

Konfigurieren von Duo und sicheren Endgeräten zur Reaktion auf Bedrohungen

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Konfiguration und Anwendungsfall](#)

[Konfigurieren der Integration in Duo](#)

[Konfigurieren der Integration in Cisco Secure EndPoint](#)

[Konfigurieren von Richtlinien im Duo](#)

[Konfigurieren der Richtlinie zum Erkennen eines vertrauenswürdigen Geräts](#)

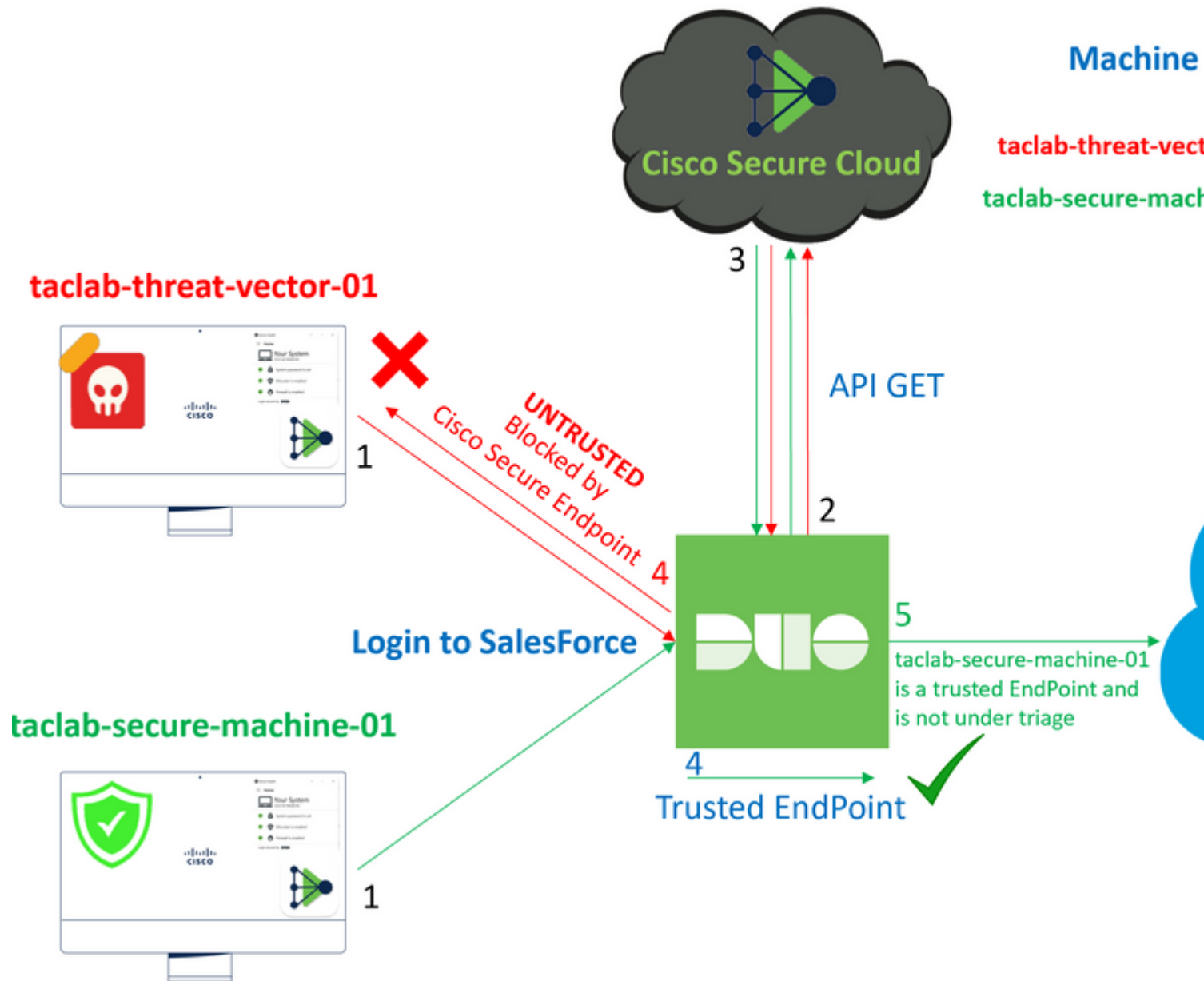
[Testen vertrauenswürdiger Systeme](#)

[Konfigurieren der Richtlinie für Cisco Secure EndPoint](#)

[Testen Sie die vertrauenswürdigen Systeme mit Cisco Secure EndPoint.](#)

[Zugriff auf einen Computer nach Überprüfung zulassen](#)

Einleitung



In diesem Dokument wird beschrieben, wie Sie Duo Trusted EndPoints in Cisco Secure EndPoint integrieren.

Hintergrundinformationen

Die Integration von Cisco Secure EndPoint und Duo ermöglicht eine effektive Zusammenarbeit bei der Reaktion auf Bedrohungen, die auf vertrauenswürdigen Netzwerkgeräten erkannt werden. Diese Integration wird durch mehrere Geräteverwaltungstools erreicht, die die Zuverlässigkeit der einzelnen Geräte gewährleisten. Zu diesen Tools gehören:

- Active Directory Domain Services
- Active Directory mit Gerätestatus
- Allgemein mit Gerätezustand
- Anpassung an den Gerätezustand
- Jamf Pro mit Gerätestatus
- LANDESK Management-Suite
- Mac OS X Enterprise Asset Management-Tool
- Manuell mit Gerätestatus
- Windows Enterprise Asset Management-Tool

- Workspace 1 mit Geräteintegration

Sobald die Geräte in ein Tool für das Gerätemanagement integriert sind, können Cisco Secure EndPoint und Duo über API im Administration Panel. Anschließend muss die entsprechende Richtlinie in Duo konfiguriert werden, um die Überprüfung vertrauenswürdiger Geräte auszuführen und kompromittierte Geräte zu erkennen, die von Duo geschützte Anwendungen beeinträchtigen können.

Hinweis: In diesem Fall arbeiten wir mit Active Directory und Device Health.

Voraussetzungen

- Active Directory für die Integration.
- Um Duo mit vertrauenswürdigen Endgeräten zu integrieren, müssen Ihre Geräte in der Active Directory-Domäne registriert sein. So kann Duo den Zugriff auf Netzwerkressourcen und -services sicher authentifizieren und autorisieren.
- Duo hinter Plan.

Konfiguration und Anwendungsfall

Konfigurieren der Integration in Duo

Melden Sie sich beim Admin Panel und gehe zu:

- **Trusted EndPoints > Add Integration**
- Auswählen 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

Anschließend werden Sie umgeleitet, um die **Active Directory and Device Health**.

Beachten Sie, dass dies nur mit Computern in der Domäne funktioniert.

Wechseln Sie zum Active Directory, und führen Sie den nächsten Befehl in PowerShell aus:

```
(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> |
```

Stellen Sie anschließend sicher, dass Sie die Sicherheits-ID Ihres Active Directory in die Zwischenablage kopiert haben.

Beispiel

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

Dies wird bei der Integration von Active Directory und Geräteintegrität verwendet.

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

Klicken Sie auf **save** und ermöglicht die Integration und **Activate for all**. Andernfalls ist die Integration in Cisco Secure EndPoint nicht möglich.

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

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



Cisco Secure Endpoint

[Add this integration](#)

Note

Cisco Secure Endpoint is supported in the following devices:

- Active Directory
- Active Directory (highlighted)
- General
- Intune
- Jamf
- LAN
- Mac OS
- Tool
- Man
- Win
- Work

We integrated this in the previous steps

Sie befinden sich jetzt auf der Hauptseite der Integration für 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

Danach gehen Sie zum **Admin Panel** des Cisco Secure EndPoint.

Konfigurieren der Integration in Cisco Secure EndPoint

- <https://console.eu.amp.cisco.com/> EMEAR-KONSOLENANMELDUNG
- <https://console.amp.cisco.com/> ANMELDUNG AN DER AMER-KONSOLE

Navigieren Sie zu Accounts > API Credentials und wählen 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

Hinweis: Nur Read-only ist für diese Integration erforderlich, da Duo GET fragt an Cisco Secure EndPoint ab, ob das Gerät die Anforderungen der Richtlinie erfüllt.

Einfügen Application Name, Scope, und Create.

< API Key Details

3rd Party API Client ID

API Key

- Kopieren Sie 3rd API Party Client ID VON Cisco Secure EndPoint zu Duo Admin Panel in Client ID.
- Kopieren Sie API Key VON Cisco Secure EndPoint zu 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 the console.

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

Testen Sie die Integration, und klicken Sie auf **save** um die Integration zu speichern.

Konfigurieren von Richtlinien im Duo

Um die Richtlinien für die Integration zu konfigurieren, durchlaufen Sie die Anwendung:

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

Name	Type	Application Policy	Group Policies
Splunk	Splunk	TrustedEndPoint	

Konfigurieren der Richtlinie zum Erkennen eines vertrauenswürdigen Geräts

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 all 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](#) ▾


Testen vertrauenswürdiger Systeme

Maschine mit Duo Device Health und trat der Domäne bei

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 Trusted Endpoint determined by Device Health

Maschine außerhalb der Domäne ohne 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.

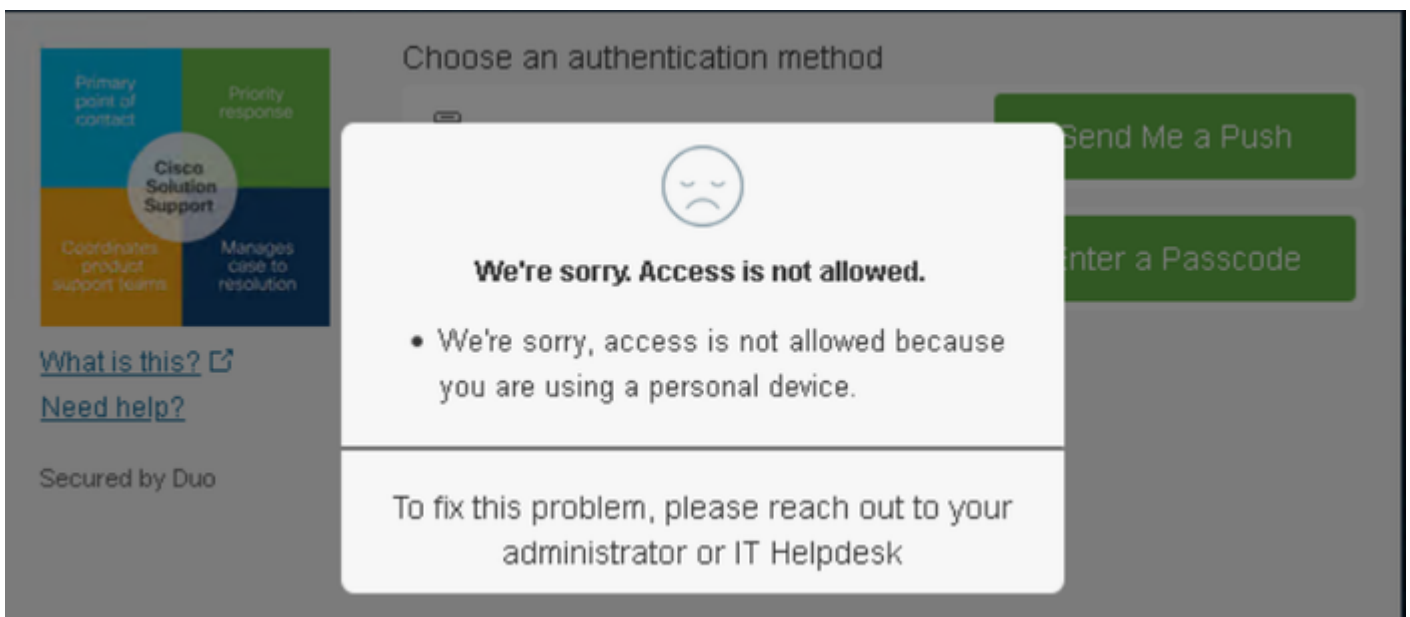
Download now
 or
 Already have the app installed?
[Launch the app](#)

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

Secured by Duo

Computer außerhalb der Domäne mit 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 <div style="border: 1px solid blue; padding: 2px; display: inline-block;"> Not a Trusted Endpoint <small>determined by Device Health</small> </div>



Konfigurieren der Richtlinie für Cisco Secure EndPoint

Konfigurieren Sie in dieser Richtlinienkonfiguration das bereits vertrauenswürdige Gerät so, dass es die Anforderungen an Bedrohungen erfüllt, die sich auf Ihre Anwendung auswirken können. Wenn also ein Gerät infiziert wird oder bestimmte Verhaltensweisen den Computer mit **suspicious artifacts** Oder Indicators of Compromise können Sie den Zugriff auf die gesicherten Anwendungen blockieren.

- 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](#) ▾

Testen Sie die vertrauenswürdigen Systeme mit Cisco Secure EndPoint.

Computer ohne installierten Cisco Secure Agent

In diesem Fall kann die Maschine ohne AMP-Verifizierung passieren.

<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 (19042.1001) 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> <table border="0"> <tr><td>Firewall</td><td>On</td></tr> <tr><td>Encryption</td><td>Off</td></tr> <tr><td>Password</td><td>Set</td></tr> <tr><td>Security Agents</td><td>Running: Windows Defender</td></tr> </table> <p>Location Unknown 173.38.220.51</p> <p>Trusted Endpoint determined by Device Health</p>	Firewall	On	Encryption	Off	Password	Set	Security Agents	Running: Windows Defender
Firewall	On										
Encryption	Off										
Password	Set										
Security Agents	Running: Windows Defender										

Wenn Sie eine restriktive Richtlinie verwenden möchten, können Sie die Richtlinie so einrichten, dass sie restriktiver ist, wenn Sie die Device Health Application Richtlinie von **Reporting** zu **Enforcing**.

und hinzufügen 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.

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](#) ↗

Computer

ohne Infektion

Bei einem Computer ohne Infektion können Sie testen, wie Duo mit Cisco Secure EndPoint Informationen über den Computerstatus austauscht und wie die Ereignisse in diesem Fall in Duo und Cisco Secure EndPoint angezeigt werden.

Wenn Sie den Status Ihres Computers in Cisco Secure EndPoint überprüfen:

Navigate to **Management > Computers**.

Wenn Sie nach Ihrem Computer filtern, können Sie das Ereignis sehen, und in diesem Fall können Sie feststellen, dass Ihr Computer sauber ist.

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

Sie können sehen, es gibt keine Erkennung für Ihr Gerät, und es ist auch auf einem Status der sauberen, was bedeutet, dass Ihr Computer nicht in der Triage zu besuchen.

▶	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		

So kategorisiert Duo diese Maschine:

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>

Die Maschine wartet die trusted beschriften.

Was passiert, wenn derselbe Computer von einem Malicious Actorwiederholte Infektionsversuche hat oder Indicators of Compromise Warnungen über diesen Computer?

Computer mit Infektion

Um die Funktion anhand eines Beispiels von **EICAR** zu testen, rufen Sie <https://www.eicar.org/> auf, und laden Sie eine schädliche Probe herunter.

Hinweis: Keine Sorge. Sie können diesen EICAR-Test herunterladen, er ist sicher und nur eine Testdatei.

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

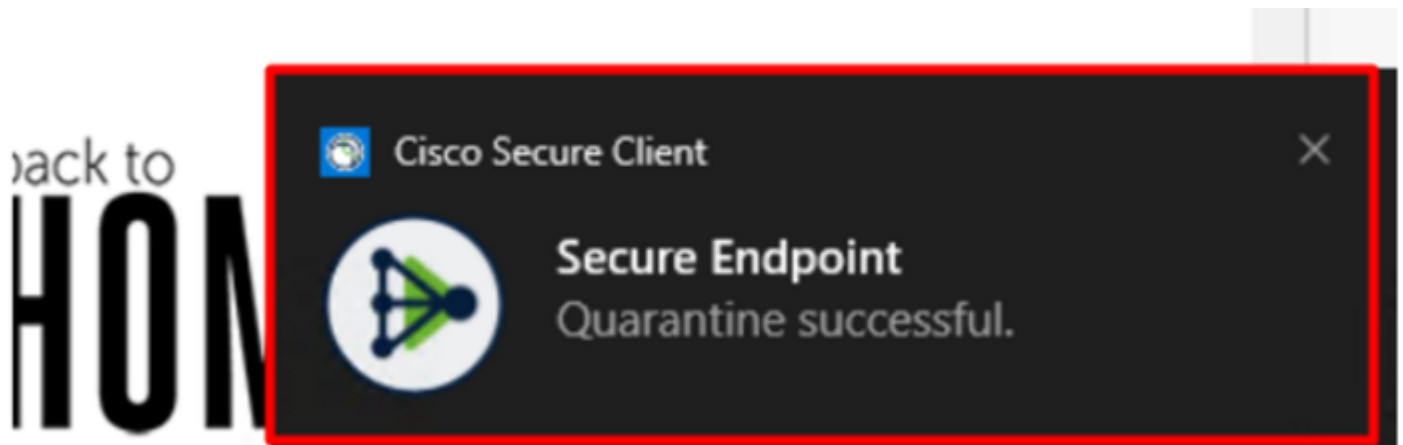


Blättern Sie nach unten, gehen Sie zum Abschnitt, und laden Sie die Testdatei herunter.

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 erkennt die Malware und verschiebt sie in die Quarantäne.



So sieht die Änderung aus, wie im Cisco Secure EndPoint Admin-Bereich gezeigt.

▶ 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				

Sie haben auch die Erkennung der Malware im System, dies bedeutet jedoch, dass die Endpunkte gemäß der Einstufung von Cisco Secure EndPoint auf dem Inbox.

Hinweis: Um einen Endpunkt zur Triage zu senden, müssen mehrere Artefakte oder merkwürdiges Verhalten erkannt werden, die einige aktivieren. Indicators of Compromise im Endgerät.

Im Dashboard, klicken Sie in das **Inbox**.



Secure Endpoint
Premier

Dashboard

Analysis ▾

Outbreak Control ▾

Management ▾

Accounts ▾

Dashboard

Dashboard

Inbox

Overview

Events

iOS Clarity

Refresh All

Auto-Refresh



Jetzt haben Sie eine Maschine, die Aufmerksamkeit erfordert.

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

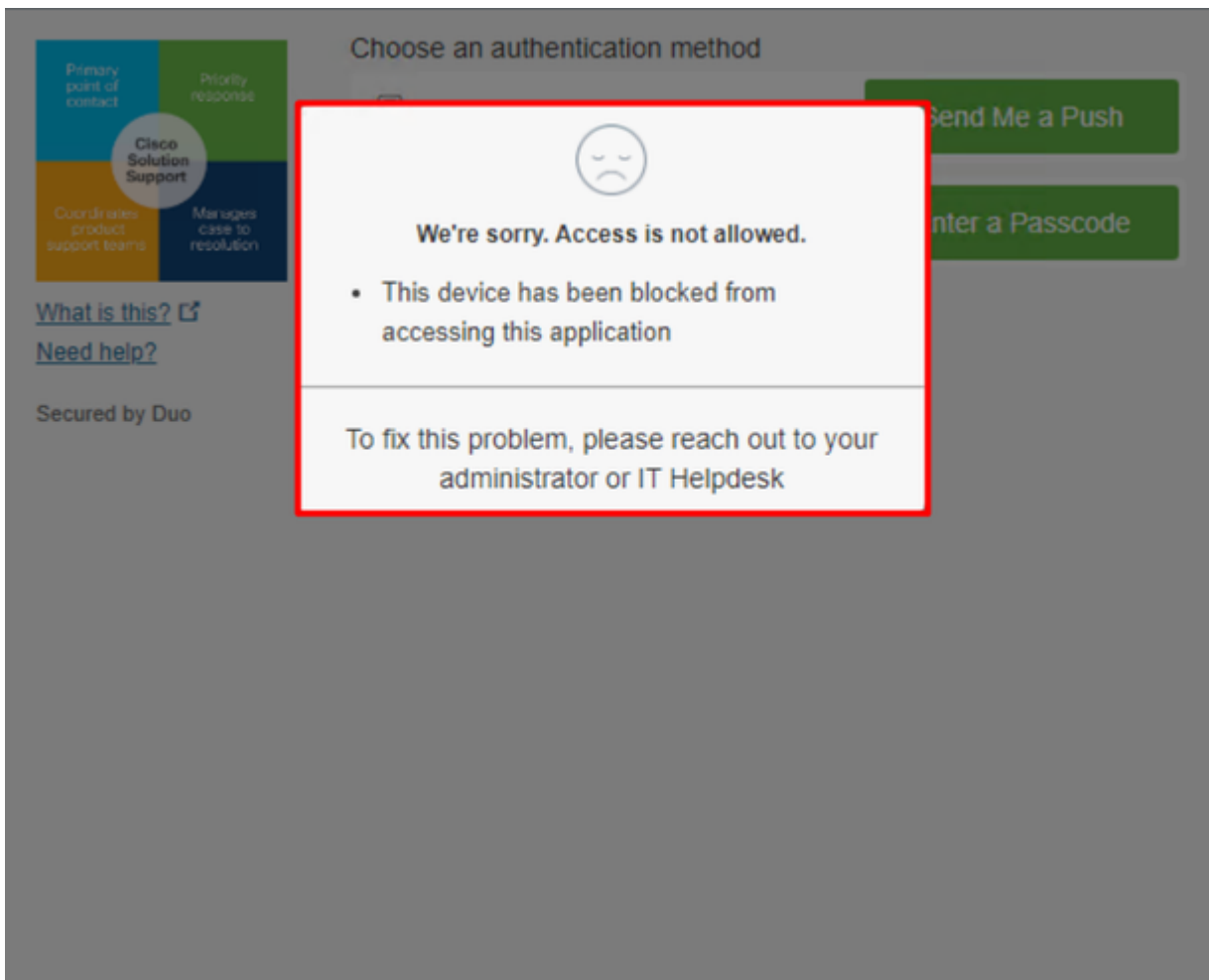
No known software vulnerabilities observed.

Take Forensic Snapshot View Snapshot Orbital Query Events Device Trajectory Diagnostics

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

Wechseln Sie jetzt zu Duo, und sehen Sie sich den Status an.

Es wird zuerst versucht, das Verhalten nach dem Aufsetzen des Computers auf Cisco Secure EndPoint anzuzeigen. Require Attention.



So ändert sich das in Duo und so wird das Ereignis unter Authentifizierungsereignissen angezeigt.

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



Ihr Computer wurde als nicht als Sicherheitsgerät für Ihr Unternehmen erkannt.

Zugriff auf einen Computer nach Überprüfung zulassen

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

Nach der Verifizierung durch Cisco Secure EndPoint und Ihren Cybersicherheitspezialisten können Sie Ihrem Duo-Gerät den Zugriff auf diesen Computer gestatten.

Nun stellt sich die Frage, wie man den Zugriff auf die von Duo geschützte App wieder erlaubt.

Gehen Sie zu Cisco Secure EndPoint, und `Inbox`, markieren Sie dieses Gerät als **resolved** um den Zugriff auf die von Duo geschützte Anwendung zu ermöglichen.

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

Danach haben Sie den Rechner nicht mehr mit dem Status attention required. Dies änderte sich zu resolved status.

0 Require Attention 0 In Progress 2 Resolved

In wenigen Worten, jetzt sind Sie bereit, den Zugriff auf unsere von Duo geschützte Anwendung erneut zu testen.

Cisco Solution Support

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

Secured by Duo

Choose an authentication method

Duo Push RECOMMENDED Send Me a Push

Passcode Enter a Passcode

Jetzt haben Sie die Berechtigung, den Push an Duo zu senden, und Sie sind bei der App angemeldet.

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**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.