

# 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.

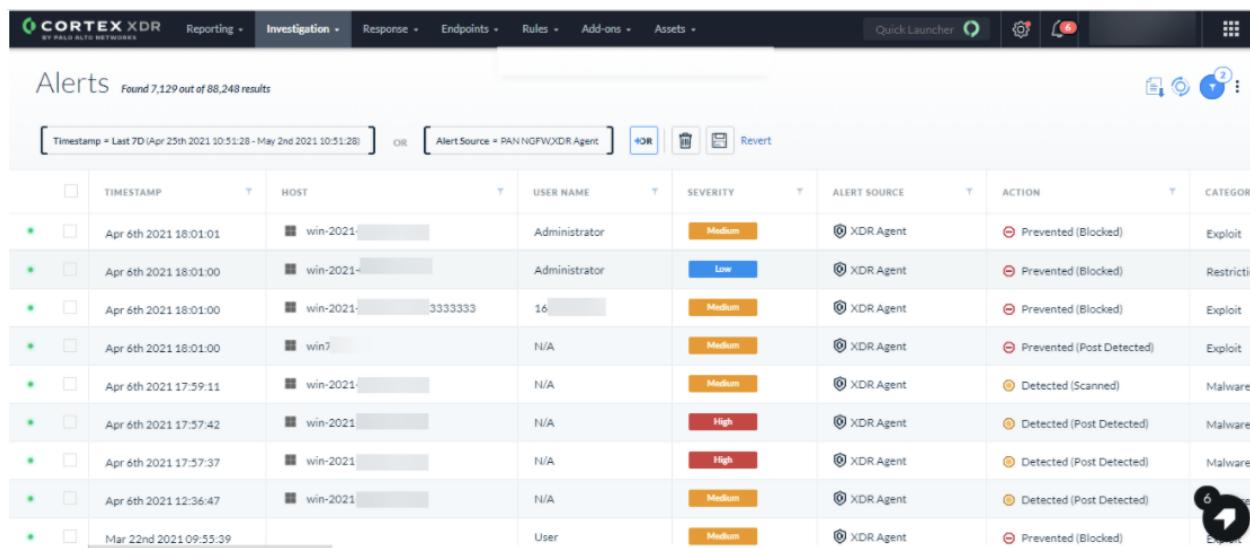
## Cortex XDR and XDR Health Score for Endpoint

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 interface with the 'Alerts' tab selected. The top navigation bar includes links for Reporting, Investigation, Response, Endpoints, Rules, Add-ons, Assets, and a Quick Launcher. Below the navigation is a search bar with filters for 'Timestamp' (Last 7D), 'Alert Source' (PAN NGFW/XDR Agent), and buttons for 'OR', 'Revert', and a trash icon. The main area displays a table of alerts with the following columns: TIMESTAMP, HOST, USER NAME, SEVERITY, ALERT SOURCE, ACTION, and CATEGORY. The table lists several incidents, mostly from April 6th, 2021, involving hosts like 'win-2021' and 'win7'. Most alerts are categorized as 'Exploit' or 'Malware' and show actions like 'Prevented (Blocked)' or 'Detected (Scanned)'. One alert from March 22nd, 2021, is categorized as 'Endpoint'.

TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
Apr 6th 2021 18:01:01	win-2021	Administrator	Medium	XDR Agent	Prevented (Blocked)	Exploit
Apr 6th 2021 18:01:00	win-2021	Administrator	Low	XDR Agent	Prevented (Blocked)	Restrictive
Apr 6th 2021 18:01:00	win-2021-333333	16	Medium	XDR Agent	Prevented (Blocked)	Exploit
Apr 6th 2021 18:01:00	win7	N/A	Medium	XDR Agent	Prevented (Post Detected)	Exploit
Apr 6th 2021 17:59:11	win-2021	N/A	Medium	XDR Agent	Detected (Scanned)	Malware
Apr 6th 2021 17:57:42	win-2021	N/A	High	XDR Agent	Detected (Post Detected)	Malware
Apr 6th 2021 17:57:37	win-2021	N/A	High	XDR Agent	Detected (Post Detected)	Malware
Apr 6th 2021 12:36:47	win-2021	N/A	Medium	XDR Agent	Detected (Post Detected)	Endpoint
Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	Prevented (Blocked)	Endpoint

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 severity of the incident associated with an endpoint. Here is the possible XDR Health Score:

- Very Good
- Good
- Neutral

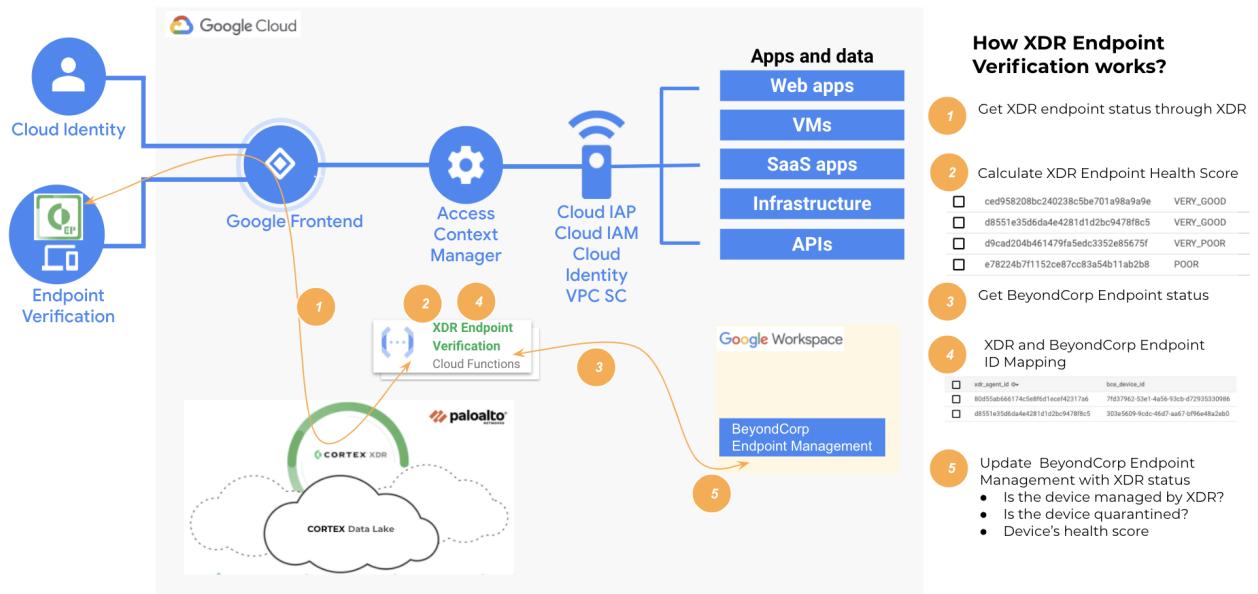
- Poor
- Very Poor

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 Endpoint Verification for Beyondcorp Enterprise



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.

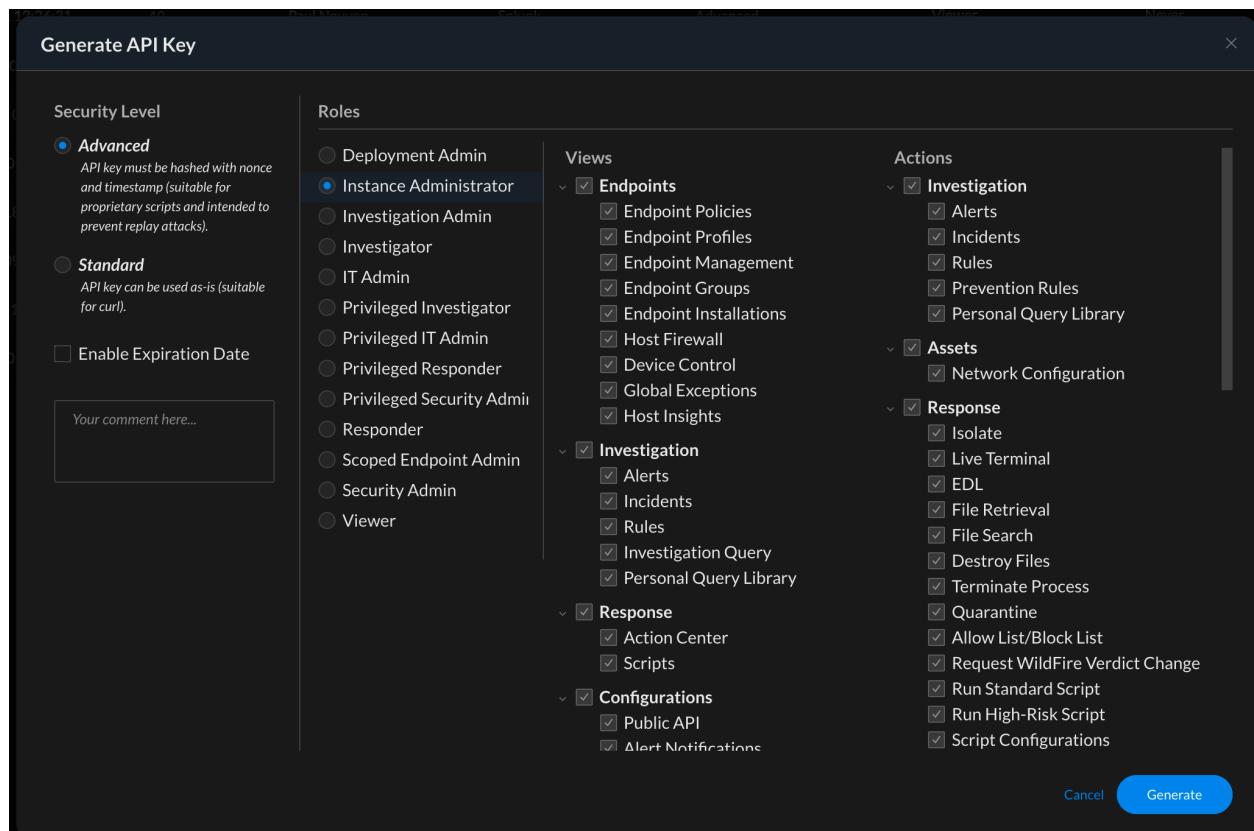
This enables you to control the application access in IAP using the Cortex XDR Endpoint Access Level you created in ACM.

## 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”.



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 <small>Found 9 results</small>									
	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.

The screenshot shows the Google Admin Portal interface. The left sidebar has icons for Home, Devices, Groups, Organizational Units, Search, and Help. The main navigation bar says "Devices > Mobile and endpoints > Third-party integrations". The main content area has a sidebar titled "Third-party integrations" with "Organizational Units" expanded, showing "Palo Alto Networks, Inc.". The main panel displays "Showing settings for users in Palo Alto Networks, Inc." and lists "Third-party integrations" for "Android EMM" and "Security and MDM partners". Both entries show "Not enabled". There is a "Manage" button next to the partners section. At the bottom right is a blue checkmark icon, the text "PANW ALPHA", and a yellow "ALPHA" button.

## Create Custom Access Level at ACM

The screenshot shows the Google Cloud Platform interface for Access Context Manager. On the left, there's a sidebar with various security services like Security Command Center, reCAPTCHA Enterprise, BeyondCorp Enterprise, Identity-Aware Proxy, VPC Service Controls, Binary Authorization, Data Loss Prevention, Key Management, Certificate Authority Service, Secret Manager, Risk Manager, Access Approval, Web Security Scanner, Chronicle, and Managed Microsoft AD. The 'Access Context Manager' option is selected. The main pane displays a list of access levels under a specific policy. One access level, 'xdr', is highlighted with a red box and labeled 'Access level for XDR'. A red arrow points from the text 'Access level for XDR' to the 'xdr' entry in the list.

Name	Description
test	accessPolicies/515250846142/accessLevels/test_1j3vd55n
require-corp-owned-device	accessPolicies/515250846142/accessLevels/require_corp_owned_device
prisma_access_address	accessPolicies/515250846142/accessLevels/prisma_access_address
xdr	accessPolicies/515250846142/accessLevels/xdr

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":

The screenshot shows the 'Roles' section of the Google Cloud IAM & Admin interface. It includes tabs for 'Roles' (selected), '+ CREATE ROLE', and 'CREATE ROLE FROM SELECTION'.

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
<input checked="" type="checkbox"/> pubsub.topics.publish	Supported
<input checked="" type="checkbox"/> spanner.databases.beginOrRollbackReadWriteTransaction	Supported

Find permissions filter by “Cloud Spanner Admin”

## Add permissions

Filter permissions by role		
Cloud Spanner Admin		
<input checked="" type="checkbox"/>	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 <span style="color:red;">!</span>
<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 X C

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

**1 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](#)

**Add users access to this service account (optional)** 

**DONE** **CANCEL**

[←](#) **xdr-bce-sa**

[DETAILS](#) [PERMISSIONS](#) [KEYS](#) [METRICS](#) [LOGS](#)

**Service account details**

Name **xdr-bce-sa** 

Description 

Email **xdr-bce-sa@ha-failover2.iam.gserviceaccount.com**

Unique ID **112877 293416** 

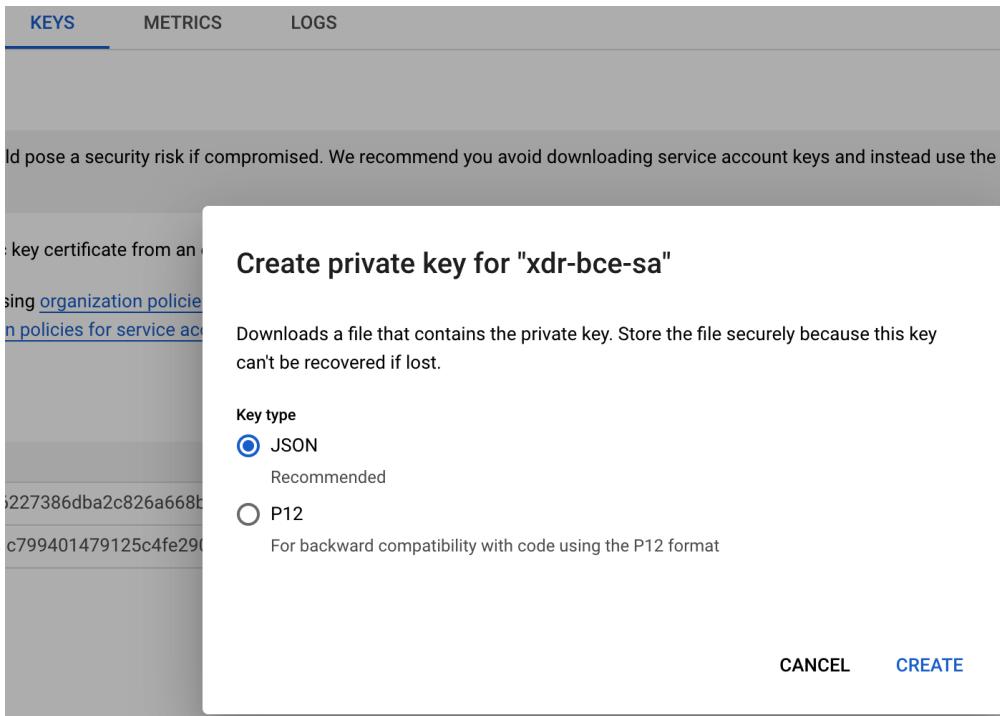
**Service account status**

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

Account currently active

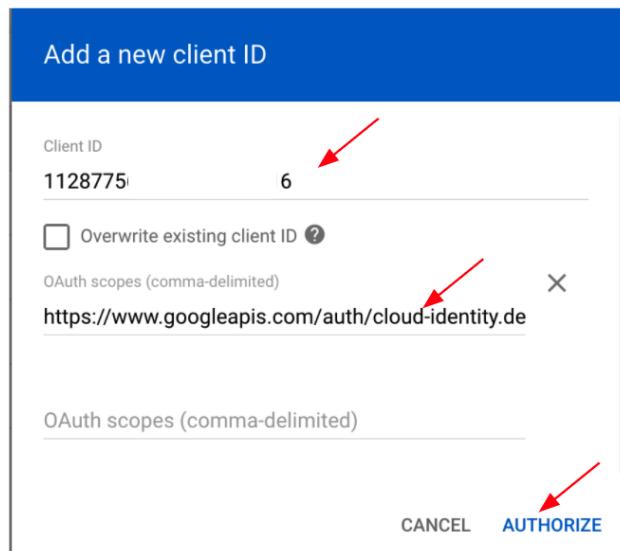
[DISABLE SERVICE ACCOUNT](#)

2. 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.

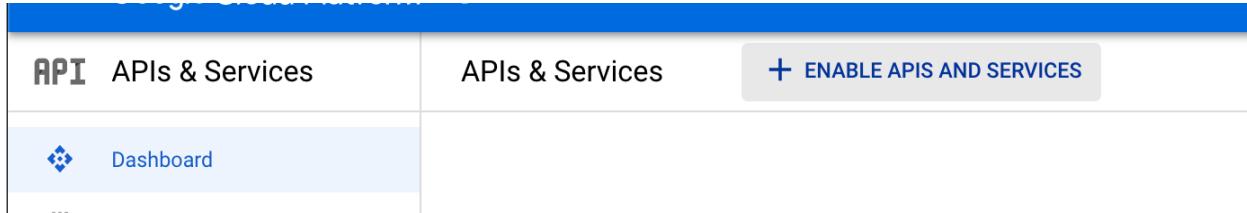
- Now you need to go to Google Admin Site to grant this service account for the Google Admin API Call scope. Go to Google Admin (<https://admin.google.com/>), login with your administrator account. Go to Security -> API Controls -> Add new client by clicking “Add New”. Import the Unique ID you copied 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"

A screenshot of the Google Cloud API Library search results for "identity". The search bar at the top contains the text "identity". Below the search bar, there is a filter section labeled "Filter by" with the value "identity". Under the "CATEGORY" heading, there are three items: "Developer tools (1)", "Google Enterprise APIs (5)", and "Security (1)". The first result listed is "Cloud Identity-Aware Proxy API", which is a "Google Enterprise API". Its description states: "Controls access to cloud applications running on Google Cloud Platform.". The second result is "Identity Toolkit API", also a "Google Enterprise API". Its description states: "The Google Identity Toolkit API lets you use open standards to verify a user's identity.". The third result is "Cloud Identity", which is also a "Google Enterprise API". Its description states: "Cloud Identity is the most secure platform for managing your company's users, devices and applications in the cloud. Stay secure on the same infrastructure Google uses to manage billions of enterprise and consumer identities. Backed by Google Cloud, you can scale from prototype to planet-scale without having to think about capacity. Cloud Identity features include user lifecycle management, account security, single sign-on,...".

And click "Cloud Identity"

Enable the API

[!\[\]\(39a2a7c32eb02bb191b0cf30062c9d1b\_img.jpg\)](#)

## 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](#)

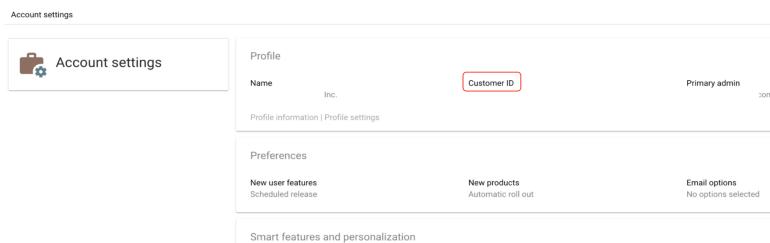
## Parameters details:

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-&lt;tenant_id&gt;.xdr.us.paloaltonetworks.com/public_api/v1/">https://api-&lt;tenant_id&gt;.xdr.us.paloaltonetworks.com/public_api/v1/</a> ) Reference to <a href="#">Doc</a>
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.

<b>global_prefix</b>	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 health score 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	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"]. <b>For example: ["XDR Agent", "XDR BIOC", "XDR Analytics"].</b> This means any incidents triggered by either of these 3 alert sources, will affect the health score.

#### 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:



# Integration Deployment

Step 1. Provide deployment details (see attached screenshot) according to the Parameters details section.

Google Cloud [redacted]

New XDR endpoint Verification deployment

Product preview. Go through the deployment flow available to Cloud Marketplace customers. Pricing info may not reflected in the preview

Deployment name \*

Zone  ?

Machine type

Machine family

GENERAL-PURPOSE COMPUTE-OPTIMIZED MEMORY-OPTIMIZED

Machine types for common workloads, optimized for cost and flexibility

Series  ?

Powered by Intel Skylake CPU platform or one of its predecessors

Machine type  ?

	vCPU	Memory
	0.25-1 vCPU (1 shared core)	614 MB

Cred JSON \*  ?

Customer email \*  ?

Global prefix \*  ?

Service account email \*  ?

Update XDR info healthscore source \*  ?

Update XDR info source list \*  ?

XDR base URL \*  ?

XDR key \*  ?

XDR key ID \*  ?

Customer ID \*  ?

< select VM size (recommended the smallest)

< provide previously configured Service Account Key

< select from dropdown

< provide list of XDR source list in presented format

## Step 2. Configure Boot Disk size and Networking.

The screenshot shows the Google Cloud VM configuration interface. At the top, it says "Google Cloud" and "Navigation menu: Now: Stackdriver Endpoint Verification deployment".

**Boot Disk**

- Boot disk type \* — Standard Persistent Disk
- Boot disk size in GB \* — 10

**Networking**

**Network interfaces**

Network interface	^
Network default	▼ ?
Subnetwork default	▼ ?
External IP None	▼ ?

DONE

**ADD NETWORK INTERFACE**

**Firewall** ?

Add tags and firewall rules to allow specific network traffic from the Internet

⚠ Creating certain firewall rules may expose your instance to the Internet. Please check if the rules you are creating are aligned with your security preferences. [Learn more](#)

Allow HTTP traffic from the Internet

Source IP ranges for HTTP traffic

Allow HTTPS traffic from the Internet

Source IP ranges for HTTPS traffic

**API Access**

Google Cloud Platform API

Allow full access to all of Google Cloud Platform APIs on the VM

**Stackdriver**

Monitoring and management for services, containers, applications, and infrastructure

< we recommend disabling External IP and using IAP to connect to VM

< HTTP and HTTPS traffic can be disabled

< Make sure “Allow full access to all of Google Cloud Platform APIs on the VM” is enabled

Step 3. Accept the GCP Marketplace Terms of Service and deploy the integration.

Google Cloud [REDACTED]

New XDR endpoint Verification deployment

XDR key ID \* 4 ?

Customer ID \* [REDACTED] ?

**Boot Disk**

Boot disk type \* Standard Persistent Disk ?

Boot disk size in GB \* 10 ?

**Networking**

**Network interfaces**

default default (10.128.0.0/20) ▼

ADD NETWORK INTERFACE

**Firewall** ?

Add tags and firewall rules to allow specific network traffic from the Internet

⚠ Creating certain firewall rules may expose your instance to the Internet.  
Please check if the rules you are creating are aligned with your security preferences. [Learn more](#)

Allow HTTP traffic from the Internet

Source IP ranges for HTTP traffic ?

Allow HTTPS traffic from the Internet

Source IP ranges for HTTPS traffic ?

**API Access**

Google Cloud Platform API

Allow full access to all of Google Cloud Platform APIs on the VM

**Stackdriver**

Monitoring and management for services, containers, applications, and infrastructure

Enable Stackdriver Logging ?

Enable Stackdriver Monitoring ?

I accept the [GCP Marketplace Terms of Service](#).

**DEPLOY**

Step 4. After the deployment is complete you will see suggested next steps (APIs that need to be enabled as well as service account that you will have to configure).

At the same time at the top of the integration deployment description you still see an SSH button that you can use to connect the VM to proceed with integration deployment.

The screenshot shows the Google Cloud Deployment Manager interface. On the left, there's a sidebar with 'Deployment Manager' selected. The main area shows a deployment named 'xdr-endpoint-verification-draft-1' has been deployed. Underneath, it lists 'solution.jinja' and 'solution-vm-tmpl vm\_instance.py'. A right-hand panel titled 'solution' provides details about the XDR endpoint Verification solution by Palo Alto Networks, Inc. It includes sections for 'Instance' (xdr-endpoint-verification-draft-1-vm), 'Instance zone' (us-central1-c), 'Instance machine type' (f1-micro), and 'MORE ABOUT THE SOFTWARE'. Below this, a 'Get started with XDR endpoint Verification' section offers an 'SSH' button. A 'Suggested next steps' list includes items like 'No external IP configured' (with a note about bastion host access) and 'For integration deployment please make sure that' (listing Pub/Sub, Scheduler, Cloud Functions, and Cloud Spanner). Another section, 'Used for integration deployment', lists Compute Engine, Cloud Build, Cloud Deployment Manager V2, and Cloud Runtime Configuration. At the bottom, it mentions service accounts with Storage Object Admin IAM roles and links to Cortex XDR Endpoint Verification Integration and Learn more about firewall rules.

Google Cloud

Deployment Manager

xdr-endpoint-verification-draft-1

DELETE

Deployments

Type registry

xdr-endpoint-verification-draft-1 has been deployed

Overview - xdr-endpoint-verification-draft-1

solution solution.jinja

solution-vm-tmpl vm\_instance.py

xdr-endpoint-verification-draft-1-vm vm instance

XDR endpoint Verification

Solution provided by Palo Alto Networks, Inc.

Instance: xdr-endpoint-verification-draft-1-vm

Instance zone: us-central1-c

Instance machine type: f1-micro

MORE ABOUT THE SOFTWARE

Get started with XDR endpoint Verification

SSH

Suggested next steps

- No external IP configured  
The VM instance has been configured with no external IP or internet access. Connecting to it directly may not be possible. Consider using a [bastion host](#) to access this VM.
- For integration deployment please make sure that:  
You enabled following APIs  
Used in integration:
  - Pub/Sub
  - Scheduler
  - Cloud Functions
  - Cloud Spanner

Used for integration deployment:

- Compute Engine
- Cloud Build
- Cloud Deployment Manager V2
- Cloud Runtime Configuration

Following service accounts are granted with Storage Object Admin IAM role:

- [REDACTED] compute@developer.gserviceaccount.com
- [REDACTED] @cloudservices.gserviceaccount.com

For more information please visit [Cortex XDR Endpoint Verification Integration](#).

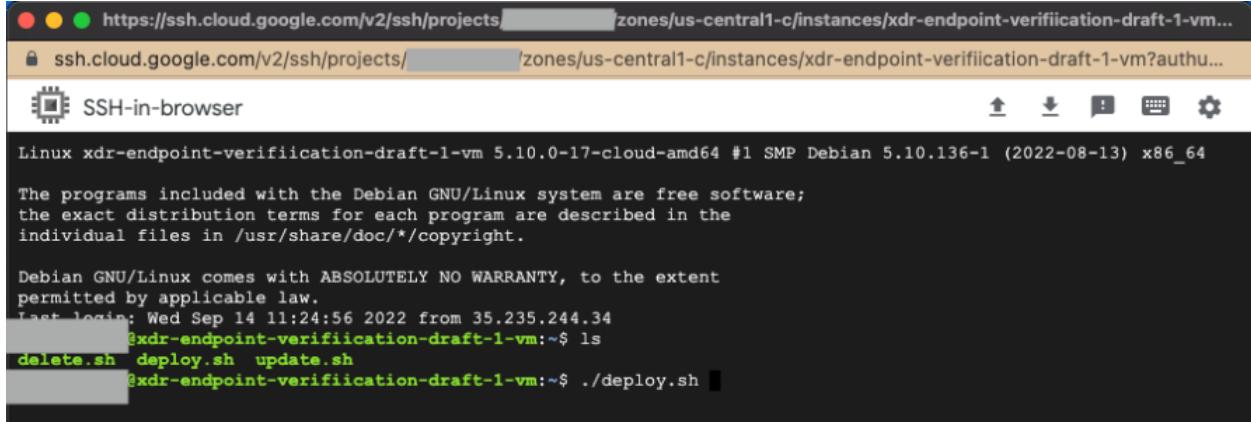
Open HTTP traffic  
This firewall rule is not enabled. To allow specific network traffic from the Internet, create a firewall rule to open HTTP traffic for target tag "xdr-endpoint-verification-draft-1-deployment". [Learn more](#). If you are using Google Cloud SDK, type the following command in the terminal:

```
$ gcloud --project= [REDACTED] compute firewall-rules
```

Open HTTPS traffic

Step 5. On the VM you will have access to 3 scripts

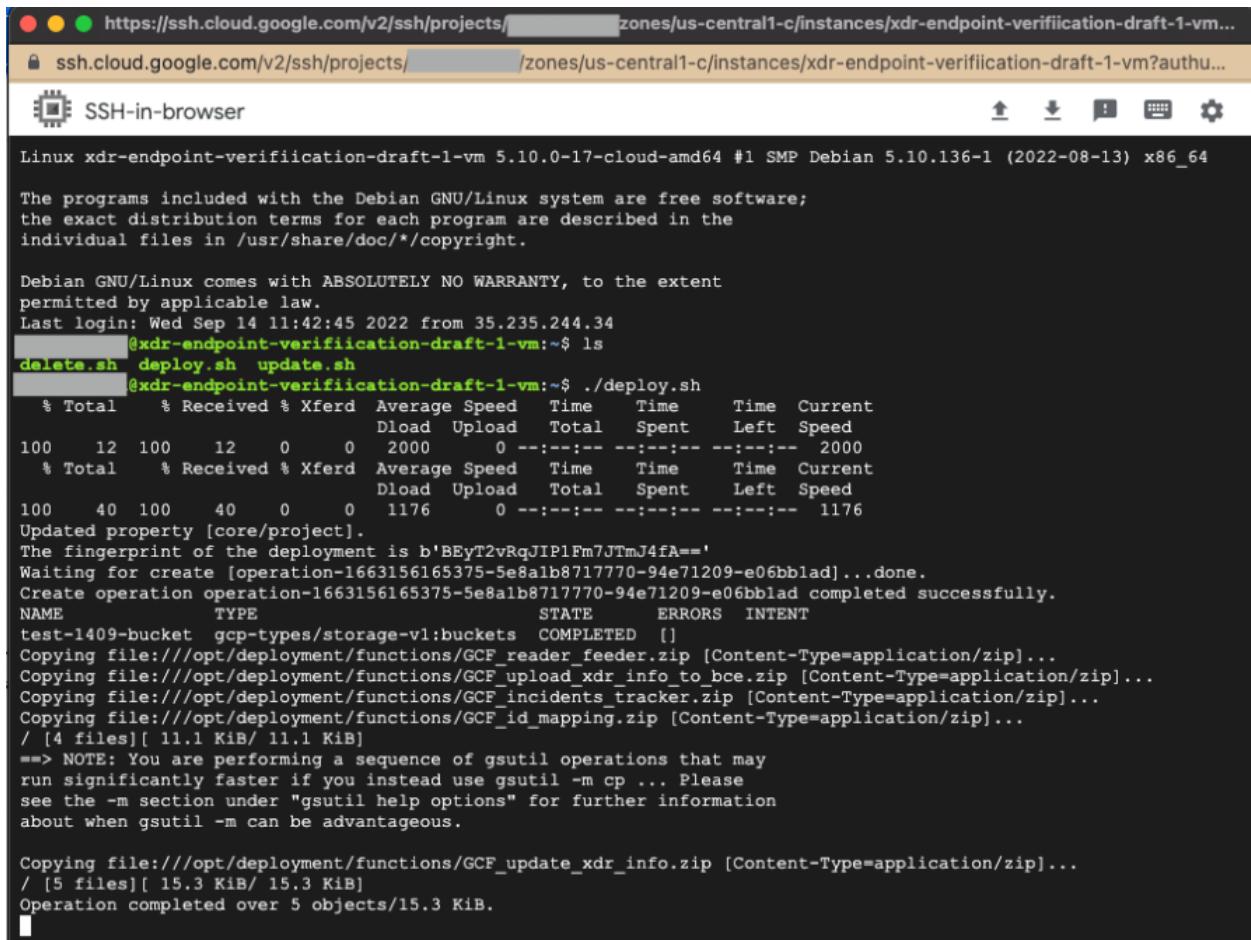
- 1) Deploy - to deploy integration resources
- 2) Update - to update integration configuration (or redeploy failed resources)
- 3) Delete - script that removes all resources (something deployment manager cannot remove fully - GCS)



```
Linux xdr-endpoint-verifiication-draft-1-vm 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 14 11:24:56 2022 from 35.235.244.34
@xdr-endpoint-verifiication-draft-1-vm:~$ ls
delete.sh deploy.sh update.sh
@xdr-endpoint-verifiication-draft-1-vm:~$ ./deploy.sh
```

type: “./deploy.sh” and press enter to deploy the solution

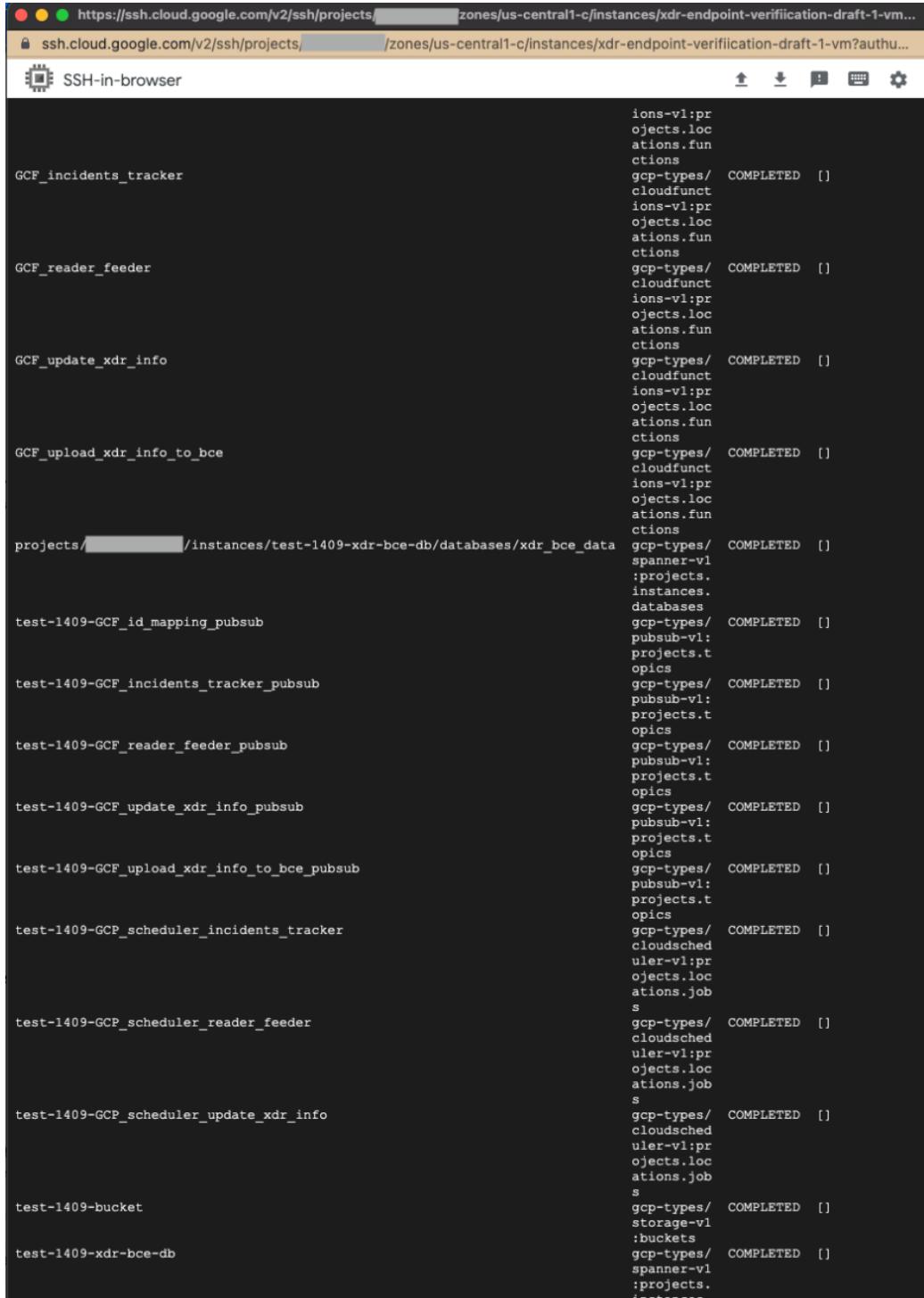


```
Linux xdr-endpoint-verifiication-draft-1-vm 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 14 11:42:45 2022 from 35.235.244.34
@xdr-endpoint-verifiication-draft-1-vm:~$ ls
delete.sh deploy.sh update.sh
@xdr-endpoint-verifiication-draft-1-vm:~$ ./deploy.sh
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload   Total Spent   Left  Speed
100      12  100    12    0     0  2000      0 ---:--- ---:--- 2000
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload   Total Spent   Left  Speed
100      40  100    40    0     0  1176      0 ---:--- ---:--- 1176
Updated property [core/project].
The fingerprint of the deployment is b'BxEyT2vRqJIP1Fm7JTmJ4fA=='.
Waiting for create [operation-1663156165375-5e8alb8717770-94e71209-e06bb1ad]...done.
Create operation operation-1663156165375-5e8alb8717770-94e71209-e06bb1ad completed successfully.
NAME           TYPE        STATE    ERRORS   INTENT
test-1409-bucket  gcp-types/storage-v1:buckets  COMPLETED []
Copying file:///opt/deployment/functions/GCF_reader_feeder.zip [Content-Type=application/zip]...
Copying file:///opt/deployment/functions/GCF_upload_xdr_info_to_bce.zip [Content-Type=application/zip]...
Copying file:///opt/deployment/functions/GCF_incidents_tracker.zip [Content-Type=application/zip]...
Copying file:///opt/deployment/functions/GCF_id_mapping.zip [Content-Type=application/zip]...
/ [4 files][ 11.1 KiB/ 11.1 KiB]
---> NOTE: You are performing a sequence of gsutil operations that may
run significantly faster if you instead use gsutil -m cp ... Please
see the -m section under "gsutil help options" for further information
about when gsutil -m can be advantageous.

Copying file:///opt/deployment/functions/GCF_update_xdr_info.zip [Content-Type=application/zip]...
/ [5 files][ 15.3 KiB/ 15.3 KiB]
Operation completed over 5 objects/15.3 KiB.
```

after successful deployment you should see following information (that all resources deployment is “COMPLETED”):



The screenshot shows an SSH-in-browser terminal window with the URL <https://ssh.cloud.google.com/v2/ssh/projects/.../zones/us-central1-c/instances/xdr-endpoint-verifiication-draft-1-vm...>. The terminal displays a list of GCP resources and their deployment status. Most resources are marked as "COMPLETED". The list includes:

- GCF\_incidents\_tracker
- GCF\_reader\_feeder
- GCF\_update\_xdr\_info
- GCF\_upload\_xdr\_info\_to\_bce
- projects/.../instances/test-1409-xdr-bce-db/databases/xdr\_bce\_data
- test-1409-GCF\_id\_mapping\_pubsub
- test-1409-GCF\_incidents\_tracker\_pubsub
- test-1409-GCF\_reader\_feeder\_pubsub
- test-1409-GCF\_update\_xdr\_info\_pubsub
- test-1409-GCF\_upload\_xdr\_info\_to\_bce\_pubsub
- test-1409-GCP\_scheduler\_incidents\_tracker
- test-1409-GCP\_scheduler\_reader\_feeder
- test-1409-GCP\_scheduler\_update\_xdr\_info
- test-1409-bucket
- test-1409-xdr-bce-db

Each resource entry shows its name followed by a series of fields: gcp-types/, COMPLETED, and a list of actions. The actions listed include: pr, objects.loc, ations.fun, ctions, cloudfunct, ions-v1:pr, objects.loc, ations.fun, ctions, gcp-types/, COMPLETED, spanner-v1, :projects, instances, databases, gcp-types/, COMPLETED, pubsub-v1, projects.t, opics, gcp-types/, COMPLETED, cloudsched, uler-v1:pr, objects.loc, ations.job, s, gcp-types/, COMPLETED, cloudsched, uler-v1:pr, objects.loc, ations.job, s, gcp-types/, COMPLETED, cloudsched, uler-v1:pr, objects.loc, ations.job, s, gcp-types/, COMPLETED, storage-v1, :buckets, gcp-types/, COMPLETED, spanner-v1, :projects, instances.

Step 6. Going to you deployment list you should now see second deployment (actual integration resources deployment)

Name	Created on	Last modified	Labels
<a href="#">test-1409-xdr-endpoint-verification</a>	4 minutes ago	Just now	None
<a href="#">xdr-endpoint-verification-draft-1</a>	30 minutes ago	29 minutes ago	cloud-mark... : paloalto...

Clicking details you should see information about deployed resources and success status at the top of the list

Deployment properties	
ID	4713211008306118954
Created On	2022-09-14 (13:49:25)
Manifest Name	manifest-1663156176904
Config	<a href="#">View</a>
Imports	<a href="#">GCF_id_mapping.py</a> <a href="#">GCF_incidents_tracker.py</a> <a href="#">GCF_pubsub.py</a> <a href="#">GCF_reader_feeder.py</a> <a href="#">GCF_update_xdr_info.py</a> <a href="#">GCF_upload_xdr_info_to_bce.py</a> <a href="#">GCP_scheduler.py</a> <a href="#">GCP_spanner.py</a> <a href="#">GCS_bucket.py</a> <a href="#">config.json</a> <a href="#">create_incident_table.sql</a> <a href="#">create_xdr_bce.sql</a> <a href="#">create_xdr_info.sql</a>
Layout	<a href="#">View</a>
Expanded Config	<a href="#">View</a>

you can check the status of Cloud Function:

The screenshot shows the Google Cloud Functions dashboard. At the top, there are tabs for 'Cloud Functions' (selected), 'Functions', 'CREATE FUNCTION', and 'REFRESH'. A search bar at the top right says 'Search Products, resources, docs (/)'. Below the tabs is a filter section labeled 'Filter' with 'Filter functions' selected. The main area is a table with the following columns: Environment, Name, Last deployed, Region, Trigger, Runtime, Memory allocated, Executed function, Authentication, and Actions. There are six rows listed, all under the '1st gen' environment:

Environment	Name	Last deployed	Region	Trigger	Runtime	Memory allocated	Executed function	Authentication	Actions
1st gen	test-1409-id_mapping-function	Sep 14, 2022, 1:51:53 PM	us-central1	Custom integrations	Python 3.9	256 MB	hello_pubsub		⋮
1st gen	test-1409-incidents_tracker-function	Sep 14, 2022, 1:52:02 PM	us-central1	Custom integrations	Python 3.9	256 MB	hello_pubsub		⋮
1st gen	test-1409-reader_feeder-function	Sep 14, 2022, 1:51:58 PM	us-central1	Custom integrations	Python 3.9	256 MB	hello_pubsub		⋮
1st gen	test-1409-update_xdr_info-function	Sep 14, 2022, 1:52:19 PM	us-central1	Custom integrations	Python 3.9	256 MB	hello_pubsub		⋮
1st gen	test-1409-upload_xdr_info_to_bce-function	Sep 14, 2022, 1:52:48 PM	us-central1	Custom integrations	Python 3.9	256 MB	hello_pubsub		⋮

Spanner instance:

The screenshot shows the Google Cloud Spanner instance overview page. At the top, there are tabs for 'Spanner' (selected) and 'All instances'. Below the tabs is a 'Instances' section with 'CREATE INSTANCE' and '+ CREATE FREE INSTANCE' buttons. A descriptive text explains that Cloud Spanner is a fully managed relational database service. Below this is a filter section and a table with columns: Name, ID, Configuration, Processing units, Nodes, Storage utilization, and Labels. One instance is listed:

Name	ID	Configuration	Processing units	Nodes	Storage utilization	Labels
test-1409-xdr-bce-db	test-1409-xdr-bce-db	us-central1 (Iowa)	1,000	1	0 B / 4 TB	

and finally Spanner tables

The screenshot shows the Google Cloud Spanner database overview page. At the top, there are tabs for 'Spanner' (selected), 'All instances', 'INSTANCE test-1409-xdr-bce-db: Overview', and 'GOOGLE STANDARD SQL DATABASE xd\_r\_bce\_data: Overview'. Below the tabs is a sidebar with sections for 'DATABASE' (Overview, Import/Export, Backup/Restore, Query, Change streams) and 'INSIGHTS' (Monitoring, Key Visualizer, Query insights). The main area has tabs for 'OVERVIEW' and 'TABLES'. The 'OVERVIEW' tab shows CPU utilization (mean: 2.39%), Operations (Read: 0.00/s, Write: 0.00/s), Throughput (Read: ~s, Write: 0 B/s), and Total database storage (0 B). The 'TABLES' tab shows three tables: 'xd\_r\_bce', 'xd\_r\_incidents', and 'xd\_r\_info'. Each table has columns for Name, Indexes, Interleaved in, and Watched by.

Step 7. Now you can shut down a VM instance on the Compute Engine screen (keep it in case you need to update configuration or delete resources).

# Removing integrations

Step 1. Go to the VM integration deployment page and press SSH to connect to the VM.

The screenshot shows the Google Cloud Deployment Manager interface. A deployment named 'xdr-endpoint-verification-draft-1' is listed, with its status as 'has been deployed'. Under this deployment, there is a 'solution' sub-deployment. On the right side of the screen, an 'SSH-in-browser' terminal window is open, connected to an instance named 'xdr-endpoint-verification-draft-1-vm'. The terminal shows the command 'ssh -t ./delete.sh' being run, which triggers a series of file removal operations on the VM.

Step 2. In the SSH session type “./delete.sh” and press enter.

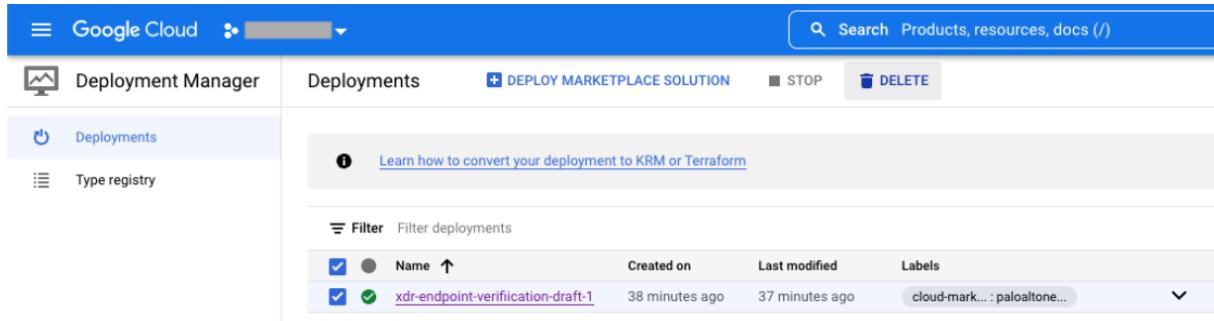
```
Linux xdr-endpoint-verifiication-draft-1-vm 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 14 11:47:58 2022 from 35.235.245.129
@xdr-endpoint-verifiication-draft-1-vm:~$ ./delete.sh
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total Spent   Left  Speed
100  12  100  12  0    0  2000      0 --:--:-- --:--:-- 2000
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          Dload  Upload   Total Spent   Left  Speed
100  40  100  40  0    0  1081      0 --:--:-- --:--:-- 1081
Updated property [core/project].
Removing gs://test-1409-bucket/functions/GCF_id_mapping.zip#1663156175660011...
Removing gs://test-1409-bucket/functions/GCF_reader_feeder.zip#1663156175349209...
Removing gs://test-1409-bucket/functions/GCF_upload_xdr_info_to_bce.zip#1663156175476572...
Removing gs://test-1409-bucket/functions/GCF_incidents_tracker.zip#1663156175550457...
Removing gs://test-1409-bucket/functions/GCF_update_xdr_info.zip#1663156175772690...
Completed 5/5
Removing Buckets:
Removing gs://test-1409-bucket/...
Completed 1/1
The following deployments will be deleted:
- test-1409-xdr-endpoint-verification

Do you want to continue (y/N)? y

Waiting for delete [operation-1663156864857-5e8ale222b75e-124e5394-e0b630d8]...done.
Delete operation operation-1663156864857-5e8ale222b75e-124e5394-e0b630d8 completed successfully.
```

Step 3. Confirm that the integration resources were removed (you should only see VM integration deployment in the Deployment Manager screen).



The screenshot shows the Google Cloud Deployment Manager interface. The left sidebar has 'Deployment Manager' selected. The main area shows a table of deployments:

	Name	Created on	Last modified	Labels
<input checked="" type="checkbox"/>	xdr-endpoint-verification-draft-1	38 minutes ago	37 minutes ago	cloud-mark... : paloalton...

Step 4. Remove VM integration deployment using DELETE button.

# 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.POOR
```

You can define yours based on your requirements.

The screenshot shows the Google Cloud Platform interface for creating a new Access Level. On the left, the navigation menu includes 'Security', 'Access Context Manager', and 'XDR'. The 'Access Context Manager' section is active, showing a list of existing access levels: 'test', 'require-corp-owned-device', 'prisma\_access\_address', and 'xdr'. The 'xdr' entry is highlighted with a red box and an arrow pointing to it from the text 'Access level for XDR'. To the right, a modal window titled 'Options to create a Access Level' is open. It has fields for 'Access level title' (set to 'XDR'), 'Access level name' (auto-generated), 'Create conditions in' (set to 'Only conditions in the selected mode will be saved'), and 'Conditions' (containing the CEL expression: `device.vendors["PANW"].is_compliant_device == true && device.vendors["PANW"].is_managed_device == true && device.vendors["PANW"].device_health_score == DeviceHealthScore.VERY_GOOD`). There are also 'Basic Mode' and 'Advanced Mode' buttons, with 'Advanced Mode' being selected.

## 2. Enforce XDR Endpoint Verification Access Level for Application Access

The screenshot shows the Google Cloud Platform Identity-Aware Proxy (IAP) interface. On the left, there's a sidebar with various security-related services like Security Command Center, reCAPTCHA Enterprise, BeyondCorp Enterprise, and Identity-Aware Proxy. The main area is titled 'Identity-Aware Proxy' and shows 'HTTPS RESOURCES'. It lists several resources, including 'All Web Services', 'App Engine app', and 'default'. The 'default' resource is selected, showing its details: URL <https://ha-failover2.uc.r.appspot.com>, Method IAM, Status OK. To the right, there's an 'Access Control' panel with a table of roles and members. A red box highlights the 'Access level for XDR' entry in the list.

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

The screenshot shows the Google Admin Site under 'Devices > Mobile and endpoints > Google Compute Engine'. The page displays device security information for a Windows 10.0.14393 device named 'demo user'. It includes sections for 'Device security', 'Device information', and 'User information'. In the 'Device information' section, there's a 'Third-party services' box containing the PANW logo and the text 'Health Score: Very Good'. A red box highlights this specific section.

## **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