



Duo Security

Integration - Technical Documentation

Cigent Technology Inc.

Website: www.cigent.com

Product: Dynamic Data Defense Engine
(D3E)

Version: 2.08

Date: October, 2020

Contents

Overview	2
Key Benefits	2
Zero Trust Access Controls	2
Cigent Secure Drive	2
Active Lock Threat Response	2
Cigent Product Integration Architecture	3
Duo Integration	3
Integration Prerequisites	3
Cisco Duo Installation	4
Cigent D3E Endpoint Installation	4
Cisco Duo Integration Configuration	4
Cigent Integration Configuration	5
Cigent D3E Endpoint Configuration	6

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

Key Benefits

Zero Trust Access Controls

D3E adds Duo authentication for access to sensitive files as well as Cigent Secure Drive. Verification with Duo that the trusted user is accessing files protects against data theft, ransomware, and insider theft. Files and folders can be configured to require Duo for access when threats are detected by Active Lock.

Cigent Secure Drive

When a system has Cigent DataSafe Storage, Secure Drive can be created to store sensitive files. Secure Drive is hidden from the entire PC unless and until the trusted user enables it with Duo. When a threat is detected, the O/S locks, or the PC shuts down, Secure Drive is hidden. The only way to unlock Secure Drive is with Duo using D3E installed on the machine which created Secure Drive. It uses firmware security to protect against the vast majority of endpoint threat vectors including below-the-OS attacks such as kernel and hypervisor attacks, chip implants, boot/rootkits, and firmware/BIOS malware, as well as credential compromise, software vulnerabilities, etc.

Active Lock Threat Response

Active Lock integrates with Cisco AMP and other endpoint protection solutions to monitor for attacks on PCs. When a threat is detected, Active Lock protects designated files and Cigent Secure Drives, requiring Duo for access, until the threat is cleared.

Cigent Product Integration Architecture

Cigent D3E directly accesses the Cisco Duo Auth APIs to request and validate user requests for activities requiring a second factor authentication. Therefore, use of this authentication method requires connectivity to Cisco Duo's endpoints from the host running D3E. See Connectivity Requirements in Cisco Duo's Auth API documentation for more information (<https://duo.com/docs/authapi#endpoints>)

Cigent administrators can centrally configure and manage Cisco Duo API credentials for all D3E endpoints under management.

Cigent High Level Architecture

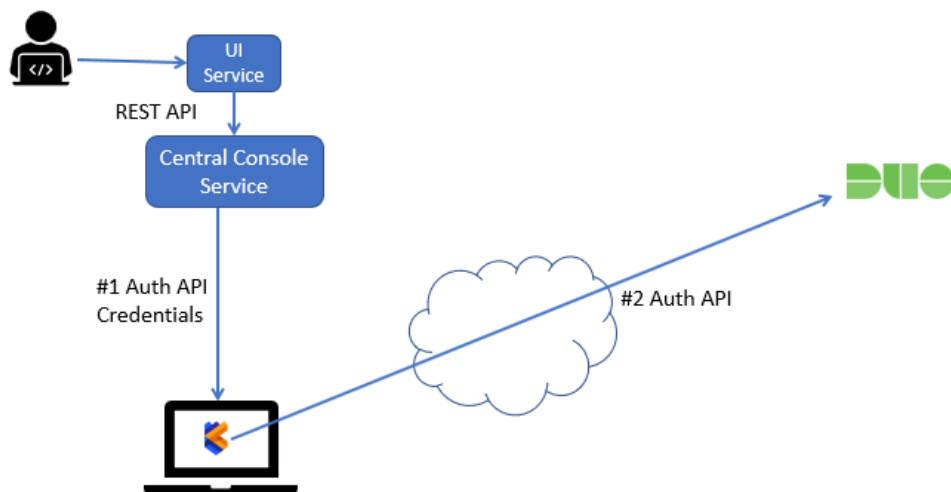


Figure 1 Cigent and Cisco Duo Integration Architecture

Duo Integration

Cigent Management Console administrators can set up, activate and delete the integration to their company's Cisco Duo account autonomously. Once setup, each D3E user can configure either Cisco Duo One Time Password or Push as a means of D3E authentication.

Integration Prerequisites

Users must have administrative access to both Cigent and Duo's management consoles. Cigent D3E must be installed on the endpoint and Cisco Duo installed on the user's device.

Cisco Duo Installation

Refer to Cisco Duo installation documentation for guidance.

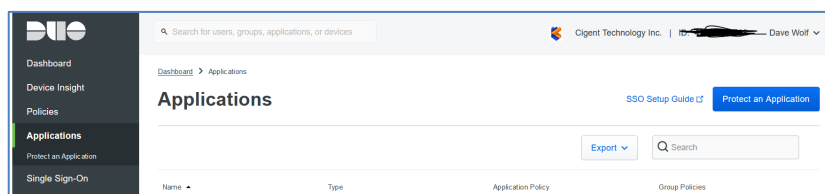
Cigent D3E Endpoint Installation

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>

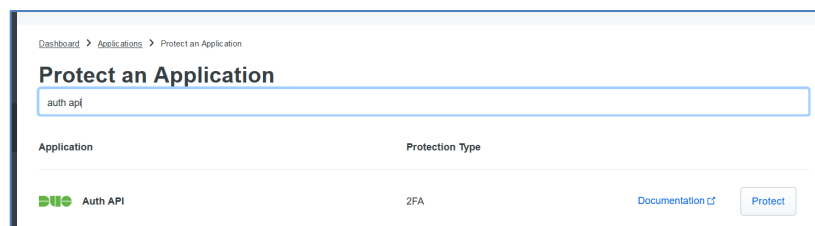
Cisco Duo Integration Configuration

Start by adding a protected application in the Cisco Duo console.

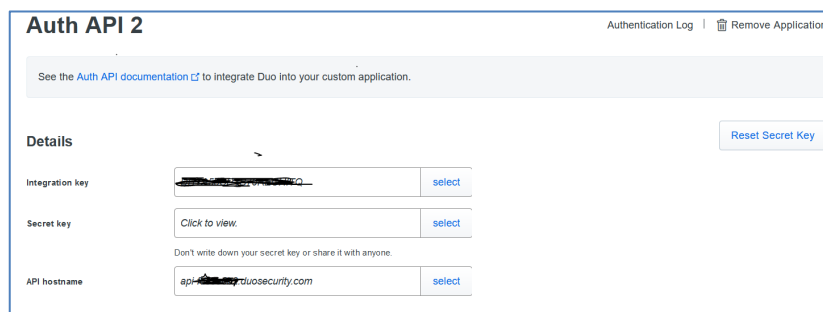
1. Log in to the Duo Admin Panel and navigate to Applications.



2. Click **Protect an Application** and locate the entry for Auth API in the applications list.



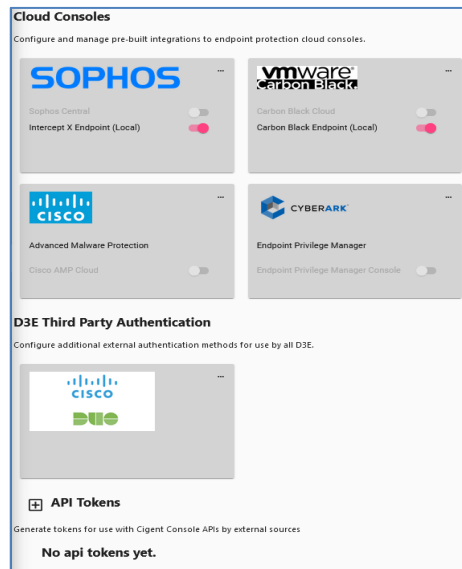
3. Click Protect. Note the **Integration Key**, **Secret Key** and **API hostname** for use in configuring the Cigent Integration in the next section.



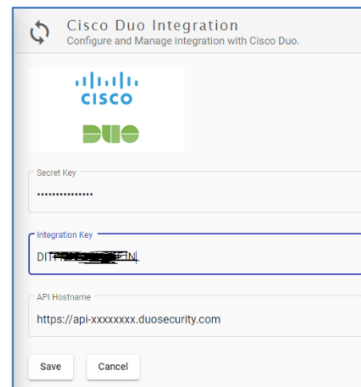
4. Configure any additional desired option and Click **Save**.

Cigent Integration Configuration

1. Login to the Cigent Management Console and navigate to Integrations.



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

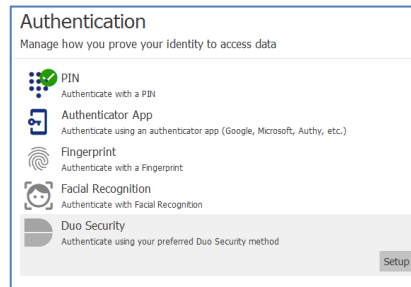


3. Enter the following information into the integration page:
 - Secret Key:** The Auth API Secret key created in previous section.
 - Integration Key:** The Auth API Integration key created in previous section.
 - API Hostname:** The API Auth API Hostname as created in previous section.
4. Click **Save** to start the integration.

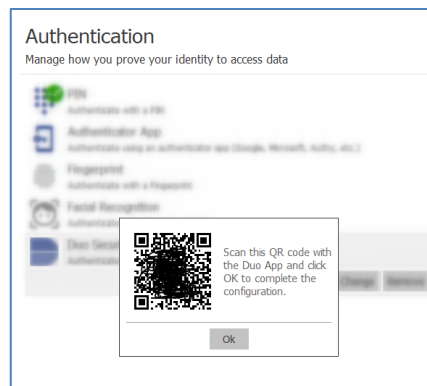
The Cisco Duo integration information will be securely sent to all currently connected D3E endpoints in the subscription or when they next connect to the Cigent Console.

Cigent D3E Endpoint Configuration

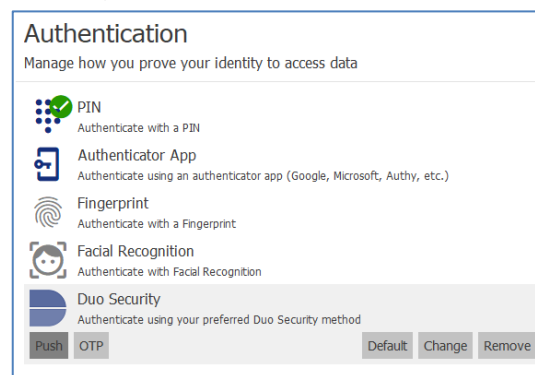
Once Cigent D3E receives the integration update, the Cisco Duo authentication option will become active in the Authentication page.



1. Click Setup and authenticate to D3E using your current authentication method.
2. Cigent D3E will display a QR code to scan from the Cisco Duo app.



3. Click '+' in the Cisco Duo application and scan the QR code.
4. A new Duo-Protect entry will appear with the Account name configured in Duo.
5. Users can now choose the method of Duo authentication they want to use OTP (One Time Password) or Push (notification.) The default is Push.



Setup Complete
