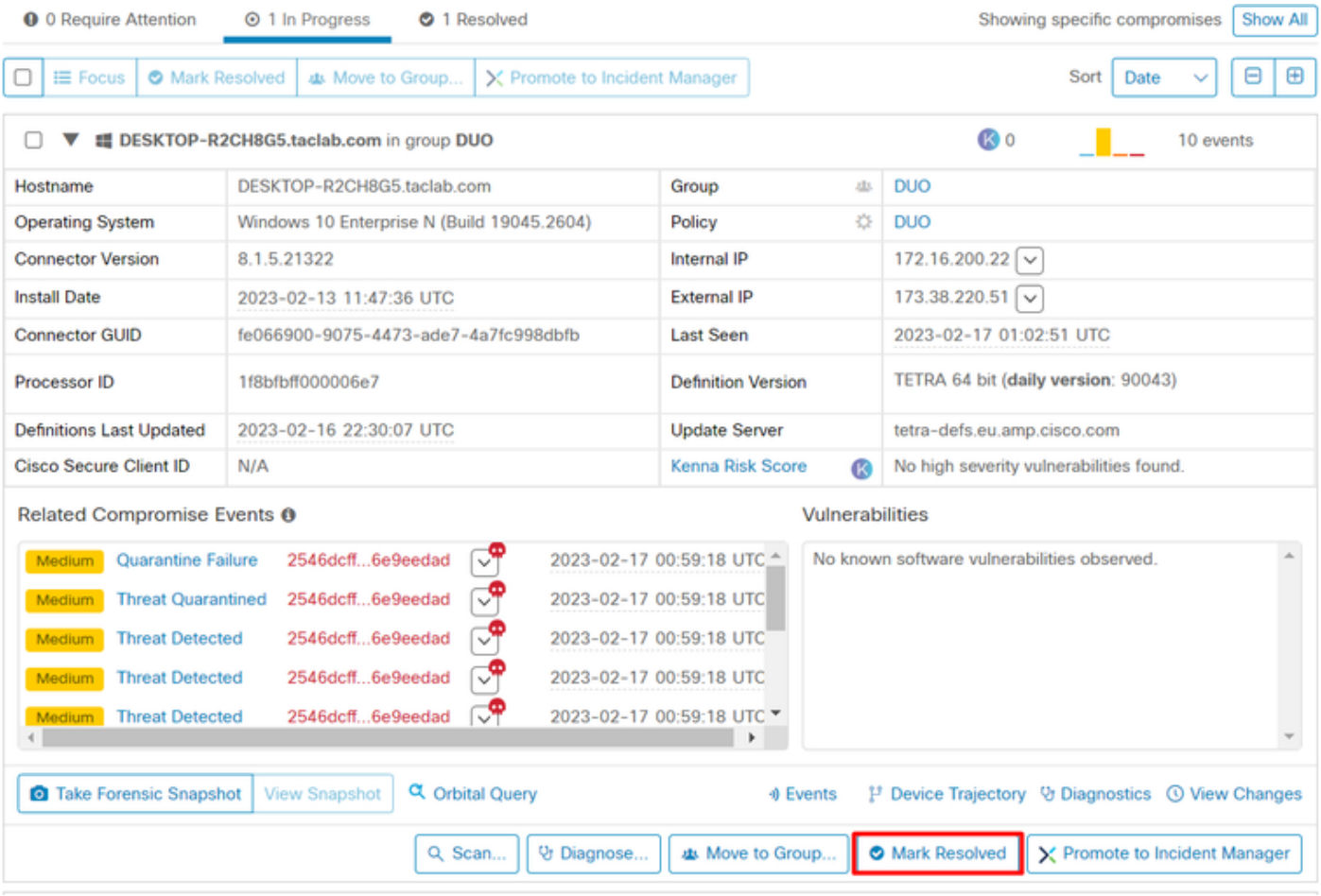
审阅后允许访问计算机



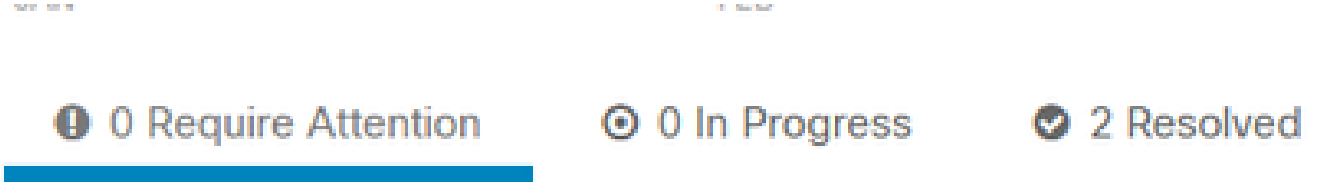
在Cisco Secure EndPoint和网络安全专家进行验证后，您可以在双核允许访问此计算机到您的应用。

现在的问题是如何允许再次访问由Duo保护的应用。

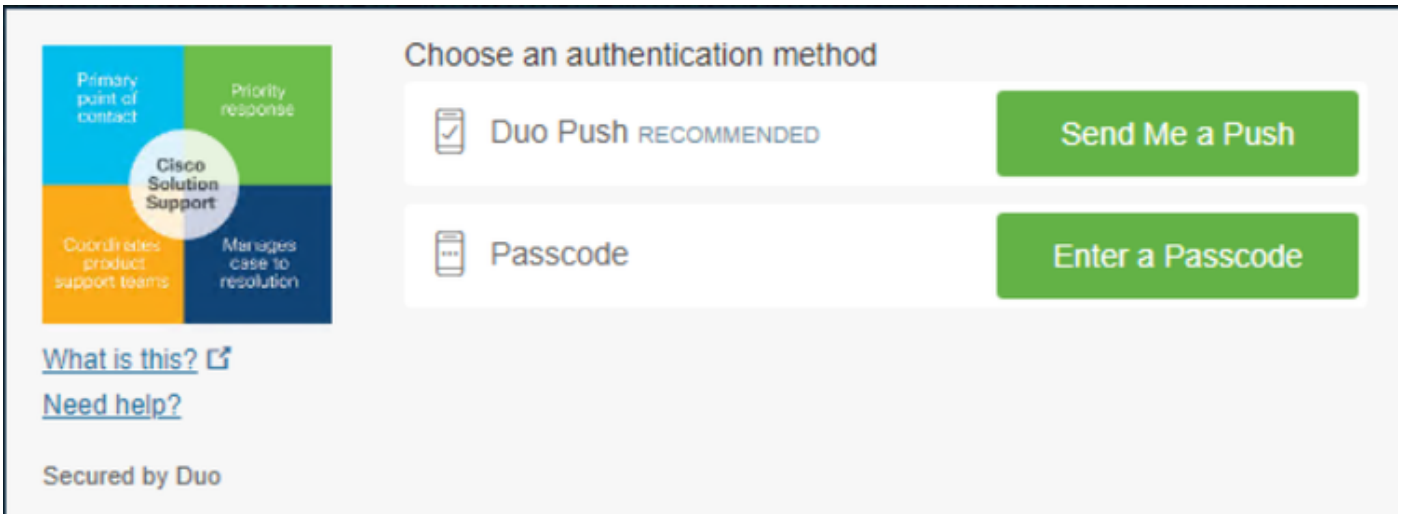
您需要使用思科安全终端和 Inbox，将此设备标记为 **resolved** 允许访问受Duo保护的应用程序。



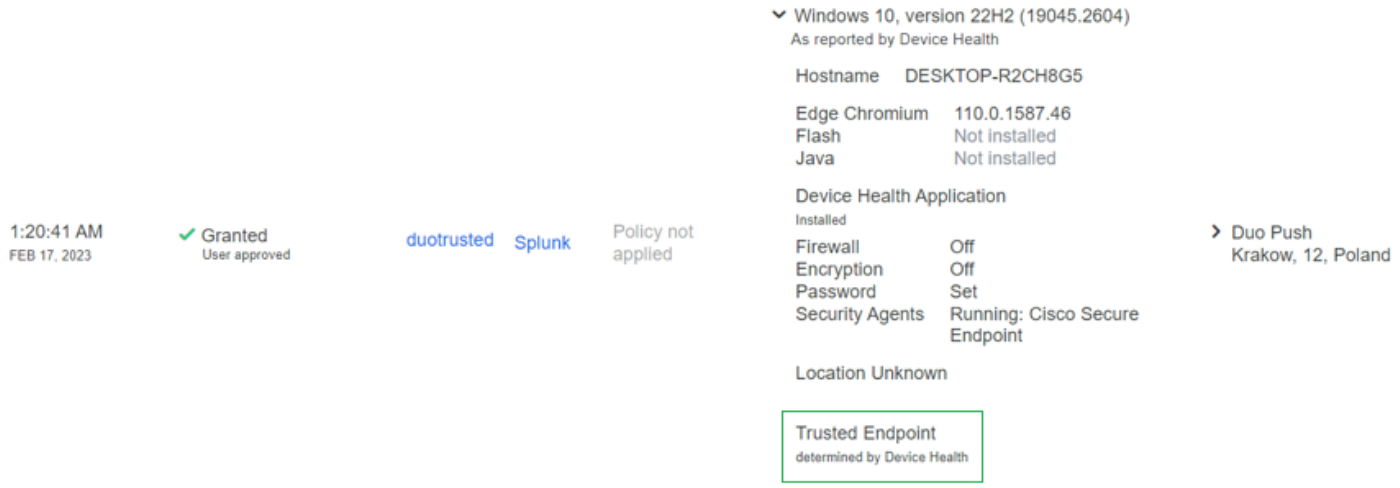
之后，您的计算机没有此状态 attention required.这更改为 resolved 状态.



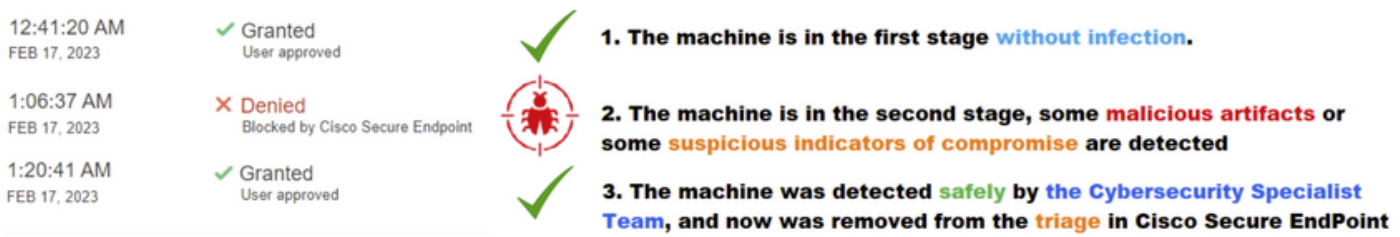
简而言之，现在您已经准备好再次测试对我们受Duo保护的应用程序的访问情况。



现在，您拥有了将推送发送到Duo的权限，并且您已登录该应用。



分类工作流



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。