Inventory Device Ipping

Endpoints Summary

Method	Path	Swagger
`GET`	`/inventory_device_ipping/{id}/`	Swagger ↗

> The Inventory Device IP Ping API provides functionality to retrieve ping test information for network devices in your inventory. This endpoint allows you to monitor network connectivity and troubleshoot device accessibility issues across your infrastructure.

Base URL: `https://control.zequenze.com/api/v1`

Authentication: All endpoints require a Bearer token:

```
Authorization: Bearer <your-api-token>
```

Overview

The Inventory Device IP Ping API category enables you to access ping test results and network connectivity data for devices in your inventory management system. This API is essential for network monitoring, device health checks, and troubleshooting connectivity issues.

Key capabilities include:

- Retrieving ping test results for specific devices
- Monitoring network device accessibility
- Accessing historical connectivity data
- Supporting network troubleshooting workflows

This endpoint is commonly used by network administrators, monitoring systems, and automated scripts that need to verify device connectivity status. The ping data helps identify network issues, validate device configurations, and ensure infrastructure reliability.

The API follows RESTful conventions and returns detailed ping information including response times, packet loss statistics, and connection status indicators.

Endpoints

GET /inventory_device_ipping/{id}/

Description: Retrieves ping test information for a specific inventory device. This endpoint returns detailed network connectivity data including ping response times, packet loss statistics, and overall connection status for the specified device.

Use Cases:

- Monitor network device health and connectivity status
- Troubleshoot network connectivity issues for specific devices
- Retrieve ping statistics for network performance analysis
- Validate device accessibility before performing maintenance operations

Full URL Example:

```
https://control.zequenze.com/api/v1/inventory_device_ipping/123/
```

Parameters:

Parameter	Type	In	Required	Description
id	integer	path	Yes	The unique identifier of the device ping record to retrieve

cURL Example:

```
curl -X GET "https://control.zequenze.com/api/v1/inventory_device_ipping/123/" \
  -H "Authorization: Bearer YOUR_API_TOKEN" \
  -H "Content-Type: application/json"
```

Example Response:

```
{
  "id": 123,
  "device_id": 456,
```

```
  "device_name": "Core Switch 01",
  "ip_address": "192.168.1.10",
  "status": "online",
  "last_ping_time": "2024-01-15T10:30:00Z",
  "response_time_ms": 2.45,
  "packet_loss_percent": 0.0,
  "ping_count": 4,
  "successful_pings": 4,
  "average_response_time": 2.38,
  "min_response_time": 2.12,
  "max_response_time": 2.67,
  "is_reachable": true,
  "last_successful_ping": "2024-01-15T10:30:00Z",
  "last_failed_ping": null,
  "consecutive_failures": 0,
  "uptime_percentage": 99.95
}
```


Response Codes:

Status	Description
200	Success - Returns the ping data for the specified device
401	Unauthorized - Invalid or missing API token
404	Not Found - Device ping record with specified ID does not exist
403	Forbidden - Insufficient permissions to access this device

---

Common Use Cases

Use Case 1: Network Health Monitoring

Monitor the connectivity status of critical network infrastructure devices by regularly checking their ping statistics. This helps identify devices that may be experiencing intermittent connectivity issues or degraded performance.

Use Case 2: Troubleshooting Network Issues

When users report connectivity problems, retrieve ping data for affected devices to quickly identify whether the issue is related to network connectivity, high latency, or packet loss.

Use Case 3: Maintenance Planning

Before performing maintenance on network devices, check their current ping status to ensure they are accessible and functioning properly. This helps avoid scheduling maintenance during existing outages.

Use Case 4: Performance Analysis

Analyze ping response times and packet loss statistics over time to identify trends in network performance and plan infrastructure improvements.

Use Case 5: Automated Alerting

Integrate ping data into monitoring systems to trigger alerts when devices become unreachable or when response times exceed acceptable thresholds.

Best Practices

- **Regular Monitoring**: Poll device ping status at appropriate intervals based on your monitoring requirements, but avoid excessive requests that could impact network performance
- **Error Handling**: Implement proper error handling for cases where devices may be temporarily unreachable or ping records may not exist
- **Threshold Management**: Establish reasonable thresholds for response times and packet loss percentages based on your network requirements and SLAs
- **Historical Tracking**: Store ping data over time to identify patterns and trends in network performance
- **Security Considerations**: Ensure API tokens are properly secured and rotated regularly, and limit access to ping data based on user permissions
- **Rate Limiting**: Be mindful of API rate limits when implementing automated monitoring solutions
- **Correlation with Events**: Correlate ping failures with other network events or maintenance activities to better understand connectivity issues

---

Revision #4
Created 2026-02-04 05:04:42 UTC by ipena@zequenze.com
Updated 2026-02-11 02:51:40 UTC by ipena@zequenze.com