

ةنمآلا ةياهنلا ةطقنو Duo نيوكت تاديدهتلل ةباجتسالل

تايوتحمل

[ةمدقملا](#)

[ةيساسأ تامولعم](#)

[ةيساسألا تابلطتملا](#)

[مادختسال او نيوكتلا ةلج](#)

[يئانثلال يف لمكتلا نيوكت](#)

[Cisco Secure EndPoint يف لمكتلا نيوكت](#)

[Duo يف تاسايسلا نيوكت](#)

[وب قووم زامج فاشتكال جهنلا نيوكت](#)

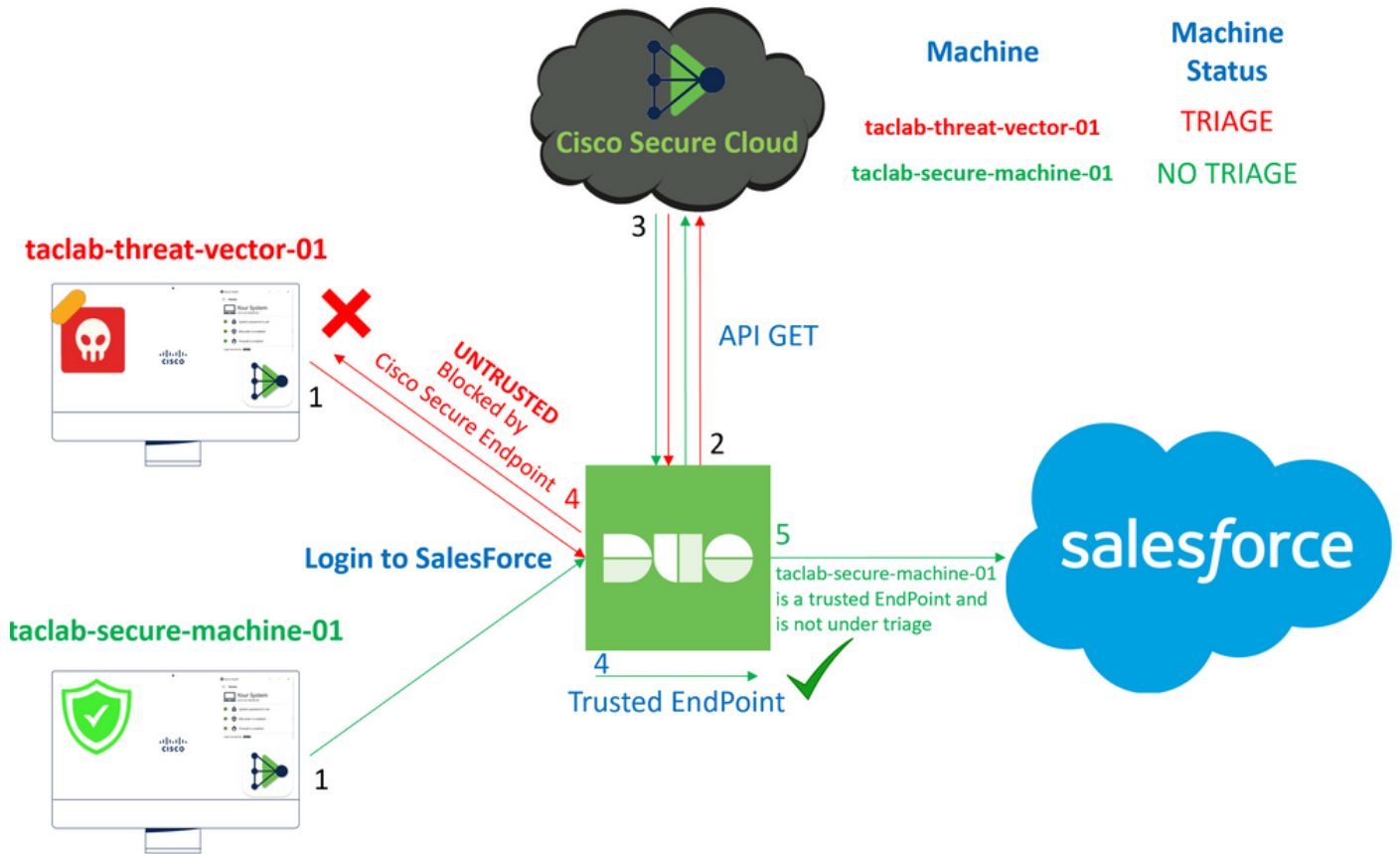
[اب قووملا ةزوجلابلتخا](#)

[Cisco Secure EndPoint جهن نيوكت](#)

[Cisco Secure EndPoint مادختساب اب قووملا ةزوجلابلتخا](#)

[ةعجارملا دعب زاهجلا لىلا لوصولابلتخا](#)

ةمدقملا




Cisco Secure EndPoint عم قووملا ةيئانثلال ةياهنلا طاقن جم ةيفيكن دنتمسلا اذه حضوي.

ةيساسأ تامولعم

ةباجتسالال في لالعفلل نواعتللاب Duo و Cisco Secure EndPoint نيب لماكلتلل حمسي جمدللا اذه قيقحت متي و. اهب قووثوملا ةكبشلا ةزهجالىل ع اهنع فشكلا متي تللا تاديدهتلل ضع بنمضتت و. زاهج لكل ةماتلا ةيقووثوملا ددحت يتلا ةزهجالا ةرادلا ةددعتم تاودأ لالخنم يلي ام تاوداللا هذه:

- ةمدخ لاجم تامدخ Active Directory
- زاهجال ةياعم عم Active Directory ةمدخ
- زاهجال ةحص عم ماع
- زاهجال ةحص عم Intune
- زاهجال ةياعم عم JAMF Pro
- ةرادلا ةعومجم LANDESK
- ةسسؤملا لوصأ ةرادلا ةادأ Mac OS X
- زاهجال ةياعم عم ليلد
- زاهجال ةياعم عم Windows Enterprise Asset Management ةادأ
- زاهجال ةياعم عم لولألا لمعلا ةحاسم

Duo و Cisco Secure EndPoint جم دنكمملا نم، ةزهجالا ةرادلا ةادأ مادختساب ةزهجالا جم دنم درجمب يئانث لكشب ةبسانملا ةسايسلل نيوكت بجي، كلذ دعبو. Administration Panel في API ةطساوب فلتلل ضرعتت دق يتلا ةزهجالا فاشتك او اهب قووثوملا ةزهجالا نم ققحتلا ةيلمع ذيفنتل Duo ةطساوب ةيحمملا تاقيبطلل لىل ع رثوت نأ نكمي يتلاو.

 ةطخالم Active Directory و Device Health عم لمعن، ةلجاللا هذه في: ةطخالم.

ةيساساللا تابلطتملا

- لماكلتلا ءارجلا Active Directory ةمدخ.
- Active Directory لاجم في كتزهجال ليحست بجي، اهب قووثوملا ةياهنلا طاقن عم Duo جم دل.
- نمآ لكشب هليوخت و اهتامدخو ةكبشلا دراوم لىل لوصولا ةقداصمب Duo ل حمسي اذهو.
- ةطخال جراح يئانثلا.

مادختسالالاو نيوكتلا ةلح

يئانثلا في لماكلتلا نيوكت

لىل لقتن Admin Panel لىل لوخدلا ليحست:

- **Trusted EndPoints > Add Integration**
- Active Directory Domain Services دي دحت

Add Management Tools Integration

222 days left

Device Management Tools Endpoint Detection & Response Systems

Management Tools



Active Directory Domain Services

Windows

Add

| [Read the Documentation](#)

Active Directory and Device Health. نيوكتل كهيجوت ةداعإ متت ،كلذ دعب

لإحمالا يف تالآلا عم طقف لمعي اذه نأ رابتعإلا نيغب ذخ

PowerShell: يف يلاتلا رمألا ليغشتب مقو Active Directory ةمدخى لإلقنتنا

```
(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> |
```

ةظفاحلا لىلإ Active Directory ب صاخلا نامألا فرعم خسنب تمق كنأ نم دكأت ،كلذ دعب

لاثم

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

زاهجلا ةحص جم دو Active Directory يف اذه مدختسي

Windows



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

1. Login to the domain controller to which endpoints are joined
2. Open PowerShell
3. Execute the following command, then retrieve the domain Security Identifier (SID) from your clipboard

After running the command, the domain SID will be copied to your clipboard. The SID is used to know if your user's computer is joined to the domain controller.

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

Copy

4. Paste the domain SID

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

Cisco Secure EndPoint. مع لم اكتب لا كنكمي نل ف، ال او. Activate for all. لم اكتب لا نيكم تو Save رقنا

Change Integration Status

Once this integration is activated, Duo will start reporting your devices as trusted or not trusted on the [endpoints page](#) and the [device insight page](#).



Integration is active

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



Test with a group

Select a group



See Duo's documentation on [how to create a desired testing environment](#)



Activate for all

Save

Trusted EndPoints > Select Endpoint Detection & Response System > Add this integration. الى لاقتنال



Cisco Secure Endpoint

Add this integration

Note

Cisco Secure Endpoint requires one of the following device management tools to be enabled:

- Active Directory Domain Services
- Active Directory with Device Health
- Generic with Device Health
- Intune with Device Health
- Jamf Pro with Device Health
- LANDESK Management Suite
- Mac OS X Enterprise Asset Management Tool
- Manual with Device Health
- Windows Enterprise Asset Management Tool
- Workspace ONE with Device Health


We integrated this in the previous steps

Cisco Secure EndPoint ل لم ا ك ت ل ا ن م ة س ي ئ ر ل ا ة ح ف ص ل ا ي ف ت ن ا ن آ ل ا

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.

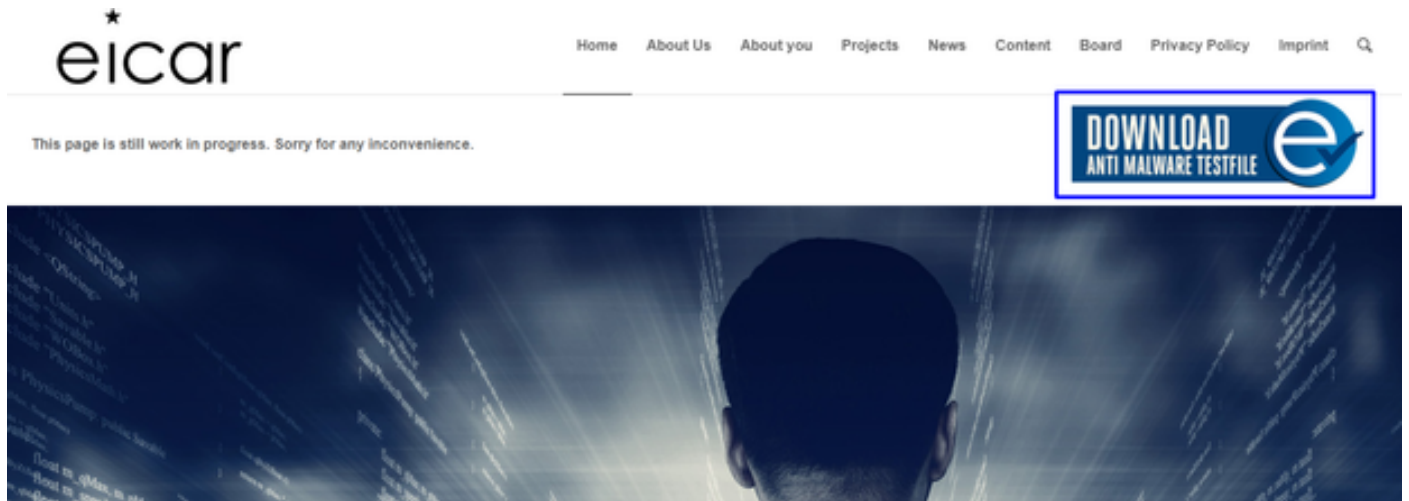
Hostname

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

[Test Integration](#)

ىل لوصول كنكمي ،ةزيملا رابتخال EICAR ىل لاثم مادختسا ةلواحمل
<https://www.eicar.org/>، ةراض ةنيع ليزنتو.

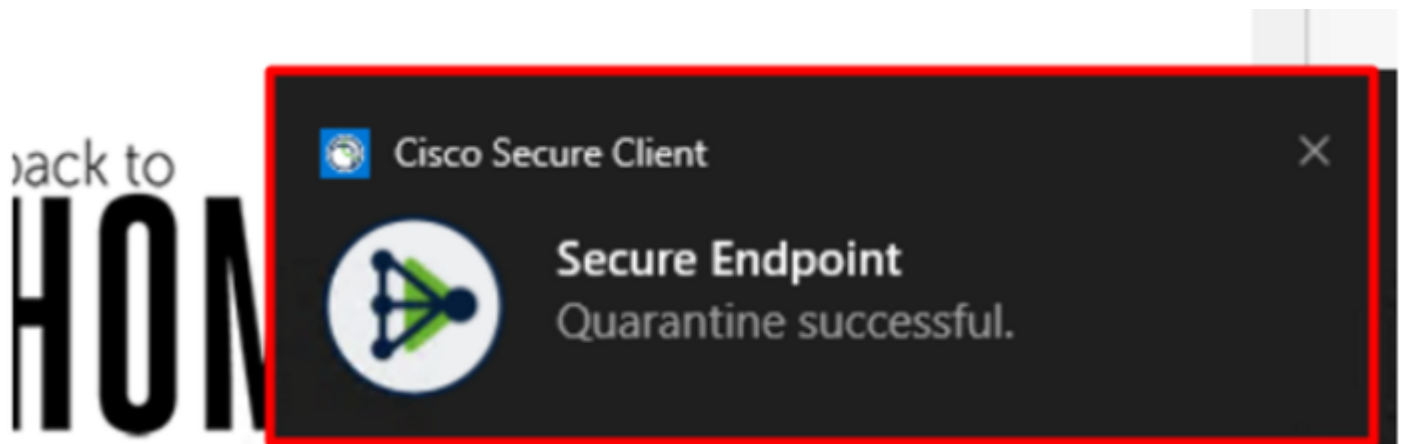
رابتخال فلم طقف وهو ،نمآ هنا ،اذه EICAR رابتخال ليزنت كنكمي .قلقت ال :ةظحال



رابتخال فلم ليزنتب مقو مسقلا ىل لقتناو لفسأل ريرمتلاب مق

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

لزعلا ىل اهلقنو ةراضلا جماربال فاشتكاب Cisco Secure EndPoint موقت



Cisco Secure EndPoint ةرادا ةحول في حضورم وه امك ،اهب ريغتت يتلا ةقيرطال يه هذو

▶ 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.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Quarantine: Failed	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar:95.sbx.tg	Medium				Threat Detected	2023-02-17 00:59:18 UTC
▶ DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar:95.sbx.tg	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

طاقن رابتعإ متي هنأ ينعي اذه نكلو، زاهجال في ةراضلا جماربلا فاشتكأ اضيأ كيدل Inbox. لعل Cisco Secure EndPoint زرف لفسأ اهليلحت متيل ةياهنلا

وأ جئاتنلل تافاشتكأ ةدع هيدل نوكي نأ مزلي، زرفلا لىإ ةياهن ةطقن لاسرال: ةظحال م ةياهنلا ةطقن في Indicators of Compromise ضعب طيشنتب موقوي بي رغ كولس

Inbox. في رقنا، Dashboard تحت



Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

Refresh All Auto-Refresh ▾ ?

هابتنالا بلطتت ةلأ كيدل نألا

1 Requires Attention 0 In Progress 1 Resolved

Begin Work Mark Resolved Move to Group... Promote to Incident Manager Sort Date

DESKTOP-R2CH8G5.taclab.com in group DUO 0 10 events

Hostname	DESKTOP-R2CH8G5.taclab.com	Group	DUO
Operating System	Windows 10 Enterprise N (Build 19045.2604)	Policy	DUO
Connector Version	8.1.5.21322	Internal IP	172.16.200.22
Install Date	2023-02-13 11:47:36 UTC	External IP	173.38.220.51
Connector GUID	fe066900-9075-4473-ade7-4a7fc998dbfb	Last Seen	2023-02-17 01:02:51 UTC
Processor ID	1f8bfbff000006e7	Definition Version	TETRA 64 bit (daily version: 90043)
Definitions Last Updated	2023-02-16 22:30:07 UTC	Update Server	tetra-defs.eu.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

Related Compromise Events

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

Vulnerabilities

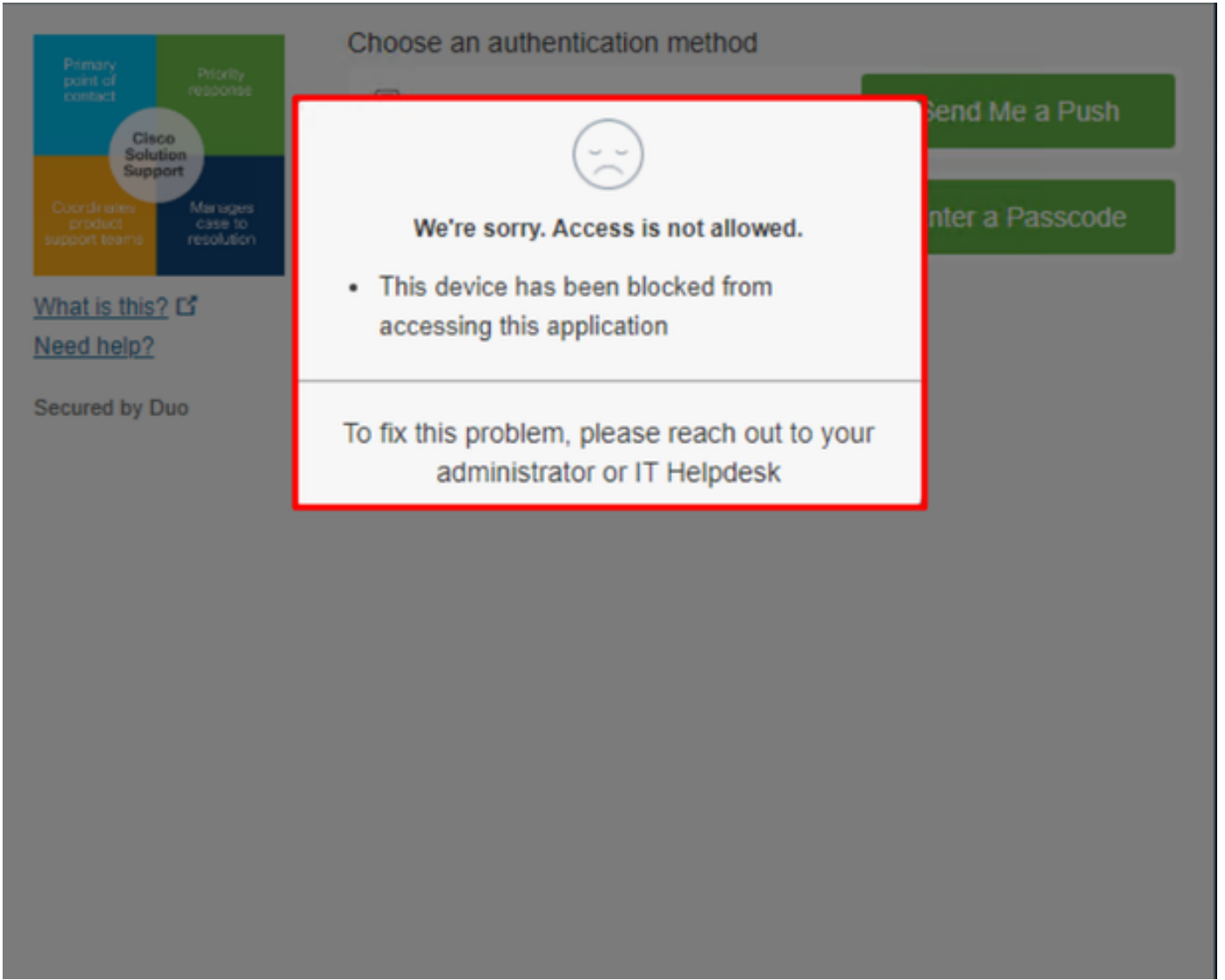
No known software vulnerabilities observed.

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

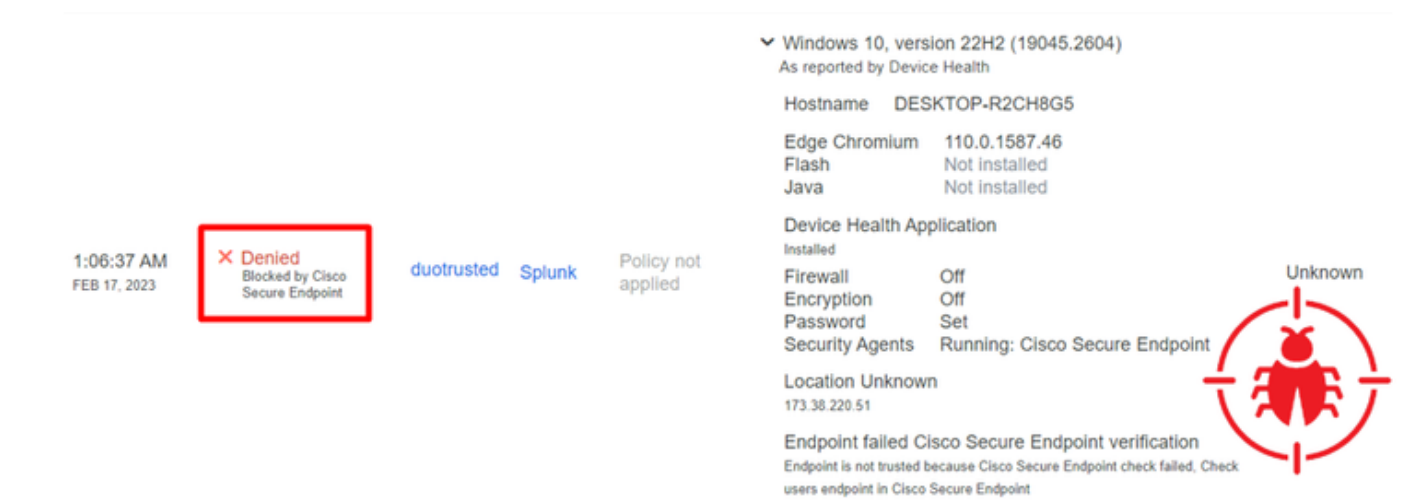
Scan... Diagnose... Move to Group... Begin Work Mark Resolved Promote to Incident Manager

ةلأجل إه ام رظناو Duo لىل لقتنا ،نألا

ةنمألا ةياهنللا ةطقن لىل ع زاوجلل عضو دعب كولسلا لىل ع اللطالل اللو ةقداصلملا ةبرجت متي
 نم Require Attention لفسأ ةدوجلل Cisco نم



ةقد اصملا ثادحأ نمض ثدحلل ضرع متي فيك و Duo في اهب ريغتت يتلا ةقيرطلا يه هذو.



ك.تسؤول نامأ زاهج سيل زاهجلا نأ فاشتكا مت.

ةعجارملا دعب زاهجلا ىلإ لوصولاب حامسلا

Triage

REQUIRE ATTENTION

The machine was detected with many **malicious detections** or **active IOC** which makes doubt about the status of the machine



IN PROGRESS

Cybersecurity Team checks the device to determine what to do with the alerts detected and see how to proceed under triage status

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

RESOLVED

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



Machine on triage status in Cisco Secure Endpoint

تنترتن إال نام أ صصختم لبق نم و Cisco Secure EndPoint بجم ب حصل ال نم ققحت ال دعب
Duo في كقيبت ال إ زاه ال اذه إ لوصولاب حامس ال ك نكم مي، كيدل

Duo ةطساوب يمحمل ال قيبطت ال إ رخأ ةرم لوصولاب حامس ال ةيفي ك وه نآلا لاؤسل او

resolved زاه ال اذه إ لعل ةمالع عضو Inbox في و ةياهن ةطقن نم أي Cisco تحت ب هذي نأ جاتحت تنأ
Duo لبق نم يمحمل ال قيبطت ال إ لوصولاب حامس ال

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


ة.الاحال resolved الى اذة ريغت .attention required. ةالاحالاب زاهجال كيدل سيل ،كلذ دعب

0 Require Attention

0 In Progress

2 Resolved

متم يتال انقيبطت الى لوصول ةينانكم رابتخال ادعتسم نآلآ تحبصأ ،تاملك عضب دعب ىرخأ ةرم Duo ةطساوب اهتياحم



Primary point of contact
Priority response
Coordinates product support teams
Manages case to resolution

Choose an authentication method

Duo Push **RECOMMENDED** Send Me a Push

Passcode Enter a Passcode

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

Secured by Duo

قيبطتال الى كلوخذ ليجست متيو ،Duo الى عفدال لاسرال نذال كيدل نآلآ

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

1:20:41 AM FEB 17, 2023 ✔ Granted User approved duotrusted Splunk Policy not applied ➤ Duo Push Krakow, 12, Poland

زرفال لمع ريس

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**

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا