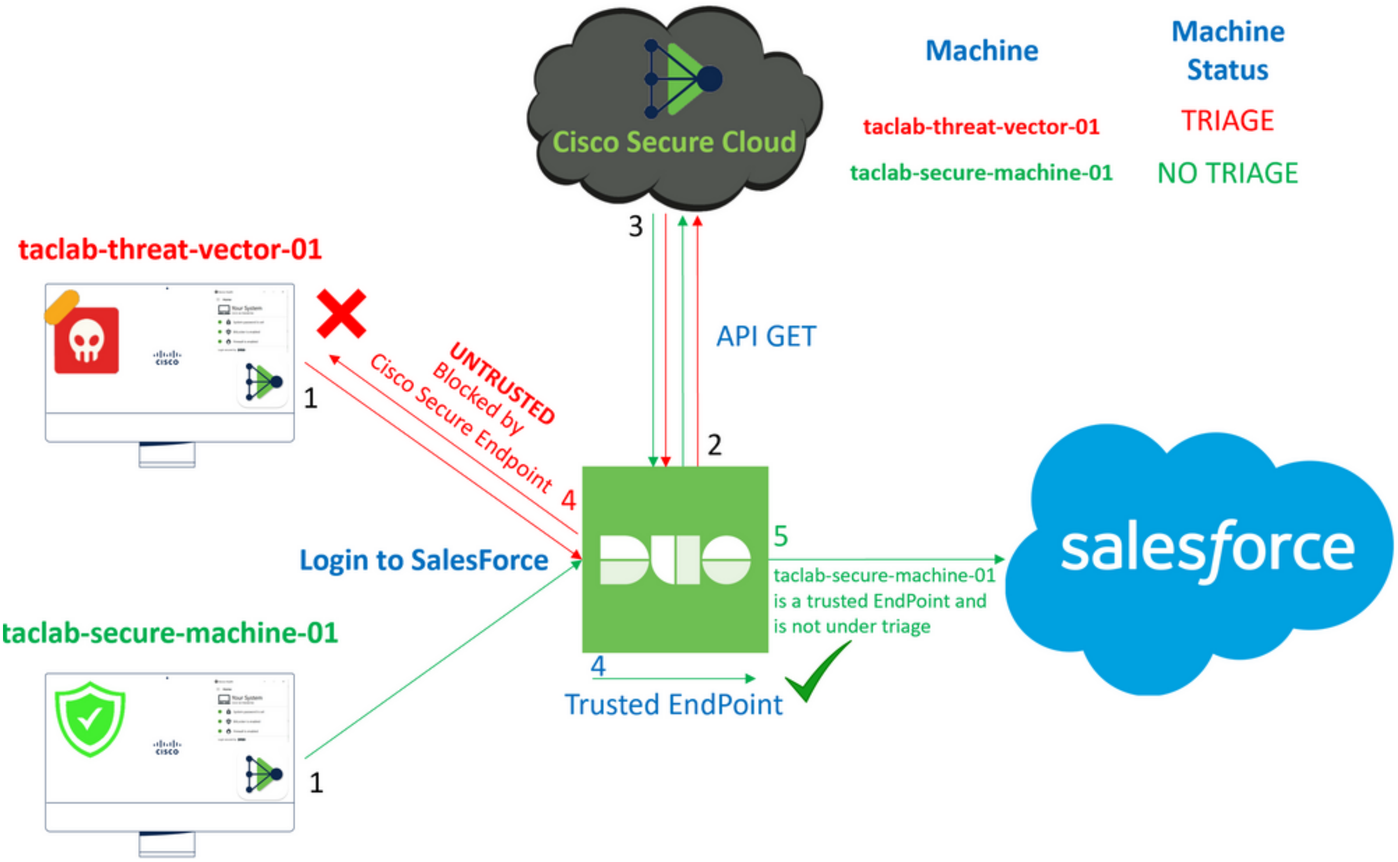
Configurazione di Duo e Secure Endpoint per rispondere alle minacce

Sommario

Introduzione



Questo documento descrive come integrare Duo Trusted EndPoint con Cisco Secure EndPoint.

Premesse

L'integrazione tra Cisco Secure EndPoint e Duo consente una collaborazione efficace in risposta alle minacce rilevate su dispositivi di rete attendibili. L'integrazione è possibile grazie a più strumenti di gestione dei dispositivi che stabiliscono l'affidabilità di ciascun dispositivo. Alcuni di questi strumenti includono:

- Servizi di dominio Active Directory
- Active Directory con stato del dispositivo
- Generico con stato del dispositivo
- Intune con stato del dispositivo
- Jamf Pro con stato del dispositivo
- LANDESK Management Suite
- Strumento di gestione delle risorse aziendali Mac OS X
- Manuale con stato del dispositivo
- Strumento Windows Enterprise Asset Management
- Workspace ONE con stato del dispositivo

Una volta integrati i dispositivi con uno strumento di gestione, è possibile integrare Cisco Secure EndPoint e Duo API nel Administration Panel. Successivamente, è necessario configurare la policy appropriata in Duo per eseguire la verifica dei dispositivi attendibili e rilevare i dispositivi compromessi che possono influire sulle applicazioni protette da Duo.

✎ Nota: in questo caso, utilizziamo Active Directory e l'integrità del dispositivo.

Prerequisiti

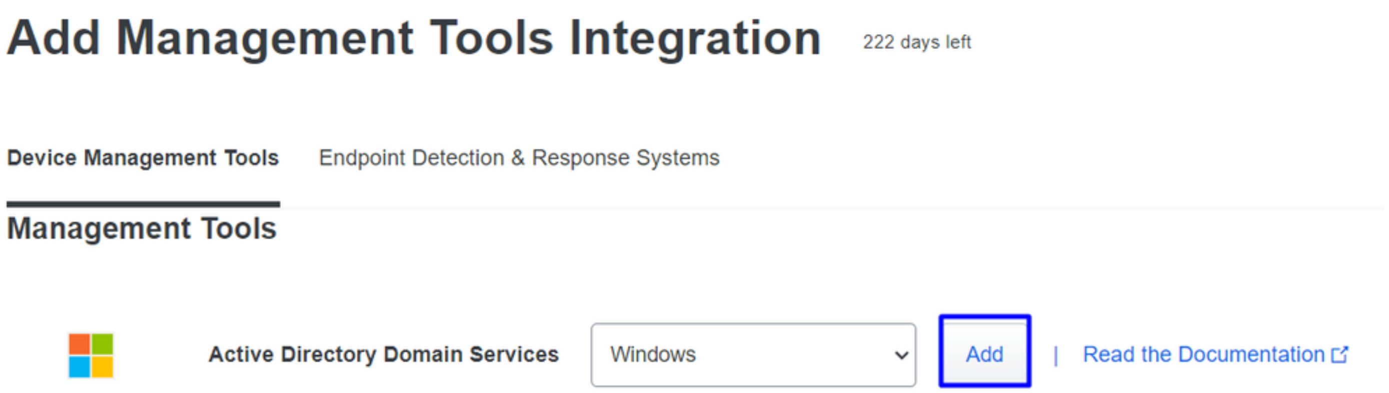
- Active Directory per eseguire l'integrazione.
- Per integrare Duo con gli endpoint trusted, è necessario che i dispositivi siano registrati nel dominio di Active Directory. Ciò consente a Duo di autenticare e autorizzare l'accesso alle risorse e ai servizi di rete in modo sicuro.
- Duo Beyond Plan.

Configurazione e caso di utilizzo

Configurazione dell'integrazione in Duo

Accedere a **Admin Panel** e andare al seguente indirizzo:

- **Trusted EndPoints > Add Integration**
- Seleziona Active Directory Domain Services



Add Management Tools Integration 222 days left

Management Tools

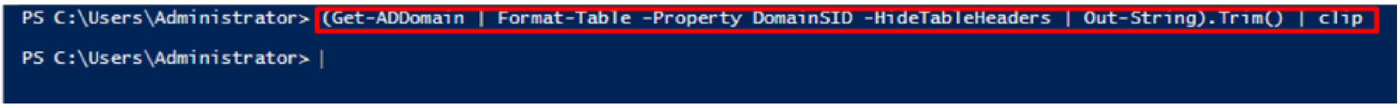
Active Directory Domain Services

Quindi, viene eseguito il reindirizzamento per configurare **Active Directory and Device Health**.

Tenere presente che questa opzione funziona solo con i computer nel dominio.

Passare alla directory attiva ed eseguire il comando successivo in PowerShell:

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



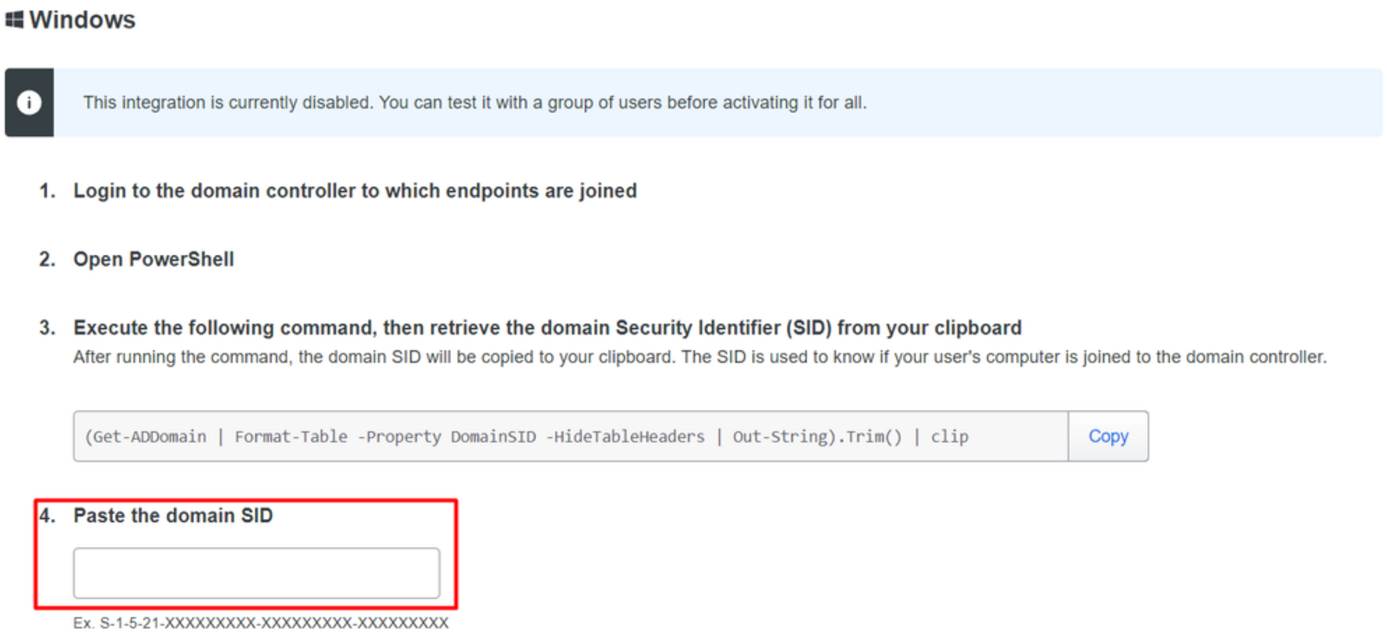
```
PS C:\Users\Administrator> (Get-ADDomain | Format-Table -Property DomainSID -HideTableHeaders | Out-String).Trim() | clip
PS C:\Users\Administrator> |
```

Accertarsi quindi di aver copiato negli Appunti l'identificatore di protezione di Active Directory.

Esempio

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

Viene utilizzato nell'integrazione di Active Directory e dell'integrità del dispositivo.



Windows

This integration is currently disabled. You can test it with a group of users before activating it for all.

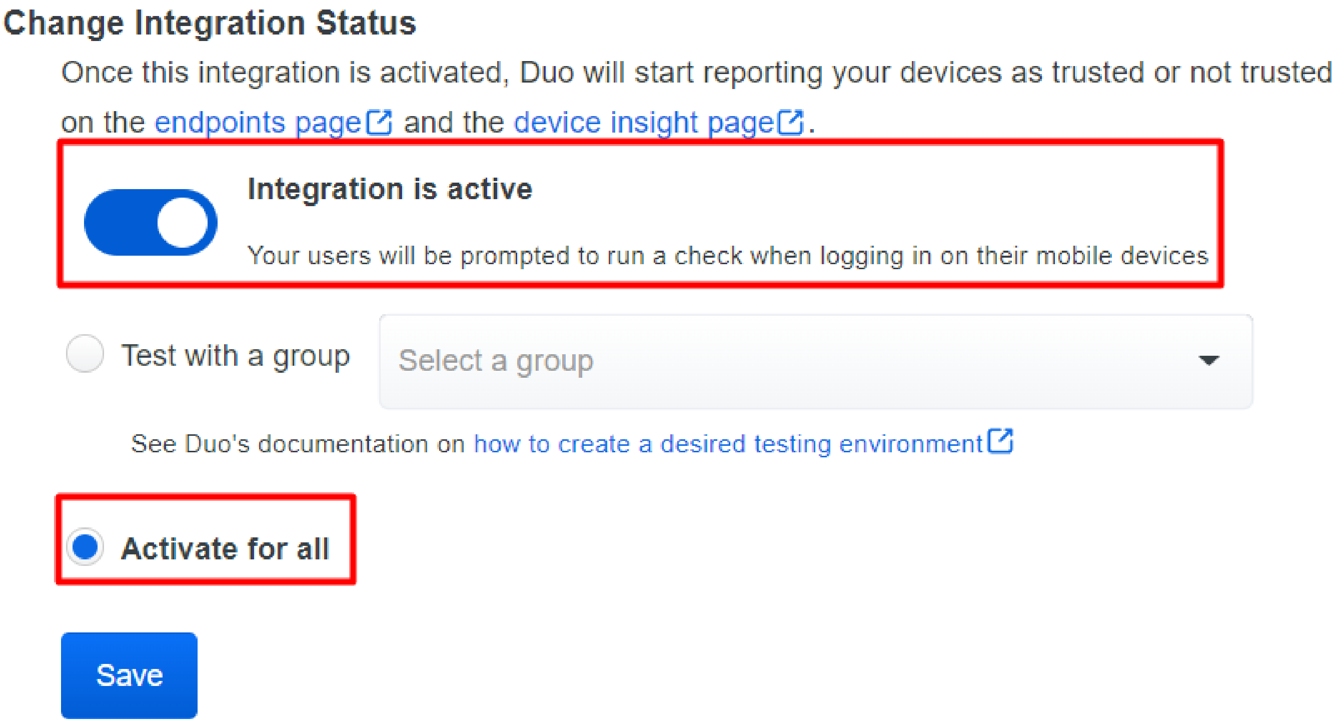
1. Login to the domain controller to which endpoints are joined
2. Open PowerShell
3. Execute the following command, then retrieve the domain Security Identifier (SID) from your clipboard
   After running the command, the domain SID will be copied to your clipboard. The SID is used to know if your user's computer is joined to the domain controller.

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

4. Paste the domain SID

Ex. S-1-5-21-XXXXXXXXX-XXXXXXXXX-XXXXXXXXX

Fare clic su **Save** e consentono l'integrazione e Activate for all. In caso contrario, non è possibile eseguire l'integrazione con Cisco Secure EndPoint.



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

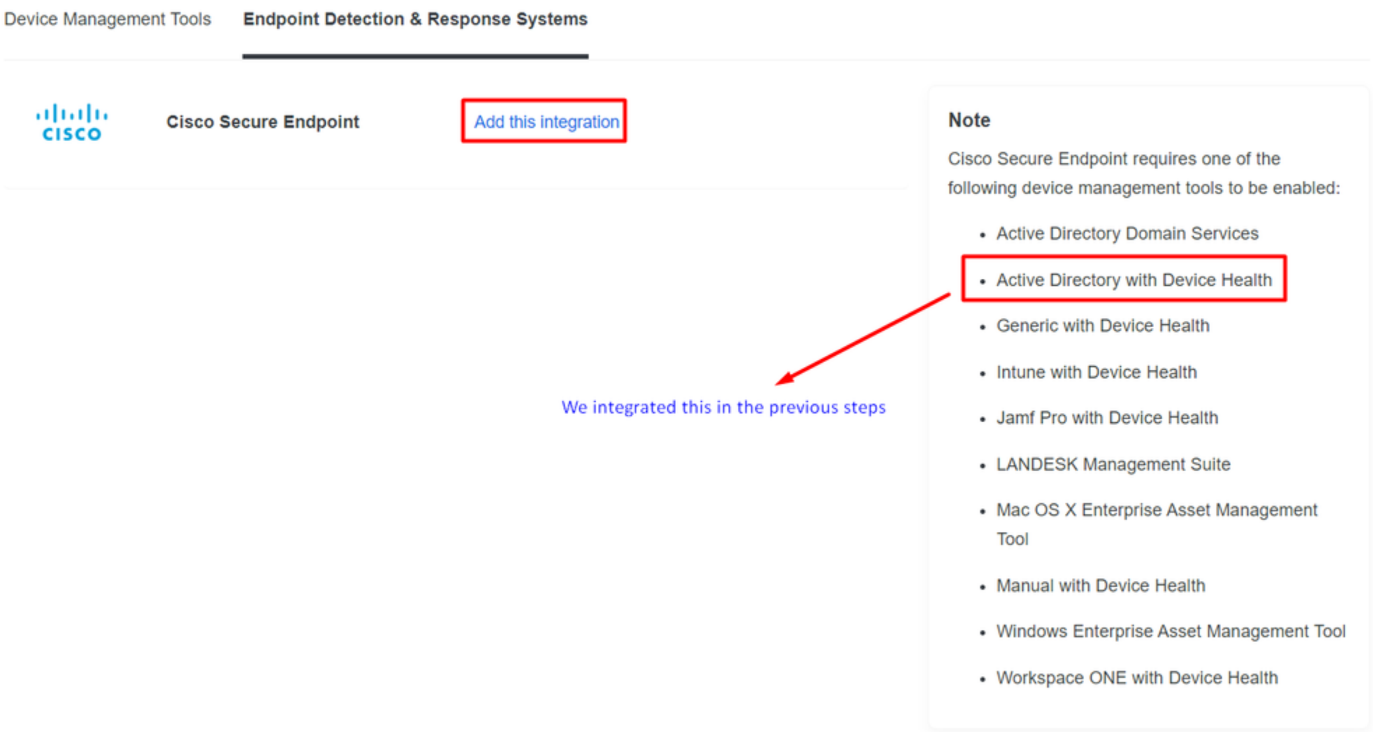
Your users will be prompted to run a check when logging in on their mobile devices

○ Test with a group Select a group

See Duo's documentation on how to create a desired testing environment

● Activate for all

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



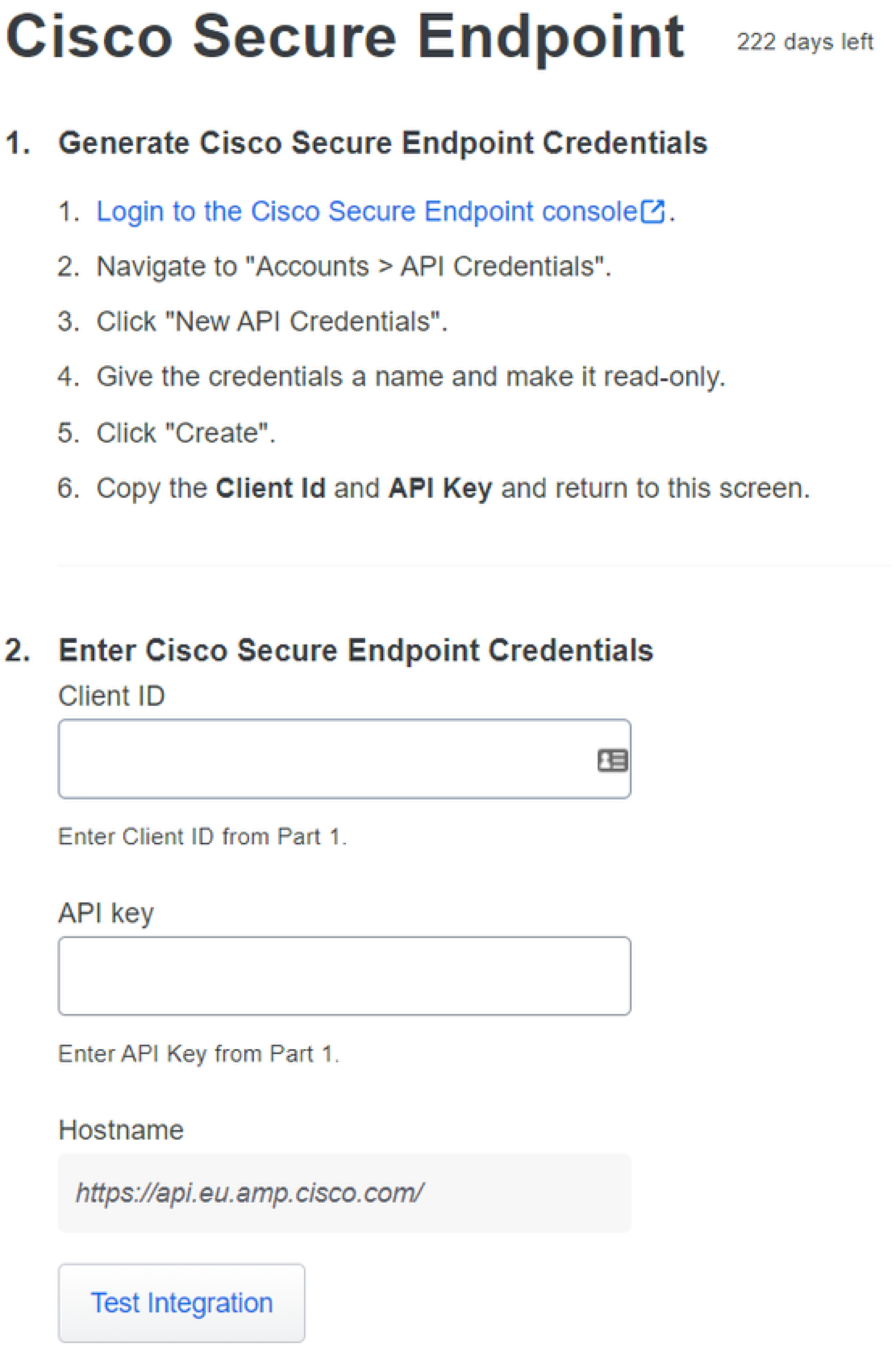
Device Management Tools
Endpoint Detection & Response Systems
Cisco Secure Endpoint
Add this integration
We integrated this in the previous steps

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

A questo punto, è possibile accedere alla pagina principale dell'integrazione di 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

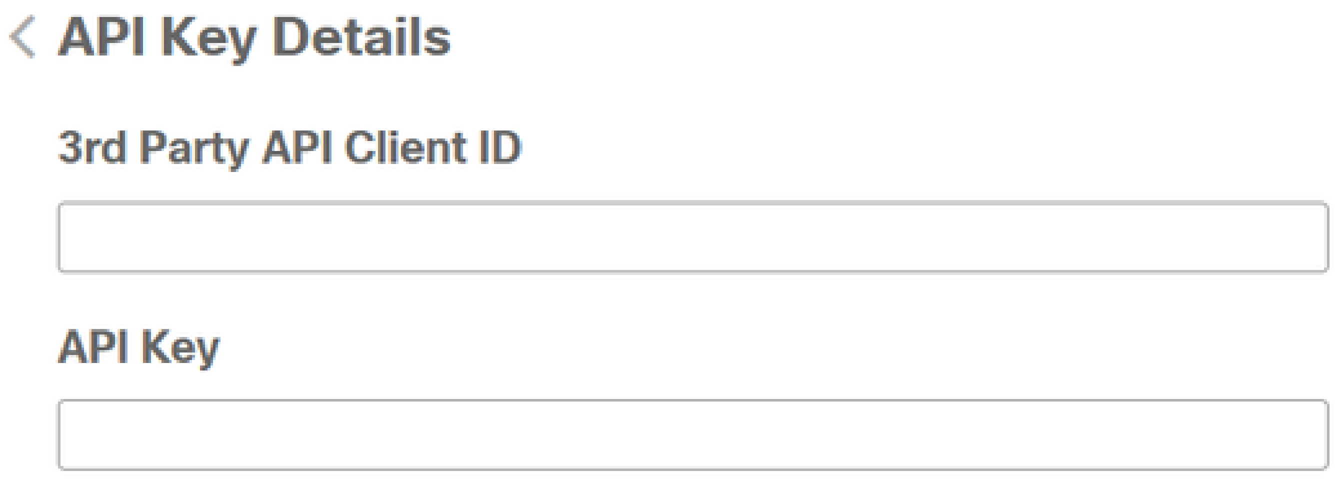
Enter API Key from Part 1.

Hostname

https://api.eu.amp.cisco.com/

invia una query a Cisco Secure EndPoint per verificare se il dispositivo soddisfa i requisiti della policy.

Inserisci **Application Name**, Scope, e **Create**.

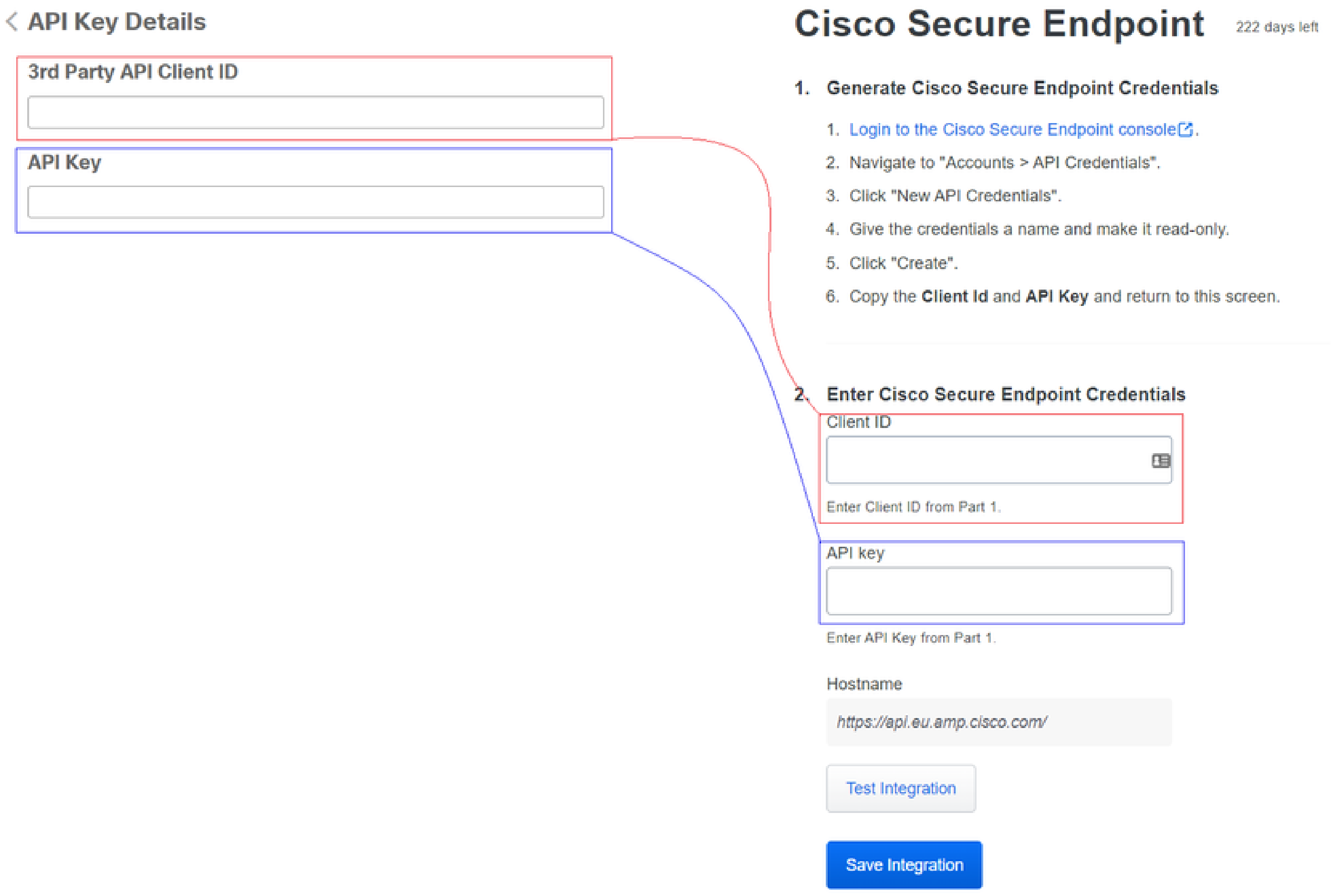


< API Key Details

3rd Party API Client ID

API Key

- Copiare 3rd API Party Client ID da Cisco Secure EndPoint Duo Admin Panel in Client ID.
- Copiare API Key da Cisco Secure EndPoint Duo Admin Panel in API Key.



< API Key Details

3rd Party API Client ID

API Key

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

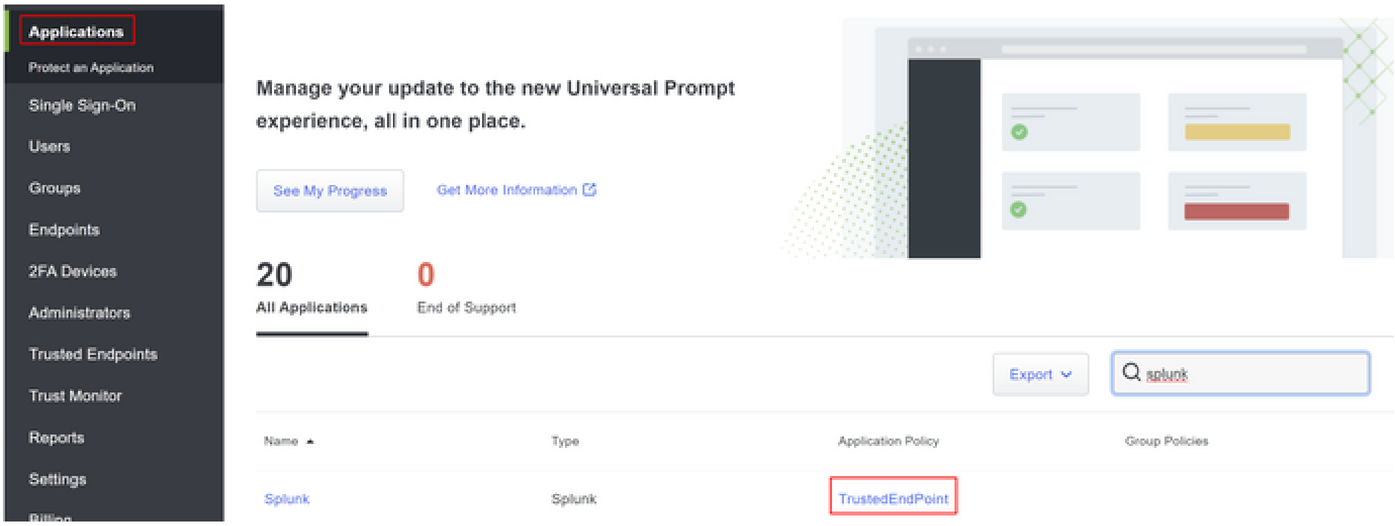
Save Integration

Testare l'integrazione. Se tutto funziona correttamente, fare clic su **Save** per salvare l'integrazione.

Configurare i criteri in Duo

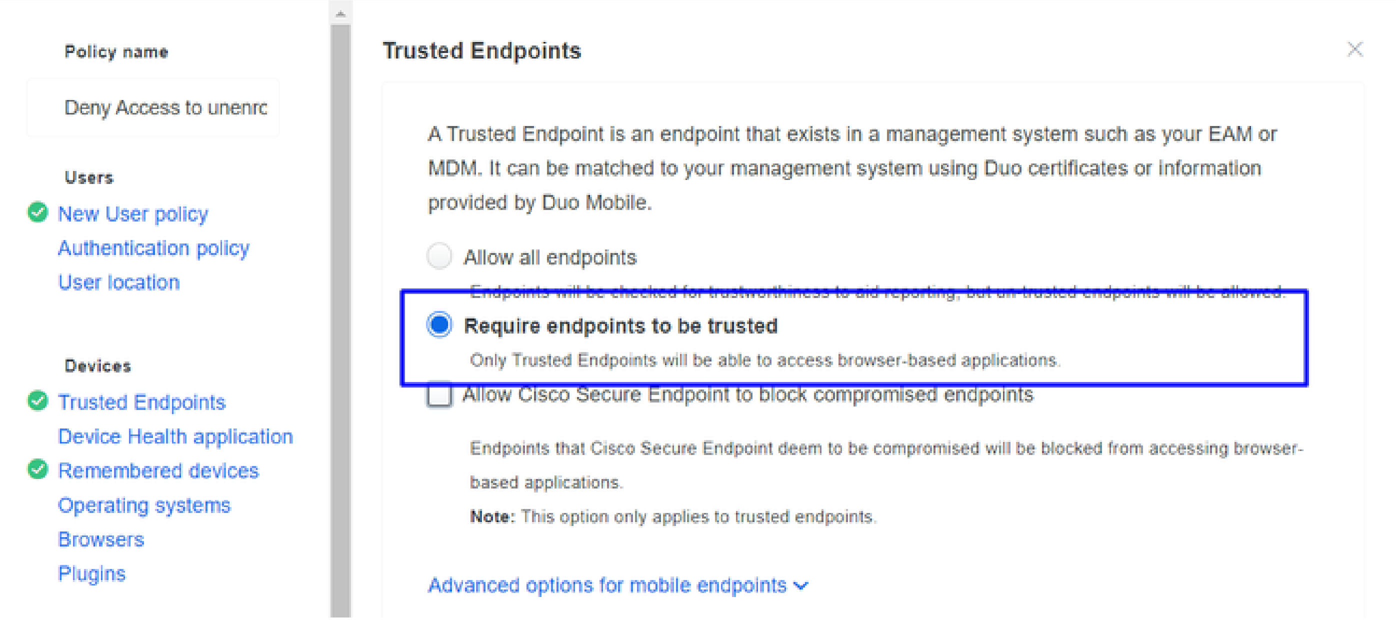
Per configurare i criteri per l'integrazione, è necessario eseguire l'applicazione:

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



Name	Type	Application Policy	Group Policies
Splunk	Splunk	TrustedEndPoint	

Configurare il criterio per rilevare un dispositivo attendibile



Policy name: Deny Access to unenrc

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.

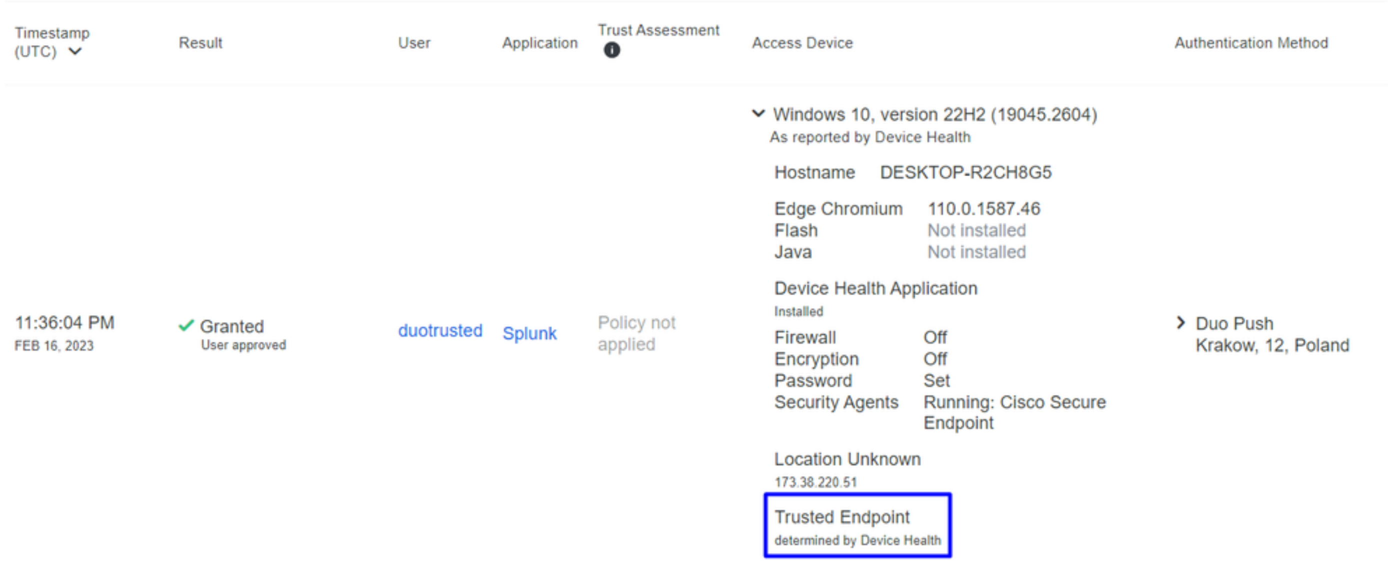
□ Allow Cisco Secure Endpoint to block compromised endpoints

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.

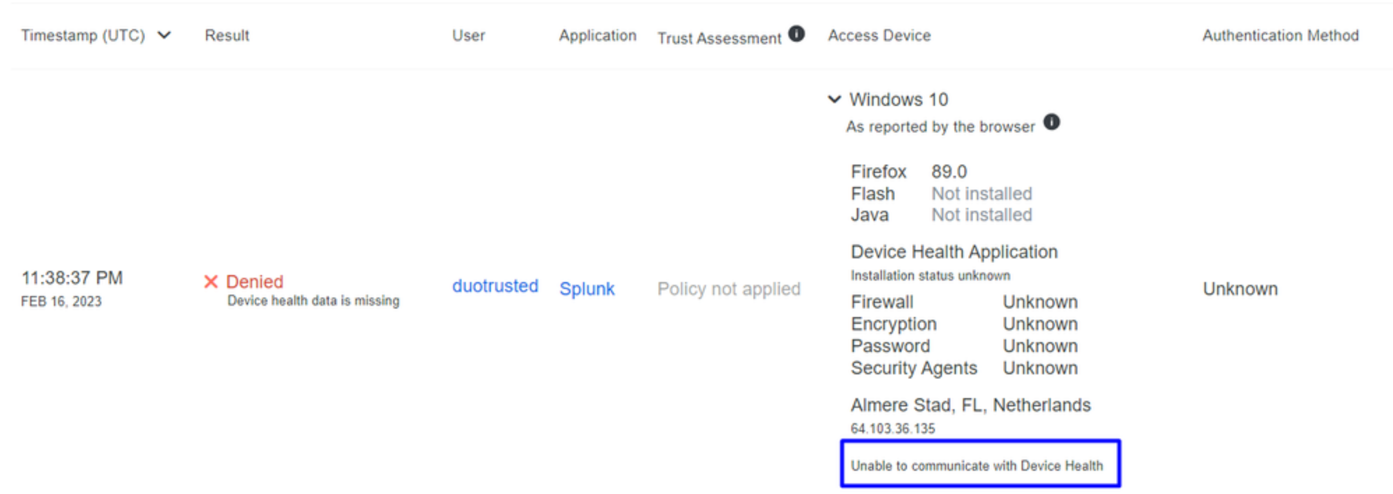
Verifica computer attendibili

Computer con Duo Device Health e aggiunta al dominio

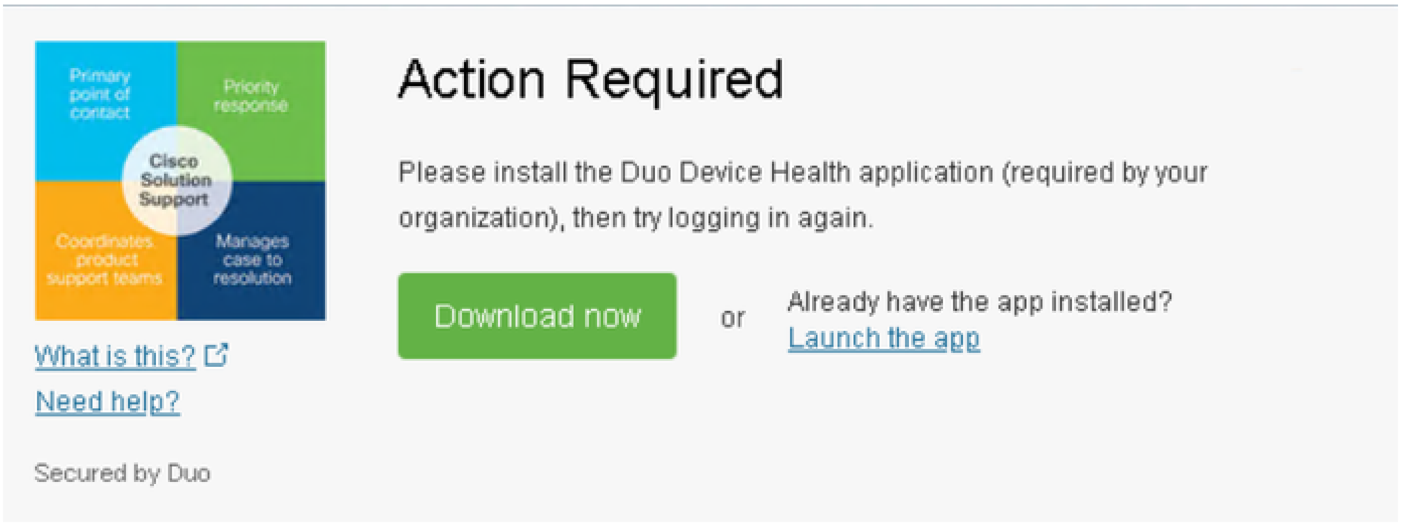


Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device	Authentication Method
11:36:04 PM FEB 16, 2023	✓ Granted User approved	duotrusted	Splunk	Policy not applied	Windows 10, version 22H2 (19045.2604) As reported by Device Health Hostname DESKTOP-R2CH8G5 Edge Chromium 110.0.1587.46 Flash 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 Trusted Endpoint determined by Device Health	Duo Push Krakow, 12, Poland

Computer all'esterno del dominio senza Duo Device Health



Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device	Authentication Method
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 Unknown Encryption Unknown Password Unknown Security Agents Unknown Almere Stad, FL, Netherlands 64.103.36.135 Unable to communicate with Device Health	Unknown



What is this?

Need help?

Secured by Duo

Action Required

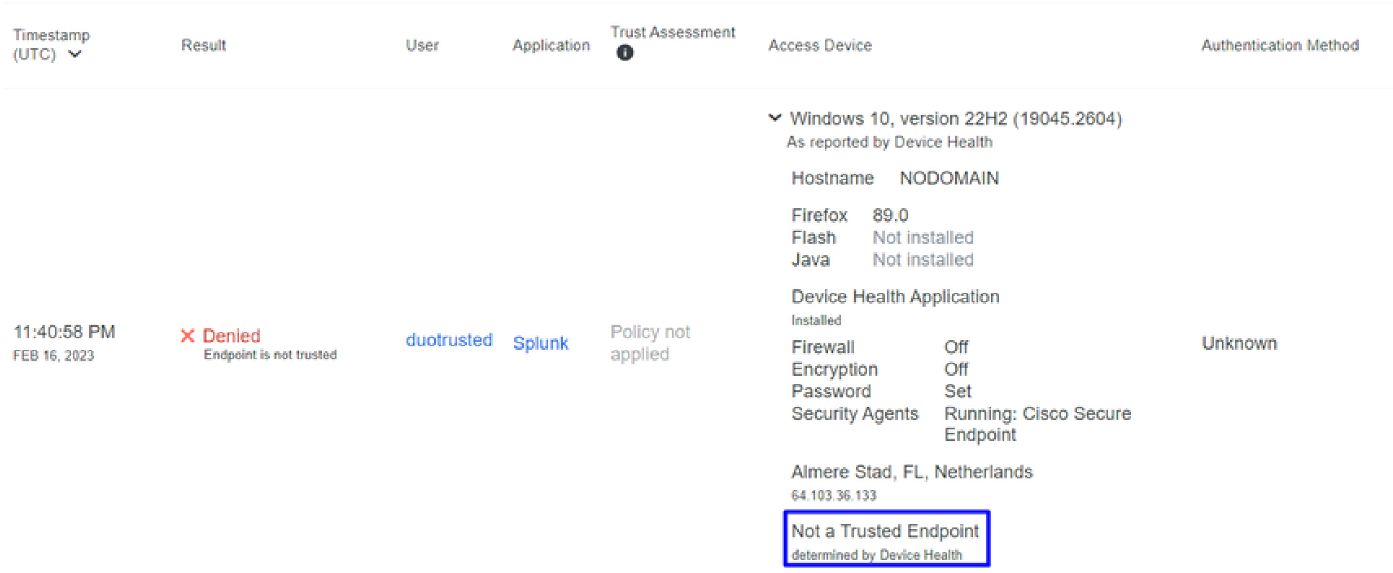
Please install the Duo Device Health application (required by your organization), then try logging in again.

Download now

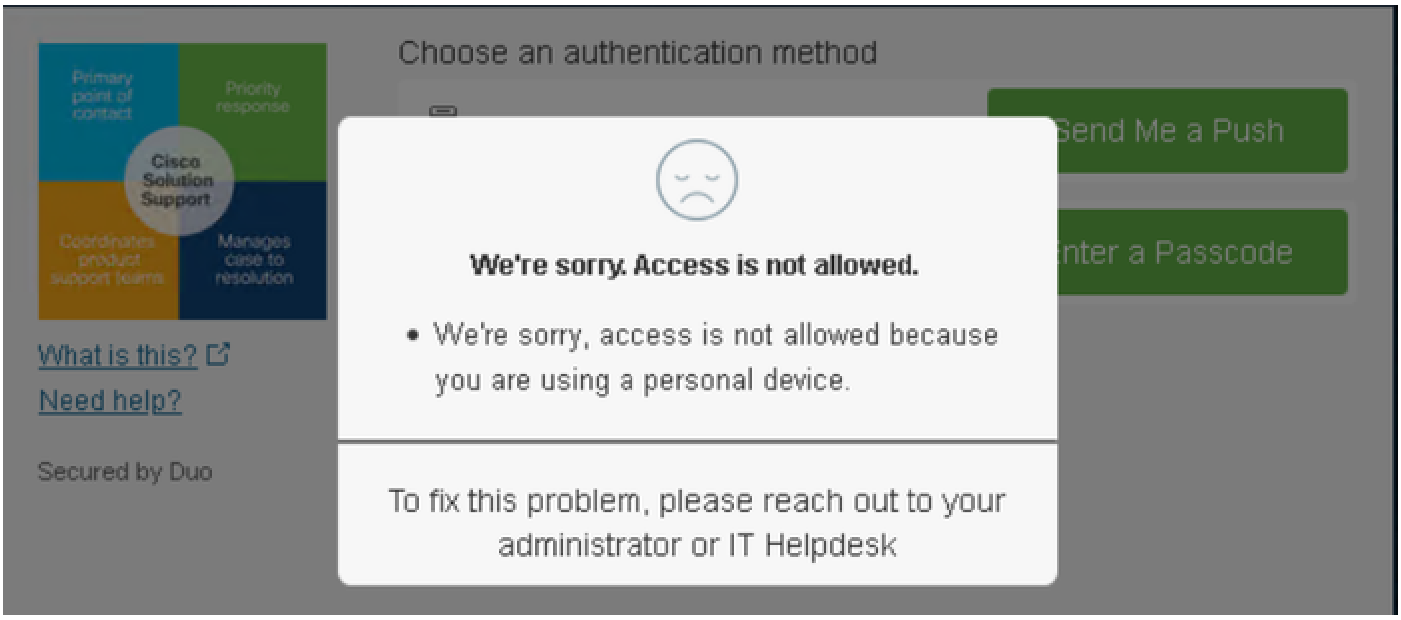
or

Already have the app installed? Launch the app

Computer all'esterno del dominio con Duo Device Health



Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device	Authentication Method
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 determined by Device Health	Unknown



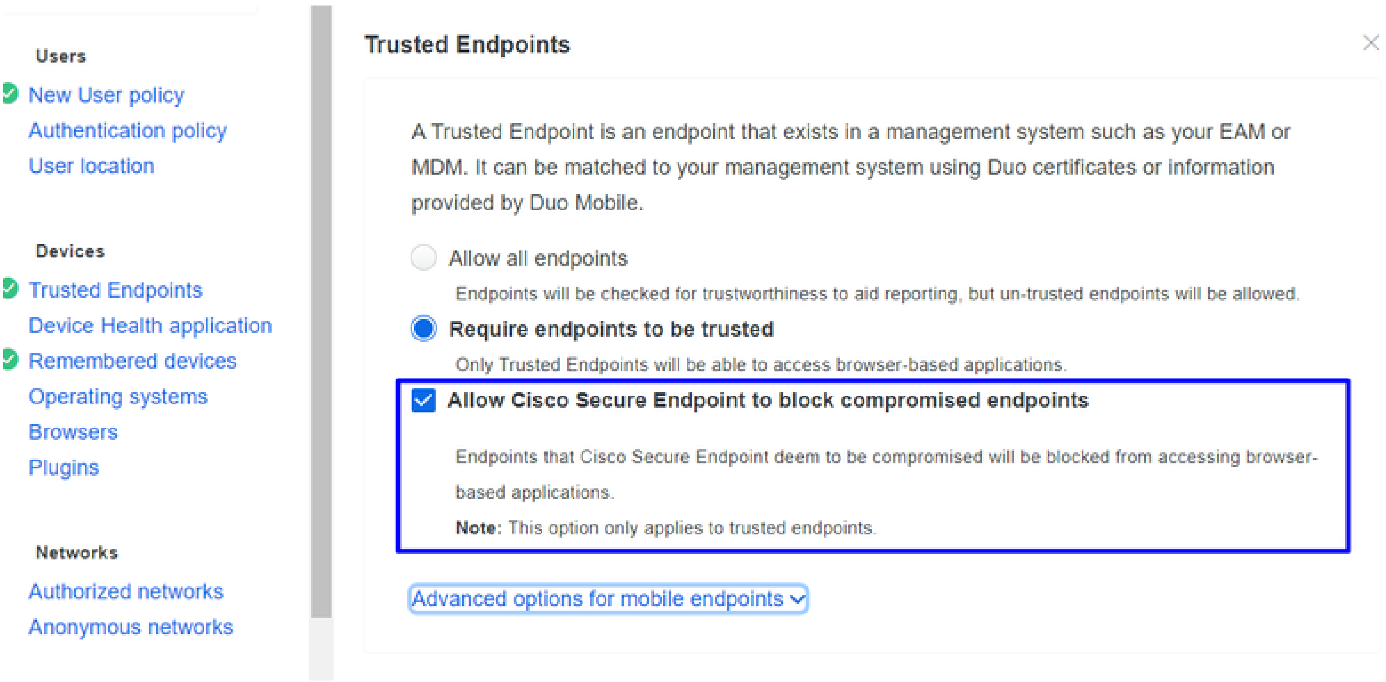
We're sorry. Access is not allowed.

- We're sorry, access is not allowed because you are using a personal device.

To fix this problem, please reach out to your administrator or IT Helpdesk

Configurare il criterio per Cisco Secure EndPoint

In questa impostazione dei criteri configurare il dispositivo già attendibile in modo che soddisfi i requisiti relativi alle minacce che possono influire sull'applicazione, in modo che se un dispositivo viene infettato o se alcuni comportamenti contrassegnano il computer con **suspicious artifacts** o Indicators of Compromise, è possibile bloccare l'accesso del computer alle applicazioni protette.



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**

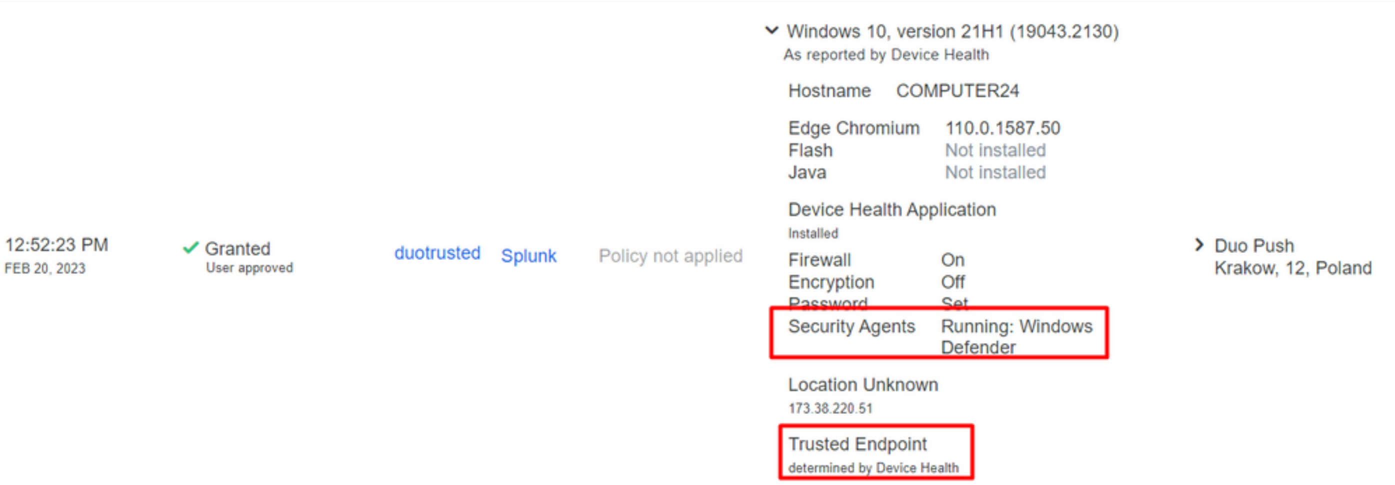
Endpoints that Cisco Secure Endpoint deem to be compromised will be blocked from accessing browser-based applications.

Note: This option only applies to trusted endpoints.

Verifica dei computer attendibili con Cisco Secure EndPoint

Computer senza Cisco Secure Agent installato

In questo caso, la macchina può passare senza la verifica AMP.



12:52:23 PM
FEB 20, 2023

✓ Granted
User approved

duotrusted

Splunk

Policy not applied

Windows 10, version 21H1 (19043.2130)
As reported by Device Health

Hostname COMPUTER24

Edge Chromium 110.0.1587.50
Flash Not installed
Java Not installed

Device Health Application
Installed
Firewall On
Encryption Off
Password Set
Security Agents Running: Windows Defender

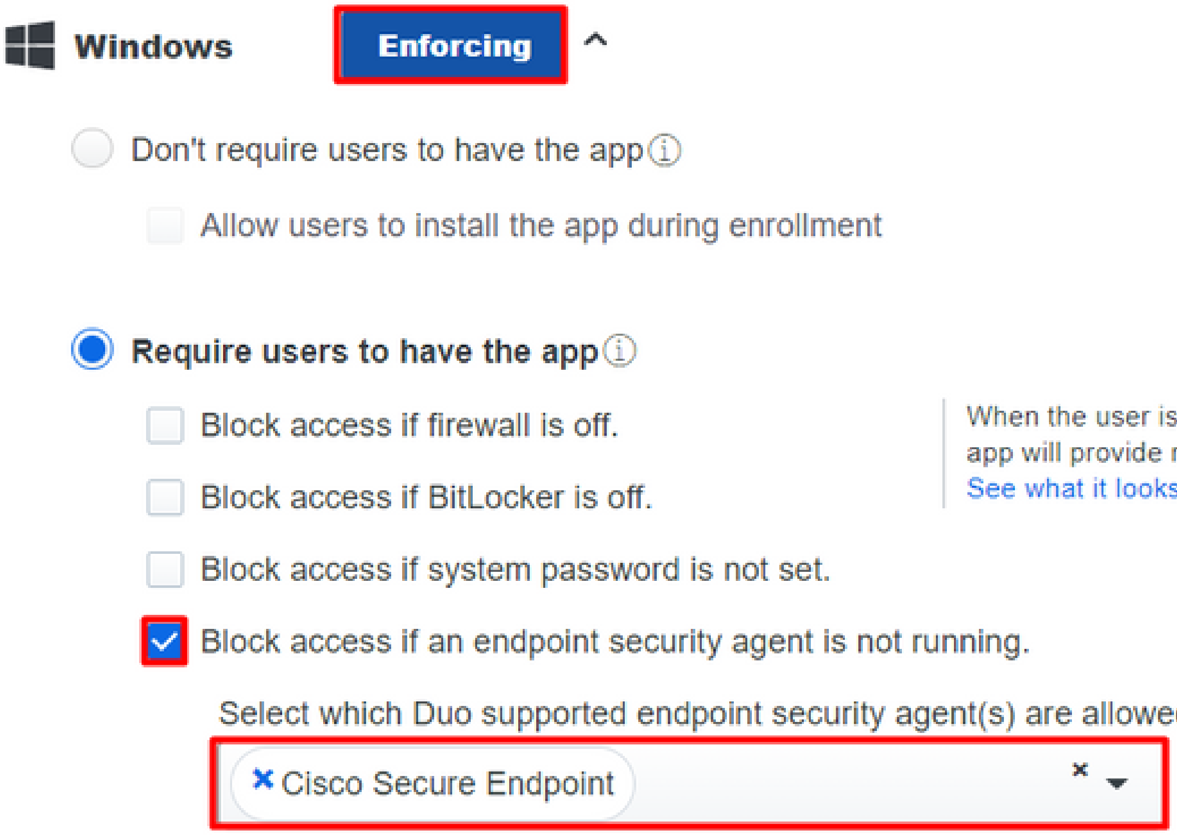
Location Unknown
173.38.220.51

Trusted Endpoint
determined by Device Health

Duo Push
Krakow, 12, Poland

Se si desidera impostare un criterio restrittivo, è possibile impostarlo in modo che sia più restrittivo modificando il Device Health Application criteri da **Reporting** a **Enforcing**.

E aggiungi 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.

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

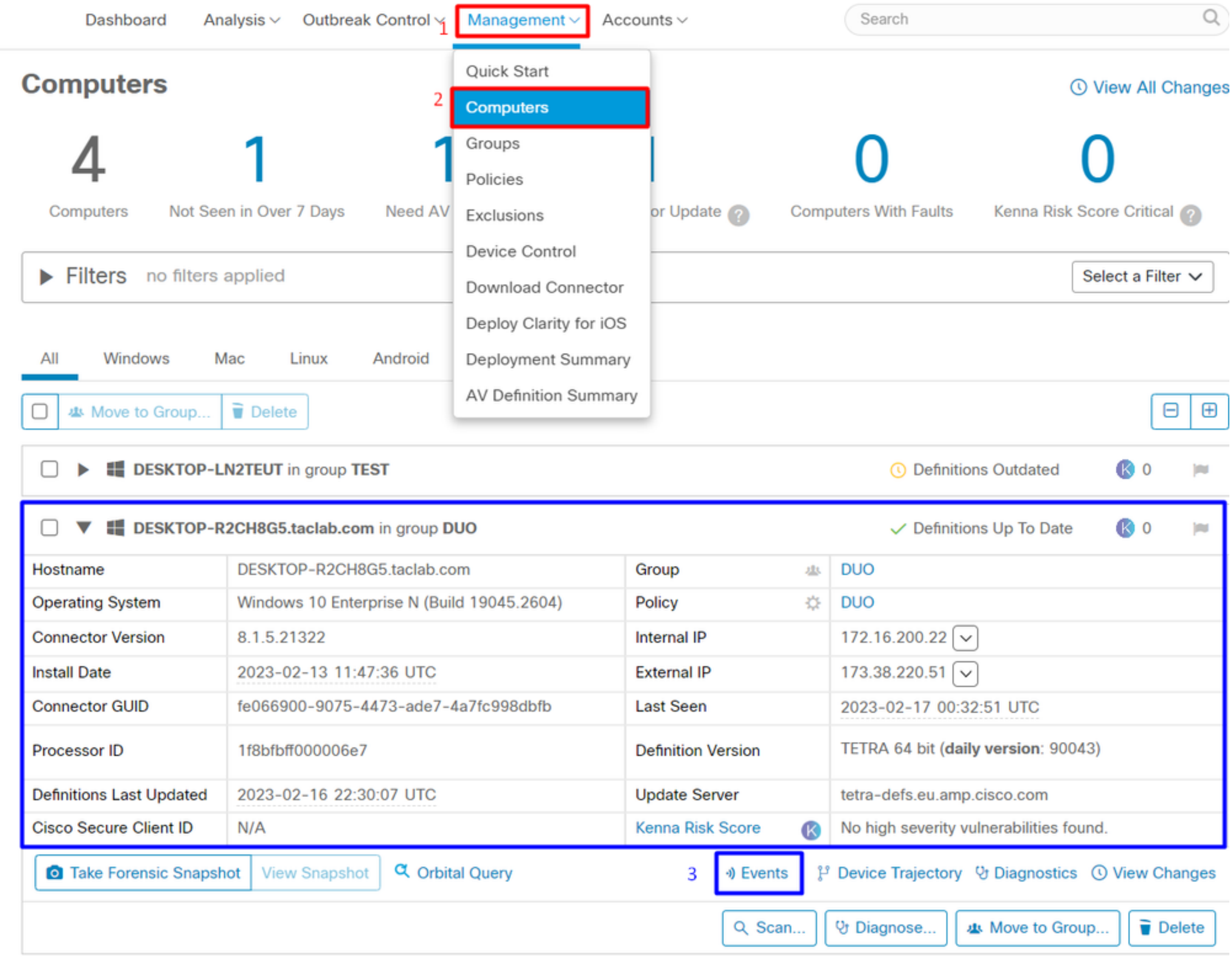
Computer senza infezione

Su un computer, senza infezioni, è possibile verificare il funzionamento di Duo con Cisco Secure EndPoint per scambiare informazioni sullo stato del computer e su come gli eventi vengono mostrati in questo caso in Duo e Cisco Secure EndPoint.

Se si controlla lo stato del computer in Cisco Secure EndPoint:

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

Quando si applica un filtro al computer, è possibile visualizzare l'evento relativo e, in questo caso, determinare che il computer è pulito.

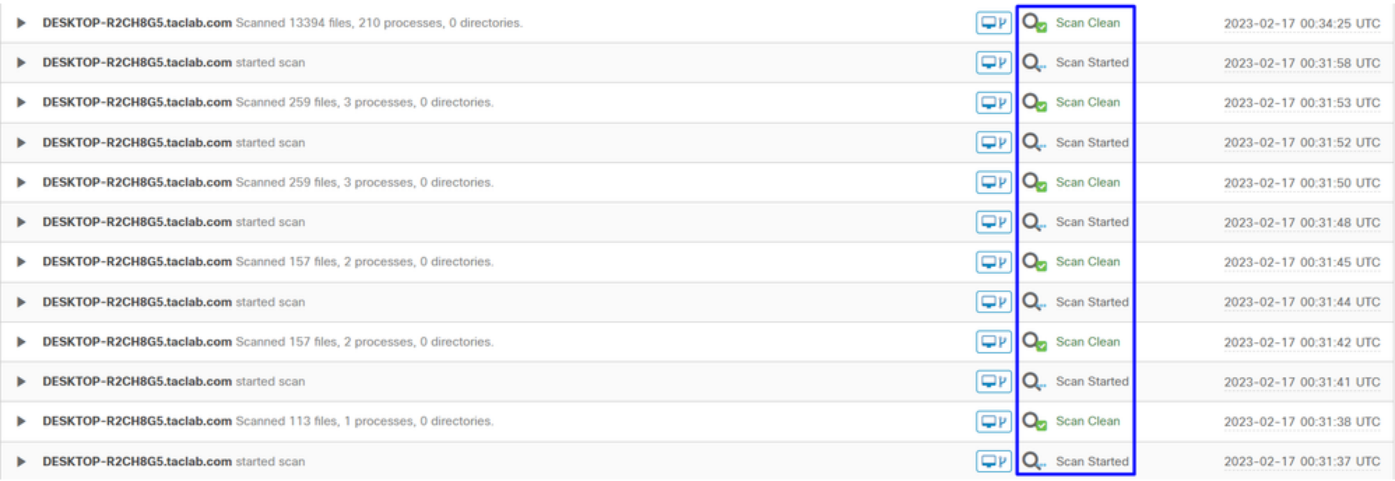


□ ▶ **DESKTOP-LN2TEUT** in group **TEST** — Definitions Outdated — 0

□ ▼ **DESKTOP-R2CH8G5.taclab.com** in group **DUO** — ✓ Definitions Up To Date — 0

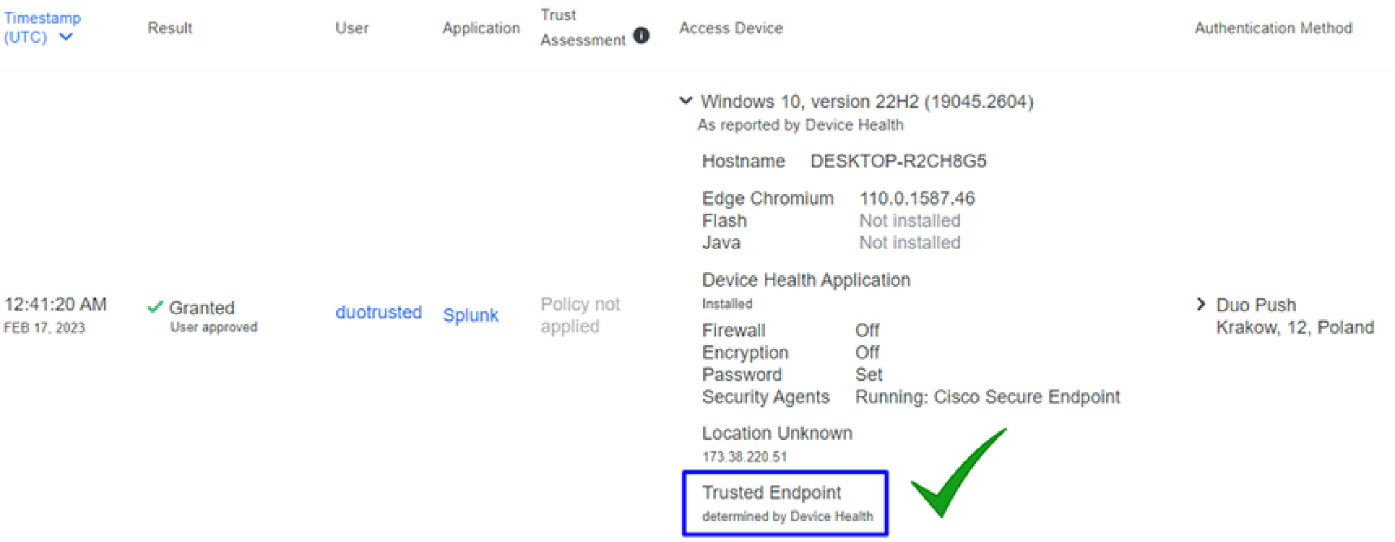
Hostname	DESKTOP-R2CH8G5.taclab.com	Group	DUO
Operating System	Windows 10 Enterprise N (Build 19045.2604)	Policy	DUO
Connector Version	8.1.5.21322	Internal IP	172.16.200.22
Install Date	2023-02-13 11:47:36 UTC	External IP	173.38.220.51
Connector GUID	fe066900-9075-4473-ade7-4a7fc998dbfb	Last Seen	2023-02-17 00:32:51 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.

È possibile notare che non è stato rilevato alcun dispositivo e che il dispositivo è in stato clean (pulito), il che significa che il computer non è in grado di partecipare.



▶ **DESKTOP-R2CH8G5.taclab.com** Scanned 13394 files, 210 processes, 0 directories.	Scan Clean	2023-02-17 00:34:25 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** started scan	Scan Started	2023-02-17 00:31:58 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** Scanned 259 files, 3 processes, 0 directories.	Scan Clean	2023-02-17 00:31:53 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** started scan	Scan Started	2023-02-17 00:31:52 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** Scanned 259 files, 3 processes, 0 directories.	Scan Clean	2023-02-17 00:31:50 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** started scan	Scan Started	2023-02-17 00:31:48 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** Scanned 157 files, 2 processes, 0 directories.	Scan Clean	2023-02-17 00:31:45 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** started scan	Scan Started	2023-02-17 00:31:44 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** Scanned 157 files, 2 processes, 0 directories.	Scan Clean	2023-02-17 00:31:42 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** started scan	Scan Started	2023-02-17 00:31:41 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** Scanned 113 files, 1 processes, 0 directories.	Scan Clean	2023-02-17 00:31:38 UTC
▶ **DESKTOP-R2CH8G5.taclab.com** started scan	Scan Started	2023-02-17 00:31:37 UTC

In questo modo Duo classifica quel computer:



Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device	Authentication Method
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 Trusted Endpoint determined by Device Health	Duo Push Krakow, 12, Poland

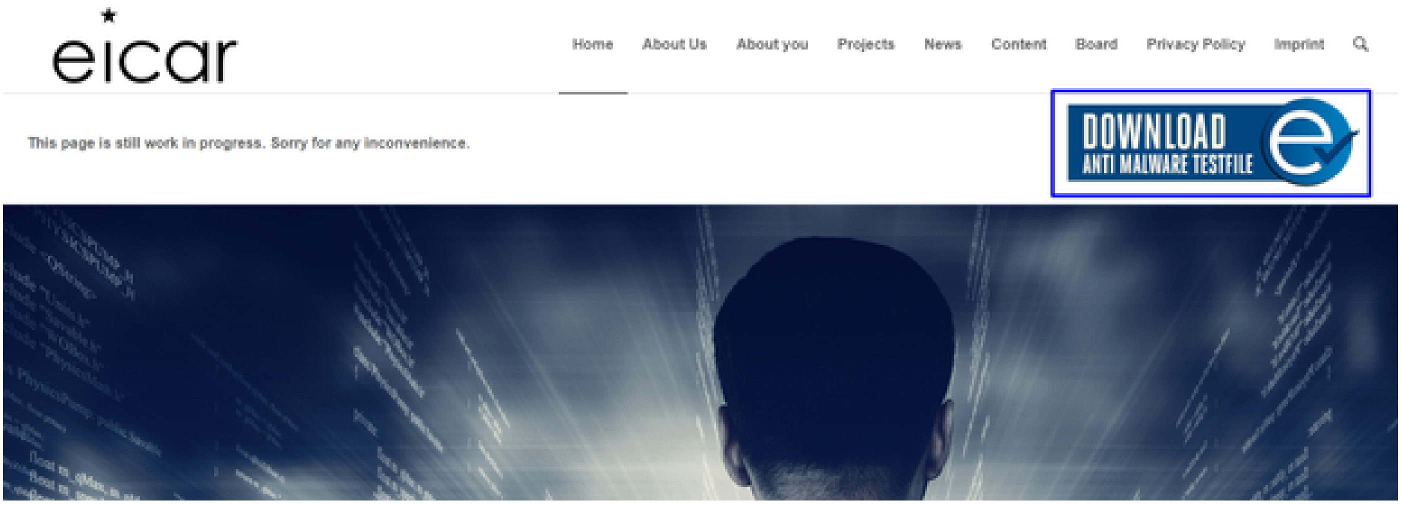
La macchina gestisce trusted etichetta.

Cosa succede se la stessa macchina viene infettata da un Malicious Actor, abbia ripetuti tentativi di infezione, o Indicators of Compromise avvisi relativi a questo computer?

Computer infetto

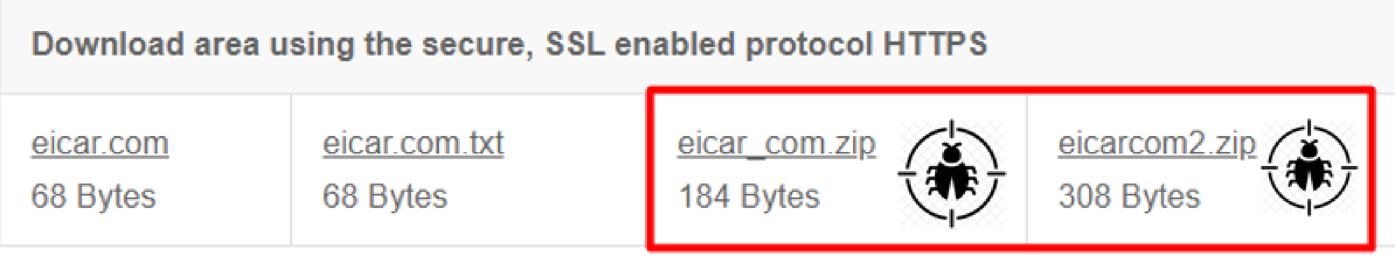
Per provare con un esempio di EICAR per verificare la funzionalità, accedere a https://www.eicar.org/ e scaricare un esempio dannoso.

Nota: non preoccuparti. È possibile scaricare il test EICAR, è sicuro ed è solo un file di test.



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

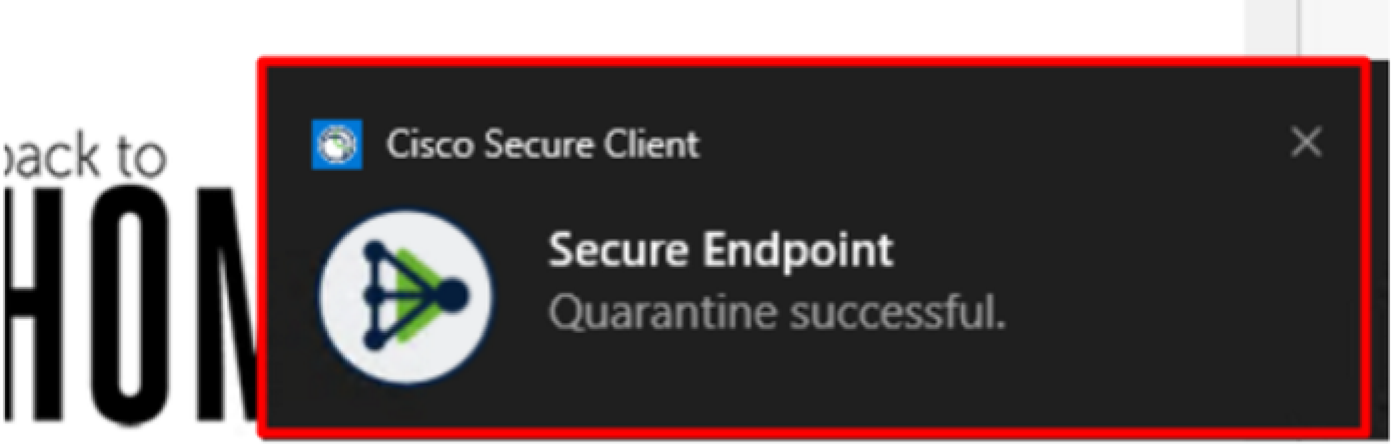
Scorrere verso il basso e andare alla sezione e scaricare il file di test.



Download area using the secure, SSL enabled protocol HTTPS

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

Cisco Secure EndPoint rileva il malware e lo sposta in quarantena.

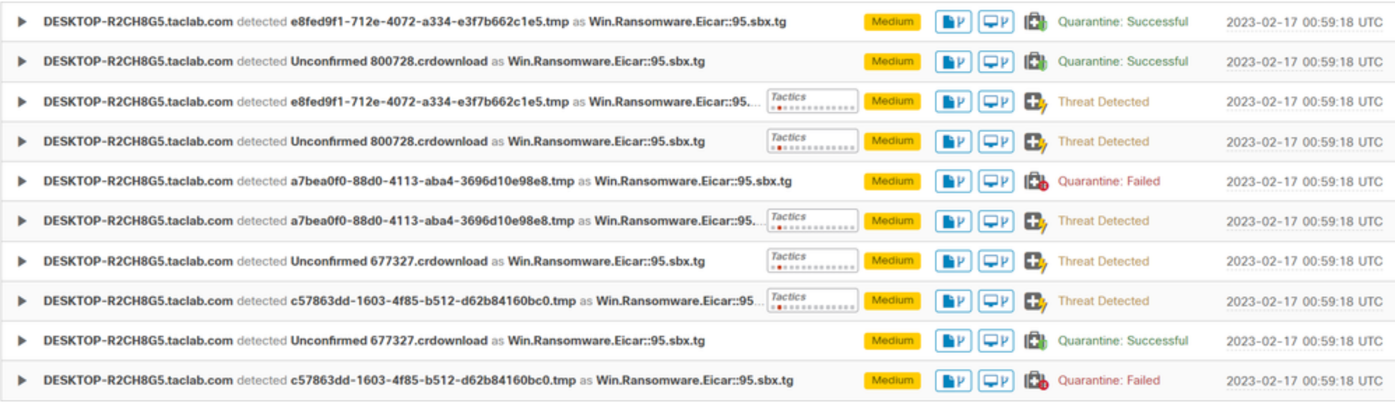


Cisco Secure Client

Secure Endpoint

Quarantine successful.

Questo è il modo in cui cambia, come mostrato nel pannello Cisco Secure EndPoint Admin.

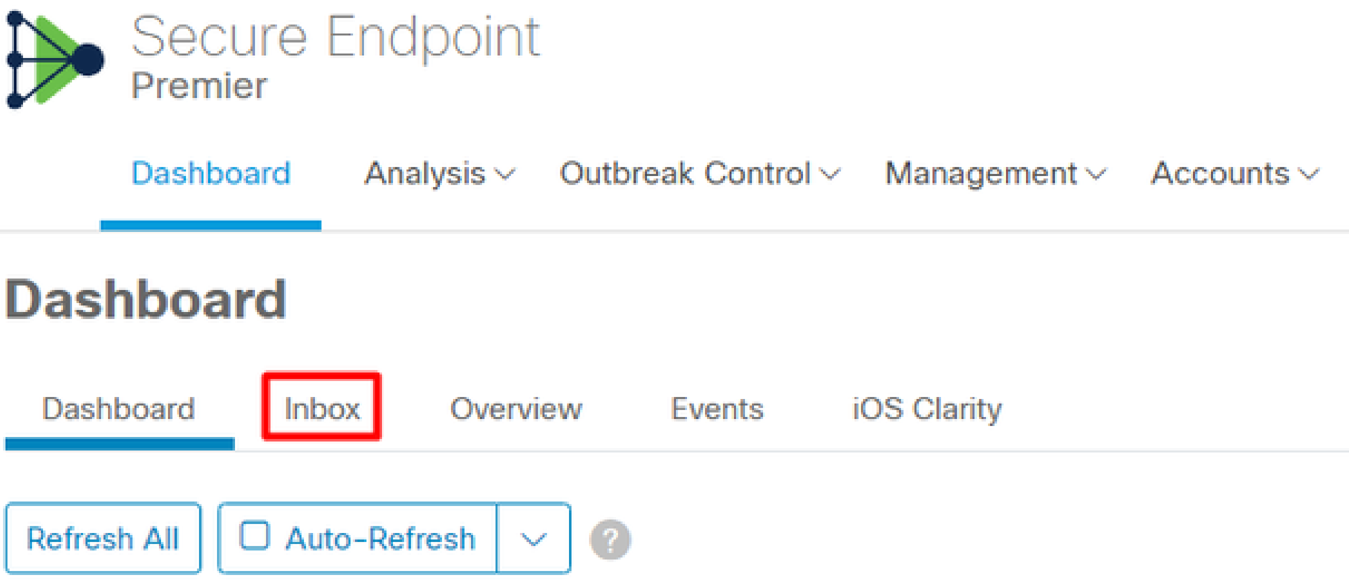


▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar::95.sbx.tg		Medium	Quarantine: Successful	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar::95.sbx.tg		Medium	Quarantine: Successful	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar::95...	Tactics	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	Tactics	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...	Tactics	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	Tactics	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...	Tactics	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

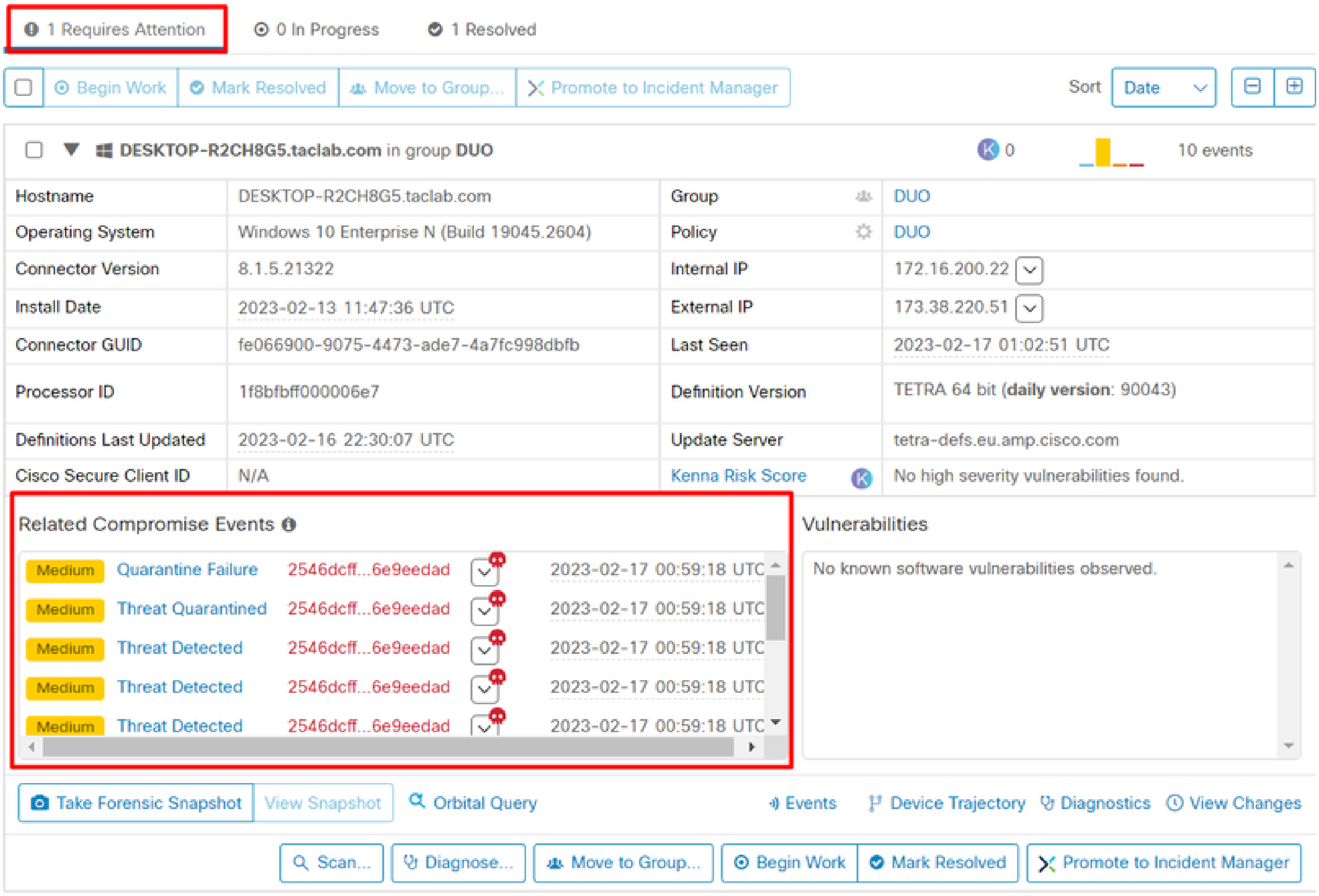
Anche il rilevamento del malware è presente nel computer, ma ciò significa che gli endpoint vengono considerati analizzati con la valutazione di Cisco Secure EndPoint su Inbox.

Nota: per inviare un endpoint alla valutazione, è necessario che vengano rilevati più artefatti o uno strano comportamento che ne attivi alcuni Indicators of Compromise nell'endpoint.

Nell'ambito Dashboard, fare clic su **Inbox**.



Ora avete una macchina che richiede attenzione.



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

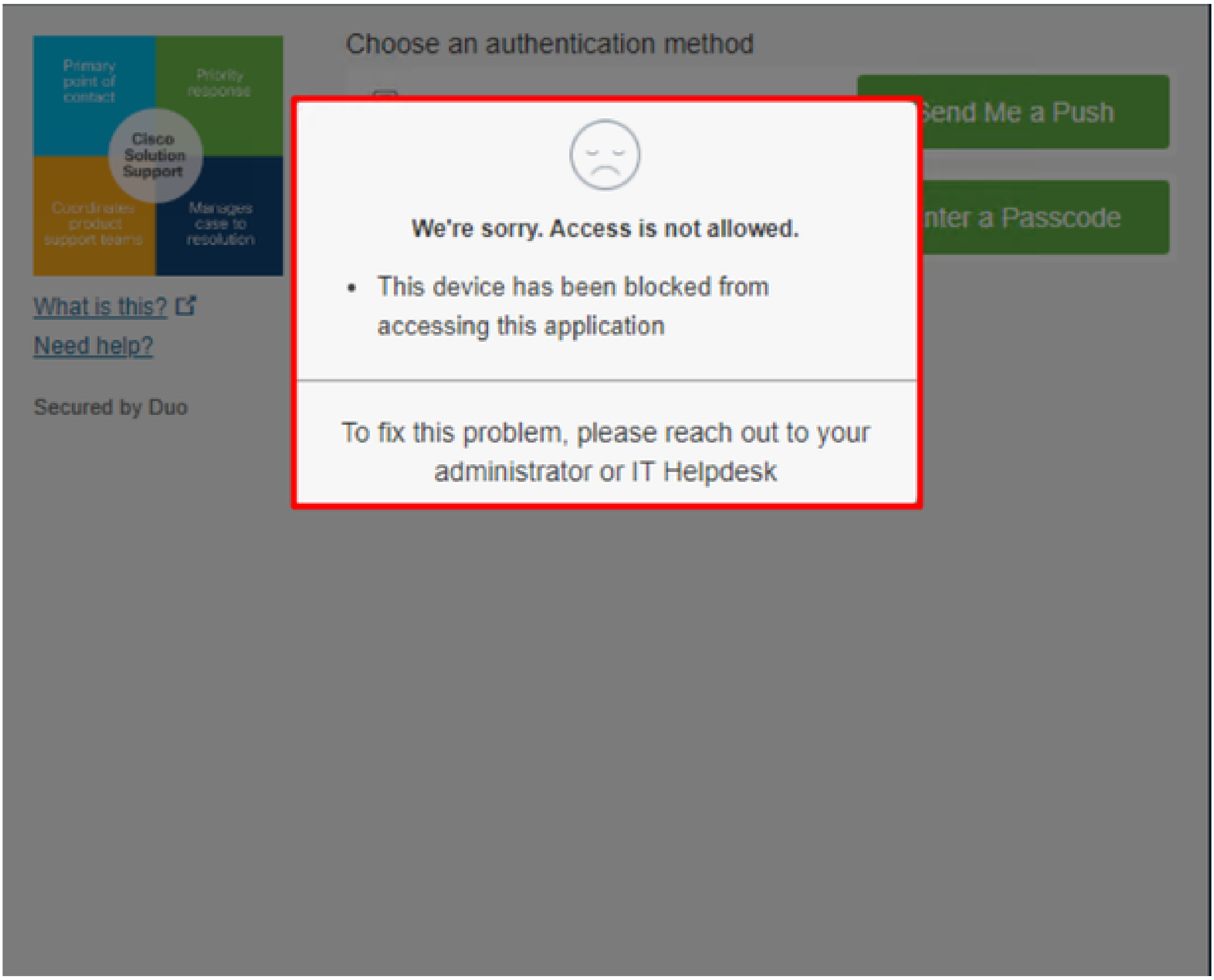
Medium	Quarantine Failure	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Quarantined	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC

Vulnerabilities

No known software vulnerabilities observed.

Ora, passate a Duo e vedete di che stato si tratta.

L'autenticazione viene tentata per prima per verificare il comportamento dopo che il computer è stato inserito nell'endpoint sicuro Cisco in Require Attention.

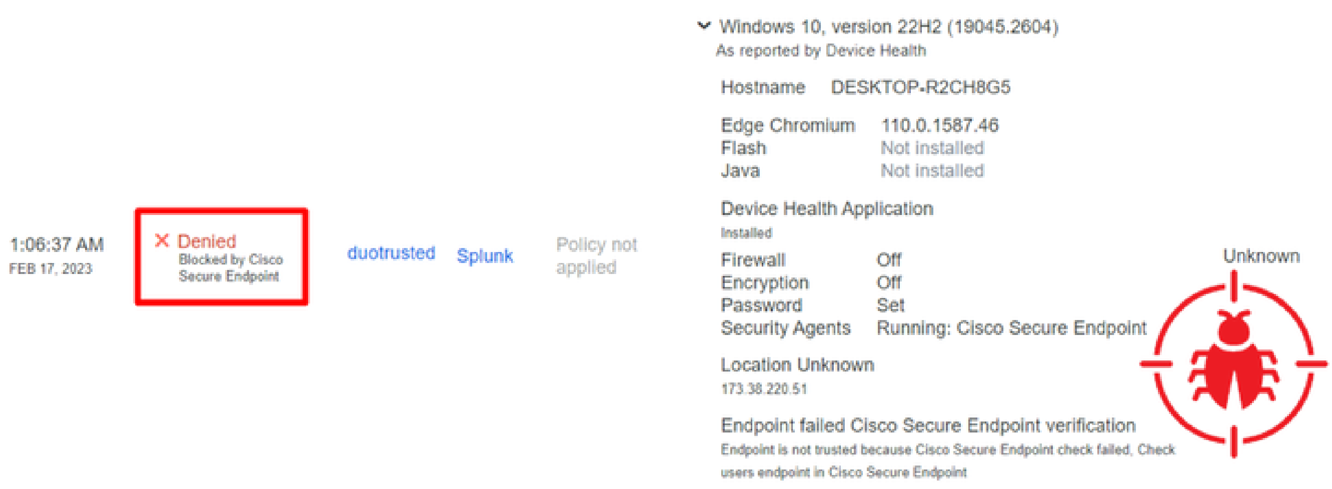

Choose an authentication method

We're sorry. Access is not allowed.

- This device has been blocked from accessing this application

To fix this problem, please reach out to your administrator or IT Helpdesk

Questa è la modalità di modifica in Duo e di visualizzazione dell'evento in eventi di autenticazione.


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

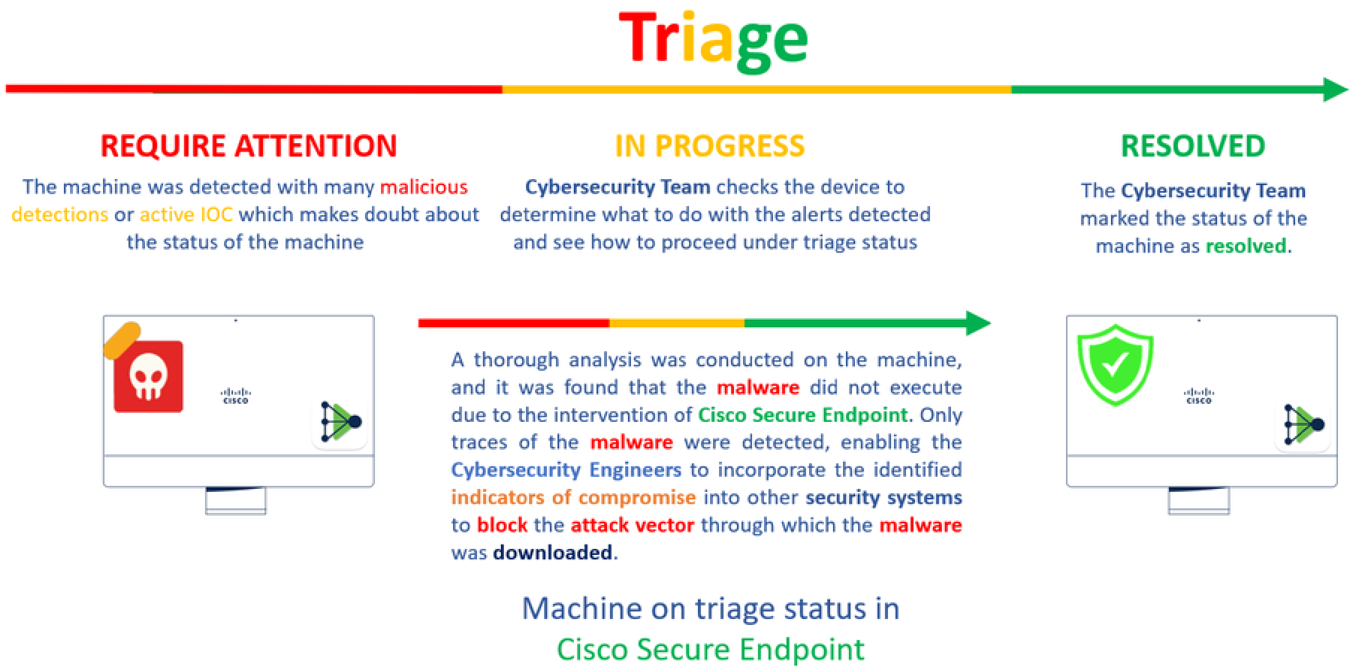
Firewall Off
Encryption Off
Password Set
Security Agents Running: Cisco Secure Endpoint

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

Il computer non è stato rilevato come dispositivo di sicurezza per l'organizzazione.

Autorizza l'accesso a un computer dopo la revisione



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

RESOLVED

The **Cybersecurity Team** marked the status of the machine as **resolved**.

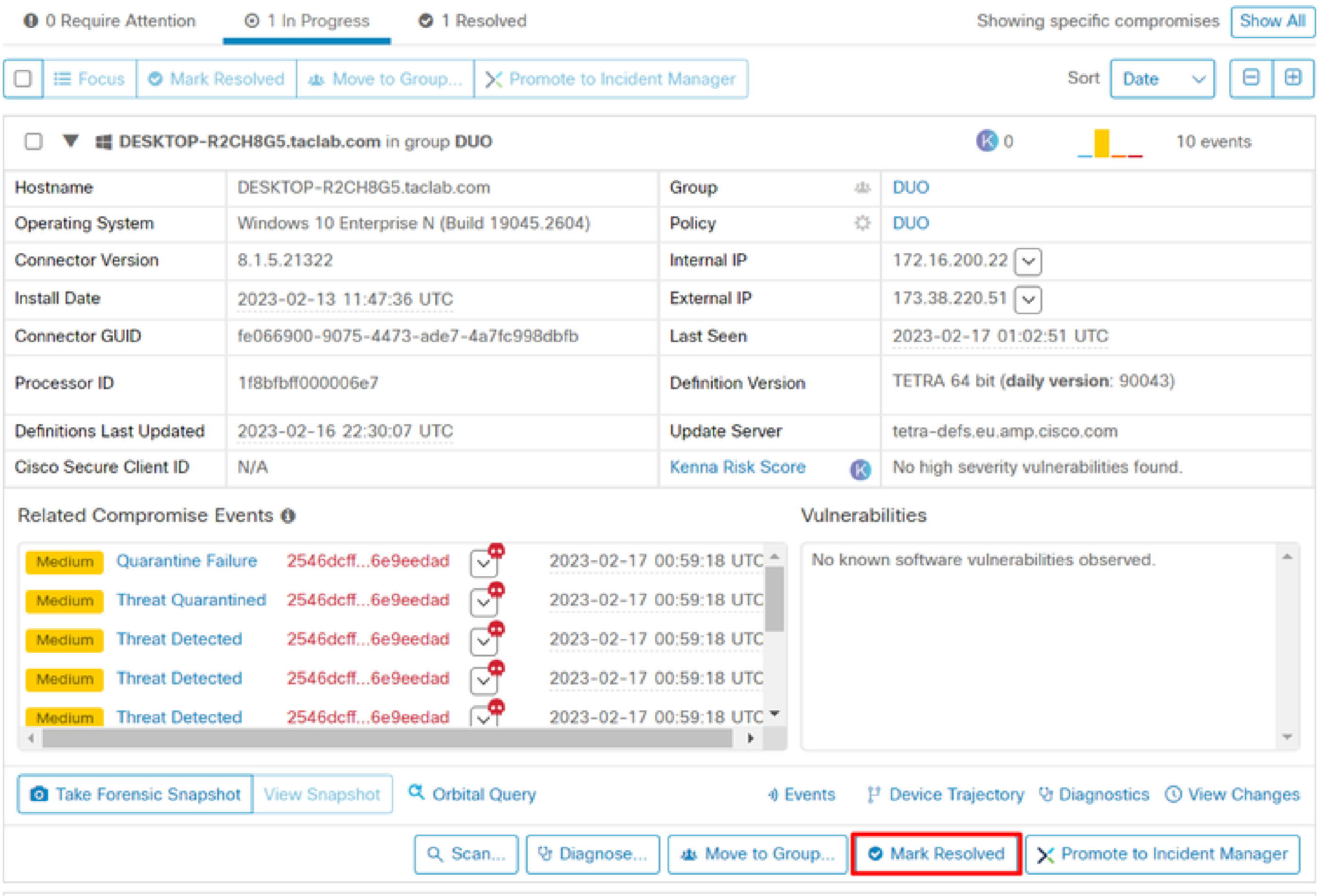
A thorough analysis was conducted on the machine, and it was found that the **malware** did not execute due to the intervention of **Cisco Secure Endpoint**. Only traces of the **malware** were detected, enabling the **Cybersecurity Engineers** to incorporate the identified **indicators of compromise** into other **security systems** to **block** the **attack vector** through which the **malware** was **downloaded**.

Machine on triage status in
Cisco Secure Endpoint

Dopo la verifica in Cisco Secure EndPoint e da parte dell'esperto di cybersicurezza, puoi consentire l'accesso a questo computer per la tua app in Duo.

Ora la domanda è come permettere di nuovo l'accesso all'app protetta da Duo.

È necessario passare a Cisco Secure EndPoint e nella Inbox, contrassegna il dispositivo come **resolved** per consentire l'accesso all'applicazione protetta da Duo.



☐ ▼ 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.

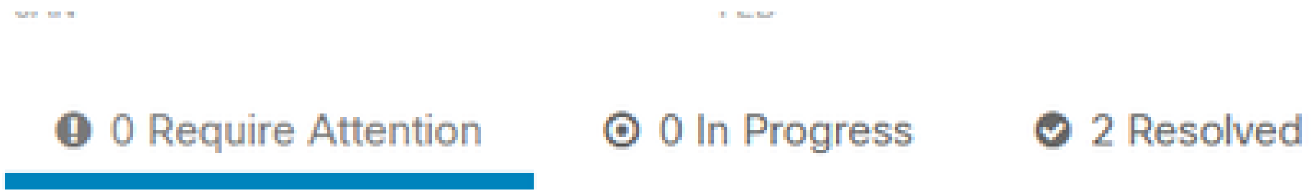
Related Compromise Events

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.

In seguito, non si dispone della macchina con lo stato attention required. È stato modificato in resolved stato.

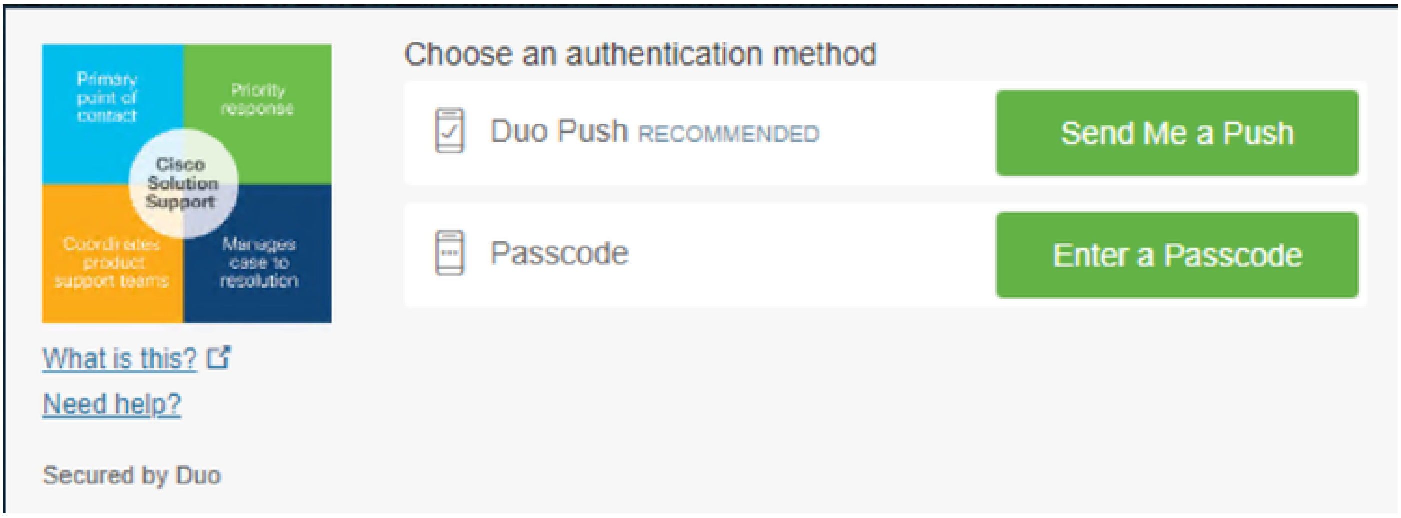


0 Require Attention

0 In Progress

2 Resolved

In poche parole, ora sei pronto a testare di nuovo l'accesso alla nostra applicazione protetta da Duo.



What is this?

Need help?

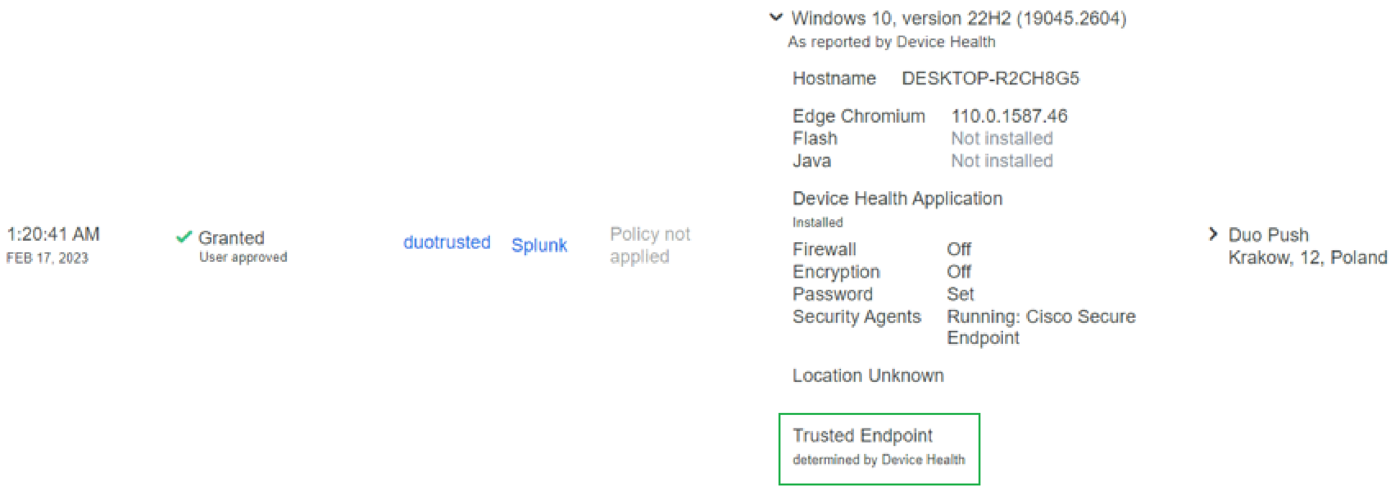
Secured by Duo

Choose an authentication method

Duo Push RECOMMENDED — Send Me a Push

Passcode — Enter a Passcode

Ora hai l'autorizzazione per inviare il push a Duo e hai eseguito l'accesso all'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

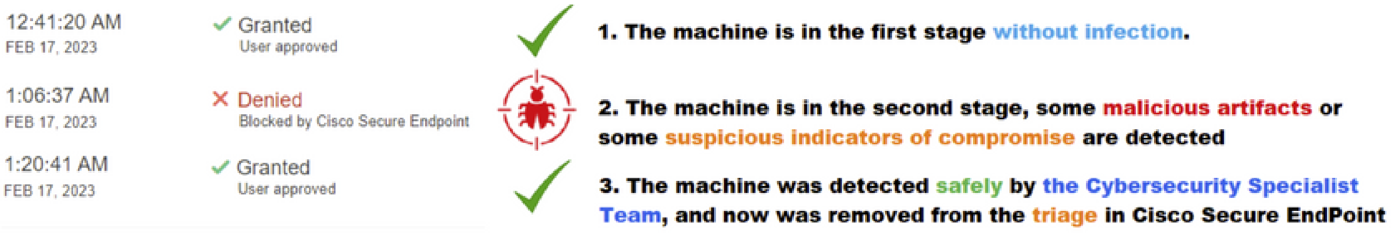
Firewall Off
Encryption Off
Password Set
Security Agents Running: Cisco Secure Endpoint

Location Unknown

Trusted Endpoint
determined by Device Health

Duo Push
Krakow, 12, Poland

Flusso di lavoro triage



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