

Cortex XDR Endpoint Verification for Google BeyondCorp Marketplace Deployment User Guide

PRE-REQUIREMENTS

- **Enable APIs:**
 - Used in deployment:
 - Pub/Sub
 - Scheduler
 - Cloud Functions
 - Cloud Spanner
 - Used for deployment:
 - Compute Engine
 - Cloud Build
 - Cloud Deployment Manager V2
 - Cloud Runtime Configuration
 - Used by integration:
 - Cloud Identity
- **Grant below two service accounts necessary roles for the build:**
 - **PROJECT_ID**-compute@developer.gserviceaccount.com -add storage object admin IAM role
 - **PROJECT_ID**@cloudservices.gserviceaccount.com - add storage object admin IAM role
- **Enable IAP access control**
- **License from Google:**
 - Cloud Identity Premium
 - BeyondCorp Enterprise

Overview

Google announced [BeyondCorp Remote Access](#), a cloud-based solution that helps make access to internal applications easier and more secure. Palo Alto Networks partners with Google to enhance the Zero Trust security in consideration of the risk factors of remote users' endpoint devices. Cortex XDR Endpoint Verification for Google

BeyondCorp by Palo Alto Networks provides XDR endpoint risk exposures rating to Google Endpoint Management. Cortex XDR Endpoint Verification allows you control your critical applications access based on XDR endpoint risk exposure rating.

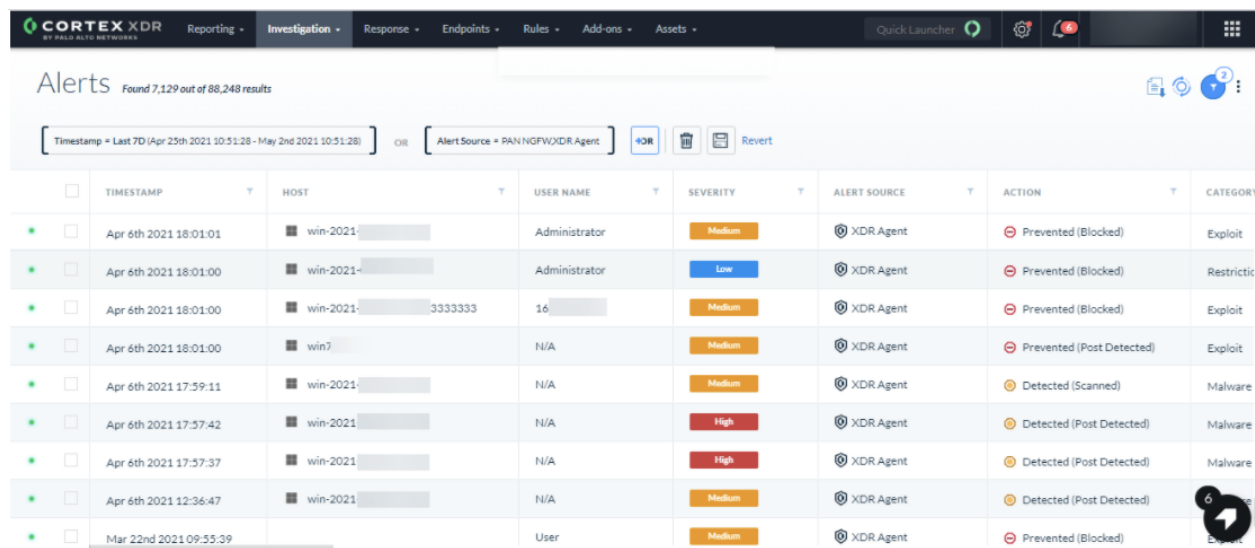
Cortex XDR and XDR Health Score for Endpoint

Cortex® XDR™ is the world's first extended detection and response platform that gathers and integrates all security data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency.

The Cortex XDR agent safeguards endpoints from malware, exploits, and fileless attacks with industry-best, AI-driven local analysis and behavior-based protection. Organizations can stop never-before-seen threats with a single cloud-delivered agent for endpoint protection, detection, and response.

XDR Health Score for Endpoint

Cortex XDR Alerts page consolidates non-informational alerts from your detection sources including the XDR agents running at the endpoints.



The screenshot shows the Cortex XDR Alerts page with a search bar and a table of alerts. The table has the following columns: Timestamp, Host, User Name, Severity, Alert Source, Action, and Category. The alerts are filtered by 'Timestamp = Last 7D (Apr 25th 2021 10:51:28 - May 2nd 2021 10:51:28)' and 'Alert Source = PAN/NGFW/XDR Agent'. The table shows several alerts with various severities (Low, Medium, High) and actions (Prevented (Blocked), Detected (Scanned), Detected (Post Detected)).

	TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
<input type="checkbox"/>	Apr 6th 2021 18:01:01	win-2021-	Administrator	Medium	XDR Agent	Prevented (Blocked)	Exploit
<input type="checkbox"/>	Apr 6th 2021 18:01:00	win-2021-	Administrator	Low	XDR Agent	Prevented (Blocked)	Restrictio
<input type="checkbox"/>	Apr 6th 2021 18:01:00	win-2021-3333333	16	Medium	XDR Agent	Prevented (Blocked)	Exploit
<input type="checkbox"/>	Apr 6th 2021 18:01:00	win7	N/A	Medium	XDR Agent	Prevented (Post Detected)	Exploit
<input type="checkbox"/>	Apr 6th 2021 17:59:11	win-2021-	N/A	Medium	XDR Agent	Detected (Scanned)	Malware
<input type="checkbox"/>	Apr 6th 2021 17:57:42	win-2021-	N/A	High	XDR Agent	Detected (Post Detected)	Malware
<input type="checkbox"/>	Apr 6th 2021 17:57:37	win-2021-	N/A	High	XDR Agent	Detected (Post Detected)	Malware
<input type="checkbox"/>	Apr 6th 2021 12:36:47	win-2021-	N/A	Medium	XDR Agent	Detected (Post Detected)	Exploit
<input type="checkbox"/>	Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	Prevented (Blocked)	Exploit

Cortex XDR Endpoint Verification calculates XDR Health Score for each endpoint and stores it in a database at your Google Cloud project. The calculation uses the number of incidents and the serenity of the incident associated with an endpoint. Here is the possible XDR Health Score:

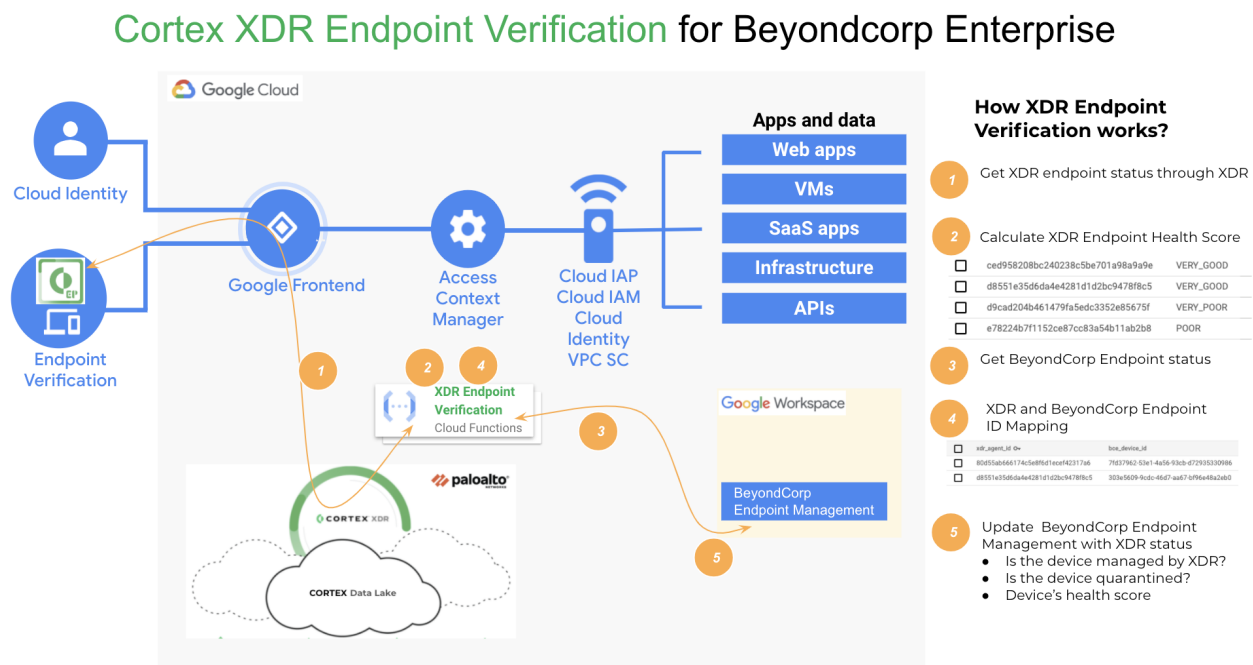
- Very Good
- Good
- Neutral

- Poor
- Very Poor

XDR endpoint security risk exposure rating is calculated base on the following factors:

1. Is the endpoint managed by Cortex XDR?
2. Is the endpoint quarantined by the Cortex XDR administrator?
3. What is the XDR Health Score?

Cortex XDR Endpoint Verification for Google BeyondCorp Architecture



Cortex XDR and Cortex Data Lake are cloud services provided by Palo Alto Networks and are running in Google Cloud. Cortex XDR manages XDR agents that are deployed to users endpoint devices. Cortex XDR Endpoint Verification is deployed as Cloud Functions to your Google Cloud project. Cortex XDR Endpoint Verification calculates the health score for XDR Endpoints based on the severity and the number of the alerts at the endpoint. Cortex XDR Endpoint Verification maps XDR agent ID to the device ID at Google Admin Endpoint Management. Cortex XDR Endpoint Verification updates the device status Google Admin Endpoint Management with XDR agent status.

Once you enable Cortex XDR Endpoint Verification as a Device Partner's Service at your Google Admin Site, you will be able to create an Access Level at Access Context Manager (ACM) based on Cortex XDR Endpoint risk factors:

- If the endpoint is a XDR managed device
- If the endpoint is quarantined by XDR administrator
- The minimum level for the endpoint health score.

This enables you to control the application access in IAP using the Cortex XDR Endpoint Access Level you created in ACM.

Prepare your Cortex XDR

Create API key needed for the cloud function to integrate with Cortex XDR.

1. Go to XDR console
2. Go to Settings -> Configurations->Integrations-> API Keys
3. Click "+New Keys" at the top right
4. In the Generate API Key page, choose Security Level to be "Advanced" (this is for additional security, which requested the API Key be hashed with nonce and timestamp to prevent replay attacks). Choose Roles to be "Instance Administrator". Then click

“Generate”.

Generate API Key

Security Level

- ☒ **Advanced**
API key must be hashed with nonce and timestamp (suitable for proprietary scripts and intended to prevent replay attacks).
- ☐ **Standard**
API key can be used as-is (suitable for curl).

☐ Enable Expiration Date

Your comment here...

Roles

- ☐ Deployment Admin
- ☒ **Instance Administrator**
- ☐ Investigation Admin
- ☐ Investigator
- ☐ IT Admin
- ☐ Privileged Investigator
- ☐ Privileged IT Admin
- ☐ Privileged Responder
- ☐ Privileged Security Admin
- ☐ Responder
- ☐ Scoped Endpoint Admin
- ☐ Security Admin
- ☐ Viewer

Views

- ☒ **Endpoints**
 - ☒ Endpoint Policies
 - ☒ Endpoint Profiles
 - ☒ Endpoint Management
 - ☒ Endpoint Groups
 - ☒ Endpoint Installations
 - ☒ Host Firewall
 - ☒ Device Control
 - ☒ Global Exceptions
 - ☒ Host Insights
- ☒ **Investigation**
 - ☒ Alerts
 - ☒ Incidents
 - ☒ Rules
 - ☒ Investigation Query
 - ☒ Personal Query Library
- ☒ **Response**
 - ☒ Action Center
 - ☒ Scripts
- ☒ **Configurations**
 - ☒ Public API
 - ☒ Alert Notifications

Actions

- ☒ **Investigation**
 - ☒ Alerts
 - ☒ Incidents
 - ☒ Rules
 - ☒ Prevention Rules
 - ☒ Personal Query Library
- ☒ **Assets**
 - ☒ Network Configuration
- ☒ **Response**
 - ☒ Isolate
 - ☒ Live Terminal
 - ☒ EDL
 - ☒ File Retrieval
 - ☒ File Search
 - ☒ Destroy Files
 - ☒ Terminate Process
 - ☒ Quarantine
 - ☒ Allow List/Block List
 - ☒ Request WildFire Verdict Change
 - ☒ Run Standard Script
 - ☒ Run High-Risk Script
 - ☒ Script Configurations

Cancel Generate

5. Copy the generated API key, and save it locally. (This key will not be access again, after you close the window)
6. And also copy the key ID, this will be needed later during the cloud function terraform deployment. (As example, the ID is 51)

API Keys Found 9 results

<input type="checkbox"/>	CREATION TIME ↓↑	ID	CREATED BY	COMMENT	SECURITY LEVEL	ROLE	EXPIRATION TIME
<input type="checkbox"/>	Sep 2nd 2021 08:48:17	51	Daniel Ma		Advanced	Instance Administrator	Never

7. Now you have done what you needed in XDR.

Deploy Cortex XDR Endpoint Verification to your Google Cloud project

Cortex XDR Endpoint Verification Components

Deploy Cortex XDR Endpoint Verification

Configure Cortex XDR Endpoint Verification

Enable Cortex XDR Endpoint Verification as a Partner Service at your Workspace Google Admin. You would need to contact Google to whitelist the integration for your Org.

Then, you can go through the google [Admin Portal](#), Device -> Mobile & endpoints -> Settings -> Third-party integrations, to enable the integration.

Google Admin

Search for users, groups or settings

Devices > Mobile and endpoints > Third-party integrations

Showing settings for users in Palo Alto Networks, Inc.

Third-party integration s

Organizational Units ^

Search for organizational units

Palo Alto Networks, Inc.

Android EMM
Applied at 'Palo Alto Networks, Inc.'

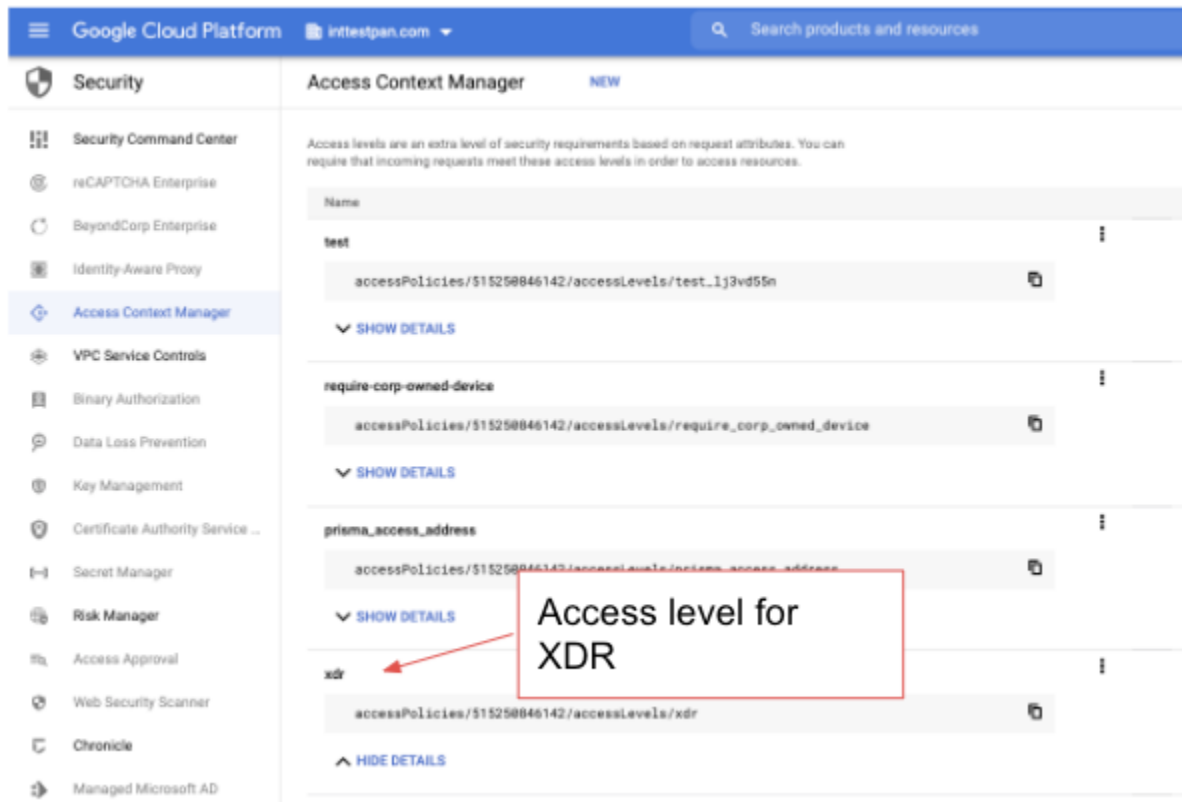
Third-party Android mobile management
Not enabled

Security and MDM partners
Applied at 'Palo Alto Networks, Inc.'

Enable BeyondCorp Alliance partner services
Partners [Manage](#)

☒ PANW **ALPHA**

Create Custom Access Level at ACM



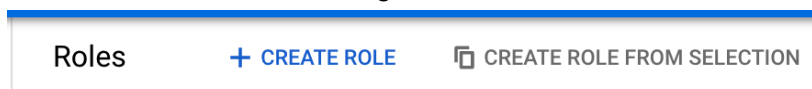
Example:

```
device.vendors["PANW"].is_compliant_device == true && device.vendors["PANW"].is_managed_device == true  
&& device.vendors["PANW"].device_health_score == DeviceHealthScore.VERY_GOOD
```

Configure Google Cloud Service Account, and secret key

This secret key will be needed by the Cloud Function (will be created later by the Marketplace installation) to communicate with the Google Workspace API.

1. Create Custom Role in IAM, go to IAM & Admin -> Roles, click "+ CREATE ROLE":



needed permission:

- pubsub.topics.publish
- spanner.databases.beginOrRollbackReadWriteTransaction
- spanner.databases.read

- spanner.databases.select
- spanner.databases.write
- spanner.instances.get
- spanner.sessions.create
- spanner.sessions.get

← Create Role

Custom roles let you group permissions and assign them to members of your project or organization. You can manually select permissions or import permissions from another role. [Learn more](#)

Title *

Custom Role

11 / 100

Description

This role is for Cloud Function work with pub/sub and spanner



61 / 256

ID *

XDR_BCE_Role

Role launch stage

General Availability

[+ ADD PERMISSIONS](#)

8 assigned permissions

Filter Enter property name or value



Permission	Status
pubsub.topics.publish	Supported
spanner.databases.beginOrRollbackReadWriteTransaction	Supported

Find permissions filter by “Cloud Spanner Admin”

Add permissions

Filter permissions by role
Cloud Spanner Admin

Filter Enter property name or value

Permission	Status
<input checked="" type="checkbox"/> spanner.databases.read	Supported
<input checked="" type="checkbox"/> spanner.databases.select	Supported
<input type="checkbox"/> spanner.databases.setIamPolicy	Supported
<input type="checkbox"/> spanner.databases.update	Not supported
<input type="checkbox"/> spanner.databases.updateDdl	Supported
<input checked="" type="checkbox"/> spanner.databases.write	Supported
<input type="checkbox"/> spanner.instanceConfigs.get	Supported
<input type="checkbox"/> spanner.instanceConfigs.list	Supported
<input type="checkbox"/> spanner.instanceOperations.cancel	Supported
<input type="checkbox"/> spanner.instanceOperations.delete	Supported

31 - 40 of 52

CANCEL ADD

1. Go to Google Cloud Console -> IAM & Admin -> Service Accounts -> Create a new Service Account (grant the role you just created), copy the Unique ID, you will need this later

1 Service account details

Service account name
xdr-bce-sa

Display name for this service account

Service account ID
xdr-bce-sa @ha-failover2.iam.gserviceaccount.com

Service account description
Describe what this service account will do

CREATE AND CONTINUE

2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

DONE CANCEL

Create service account

✓ Service account details

2 Grant this service account access to project (optional)

Grant this service account access to ha-failover2 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role
XDR_BCE_Role

Condition
[Add condition](#)

This role is for Cloud Function work with pub/sub and spanner

[+ ADD ANOTHER ROLE](#)

[CONTINUE](#)

Grant users access to this service account (optional)

[DONE](#)

[CANCEL](#)

[←](#) xdr-bce-sa

[DETAILS](#)

[PERMISSIONS](#)

[KEYS](#)

[METRICS](#)

[LOGS](#)

Service account details

Name
xdr-bce-sa [SAVE](#)

Description [SAVE](#)

Email
xdr-bce-sa@ha-fail- serviceaccount.com

Unique ID
112877 293416

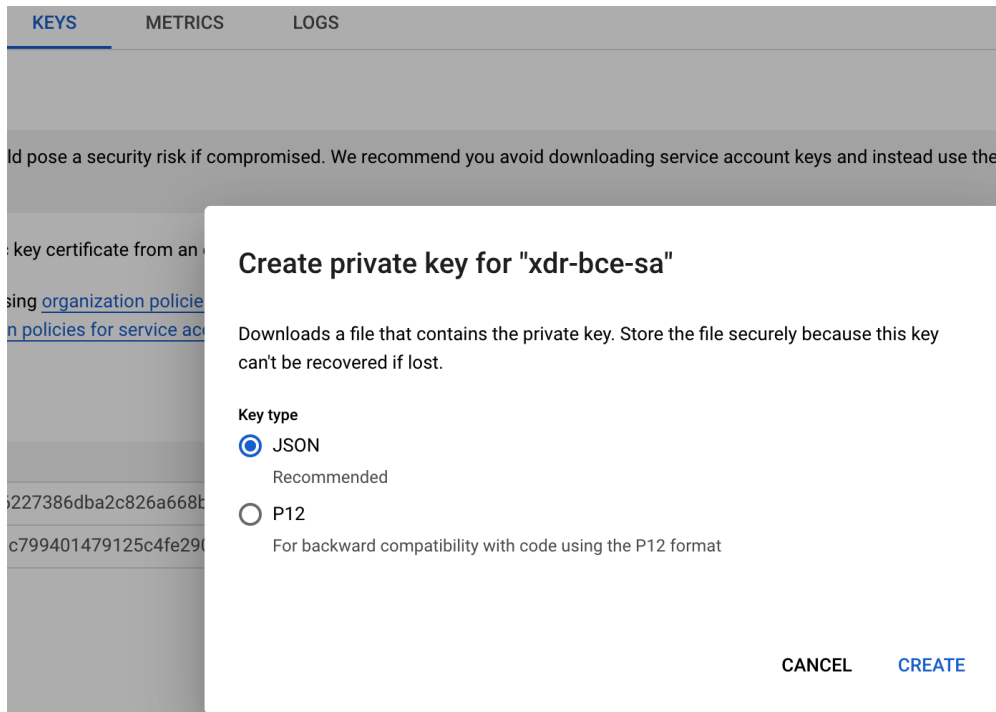
Service account status

Disabling your account allows you to preserve your policies without having to delete it.

✓ Account currently active

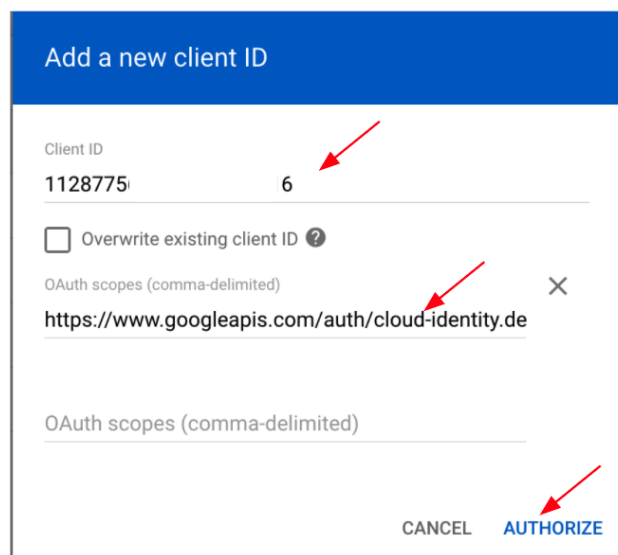
[DISABLE SERVICE ACCOUNT](#)

- Go to the “KEYS” tab, and create a new Key in JSON format:



Click "CREATE", and save the file locally. You will need this information later, and update in the Terraform template.

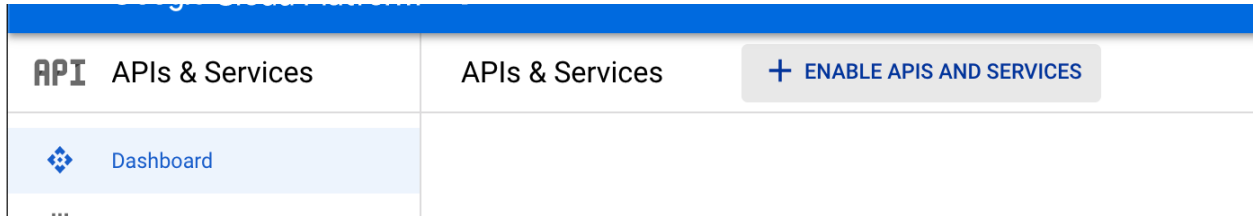
- Now you need to go to Google Admin Site to grant this service account for the Google Admin API Call scope. Go to Google Admin (<https://admin.google.com/>), login with your administrator account. Go to Security -> API Controls -> Add new client by clicking "Add New". Import the Unique ID you copied previously, and add the OAuth scope: <https://www.googleapis.com/auth/cloud-identity.devices>, like below:



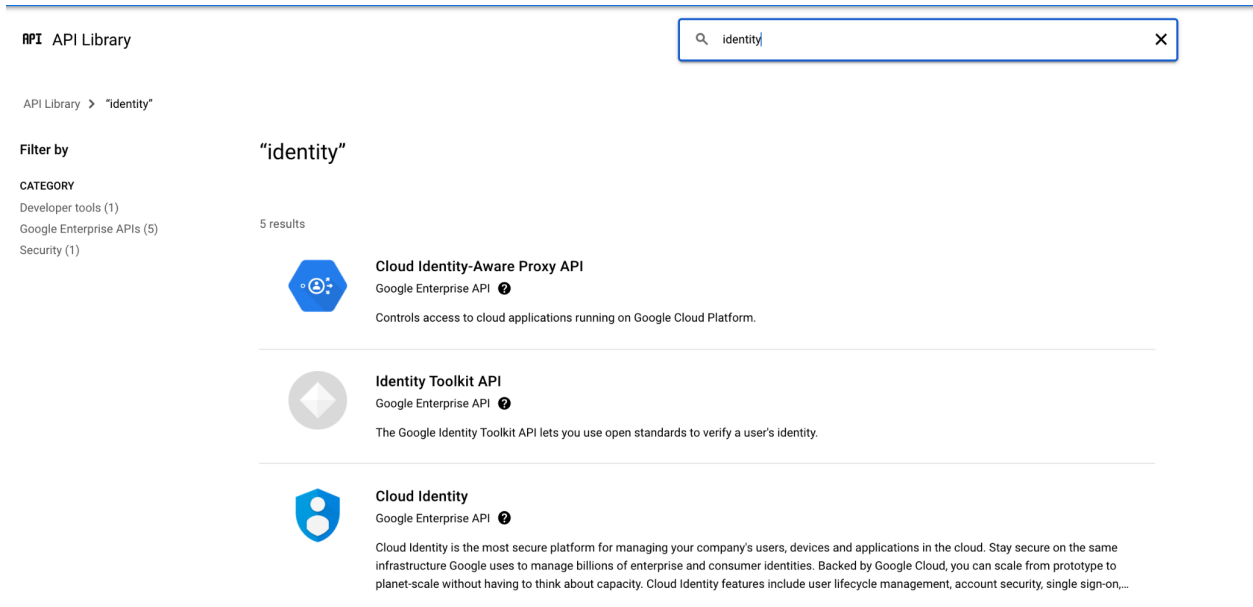
Deploy the integration through the Marketplace

Enable Cloud Identity API in Google Cloud Console (optional: if you didn't enable this before)

Goto APIs & Services -> Dashboard -> click "Enable APIS and SERVICES"



Search for "Identity"



And click "Cloud Identity"

Enable the API



Cloud Identity

Google Enterprise API

Easily manage users, devices, and apps from one console

ENABLE

TRY THIS API [↗](#)

Click to enable this API

OVERVIEW

DOCUMENTATION

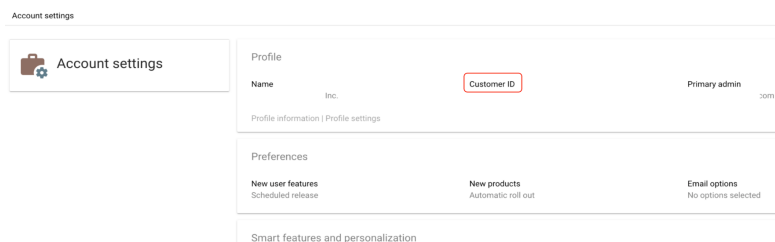
Parameters details:

variable	value
xdr_key	Your Cortex XDR key. As you created in the previous step
xdr_key_id	Your Cortex XDR key ID. As you created in the previous step
xdr_base_url	Your XDR API URL (i.e. <a href="https://api-<tenant_id>.xdr.us.paloaltonetworks.com/public_api/v1/">https://api-<tenant_id>.xdr.us.paloaltonetworks.com/public_api/v1/) Reference to Doc
customer_id	Your GCP customer ID. See Notice #1
customer_email	An email address. The Google Admin Portal Administrator email address. The service account will impersonate this user to update BeyondCorp Health Score
service_account_email	A GCP service account email.

global_prefix	A name to prepend to all cloud resources created (i.e. demo-prefix-)
Cred JSON	Get the content from the JSON file you downloaded through the service account creation, copy the whole content and paste here
Update XDR info healthscore Source	Update XDR info healthscore source available options: incidents or alerts. Incidents will be preferred, as it tracks the incident generated in the XDR instead of alerts..
Update XDR info source list	<p>Focused on the incidents triggered by the event sources, support multiple selections. Available Options: ["XDR Agent", "XDR Analytics", "XDR Managed Threat Hunting", "Threat Intelligence", "XDR Analytics BIOC", "XDR BIOC", "Correlation", "PAN NGFW", "XDR IOC"].</p> <p>For example: ["XDR Agent", "XDR BIOC", "XDR Analytics"]. This means any incidents triggered by either of these 3 alert sources, will affect the health score.</p>

Notices:

1. **Customer ID:** You can get this through [Admin Portal](#), Account -> Account Settings, find the Profile section, and you will get the customer ID. Screen Shot below:



Pls. add more details on how to deploy from the Marketplace.

Test your Cortex XDR Endpoint Verification Deployment

1. Create Access Context Manager Access Level:

Sample CEL could be:

```
device.vendors["PANW"].is_compliant_device == true &&
```

```
device.vendors["PANW"].is_managed_device == true
&& device.vendors["PANW"].device_health_score == DeviceHealthScore.VERY_GOOD
```

Or define a range for the health score:

```
device.vendors["PANW"].is_compliant_device == true &&
```

```
device.vendors["PANW"].is_managed_device == true
```

```
&& device.vendors["PANW"].device_health_score >= DeviceHealthScore.P00R
```

You can define yours based on your requirements.

Create a Access Level with XDR Endpoint Risk Context

Access level for XDR

Options to create a Access Level

New Access Level

Access level title *

XDR

Access level name

An access level name will automatically be generated based on the title.

Create conditions in

Only conditions in the selected mode will be saved.

Basic Mode

Advanced Mode

Premium

Conditions

Enter CEL expression here.

1



device.vendors["PANW"].is_compliant_device == true &&
device.vendors["PANW"].is_managed_device == true
&& device.vendors["PANW"].device_health_score ==
DeviceHealthScore.VERY_GOOD


2. Enforce XDR Endpoint Verification Access Level for Application Access


Access level for XDR


3. Check the Health Score of Endpoints in Google Admin Site (Devices -> Mobile and Endpoints):

Devices > Mobile and endpoints > Google Compute Engine

**Google Compute Engine**
Windows 10.0.14393
demo user
 Approved
Last sync: 3 hours ago

 EMAIL USER

 BLOCK DEVICE

 MORE

Device security

Managed by
Endpoint Verification

Password status
On

First sync
10/8/21, 3:37 PM

Last sync
10/13/21, 7:32 AM

Device information

Device ID
DTmnafQPZihB9CS0M7h01b5_lwAxax7Xtn0IRhle3cl

Serial number
GoogleCloud-E17ED40F94D70180CFB715B26F31F113

Ownership
User owned

Type
Windows

Operating system
Windows 10.0.14393

Wifi Mac Address
-

Host name | Device Resource ID

User information

Name
demo user

Primary email
demo@inttestpan.com

Third-party services

PANW
Health Score: Very Good

Additional Info:

Health score Calculation:

- Critical severity incident - Very Poor
- High severity incident - Poor
- Medium severity incident - Neutral
- Low severity Incident - Good
- No incident - Very Good
- For multiple incidents, the most severe incident level will be used