

Configurar Duo e endpoint seguro para responder a ameaças

Contents

[Introduction](#)

[Informações de Apoio](#)

[Prerequisites](#)

[Configuração e caso de uso](#)

[Configurar a integração no Duo](#)

[Configurar a integração no Cisco Secure EndPoint](#)

[Configurar políticas no Duo](#)

[Configure a política para detectar um dispositivo confiável](#)

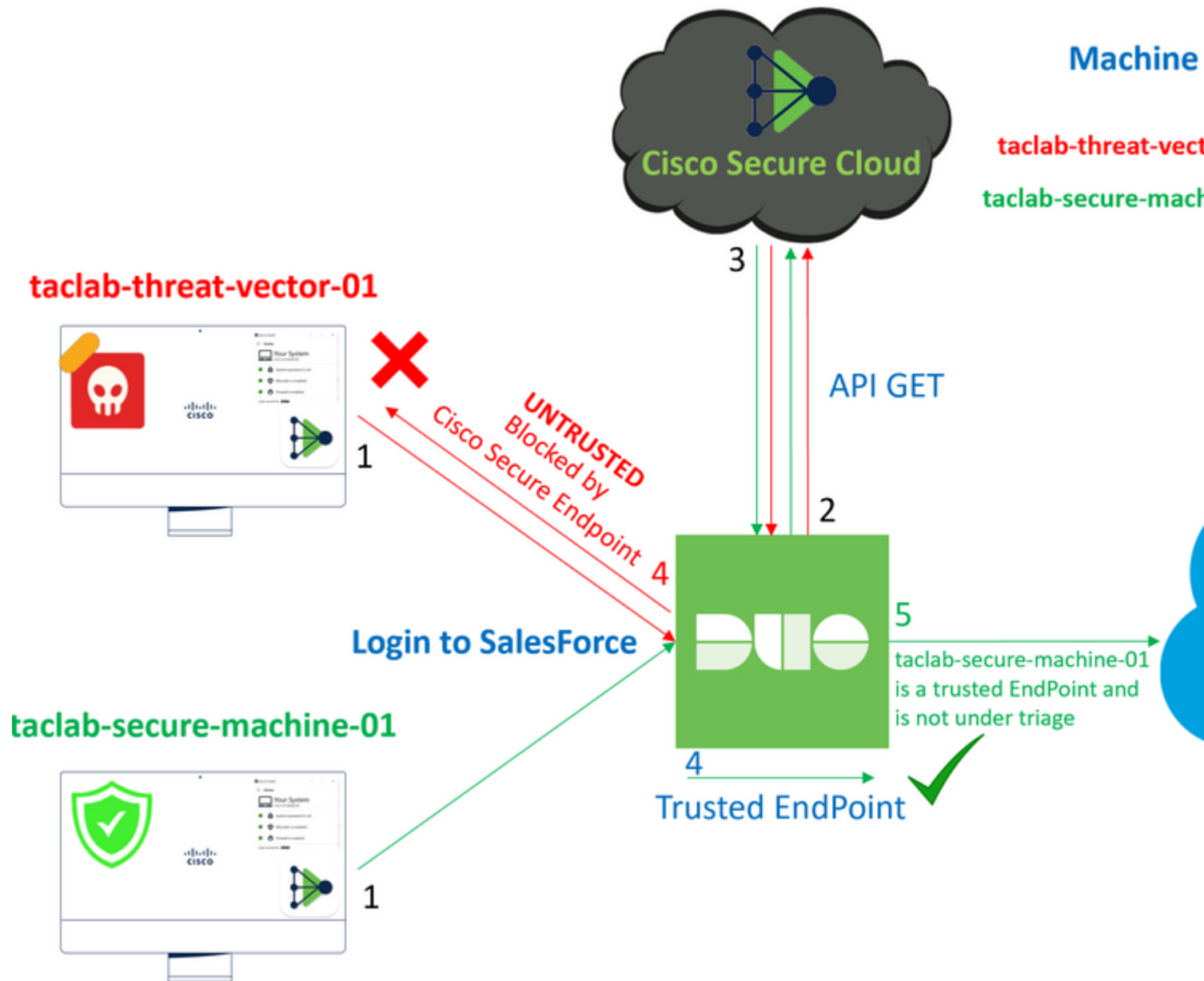
[Testar Máquinas Confiáveis](#)

[Configurar a Política para o Cisco Secure EndPoint](#)

[Teste as máquinas confiáveis com o Cisco Secure EndPoint](#)

[Permitir o acesso a uma máquina após revisão](#)

Introduction



Este documento descreve como integrar o Duo Trusted EndPoints com o Cisco Secure EndPoint.

Informações de Apoio

A integração entre o Cisco Secure EndPoint e o Duo, permite uma colaboração eficaz em resposta a ameaças detectadas em dispositivos de rede confiáveis. Essa integração é obtida através de várias ferramentas de gerenciamento de dispositivos que estabelecem a confiabilidade de cada dispositivo. Algumas dessas ferramentas incluem:

- Serviços de Domínio Ative Directory
- Ative Directory com Integridade do Dispositivo
- Genérico com Integridade do Dispositivo
- Integridade do Intune com Dispositivo
- Jamf Pro com Integridade do Dispositivo
- Pacote de gerenciamento LANDESK
- Ferramenta de gerenciamento de ativos corporativos Mac OS X
- Manual com Integridade do Dispositivo
- Ferramenta de Gerenciamento de Ativos Corporativos do Windows
- Workspace ONE com integridade de dispositivo

Depois que os dispositivos são integrados a uma ferramenta de gerenciamento de dispositivos, é possível integrar o Cisco Secure EndPoint e o Duo ao API no Administration Panel. Subsequentemente, a política apropriada deve ser configurada no Duo para executar a verificação de dispositivos confiáveis e detectar dispositivos comprometidos que possam afetar aplicativos protegidos pelo Duo.

Observação: neste caso, trabalhamos com o Active Directory e a Integridade do Dispositivo.

Prerequisites

- Active Directory para fazer a integração.
- Para integrar o Duo a endpoints confiáveis, seus dispositivos devem ser registrados no domínio do Active Directory. Isso permite que o Duo autentique e autorize o acesso aos recursos e serviços de rede com segurança.
- Duo além do plano.

Configuração e caso de uso

Configurar a integração no Duo

Efetue login no Admin Panel e vá para:

- **Trusted EndPoints > Add Integration**
- Selecionar 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

Depois disso, você será redirecionado para configurar o **Active Directory and Device Health**.

Leve em consideração que isso só funciona com máquinas no domínio.

Vá para o Active Directory e execute o próximo comando no PowerShell:

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

```
PS C:\Users\Administrator> (Get-ADDomain | Format-Table -Property DomainSID -HideTableHeaders)
PS C:\Users\Administrator> |
```

Depois disso, certifique-se de ter copiado para a área de transferência o identificador de segurança do seu Active Directory.

Exemplo

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

Isso é usado na Integração da Integridade do Active Directory e do 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

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

4. Paste the domain SID

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

Clique em **Save** e possibilitar a integração e **Activate for all**. Caso contrário, você não poderá integrar com o Cisco Secure EndPoint.

Change Integration Status

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



Integration is active

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



Test with a group

Select a group

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



Activate for all

Save

Ir para Trusted EndPoints > Select Endpoint Detection & Response System > Add this integration.



Cisco Secure Endpoint

Add this integration

Note

Cisco Secu
following d

- Activ
- Activ
- Gene
- Intur
- Jam
- LAN
- Mac
- Tool
- Man
- Winc
- Work

We integrated this in the previous steps

Agora você está na página principal da integração do 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

Depois disso, vá para a **Admin Panel** do Cisco Secure EndPoint.

Configurar a integração no Cisco Secure EndPoint

- <https://console.eu.amp.cisco.com/> LOGIN NO CONSOLE EMEAR
- <https://console.amp.cisco.com/> LOGIN NO CONSOLE AMER

E navegue até Accounts > API Credentials e selecione 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

Observação: somente Read-only é necessário para fazer essa integração porque o Duo GET consulta o Cisco Secure EndPoint para saber se o dispositivo atende aos requisitos da política.

Inserir Application Name, Scope, e Create.

< API Key Details

3rd Party API Client ID

API Key

- Copie o 3rd API Party Client ID de Cisco Secure EndPoint para Duo Admin Panel in Client ID.
- Copie o API Key de Cisco Secure EndPoint para 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

Teste a integração e, se tudo funcionar bem, clique em **Save** para salvar a integração.

Configurar políticas no Duo

Para configurar as políticas para sua integração, você passa pelo aplicativo:

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

Name	Type	Application Policy	Group Policies
Splunk	Splunk	TrustedEndPoint	

Configure a política para detectar um dispositivo confiável

The screenshot shows the configuration page for a Duo policy named "Deny Access to unenrc". The left sidebar lists categories: Users (New User policy, Authentication policy, User location) and Devices (Trusted Endpoints, Device Health application, Remembered devices, Operating systems, Browsers, Plugins). The "Trusted Endpoints" section is active, showing a description and three radio button options: "Allow all endpoints", "Require endpoints to be trusted" (selected and highlighted with a blue box), and "Allow Cisco Secure Endpoint to block compromised endpoints". A note states that the selected option only applies to trusted endpoints. A link for "Advanced options for mobile endpoints" is visible at the bottom.


Testar Máquinas Confiáveis

Computador com Integridade de Dispositivo Duo e ingressou no domínio

Timestamp (UTC) ▾	Result	User	Application	Trust Assessment i	Access Device
11:36:04 PM FEB 16, 2023	✔ Granted User approved	duotrusted	Splunk	Policy not applied	<p>Windows 10, version 22H2 (19045) As reported by Device Health</p> <p>Hostname DESKTOP-R2CH8G</p> <p>Edge Chromium 110.0.1587.46 Flash Not installed Java Not installed</p> <p>Device Health Application Installed</p> <p>Firewall Off Encryption Off Password Set Security Agents Running: Cisco Endpoint</p> <p>Location Unknown 173.38.220.51</p> <p>Trusted Endpoint determined by Device Health</p>

Computador fora do domínio sem Integridade de Dispositivo Duo

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.

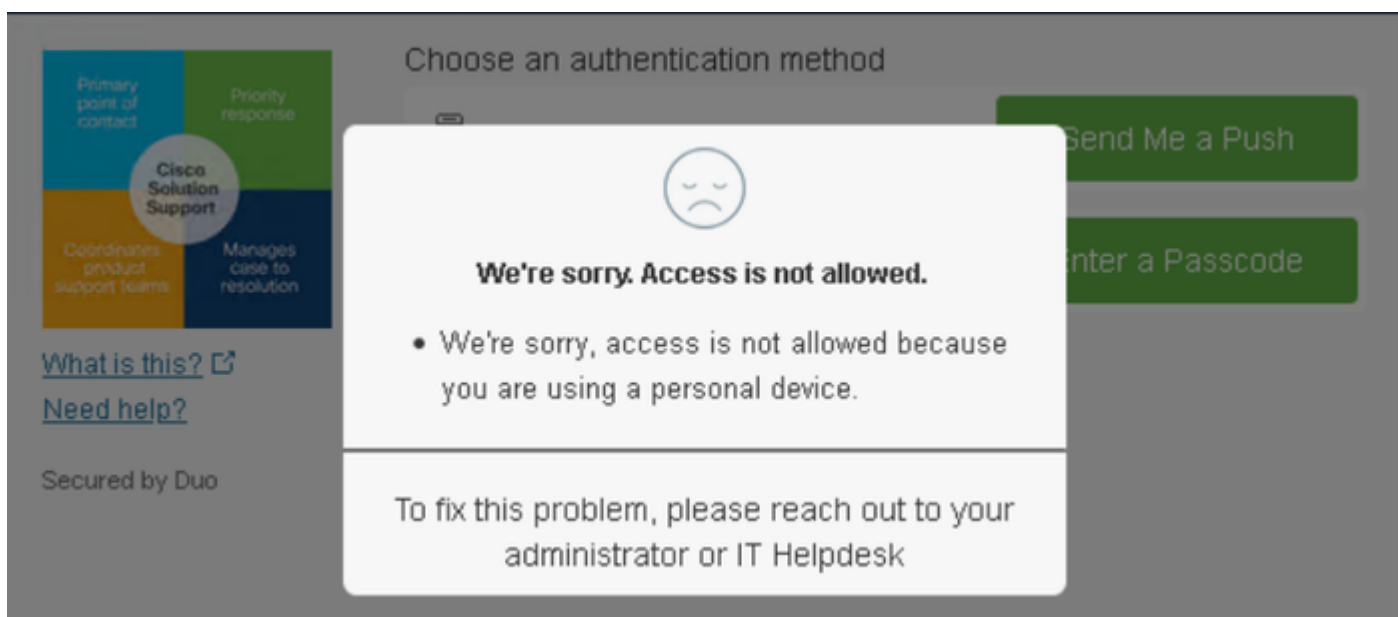
Download now
 or
 Already have the app installed?
[Launch the app](#)

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

Secured by Duo

Computador fora do domínio com Integridade de Dispositivo Duo

Timestamp (UTC) ▾	Result	User	Application	Trust Assessment 1	Access Device
11:40:58 PM FEB 16, 2023	✗ Denied Endpoint is not trusted	duotrusted	Splunk	Policy not applied	Windows 10, version 22H2 (19045.2604) As reported by Device Health Hostname NODOMAIN Firefox 89.0 Flash Not installed Java Not installed Device Health Application Installed Firewall Off Encryption Off Password Set Security Agents Running: Cisco Secure Endpoint Almere Stad, FL, Netherlands 64.103.36.133 Not a Trusted Endpoint <small>determined by Device Health</small>



Configurar a Política para o Cisco Secure EndPoint

Nessa configuração de política, configure o dispositivo já confiável para atender aos requisitos sobre ameaças que podem afetar seu aplicativo, caso um dispositivo seja infectado ou se alguns comportamentos marcarem essa máquina com **suspicious artifacts** OR Indicators of Compromise, você pode bloquear o acesso da máquina aos aplicativos protegidos.

- 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](#)

Teste as máquinas confiáveis com o Cisco Secure EndPoint

Máquina sem o Cisco Secure Agent instalado

Nesse caso, a máquina pode ser aprovada sem a verificação do AMP.

12:52:23 PM
FEB 20, 2023

✔ **Granted**
User approved

duotrusted Splunk Policy not applied

Windows 10, version 21H1 (19045.2604)
As reported by Device Health

Hostname COMPUTER24

Edge Chromium 110.0.1587.62
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

Se desejar ter uma política restritiva, você poderá configurá-la para ser mais restritiva se modificar a Device Health Application política de **Reporting** para **Enforcing**.

E adicionar Block Access if an EndPoint Security Agent is not running.

Don't require users to have the app ⓘ

Allow users to install the app during enrollment

Require users to have the app ⓘ

Block access if firewall is off.

Block access if BitLocker is off.

Block access if system password is not set.

Block access if an endpoint security agent is not running.

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

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

× Cisco Secure Endpoint × ▾

Computador sem infecção

Com uma máquina, sem infecção, você pode testar como o Duo com Cisco Secure EndPoint funciona para trocar informações sobre o status da máquina e como os eventos são mostrados nesse caso no Duo e no Cisco Secure EndPoint.

Se você verificar o status da sua máquina no Cisco Secure EndPoint:

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

Quando você filtra sua máquina, pode ver o evento disso e, nesse caso, pode determinar se a sua máquina está limpa.

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	1f8bfbff0000006e7	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

Você pode ver que não há detecção para o seu dispositivo, e também está em um status de limpo, o que significa que sua máquina não está em triagem para participar.

▶	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		

É assim que o Duo classifica essa máquina:

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>

A máquina mantém o trusted rótulo.

O que acontece se a mesma máquina for infectada por um Malicious Actor, tiver tentativas repetitivas de infecção, ou Indicators of Compromise alertas sobre esta máquina?

Computador com infecção

Para tentar usar um exemplo de **EICAR** para testar o recurso, acesse <https://www.eicar.org/> e faça download de uma amostra mal-intencionada.

Nota: Não se preocupe. Você pode fazer o download do teste EICAR, ele é seguro e é apenas um arquivo de teste.

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

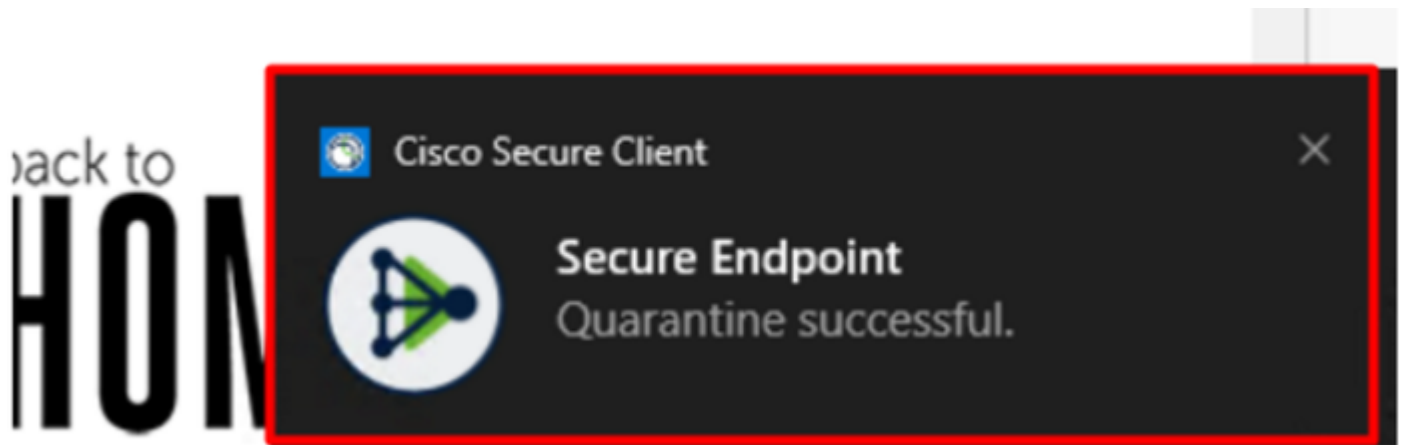


Role para baixo e vá até a seção e baixe o arquivo de teste.

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	
---------------------------------------	---	--	---	--	---

O Cisco Secure EndPoint detecta o malware e o coloca em quarentena.



É assim que ele muda, como mostrado no painel Cisco Secure EndPoint Admin.

▶	DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar::95.sbx.tg	Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar::95.sbx.tg	Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar::95...	Tactics Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar::95.sbx.tg	Tactics Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar::95.sbx.tg	Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected a7bea0f0-88d0-4113-aba4-3696d10e98e8.tmp as Win.Ransomware.Eicar::95...	Tactics Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar::95.sbx.tg	Tactics Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar::95...	Tactics Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 677327.crdownload as Win.Ransomware.Eicar::95.sbx.tg	Medium			
▶	DESKTOP-R2CH8G5.taclab.com detected c57863dd-1603-4f85-b512-d62b84160bc0.tmp as Win.Ransomware.Eicar::95.sbx.tg	Medium			

Você também tem a detecção do malware na máquina, mas isso significa que os endpoints são considerados para análise sob a triagem do Cisco Secure EndPoint no Inbox.

Observação: para enviar um endpoint para triagem, ele precisa ter várias detecções de artefatos ou comportamentos estranhos que ativam alguns Indicators of Compromise no endpoint.

Sob o comando Dashboard, clique no botão **Inbox**.



Secure Endpoint
Premier

Dashboard

Analysis ▾

Outbreak Control ▾

Management ▾

Accounts ▾

Dashboard

Dashboard

Inbox

Overview

Events

iOS Clarity

Refresh All

Auto-Refresh



Agora você tem uma máquina que requer atenção.

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	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

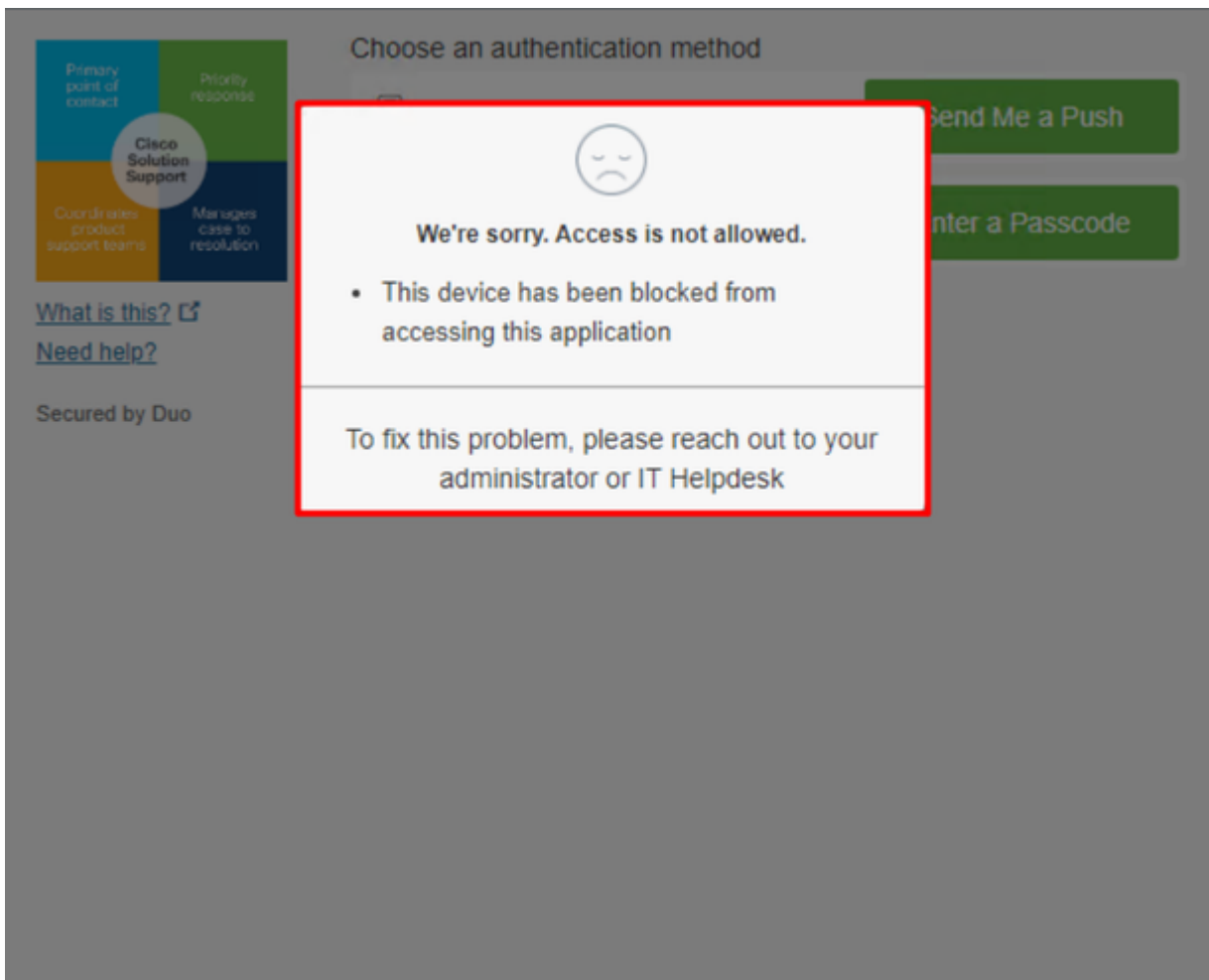
No known software vulnerabilities observed.

Take Forensic Snapshot View Snapshot Orbital Query Events Device Trajectory Diagnostics

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

Agora, mude para Duo e veja qual é o status.

A autenticação é tentada primeiro para ver o comportamento depois que a máquina foi colocada no Cisco Secure EndPoint em Require Attention.



É assim que ele muda no Duo e como o evento sob eventos de autenticação é mostrado.

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



Seu computador foi detectado como não sendo um dispositivo de segurança para sua organização.

Permitir o acesso a uma máquina após revisão

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

Após a verificação no Cisco Secure EndPoint e por seu especialista em segurança cibernética, você pode permitir acesso a esta máquina para seu aplicativo no Duo.

Agora, a questão é como permitir o acesso novamente ao aplicativo protegido pelo Duo.

Você precisa entrar no Cisco Secure EndPoint e em sua Inbox, marque este dispositivo como **resolved** para permitir o acesso ao aplicativo protegido pelo 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

Depois disso, você não tem a máquina com o status attention required. Isso mudou para resolved status.

0 Require Attention 0 In Progress 2 Resolved

Em poucas palavras, agora você está preparado para testar novamente o acesso ao nosso aplicativo protegido pelo Duo.

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

Agora você tem permissão para enviar o envio por push para o Duo e está conectado ao aplicativo.

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

Fluxo de Trabalho de Triagem

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**

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.