Resolve Secure Access API Remote Access Events 403 Access Forbidden Error

Contents

Issue

When attempting to retrieve VPN remote access logs using the Cisco Secure Access API endpoint **/reports/v2/remote-access-events**, users consistently receive a "403 Access Forbidden" response despite having enabled all required scopes including **reports.granularevents:read**. The issue occurs when making API calls with these parameters:

```
Authorization: Bearer <token>
Accept: application/json
Endpoint: https://api.sse.cisco.com/reports/v2/remote-access-events
Params: {"limit": 500, "from": "-6000minutes", "to": "now"}
HTTP status: 403
Events retrieved: 0
Access Forbidden
```

The error occurs despite the API key having multiple report scopes configured, and other API endpoints functioning correctly. Users report that they can successfully access other report endpoints but specifically encounter authorization issues with the remote access events endpoint.

Environment

- Cisco Secure Access API
- API endpoint: /reports/v2/remote-access-events
- API key with configured scopes: admin.vpn:read, admin.users:read, admin.alertrules:read, admin.alerts:read, admin.sentinel:read, reports.aggregations:read, reports.granularevents:read, reports.malware:read, reports.incidents:read, reports.dlp.events:read
- User with Full Admin permissions on Secure Access portal
- API integration with monitoring systems

Resolution

The issue was resolved by using the correct API scope for the remote access events endpoint. The documented scope and the actual implementation requirement differ for this specific endpoint.

Root Cause Analysis

Investigation revealed a discrepancy between the documented API scope and the actual implementation:

- **Documentation states**: The required scope is **reports.aggregations:read**.
- **Actual implementation**: The external API gateway ACL maps reports/v2/remote-access-events to **reports.utilities:read**.

Scope Testing Results

Testing confirmed this scope behavior:

```
Token Scope: reports.aggregations:read
GET /reports/v2/remote-access-events
Response: 403

Token Scope: reports.utilities:read
GET /reports/v2/remote-access-events
Response: 200

Token Scope: reports.* (All Reports)
GET /reports/v2/remote-access-events
Response: 200
```

Solution Implementation

To resolve the 403 Access Forbidden error, configure the API key with the correct scope:

Step 1: Access **API Key Management**.

Navigate to **Admin > API Keys** in the Secure Access dashboard.

Step 2: Create **New API Key**.

Click **Add API Key (+)** and configure:

- API Key Name
- Description (optional)
- Expiry date as desired

Step 3: Configure **Correct Scope**.

In the Scopes section, enable **reports.utilities:read** for remote access events functionality.

Step 4: Generate **Bearer Token**.

Create a new bearer token using the OAuth2 client-credentials flow with the updated API key.

Step 5: Test **API Call**.

Retry the API call using the working **curl** command format:

```
curl -L --request GET \
--url 'https://api.sse.cisco.com/reports/v2/remote-access-events?limit=10&from=-60minutes&to=now' \
--header 'Authorization: Bearer <Bearer token>' \
--header 'Accept: application/json'
```

Step 6: Verify **Resolution**.

Confirm the API call returns HTTP 200 status and retrieves the expected remote access events data.

Cause

The root cause is a mismatch between the documented API scope requirements and the actual implementation in the external API gateway ACL. The Cisco public documentation for GET /reports/v2/remote-access-events incorrectly states that the required access scope is **reports.aggregations:read**, when the actual implementation requires **reports.utilities:read**. This discrepancy causes authentication failures even when users believe they have configured the correct permissions based on the official documentation.

Related Content

- Cisco Secure Access API - Get Remote Access Events
- Cisco Technical Support & Downloads