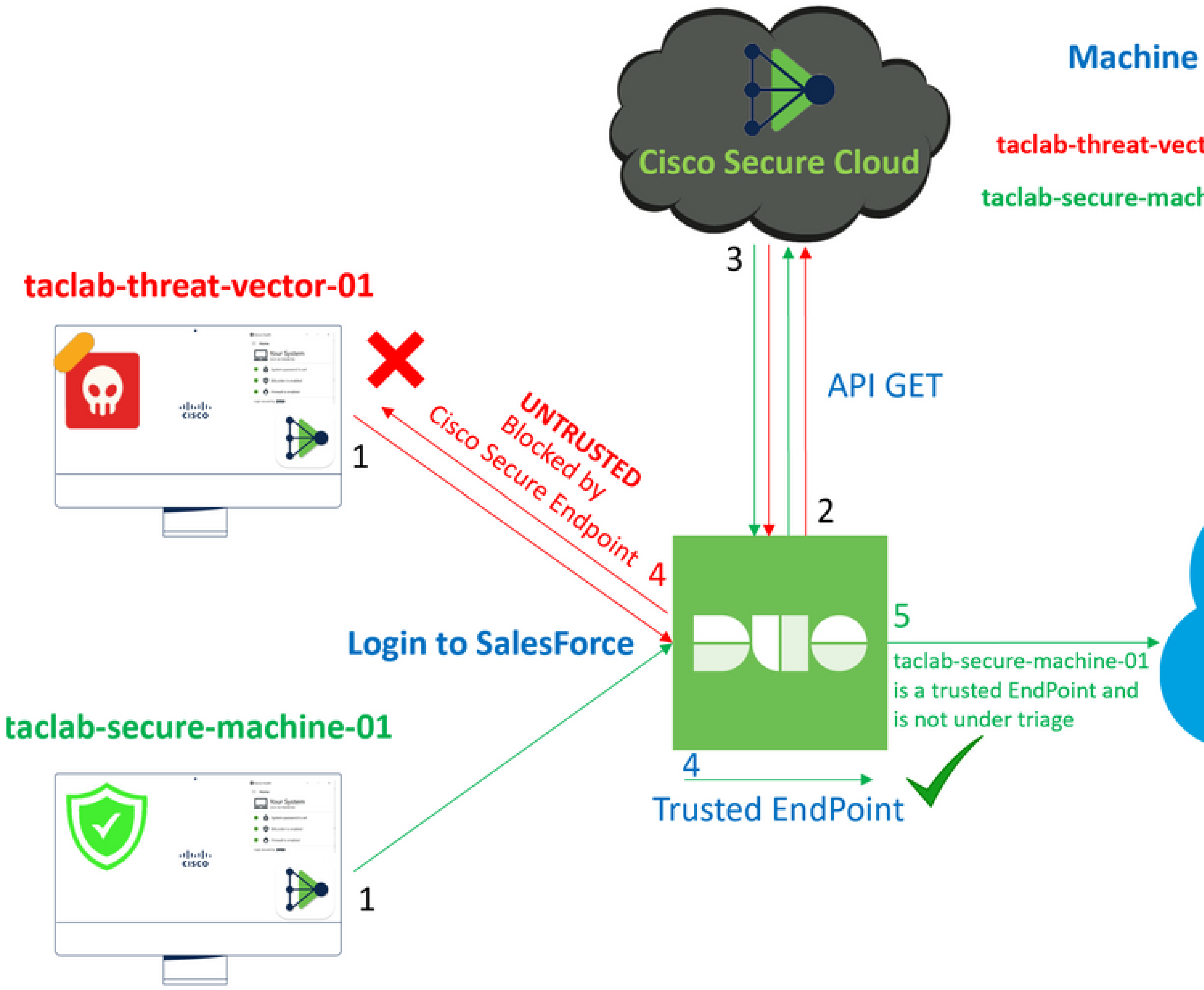
Configure Duo and Secure Endpoint to Respond to Threats

Contents

Introduction



This document describes how to integrate Duo Trusted EndPoints with Cisco Secure EndPoint.

Background Information

The integration between Cisco Secure EndPoint and Duo, allows for effective collaboration in response to threats detected on trusted network devices. This integration is achieved through multiple device management tools that establish the reliability of each device. Some of these tools include:

- 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

Once devices are integrated with a device management tool, it is possible to integrate Cisco Secure EndPoint and Duo by API in the Administration Panel. Subsequently, the appropriate policy must be configured in Duo to execute trusted device verification and detect compromised devices that can affect applications protected by Duo.

> **Note**: In this case, we work with Active Directory and Device Health.

Prerequisites

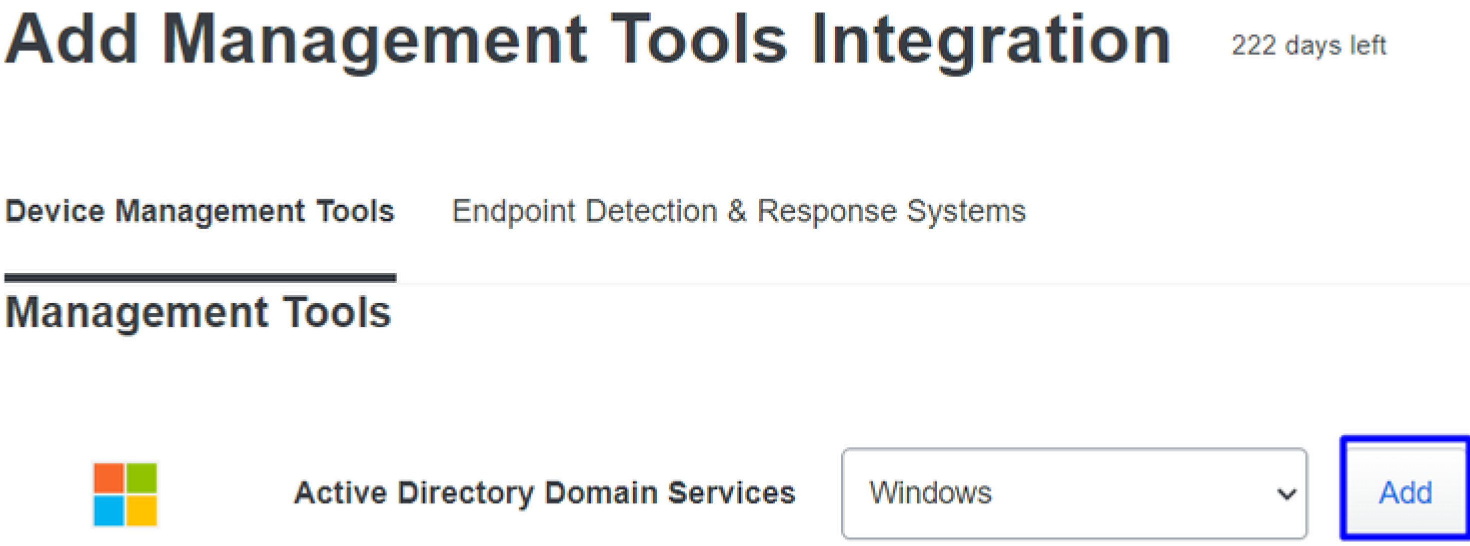
- Active Directory to make the integration.
- To integrate Duo with Trusted Endpoints, your devices must be registered in the Active Directory domain. This allows Duo to authenticate and authorize access to network resources and services securely.
- Duo Beyond Plan.

Configuration and Use Case

Configure the Integration in Duo

Log in to the **Admin Panel** and go to:

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

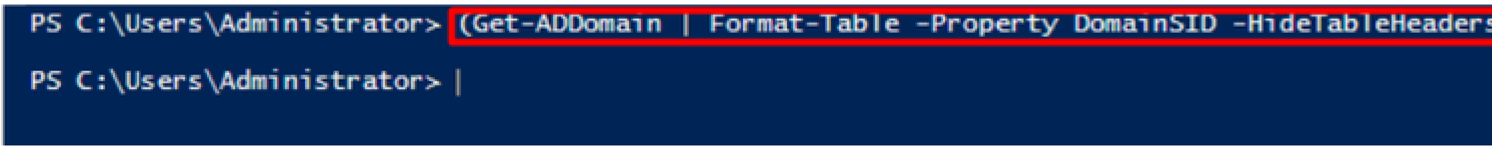

Add Management Tools Integration
222 days left
Device Management Tools
Endpoint Detection & Response Systems
Management Tools
Active Directory Domain Services
Windows
Add

After that, you are redirected to configure the **Active Directory and Device Health.**

Take into count that this only works with machines in the domain.

Go to the active directory and run the next command in PowerShell:

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



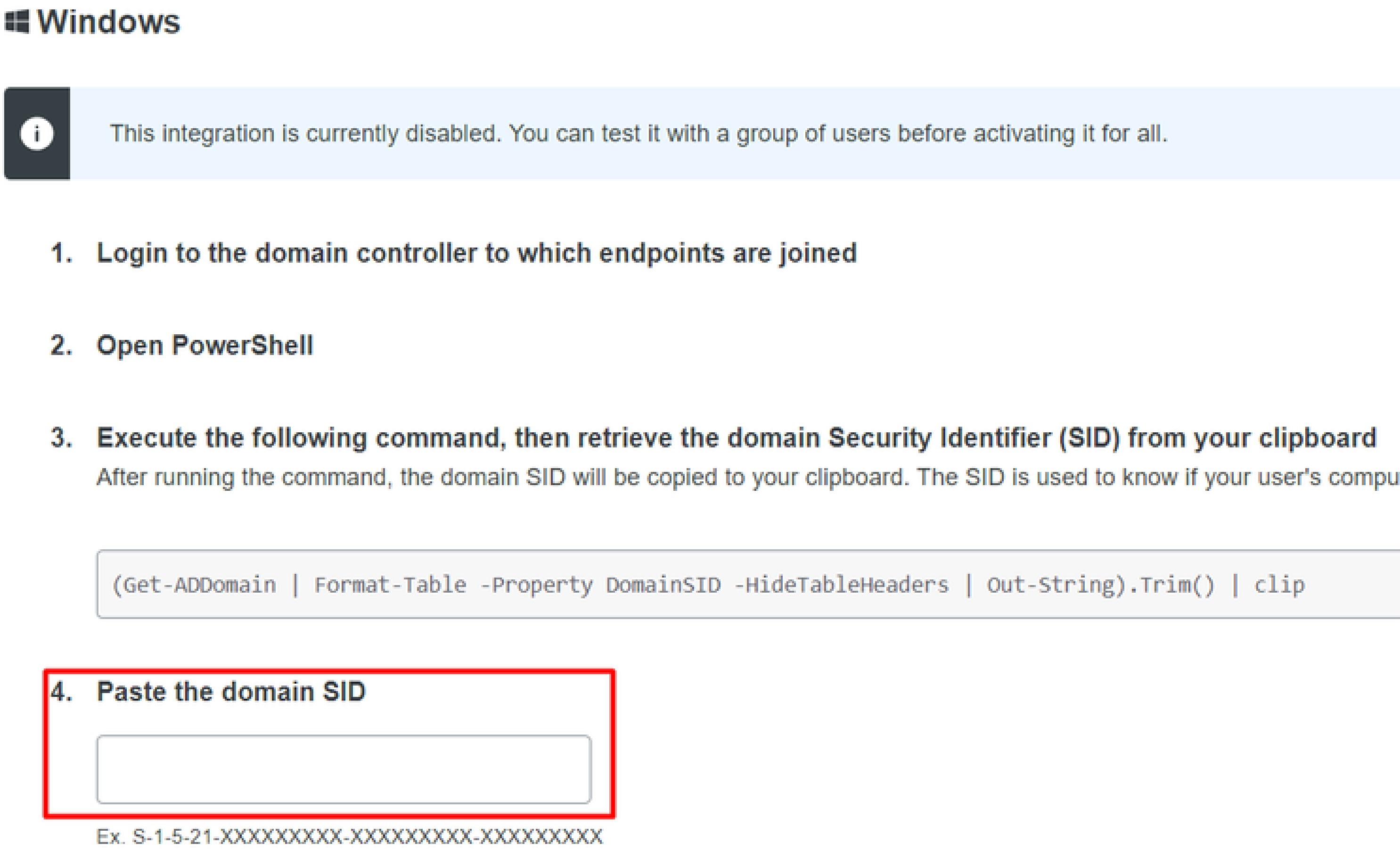
```
PS C:\Users\Administrator> (Get-ADDomain | Format-Table -Property DomainSID -HideTableHeaders
PS C:\Users\Administrator> |
```

After that, be sure you have copied to the clipboard the security identifier of your Active Directory.

Example

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

This is used in your Active Directory and Device Health Integration.



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

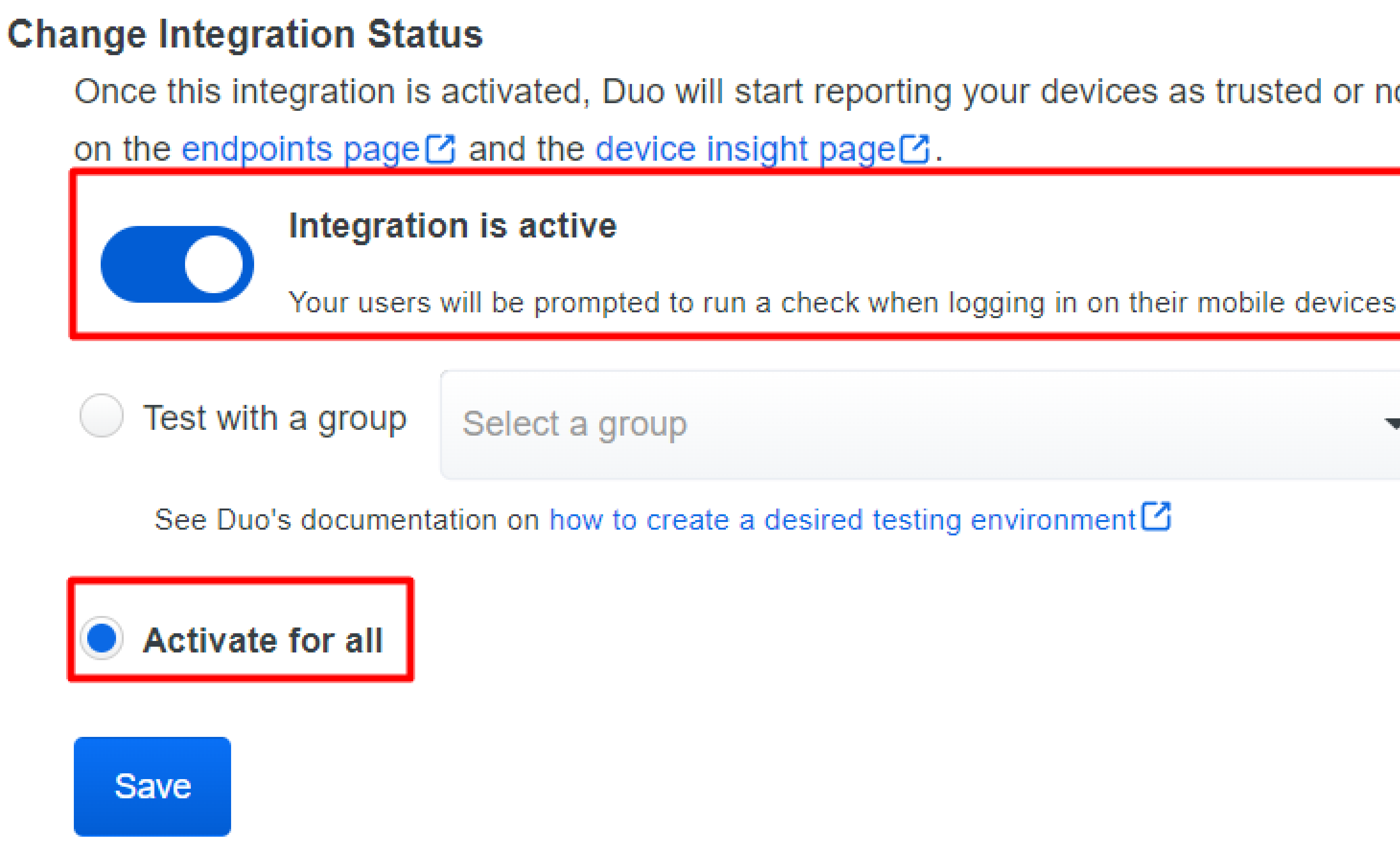
3. Execute the following command, then retrieve the domain Security Identifier (SID) from your clipboard
   After running the command, the domain SID will be copied to your clipboard. The SID is used to know if your user's compu

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

4. Paste the domain SID

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

Click **Save** and enable the integration and Activate for all. Otherwise, you cannot integrate with Cisco Secure EndPoint.



Change Integration Status

Once this integration is activated, Duo will start reporting your devices as trusted or no
on the endpoints page and the device insight page.

Integration is active

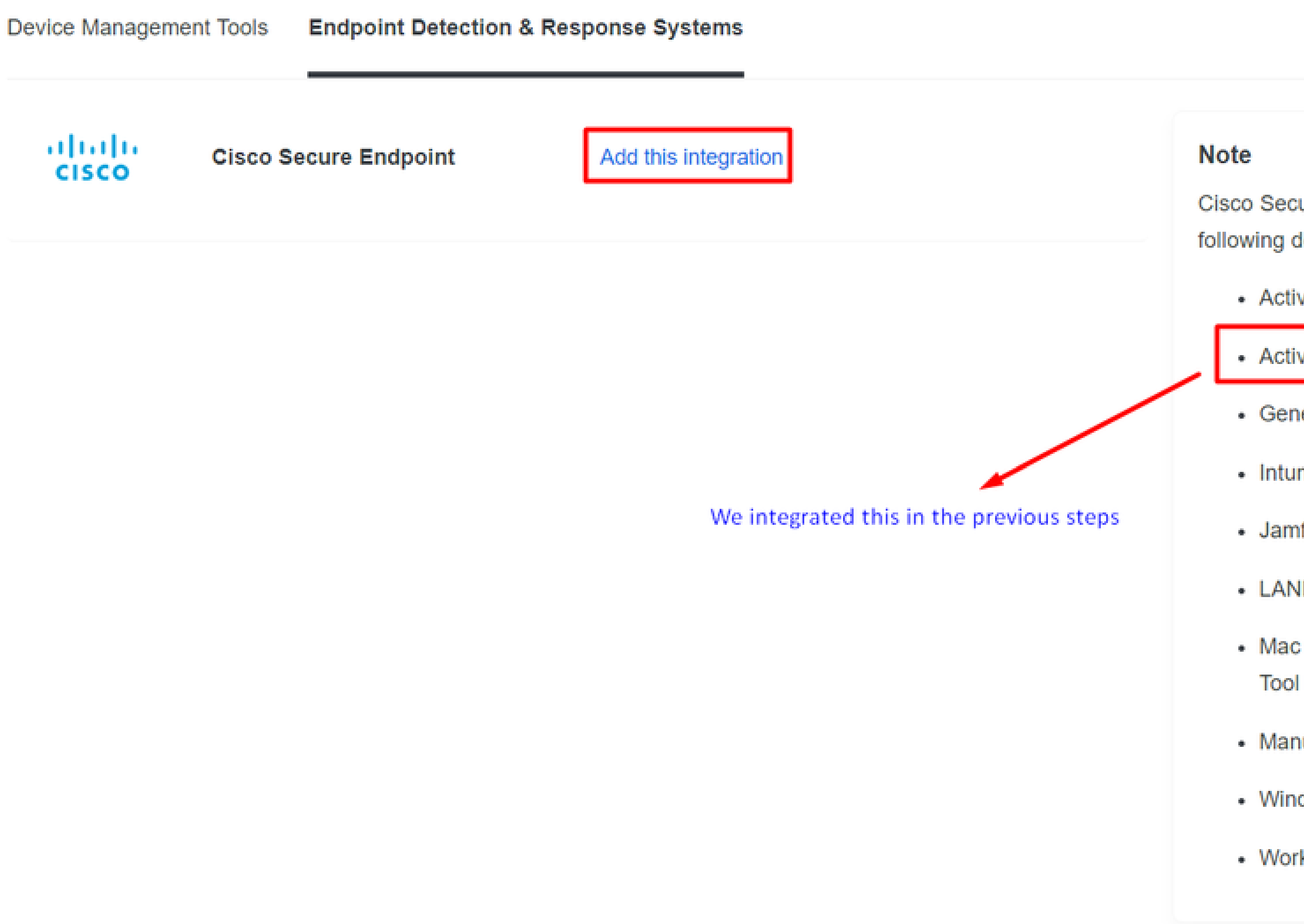
Your users will be prompted to run a check when logging in on their mobile devices

○ Test with a group Select a group

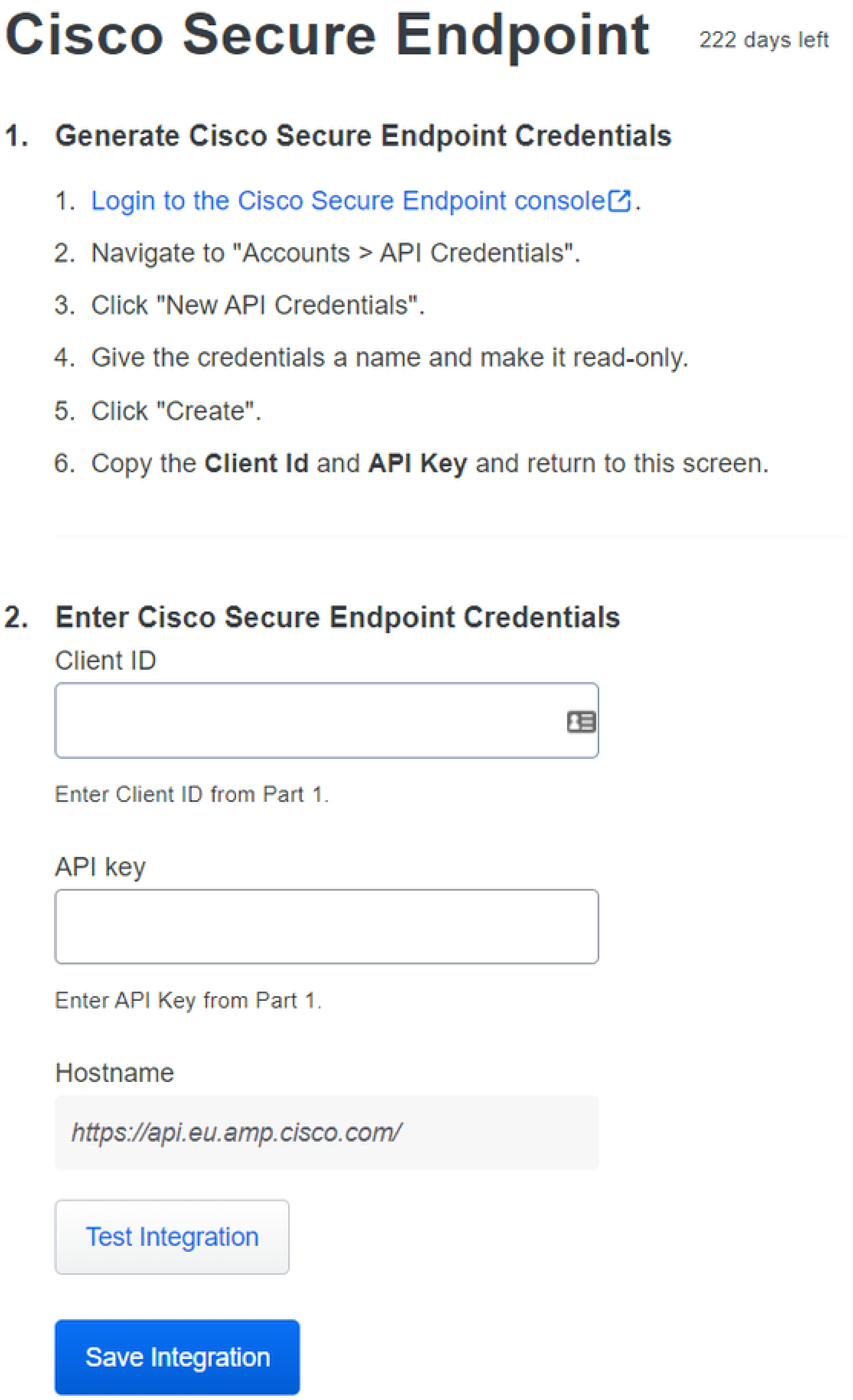
See Duo's documentation on how to create a desired testing environment

● Activate for all

Go to Trusted EndPoints > Select Endpoint Detection & Response System > Add this integration.



Now you are on the main page of the integration for 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

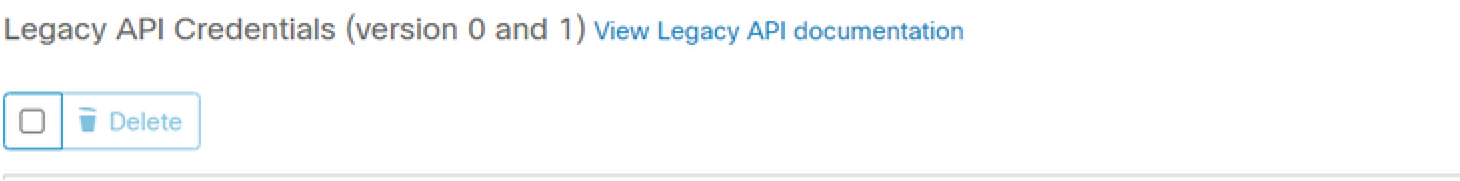
https://api.eu.amp.cisco.com/

After that, go to the **Admin Panel** of the Cisco Secure EndPoint.

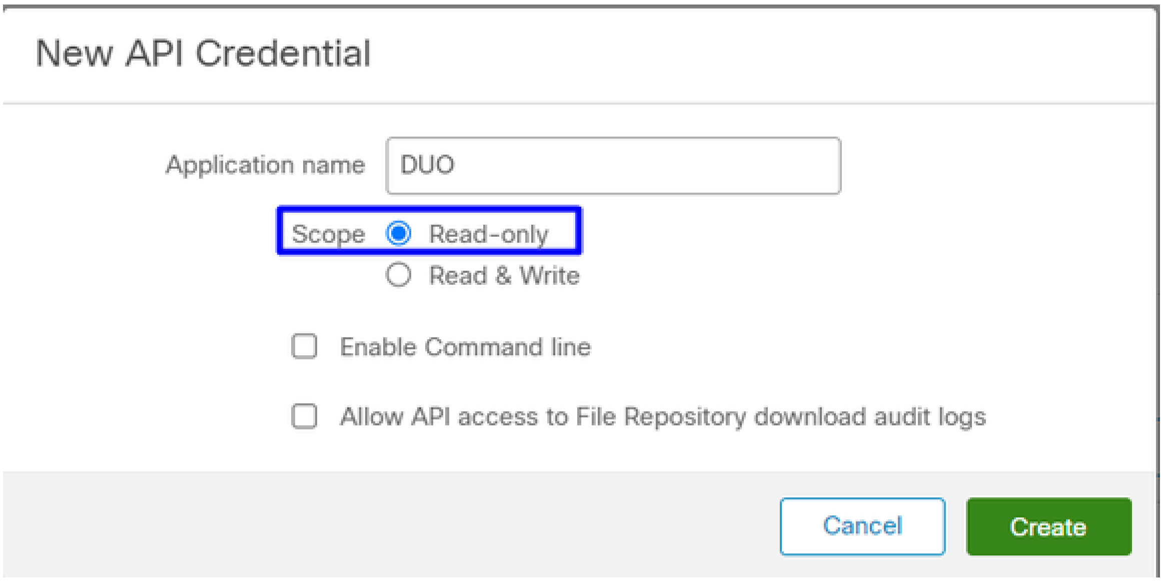
Configure the Integration in Cisco Secure EndPoint

- https://console.eu.amp.cisco.com/ **EMEAR CONSOLE LOGIN**
- https://console.amp.cisco.com/ **AMER CONSOLE LOGIN**

And navigate to Accounts > API Credentials and select **New API Credentials**.



Legacy API Credentials (version 0 and 1) View Legacy API documentation



New API Credential

Application name: DUO

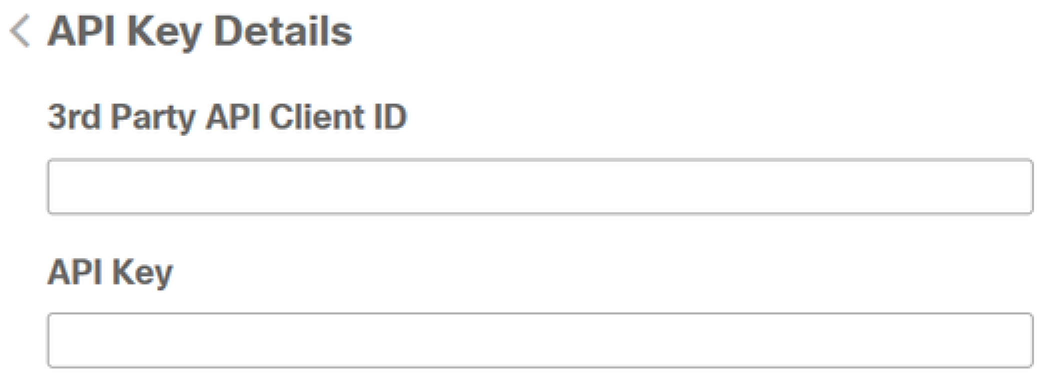
Scope ● Read-only
○ Read & Write

□ Enable Command line

□ Allow API access to File Repository download audit logs

Note: Only **Read-only** is needed to make this integration because Duo makes GET queries to Cisco Secure EndPoint to know if the device meets the requirements of the policy.

Insert **Application Name**, Scope, and **Create**.

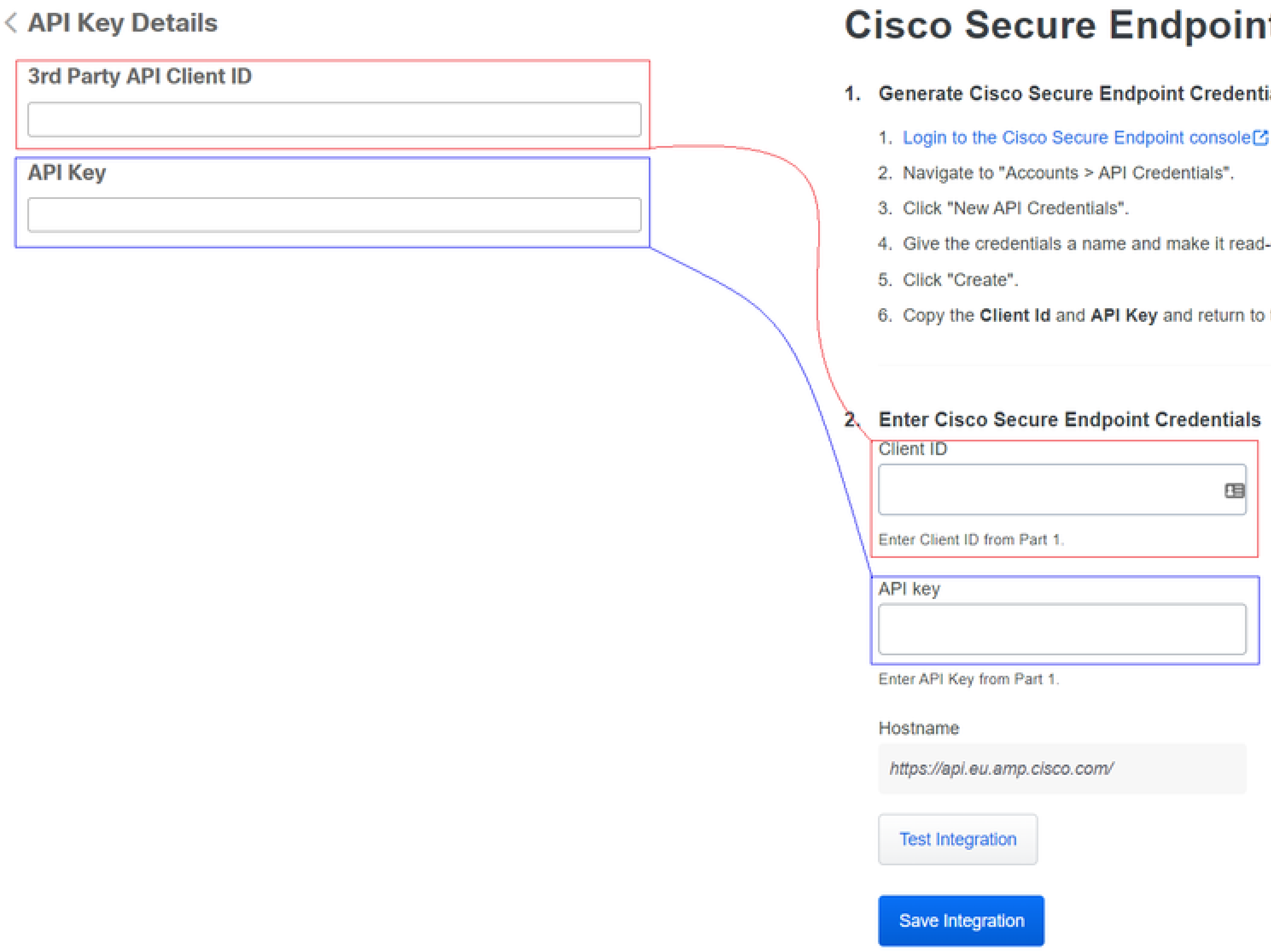


API Key Details

3rd Party API Client ID

API Key

- Copy the 3rd API Party Client ID from Cisco Secure EndPoint to Duo Admin Panel in Client ID.
- Copy the API Key from Cisco Secure EndPoint to Duo Admin Panel in API Key.



< API Key Details

3rd Party API Client ID

API Key

Cisco Secure Endpoin

1. Generate Cisco Secure Endpoint Credenti
   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-
   5. Click "Create".
   6. Copy the **Client Id** and **API Key** and return to

2. Enter Cisco Secure Endpoint Credentials

Client ID

Enter Client ID from Part 1.

API key

Enter API Key from Part 1.

Hostname

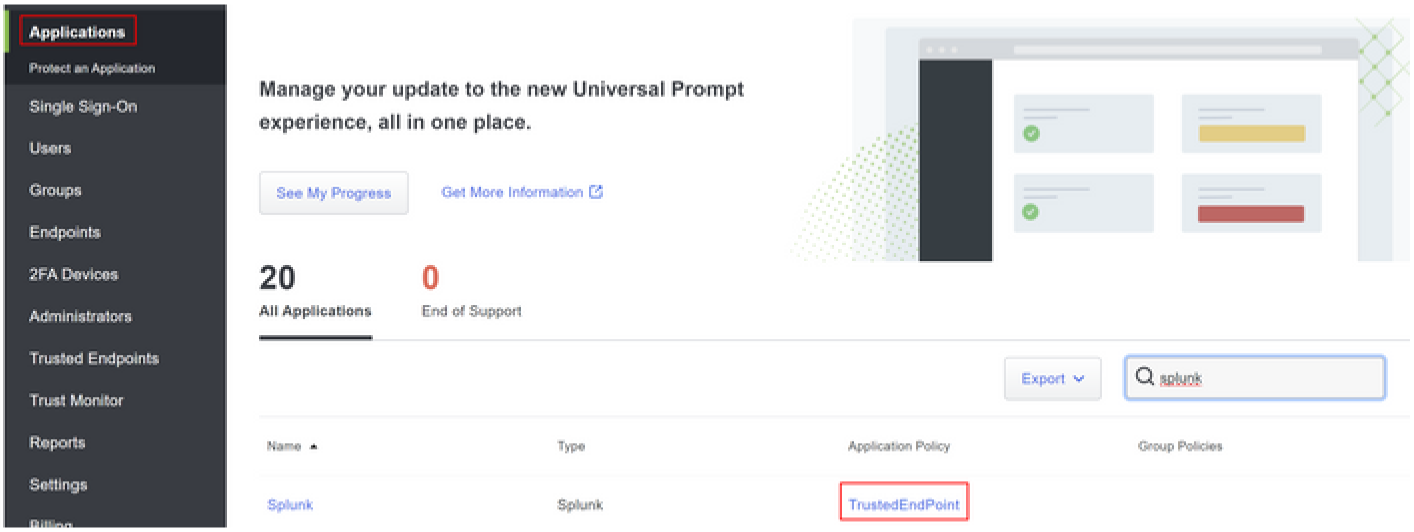
https://api.eu.amp.cisco.com/

Test the integration, and If everything works well, click **Save** to save the integration.

Configure Policies in Duo

To configure the policies for your integration, you go through your application:

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



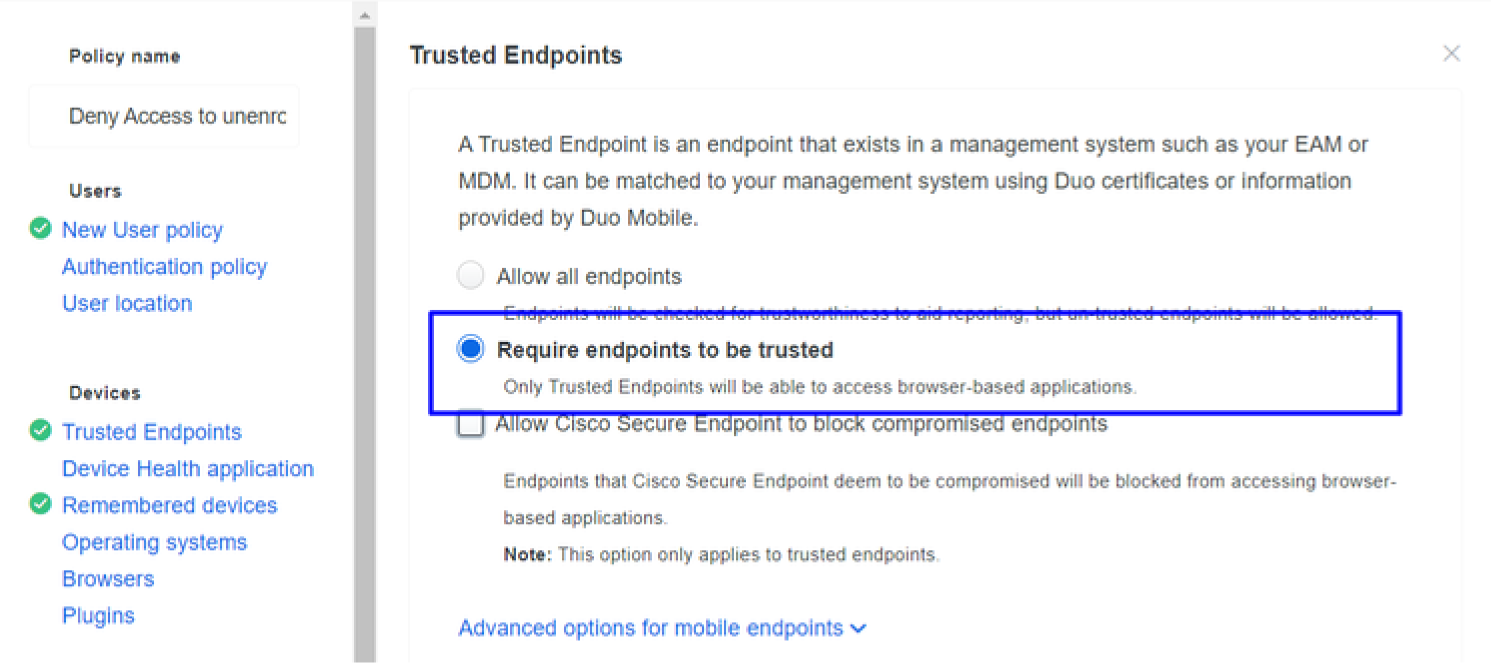
Manage your update to the new Universal Prompt experience, all in one place.

20 All Applications

0 End of Support

Name ▲	Type	Application Policy	Group Policies
Splunk	Splunk	TrustedEndPoint	

Configure the Policy to Detect a Trusted Device



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 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

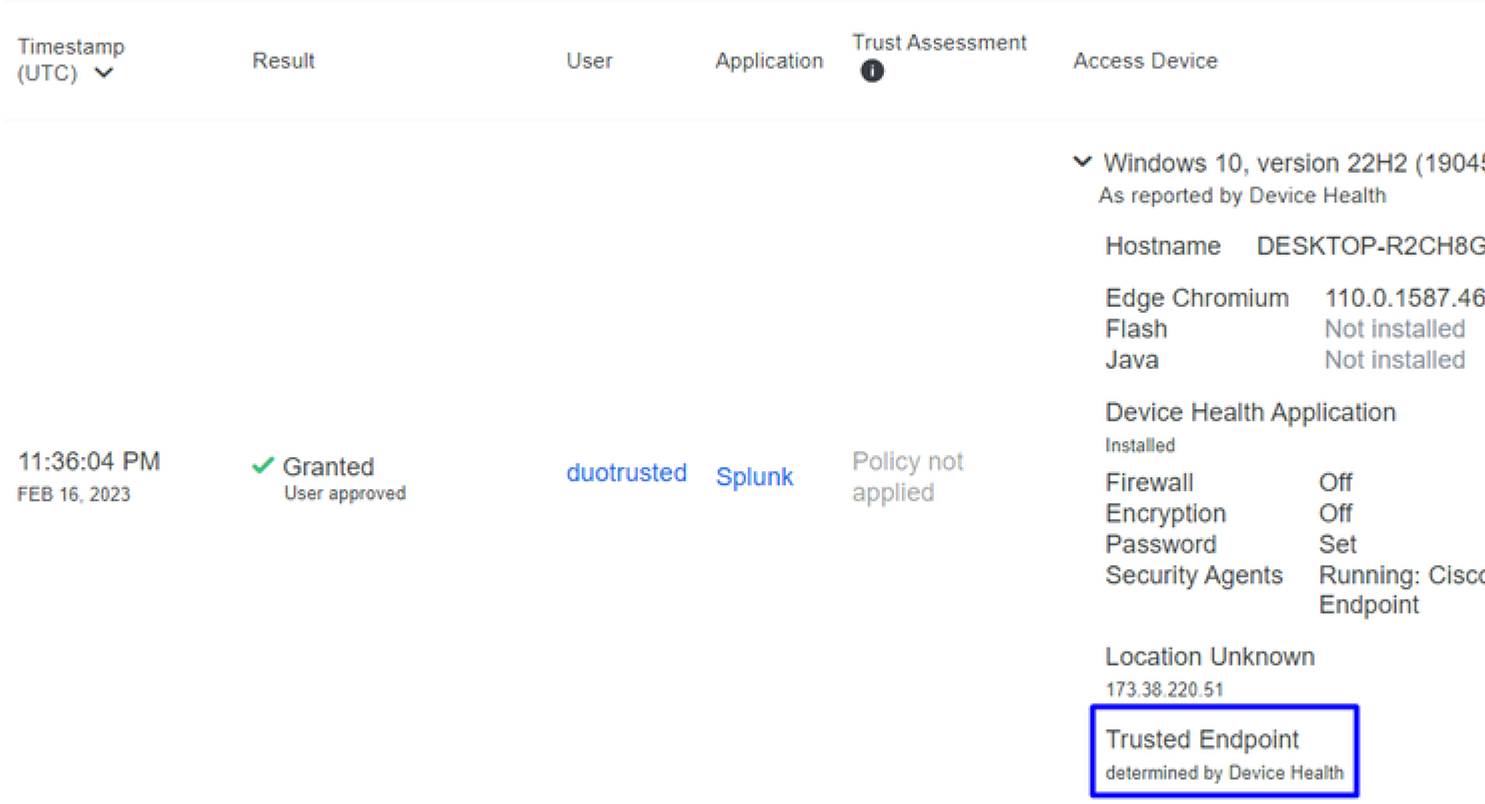
Endpoints that Cisco Secure Endpoint deem to be compromised will be blocked from accessing browser-based applications.

Note: This option only applies to trusted endpoints.

Advanced options for mobile endpoints

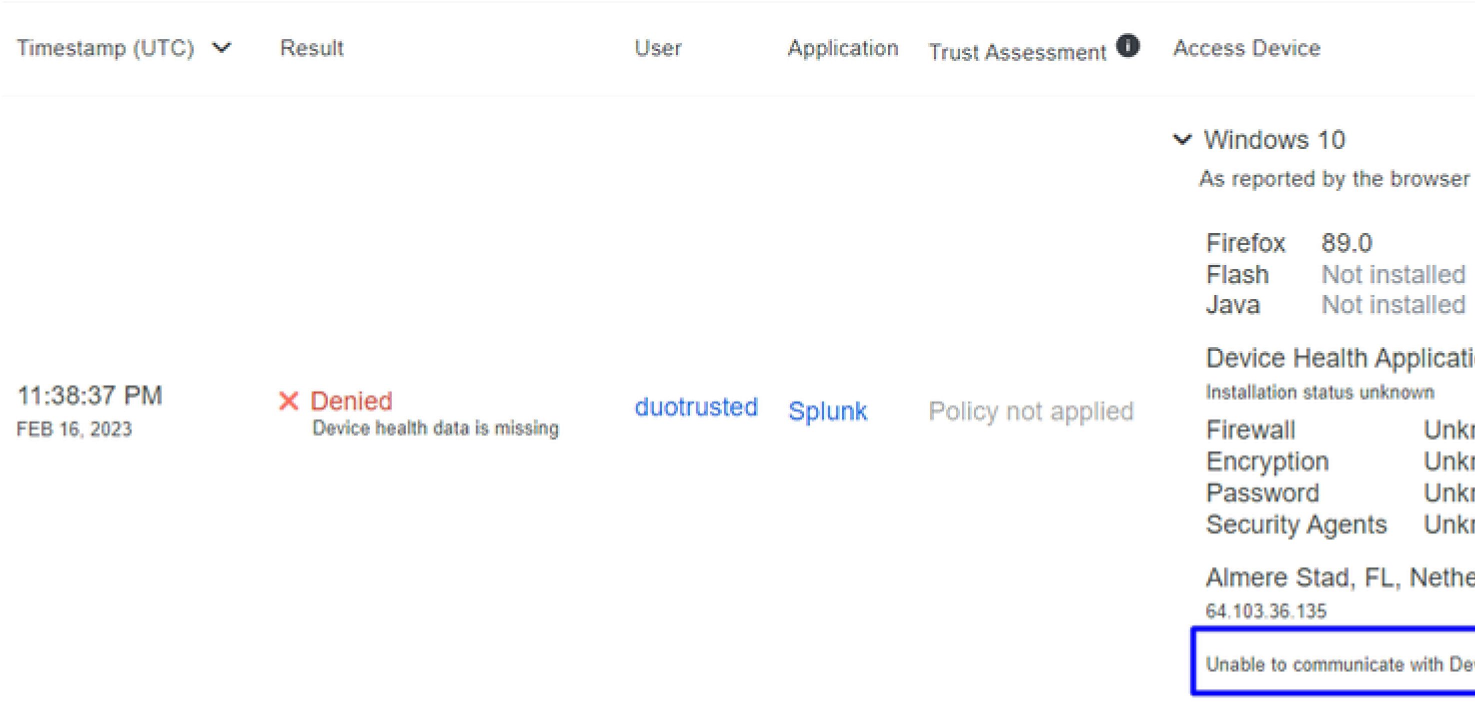
Test Trusted Machines

Machine with Duo Device Health and joined the domain

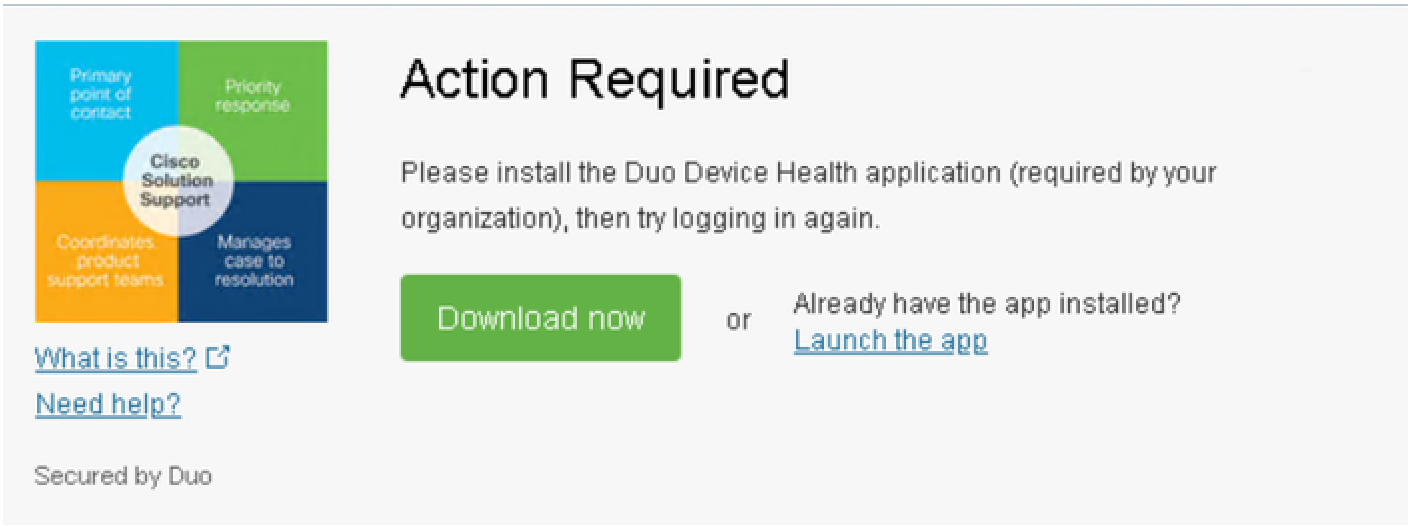


Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device
11:36:04 PM FEB 16, 2023	✓ Granted User approved	duotrusted	Splunk	Policy not applied	Windows 10, version 22H2 (1904 As reported by Device Health Hostname DESKTOP-R2CH8G Edge Chromium 110.0.1587.46 Flash Not installed Java Not installed Device Health Application Installed Firewall Off Encryption Off Password Set Security Agents Running: Cisc Endpoint Location Unknown 173.38.220.51 Trusted Endpoint determined by Device Health

Machine outside the domain without 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 Applicati Installation status unknown Firewall Unkr Encryption Unkr Password Unkr Security Agents Unkr Almere Stad, FL, Nethe 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.

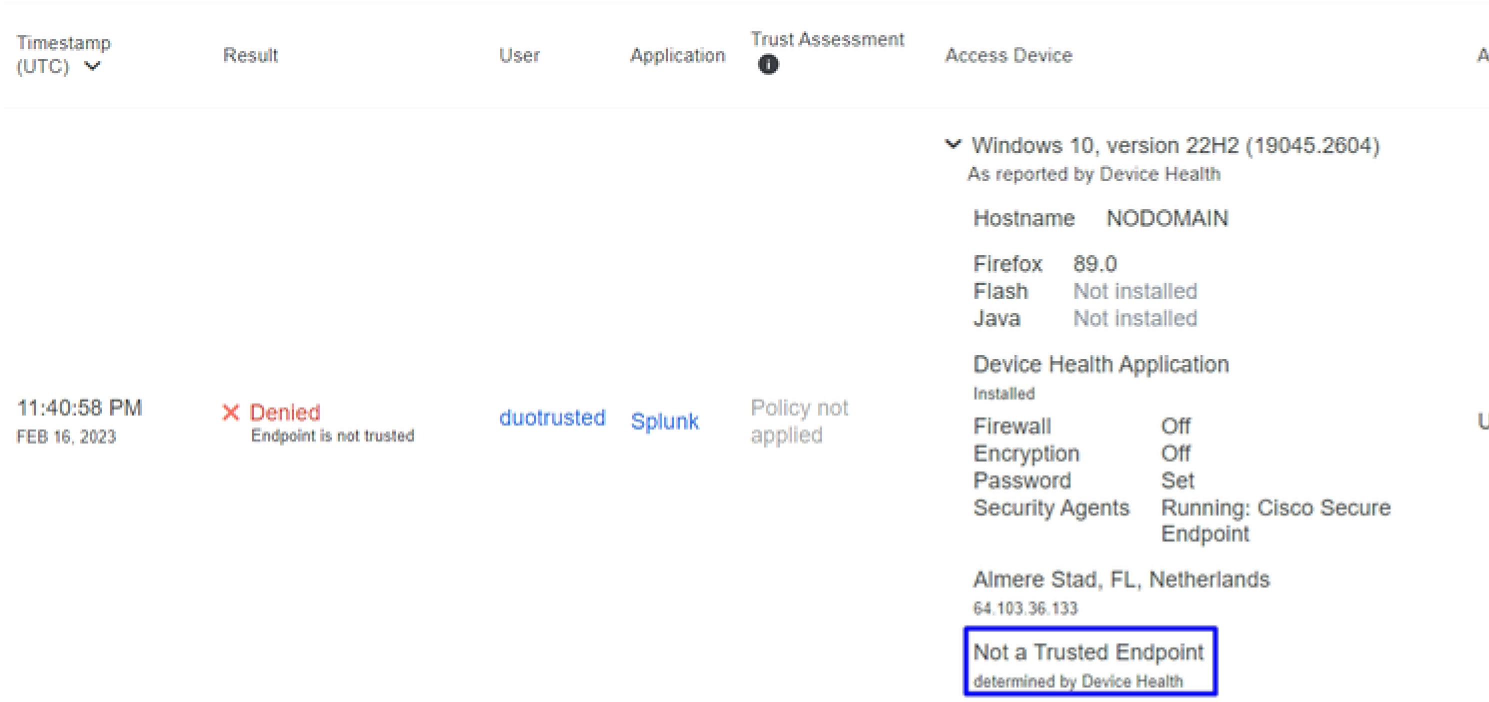
Already have the app installed? Launch the app

What is this?

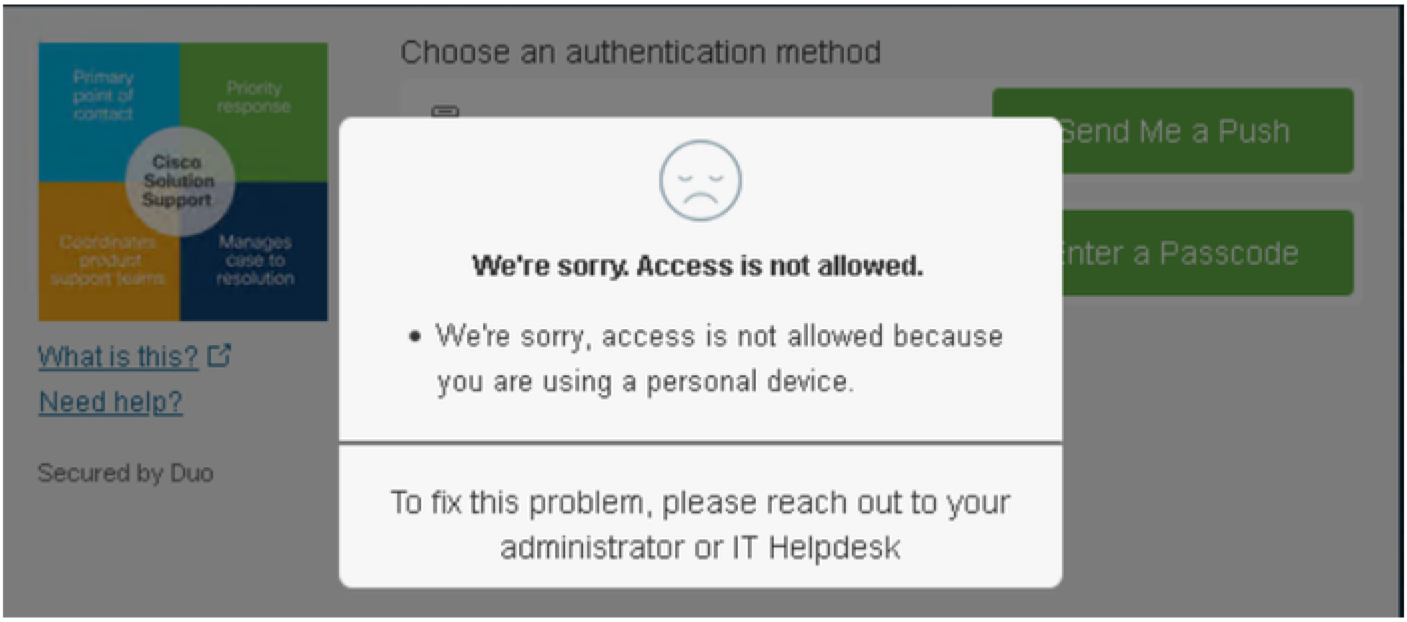
Need help?

Secured by Duo

Machine outside the domain with Duo Device Health



Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device	A
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	U



What is this?

Need help?

Secured by Duo

Choose an authentication method

Send Me a Push

Enter a Passcode

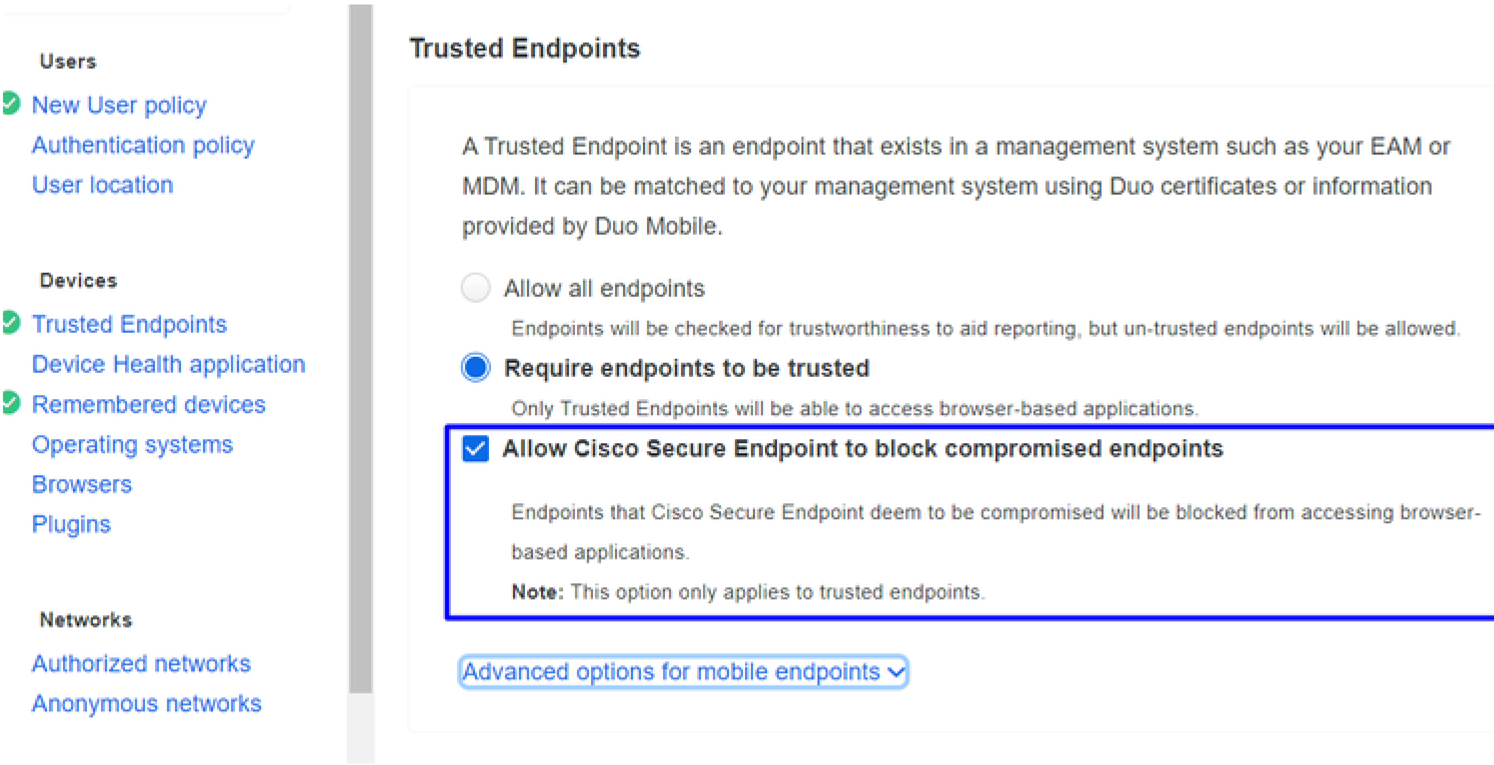
We're sorry. Access is not allowed.

- 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

Configure the Policy for Cisco Secure EndPoint

In this policy setup, configure the already trusted device to meet the requirement about threats that can affect your application, so if a device gets infected, or if some behaviors mark that machine with **suspicious artifacts** or Indicators of Compromise, you can block the machine access to the secured applications.



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.

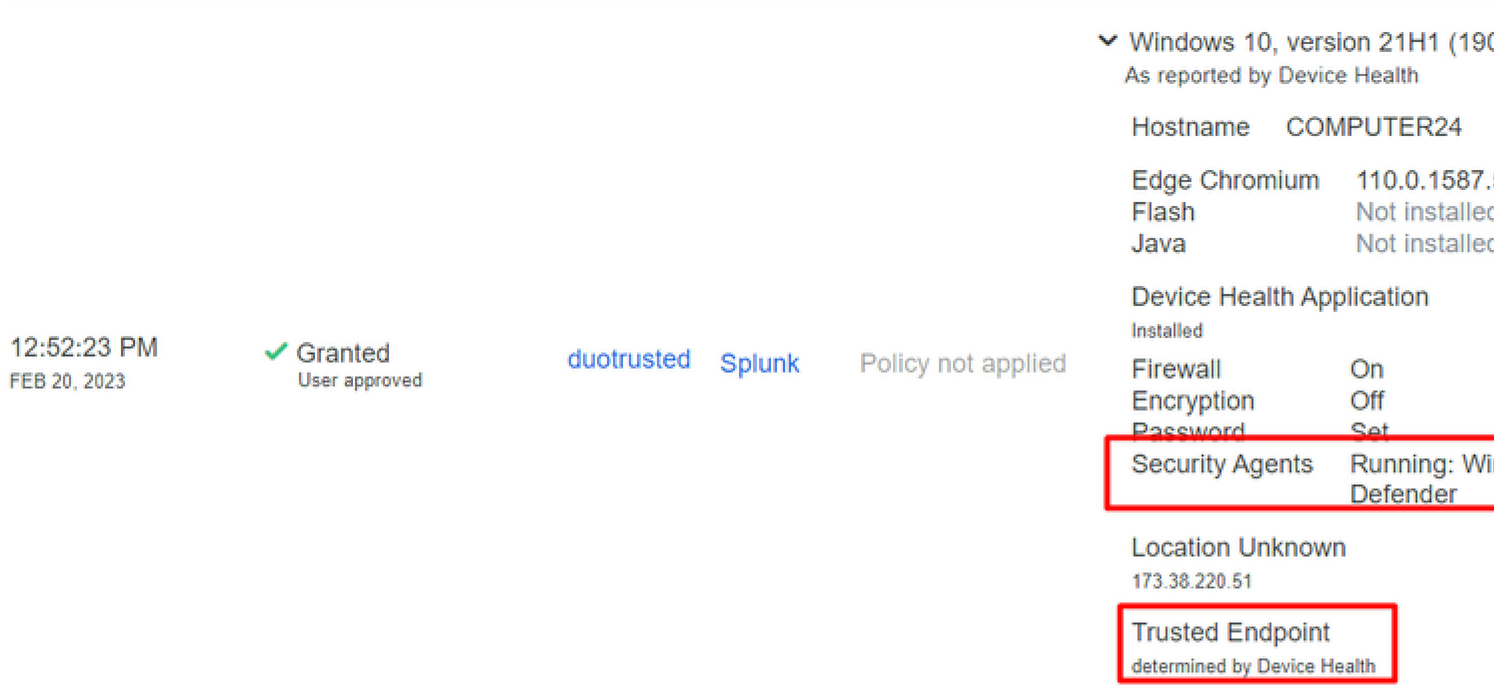
Note: This option only applies to trusted endpoints.

Advanced options for mobile endpoints

Test the Trusted Machines with Cisco Secure EndPoint

Machine without Cisco Secure Agent Installed

In this case, the machine can pass without AMP verification.



12:52:23 PM
FEB 20, 2023

✓ Granted
User approved

duotrusted

Splunk

Policy not applied

Windows 10, version 21H1 (190
As reported by Device Health

Hostname	COMPUTER24
Edge Chromium	110.0.1587.
Flash	Not installed
Java	Not installed

Device Health Application
Installed

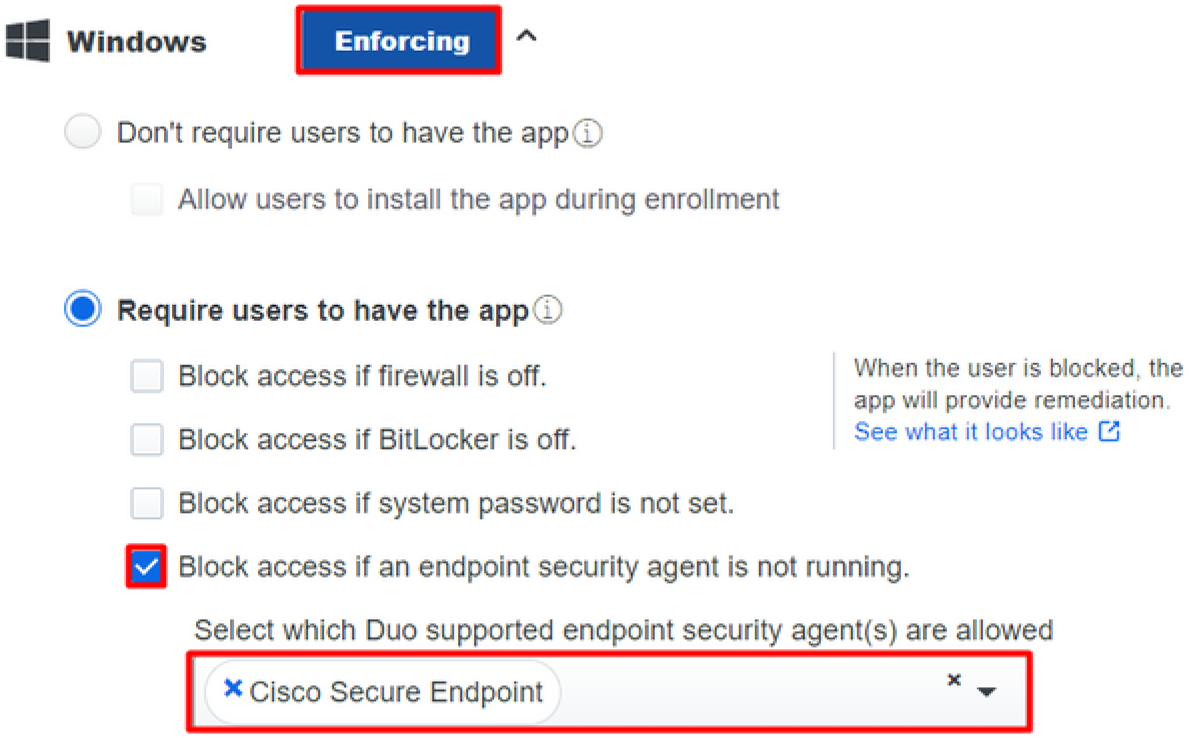
Firewall	On
Encryption	Off
Password	Set
Security Agents	Running: Wi Defender

Location Unknown
173.38.220.51

Trusted Endpoint
determined by Device Health

If you want to have a restrictive policy, you can set up the policy to be more restrictive if you modify the Device Health Application policy from **Reporting** to **Enforcing.**

And add 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.

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

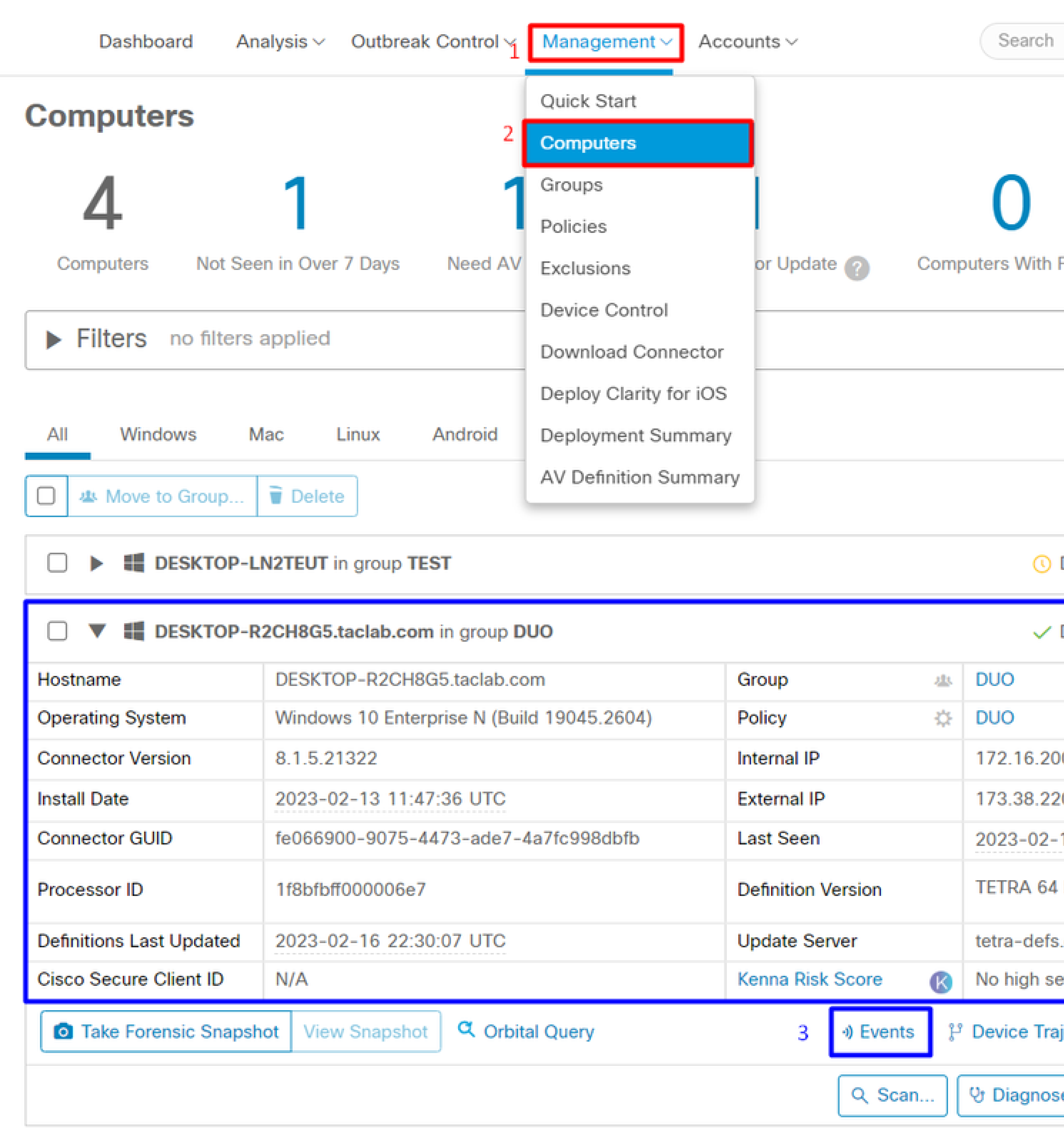
Computer without infection

With a machine, without infection, you can test how Duo with Cisco Secure EndPoint works to exchange information about the machine status and how the events are shown in this case in Duo and Cisco Secure EndPoint.

If you check the status of your machine in Cisco Secure EndPoint:

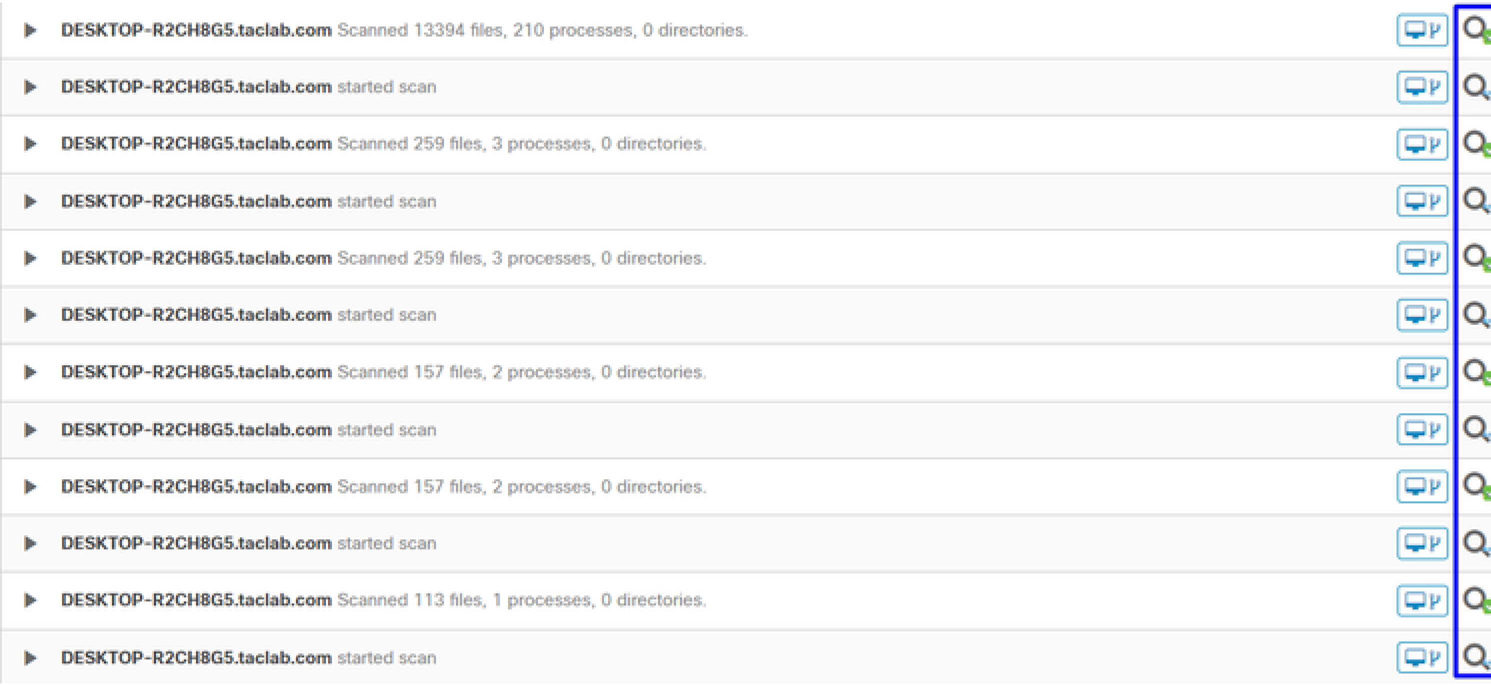
Navigate to **Management** > **Computers**.

When you filter for your machine, you can see the event of that, and in this case, you can determine your machine is clean.



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	172.16.20
Install Date	2023-02-13 11:47:36 UTC	External IP	173.38.22
Connector GUID	fe066900-9075-4473-ade7-4a7fc998dbfb	Last Seen	2023-02-1
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

You can see there is no detection for your device, and also it is on a status of clean, which means your machine is not in triage to attend.



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

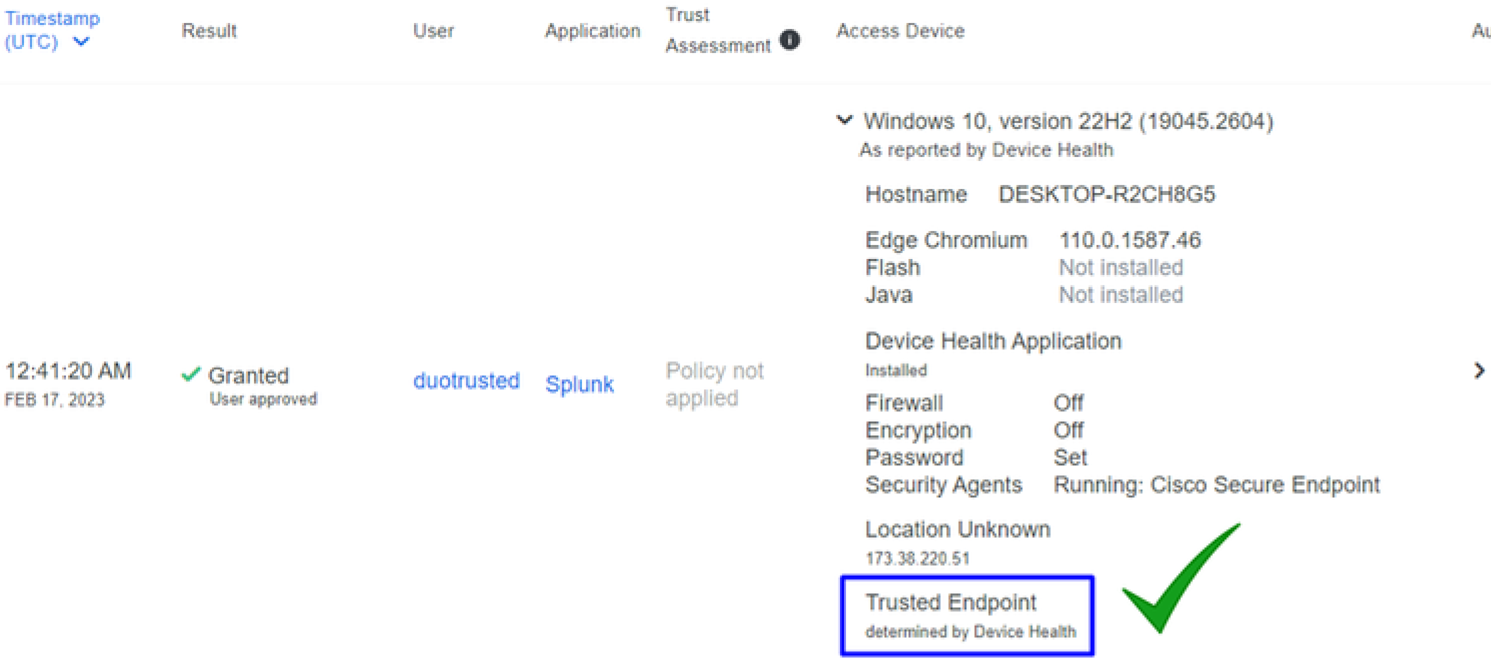
DESKTOP-R2CH8G5.taclab.com Scanned 157 files, 2 processes, 0 directories.

DESKTOP-R2CH8G5.taclab.com started scan

DESKTOP-R2CH8G5.taclab.com Scanned 113 files, 1 processes, 0 directories.

DESKTOP-R2CH8G5.taclab.com started scan

This is how Duo categorizes that machine:



Timestamp (UTC)	Result	User	Application	Trust Assessment	Access Device	Au
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	›

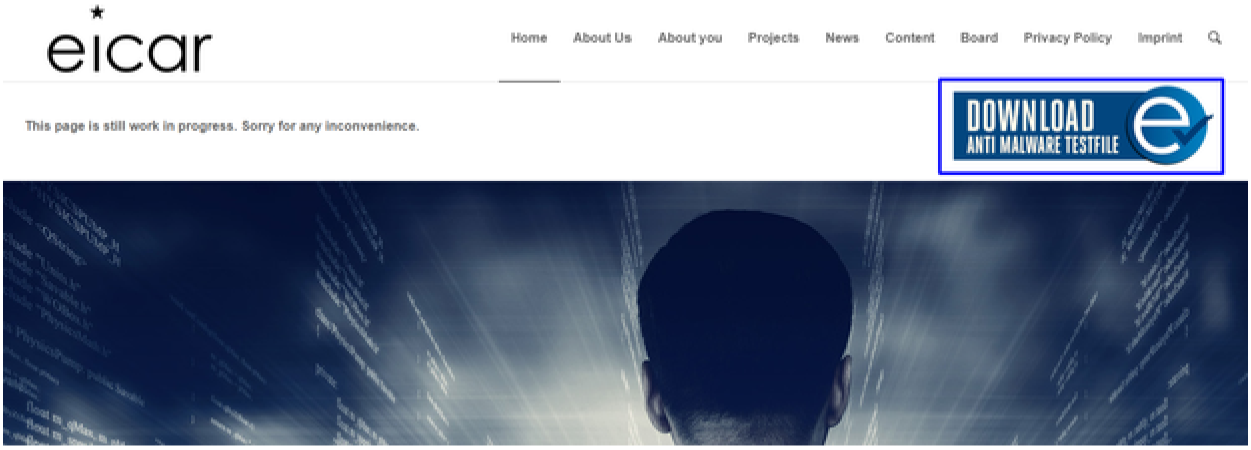
The machine maintains the trusted label.

What happens if the same machine gets infected by a Malicious Actor, has repetitive attempts of infection, or Indicators of Compromise alerts about this machine?

Computer with infection

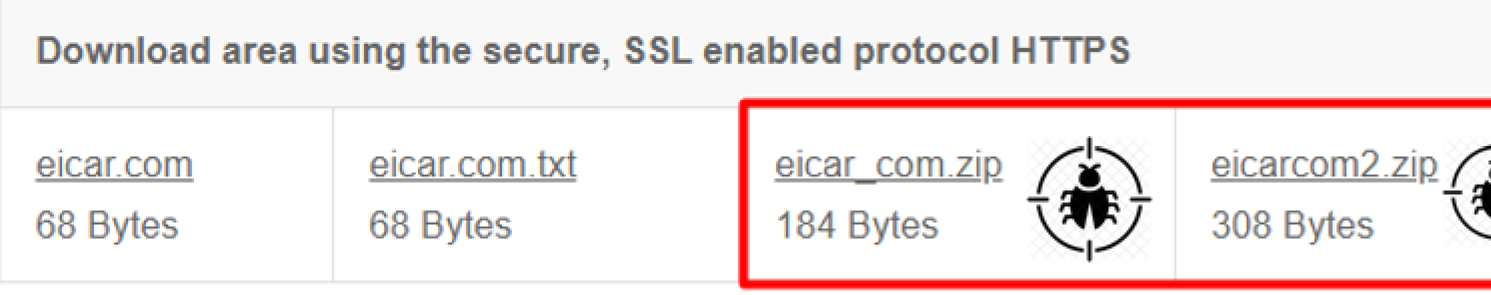
To try with an example of **EICAR** to test the feature, access https://www.eicar.org/, and download a malicious sample.

> **Note**: Do not worry. You can download that EICAR test, it is safe, and it is only a test file.



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

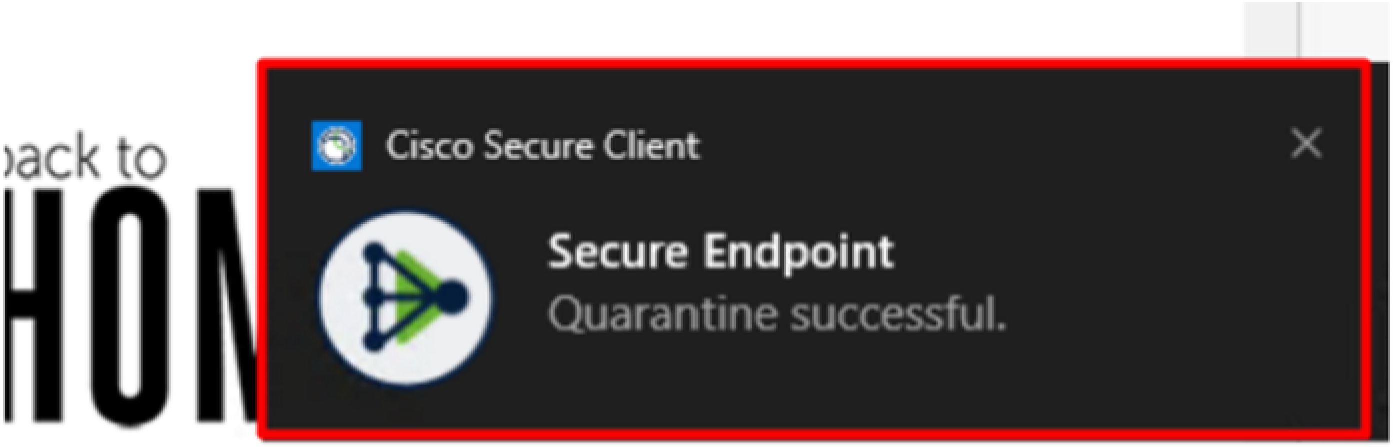
Scroll down and go to the section and download the test file.



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

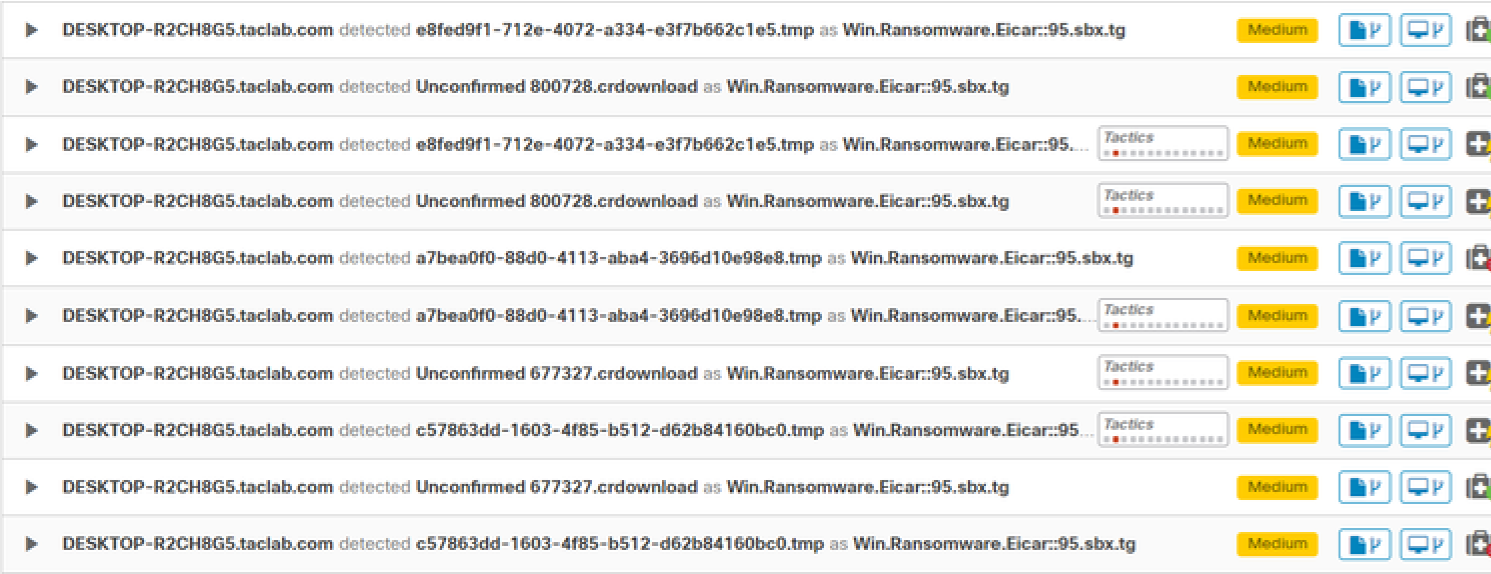
Cisco Secure EndPoint detects the malware and moves it to quarantine.



Cisco Secure Client

Secure Endpoint
Quarantine successful.

This is how it changes, as shown in the Cisco Secure EndPoint Admin panel.

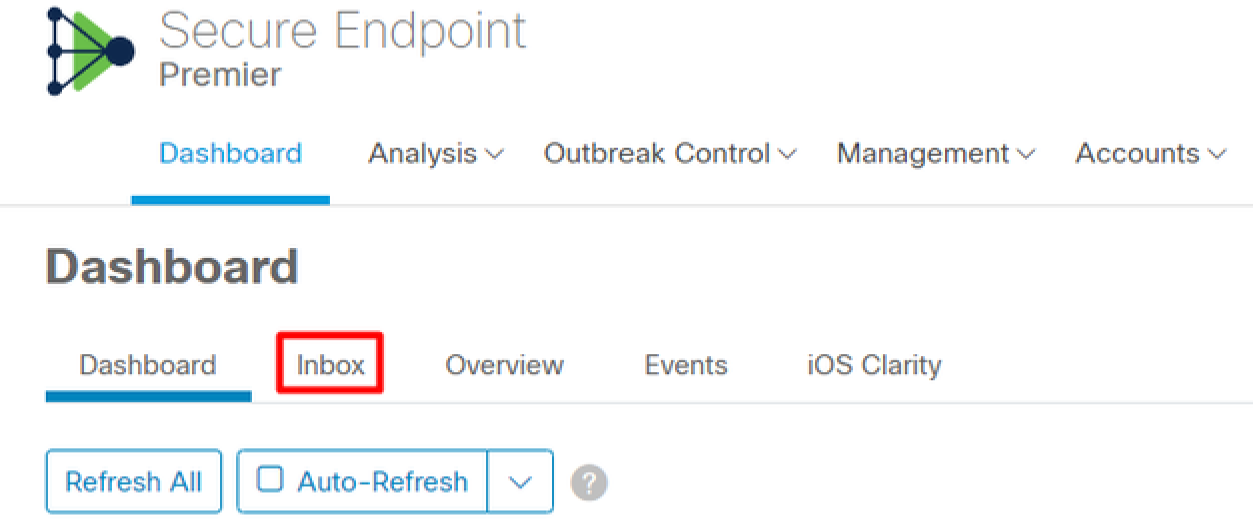


```
▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp as Win.Ransomware.Eicar::95.sbx.tg Medium
▶ DESKTOP-R2CH8G5.taclab.com detected Unconfirmed 800728.crdownload as Win.Ransomware.Eicar::95.sbx.tg Medium
▶ DESKTOP-R2CH8G5.taclab.com detected e8fed9f1-712e-4072-a334-e3f7b662c1e5.tmp 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
```

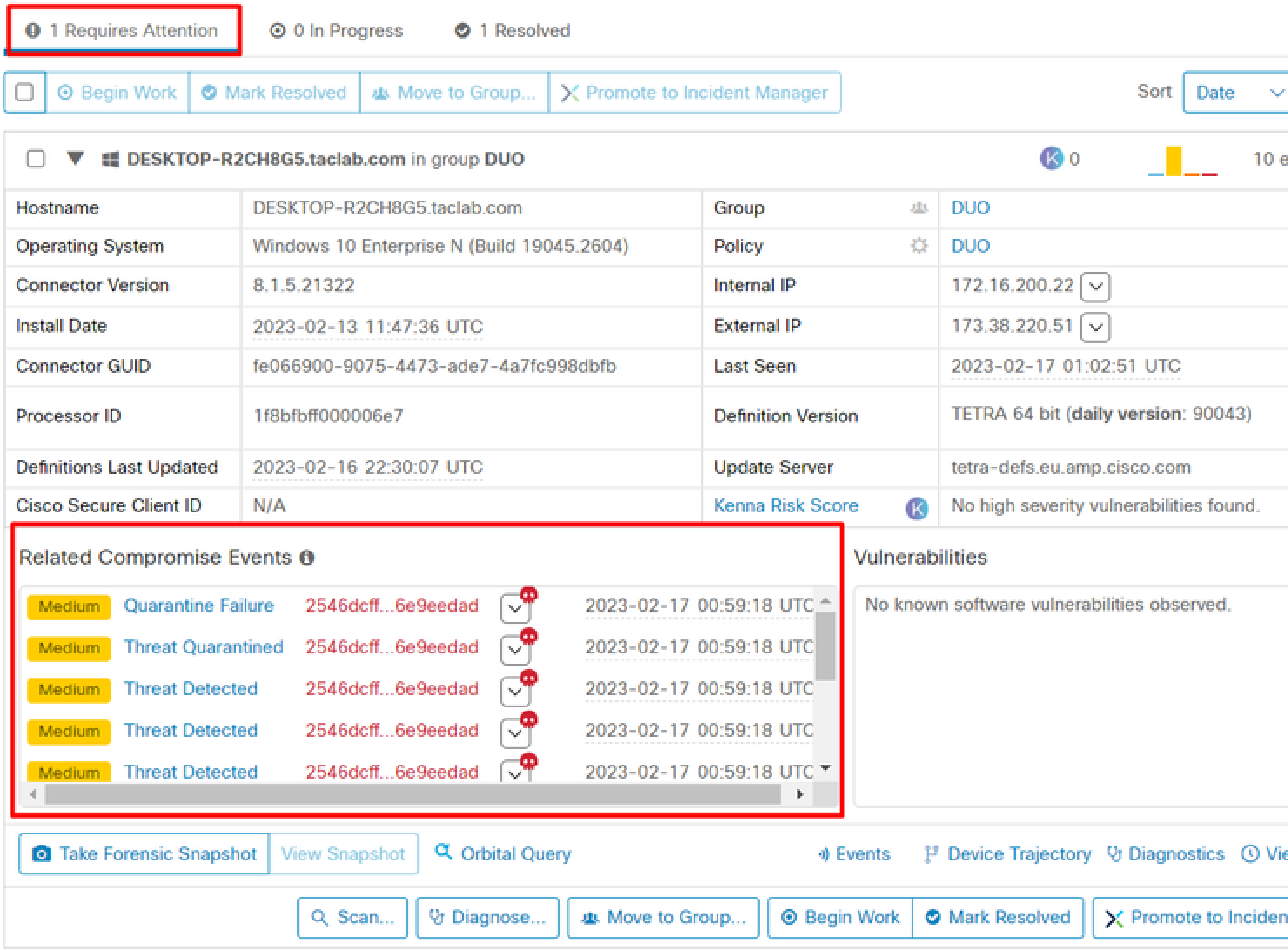
You also have the detection of the malware in the machine, but this means the endpoints are considered to be analyzed under the triage of Cisco Secure EndPoint on the Inbox.

Note: To send an endpoint to triage, it needs to have multiple detections of artifacts or strange behavior that activate some Indicators of Compromise in the endpoint.

Under the Dashboard, click in the **Inbox**.



Now you have a machine that requires attention.



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

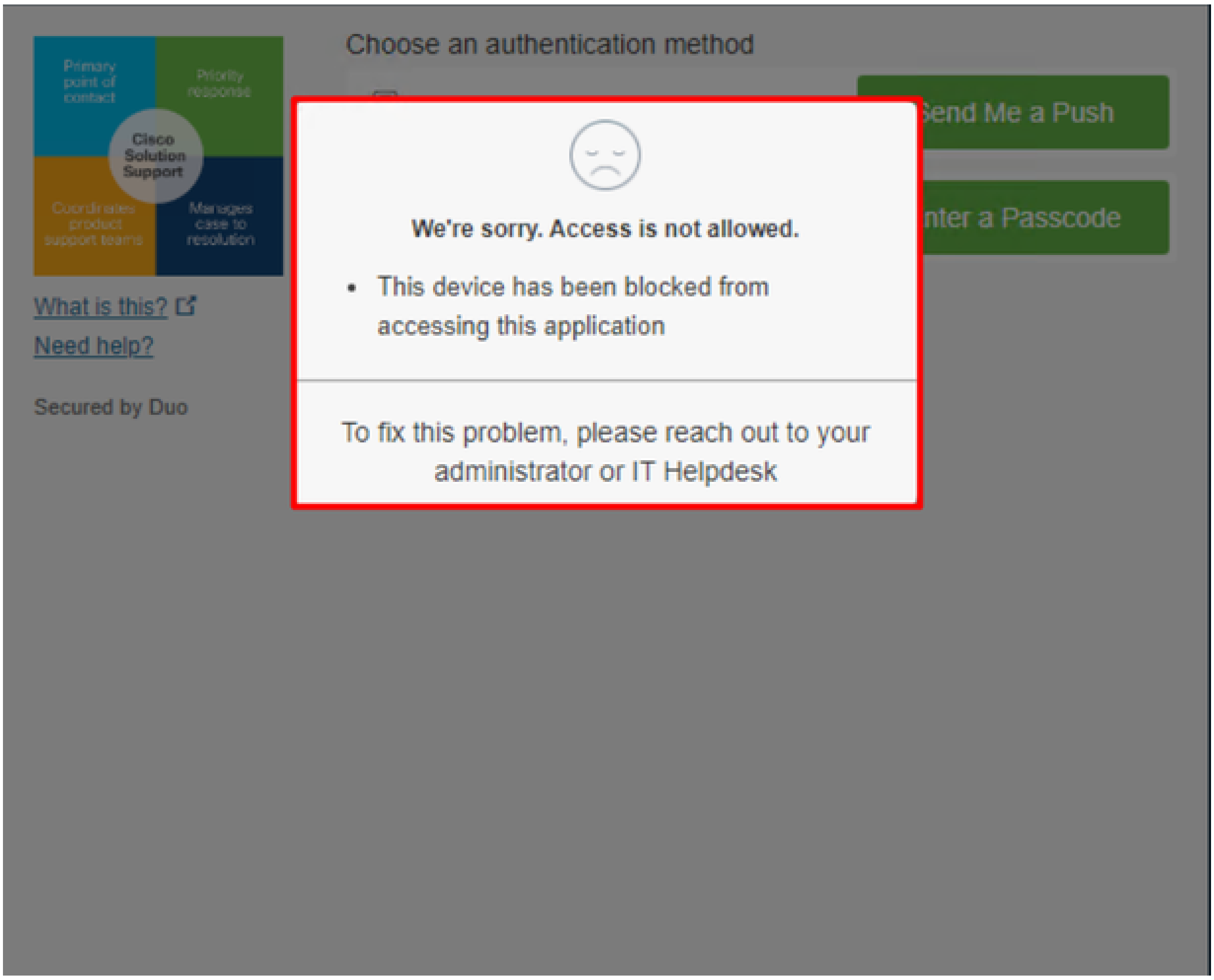
Medium	Quarantine Failure	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Quarantined	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad	2023-02-17 00:59:18 UTC
Medium	Threat Detected	2546dcff...6e9eedad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

Vulnerabilities

No known software vulnerabilities observed.

Now, switch to Duo and see what the status is.

Authentication is tried first to see the behavior after the machine was put on the Cisco Secure EndPoint under Require Attention.

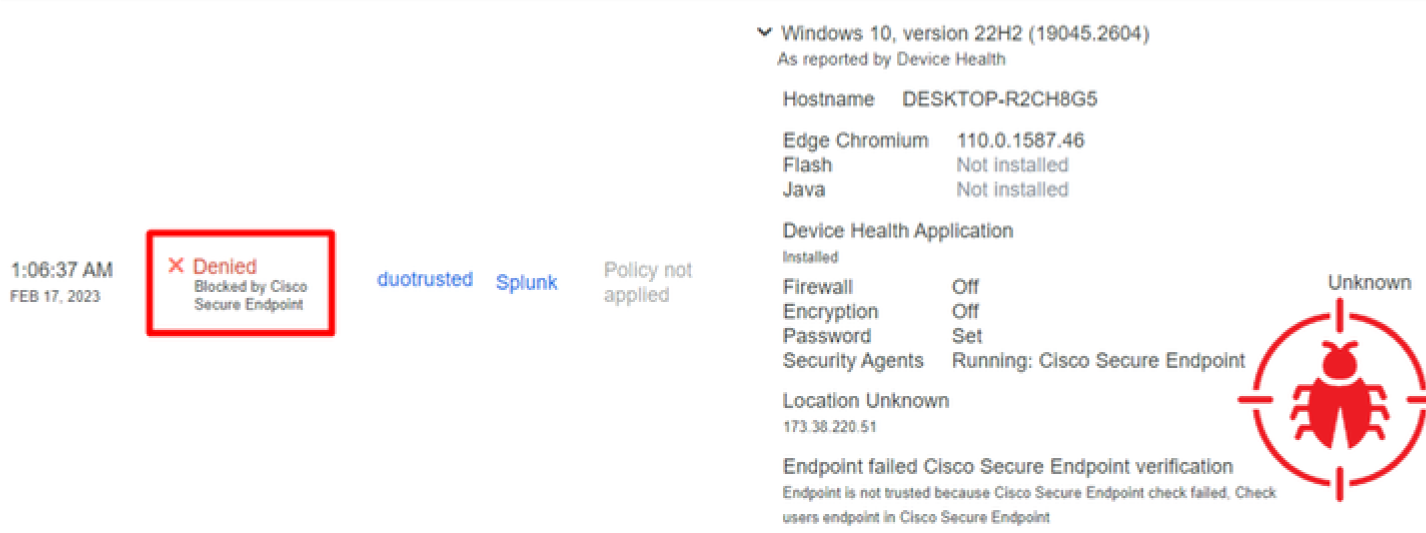


We're sorry. Access is not allowed.

- This device has been blocked from accessing this application

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

This is how it changes in Duo and how the event under authentication events is shown.



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

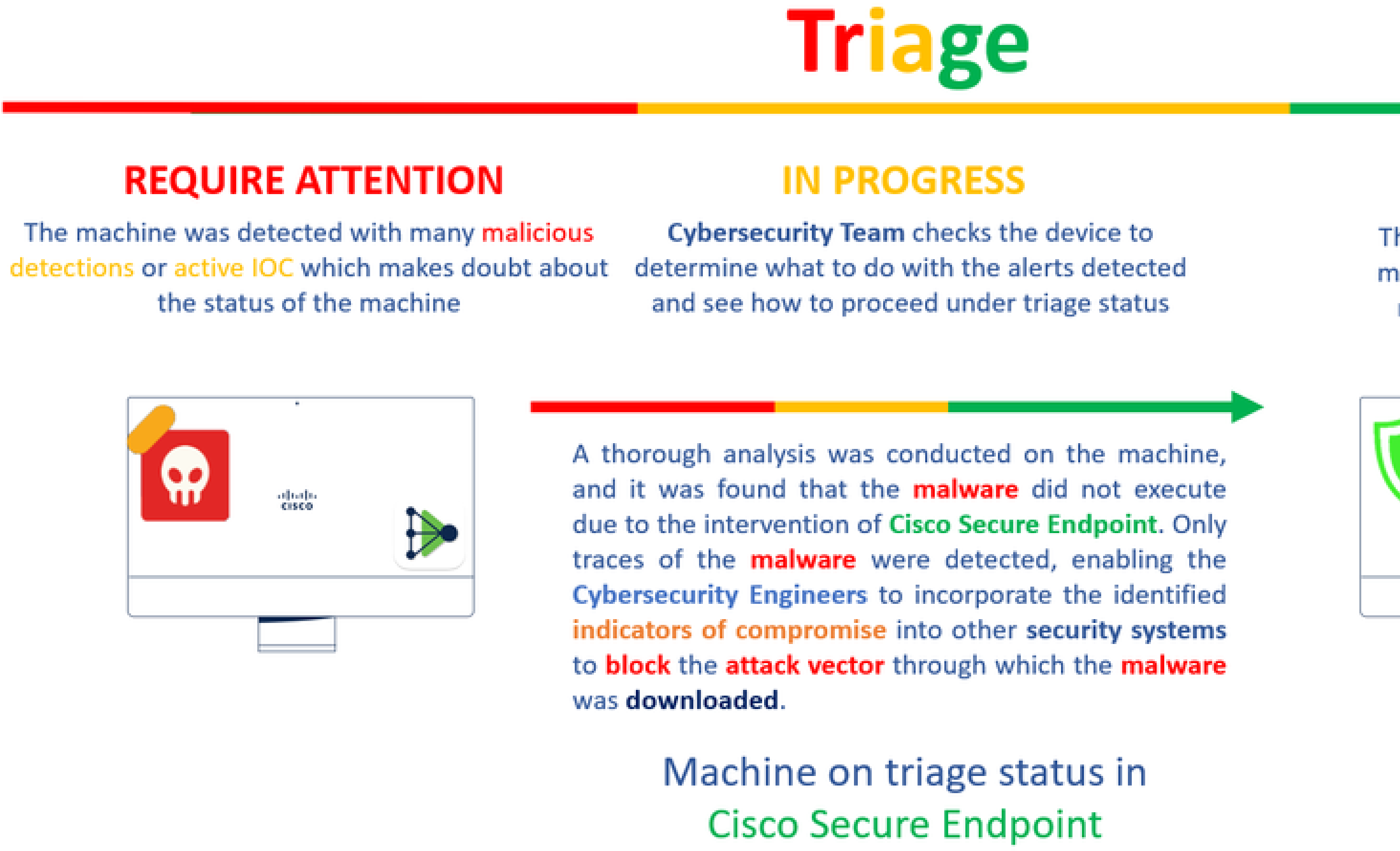
Location Unknown
173.38.220.51

Endpoint failed Cisco Secure Endpoint verification
Endpoint is not trusted because Cisco Secure Endpoint check failed. Check users endpoint in Cisco Secure Endpoint

Unknown

Your machine was detected as not a safety device for your organization.

Permit the Access to a Machine After Review



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

Th
m

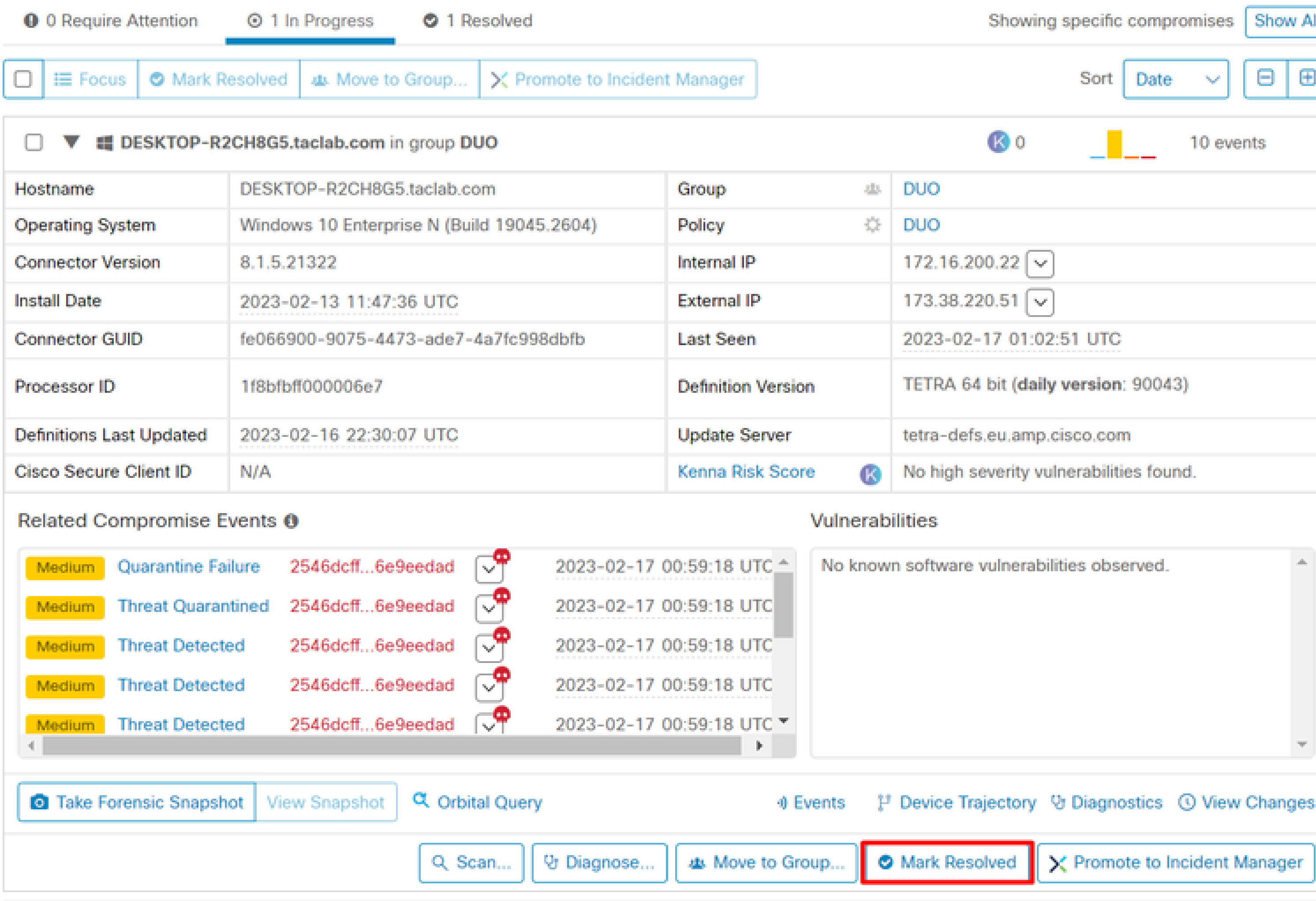
A thorough analysis was conducted on the machine, and it was found that the **malware** did not execute due to the intervention of **Cisco Secure Endpoint**. Only traces of the **malware** were detected, enabling the **Cybersecurity Engineers** to incorporate the identified **indicators of compromise**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

Machine on triage status in Cisco Secure Endpoint

After verification under Cisco Secure EndPoint and by your Cybersecurity Specialist, you can permit access to this machine to your app in Duo.

Now the question is how to permit access again to the app protected by Duo.

You need to go under Cisco Secure EndPoint and in your Inbox, mark this device as **resolved** to permit access to the application protected by 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.

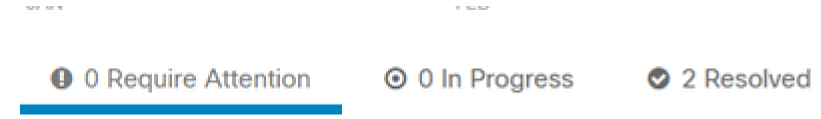
Related Compromise Events

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

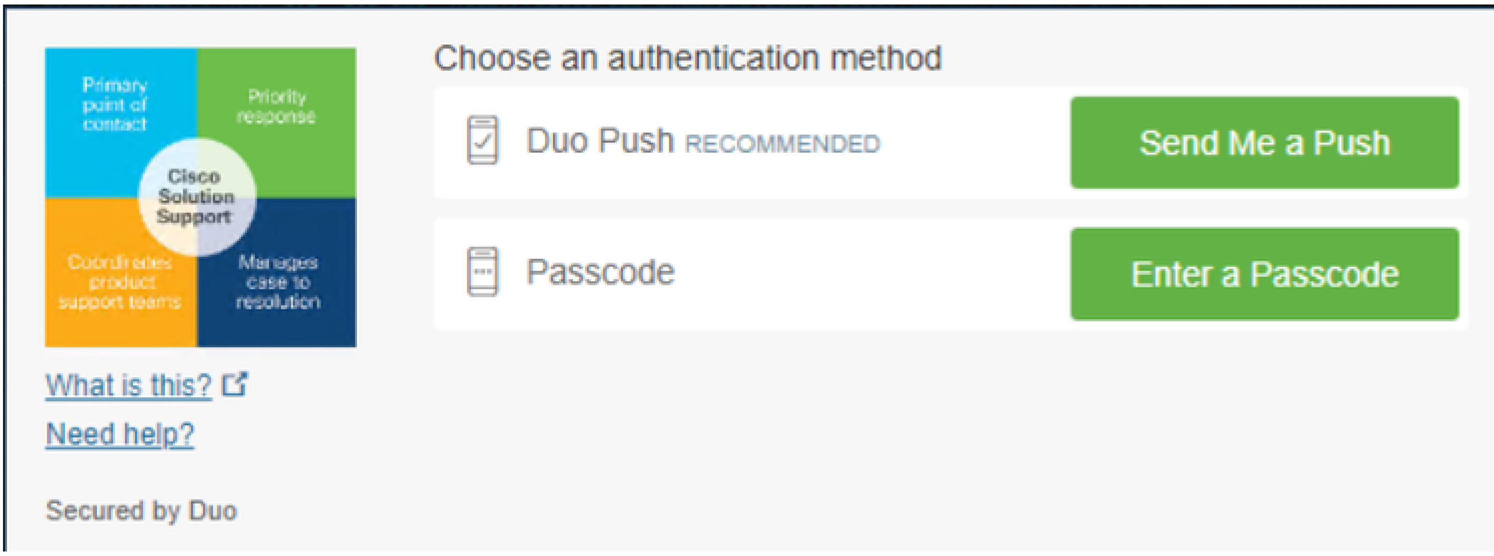
Vulnerabilities

No known software vulnerabilities observed.

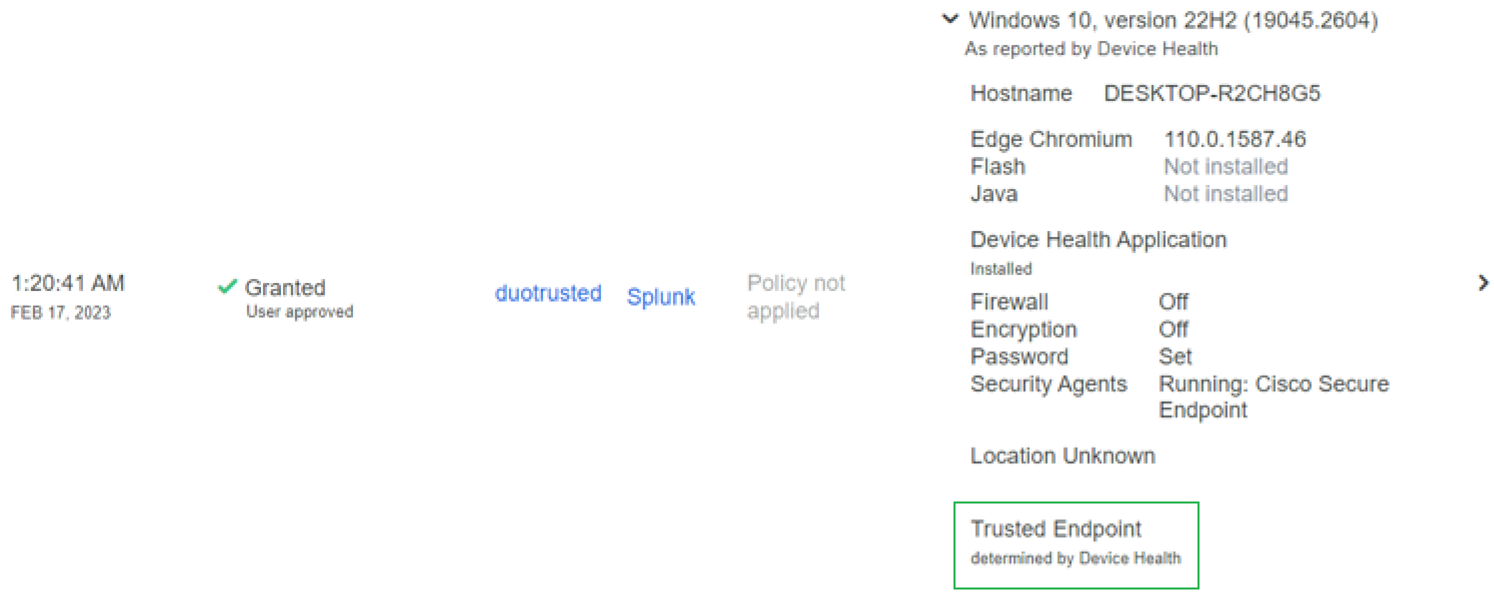
After that, you do not have the machine with the status attention required. This changed to resolved status.



In a few words, now you are prepared to test again the access to our application protected by Duo.



Now you have permission to send the push to Duo, and you are logged into the 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

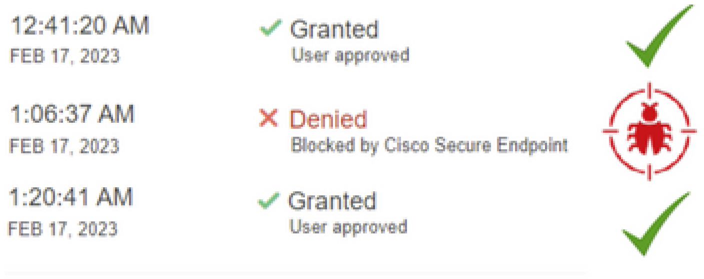
Device Health Application
Installed

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

Location Unknown

Trusted Endpoint
determined by Device Health

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 ar 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