Cisco Secure Endpoint

Integration - Technical Documentation

Cigent Technology Inc.
Website: www.cigent.com
Product: Dynamic Data Defense Engine (D3E)
Version: 2.0
Date: October, 2020

Contents

Overview 2

Key Benefits 2

Cigent Product Integration Architecture 3

Cisco Secure Endpoint Integration 3

Integration Prerequisites 3

Cisco Secure Endpoint Cloud Integration Setup 4

Cigent Integration Configuration 5

Testing the Console Integration 7

Cigent D3E Endpoint Installation 8

Cisco Secure Endpoint agent installation 8

Overview

The Cigent Dynamic Data Defense Engine™ (D3E) is a new approach to data security, one that complements existing solutions and places the importance of protecting data above **all** else. D3E takes concepts used in threat containment and continuous authentication and applies them as close to the data stream as possible, bringing proactive protection directly to your data. D3E allows users to safely and easily access critically important information, even if the system is already compromised. The result is an unprecedented level of protection, detection, and response to cyberattacks, insider threats, and lost or stolen devices.

Cigent's management console is the centralized mechanism for monitoring, managing and controlling Cigent D3E deployments. Cigent's management console natively supports integration with Cisco Secure Endpoint management console providing increased value and security to users of both solutions.

Key Benefits

Cigent D3E provides an additional response option for threats discovered by the Cisco Secure Endpoint solution. This response ensures files designated as sensitive by the end user are protected by adding a second factor authentication requirement to access the files during the heightened security state. End users can continue to access their files while in heightened security state and even clear the threat should they or their SOC determine the threat has been remediated.

Cigent Product Integration Architecture

The Cigent Management Console Connector Service communicates directly with the Cisco Secure Endpoint management console over the internet using REST APIs. No additional software or infrastructure is required by the customer to enable this integration.

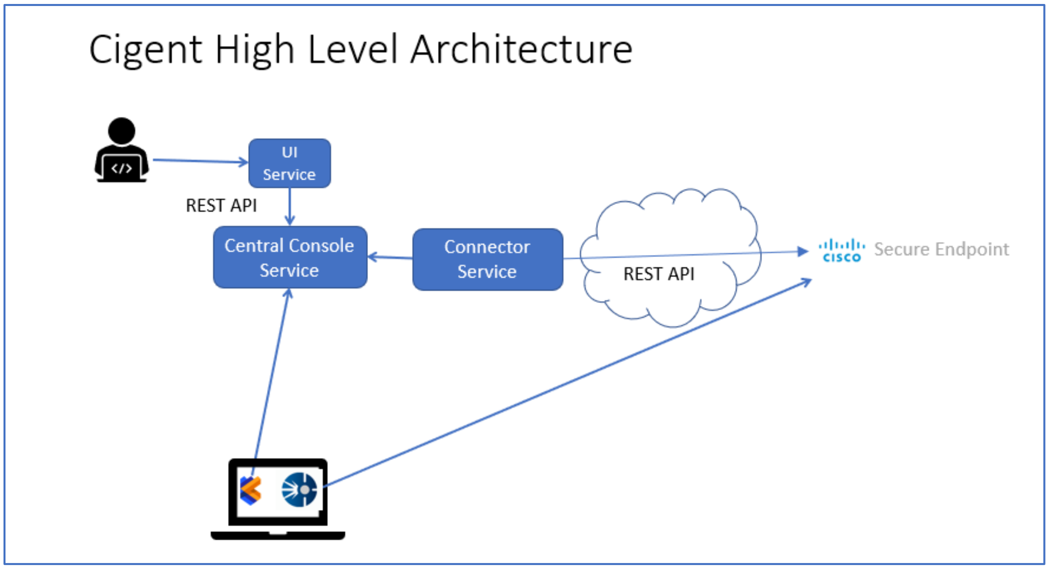


Figure 1 Cigent High Level Architecture

Cisco Secure Endpoint Integration

Cigent Management Console users can set up, activate and delete integrations to their Cisco Endpoint instance autonomously. This integration is known as a pull integration as the Cigent Management Console will monitor the Cisco Secure Endpoint console to determine if any threats have been raised for devices under Cigent management. If so, an Active Lock enable request is immediately sent to the Cigent D3E endpoint to protect the user's sensitive files.

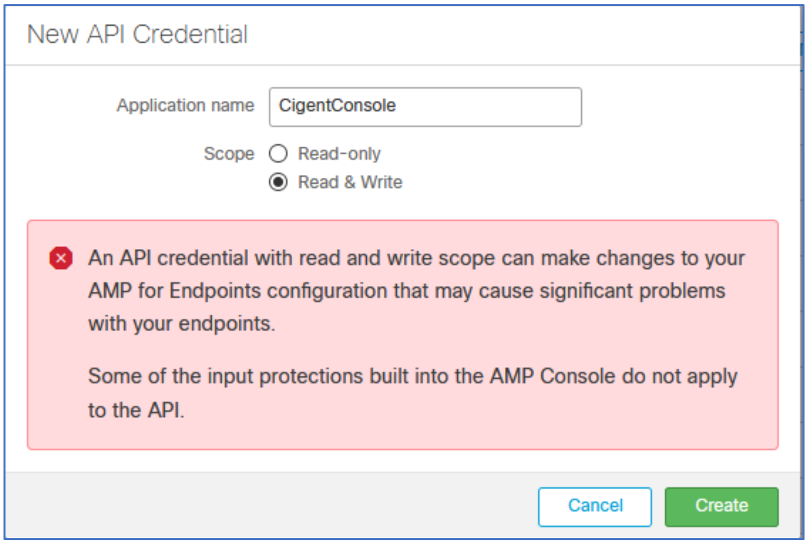
Integration Prerequisites

Both Cigent D3E and Cisco Secure Endpoint agents need to be installed on devices on which users desire this additional layer of response.

Users must have administrative access to both Cigent and Cisco Secure Endpoint management consoles.

Cisco Secure Endpoint Cloud Integration Setup

Start by creating an API credential for use by the Cigent Console integration. The API Credential page is found under the Accounts menu of the Cisco Secure Endpoint console. Click the New API Credential button. Fill in the Name (CigentConsole is recommended) and change the scope to Read & Write. The click Create.



New API Credential

Application name: CigentConsole

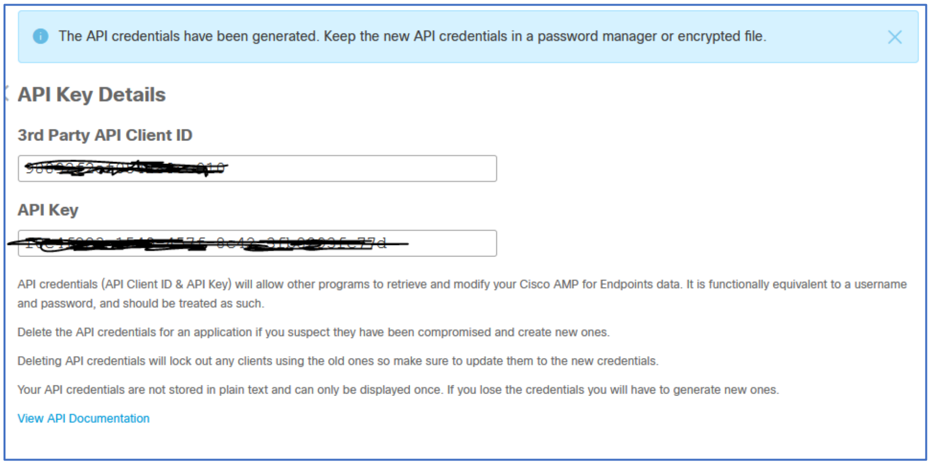
Scope: ○ Read-only ● Read & Write

An API credential with read and write scope can make changes to your AMP for Endpoints configuration that may cause significant problems with your endpoints.

Some of the input protections built into the AMP Console do not apply to the API.

Figure 2 Creating Cisco Secure Endpoint API Credentials

Make note of the API Client ID and API Key in the subsequent page. You will need to fill these values into the Cigent console in the next section.



The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

API Key Details

3rd Party API Client ID

[redacted]

API Key

[redacted]

API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a username and password, and should be treated as such.

Delete the API credentials for an application if you suspect they have been compromised and create new ones.

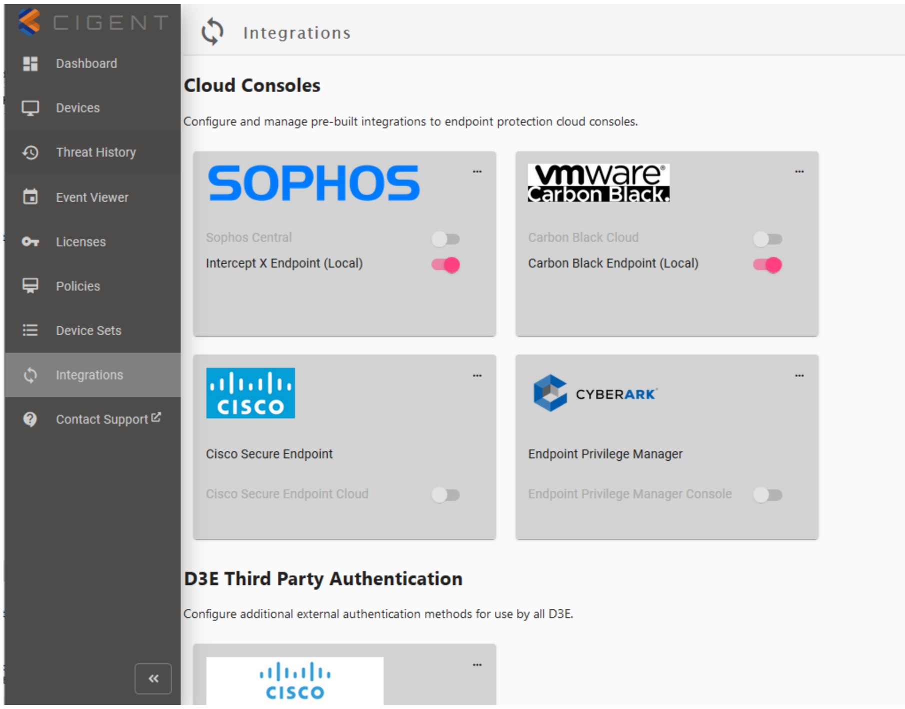
Deleting API credentials will lock out any clients using the old ones so make sure to update them to the new credentials.

Your API credentials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.

Figure 3 Cisco Secure Endpoint API Key Details

Cigent Integration Configuration

Navigate to https://central.cigent.com/integrations



Cloud Consoles

Configure and manage pre-built integrations to endpoint protection cloud consoles.

Sophos Central ○
Intercept X Endpoint (Local) ●

Carbon Black Cloud ○
Carbon Black Endpoint (Local) ●

Cisco Secure Endpoint
Cisco Secure Endpoint Cloud ○

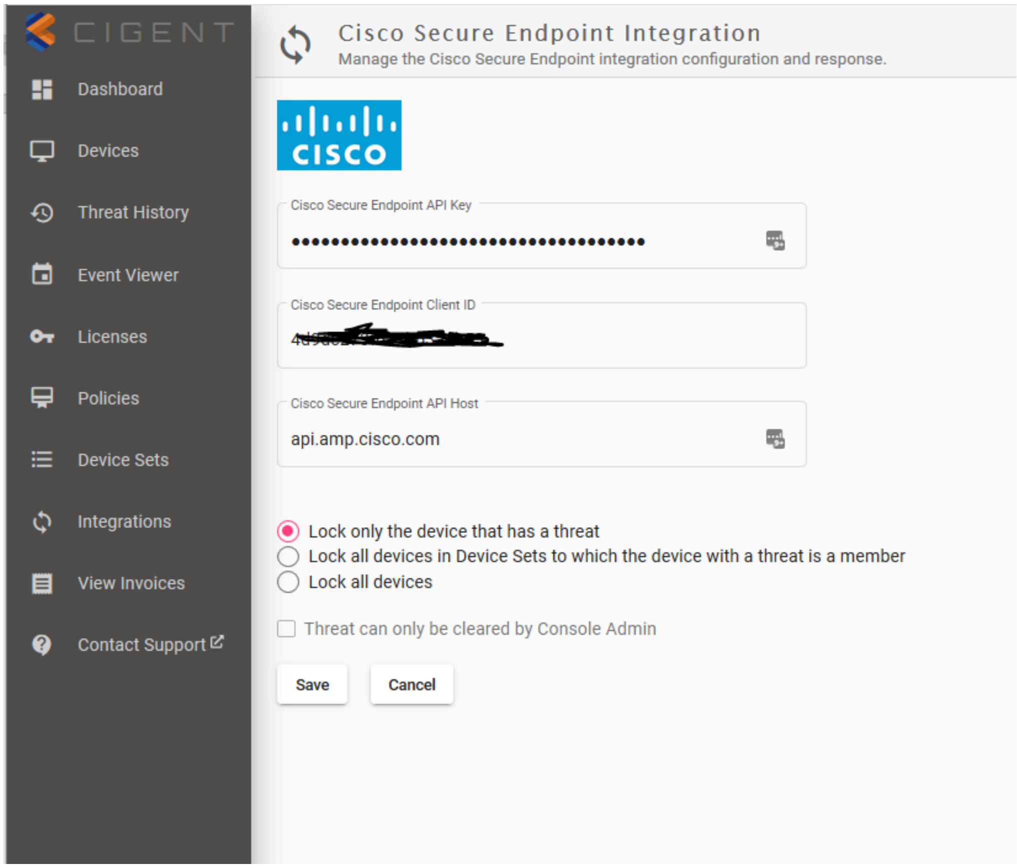
Endpoint Privilege Manager
Endpoint Privilege Manager Console ○

D3E Third Party Authentication

Configure additional external authentication methods for use by all D3E.

Figure 4 Cigent Integrations Page

To configure the Console integration, select 'Set up' from the menu available under the ellipse of the Cisco Secure Endpoint tile.



Cisco Secure Endpoint Integration

Manage the Cisco Secure Endpoint integration configuration and response.

Cisco Secure Endpoint API Key: ••••••••••••••••••••••••••••••••••••••

Cisco Secure Endpoint Client ID: [redacted]

Cisco Secure Endpoint API Host: api.amp.cisco.com

● Lock only the device that has a threat
○ Lock all devices in Device Sets to which the device with a threat is a member
○ Lock all devices

☐ Threat can only be cleared by Console Admin

Save Cancel

Figure 5 Cisco Secure Endpoint Integration Configuration

Enter the following information into the integration page:

Cisco Secure Endpoint API Key : Enter the API Key from the API Credential created in the previous section.

Cisco Secure Endpoint Client ID : Enter the API Client ID from the API Credential created in the previous section.

Cisco Secure Endpoint API Host : Enter the API host URL. See Cisco documentation at https://api-docs.amp.cisco.com/?api_host=api.amp.cisco.com for more information.

Next choose the scope of response to the threats.

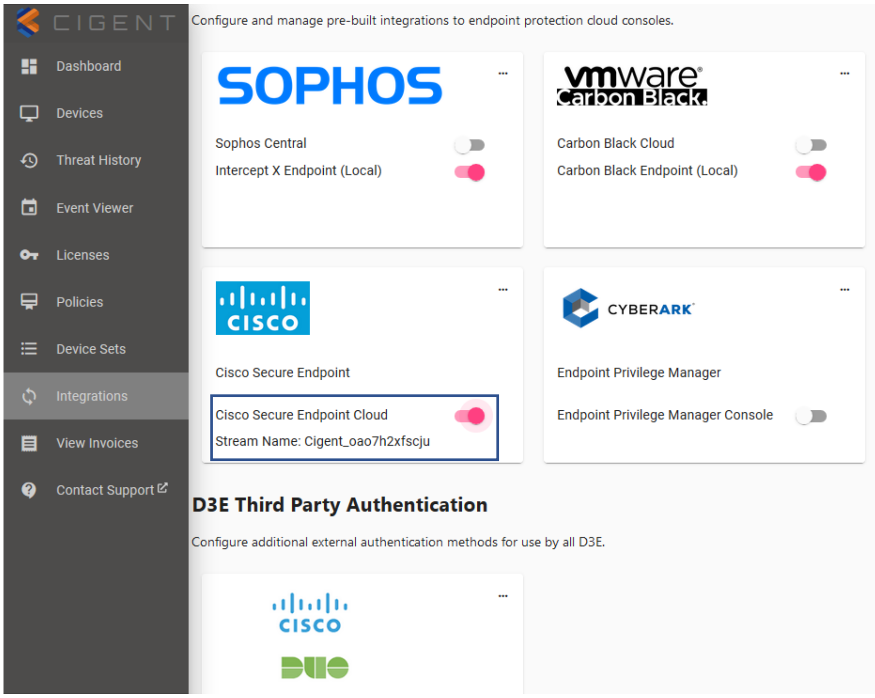
- Lock only the device that has a threat
  - This will engage Activelock only on the device with the threat
- Lock all devices in Device Sets to which the device with a threat is a member
  - If the device with a threat is a member of a Device Set (group) in the Cigent Console, all members of the group will engage Activelock. For example, if the device is a member of the HR Device Set, all members of the HR device set will engage Activelock.

- Lock all devices
    - All devices under management by the Cigent Console will engage Activelock.

Choose whether the threat can only be cleared by the Console Admininistrator (future.) Checking this option will hide the ability for the D3E user to clear the threat on the endpoint. This functionality will be enabled in an upcoming release.

Click save to return to the main Integrations page. The Cisco Secure Endpoint tile is now white indicating it has been configured.

To enable the integration, toggle the switch next to ‘Cisco Secure Endpoint Cloud’. The name of the Stream will appear once a connection to Cisco is established. This stream name will remain persistent throughout the life of the integration even if disabled. The stream connection will be deleted automatically when you disable the integration however the deletion process can take up to 1 hour to be processed by Cisco so it is recommended you wait at least an hour before re-enabling the integration.



Configure and manage pre-built integrations to endpoint protection cloud consoles.

Sophos Central
Intercept X Endpoint (Local)

Carbon Black Cloud
Carbon Black Endpoint (Local)

Cisco Secure Endpoint
Cisco Secure Endpoint Cloud
Stream Name: Cigent_oao7h2xfscju

Endpoint Privilege Manager
Endpoint Privilege Manager Console

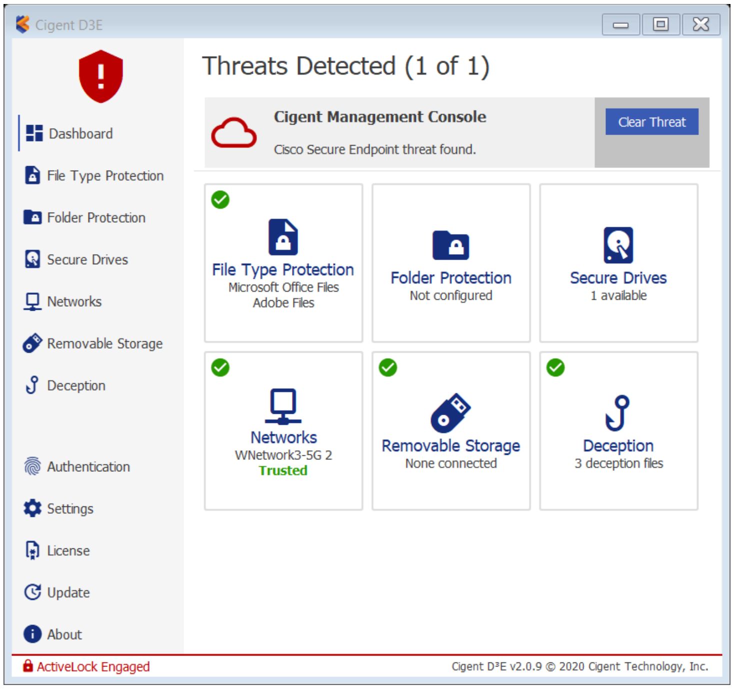
D3E Third Party Authentication

Configure additional external authentication methods for use by all D3E.

Figure 6 Enabling the Cisco Secure Endpoint Integration

Testing the Console Integration

You can test the console integration by generating a threat on an endpoint having both Cisco Secure Endpoint and Cigent D3E installed. Within a minute of generating the threat, D3E should display a message indicating ActiveLock has engaged from the console due to a Cisco Secure Endpoint detected threat.



Threats Detected (1 of 1)

Cigent Management Console

Cisco Secure Endpoint threat found.

File Type Protection
Microsoft Office Files
Adobe Files

Folder Protection
Not configured

Secure Drives
1 available

Networks
WNetwork3-5G 2
Trusted

Removable Storage
None connected

Deception
3 deception files

ActiveLock Engaged

Cigent D³E v2.0.9 © 2020 Cigent Technology, Inc.

Figure 7 Example Cisco Secure Endpoint threat in Cigent D3E

.

You can also review the threats in the Threat History page even after the threats are cleared.

Cigent D3E Endpoint Installation

Refer to “Quick Start Guide for Cigent D3E” for Cigent D3E installation guidance available on the Cigent Support site. https://support.cigent.com/kb/faq.php?id=105

Cisco Secure Endpoint agent installation

Refer to Cisco Secure Endpoint agent installation documentation for guidance.

No special setup or configuration of the Cisco Secure Endpoint agent is required to enable integration.