

# Troubleshoot Health Check of Module Failed Error Code in Secure Access XDR Integration

## Contents

---

---

## Issue

The Cisco Secure Access integration with XDR fails with an HTTP 431 "Request Header Fields Too Large" error during the health check phase. The integration had previously worked successfully but suddenly began failing with this error when attempting to establish the connection using API keys generated from the Cisco Secure Access dashboard.

The specific error message appears as:

<#root>

**Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access**

This error prevents Secure Access data from being ingested into XDR, impacting security visibility and monitoring capabilities.

## Environment

- Cisco Secure Access with Advantage license
- Cisco XDR subscription
- Cisco Secure Access Tenant
- API integration using Cisco Secure Access dashboard-generated keys
- Required API scopes: Investigate > Read-Only, Reports > Read-only, Deployments > Read-only, Policies > Read/Write

## Resolution

The issue was resolved by regenerating the API key and secret in Cisco Secure Access.

Follow these steps to resolve the 431 error:

## **Step 1: Generate New API Keys**

Navigate to the Cisco Secure Access dashboard and create new API keys with the required scopes:

- Investigate: Read-Only
- Reports: Read-only
- Deployments: Read-only
- Policies: Read/Write

## **Step 2: Apply New Keys to XDR Integration**

Replace the existing API keys in the XDR Secure Access integration configuration with the newly generated keys.

## **Step 3: Verify Integration**

Test the integration to confirm successful connection. The API calls must now return HTTP 200 responses instead of the 431 error.

## **Proactive Detection and Prevention**

To identify and prevent similar 431 errors in the future:

1.- When debugging via tools like Postman or browser console, check the size column for request headers. If request headers approach or exceed 8 KB (8192 bytes), this triggers a 431 error on API gateways. External tools like jwt.io can be used to verify OAuth token size.

2.- Analyze error patterns:

- If the 431 error occurs instantly during initial handshake of a health check, it indicates the static credentials are the issue
- If the 431 error occurs only after the integration runs for several minutes, it points to cookie accumulation over subsequent retries

## Best Practices

Disable cookie or session persistence in the integration client/browser to prevent header size accumulation.

## Cause

The HTTP 431 error was caused by the specific API key and secret pair generating an unusually large or malformed authorization header when Base64 encoded for the standard HTTP Authorization header.

The cryptographic strings in the initial API key contained a sequence of characters that, when encoded, expanded into a header size that exceeded the API gateway limits, resulting in the "Request Header Fields Too Large" rejection.

When the API key was regenerated, the new cryptographic string produced a properly sized authorization header. The process of revoking and generating a new key also cleared the cached request context on the integration manager side, normalizing the header size.

## Related Content

- [Cisco Secure Access API Authentication](#)
- [Cisco Secure Access Integration into XDR](#)
- [Collect HAR Logs from XDR Console](#)
- [Cisco Technical Support & Downloads](#)