NG SIEM - CISCO DUO

Overview

This guide provides step-by-step instructions for integrating Cisco DUO multi-factor authentication (MFA) with Elastic Fleet for centralized log collection and security monitoring.

Cisco DUO is a cloud-based access security platform that provides multi-factor authentication, device health checks, and zero-trust access policies. Elastic Fleet, part of the Elastic Stack (ELK), provides a centralized management interface for deploying and managing Elastic Agents across your infrastructure.

By integrating DUO authentication logs into Elastic Fleet, security teams gain:

- Real-time visibility into authentication events across all users and devices
- Centralized log aggregation from DUO's Admin API into Elasticsearch
- Pre-built dashboards for authentication analytics and anomaly detection
- Correlation of DUO events with other security telemetry in the Elastic SIEM

Prerequisite

Before beginning the integration, ensure all of the following prerequisites are met. Incomplete prerequisites are the most common cause of integration failures.

Cisco DUO Requirements

- Verify Admin API credentials:
  - Hostname: exactly the Duo Admin API host (e.g., api-XXXXXXXX.duosecurity.com) as shown in Duo Admin Panel > **Applications** > **Protect an Application** > **Admin API**.
  - Integration key and Secret key: copy/paste fresh to rule out typos.
- Ensure the Admin API application has the required permissions:
  - “**Grant read information**” and “**Grant read log**” must be enabled for activity logs.
- Duo IP allowlist:
  - If you have IP whitelisting in Duo, add this egress IP - 50.250.130.122(es-ui.cytechint.io)

> To enable log collection from the **Cisco DUO**, provide the following information to CyTech Support:

- **API Hostname** (e.g., api-XXXXXXXX.duosecurity.com)
- **Integration Key (ikey)**
- **Secret Key (skey)**

Conclusion

The Cisco DUO integration with Elastic Fleet enables centralized visibility into authentication events across your environment. By leveraging DUO's Admin API alongside Elastic's log collection and SIEM capabilities, security teams can monitor, analyze, and respond to authentication activity in real time — all from a single platform.

Revision #3
Created 25 March 2026 01:38:40
Updated 16 April 2026 15:05:23 by Richmond Abella