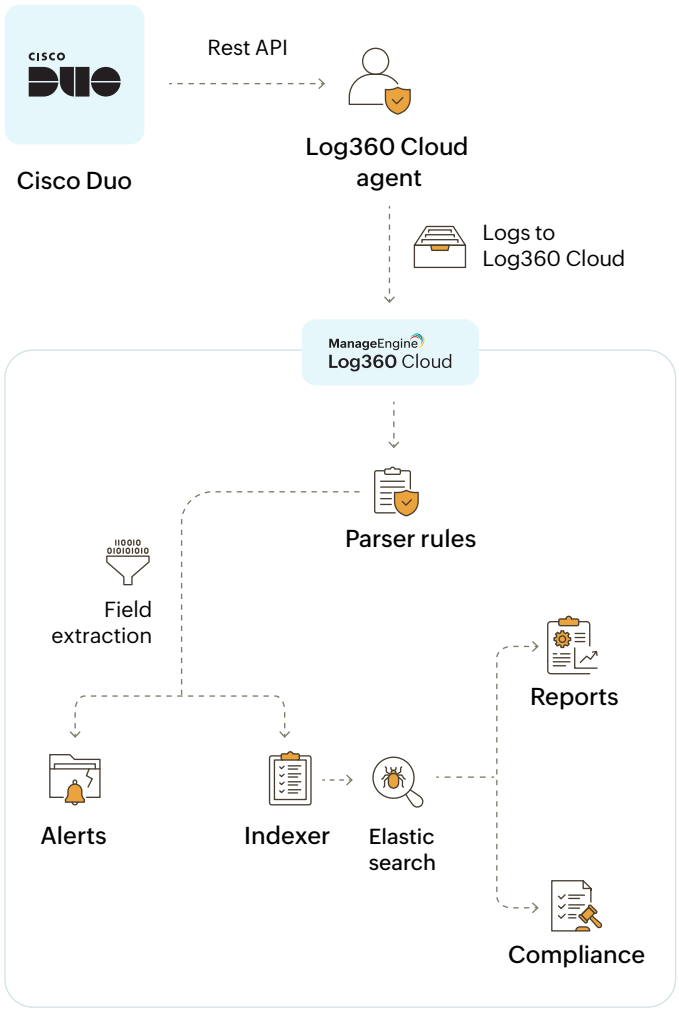
ManageEngine
Log360

DATASHEET

Strengthening access security and compliance with Log360's Cisco Duo extension

How this extension helps

ManageEngine Log360 collects, analyzes, and correlates authentication and policy change logs from Cisco Duo to enhance security monitoring and compliance enforcement. The extension provides visibility into authentication attempts, user activities, and security policy modifications, helping IT teams detect anomalies, prevent unauthorized access, and enforce strong authentication policies.



Key capabilities:

Detect brute force attacks

Monitor authentication logs to identify excessive failed login attempts that could indicate a brute-force attack. Track logins from unusual geolocations and flag suspicious authentication patterns to prevent credential-based attacks.

Investigate fraud MFA attempts

Identify MFA push request anomalies to detect MFA fatigue attacks. Provide a separate report for fraudulent authentication attempts, allowing users to review if they unknowingly approved malicious MFA requests. Trigger alerts whenever a fraud authentication event is reported.

Monitor new enrollments

Ensure that only legitimate users are enrolled in Cisco Duo MFA. Detect and analyze suspicious new enrollees that may indicate an attacker attempting to add their own devices. Generate detailed reports on all enrollment events to track potential security risks.

Identify sudden admin escalations

Capture and analyze events related to privilege escalations, including new admin account creations and role modifications. Detect unauthorized admin privilege changes that could indicate a security breach or insider threat.

Track MFA bypass policy changes

Ingest Duo administrator logs to monitor MFA bypass rule modifications. Track specific events such as user-based MFA exemptions, group-wide bypasses, and administrators modifying MFA policies for themselves or others. Detect unauthorized changes that could weaken authentication security.

Enhance security through event

Identify complex attack patterns by correlating authentication anomalies, policy changes, and access attempts. For example, you can detect scenarios where an attacker escalates privileges and simultaneously disables MFA protections to maintain persistent access.

Secure Your Cisco Duo Environment with Log360

Plug-in Cisco Duo log collector

Try Log360 Cloud

Get a personalized walkthrough

About Log360:

Log360 is a unified security platform designed for scalability, customization, and seamless integration, allowing organizations to adapt it to their unique network environments. It combines advanced threat detection, log management, user behavior analytics, and compliance reporting into a single console. Supporting on-premises, cloud, and hybrid infrastructures, Log360 enables security teams to ingest, analyze, and correlate data in real time for proactive threat detection and incident response.

About Cisco Duo

Cisco Duo is a cloud-based multi-factor authentication (MFA) solution that enhances security by requiring users to verify their identity through multiple authentication methods before accessing applications or systems. It helps organizations protect against credential-based attacks, unauthorized access, and phishing attempts by enforcing strong authentication policies, monitoring device trust, and providing adaptive access controls.

Built by: ManageEngine

Category: Cloud based authorization

Support:

Email: support@log360cloud.com

Call: +1-408-916-9393