Integrate Security and Automate Workflows with the Umbrella API

Contents

Introduction

This document describes the features, configuration options, and available resources for the Umbrella API platform.

Overview of Umbrella API

The Umbrella API platform provides a secure environment for building, extending, and integrating with Umbrella. Use the API to create cross-platform workflows that aggregate threat intelligence with other security solutions to expand enforcement, increase visibility, and automate incident response.

API Endpoints and Management

- All Umbrella API endpoints are hosted at api.umbrella.com.
- Endpoints are grouped by use case, each with a specific path.
- Manage API keys in the Umbrella dashboard under **Admin > API keys** or programmatically using the KeyAdmin API.

API Use Cases and Endpoint Groups

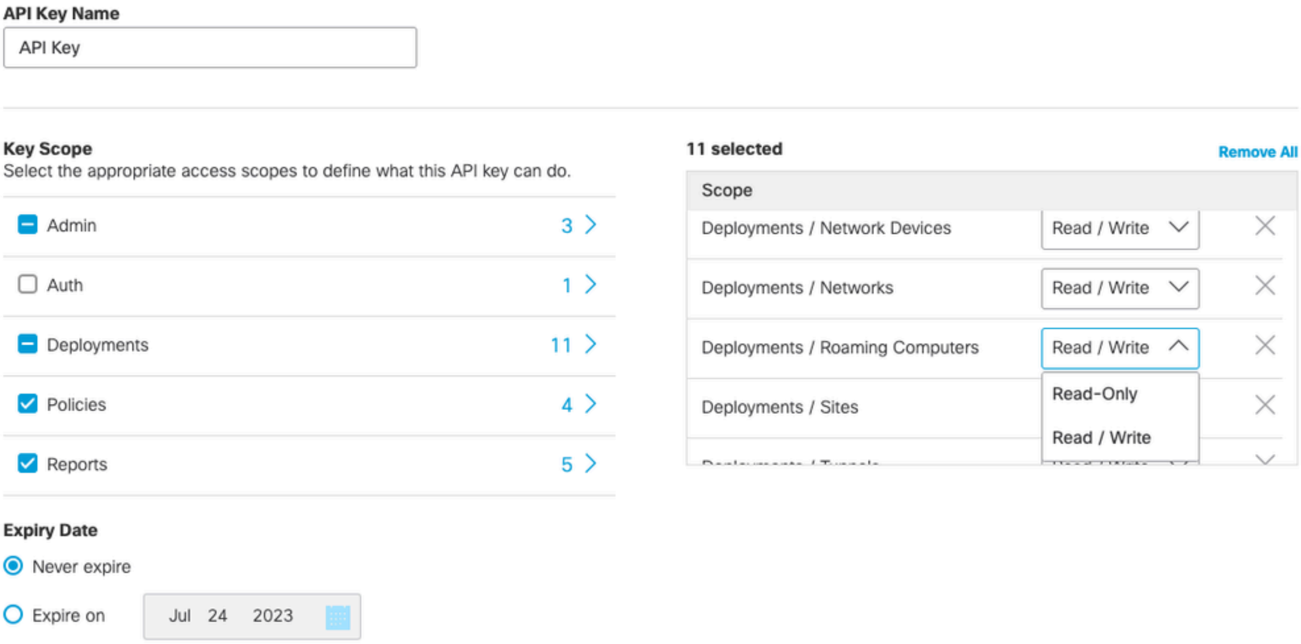
Configure each API key with granular scopes grouped under these primary use cases:

- **Admin API endpoints**: Provision and manage API keys and users, view roles, and manage customers for providers and managed providers.
- **Auth API endpoints**: Authorize integrations between Umbrella and other services.
- **Deployments API endpoints**: Provision, monitor, and manage networks and entities, securing them by configuring them in existing Umbrella policies.
- **Policies API endpoints**: Provision and manage destination lists and destinations per list.
- **Investigate API endpoints**: Research domains, IP addresses, and URLs observed by Umbrella resolvers.
- **Reports API endpoints**: Read and audit real-time security information about deployments. The App

Discovery API provides insights into cloud-based applications.

API Key Access and Expiry

- Set the access level for each scope to Read / Write or Read-Only according to the intended use.
- Configure API keys to expire on a predefined date as required.



API Key Name

API Key

Key Scope

Select the appropriate access scopes to define what this API key can do.

▬ Admin	3 >
□ Auth	1 >
▬ Deployments	11 >
☑ Policies	4 >
☑ Reports	5 >

11 selected Remove All

Scope		
Deployments / Network Devices	Read / Write	×
Deployments / Networks	Read / Write	×
Deployments / Roaming Computers	Read / Write Read-Only Read / Write	×
Deployments / Sites		×

Expiry Date

● Never expire

○ Expire on Jul 24 2023

15143392160916

Authentication and Token Lifecycle

- API credentials generate access tokens valid for 60 minutes.
- The authentication process uses the OAuth 2.0 client credentials flow.
- In multi-organization or service provider environments, parent organization API credentials can generate access tokens with the same scopes for a specified child organization during authorization.

Documentation and Resources

- Access comprehensive instructions and use case documentation.
- Each API use case is documented under API Reference.
- All endpoints and parameters are listed in the **OpenAPI Specification**, linked at the bottom of each use case overview.
- If you use Legacy Umbrella APIs, review the API Migration Guide.
- Use the Postman Collection for the Umbrella API for initial testing.
- Explore additional resources, learning labs, and a Sandbox for API testing in the Cloud Security section of the Cisco developer page.

Support

For questions or additional assistance with the Umbrella API, contact Umbrella support.