

Configuration des terminaux Duo et Secure Endpoint pour répondre aux menaces

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exemple de configuration et d'utilisation](#)

[Configuration de l'intégration dans Duo](#)

[Configuration de l'intégration dans Cisco Secure EndPoint](#)

[Configuration des stratégies dans Duo](#)

[Configurer la stratégie de détection d'un périphérique approuvé](#)

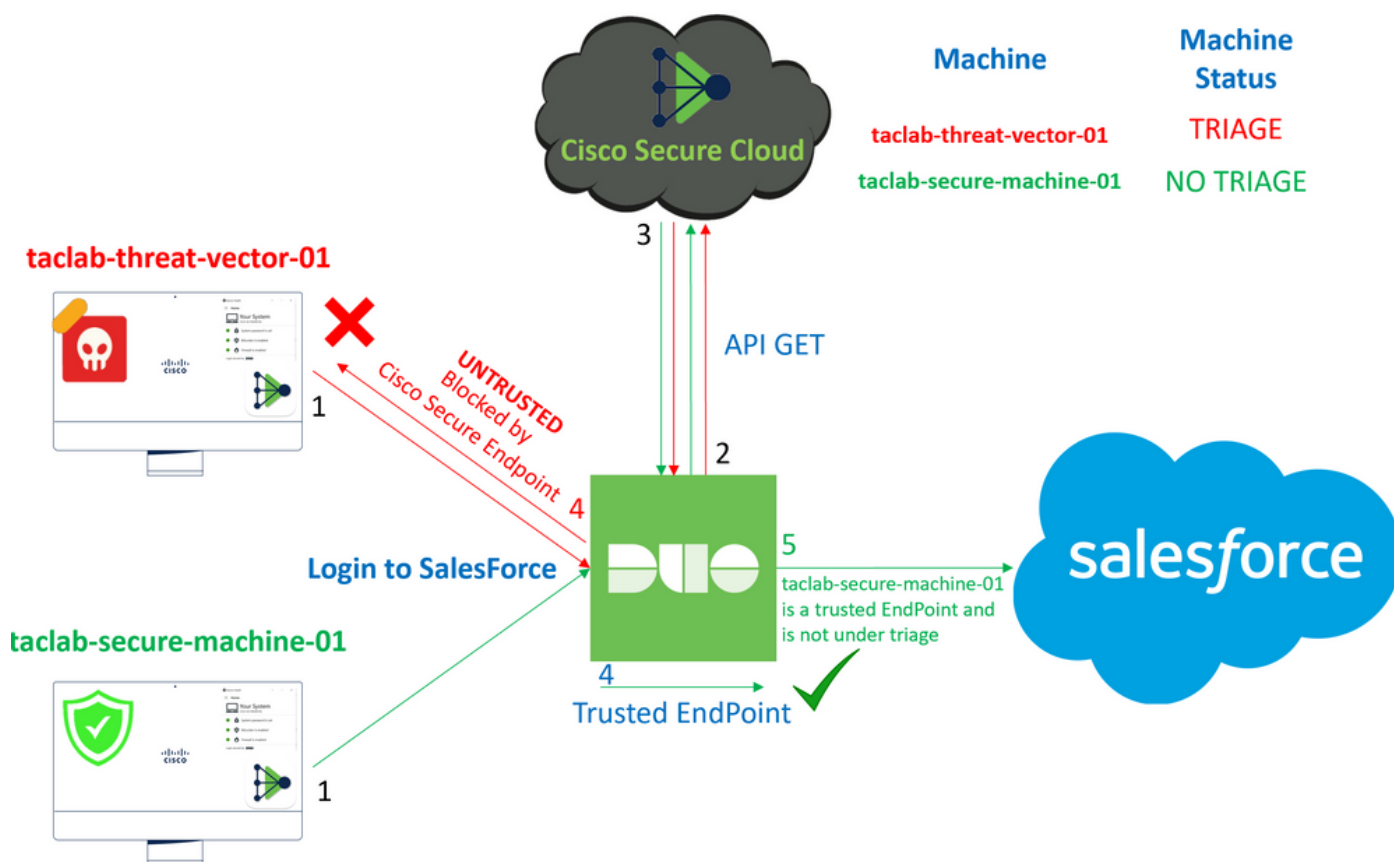
[Tester les machines de confiance](#)

[Configuration de la stratégie pour Cisco Secure EndPoint](#)

[Tester les machines de confiance avec Cisco Secure EndPoint](#)

[Autoriser l'accès à une machine après examen](#)

Introduction



Ce document décrit comment intégrer deux terminaux sécurisés avec Cisco Secure EndPoint.

Informations générales

L'intégration entre Cisco Secure EndPoint et Duo permet une collaboration efficace en réponse aux menaces détectées sur les périphériques réseau de confiance. Cette intégration est réalisée par le biais de plusieurs outils de gestion des périphériques qui établissent la fiabilité de chaque périphérique. Voici quelques-uns de ces outils :

- Active Directory Domain Services
- Active Directory avec état des périphériques
- Générique avec état du périphérique
- Intune avec l'état du périphérique
- Jamf Pro avec état des périphériques
- Suite de gestion LANDESK
- Outil de gestion des ressources d'entreprise Mac OS X
- Manuel avec état du périphérique
- Outil Windows Enterprise Asset Management
- Workspace ONE avec état du périphérique

Une fois les périphériques intégrés à un outil de gestion des périphériques, il est possible d'intégrer Cisco Secure EndPoint et Duo en API dans le Administration Panel. Par la suite, la stratégie appropriée doit être configurée dans Duo pour exécuter la vérification des périphériques approuvés et détecter les périphériques compromis pouvant affecter les applications protégées par Duo.



Remarque : dans ce cas, nous utilisons Active Directory et l'intégrité des périphériques.

Conditions préalables

- Active Directory pour effectuer l'intégration.
- Pour intégrer Duo aux terminaux approuvés, vos périphériques doivent être enregistrés dans le domaine Active Directory. Cela permet à Duo d'authentifier et d'autoriser l'accès aux ressources et services réseau en toute sécurité.
- Duo Au-Delà Du Plan.

Exemple de configuration et d'utilisation

Configuration de l'intégration dans Duo

Connectez-vous à l' Admin Panel et accédez à :

- **Trusted EndPoints > Add Integration**
- Sélectionner 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

| [Read the Documentation](#)

Après cela, vous êtes redirigé vers la configuration du **Active Directory and Device Health**.

Notez que cela ne fonctionne qu'avec les machines du domaine.

Accédez à Active Directory et exécutez la commande suivante dans 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> |
```

Après cela, assurez-vous d'avoir copié dans le Presse-papiers l'identificateur de sécurité de votre Active Directory.

Exemple

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

Il est utilisé dans l'intégration d'Active Directory et de l'intégrité des périphériques.

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

Cliquer **Save** et permettent l'intégration et **Activate for all**. Sinon, vous ne pouvez pas intégrer 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

Save

Aller à Trusted EndPoints > Select Endpoint Detection & Response System > Add this integration.



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](#)

Vous êtes maintenant sur la page principale de l'intégration de Cisco Secure EndPoint.

Cisco Secure Endpoint

222 days left

1. Generate Cisco Secure Endpoint Credentials

1. [Login to the Cisco Secure Endpoint console](#) .
2. Navigate to "Accounts > API Credentials".
3. Click "New API Credentials".
4. Give the credentials a name and make it read-only.
5. Click "Create".
6. Copy the **Client Id** and **API Key** and return to this screen.

2. Enter Cisco Secure Endpoint Credentials

Client ID

Enter Client ID from Part 1.

API key


Enter API Key from Part 1.

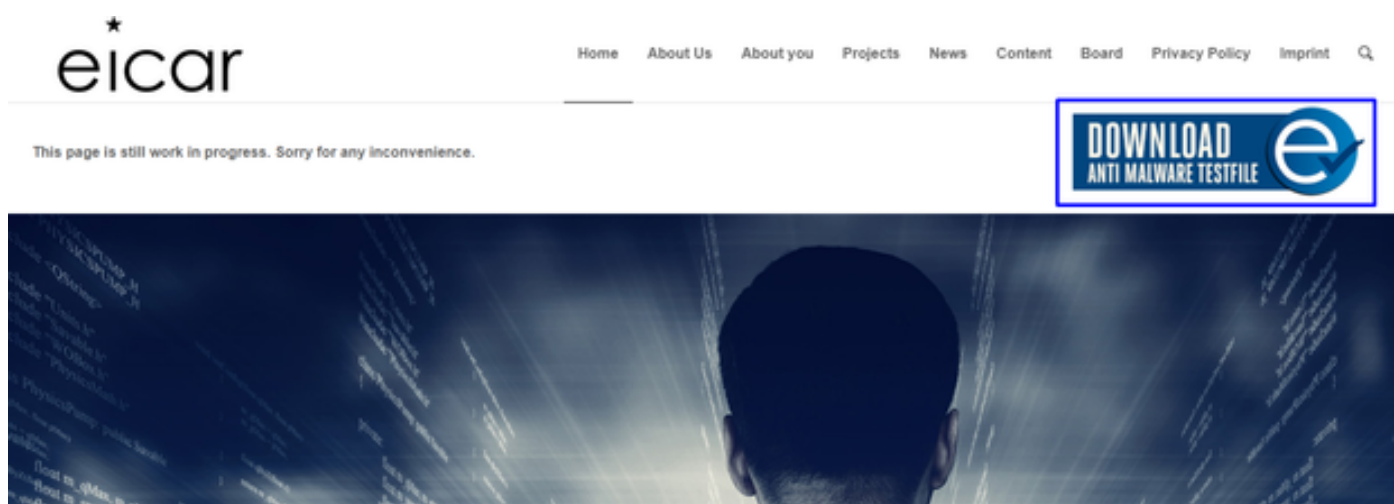
Hostname

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

[Test Integration](#)



Pour essayer avec un exemple d'EICAR pour tester la fonctionnalité, accédez à <https://www.eicar.org/>, et téléchargez un exemple malveillant.

 Remarque : Ne vous inquiétez pas. Vous pouvez télécharger ce test EICAR, il est sûr et il ne s'agit que d'un fichier de test.

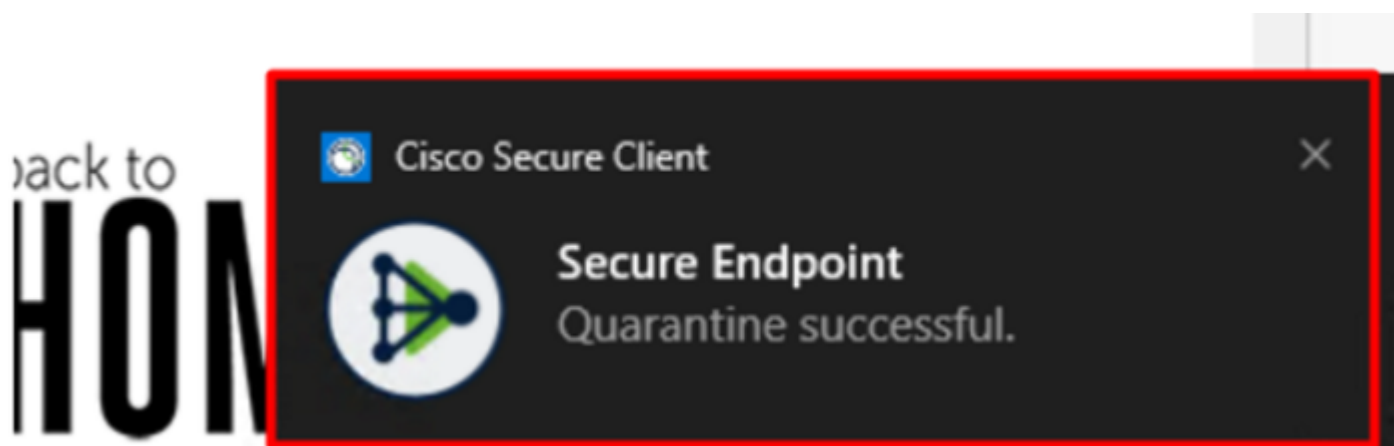


Faites défiler la page vers le bas, accédez à la section et téléchargez le fichier de test.

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 détecte le programme malveillant et le place en quarantaine.



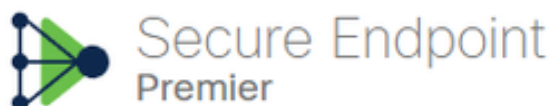
C'est ainsi qu'il change, comme indiqué dans le panneau d'administration de Cisco Secure EndPoint.

▶ 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...	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...	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...	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

Vous avez également la détection du programme malveillant dans la machine, mais cela signifie que les terminaux sont considérés comme étant analysés selon le triage de Cisco Secure EndPoint sur le Inbox.

Remarque : pour envoyer un terminal au triage, il doit avoir plusieurs détections d'artefacts ou de comportements étranges qui activent certains Indicators of Compromise dans le terminal.

Sous la Dashboard, cliquez sur l'icône Inbox.



Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

Dashboard

Dashboard **Inbox** Overview Events iOS Clarity

Refresh All

Auto-Refresh



Maintenant vous avez une machine qui demande de l'attention.

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

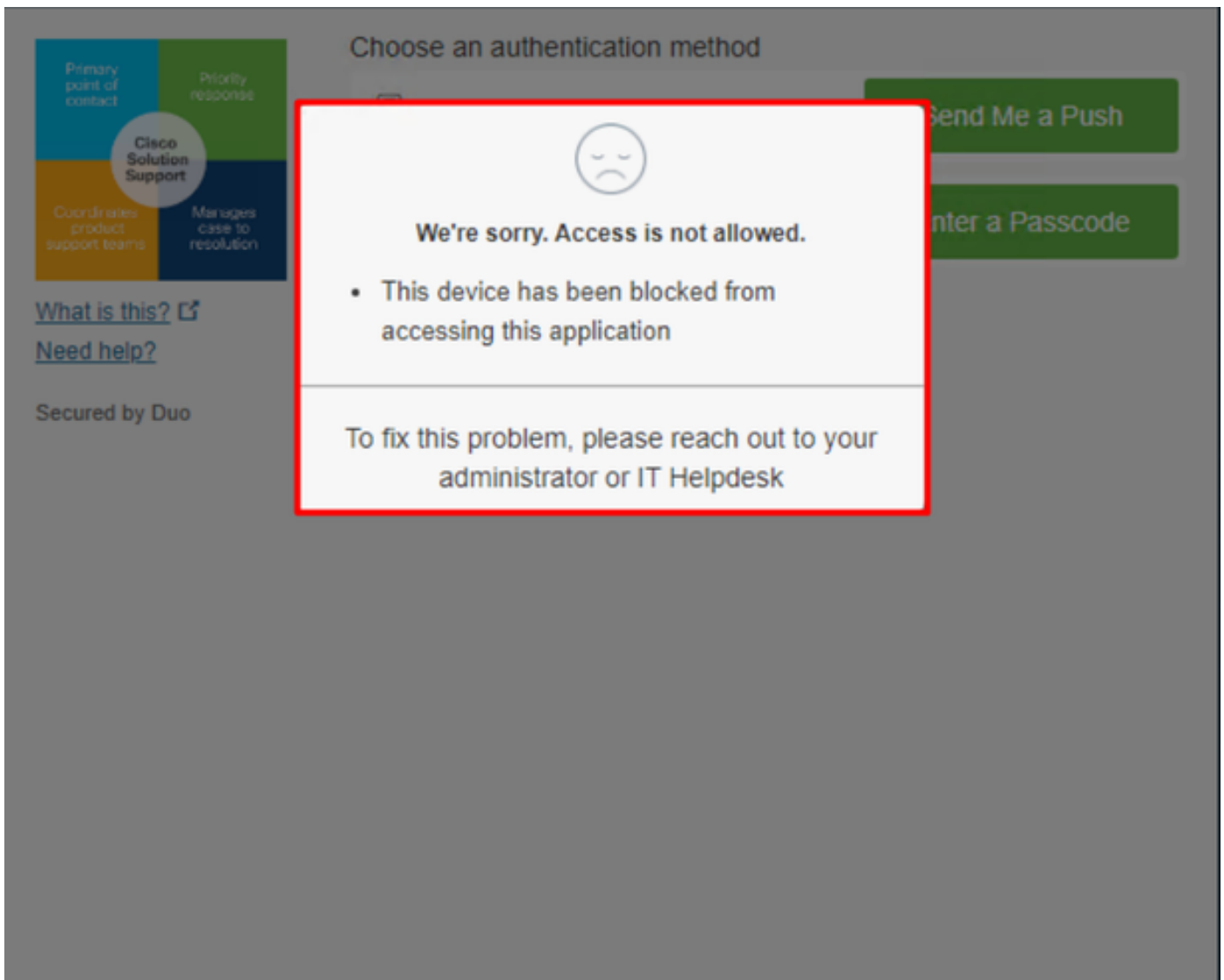
No known software vulnerabilities observed.

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

Maintenant, passez à Duo et voyez quel est l'état.

L'authentification est tentée en premier pour voir le comportement après que la machine a été placée sur le point d'extrémité sécurisé Cisco sous Require Attention.



C'est ainsi qu'il change dans Duo et que l'événement sous événements d'authentification s'affiche.

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



Votre ordinateur a été détecté comme n'étant pas un dispositif de sécurité pour votre organisation.

Autoriser l'accès à une machine après examen

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

Après vérification sous Cisco Secure EndPoint et par votre spécialiste de la cybersécurité, vous pouvez autoriser l'accès à cette machine à votre application dans Duo.

Maintenant, la question est de savoir comment autoriser à nouveau l'accès à l'application protégée par Duo.

Vous devez passer sous Cisco Secure EndPoint et dans votre Inbox, marquez ce périphérique comme **resolved** pour permettre l'accès à l'application protégée par Duo.

0 Require Attention 1 In Progress 1 Resolved Showing specific compromises [Show All](#)

Focus Mark Resolved Move to Group... Promote to Incident Manager Sort: Date

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

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

Related Compromise Events

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

Après cela, vous n'avez pas la machine avec l'état *attention required*. Cette configuration est devenue *resolved* état.

000000

000000

0 Require Attention

0 In Progress

2 Resolved

En quelques mots, vous êtes maintenant prêt à tester à nouveau l'accès à notre application protégée par Duo.

Cisco Solution Support

Primary point of contact Priority response

Coordinates product support teams Manages case to resolution

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

Secured by Duo

Choose an authentication method


Duo Push **RECOMMENDED** [Send Me a Push](#)

Passcode [Enter a Passcode](#)

Vous avez maintenant l'autorisation d'envoyer le push à Duo et vous êtes connecté à l'application.

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	> Duo Push Krakow, 12, Poland
				Trusted Endpoint determined by Device Health	

Workflow de triage

12:41:20 AM FEB 17, 2023	✔ Granted User approved		✔ 1. The machine is in the first stage without infection.
1:06:37 AM FEB 17, 2023	✘ Denied Blocked by Cisco Secure Endpoint		2. The machine is in the second stage, some malicious artifacts or some suspicious indicators of compromise are detected
1:20:41 AM FEB 17, 2023	✔ Granted User approved	✔	3. The machine was detected safely by the Cybersecurity Specialist Team, and now was removed from the triage in Cisco Secure EndPoint

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.