

Duo en Secure Endpoint configureren om op bedreigingen te reageren

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Configuratie- en gebruikscase](#)

[De integratie in Duo configureren](#)

[De integratie in Cisco Secure End-point configureren](#)

[Configuratie van beleid in Duo](#)

[Configureer het beleid om een betrouwbaar apparaat te detecteren](#)

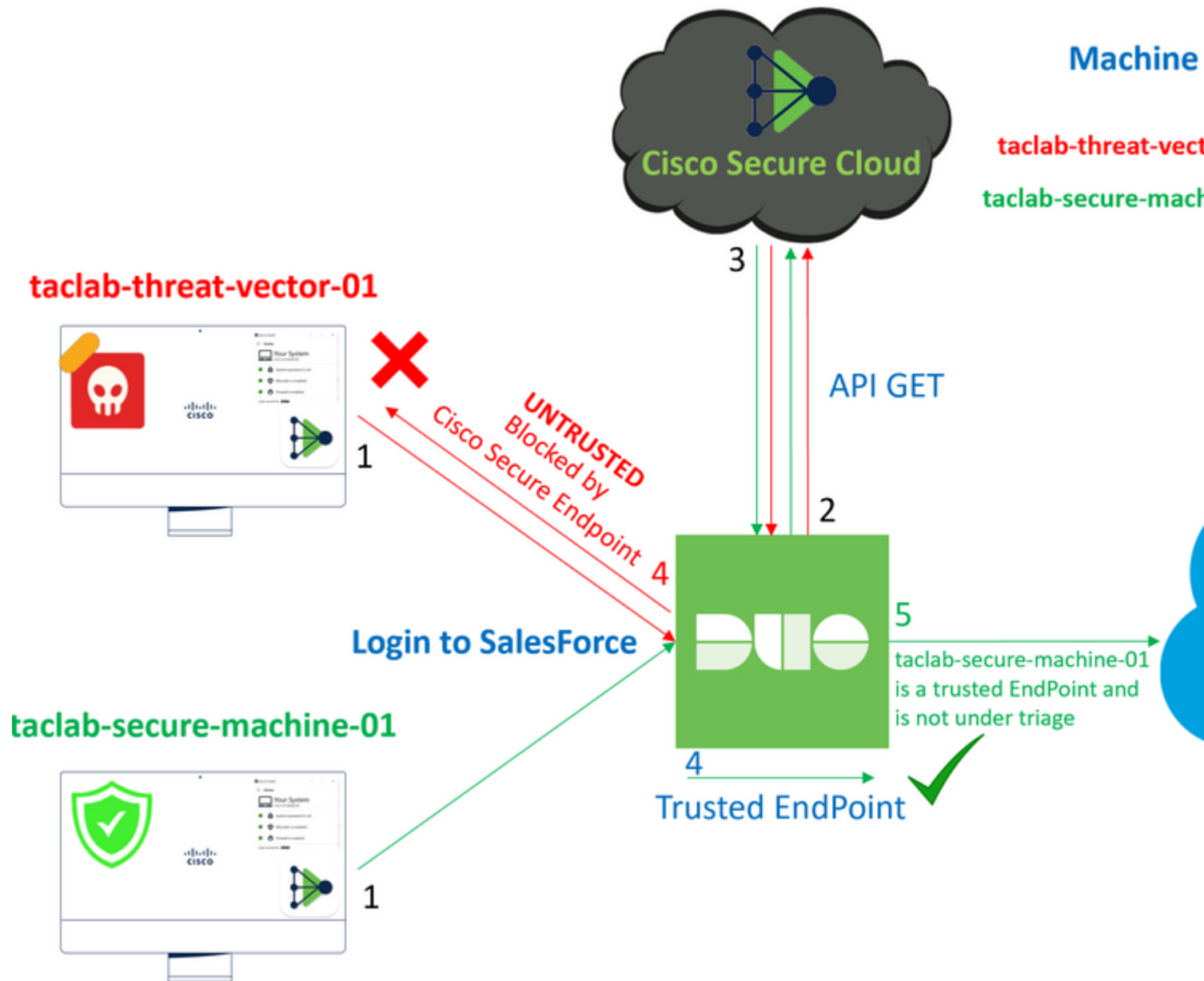
[Test Trusted Machines](#)

[Het beleid voor Cisco Secure End-point configureren](#)

[Test de vertrouwde machines met Cisco Secure EndPoint](#)

[Toegang tot een machine na review toestaan](#)

Inleiding



Dit document beschrijft hoe u Duo Trusted End Point kunt integreren met Cisco Secure End Point.

Achtergrondinformatie

De integratie tussen Cisco Secure End Point en Duo maakt effectieve samenwerking mogelijk in reactie op bedreigingen die op vertrouwde netwerkapparaten worden gedetecteerd. Deze integratie wordt bereikt door meerdere apparaatbeheertools die de betrouwbaarheid van elk apparaat vaststellen. Enkele van deze hulpmiddelen omvatten:

- Active Directory Domain Services
- Active Directory met apparaatstatus
- Generiek met apparaatstatus
- Intune met apparaatstatus
- Jamf Pro met Apparaatstatus
- LANDESK Management Suite
- Mac OS X Enterprise Asset Management Tool
- Handmatig met status apparaat
- Windows Enterprise Asset Management Tool
- Workspace ONE met apparaatstatus

Zodra apparaten zijn geïntegreerd met een apparaatbeheerprogramma, is het mogelijk om Cisco Secure End Point en Duo te integreren via API in het Administration Panel. Vervolgens moet het juiste beleid worden geconfigureerd in Duo om betrouwbare apparaatverificatie uit te voeren en gecompromitteerde apparaten te detecteren die toepassingen kunnen beïnvloeden die worden beschermd door Duo.

Opmerking: In dit geval werken we met Active Directory en Device Health.

Voorwaarden

- Active Directory voor de integratie.
- Om Duo met Trusted Endpoints te kunnen integreren, moeten uw apparaten worden geregistreerd in het domein van Active Directory. Hierdoor kan Duo de toegang tot netwerkbronnen en -services op een veilige manier authenticeren en autoriseren.
- Het is een vervolg op Plan.

Configuratie- en gebruikscase

De integratie in Duo configureren

Log in op de Admin Panel en ga naar:

- **Trusted EndPoints > Add Integration**
- **Kiezen** 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

Daarna wordt u doorgestuurd om de **Active Directory and Device Health**.

Houd er rekening mee dat dit alleen werkt met machines in het domein.

Ga naar de actieve map en voer de volgende opdracht uit in 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> |
```

Daarna, zorg ervoor dat u hebt gekopieerd naar het klembord de security identifier van uw Active Directory.

Voorbeeld

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

Dit wordt gebruikt in uw Active Directory en 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 computer

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

4. Paste the domain SID

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

Klik **Save** en de integratie en **Activate for all**. Anders kunt u niet integreren met 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

Ga naar veld 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

U bevindt zich nu op de hoofdpagina van de integratie voor 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

Ga daarna naar de **Admin Panel** van het Cisco Secure End-punt.

De integratie in Cisco Secure End-point configureren

- <https://console.eu.amp.cisco.com/> EMEAR CONSOLE LOGIN
- <https://console.amp.cisco.com/> AMER CONSOLE LOGIN

En navigeer naar Accounts > API Credentials en selecteer 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

Opmerking: alleen Read-only is nodig om deze integratie te realiseren, omdat Duo GET Vragen aan Cisco Secure EndPoint om te weten of het apparaat voldoet aan de vereisten van het beleid.

Invoegen Application Name, Scope, en Create.

< API Key Details

3rd Party API Client ID

API Key

- Kopieert de 3rd API Party Client ID van Cisco Secure EndPoint naar Duo Admin Panel in Client ID.
- Kopieert de API Key van Cisco Secure EndPoint naar 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 read-only.
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

Test de integratie en als alles goed werkt, klikt u op **Save** de integratie redden.

Configuratie van beleid in Duo

Om het beleid voor uw integratie te vormen, gaat u door uw toepassing:

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

Search: splunk

Name	Type	Application Policy	Group Policies
Splunk	Splunk	TrustedEndPoint	

Configureer het beleid om een betrouwbaar apparaat te detecteren

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 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](#) ▾


Test Trusted Machines

Machine met Duo Device Health en aangesloten bij het domein

Timestamp (UTC) ▾	Result	User	Application	Trust Assessment !	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 <div style="border: 2px solid blue; padding: 2px; display: inline-block;"> Trusted Endpoint determined by Device Health </div>

Machine buiten het domein zonder 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 Unable to communicate with De



Action Required

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

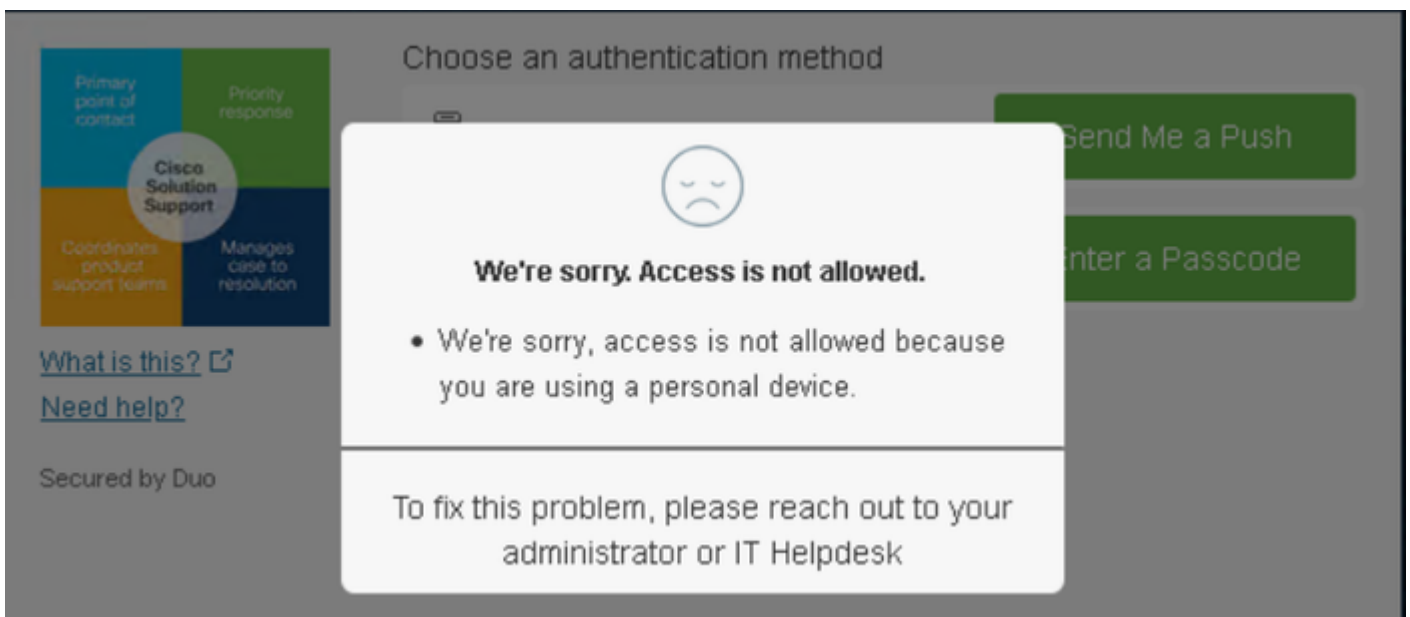
Download now
or
Already have the app installed?
[Launch the app](#)

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

Secured by Duo

Machine buiten het domein met 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>



Het beleid voor Cisco Secure End-point configureren

In deze beleidsopstelling, vorm het reeds vertrouwde op apparaat om aan het vereiste over bedreigingen te voldoen die uw toepassing kunnen beïnvloeden, zodat als een apparaat geïnfecteerd wordt, of als sommige gedragingen merken die machine met **suspicious artifacts** Of Indicators of Compromise, kunt u de toegang van de machine tot de beveiligde toepassingen blokkeren.

- 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](#) ▾

Test de vertrouwde machines met Cisco Secure EndPoint

Machine zonder Cisco Secure Agent geïnstalleerd

In dit geval kan de machine zonder AMP-verificatie doorgaan.

<p>12:52:23 PM FEB 20, 2023</p>	<p>✔ Granted User approved</p>	<p>duotrusted Splunk</p>	<p>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>
-------------------------------------	---	--------------------------	---------------------------	--

Als u een restrictief beleid wilt hebben, kunt u het beleid instellen om restrictiever te zijn als u de Device Health Application beleid van **Reporting in Enforcing**.

En toevoegen Block Access if an EndPoint Security Agent is not running.

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.

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

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

× Cisco Secure Endpoint × ▾

Computer

zonder infectie

Met een machine, zonder infectie, kunt u testen hoe Duo met Cisco Secure EndPoint werkt om informatie uit te wisselen over de status van de machine en hoe de gebeurtenissen in dit geval worden getoond in Duo en Cisco Secure EndPoint.

Als u de status van uw machine in Cisco Secure EndPoint controleert:

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

Als je voor je machine filtert, kun je het resultaat zien en in dit geval kun je bepalen of de machine schoon is.

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

U kunt zien dat er geen detectie is voor uw apparaat, en het is ook op een status van schoon, wat betekent dat uw machine niet in staat is om bij te wonen.

▶	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		

Zo categoriseert Duo die machine als volgt:

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: 2px solid blue; padding: 2px; display: inline-block;">Trusted Endpoint determined by Device Health</div>

De machine onderhoudt het trusted etiket.

Wat gebeurt er als dezelfde machine geïnfecteerd raakt met een Malicious Actor herhaalde pogingen tot infectie heeft, of Indicators of Compromise Waarschuwingen over deze machine?

Computer met infectie

Om met een voorbeeld van **EICAR** te proberen om de functie te testen, toegang te krijgen tot <https://www.eicar.org/>, en een kwaadaardige steekproef te downloaden.

Opmerking: maak u geen zorgen. U kunt die EICAR-test downloaden, het is veilig en het is slechts een testbestand.

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

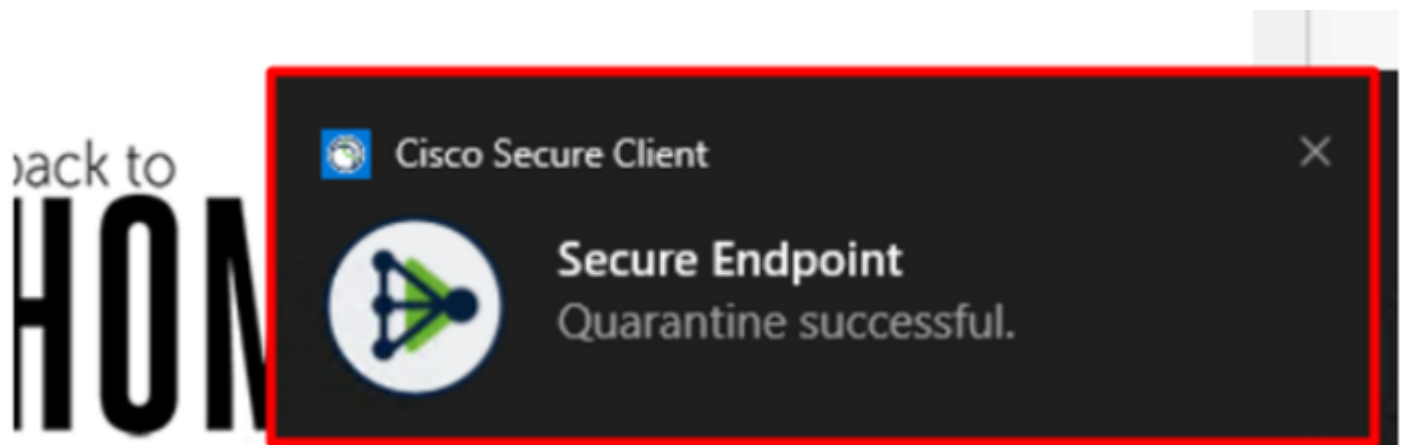


Scroll naar beneden, ga naar de sectie en download het testbestand.

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 detecteert de malware en verplaatst deze naar quarantaine.



Dit is de manier waarop dit verandert, zoals wordt getoond in het paneel 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 Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar::95.sbx.tg	Tactics 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 Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar::95.sbx.tg	Tactics Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar::95...	Tactics 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			

U hebt ook de detectie van de malware in de machine, maar dit betekent dat de endpoints worden beschouwd als geanalyseerd onder het proces van Cisco Secure EndPoint op de Inbox.

Opmerking: om een eindpunt naar triage te sturen, moet het meerdere detecties van artefacten of vreemd gedrag hebben die een aantal Indicators of Compromise in het eindpunt.

In het Dashboard klikt u op in het **Inbox**.



Secure Endpoint
Premier

Dashboard

Analysis ▾

Outbreak Control ▾

Management ▾

Accounts ▾

Dashboard

Dashboard

Inbox

Overview

Events

iOS Clarity

Refresh All

Auto-Refresh



Nu heb je een machine die aandacht nodig heeft.

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	1f8bf0000006e7	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

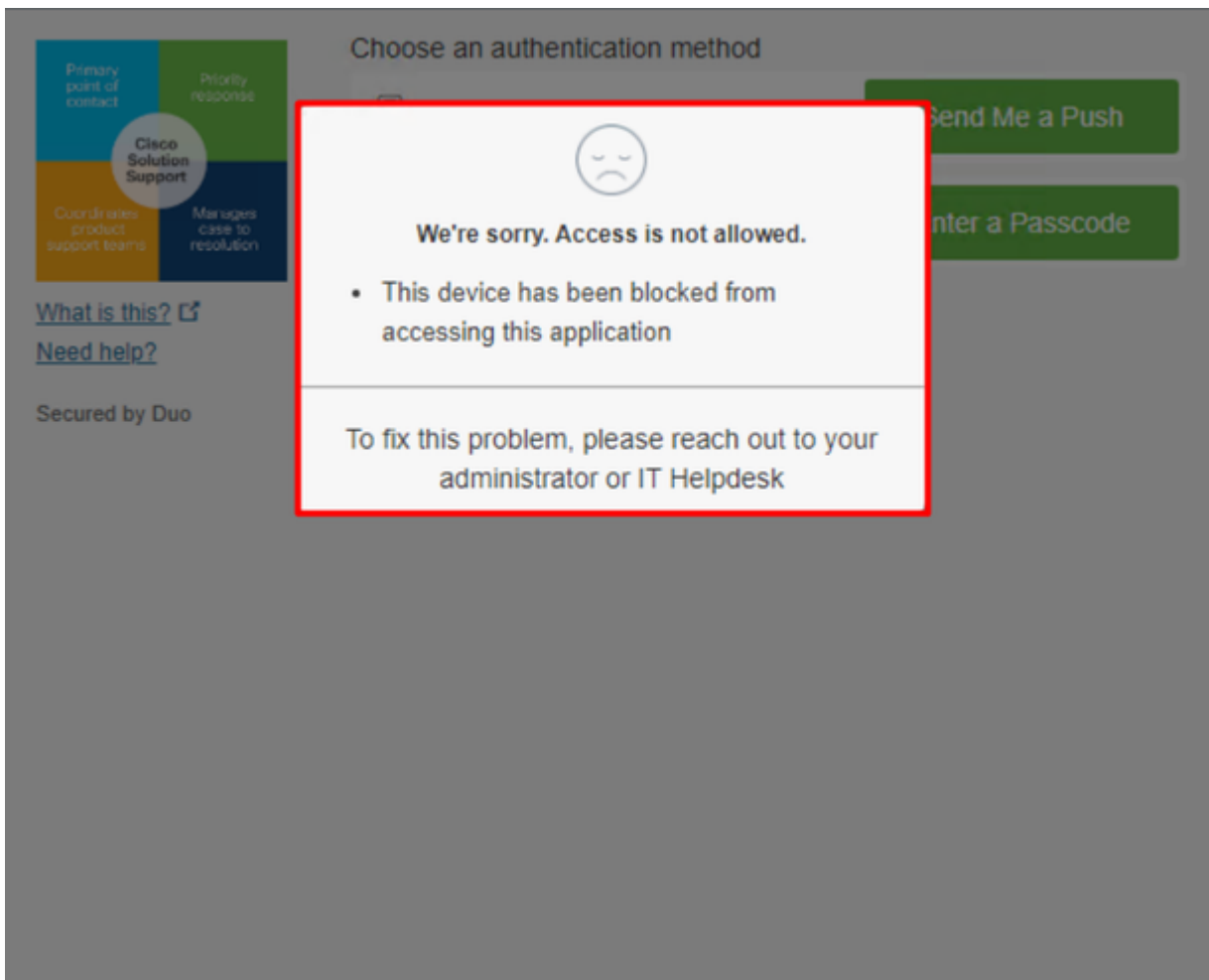
No known software vulnerabilities observed.

Take Forensic Snapshot View Snapshot Orbital Query Events Device Trajectory Diagnostics

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

Switch nu naar Duo en kijk wat de status is.

Verificatie wordt eerst geprobeerd om het gedrag te zien nadat de machine onder op Cisco Secure End-point is gezet Require Attention.



Zo verandert het in Duo en hoe wordt de gebeurtenis onder authenticatie gebeurtenissen getoond.

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



Uw machine is gedetecteerd als geen veiligheidsapparaat voor uw organisatie.

Toegang tot een machine na review toestaan

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

Na verificatie onder Cisco Secure EndPoint en door uw Cybersecurity Specialist, kunt u toegang tot deze machine aan uw app in Duo toestaan.

De vraag is nu hoe je de toegang weer kunt toestaan tot de app die door Duo wordt beschermd.

U moet onder Cisco Secure EndPoint en in uw Inbox, moet dit apparaat worden gemarkeerd als **resolved** toegang te verlenen tot de door Duo beschermde applicatie.

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

Daarna hebt u de machine niet meer met de status attention required. Dit veranderde in resolved status.

0 Require Attention 0 In Progress 2 Resolved

Kort samengevat bent u nu bereid om de toegang tot onze door Duo beschermde applicatie opnieuw te testen.

What is this?

Need help?

Secured by Duo

Choose an authentication method

Duo Push **RECOMMENDED**
Send Me a Push

Passcode
 Enter a Passcode

Nu heb je toestemming om de push naar Duo te sturen, en je bent ingelogd op de app.

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

Triage 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 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**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.