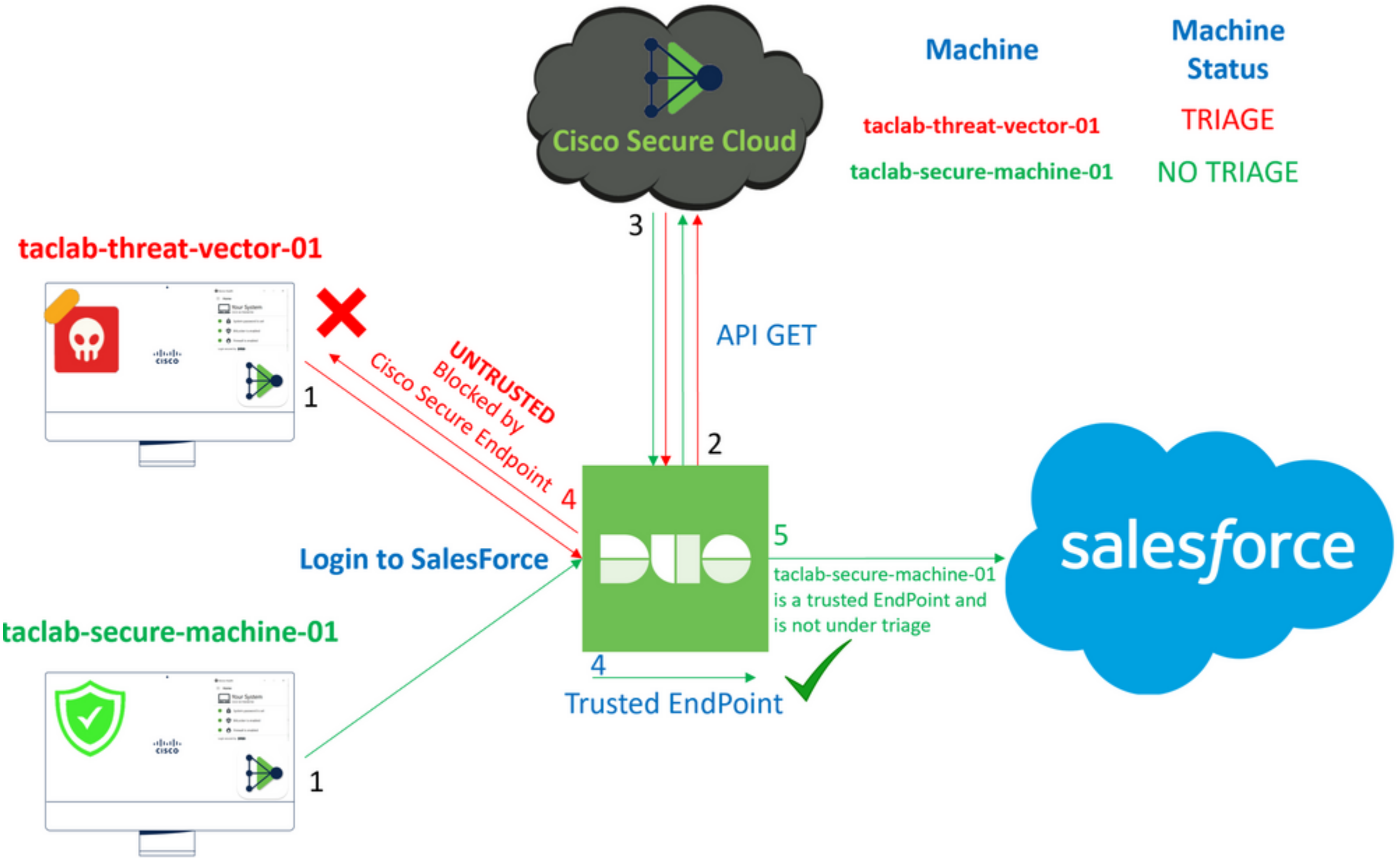
配置Duo和安全終端以響應威脅

目錄

簡介



本文檔介紹如何將Duo Trusted EndPoint與Cisco Secure EndPoint整合。

背景資訊

思科安全終端和Duo之間的整合可針對在受信任的網路裝置上檢測到的威脅進行有效合作。這種整合是通過多個裝置管理工具實現的，這些工具確定了每個裝置的可靠性。這些工具包括：

- Active Directory域服務
- 具有裝置運行狀況的Active Directory
- 與裝置運行狀況共用
- Intune with Device Health
- 含裝置健康狀態的Jamf Pro
- LANDESK管理套件
- Mac OS X企業資產管理工具
- 裝置運行狀況手冊
- Windows企業資產管理工具
- 具有裝置運行狀況的工作空間ONE

裝置與裝置管理工具整合後，可通過以下方式整合思科安全終端和Duo API 在 Administration Panel.隨後，必須在Duo中配置相應的策略，以執行可信裝置驗證並檢測可能會影響Duo保護的應用程式的受危害裝置。

注意：在這種情況下，我們使用Active Directory和裝置健康狀況。

必要條件

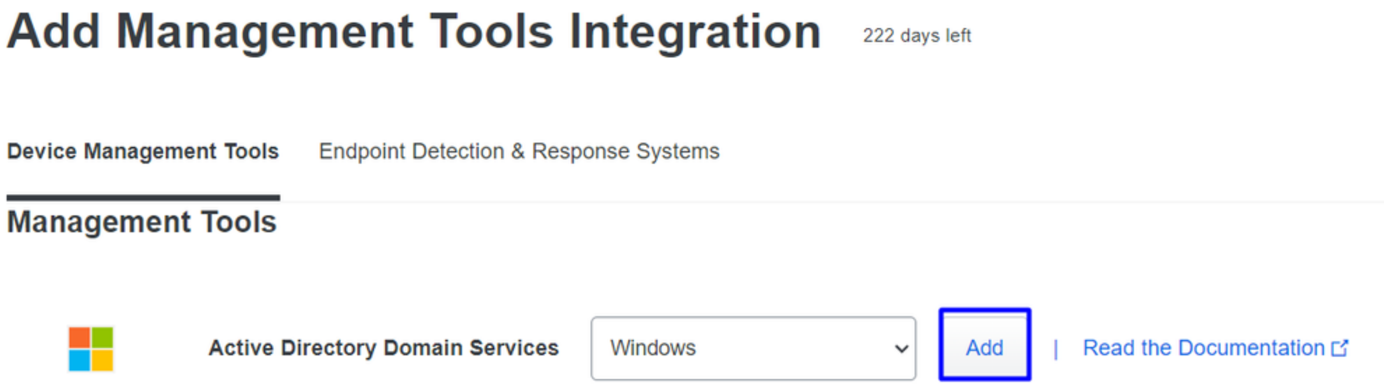
- 進行整合的Active Directory。
- 要將Duo與受信任的終端整合，您的裝置必須在Active Directory域中註冊。這允許Duo安全地驗證和授權對網路資源和服務的訪問。
- Duo Beyond Plan。

配置和使用案例

配置Duo中的整合

登入到 **Admin Panel** 並轉至：

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

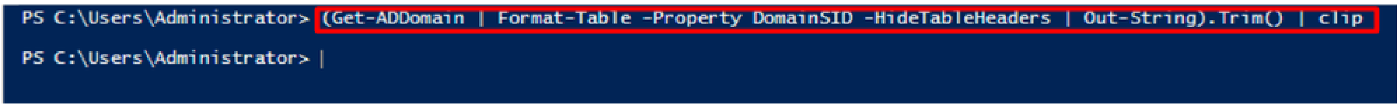

Add Management Tools Integration
222 days left
Device Management Tools
Endpoint Detection & Response Systems
Management Tools
Active Directory Domain Services
Windows
Add
|
Read the Documentation

之後，系統會將您重新導向至 **Active Directory and Device Health**.

請考慮這隻適用於域中的電腦。

轉到Active Directory並在PowerShell中運行下一個命令：

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



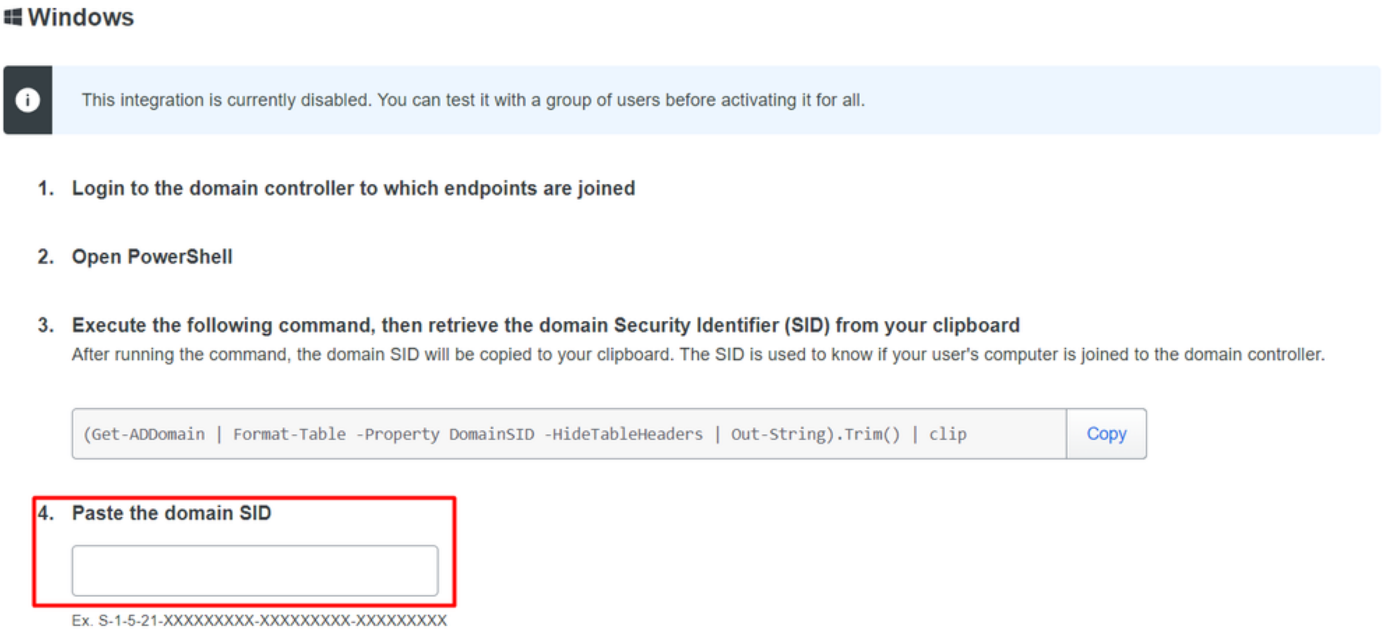
```
PS C:\Users\Administrator> (Get-ADDomain | Format-Table -Property DomainSID -HideTableHeaders | Out-String).Trim() | clip
PS C:\Users\Administrator> |
```

之後，請確保您已將Active Directory的安全識別符號複製到剪貼簿。

範例

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

這用於Active Directory和裝置運行狀況整合。



Windows

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

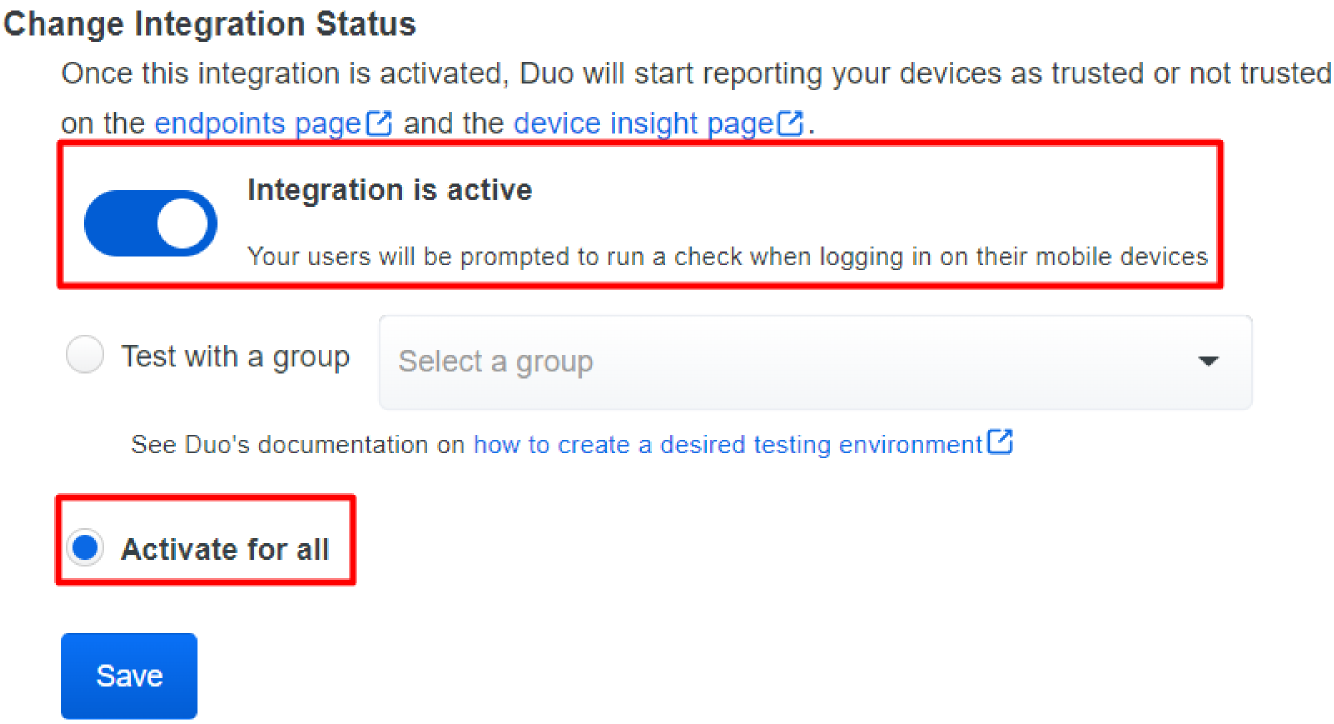
1. **Login to the domain controller to which endpoints are joined**
2. **Open PowerShell**
3. **Execute the following command, then retrieve the domain Security Identifier (SID) from your clipboard**
   After running the command, the domain SID will be copied to your clipboard. The SID is used to know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

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

4. **Paste the domain SID**

Ex. S-1-5-21-XXXXXXXXX-XXXXXXXXX-XXXXXXXXX

按一下 **Save** 並啟用整合和 Activate for all. 否則，您將無法與思科安全終端整合。



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

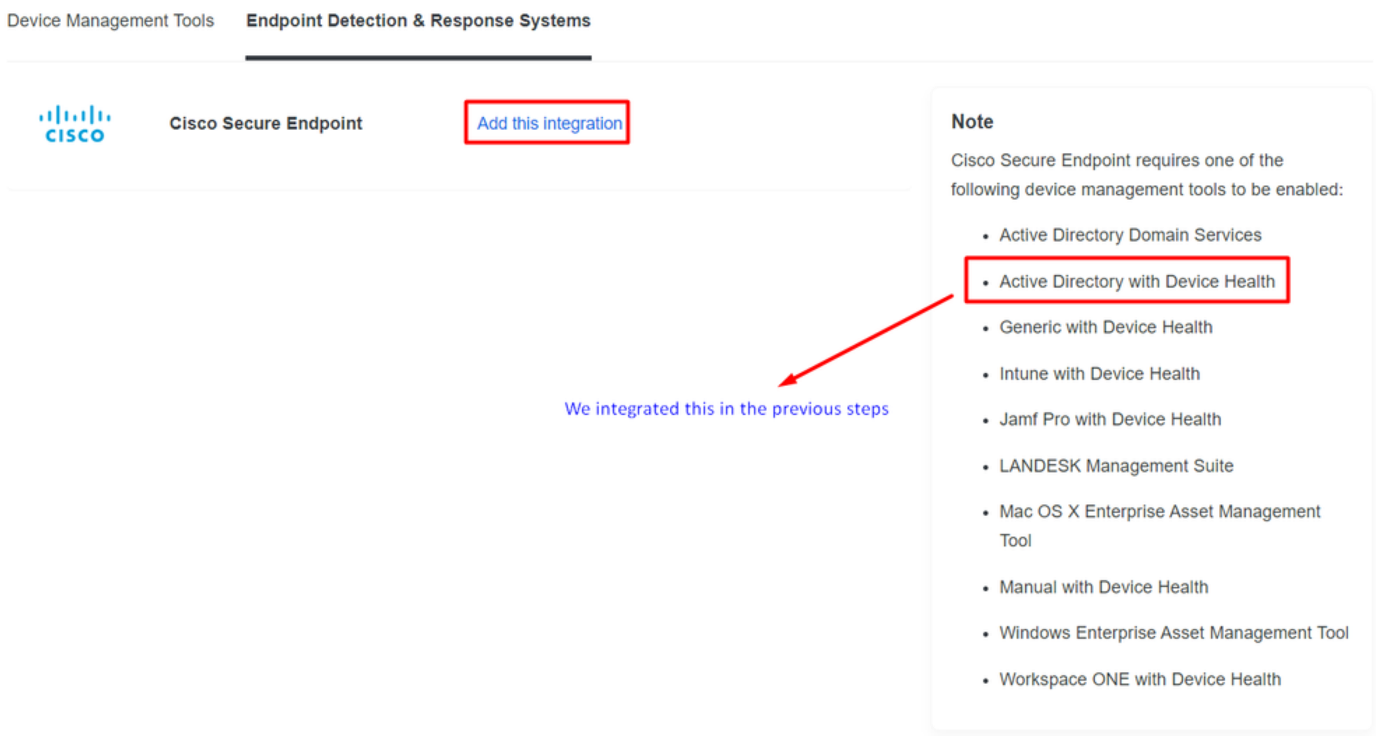
Your users will be prompted to run a check when logging in on their mobile devices

○ Test with a group

See Duo's documentation on how to create a desired testing environment

● **Activate for all**

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



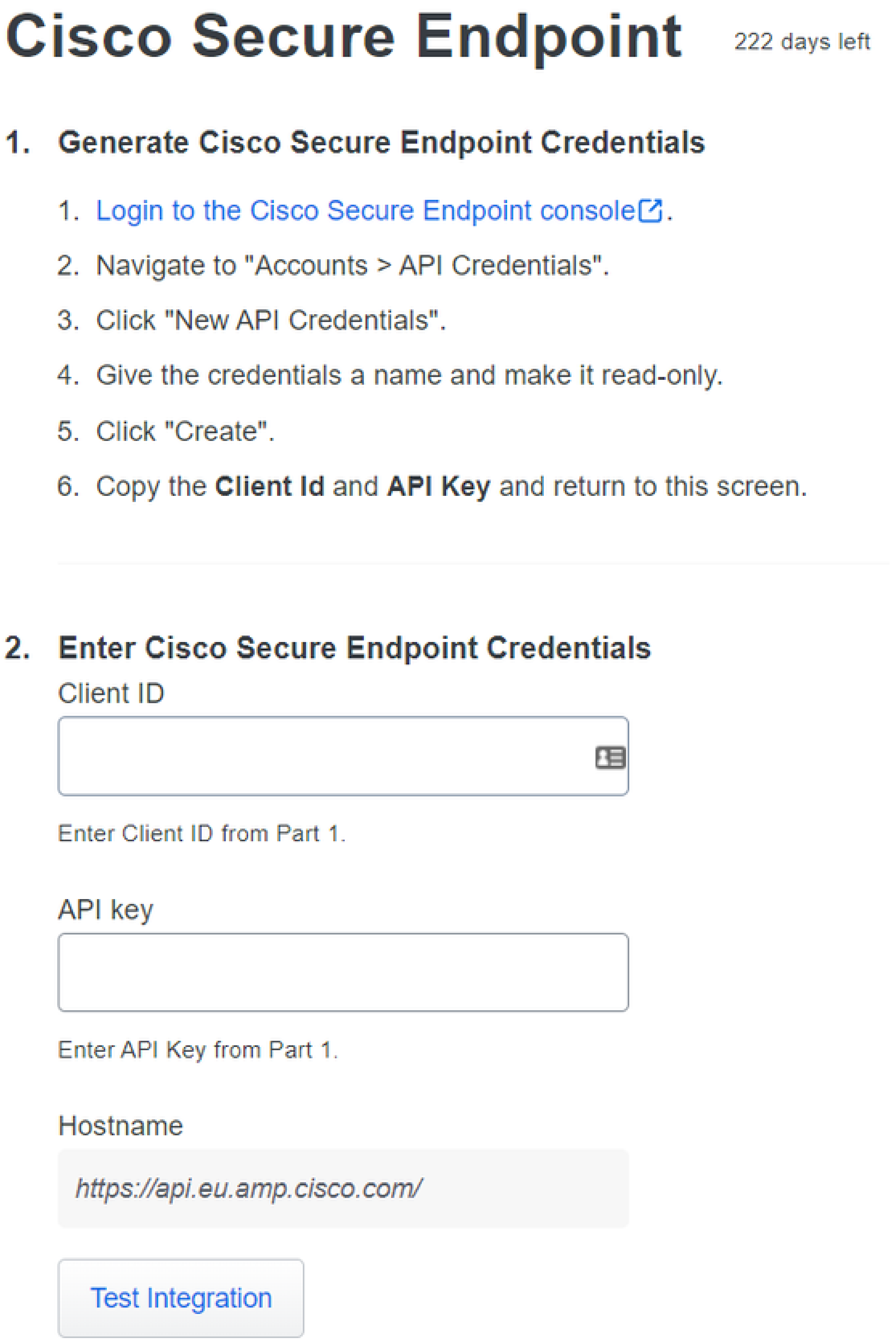
Device Management Tools
Endpoint Detection & Response Systems
Cisco Secure Endpoint
Add this integration
We integrated this in the previous steps

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

現在，您將進入思科安全終端整合首頁。



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

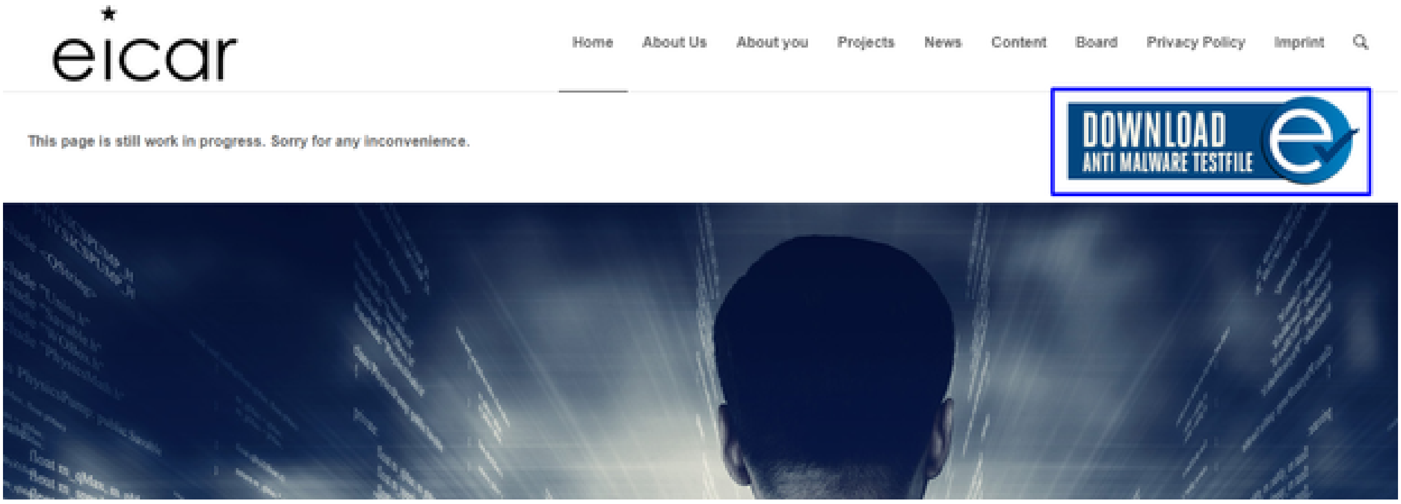
Enter API Key from Part 1.

Hostname

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

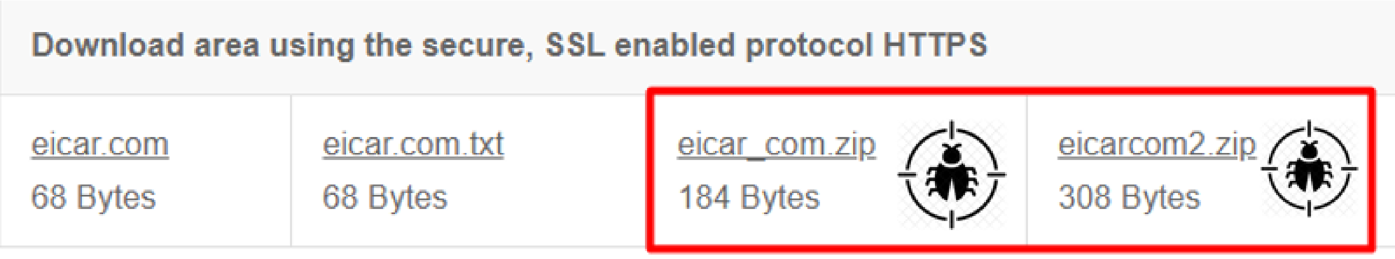
若要嘗試使用EICAR範例來測試功能，請存取https://www.eicar.org/，並下載惡意範例。

註：不要擔心。您可以下載該EICAR測試，它是安全的，它只是一個測試檔案。



This page is still work in progress. Sorry for any inconvenience.

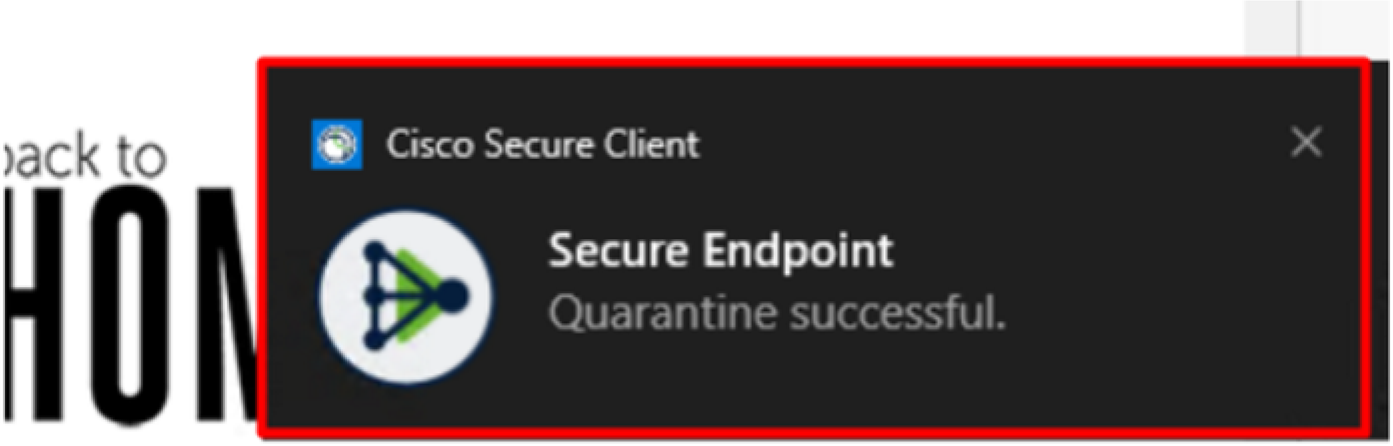
向下滾動並轉到部分並下載測試檔案。



Download area using the secure, SSL enabled protocol HTTPS

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

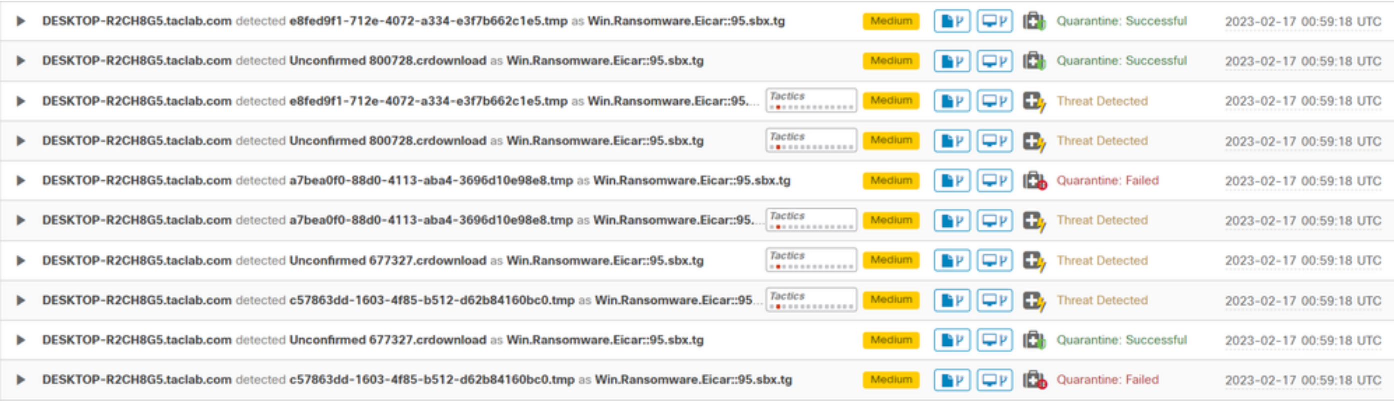
思科安全終端檢測到惡意軟體並將其移動到隔離區。



Cisco Secure Client

Secure Endpoint
Quarantine successful.

這是更改的方式，如思科安全終端管理面板所示。

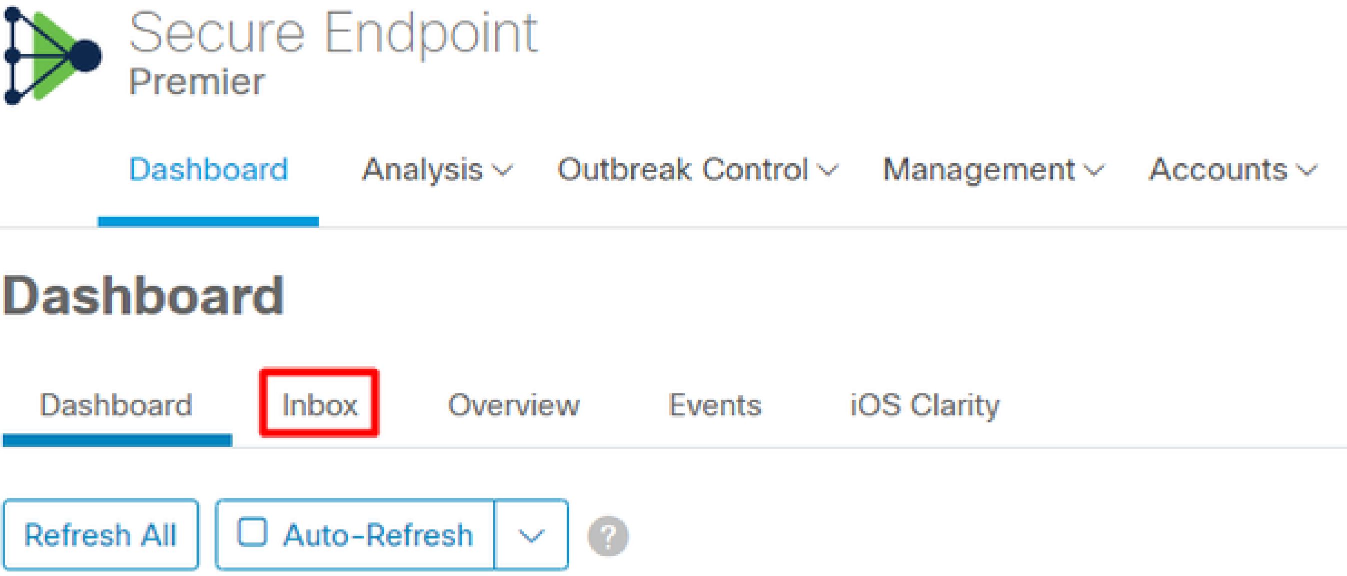


▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar::95.sbx.tg		Medium	Quarantine: Successful	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar::95.sbx.tg		Medium	Quarantine: Successful	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar::95...	Tactics	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	Tactics	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...	Tactics	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	Tactics	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...	Tactics	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

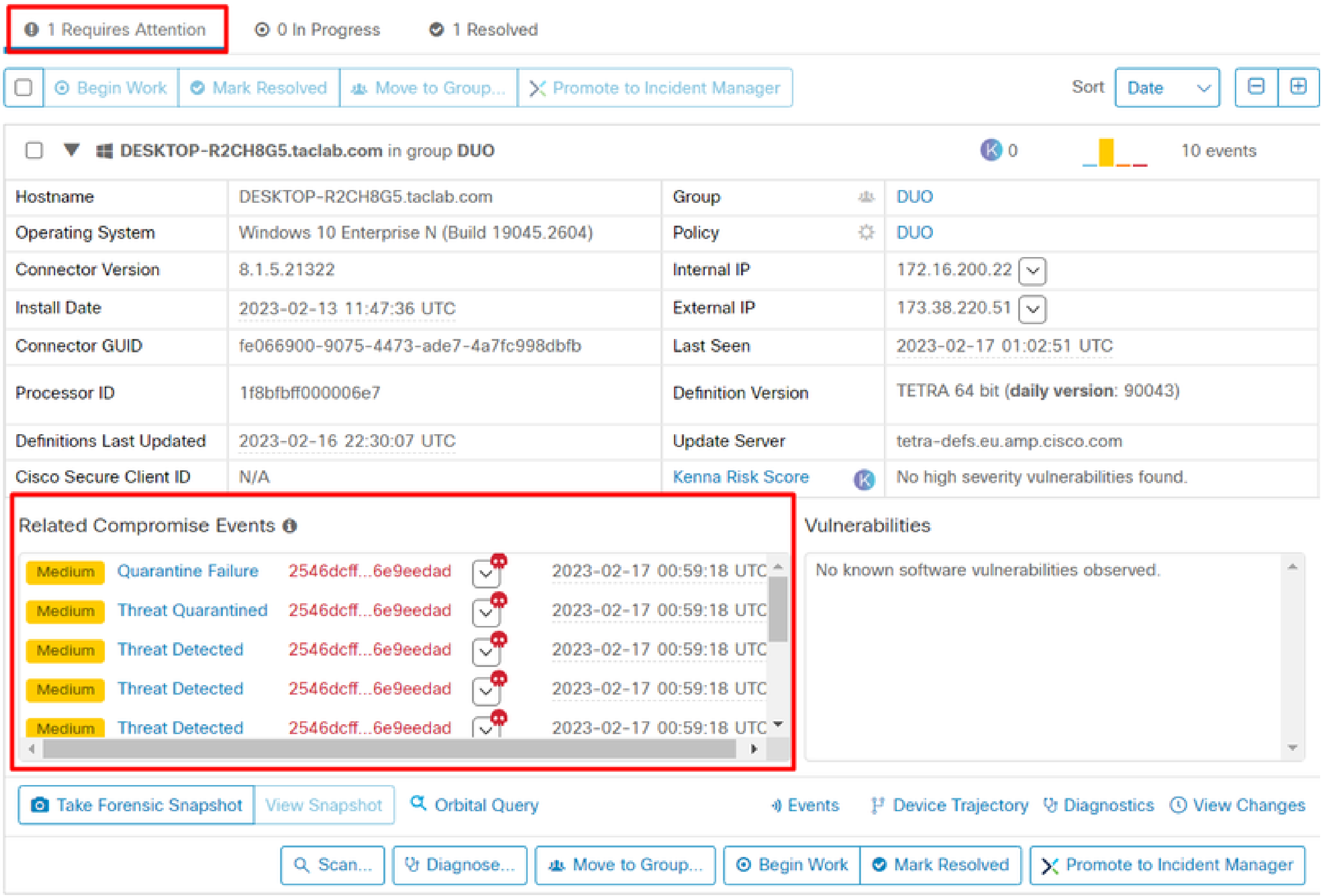
您還檢測到電腦中的惡意軟體，但這意味著端點被視為在 Inbox.

注意：要將端點傳送到分類程式，它需要多次檢測對象或啟用某些對象的奇怪行為 Indicators of Compromise 在端點中。

在 Dashboard中，按一下 **Inbox.**



現在，你擁有了一台需要關注的機器。



□ ▼ 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

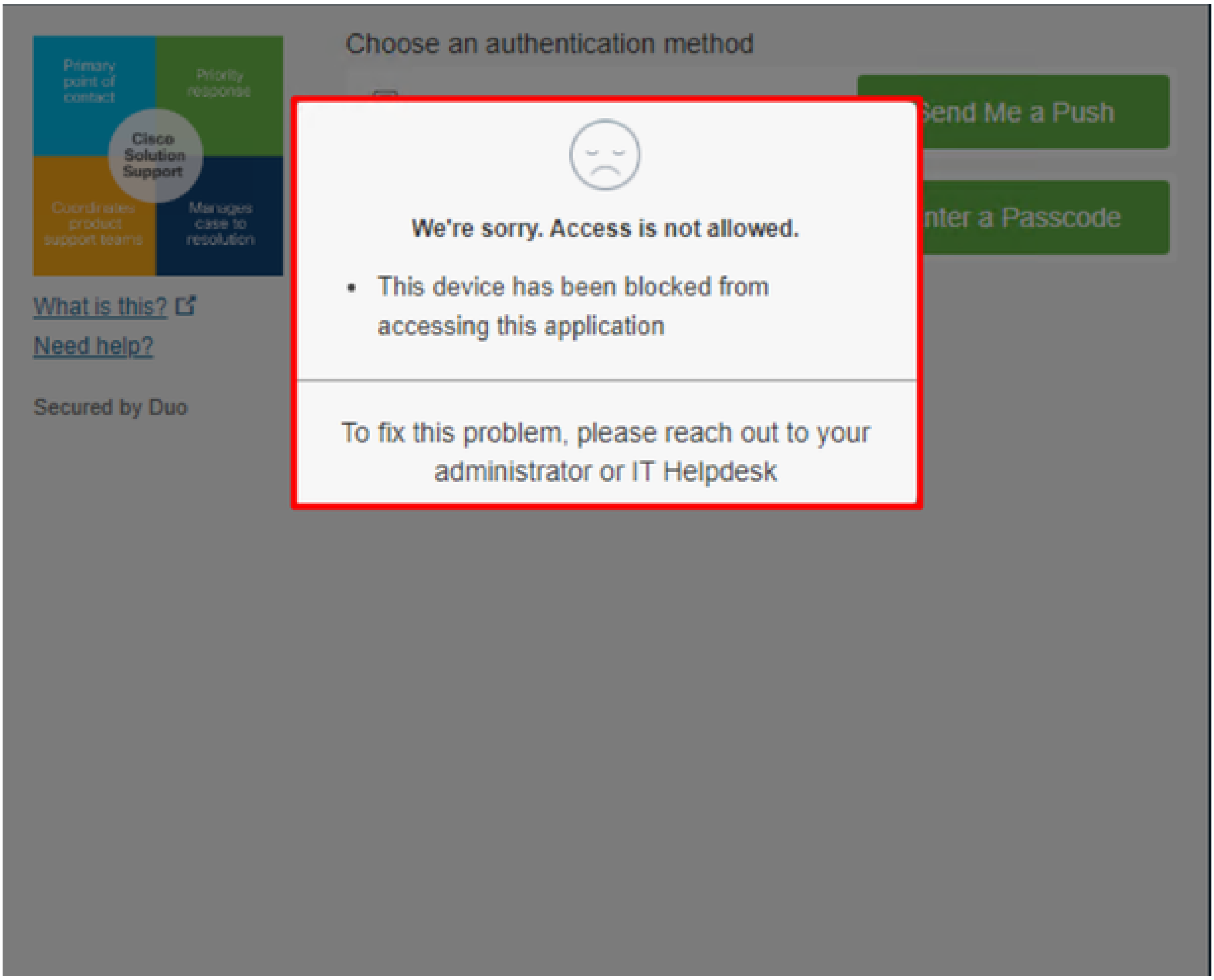
Medium	Quarantine Failure	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Quarantined	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad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

Vulnerabilities

No known software vulnerabilities observed.

現在，切換到Duo並檢視狀態。

首先嘗試進行驗證，以檢視電腦在思科安全終端上放置在 Require Attention.



Choose an authentication method

We're sorry. Access is not allowed.

- This device has been blocked from accessing this application

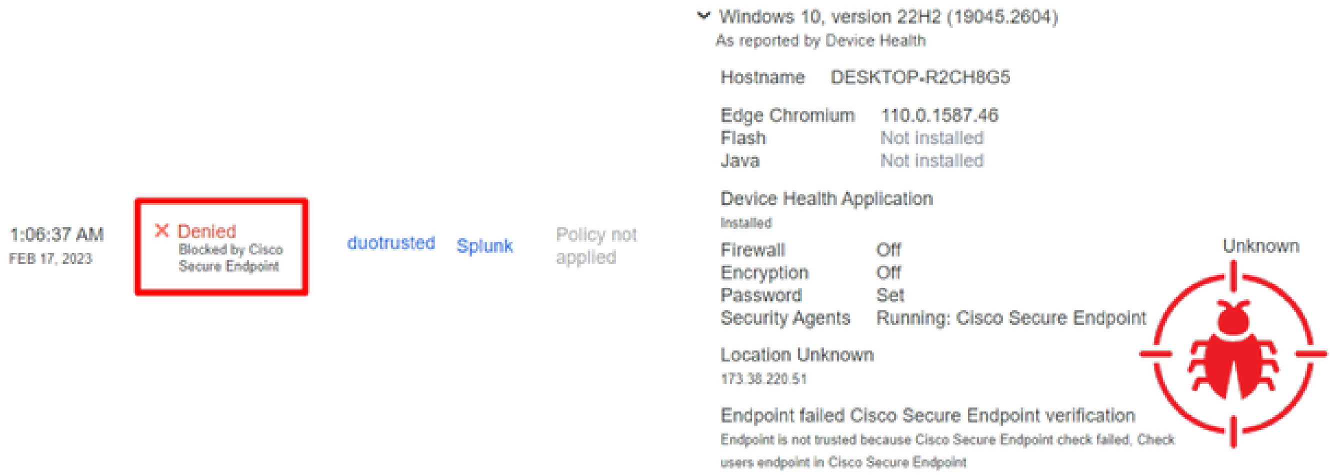
To fix this problem, please reach out to your administrator or IT Helpdesk

What is this?

Need help?

Secured by Duo

這就是Duo中的更改以及身份驗證事件下的事件顯示方式。



1:06:37 AM
FEB 17, 2023

✕ Denied
Blocked by Cisco Secure Endpoint

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

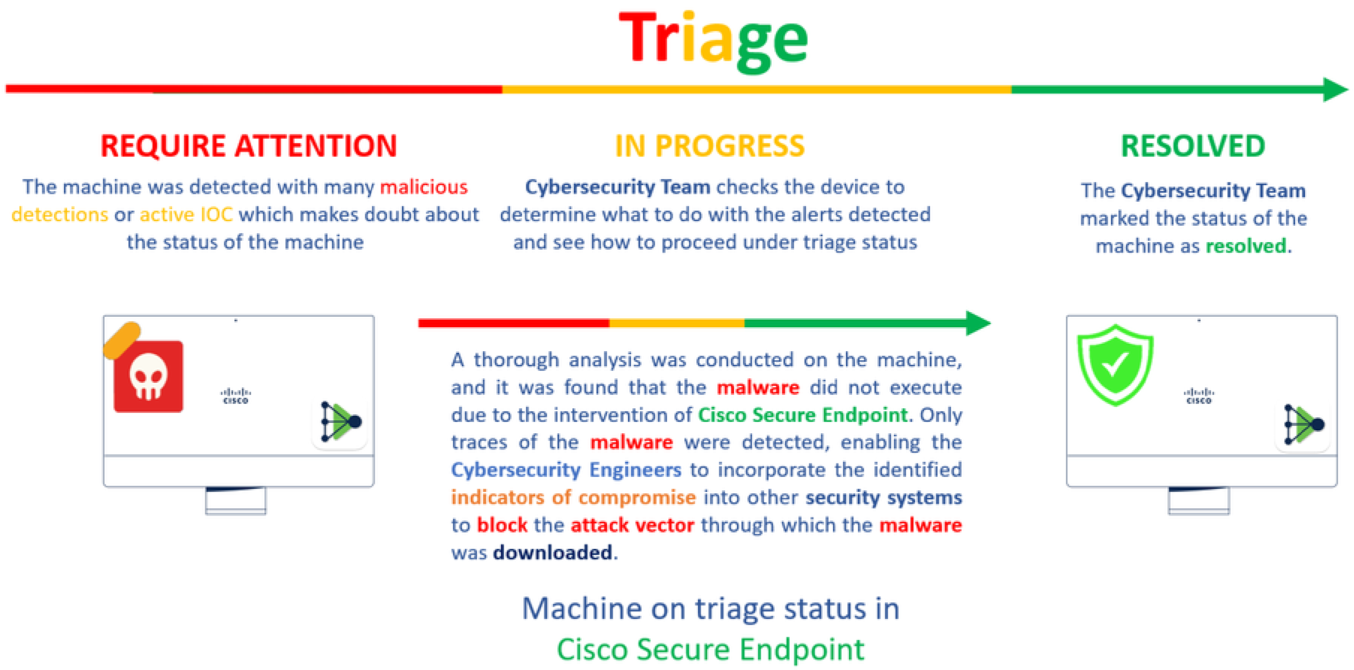
Firewall Off
Encryption Off
Password Set
Security Agents Running: Cisco Secure Endpoint

Location Unknown
173.38.220.51

Endpoint failed Cisco Secure Endpoint verification
Endpoint is not trusted because Cisco Secure Endpoint check failed, Check users endpoint in Cisco Secure Endpoint

已檢測到您的電腦不是組織的安全裝置。

審閱後允許訪問電腦



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

RESOLVED

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

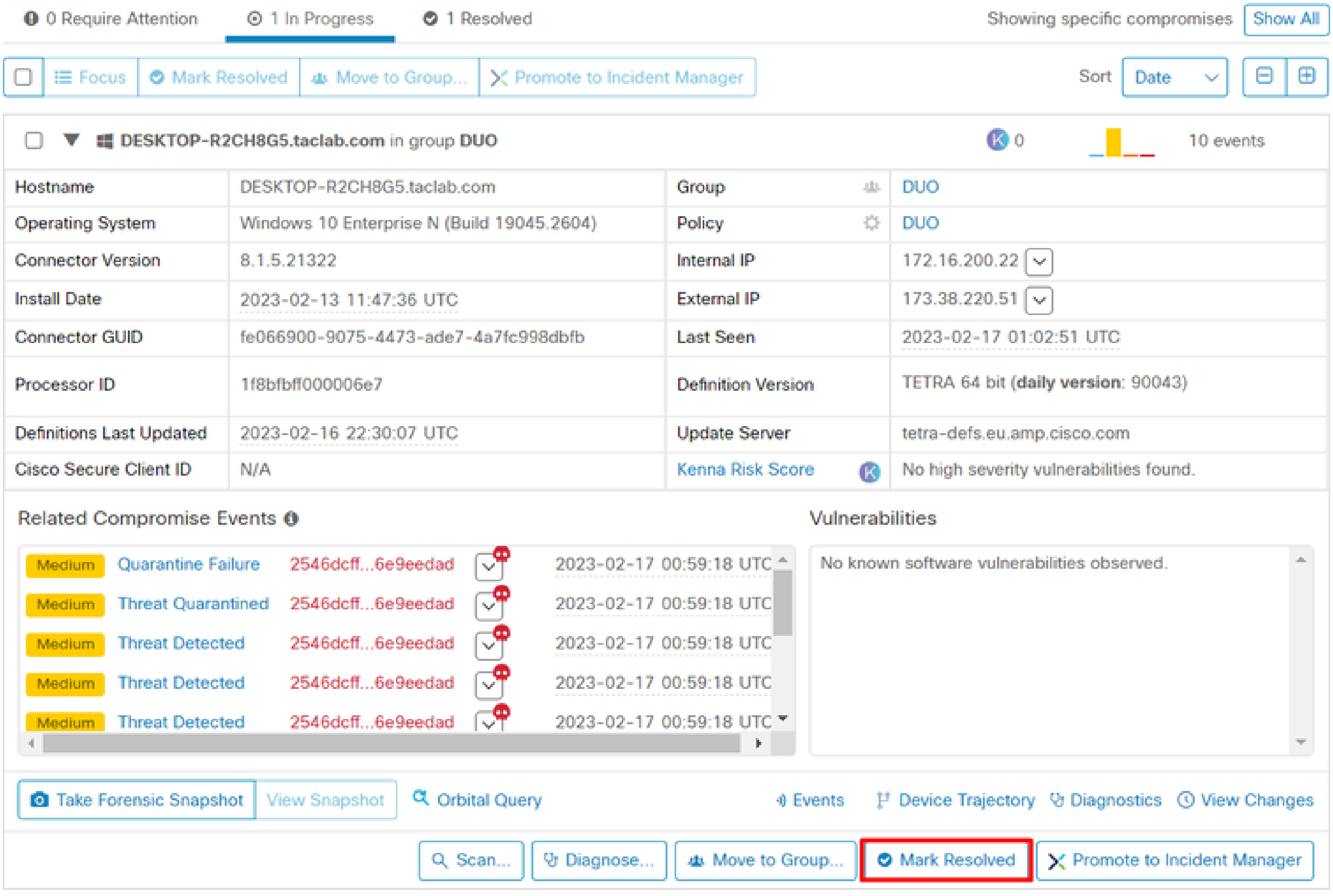
A thorough analysis was conducted on the machine, and it was found that the malware did not execute due to the intervention of Cisco Secure Endpoint. Only traces of the malware were detected, enabling the Cybersecurity Engineers to incorporate the identified indicators of compromise into other security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

Machine on triage status in
Cisco Secure Endpoint

在Cisco Secure EndPoint和網路安全專家進行驗證後，您可以在Duo中允許訪問您的應用。

現在的問題是，如何再次允許訪問受Duo保護的應用。

您需要使用思科安全終端和 Inbox，將此裝置標籤為 **resolved** ，允許訪問受Duo保護的應用程式。



□ ▼ DESKTOP-R2CH8G5.taclab.com in group DUO   K 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.

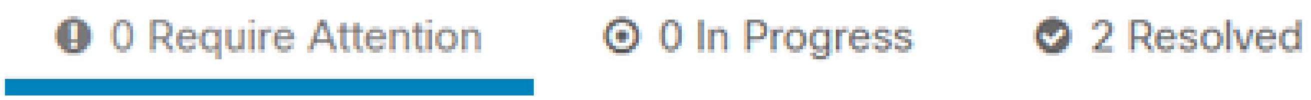
Related Compromise Events ❶

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

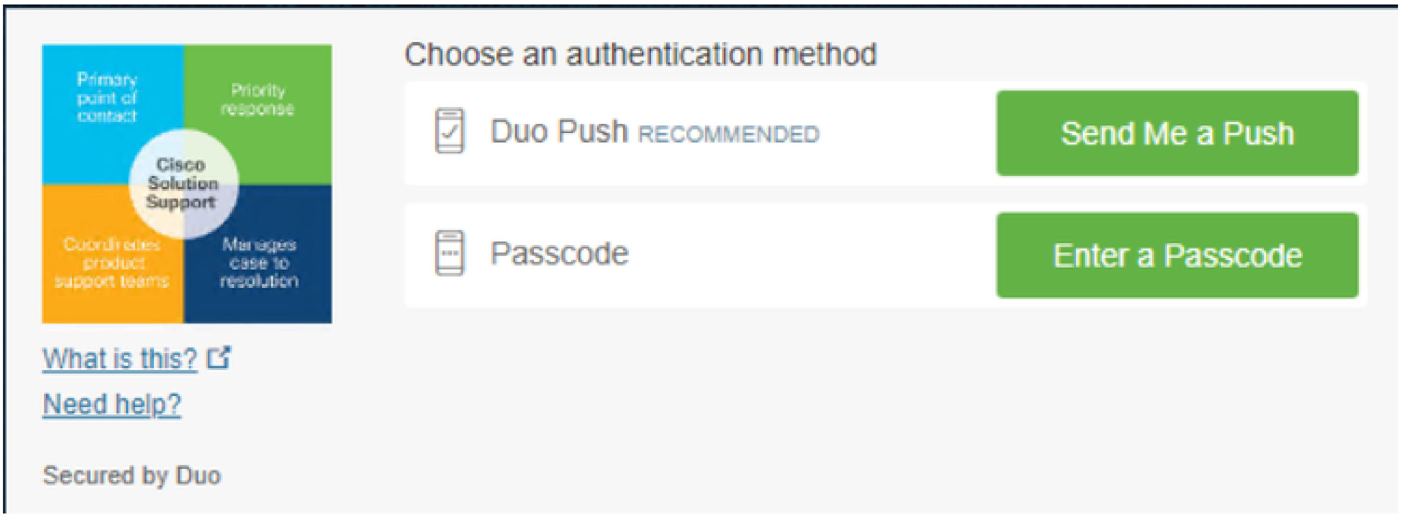
Vulnerabilities

No known software vulnerabilities observed.

之後，您的電腦將不會處於該狀態 attention required.此更改為 resolved 狀態.



簡而言之，現在您已經準備好再次測試對我們受Duo保護的應用程式的訪問。



Choose an authentication method

Duo Push RECOMMENDED

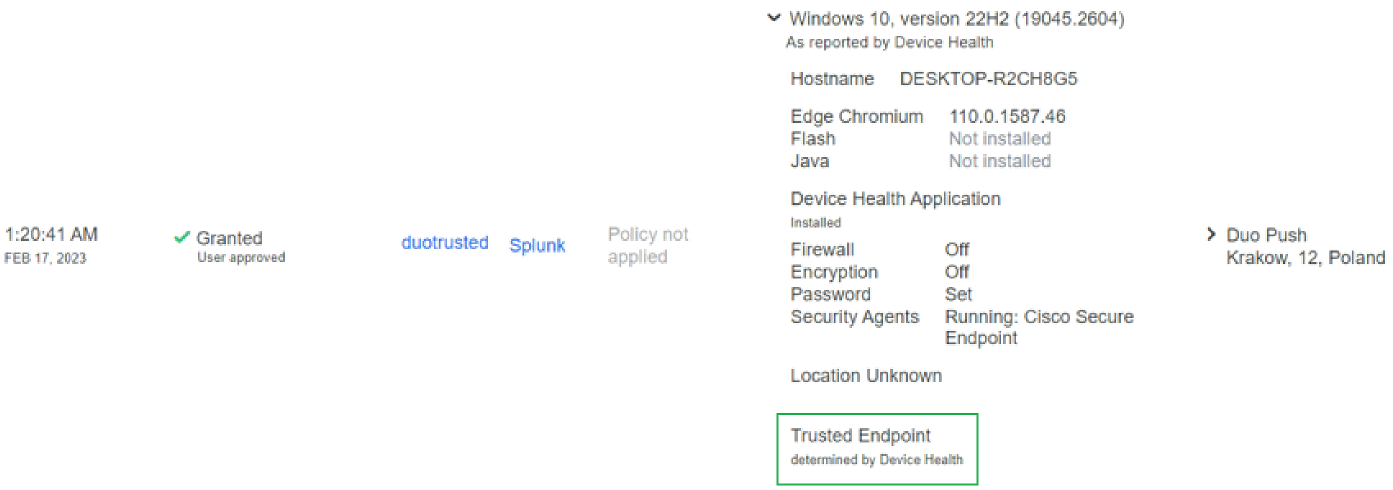
Passcode

What is this?

Need help?

Secured by Duo

現在，你擁有了向Duo傳送推送的許可權，並且你已登入該應用。



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

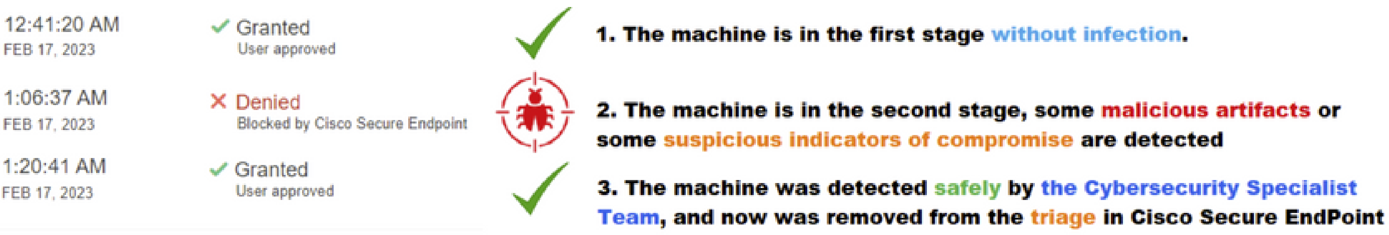
Firewall Off
Encryption Off
Password Set
Security Agents Running: Cisco Secure Endpoint

Location Unknown

Trusted Endpoint
determined by Device Health

Duo Push
Krakow, 12, Poland

分類工作流



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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。