

Configuración de Duo y un terminal seguro para responder a las amenazas

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Configuración y caso práctico](#)

[Configuración de la integración en Duo](#)

[Configuración de la integración en Cisco Secure EndPoint](#)

[Configurar políticas en dúo](#)

[Configuración de la política para detectar un dispositivo de confianza](#)

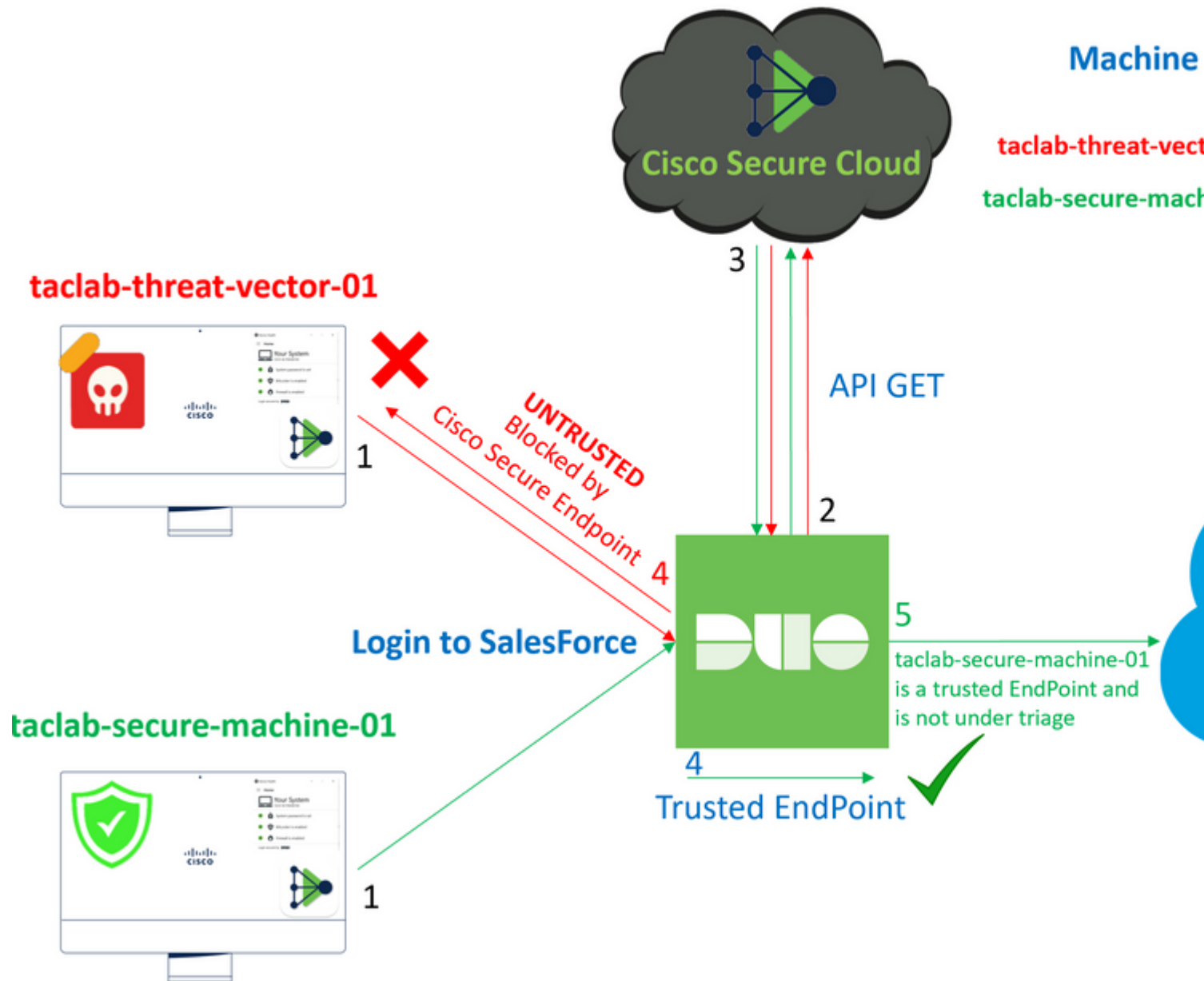
[Probar máquinas de confianza](#)

[Configuración de la política para Cisco Secure EndPoint](#)

[Pruebe las máquinas de confianza con Cisco Secure EndPoint](#)

[Permitir el acceso a un equipo después de la revisión](#)

Introducción



Este documento describe cómo integrar Duo Trusted EndPoints con Cisco Secure EndPoint.

Antecedentes

La integración entre Cisco Secure EndPoint y Duo permite una colaboración eficaz en respuesta a las amenazas detectadas en los dispositivos de red de confianza. Esta integración se consigue a través de varias herramientas de gestión de dispositivos que establecen la fiabilidad de cada dispositivo. Algunas de estas herramientas son:

- Servicios de dominio de Active Directory
- Active Directory con estado del dispositivo
- Genérico con estado del dispositivo
- Intune con el estado del dispositivo
- Jamf Pro con Device Health
- LANDESK Management Suite
- Herramienta de gestión de activos empresariales Mac OS X
- Manual con estado del dispositivo
- Herramienta Windows Enterprise Asset Management
- Espacio de trabajo UNO con estado del dispositivo

Una vez que los dispositivos se han integrado con una herramienta de gestión de dispositivos, es posible integrar Cisco Secure EndPoint y Duo mediante API en el Administration Panel. Posteriormente, debe configurarse la política adecuada en Duo para ejecutar la verificación de dispositivos de confianza y detectar dispositivos comprometidos que puedan afectar a las aplicaciones protegidas por Duo.

Nota: En este caso, trabajamos con Active Directory y Device Health.

Prerequisites

- Active Directory para realizar la integración.
- Para integrar Duo con terminales de confianza, los dispositivos deben estar registrados en el dominio de Active Directory. Esto permite a Duo autenticar y autorizar el acceso a los recursos y servicios de la red de forma segura.
- Duo más allá del plan.

Configuración y caso práctico

Configuración de la integración en Duo

Inicie sesión en el Admin Panel y vaya a:

- **Trusted EndPoints > Add Integration**
- Seleccionar 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

Después de esto, se le redirige para configurar el **Active Directory and Device Health**.

Tenga en cuenta que esto sólo funciona con equipos del dominio.

Vaya al directorio activo y ejecute el siguiente comando en PowerShell:

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

```
PS C:\Users\Administrator> (Get-ADDomain | Format-Table -Property DomainSID -HideTableHeaders)
PS C:\Users\Administrator> |
```

Después de esto, asegúrese de haber copiado en el portapapeles el identificador de seguridad de su Active Directory.

Ejemplo:

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

Esto se utiliza en Active Directory y Device Health Integration.

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 compu

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

4. Paste the domain SID

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

Haga clic en **Save** y posibilitar la integración y **Activate for all**. De lo contrario, no podrá realizar la integración con Cisco Secure EndPoint.

Change Integration Status

Once this integration is activated, Duo will start reporting your devices as trusted or not 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

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



Cisco Secure Endpoint

[Add this integration](#)

Note

Cisco Secu
following d

- Activ
- Activ
- Gene
- Intur
- Jam
- LAN
- Mac
Tool
- Man
- Winc
- Work

We integrated this in the previous steps

Ahora se encuentra en la página principal de la integración de Cisco Secure EndPoint.

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

Save Integration

Después de esto, vaya a la Admin Panel de Cisco Secure EndPoint.

Configuración de la integración en Cisco Secure EndPoint

- <https://console.eu.amp.cisco.com/> INICIO DE SESIÓN EN LA CONSOLA EMEAR
- <https://console.amp.cisco.com/> INICIO DE SESIÓN EN LA CONSOLA AMER

Y navegue hasta Accounts > API Credentials y seleccione New API Credentials.

Legacy API Credentials (version 0 and 1) [View Legacy API documentation](#)



New API Credential

Application name

Scope Read-only
 Read & Write

Enable Command line

Allow API access to File Repository download audit logs

Nota: sólo Read-only se necesita para realizar esta integración, ya que Duo hace GET consultas a Cisco Secure EndPoint para saber si el dispositivo cumple los requisitos de la política.

Insertar Application Name, Scope, y Create.

< API Key Details

3rd Party API Client ID

API Key

- Copie el 3rd API Party Client ID desde Cisco Secure EndPoint a Duo Admin Panel in Client ID.
- Copie el API Key desde Cisco Secure EndPoint a Duo Admin Panel in API Key.

< API Key Details

3rd Party API Client ID

API Key

Cisco Secure Endpoint

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 readable.
5. Click "Create".
6. Copy the **Client Id** and **API Key** and return to

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

Save Integration

Pruebe la integración y, si todo funciona correctamente, haga clic en **Save** para guardar la integración.

Configurar políticas en dúo

Para configurar las políticas de integración, vaya a través de la aplicación:

Navigate to **Application** > **Search for your Application** > **Select your policy**

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Trusted Endpoints

Trust Monitor

Reports

Settings

Billing

Manage your update to the new Universal Prompt experience, all in one place.

[See My Progress](#) [Get More Information](#)

20 All Applications 0 End of Support

Export

| Name | Type | Application Policy | Group Policies |
|--------|--------|--------------------|----------------|
| Splunk | Splunk | TrustedEndPoint | |

Configuración de la política para detectar un dispositivo de confianza

Policy name
Deny Access to unenrc

Users

- ✓ New User policy
- Authentication policy
- User location

Devices

- ✓ Trusted Endpoints
 - Device Health application
 - Remembered devices
 - Operating systems
 - Browsers
 - Plugins

Trusted Endpoints

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.

Allow all endpoints
Endpoints will be checked for trustworthiness to aid reporting, but untrusted endpoints will be allowed.

Require endpoints to be trusted
Only Trusted Endpoints will be able to access browser-based applications.

Allow Cisco Secure Endpoint to block compromised endpoints
Endpoints that Cisco Secure Endpoint deem to be compromised will be blocked from accessing browser-based applications.
Note: This option only applies to trusted endpoints.

[Advanced options for mobile endpoints](#) ▾


Probar máquinas de confianza

Equipo con Duo Device Health y se unió al dominio

| Timestamp (UTC) ▾ | Result | User | Application | Trust Assessment 1 | Access Device |
|-----------------------------|----------------------------|------------|-------------|---------------------------------|--|
| 11:36:04 PM FEB 16, 2023 | ✓ Granted User approved | duotrusted | Splunk | Policy not applied | ▾ Windows 10, version 22H2 (19045) As reported by Device Health Hostname DESKTOP-R2CH8G 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 Endpoint Location Unknown 173.38.220.51 Trusted Endpoint determined by Device Health |

Equipo fuera del dominio sin Duo Device Health

| Timestamp (UTC) ▾ | Result | User | Application | Trust Assessment ⓘ | Access Device |
|-----------------------------|--|------------|-------------|--------------------|--|
| 11:38:37 PM FEB 16, 2023 | ✗ Denied Device health data is missing | duotrusted | Splunk | Policy not applied | ▾ Windows 10 As reported by the browser Firefox 89.0 Flash Not installed Java Not installed Device Health Application Installation status unknown Firewall Unkr Encryption Unkr Password Unkr Security Agents Unkr Almere Stad, FL, Neth 64.103.36.135 <div style="border: 2px solid blue; padding: 2px;">Unable to communicate with De</div> |



Action Required

Please install the Duo Device Health application (required by your organization), then try logging in again.

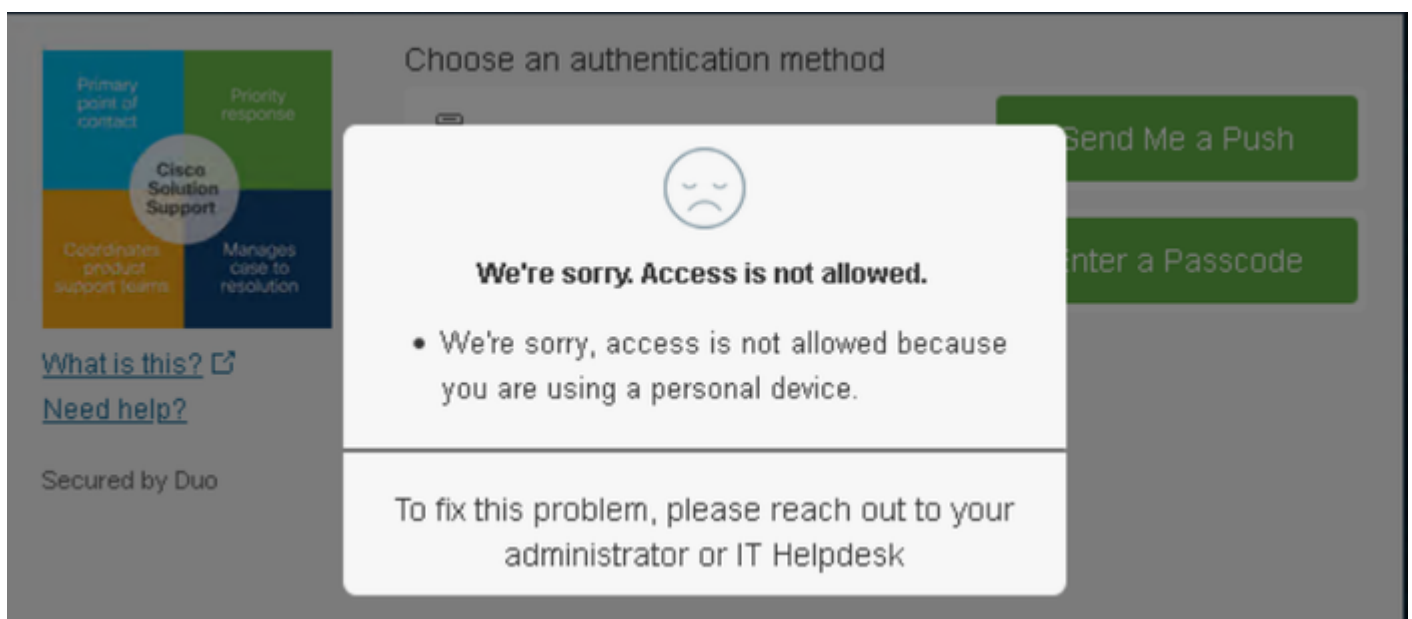
Download now
 or
 Already have the app installed?
[Launch the app](#)

[What is this?](#) [Need help?](#)

Secured by Duo

Equipo fuera del dominio con Duo Device Health

| Timestamp (UTC) ▾ | Result | User | Application | Trust Assessment 1 | Access Device |
|-----------------------------|--|------------|-------------|---------------------------|---|
| 11:40:58 PM FEB 16, 2023 | ✗ Denied Endpoint is not trusted | duotrusted | Splunk | Policy not applied | Windows 10, version 22H2 (19045.2604) As reported by Device Health Hostname NODOMAIN Firefox 89.0 Flash Not installed Java Not installed Device Health Application Installed Firewall Off Encryption Off Password Set Security Agents Running: Cisco Secure Endpoint Almere Stad, FL, Netherlands 64.103.36.133 Not a Trusted Endpoint <small>determined by Device Health</small> |



Configuración de la política para Cisco Secure EndPoint

En esta configuración de directiva, configure el dispositivo ya de confianza para cumplir los requisitos sobre amenazas que pueden afectar a la aplicación, de modo que si un dispositivo se infecta o si algunos comportamientos marcan ese equipo con **suspicious artifacts** or Indicators of Compromise, puede bloquear el acceso del equipo a las aplicaciones seguras.

- Users
 - New User policy
 - Authentication policy
 - User location
- Devices
 - Trusted Endpoints
 - Device Health application
 - Remembered devices
 - Operating systems
 - Browsers
 - Plugins
- Networks
 - Authorized networks
 - Anonymous networks

Trusted Endpoints

A Trusted Endpoint is an endpoint that exists in a management system such as your EAM or MDM. It can be matched to your management system using Duo certificates or information provided by Duo Mobile.

Allow all endpoints
Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.

Require endpoints to be trusted
Only Trusted Endpoints will be able to access browser-based applications.

Allow Cisco Secure Endpoint to block compromised endpoints
Endpoints that Cisco Secure Endpoint deem to be compromised will be blocked from accessing browser-based applications.
Note: This option only applies to trusted endpoints.

[Advanced options for mobile endpoints](#)

Pruebe las máquinas de confianza con Cisco Secure EndPoint

Equipo sin Cisco Secure Agent instalado

En este caso, la máquina puede pasar sin la verificación de AMP.

| | | | |
|-------------------------------------|--|---|---|
| <p>12:52:23 PM FEB 20, 2023</p> | <p>✔ Granted User approved</p> | <p>duotrusted Splunk Policy not applied</p> | <p>Windows 10, version 21H1 (19045.0) As reported by Device Health</p> <p>Hostname COMPUTER24</p> <p>Edge Chromium 110.0.1587.62 Flash Not installed Java Not installed</p> <p>Device Health Application Installed</p> <p>Firewall On Encryption Off Password Set</p> <p>Security Agents Running: Windows Defender</p> <p>Location Unknown 173.38.220.51</p> <p>Trusted Endpoint determined by Device Health</p> |
|-------------------------------------|--|---|---|

Si desea tener una política restrictiva, puede configurar la política para que sea más restrictiva si modifica la Device Health Application política de **Reporting** a **Enforcing**.

Y añade Block Access if an EndPoint Security Agent is not running.

Windows

Enforcing ^

Don't require users to have the app ⓘ

Allow users to install the app during enrollment

Require users to have the app ⓘ

Block access if firewall is off.

Block access if BitLocker is off.

Block access if system password is not set.

Block access if an endpoint security agent is not running.

Select which Duo supported endpoint security agent(s) are allowed

× Cisco Secure Endpoint × ▾

When the user is blocked, the app will provide remediation.
[See what it looks like](#) ↗

Ordenador

sin infección

Con una máquina, sin infección, puede probar cómo funciona Duo con Cisco Secure EndPoint para intercambiar información sobre el estado de la máquina y cómo se muestran los eventos en este caso en Duo y Cisco Secure EndPoint.

Si comprueba el estado de su equipo en Cisco Secure EndPoint:

Navigate to **Management** > **Computers**.

Cuando filtra para su máquina, puede ver el evento de eso, y en este caso, puede determinar que su máquina está limpia.

Dashboard Analysis Outbreak Control **Management** Accounts Search

Computers

4 Computers 1 Not Seen in Over 7 Days 1 Need AV 0 Computers With P

Filters no filters applied

All Windows Mac Linux Android

Move to Group... Delete

DESKTOP-LN2TEUT in group TEST

DESKTOP-R2CH8G5.taclab.com in group DUO

| | | | |
|--------------------------|--|--------------------|-------------------------|
| 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 | 172.16.200.1 |
| Install Date | 2023-02-13 11:47:36 UTC | External IP | 173.38.220.1 |
| Connector GUID | fe066900-9075-4473-ade7-4a7fc998dbfb | Last Seen | 2023-02-13 11:47:36 UTC |
| Processor ID | 1f8bfbff000006e7 | Definition Version | TETRA 64 |
| Definitions Last Updated | 2023-02-16 22:30:07 UTC | Update Server | tetra-defs. |
| Cisco Secure Client ID | N/A | Kenna Risk Score | No high se |

Take Forensic Snapshot View Snapshot Orbital Query 3 Events Device Traj

Scan... Diagnose

Puede ver que no hay detección para su dispositivo, y también está en un estado de limpio, lo que significa que su máquina no está en triage para asistir.

| | | | | |
|---|----------------------------|--|--|--|
| ▶ | DESKTOP-R2CH8G5.taclab.com | Scanned 13394 files, 210 processes, 0 directories. | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | started scan | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | Scanned 259 files, 3 processes, 0 directories. | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | started scan | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | Scanned 259 files, 3 processes, 0 directories. | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | started scan | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | Scanned 157 files, 2 processes, 0 directories. | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | started scan | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | Scanned 157 files, 2 processes, 0 directories. | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | started scan | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | Scanned 113 files, 1 processes, 0 directories. | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com | started scan | | |

Así es como Duo clasifica esa máquina:

| Timestamp (UTC) ▼ | Result | User | Application | Trust Assessment ⓘ | Access Device |
|-----------------------------|----------------------------|------------|-------------|--------------------|---|
| 12:41:20 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 173.38.220.51 <div style="border: 1px solid blue; padding: 2px; display: inline-block;">Trusted Endpoint determined by Device Health</div> |

La máquina mantiene el trusted etiqueta.

¿Qué sucede si la misma máquina se infecta por una Malicious Actor tiene intentos repetitivos de infección, O Indicators of Compromise alertas sobre esta máquina?

Ordenador con infección

Para probar la función con un ejemplo de **EICAR**, acceda a <https://www.eicar.org/> y descargue una muestra maliciosa.

Nota: No se preocupe. Puede descargar esa prueba EICAR, es segura y es sólo un archivo de prueba.

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

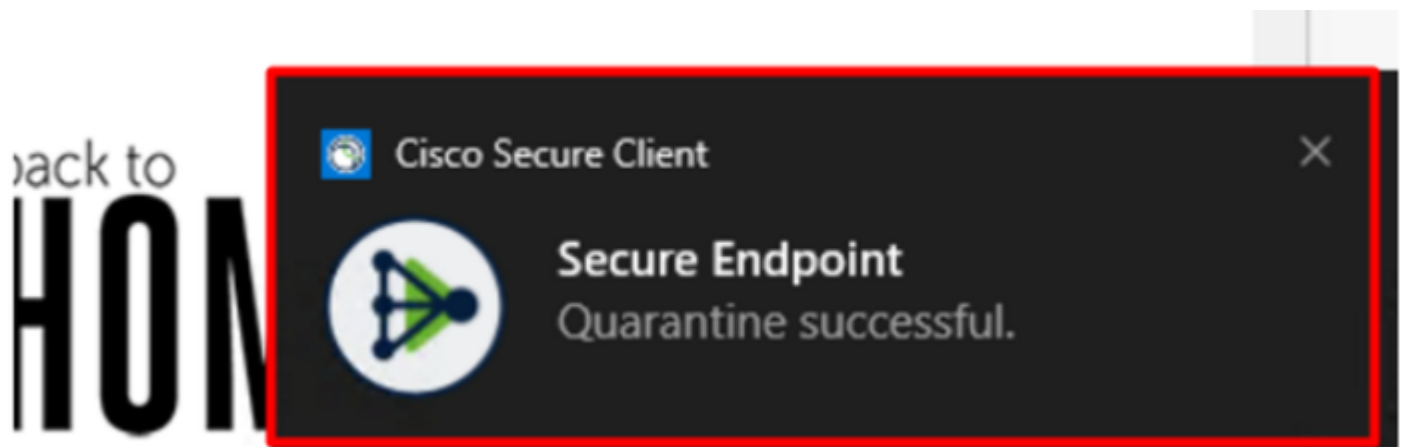


Desplácese hacia abajo y vaya a la sección y descargue el archivo de prueba.

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 |  |
|---------------------------------------|---|--|---|--|---|

Cisco Secure EndPoint detecta el malware y lo pone en cuarentena.



Así es como cambia, como se muestra en el panel Cisco Secure EndPoint Admin.

| | | | | | |
|---|--|-------------------------------------|--|--|--|
| ▶ | DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar:95.sbx.tg | Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar:95.sbx.tg | Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar:95... | Tactics <input type="text"/> Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar:95.sbx.tg | Tactics <input type="text"/> Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar:95.sbx.tg | Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar:95... | Tactics <input type="text"/> Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar:95.sbx.tg | Tactics <input type="text"/> Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar:95... | Tactics <input type="text"/> Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar:95.sbx.tg | Medium | | | |
| ▶ | DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar:95.sbx.tg | Medium | | | |

También dispone de la detección del malware en la máquina, pero esto significa que se considera que los terminales están analizados en la clasificación de Cisco Secure EndPoint en la Inbox.

Nota: Para enviar un terminal al triaje, necesita tener varias detecciones de artefactos o comportamientos extraños que activen algunos Indicators of Compromise en el terminal.

En la sección Dashboard, haga clic en el **Inbox**.



Secure Endpoint
Premier

Dashboard

Analysis ▾

Outbreak Control ▾

Management ▾

Accounts ▾

Dashboard

Dashboard

Inbox

Overview

Events

iOS Clarity

Refresh All

Auto-Refresh



Ahora tienes una máquina que requiere atención.

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

| | | | |
|--------------------------|--|--------------------|---|
| 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.

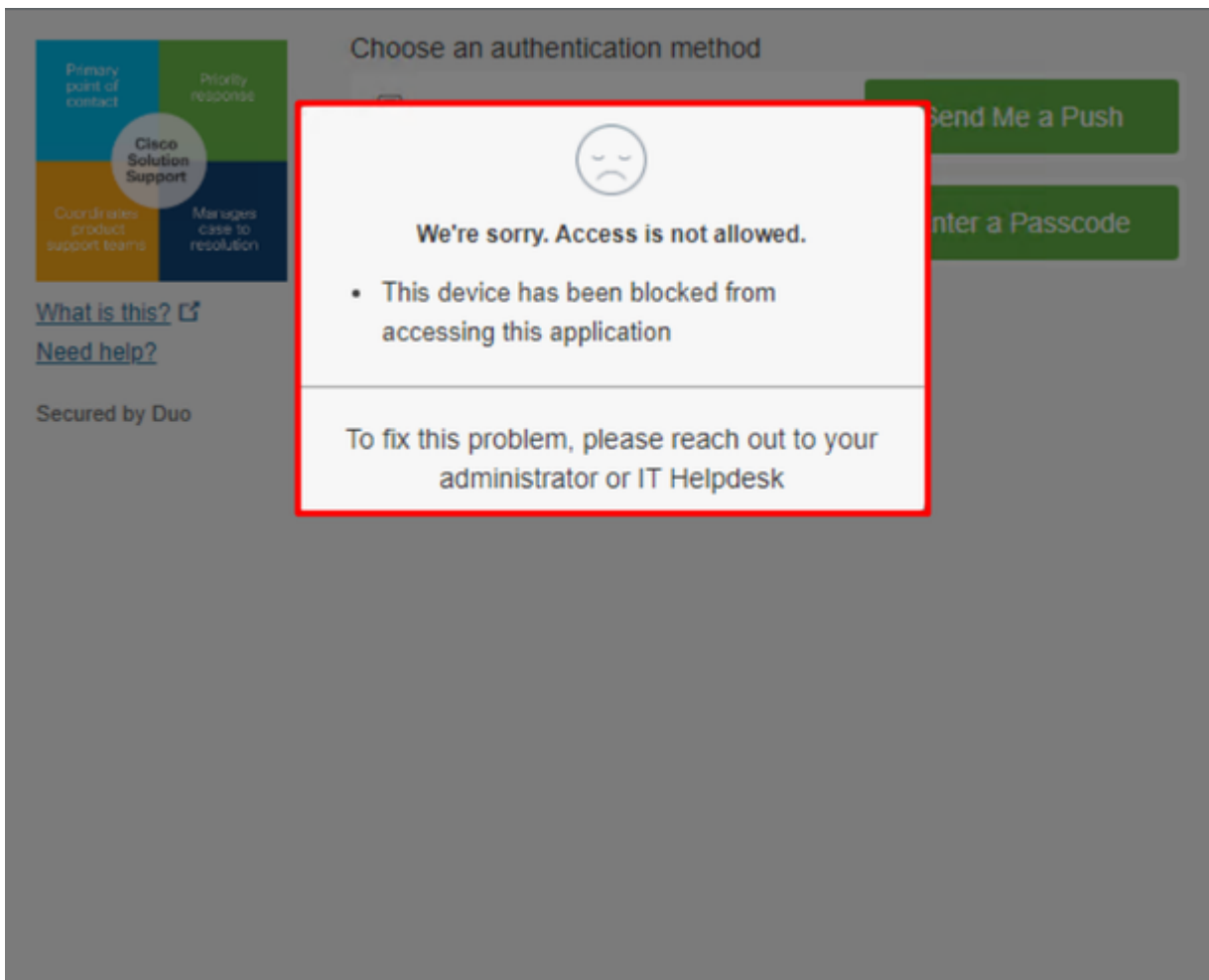
Take Forensic Snapshot View Snapshot Orbital Query

Events Device Trajectory Diagnostics

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

Ahora, cambie a Duo y vea cuál es el estado.

La autenticación se intenta primero para ver el comportamiento después de que el equipo se haya colocado en el Cisco Secure EndPoint en Require Attention.



Así es como cambia en Duo y como se muestra el evento bajo eventos de autenticación.

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

Unknown



Se ha detectado que su equipo no es un dispositivo de seguridad para su organización.

Permitir el acceso a un equipo después de la revisión

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**.

Machine on triage status in
Cisco Secure Endpoint

Después de la verificación en Cisco Secure EndPoint y por su especialista en ciberseguridad, puede permitir el acceso a esta máquina a su aplicación en Duo.

Ahora la pregunta es cómo permitir el acceso de nuevo a la aplicación protegida por Duo.

Debe pasar por Cisco Secure EndPoint y, en su Inbox, marque este dispositivo como **resolved** para permitir el acceso a la aplicación protegida por Duo.

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 Vulnerabilities

| | | | | |
|--------|--------------------|---------------------|---|-------------------------|
| 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 |

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

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

Después de eso, no tiene la máquina con el estado attention required. Esto cambió a resolved estado.

0 Require Attention 0 In Progress 2 Resolved

En pocas palabras, ahora está preparado para volver a probar el acceso a nuestra aplicación protegida por Duo.

Cisco Solution Support

Primary point of contact Priority response

Coordinates product support teams Manages case to resolution

[What is this?](#) [Need help?](#)

Secured by Duo

Choose an authentication method

Duo Push **RECOMMENDED**
Send Me a Push

Passcode
 Enter a Passcode

Ahora tiene permiso para enviar la pulsación a Duo y ha iniciado sesión en la aplicación.

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

Flujo de trabajo de selección

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 and some suspicious indicators of compromise are detected**
- 3. The machine was detected safely by the Cybersecurity Team, and now was removed from the triage in Cisco Sec**

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).