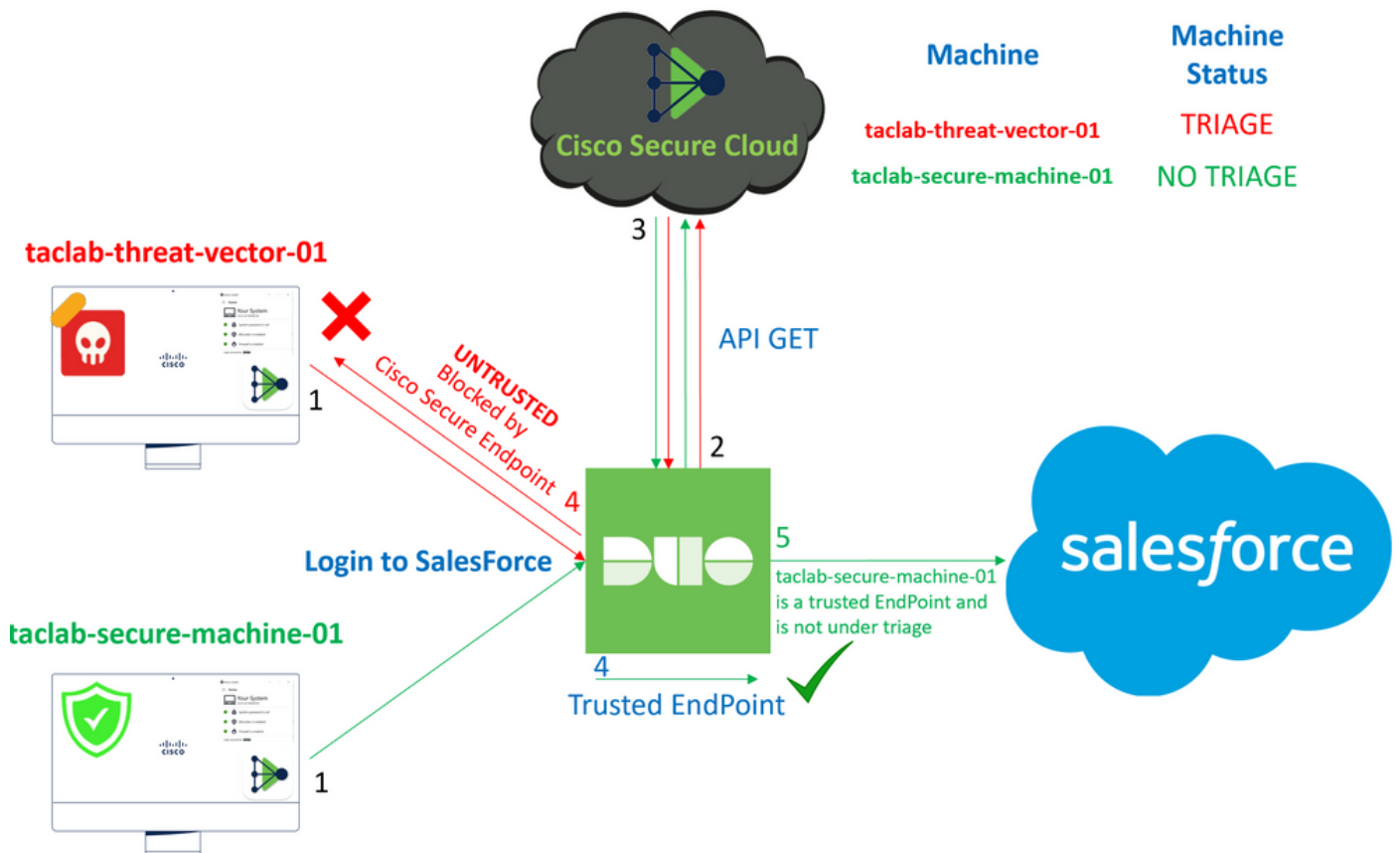


# 위협에 대응하기 위한 Duo 및 보안 엔드포인트 구성

## 목차

- [소개](#)
- [배경 정보](#)
- [사전 요구 사항](#)
- [구성 및 활용 사례](#)
  - [Duo에서 통합 구성](#)
  - [Cisco Secure EndPoint에서 통합 구성](#)
  - [듀오에서 정책 구성](#)
    - [신뢰할 수 있는 디바이스를 탐지하도록 정책 구성](#)
    - [신뢰할 수 있는 컴퓨터 테스트](#)
    - [Cisco Secure EndPoint용 정책 구성](#)
    - [Cisco Secure EndPoint로 신뢰할 수 있는 시스템 테스트](#)
    - [검토 후 시스템에 대한 액세스 허용](#)

## 소개



이 문서에서는 Duo Trusted EndPoint를 Cisco Secure EndPoint와 통합하는 방법에 대해 설명합니다.

## 배경 정보

Cisco Secure EndPoint와 Duo의 통합으로 신뢰할 수 있는 네트워크 장치에서 탐지된 위협에 효과적으로 대응할 수 있습니다. 이러한 통합은 각 장치의 신뢰성을 확립하는 여러 장치 관리 툴을 통해 이루어집니다. 이러한 툴에는 다음이 포함됩니다.

- Active Directory 도메인 서비스
- 디바이스 상태가 있는 Active Directory
- 장치 상태가 있는 일반
- 장치 상태가 있는 Intune
- Jamf Pro with Device Health
- LANDESK Management Suite
- Mac OS X Enterprise Asset Management 툴
- 디바이스 상태를 포함한 수동
- Windows 엔터프라이즈 자산 관리 도구
- Workspace ONE(디바이스 상태 포함)

디바이스가 디바이스 관리 툴과 통합되면 다음을 통해 Cisco Secure EndPoint 및 Duo를 통합할 수 있습니다. API 의 Administration Panel. 그런 다음 신뢰할 수 있는 장치 확인을 실행하고 Duo가 보호하는 애플리케이션에 영향을 줄 수 있는 손상된 장치를 탐지하려면 Duo에서 적절한 정책을 구성해야 합니다.

---

 참고: 이 경우 Active Directory 및 Device Health를 사용합니다.

---

## 사전 요구 사항

- Active Directory를 사용하여 통합합니다.
- Duo를 신뢰할 수 있는 엔드포인트와 통합하려면 디바이스가 Active Directory 도메인에 등록되어 있어야 합니다. 이를 통해 Duo는 네트워크 리소스 및 서비스에 대한 액세스를 안전하게 인증하고 권한을 부여할 수 있습니다.
- Duo Beyond Plan.

## 구성 및 활용 사례

### Duo에서 통합 구성

에 로그인합니다 Admin Panel 다음 사이트로 이동합니다.

- **Trusted EndPoints > Add Integration**
- 선택 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](#)

그런 다음 리디렉션하여 **Active Directory and Device Health**.

도메인의 시스템에서만 작동한다는 점을 고려하십시오.

Active Directory로 이동하여 PowerShell에서 다음 명령을 실행합니다.

```
(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> |
```

그런 다음 Active Directory의 보안 식별자를 클립보드에 복사해야 합니다.

예

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

이는 Active Directory 및 디바이스 상태 통합에서 사용됩니다.

## 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

클릭 **Save 통합 및 Activate for all**. 그렇지 않으면 Cisco Secure EndPoint와 통합할 수 없습니다.

### 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

이동 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

이제 Cisco Secure EndPoint의 통합 메인 페이지에 나와 있습니다.

# 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.

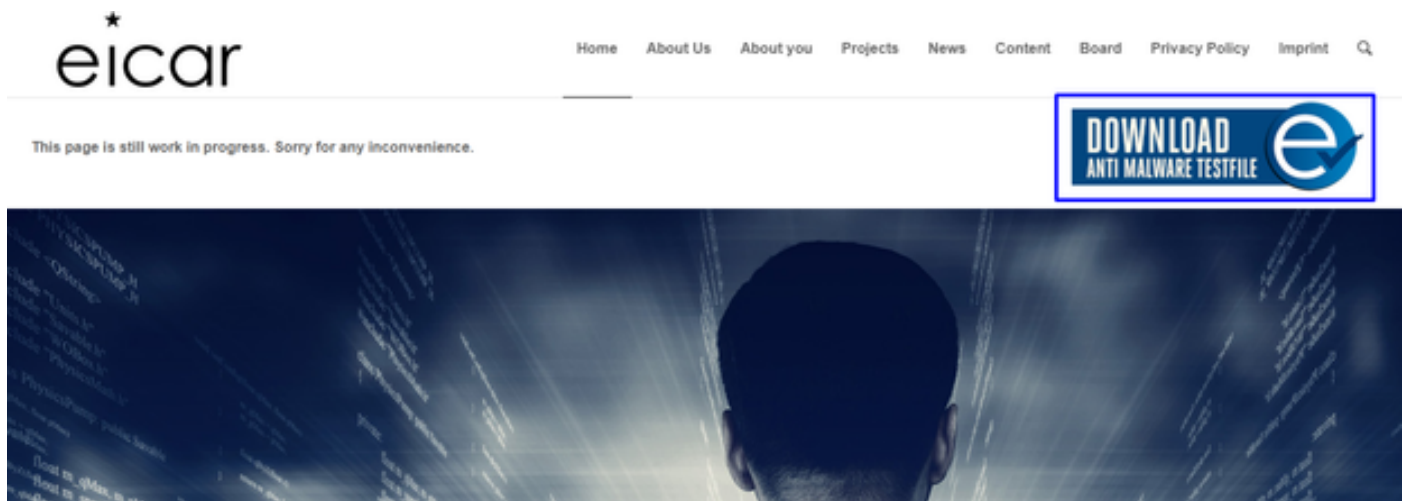
Hostname

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



[Test Integration](#)

EICAR의 예를 사용하여 기능을 테스트하려면 <https://www.eicar.org/>에 [액세스하고](#) 악성 샘플을 다운로드합니다.

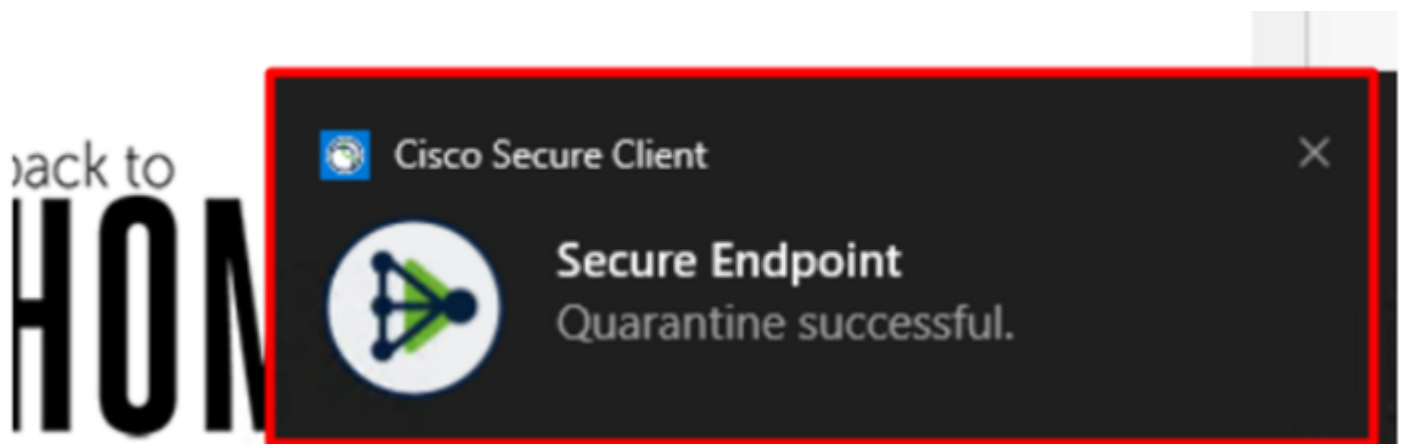
 참고: 걱정하지 마십시오. EICAR 테스트를 다운로드할 수 있으며, 안전하며 테스트 파일일 뿐입니다.



아래로 스크롤하여 섹션으로 이동하고 테스트 파일을 다운로드합니다.

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 EndPoint는 악성코드를 탐지하여 격리로 이동합니다.



이것이 Cisco Secure EndPoint Admin(Cisco Secure EndPoint 관리) 패널에 표시된 대로 변경되는 방법입니다.

▶ 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...	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...	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...	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

또한 시스템에서 악성코드를 탐지했지만, 이는 엔드포인트가 Cisco Secure EndPoint의 분류에 따라 분석된 것으로 간주된다는 것을 의미합니다. Inbox.

참고: 분류하기 위해 엔드포인트를 전송하려면 아티팩트를 여러 번 탐지하거나 일부를 활성화하는 이상한 동작이 있어야 합니다 Indicators of Compromise 엔드포인트에서 실행됩니다.

아래 Dashboard, 를 클릭합니다. Inbox.



[Dashboard](#) [Analysis](#) [Outbreak Control](#) [Management](#) [Accounts](#)

## Dashboard

[Dashboard](#) [Inbox](#) [Overview](#) [Events](#) [iOS Clarity](#)

[Refresh All](#)  [Auto-Refresh](#)

이제 주의해야 할 기계가 생겼네요.



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

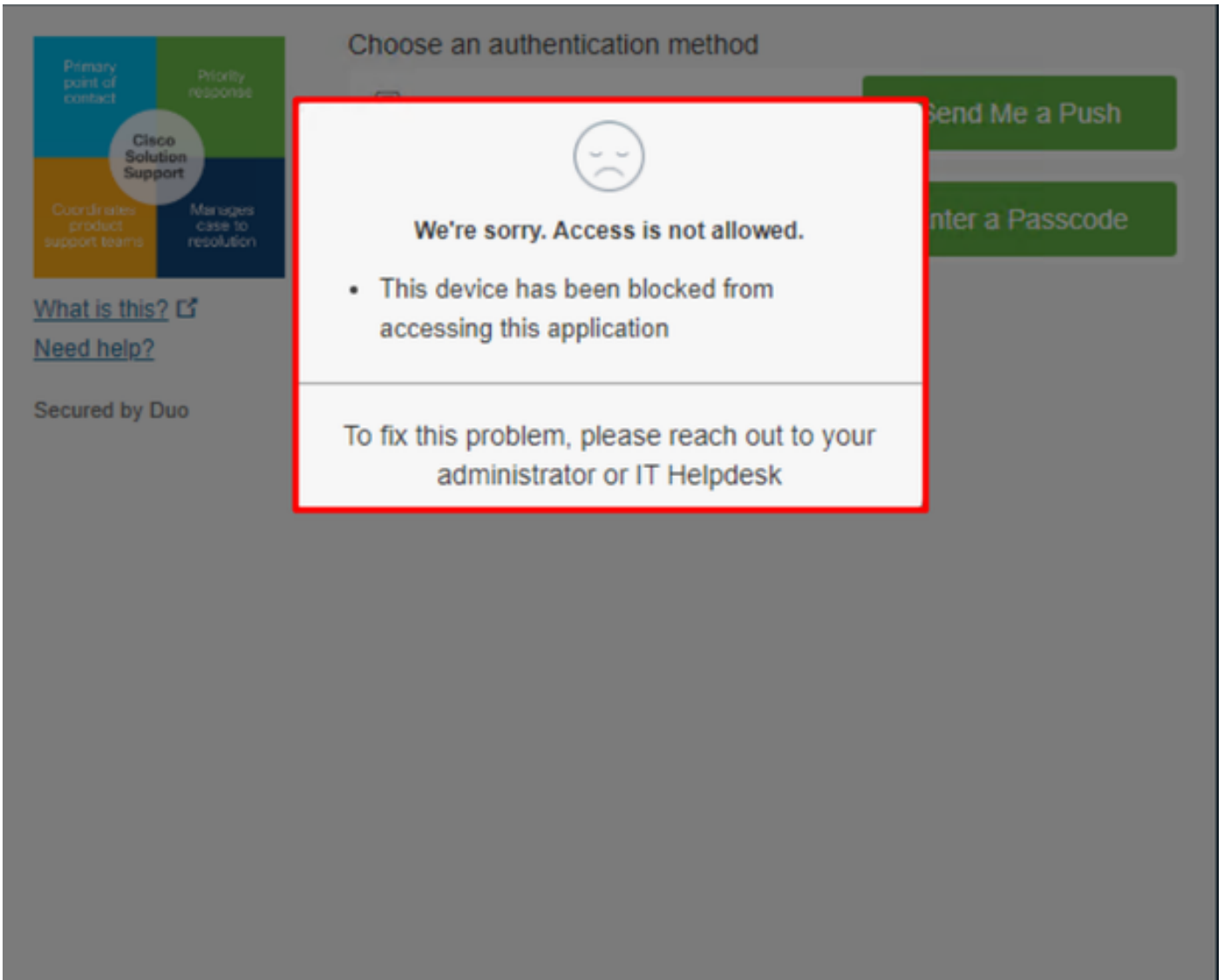
No known software vulnerabilities observed.

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

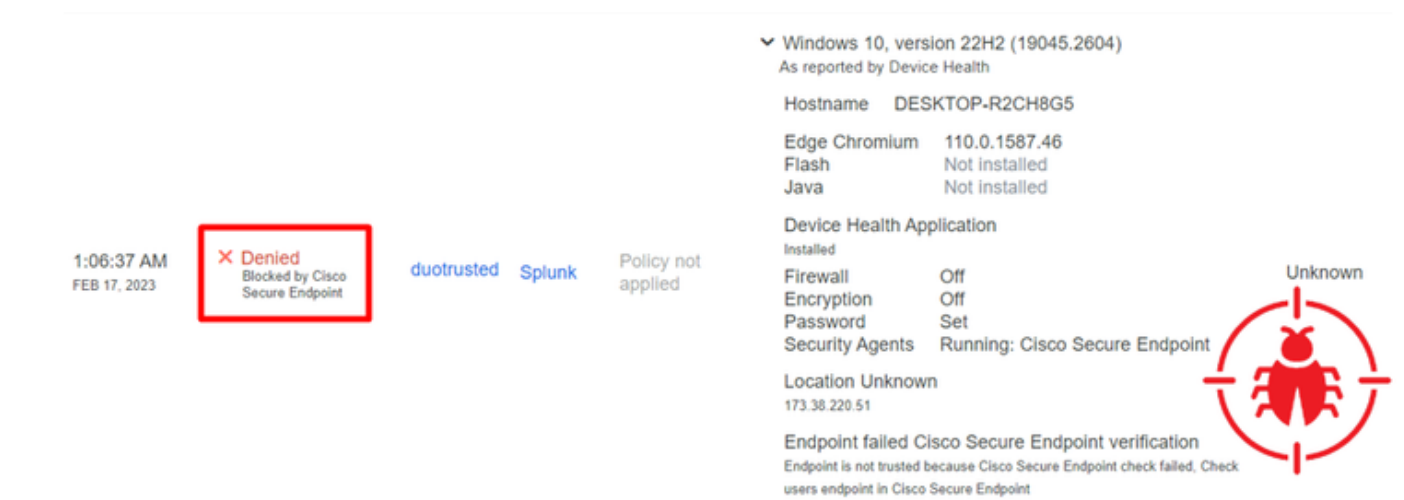
Scan... Diagnose... Move to Group... Begin Work Mark Resolved Promote to Incident Manager

이제 듀오로 전환하여 상태를 확인합니다.

아래 Cisco Secure EndPoint에 시스템을 설치한 후 동작을 확인하기 위해 먼저 인증을 시도합니다.  
Require Attention.



이는 Duo에서 어떻게 변경되고 인증 이벤트 아래의 이벤트가 어떻게 표시되는지 보여줍니다.



컴퓨터가 조직의 안전 장치가 아닌 것으로 검색되었습니다.

검토 후 시스템에 대한 액세스 허용

# 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 EndPoint와 사이버 보안 전문가의 검증을 거친 후 Duo에서 이 머신에 대한 앱의 액세스를 허용할 수 있습니다.

이제 문제는 Duo가 보호하는 앱에 대한 액세스를 다시 허용하는 방법입니다.

Cisco Secure EndPoint로 이동하여 `Inbox`, 이 디바이스를 다음으로 표시 `resolved` Duo가 보호하는 애플리케이션에 대한 액세스를 허용합니다.

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

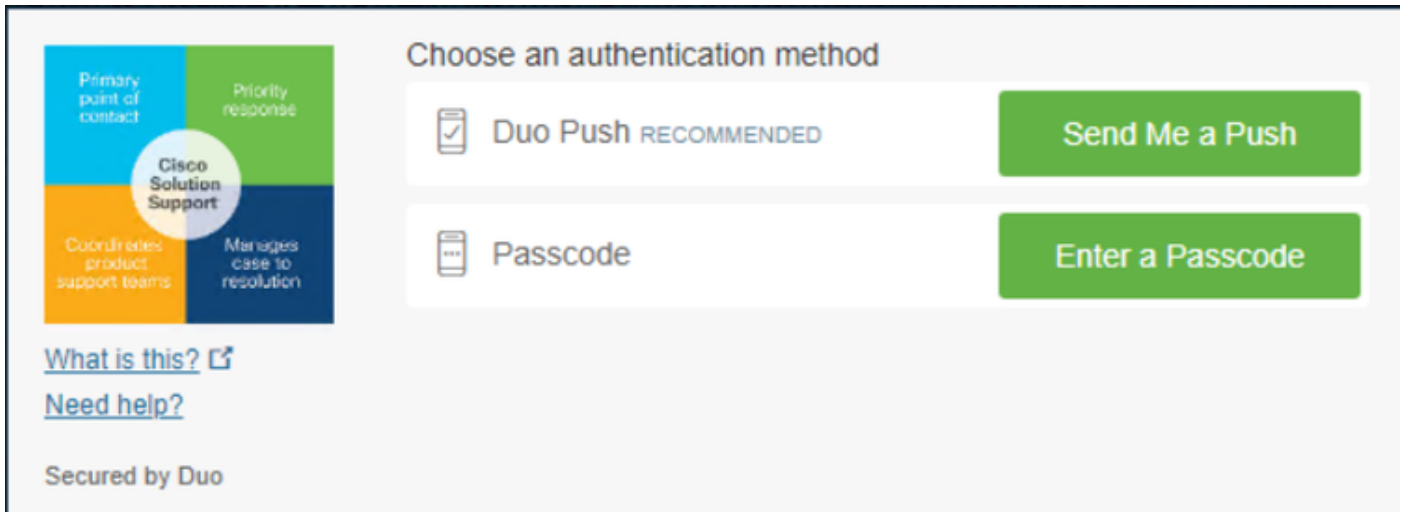
그 이후에는 상태가 지정된 시스템이 없습니다. attention required. 다음으로 변경됨: resolved 상태.

0 Require Attention

0 In Progress

2 Resolved

간단히 말해, 이제 Duo가 보호하는 Cisco 애플리케이션에 대한 액세스를 다시 테스트할 준비가 되었습니다.



이제 Duo에게 푸시를 보낼 수 있는 권한이 있으며, 앱에 로그인했습니다.

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

### 분류 워크플로

- 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**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.