

# 脅威に対応するためのDuoおよびセキュアエンドポイントの設定

## 内容

[はじめに](#)

[背景説明](#)

[前提条件](#)

[設定と使用例](#)

[Duoでの統合の設定](#)

[Cisco Secure EndPointでの統合の設定](#)

[Duoでのポリシーの設定](#)

[信頼できるデバイスを検出するためのポリシーの設定](#)

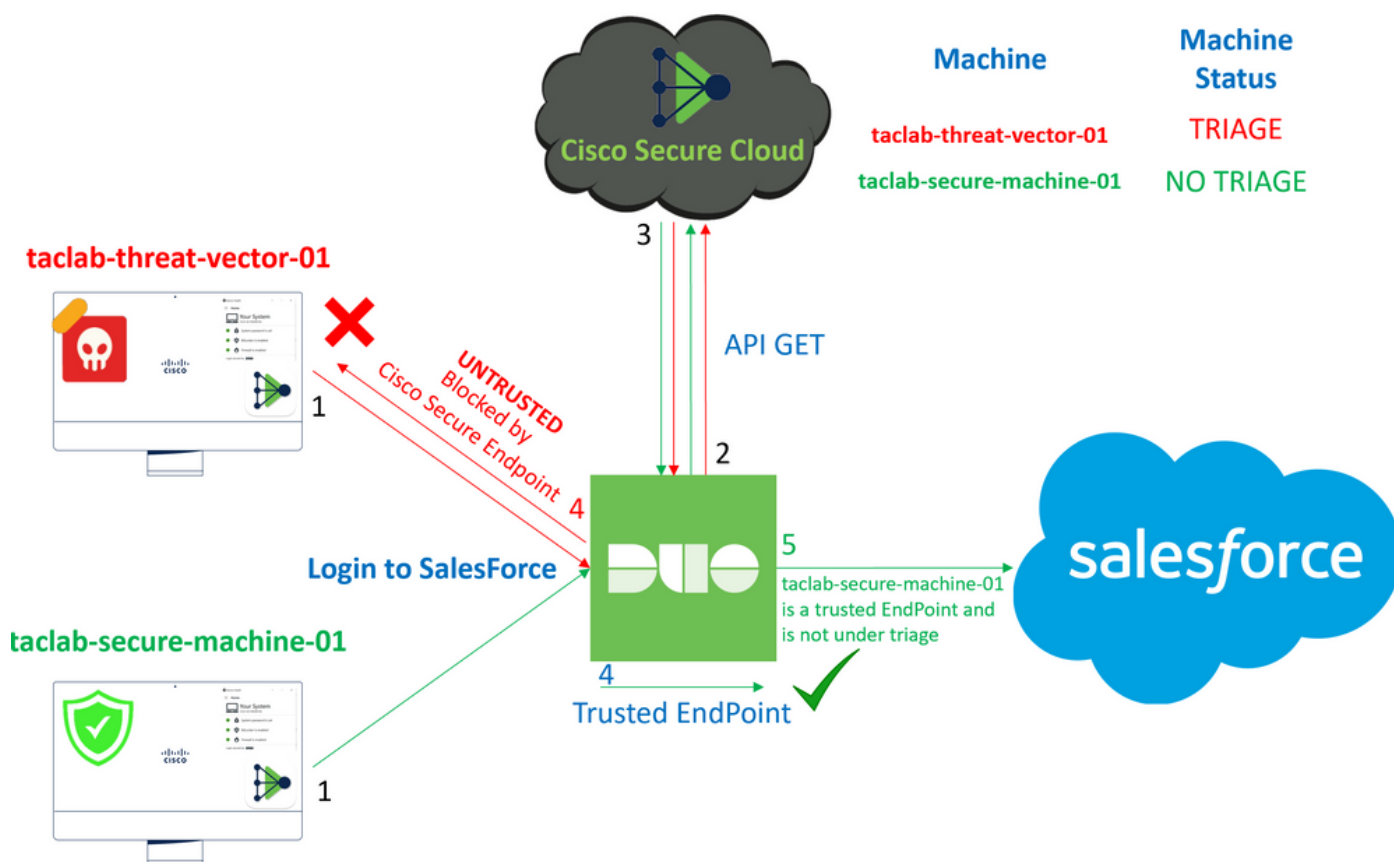
[信頼できるマシンのテスト](#)

[Cisco Secure EndPointのポリシーの設定](#)

[Cisco Secure EndPointを使用した信頼できるマシンのテスト](#)

[レビュー後にマシンへのアクセスを許可する](#)

## はじめに



このドキュメントでは、Duo Trusted EndPoint(CTI)とCisco Secure EndPointを統合する方法について説明します。

## 背景説明

Cisco Secure EndPointとDuoの統合により、信頼できるネットワークデバイス上で検出された脅威に対する効果的なコラボレーションが可能になります。この統合は、各デバイスの信頼性を確立する複数のデバイス管理ツールによって実現されます。これらのツールの一部は次のとおりです。

- Active Directoryドメインサービス
- Active Directoryとデバイスヘルス
- デバイスヘルスを含む汎用
- Intuneとデバイスのヘルス
- Jamf Proとデバイスヘルス
- LANDESK管理スイート
- Mac OS Xエンタープライズ資産管理ツール
- デバイスの状態を手動で確認
- Windows Enterprise Asset Managementツール
- デバイスヘルス機能を備えたWorkspace ONE

デバイスをデバイス管理ツールと統合すると、次の方法でCisco Secure EndPointとDuoを統合できます [API の Administration Panel](#) を参照。その後、Duoで適切なポリシーを設定して、信頼できるデバイスの検証を実行し、Duoで保護されたアプリケーションに影響を与える可能性がある侵害されたデバイスを検出する必要があります。



注：この場合、Active Directoryとデバイスの状態を使用します。

---

## 前提条件

- 統合を行うためのActive Directory。
- DuoとTrusted Endpointsを統合するには、デバイスをActive Directoryドメインに登録する必要があります。これにより、Duoはネットワークリソースとサービスへのアクセスを安全に認証および許可できます。
- Duo Beyond Planの略。

## 設定と使用例

### Duoでの統合の設定

にログインします [Admin Panel](#) 次のリンクに移動します。

- [Trusted EndPoints > Add Integration](#)
- **選択** [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](#)

その後で、 **Active Directory and Device Health**を参照。

これはドメイン内のマシンでのみ機能することを考慮してください。

Active Directoryに移動し、PowerShellで次のコマンドを実行します。

```
(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> |
```

その後、Active DirectoryのセキュリティIDをクリップボードにコピーしたことを確認します。

例

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

これは、Active Directoryとデバイスの正常性の統合で使用されます。

## 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
```

Copy

4. Paste the domain SID

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

クリック [Save 統合を実現し – Activate for all](#) を参照。 そうしないと、Cisco Secure EndPointと統合できません。

## 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

Select a group



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



**Activate for all**

Save

次に [Trusted EndPoints > Select Endpoint Detection & Response System > Add this integration](#) を参照。



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](#)

これで、Cisco Secure EndPointの統合のメインページが表示されます。

# 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.

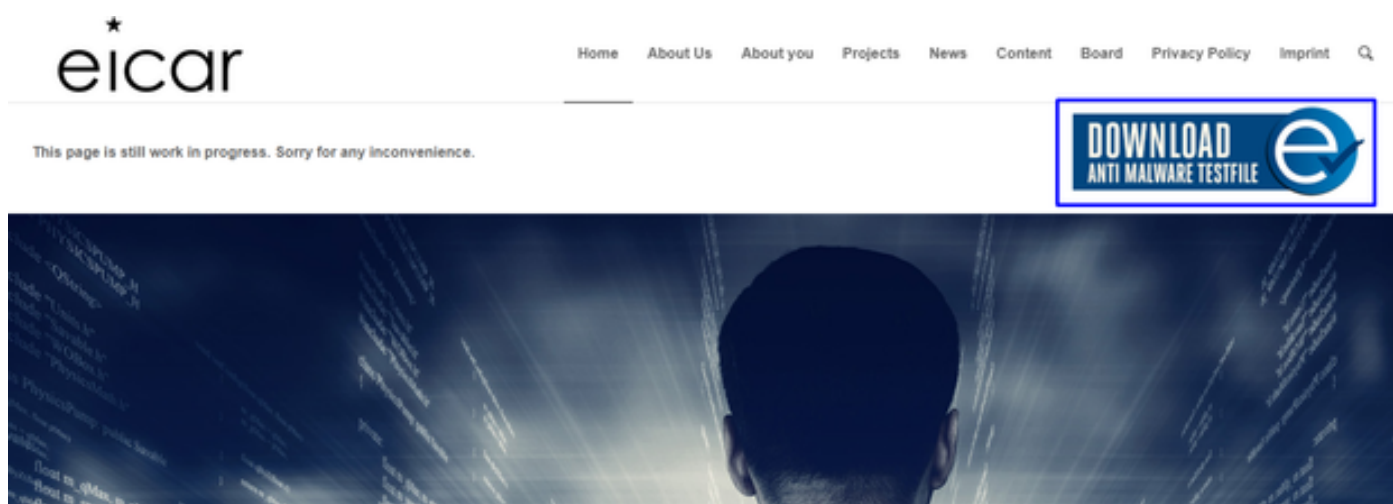
Hostname

*<https://api.eu.amp.cisco.com/>*



[Test Integration](#)

EICARの例を使用して機能をテストするには、<https://www.eicar.org/>にアクセスし、悪意のあるサンプルをダウンロードします。

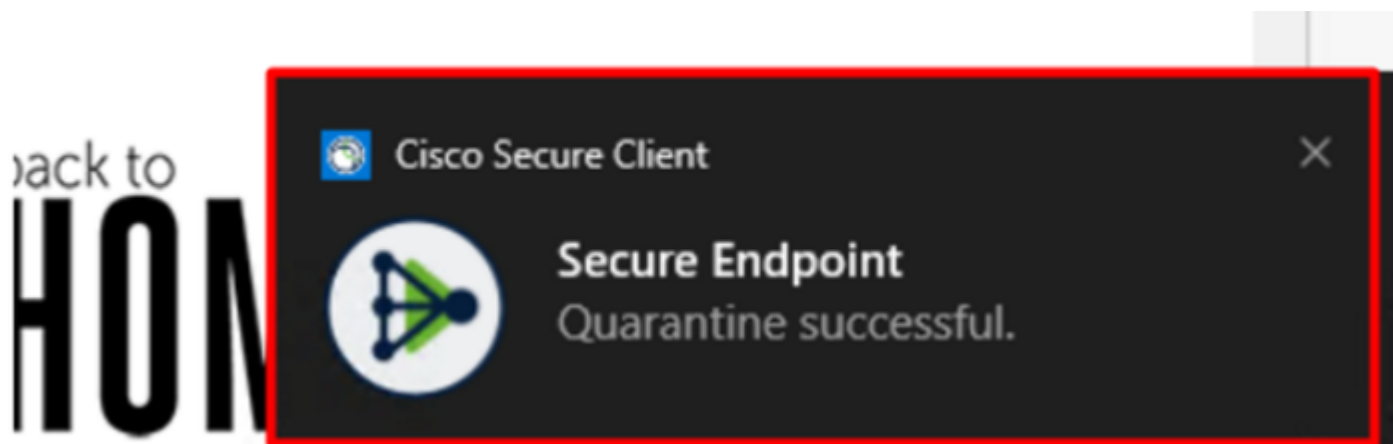
 注：心配しないでください。EICARテストをダウンロードできます。これは安全で、テストファイルだけです。



下にスクロールしてセクションに移動し、テストファイルをダウンロードします。

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がマルウェアを検出し、検疫に移動します。



これが、Cisco Secure EndPoint Adminパネルに表示される変更方法です。

▶ 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

マシン内のマルウェアも検出されますが、これはエンドポイントがCisco Secure EndPointのトリアージで分析されると見なされることを意味します。Inboxを参照。

注：エンドポイントをトリアージに送信するには、複数のアーティファクトの検出または一部の動作をアクティブ化する異常な動作が必要です Indicators of Compromise 確認します。

の下 Dashboardをクリックし、Inboxを参照。



Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

## Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

Refresh All

Auto-Refresh



今、あなたは注意を必要とするマシンを持っています。



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

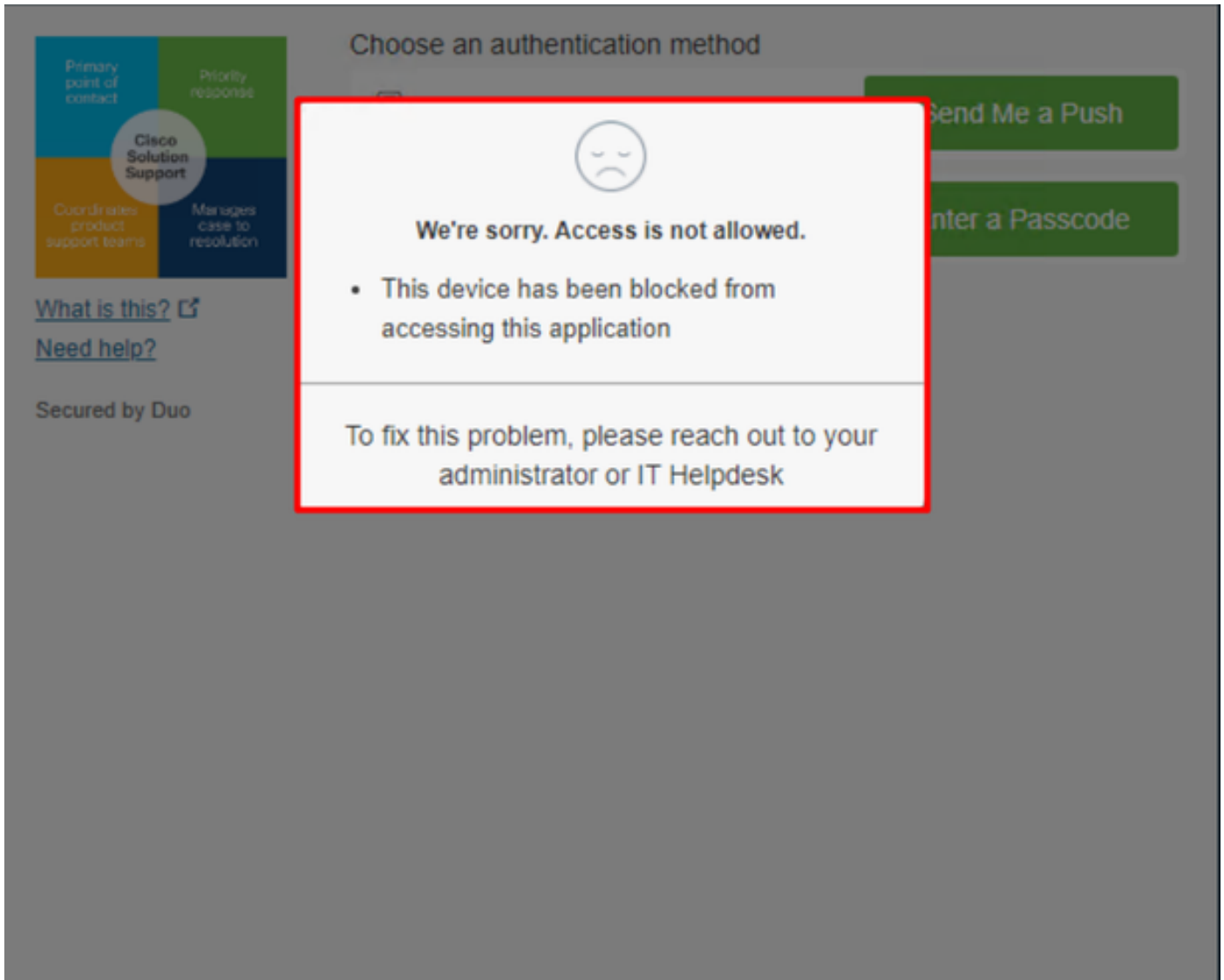
No known software vulnerabilities observed.

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

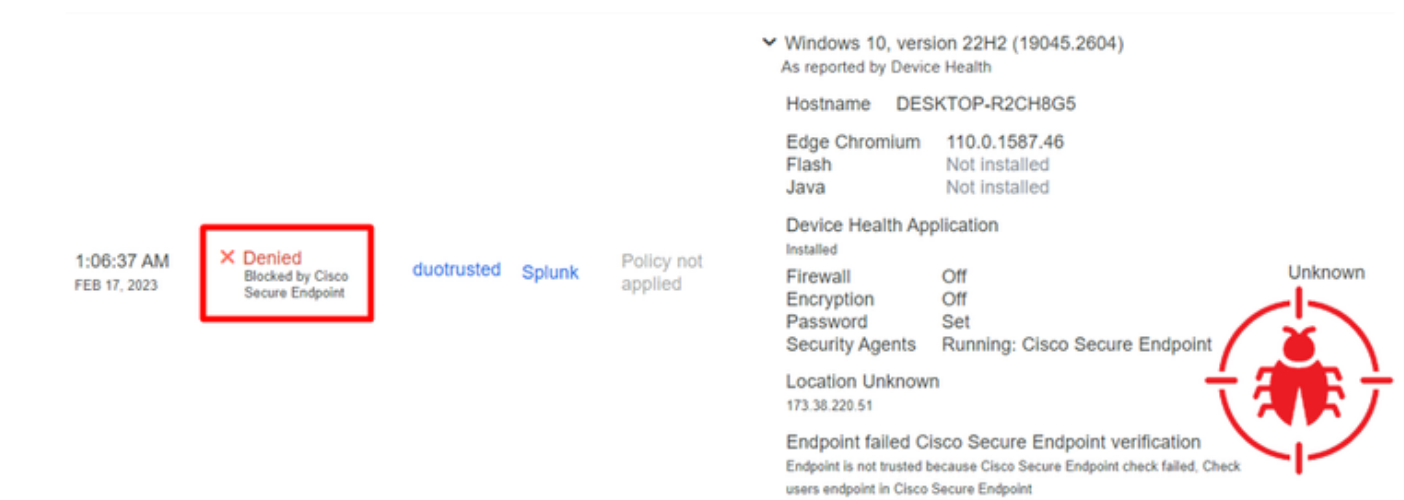
Scan... Diagnose... Move to Group... Begin Work Mark Resolved Promote to Incident Manager

次に、Duoに切り替えて、ステータスを確認します。

マシンがCisco Secure EndPointの下に配置された後、最初に認証が試行されて動作が確認されま  
す Require Attentionを参照。



これは、Duoでの変更と、認証イベントでのイベントの表示方法です。



お使いのコンピューターは、組織の安全装置として検出されませんでした。

レビュー後にマシンへのアクセスを許可する

# 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

Cisco Secure EndPointで検証を行い、Cybersecurity Specialistの認定を受けた後、Duoでこのマシンからアプリへのアクセスを許可できます。

ここで問題は、Duoによって保護されたアプリへのアクセスを再び許可する方法です。

Cisco Secure EndPointにアクセスし、Inbox、このデバイスを次のようにマーク resolved Duoで保護されたアプリケーションへのアクセスを許可します。

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	1f8bfbff0000006e7	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

その後、ステータスのマシンはありません *attention required* を参照。これは次のように変化しました  
resolved ステータス。

00:00:00

00:00:00

0 Require Attention

0 In Progress

2 Resolved

一言で言えば、今、あなたはDuoによって保護された私たちのアプリケーションへのアクセスを再びテストする準備ができています。

これで、Duoにプッシュを送信する権限が与えられ、アプリにログインしました。

### トリアージワークフロー

- 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**

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。