



Sophos Central

Sophos Central with Intercept X Endpoint

Integration - Technical Documentation

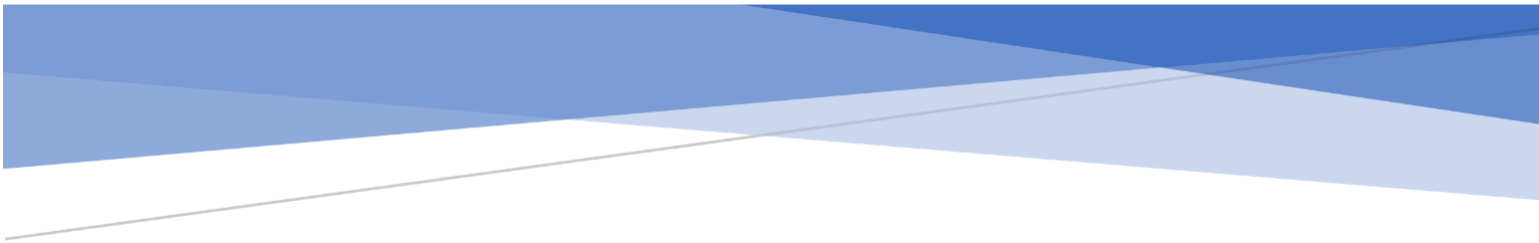
Cigent Technology Inc.

Website: www.cigent.com

Product: Dynamic Data Defense Engine
(D3E)

Version: 2.0

Date: September, 2020



Contents

Overview	2
Key Benefits	2
Cigent Product Integration Architecture	3
Sophos Integration	3
Integration Prerequisites	3
Cigent Integration Configuration	4
Cigent D3E Endpoint Installation	4
Sophos Intercept X Agent Installation	5

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 Sophos's Central management console providing increased value and security to users of both solutions.

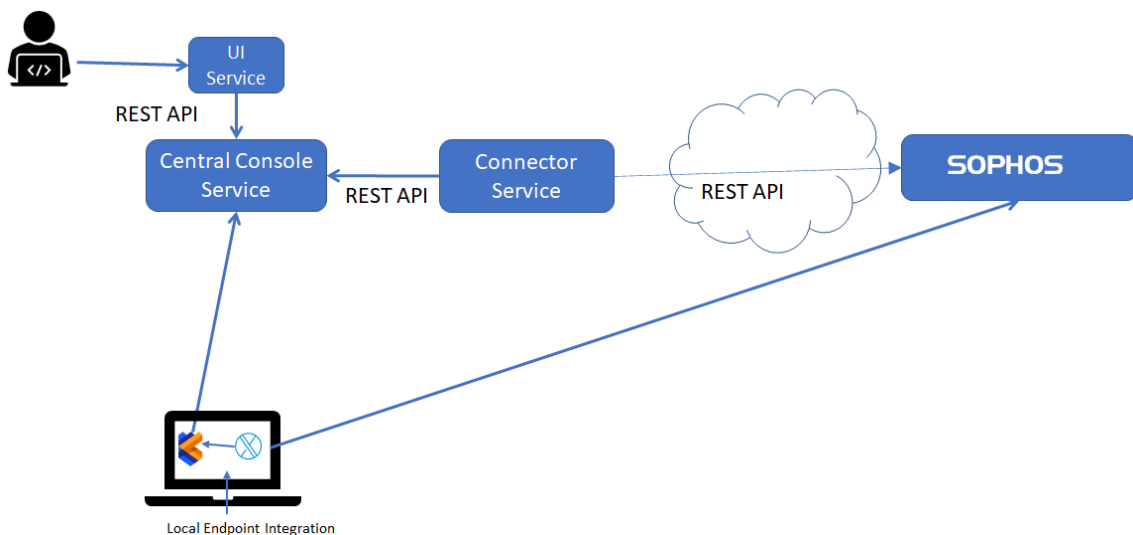
Key Benefits

Cigent D3E provides an additional response option for threats discovered by Sophos's Central with Intercept X 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 Sophos Central management console over the internet using Sophos REST APIs. No additional software or infrastructure is required by the customer to enable this integration.

Cigent High Level Architecture



Sophos Integration

Cigent Management Console users can set up, activate and delete integrations to their Sophos Intercept X instance autonomously. This integration is known as a pull integration as the Cigent Management Console will poll the Sophos Central console periodically 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

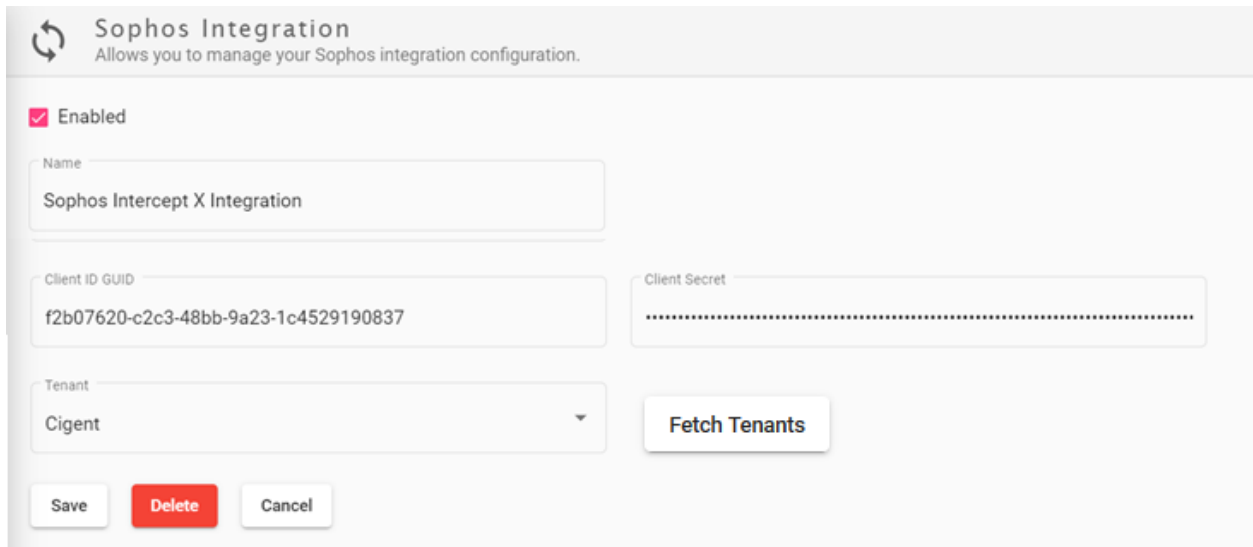
Both Cigent D3E and Sophos Intercept X endpoints need to be installed on devices on which users desire this additional layer of response.

Users must have administrative access to both Cigent and Sophos's management consoles.

Cigent Integration Configuration

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

Select 'New Sophos Integration' fill in the mandatory fields then click save.



The screenshot shows the 'Sophos Integration' configuration page. At the top, there is a header with a refresh icon, the title 'Sophos Integration', and a subtitle 'Allows you to manage your Sophos integration configuration.' Below the header, there is a checkbox labeled 'Enabled' which is checked. The main form contains several fields: 'Name' with the value 'Sophos Intercept X Integration', 'Client ID GUID' with the value 'f2b07620-c2c3-48bb-9a23-1c4529190837', and 'Client Secret' which is masked with dots. There is also a 'Tenant' dropdown menu currently showing 'Cigent' and a 'Fetch Tenants' button. At the bottom of the form, there are three buttons: 'Save', 'Delete', and 'Cancel'.

POPULATE MANDATORY FIELDS:

Name : Unique name for the Integration. This will appear on the home page along with health status.

Create an API Credential in Sophos Central following Sophos documentation at <https://docs.sophos.com/central/Custom/help/en-us/central/Custom/tasks/APICredentials.html> to obtain the **Client ID** and **Secret**. Be sure to copy the secret in the create step as it is not available afterwards.

Once you have entered the Client ID and Secret, click Fetch Tenants button. If you have an Enterprise or MSP Sophos account, a list of tenants will be populated in the dropdown list. Choose the corresponding tenant matching the Cigent tenant for which you are configuring this integration. If you are not an Enterprise or MSP user, a Default tenant will be displayed.

Click **Save** to start the integration.

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>

Sophos Central with Intercept X Endpoint agent installation

Refer to Sophos Intercept X Agent installation documentation for guidance.

No special setup or configuration of the Sophos Intercept X Agent is required to enable integration.