

# 配置Duo和安全终端以响应威胁

## 目录

[简介](#)

[背景信息](#)

[先决条件](#)

[配置和使用案例](#)

[配置Duo集成](#)

[配置思科安全终端中的集成](#)

[在Duo中配置策略](#)

[配置策略以检测受信任设备](#)

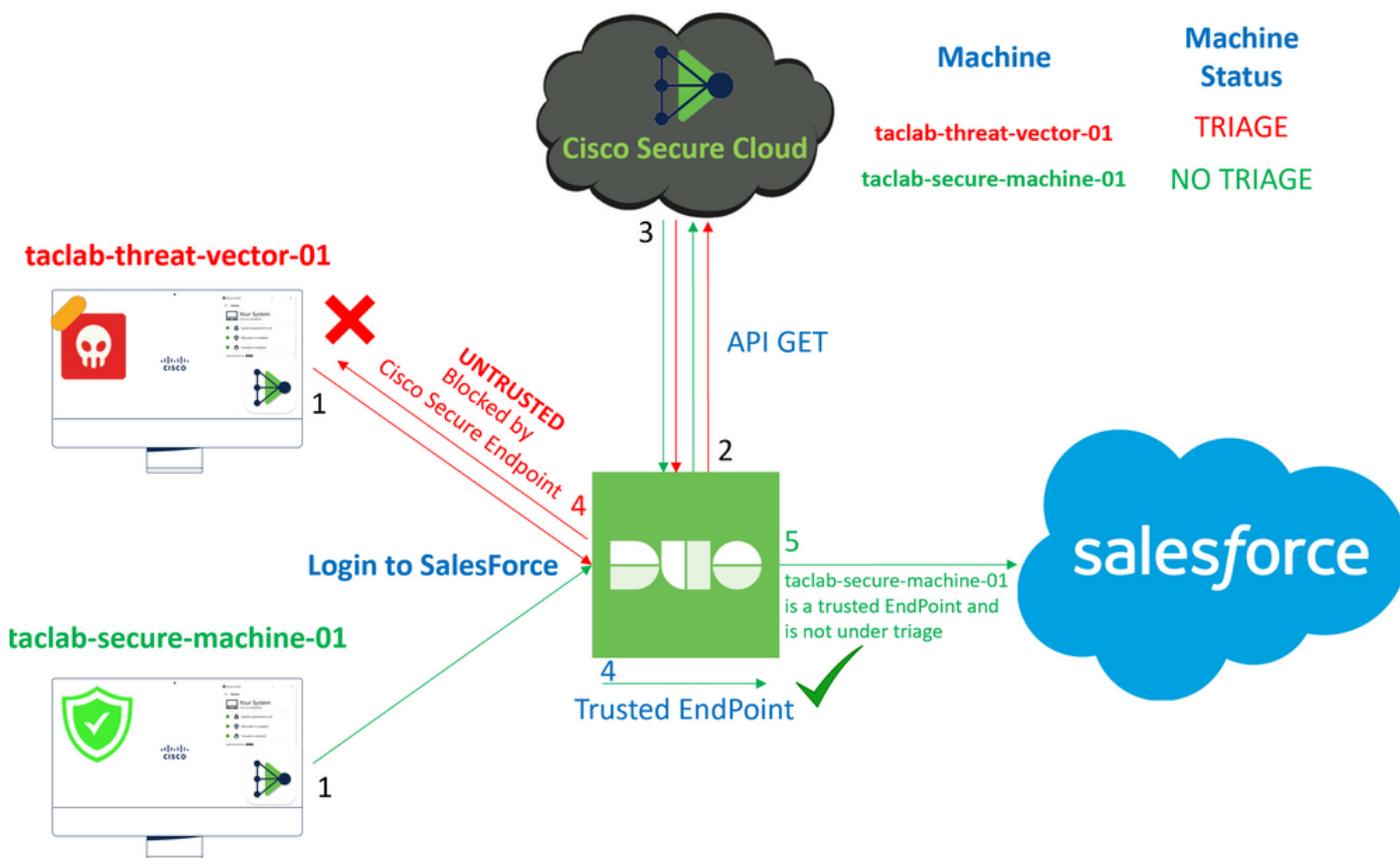
[测试受信任的计算机](#)

[配置思科安全终端的策略](#)

[使用Cisco Secure EndPoint测试可信计算机](#)

[审阅后允许访问计算机](#)

## 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

# Add Management Tools Integration 222 days left

Device Management Tools Endpoint Detection & Response Systems

## Management Tools



Active Directory Domain Services

Windows

Add

| [Read the Documentation](#)

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
```

```
PS C:\Users\Administrator> (Get-ADDomain | Format-Table -Property DomainSID -HideTableHeaders | Out-String).Trim() | clip
PS C:\Users\Administrator> |
```

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。

**i** This integration is currently disabled. You can test it with a group of users before activating it for all.

1. Login to the domain controller to which endpoints are joined
2. Open PowerShell
3. Execute the following command, then retrieve the domain Security Identifier (SID) from your clipboard  
After running the command, the domain SID will be copied to your clipboard. The SID is used to know if your user's computer is joined to the domain controller.

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

4. Paste the domain SID

  
Ex. S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX

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。

### Change Integration Status

Once this integration is activated, Duo will start reporting your devices as trusted or not trusted on the [endpoints page](#) and the [device insight page](#).

**Integration is active**  
Your users will be prompted to run a check when logging in on their mobile devices

Test with a group

See Duo's documentation on [how to create a desired testing environment](#)

**Activate for all**

**Save**

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



Cisco Secure Endpoint

[Add this integration](#)

**Note**

Cisco Secure Endpoint requires one of the following device management tools to be enabled:

- Active Directory Domain Services
- **Active Directory with Device Health**
- Generic with Device Health
- Intune with Device Health
- Jamf Pro with Device Health
- LANDESK Management Suite
- Mac OS X Enterprise Asset Management Tool
- Manual with Device Health
- Windows Enterprise Asset Management Tool
- Workspace ONE with Device Health

[We integrated this in the previous steps](#)

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.

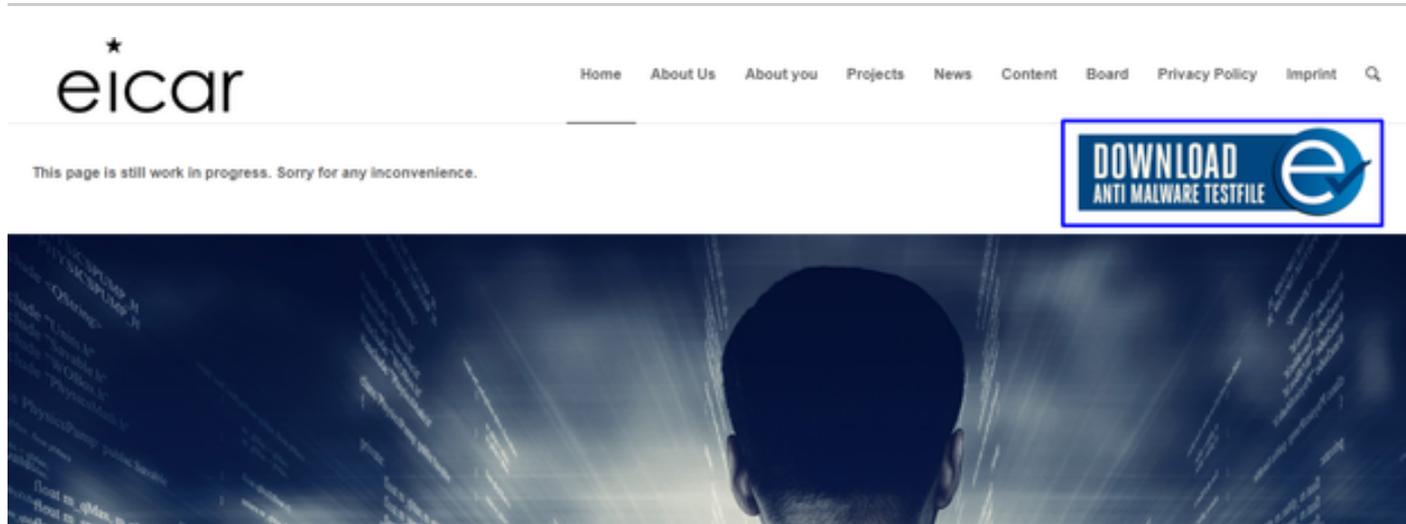
Hostname

*<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。

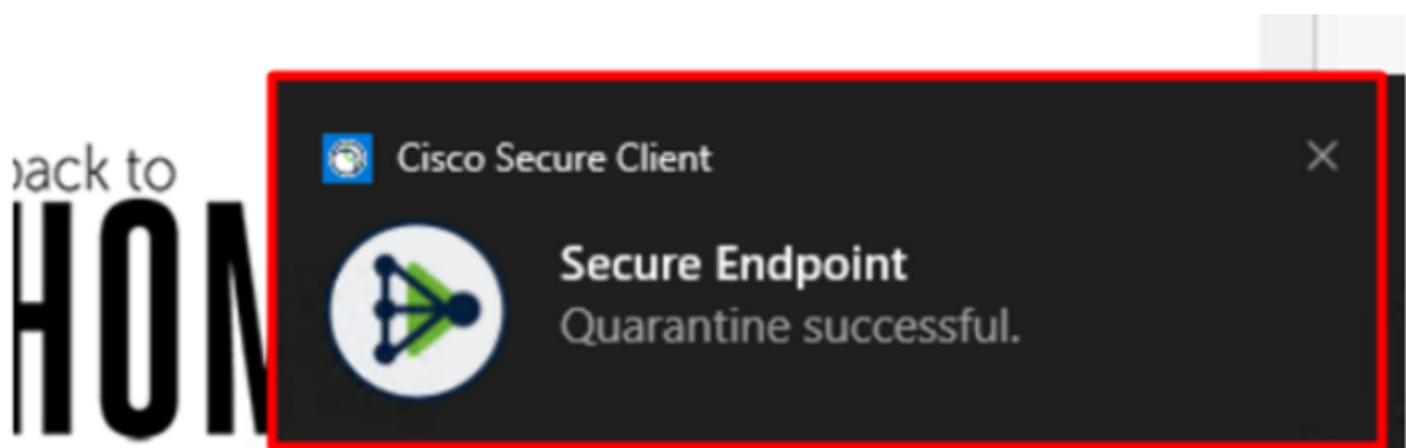
 注：不要担心。您可以下载该EICAR测试，它是安全的，并且它只是一个测试文件。



向下滚动并转到部分并下载测试文件。

Download area using the secure, SSL enabled protocol HTTPS			
<a href="#">eicar.com</a> 68 Bytes	<a href="#">eicar.com.txt</a> 68 Bytes	<a href="#">eicar_com.zip</a> 184 Bytes	<a href="#">eicarcom2.zip</a> 308 Bytes

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。

▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Quarantine: Successful	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar:95.sbx.tg	Medium				Quarantine: Successful	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Quarantine: Failed	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar:95.sbx.tg	Medium				Quarantine: Successful	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Quarantine: Failed	2023-02-17 00:59:18 UTC

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。



Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

## Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

Refresh All  Auto-Refresh ▾ ?

现在，您拥有一台需要关注的机器。

1 Requires Attention 0 In Progress 1 Resolved

Begin Work Mark Resolved Move to Group... Promote to Incident Manager Sort Date

DESKTOP-R2CH8G5.taclab.com in group DUO 0 10 events

Hostname	DESKTOP-R2CH8G5.taclab.com	Group	DUO
Operating System	Windows 10 Enterprise N (Build 19045.2604)	Policy	DUO
Connector Version	8.1.5.21322	Internal IP	172.16.200.22
Install Date	2023-02-13 11:47:36 UTC	External IP	173.38.220.51
Connector GUID	fe066900-9075-4473-ade7-4a7fc998dbfb	Last Seen	2023-02-17 01:02:51 UTC
Processor ID	1f8bfbff000006e7	Definition Version	TETRA 64 bit (daily version: 90043)
Definitions Last Updated	2023-02-16 22:30:07 UTC	Update Server	tetra-defs.eu.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

Related Compromise Events

Medium	Quarantine Failure	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Quarantined	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC

Vulnerabilities

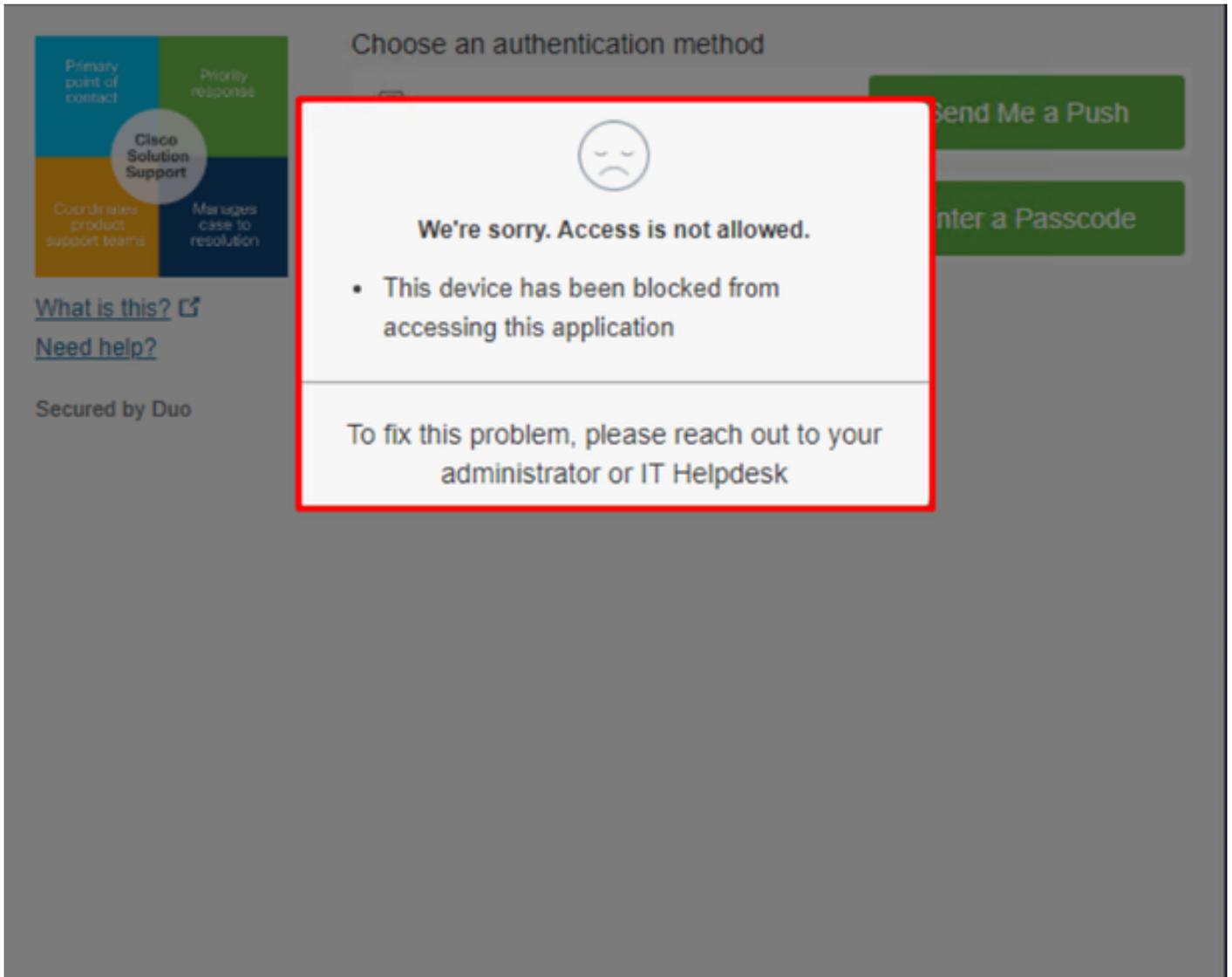
No known software vulnerabilities observed.

Take Forensic Snapshot View Snapshot Orbital Query Events Device Trajectory Diagnostics View Changes

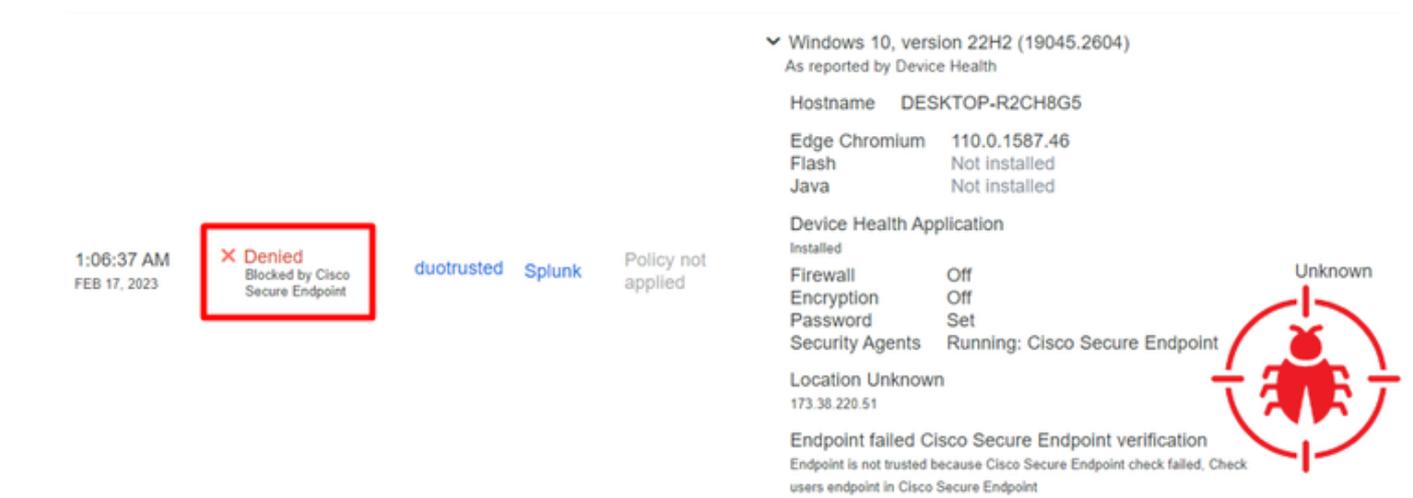
Scan... Diagnose... Move to Group... Begin Work Mark Resolved Promote to Incident Manager

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

# Triage

## REQUIRE ATTENTION

The machine was detected with many **malicious detections** or **active IOC** which makes doubt about the status of the machine



## IN PROGRESS

**Cybersecurity Team** checks the device to determine what to do with the alerts detected and see how to proceed under triage status

A thorough analysis was conducted on the machine, and it was found that the **malware** did not execute due to the intervention of **Cisco Secure Endpoint**. Only traces of the **malware** were detected, enabling the **Cybersecurity Engineers** to incorporate the identified **indicators of compromise** into other security systems to **block the attack vector** through which the **malware** was **downloaded**.

## RESOLVED

The **Cybersecurity Team** marked the status of the machine as **resolved**.



### Machine on triage status in Cisco Secure Endpoint

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。

0 Require Attention | 1 In Progress | 1 Resolved | Showing specific compromises | Show All

Focus | Mark Resolved | Move to Group... | Promote to Incident Manager | Sort: Date

DESKTOP-R2CH8G5.taclab.com in group DUO | 0 | 10 events

Hostname	DESKTOP-R2CH8G5.taclab.com	Group	DUO
Operating System	Windows 10 Enterprise N (Build 19045.2604)	Policy	DUO
Connector Version	8.1.5.21322	Internal IP	172.16.200.22
Install Date	2023-02-13 11:47:36 UTC	External IP	173.38.220.51
Connector GUID	fe066900-9075-4473-ade7-4a7fc998dbfb	Last Seen	2023-02-17 01:02:51 UTC
Processor ID	1f8bfbff000006e7	Definition Version	TETRA 64 bit (daily version: 90043)
Definitions Last Updated	2023-02-16 22:30:07 UTC	Update Server	tetra-defs.eu.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

Related Compromise Events

Medium	Quarantine Failure	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Quarantined	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC

Vulnerabilities

No known software vulnerabilities observed.

Take Forensic Snapshot | View Snapshot | Orbital Query | Events | Device Trajectory | Diagnostics | View Changes

Scan... | Diagnose... | Move to Group... | **Mark Resolved** | Promote to Incident Manager

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

00:00:00

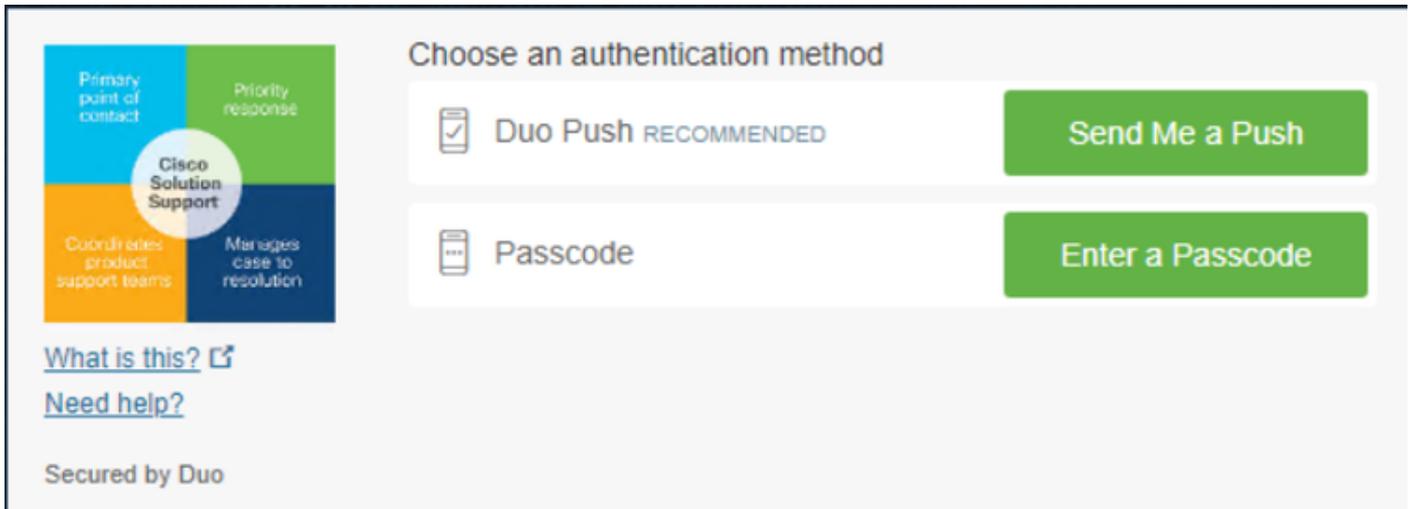
00:00:00

0 Require Attention

0 In Progress

2 Resolved

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。

1:20:41 AM FEB 17, 2023	✔ Granted User approved	duotrusted Splunk	Policy not applied	Windows 10, version 22H2 (19045.2604) As reported by Device Health Hostname DESKTOP-R2CH8G5 Edge Chromium 110.0.1587.46 Flash Not installed Java Not installed Device Health Application Installed Firewall Off Encryption Off Password Set Security Agents Running: Cisco Secure Endpoint Location Unknown Duo Push Krakow, 12, Poland
				Trusted Endpoint determined by Device Health

### 分类 workflow

- 12:41:20 AM FEB 17, 2023 ✔ Granted User approved
- 1:06:37 AM FEB 17, 2023 ✘ Denied Blocked by Cisco Secure Endpoint
- 1:20:41 AM FEB 17, 2023 ✔ Granted User approved



1. The machine is in the first stage without infection.

2. The machine is in the second stage, some malicious artifacts or some suspicious indicators of compromise are detected

3. The machine was detected safely by the Cybersecurity Specialist Team, and now was removed from the triage in Cisco Secure EndPoint

## 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）。