Endpoint Verification overview

This page describes the basic concepts of Endpoint Verification.

Available to all Google Cloud, Cloud Identity, G Suite Business, and G Suite Enterprise customers, Endpoint Verification is a product that allows you, as an admin or security operations professional, to build an inventory of devices that are accessing your organization's data. Endpoint Verification also provides critical device trust and security-based access control as a part of the Context-Aware Access (/context-aware-access/docs/overview) solution.

When to use Endpoint Verification

Use Endpoint Verification when you want an overview of the security posture of your organization's laptop, desktop, and mobile devices.

The device inventory Endpoint Verification provides valuable information that you can use to maintain security. When paired with Context-Aware Access offerings, Endpoint Verification helps enforce fine-grained access control on your Google Cloud resources.

How Endpoint Verification works

Endpoint Verification consists of a Chrome extension, although a native helper app is also required for Linux devices and for Mac and Windows devices not using Chrome 80 or higher. Chrome OS devices only require the Chrome extension.

Once enabled through the G Suite Google Admin console, you can deploy the Endpoint Verification Chrome extension to corporate devices. Employees can also install it on their unmanaged, personal devices. This extension gathers and reports device information, constantly syncing with Google Cloud.

Using the details collected from the Chrome extension, Endpoint Verification creates an inventory of devices running Chrome OS and Chrome Browser that access your organization's data. For example, once an employee installs the Endpoint Verification extension, Endpoint Verification populates information about the device the employee used to access Google Cloud

resources. As an admin, you can review information including encryption status, OS, and user details.

Collected device information

The following table describes the properties and attributes collected from the devices accessing corporate resources.

Device properties

Category	Property name	Description	Supported devices
Device compliance	Status	Device's management status: Approved or unknown	• Mac • Chrome OS • Windows • Linux
User details	Name	The user's name	• Mac • Chrome OS • Windows • Linux
	Email	The user's email ID and aliases	• Mac • Chrome OS • Windows • Linux
Policy profile	First sync	Date and time the user first synchronized corporate data on the device	• Mac • Chrome OS • Windows • Linux
	Last sync	Date and time of the most recent sync	• Mac • Chrome OS • Windows

			• Linux

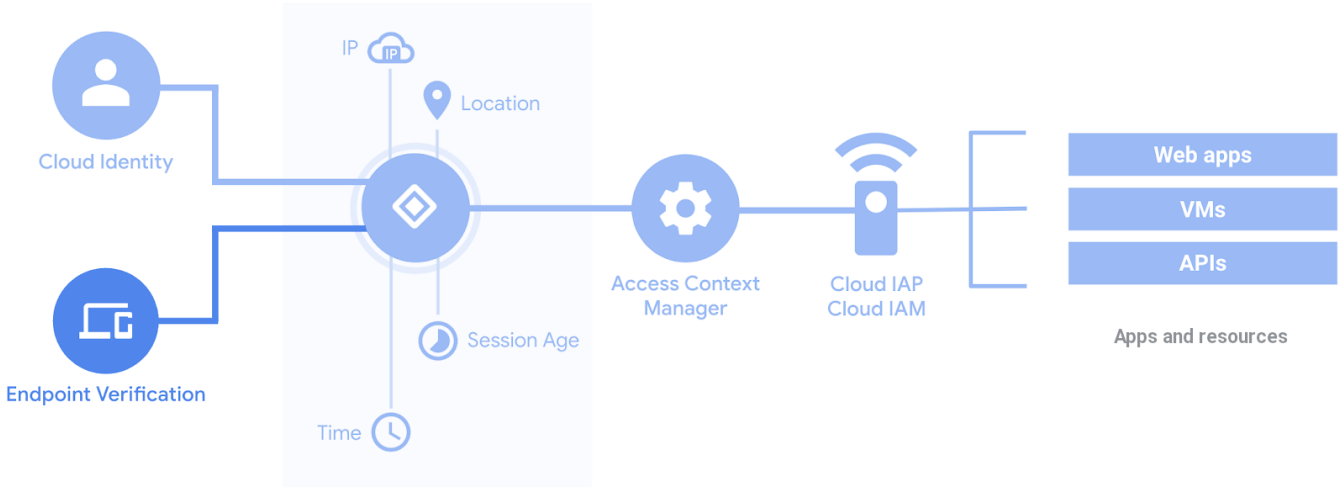
	Device password status	Whether the device has a screen lock password
		Note: This property doesn't report whether the device has any other type of password (such as a firmware password for Mac).
			• Mac (managed devices only)
			• Windows
			• Linux (supported window managers only):
			  • Gnome
			  • Cinnamon

	Encryption status	Whether the device is encrypted	• Mac • Chrome OS • Windows • Linux
Device properties	Device ID	Unique number associated with the user's device.	• Mac • Chrome OS • Windows • Linux
	Serial number	Serial number of the device	• Mac • Chrome OS • Windows • Linux
	Type	Make of device	• Mac • Chrome OS • Windows • Linux
	OS	Name of the operating system	• Mac • Chrome OS • Windows

		• Linux
Verified Access	Indicates whether Chrome OS adheres to your organization's policies Related topics: 1. Chrome OS enterprise policies (https://support.google.com/chrome/a/answer/2657289) 2. Enable Verified Access with Chrome OS devices (https://support.google.com/chrome/a/answer/7156268)	Chrome OS

Context-Aware Access

Endpoint Verification is a part of the Context-Aware Access approach to securing Google Cloud, on-premises apps and resources, and G Suite apps. The attributes Endpoint Verification collects can be used by Access Context Manager (/access-context-manager/docs) to control access to Google Cloud and G Suite resources.



Access Context Manager references the device attributes gathered by Endpoint Verification to enforce fine grained access control with access levels (/access-context-manager/docs/overview#access-levels). You can also tag individual devices (/endpoint-verification/docs/setting-up-device-approvals) and mark company-owned devices (/endpoint-verification/docs/configuring-company-owned-devices).

Manual device tagging is enforced by creating a device access level (/endpoint-verification/docs/creating-device-access-level) that requires device approval. Company-

owned devices are enforced by creating a device access level that requires company-owned devices.

Last updated 2020-07-22 UTC.