Cisco Identity Public API

Public API

Fetch end user information and react to Cisco Identity threat detection using Cisco Identity.

Authorization

Prerequisites

Generate client API credentials:

1. Sign in to **Cisco Identity**.
2. From the Integrations tab, click **Add Integration**.
3. Scroll down and click **Add API Client**.
4. Provide a **Name** and **Description**.
5. Click **Save and generate credentials**.
6. Click **Copy all** to copy the credentials to your clipboard.

Exchange the client credentials for an access token

1. Send a POST request to the **tokenUrl** with the following body:

```
{
  "client_id": "<client ID of the API client>",
  "client_secret": "<client secret of the API client>",
  "grant_type": "client_credentials"
}
```

Note: API clients created before September 2025 may require an additional `audience` field (audience of the API client) in the body of the POST request. If you are requesting a token for an existing API Client that originally included an `audience` , please ensure that this field is present in your request to avoid errors.

You can check a particular API client's settings via the Integrations page in Cisco Identity to confirm whether the `audience` field is required.

2. Extract the **access_token** from the response. An access token is valid for 10 hours.
3. When invoking the public API requests set an **Authorization** header with the value `Bearer <value ofaccess_token>`

Using a Postman Collection

Import the attached Postman collection JSON file and follow the instructions in the collection **overview** tab.

APIs

Schema Types

Query

Field	Argument	Type	Description
ping		Boolean!	Ping the API to check if it is up and running.
getEndUserState		EndUserState!	**Note: This endpoint is no longer being maintained. Please use GetEndUser.** Fetch a concise summary of end-user information, including key fields and relevant details. Use this query when you want to get a basic end-user digest.
login		String!	End-user's email address.
email		String!	End-user primary email address.
getEndUsersByIp		GetEndUsersByIpConnection!	Retrieve end-users associated with a specified IP address.
	ipAddress	String!	IP Address.
	pageSize	Int	Number of items per page. Default pageSize is 100. Max pageSize is 500.
	pageToken	String	Token for paginating through the result set.
getEndUser		GetEndUserOutput!	Fetch end-user's detailed information, including including

			devices, integrations, factors and more. Use this query when you want to get a comprehensive end-user details.
	login	String!	End-user's email address.
listEndUsers		ListEndUsersConnection!	Fetch the list of end-users. Use this query to retrieve a large number of items using paging. The default page size is 100, and the maximum page size is 500. Page token is used to retrieve the next page. If not provided, the first page is retrieved.
	input	ListEndUsersInput!	Input data for end-users listing.
	pageSize	Int	Number of items per page. Default pageSize is 100. Max pageSize is 500.
	pageToken	String	Token for paginating through the result set.
listEndUserUpdates		EndUserUpdatesConnection!	Fetch the list of updates to selected end-user properties (such as `endUserTrustScore`) since the specified date. Use this query to retrieve large result sets with paging. The default page size is

			100, and the maximum is 500. Use the page token to request the next page; if no token is provided, the first page is returned.
	input	ListEndUserUpdatesInput	Input data for end-user updates listing.
	pageSize	Int	Number of items per page. Default pageSize is 100. Max pageSize is 500.
	pageToken	String	Token for paginating through the result set.

Mutation

Field	Argument	Type	Description
registerWebhookWithApiKey		ID!	Register a Webhook Notification Target with an API key as a target for Failed Check findings. See more at https://docs.oort.io/integrations/webhooks
	input	RegisterWebhookWithApiKey!	Input data for registering a webhook with an API key.
registerWebhookWithDuoSecurityClient		ID!	Register a Webhook Notification Target with Duo Security Client as a target for Failed Checks findings.
	input	RegisterWebhookWithDuoSecurityClient!	Input data for registering a webhook with an Duo Security Client.

unregisterWebhook		Boolean!	Unregister a Webhook Notification Target.
	id	ID!	ID of the webhook to unregister.

Objects

ConnectivityStatus

Field	Argument	Type	Description
statusCode		Int!	
payload		String	
reason		String	

DailySchedule

Field	Argument	Type	Description
hour		Int!	
minute		Int!	

EndUserRef

Represents a reference to an end-user.

Field	Argument	Type	Description
id		ID!	The end-user ID in Cisco Identity.
displayName		String!	The end-user's display name.
login		String!	End-user's email address.
referenceUrl		String	End-user's URL in Cisco Identity.

EndUserState

Note: This endpoint is no longer being maintained. Please use GetEndUser.

Represents a concise summary of end-user information, including key fields and relevant details.

Field	Argument	Type	Description
id		ID!	The end-user ID in Cisco Identity.
displayName		String!	The end-user's display name.
login		String!	End-user's email address.
employeeId		[String!]	List of employee IDs associated with the end-user in the Identity Provider and HR systems.
status		String!	The aggregated end-user status in the identity providers.
userTypeClassification		UserTypeClassification	The end-user classification in Cisco Identity.
managerLogin		String	End-user's manager email address.
ipAddresses		IpAddressInfo!	List of IP Addresses used by the end-user.
phoneNumber		String	End-user's phone number.
unusedApplications		[String!]	Names of applications the

			end-user has access and did not access in the past 30 days.
usedApplications		[String!]	Names of applications the end-user has access and accessed in the past 30 days.
usedFactors		[String!]	Authentication factors used by the end-user.
referenceUrl		String	End-user's URL in Cisco Identity.
registeredLocationDetails		GeoLocation	The end-user's registered location
workingLocationDetails		LocationWithPrevalence!	List of the locations the end-user works in.

FeatureExplainabilityItem

Field	Argument	Type	Description
featureId		String!	
details		KeyValuePair!	

GeoCoordinates

Field	Argument	Type	Description
latitude		Float	
longitude		Float	

GeoLocation

IP Address geolocation information.

Field	Argument	Type	Description
city		String	The city name.
state		String	The state name.
country		String	two-letter country code defined in ISO 3166-1.

GetEndUserOutput

Field	Argument	Type	Description
endUserDetails		PublicEndUserDetails!	The unified end-user details across all providers.
providerEndUserDetails		[PublicProviderEndUserDetails!]!	The array of end-user details by provider.

GetEndUsersByIpConnection

End-users associated with a specified IP address.

Field	Argument	Type	Description
items		[EndUserRef!]!	Itemized list of end-users associated with a specified IP address.
pageToken		String	Token for paginating through the result set. If pageToken is undefined, there are no more results to fetch.

GroupExplainabilityItem

Field	Argument	Type	Description
groupId		TrustScoreGroupId!	
weight		TrustScoreWeight	Normalized trust score weight
details		FeatureExplainabilityItem!	

IpAddressInfo

IP Address information.

Field	Argument	Type	Description
ipAddress		String!	IP Address.
location		GeoLocation	IP Address geolocation information.

ItemList

Field	Argument	Type	Description
listType		ListType!	
items		[String!]!	

KeyValuePair

Field	Argument	Type	Description
key		String!	
value		String!	

LabelCount

Field	Argument	Type	Description
value		String!	
count		Int!	

ListEndUsersConnection

End-users list.

Field	Argument	Type	Description
items		[PublicEndUser!]!	Itemized list of end-users.
pageToken		String	Token for paginating through the result set. If pageToken is undefined, there are no more results to fetch.

EndUserUpdatesConnection

Changes for a predefined subset of end-user properties.

Field	Argument	Type	Description
items		[PublicEndUserUpdate!]!	Itemized list of end-user properties update
pageToken		String	Token for paginating through the result set. If pageToken is undefined, there are no more results to fetch.

LocationWithPrevalence

Field	Argument	Type	Description
location		GeoLocation!	
userLocationPrevalence		Float!	

PublicEndUser

Represents end-user basic data.

Field	Argument	Type	Description

id	ID!	The end-user ID in Cisco Identity.
displayName	String	The end-user's display name.
login	String!	End-user's email address.
emails	[String!]	List of emails associated with the end-user in the IdP and HR system.
status	EndUserStatus	The unified status of the end-user across all providers.
company	String	The company the end-user belongs to.
department	String	The department the end-user belongs to.
title	String	The end-user's title.
userTypeClassification	UserTypeClassification	The unified classification of the end-user type across all providers.
employeeIds	[String!]	List of employee IDs associated with the end-user in the Identity Provider and HR systems.
userKeys	[String!]	List of user keys associated with

		the end-user in the Identity Provide
linkedEndUserLogins	[String!]	List of linked end-users' logins.
groupNames	[String!]	List of names of the groups the end-user is a member of. Maximum 10 items.
hasMoreGroups	Boolean!	The indication if more groups exist for the end-user.
phoneNumbers	[String!]	The end-user's phone numbers used for authentication.
managerLogin	String	The end-user's manager login.
devices	PublicUserDevice	List of devices the end-user uses.
mfaEnabled	Boolean	Indicates if the MFA is enabled for the end-user.
lastSignIn	PublicUserSignInInfo	The last sign details for the end-user.
lastActive	AWSDateTime	The last active timestamp for the end-user.
failingChecks	[String!]	The checks that the end-user has

			failed.
firstCreatedDate		AWSDateTime	The first created date of the account across all providers.
providers		[Provider!]!	List of provider types for the integrations the end-user data is collected from.
referenceUrl		String!	End-user's URL in Cisco Identity.
endUserTrustScore		PublicEndUserTrustScore	

PublicEndUserUpdate

Field	Argument	Type	Description
id		ID!	The end-user ID in Cisco Identity.
login		String!	End-user's email address.
userKeys		[String!]!	List of user keys associated with the end-user in the Identity Provide
failingChecks		[String!]	The checks that the end-user has failed.
endUserTrustScore		PublicEndUserTrustScore	

PublicEndUserDetails

Represents end-user data.

Field	Argument	Type	Description

id	ID!	The end-user ID in Cisco Identity.
displayName	String!	The end-user's display name.
login	String!	End-user's email address.
emails	[String!]	List of emails associated with the end-user in the IdP and HR system.
status	EndUserStatus!	The unified status of the end-user across all providers.
userIds	[String!]	List of end-user IDs associated with the end-user in the Identity Provider and HR systems.
company	String	The company the end-user belongs to.
department	String	The department the end-user belongs to.
title	String	The end-user's title.
userTypeClassification	UserTypeClassification	The unified classification of the end-user type across all providers.
employeeIds	[String!]	List of employee IDs associated

		with the end-user in the Identity Provider and HR systems.
linkedEndUserLogins	[String!]	List of linked end-users' logins.
groupNames	[String!]	List of names of the groups the end-user is a member of.
phoneNumbers	[String!]	The end-user's phone numbers used for authentication.
managerLogin	String	The end-user's manager login.
devices	PublicUserDevice!	List of devices the end-user uses.
mfaEnabled	Boolean	Indicates if the MFA is enabled for the end-user.
lastSignIn	PublicUserSignInInfo	The last sign details for the end-user.
lastActive	AWSDateTime	The last active timestamp for the end-user.
firstCreatedDate	AWSDateTime	The first created date of the account across all providers.
failingChecks	[String!]	The checks that the end-user has failed.

referenceUrl		String!	End-user's URL in Cisco Identity.
endUserTrustScore		PublicEndUserTrustScore	

PublicEndUserTrustScore

Field	Argument	Type	Description
levelOfTrust		LevelOfTrust!	
scoreExplainabilitySummary		PublicScoreExplainabilitySummary	
meaningfulExplainability		String!	Human readable explainability of the score
lastUpdated			The last score evaluation timestamp

PublicProviderEndUserDetails

Field	Argument	Type	Description
userId		String!	The end-user userId.
provider		Provider!	The type of the provider.
firstName		String	The end-user's first name.
lastName		String	The end-user's last name.
displayName		String	The end-user's display name.
login		String!	End-user's email address.

status	EndUserStatus!	The unified status of the end-user across all providers.
company	String	The company the end-user belongs to.
department	String	The department the end-user belongs to.
title	String	The end-user's title.
userTypeClassification	UserTypeClassification	The unified classification of the end-user type across all providers.
employeeId	String	Employee ID associated with the end-user in the Identity Provider and HR systems.
managerLogin	String	The end-user's manager login.
mfaEnabled	Boolean	Indicates if the MFA is enabled for the end-user.
lastSignIn	PublicUserSignInInfo	The last sign details for the end-user.
creationDate	AWSDateTime	The creation date of the account across.
lastUpdated	AWSDateTime	The last updated date of the

			account.
isAdmin		Boolean	Indicates if the user is an admin in this provider.
additionalDetails		KeyValuePair!	A collection of provider-specific properties represented as key-value pairs. This field contains supplementary details that may vary depending on the provider.

PublicRiskyActivityCounts

Field	Argument	Type	Description
total		Int!	
levelOfTrust		LabelCount!	counts grouped by the level of trust

PublicScoreExplainabilitySummary

Field	Argument	Type	Description
riskyActivityCounts		PublicRiskyActivityCounts!	
combinedScoreExplainability		GroupExplainabilityItem!	

PublicUserDevice

Field	Argument	Type	Description
deviceId		String!	The device ID.
displayName		String	The device display name.
os		OsType	The device OS type.
lastSeen		AWSDateTime	The last time the end-user used the

			device.
deviceType		DeviceType	The device type: access or authentication.
provider		Provider!	The provider type.

PublicUserSignInInfo

Field	Argument	Type	Description
timestamp		AWSDateTime!	The end-user's sign-in timestamp.
result		String	The end-user's sign-in result.
reason		String	The end-user's sign-in failure reason.
ipAddress		String	The end-user's sign-in IP address.
location		GeoLocation	The end-user's sign-in location.

TotalHits

Field	Argument	Type	Description
count		Int!	
relation		String!	

TotalWithMedian

Field	Argument	Type	Description
total		Int!	
median		Float!	

TypedKeyValuePair

Field	Argument	Type	Description

key	String!
value	String!
type	String
minValue	Int
maxValue	Int

Inputs

DailyScheduleInput

Field	Type	Description
hour	Int!	
minute	Int!	

ItemListInput

Field	Type	Description
listType	ListType!	
items	[String!]!	

KeyValuePairInput

Field	Type	Description
key	String!	
value	String!	

ListEndUsersInput

Field	Type	Description
orderBy	[OrderBy!]	

ListEndUserUpdatesInput

Field	Type	Description
orderBy	[OrderBy!]	

since	AWSDateTime!	The date and time from which to start listing updates. Must be within last 7 days.

OrderBy

Field	Type	Description
name	String!	
order	Order	

RegisterWebhookWithApiKey

Input for registering a webhook with an API key.

Field	Type	Description
name	String!	Part of the name of the webhook. The webhook name is a combination of the name and a random suffix for uniqueness.
endpoint	String!	The URL of the webhook endpoint.
apiKeyName	String!	The name of the API key to use for the webhook. Sent in the webhook payload headers as the header name.
apiKey	String!	The value of the API secret key to use for the webhook. Sent in the webhook payload headers as the header value.
checkIds	[String!]!	The list of Cisco Identity check IDs to subscribe to.

RegisterWebhookWithDuoSecurityClient

Field	Type	Description

name	String!	Part of the name of the webhook. The webhook name is a combination of the name and a Webhook prefix
duoIntegrationInstanceId	String!	The ID of the existing Duo integration instance.
checkIds	[String!]!	The list of Cisco Identity check IDs to subscribe to.

TimestampRange

Field	Type	Description
startTimestamp	String!	
endTimestamp	String	

Enums

DataType

Value	Description
APPS	
APPS_TO_GROUPS	
APPS_TO_USERS	
EVENT_LOGS	
AUDIT_LOGS	
ACTIVITY_LOGS	
ADDITIONAL_LOGS	
FACTORS_TO_USERS	
GROUPS	
GROUPS_TO_USERS	
DIRECT_REPORTS	
DIRECTORY_ROLES	

IDP

USERS

DEVICES

RISKY_USERS

RISKY_USER_EVENTS

NAMED_LOCATIONS

IP_CIDR_LIST

IP_THREAT_INSIGHTS

POLICIES

POLICY_RULES

SERVICE_PRINCIPAL

API_TOKEN

EVENT_HUB

AUTHENTICATORS

AUTHENTICATORS_TO_USERS

SIGNIN_LOGS

LOGIN_HISTORY

LOGIN_GEO

AUTH_CONFIG

USER_LOGIN

END_USER_LOGINS

PROFILES

CONDITIONAL_ACCESS_POLICY

PROVISIONING_EVENTS

ORGANIZATIONS

USER_EMAILS

USER_ENTERPRISE_EMAILS

COLLABORATORS

MEMBER_INVITATIONS

COLLABORATOR_INVITATIONS

PERMISSION_SETS

USER_SCHEMA

MAILBOX_SETTINGS

MESSAGE_RULES

DEVICE_AUDIT_EVENTS

AUTH_API

ENDPOINTS

TOKENS

WEBAUTHNCREDENTIALS

BYPASS_CODES

SIGNIN_ACTIVITY

DeviceType

Value	Description
ACCESS	
AUTHENTICATION	

EndUserStatus

Value	Description
ACTIVE	
INACTIVE	
DEPROVISIONED	

LOCKED_OUT
PASSWORD_EXPIRED
PROVISIONED
RECOVERY
STAGED
SUSPENDED
INCONSISTENT
DELETED
DISABLED
BLOCKED
TRANSIENT
UNKNOWN

HttpMethod

Value	Description
GET	
POST	
PUT	
HEAD	
OPTIONS	
PATCH	
DELETE	

LevelOfTrust

Value	Description
TRUSTED	Indicates exceptional safety

FAVORABLE	Indicates a level of safety
NEUTRAL	Displaying neither positive or negative behavior. However, has been evaluated.
QUESTIONABLE	Displaying behavior that may indicate risk, or could be undesirable
UNTRUSTED	Displaying behavior that is exceptionally bad, malicious, or undesirable
UNKNOWN	Not previously evaluated, or lacking features to assert a threat level verdict

ListType

Value	Description
allow	
block	
ignore	
include	

Order

Value	Description
asc	
desc	

OsType

Value	Description
WINDOWS	
WINDOWS_MOBILE	
MACOS	
IOS	
ANDROID	

LINUX
CHROME_OS
UNKNOWN

Provider

Value	Description
AUTH0	
AWS	
AZURE_AD	
OKTA	
HRIS	
SLACK	
DUO	
G_SUITE	
WORKDAY	
SALESFORCE	
GIT_HUB	

TrustScoreGroupId

Value	Description
ACCOUNT_LOGIN_BEHAVIOR	
ACTIONS_IN_SESSION	
APPLICATION	
DEVICE	
EXTERNAL_THREAT	
FIRST_FACTOR	
SECOND_FACTOR	

NETWORK
PERMISSION
SESSION
ACCOUNT_VALIDITY

TrustScoreWeight

Value	Description
NO_RISK	
LOW_RISK	
MEDIUM_RISK	
HIGH_RISK	

UserTypeClassification

Value	Description
INTERNAL	
EXTERNAL	
MISSING	
UNCLASSIFIED	
INCONSISTENT	
SERVICE_ACCOUNT	
SHARED_MAILBOX	
LINKED_USER_ACCOUNT	
CONFERENCE_ROOM	
EQUIPMENT_MAILBOX	
OTHER_MAILBOX	

WorkflowState

Value	Description
SUCCESS	
ERROR	
UNKNOWN	
RUNNING	

Scalars

AWSDate

The AWSDate scalar type represents a valid extended ISO 8601 Date string. In other words, this scalar type accepts date strings of the form YYYY-MM-DD. This scalar type can also accept time zone offsets. For example, 1970-01-01Z, 1970-01-01-07:00 and 1970-01-01+05:30 are all valid dates. The time zone offset must either be Z (representing the UTC time zone) or be in the format ±hh:mm:ss. The seconds field in the timezone offset will be considered valid even though it is not part of the ISO 8601 standard.

AWSDateTime

The AWSDateTime scalar type represents a valid extended ISO 8601 DateTime string. In other words, this scalar type accepts datetime strings of the form YYYY-MM-DDThh:mm:ss.sssZ. The field after the seconds field is a nanoseconds field. It can accept between 1 and 9 digits. The seconds and nanoseconds fields are optional (the seconds field must be specified if the nanoseconds field is to be used). The time zone offset is compulsory for this scalar. The time zone offset must either be Z (representing the UTC time zone) or be in the format ±hh:mm:ss. The seconds field in the timezone offset will be considered valid even though it is not part of the ISO 8601 standard.

AWSEmail

The AWSEmail scalar type represents an Email address string that complies with RFC 822. For example, username@example.com is a valid Email address.

AWSIPAddress

The AWSIPAddress scalar type represents a valid IPv4 or IPv6 address string.

AWSJSON

The AWSJSON scalar type represents a JSON string that complies with RFC 8259.

Maps like {\" upvotes\" : 10}, lists like [1,2,3], and scalar values like \" AWSJSON example string\" , 1, and true are accepted as valid JSON. They will automatically be parsed and loaded in the resolver mapping templates as Maps, Lists, or Scalar values rather than as the literal input strings. Invalid JSON strings like {a: 1}, {'a': 1} and Unquoted string will throw

GraphQL validation errors.

AWSPhone

The AWSPhone scalar type represents a valid Phone Number. Phone numbers are serialized and deserialized as Strings. Phone numbers provided may be whitespace delimited or hyphenated. The number can specify a country code at the beginning but this is not required.

AWSTime

The AWSTime scalar type represents a valid extended ISO 8601 Time string. In other words, this scalar type accepts time strings of the form hh:mm:ss.sss. The field after the seconds field is a nanoseconds field. It can accept between 1 and 9 digits. The seconds and nanoseconds fields are optional (the seconds field must be specified if the nanoseconds field is to be used). This scalar type can also accept time zone offsets.

For example, 12:30Z, 12:30:24-07:00 and 12:30:24.500+05:30 are all valid time strings.

The time zone offset must either be Z (representing the UTC time zone) or be in the format hh:mm:ss. The seconds field in the timezone offset will be considered valid even though it is not part of the ISO 8601 standard.

AWSTimestamp

The AWSTimestamp scalar type represents the number of seconds that have elapsed since 1970-01-01T00:00Z. Timestamps are serialized and deserialized as numbers. Negative values are also accepted and these represent the number of seconds till 1970-01-01T00:00Z.

AWSURL

The AWSURL scalar type represents a valid URL string. The URL may use any scheme and may also be a local URL (Ex: http://localhost/). URLs without schemes are considered invalid. URLs which contain double slashes are also considered invalid.

Boolean

The `Boolean` scalar type represents `true` or `false`.

Float

The `Float` scalar type represents signed double-precision fractional values as specified by IEEE 754.

ID

The `ID` scalar type represents a unique identifier, often used to refetch an object or as key for a cache. The ID type appears in a JSON response as a String; however, it is not intended to be human-readable. When expected as an input type, any string (such as `"4"`) or integer (such as `4`) input value will be accepted as an ID.

Int

The `Int` scalar type represents non-fractional signed whole numeric values. Int can represent values between -(2^31) and 2^31 - 1.

String

The `String` scalar type represents textual data, represented as UTF-8 character sequences. The String type is most often used by GraphQL to represent free-form human-readable text.