

Alcatel Lucent IoT Inventory Integration with Google Workspace User Guide

Contents

- [1 Alcatel Lucent IoT Inventory Integration with Google Workspace](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 FAQ](#)
- [5 Introduction](#)
- [6 Prerequisites](#)
- [7 Google Workspace Device Enrollment](#)
 - [7.1 Enrollment](#)
- [8 Google Cloud/Workspace Configuration](#)
 - [8.1 Project Creation and API enablement](#)
 - [8.2 Service Account and Private Key Creation](#)
 - [8.3 Adding API scopes to Domain Wide Delegation](#)
- [9 Google Workspace on OmniVista](#)
 - [9.1 Setting up Google Workspace Account on OmniVista](#)
- [10 Conclusion](#)
- [11 Documents / Resources](#)
 - [11.1 References](#)
- [12 Related Posts](#)



Alcatel Lucent IoT Inventory Integration with Google Workspace

Product Information

Specifications

- **Google Workspace Integration Version:** OmniVista IoT Inventory Integration with Google Workspace
- **Supported Devices:** AOS Switches and Access Points running AOS 8.6R2 and later
- **Required:** NTP Server(s) for consistent inventory view
- **Internet Connection:** Required for OmniVista application

Product Usage Instructions

Enabling IoT Devices on AOS Switches/APs

The IoT application can be configured to integrate with Google Workspace to collect information on devices connected to AOS Switches and Access Points, including devices running Chrome OS.

- Ensure AOS Switches are running AOS 8.6R2 or later, or APs connected to AOS Switches are running AOS 8.6R2 or later.
- Sync Switches/APs to the same NTP Server(s) for correct display and filtering of IoT Inventory data.
- OmniVista requires an internet connection for effective use.
- Configure firewall to allow access to Device Fingerprinting Service if applicable.

Google Workspace Device Enrollment

To enroll devices in Google Workspace for integration:

1. Ensure Google Workspace Enterprise Account with Admin Privileges is available.
2. Reset Chrome devices to factory settings if previously managed by another organization.
3. Access Google Workspace Admin Console to configure and enable device enrollment.
4. Connect devices to Wi-Fi network for enrollment.

Google Cloud/Workspace Configuration

For project creation and API activation:

1. Create project in Google Cloud for integration.
2. Generate Service Account and Private Key for API access.
3. Add necessary API scopes for integration.

Setting up Google Workspace on OmniVista

To set up Google Workspace on OmniVista:

- Add Google Workspace account on OmniVista.
- Explore IoT Inventory View and IoT Enforcement features.

FAQ

• What version of AOS switches/APs are compatible with Google Workspace Integration?

AOS switches and APs running AOS 8.6R2 and later are compatible.

• Why is an NTP Server required for consistent inventory view?

Syncing Switches/APs to the same NTP Server ensures accurate display and filtering of IoT Inventory data.

• Does OmniVista require an internet connection for operation?

Yes, OmniVista requires an internet connection for effective utilization of the IoT application.

Introduction

This Application Note is designed to guide IT professionals in integrating Google Workspace with OmniVista's IoT inventory, focusing on providing a comprehensive view of Chrome Devices within organizational networks. It details how to connect Google Workspace's device management features with OmniVista's inventory capabilities, enabling organizations to gain valuable insights into their IoT landscape. The emphasis is on enhancing visibility into Chrome Devices, offering IT teams the tools they need to monitor and understand their digital environment effectively.

Prerequisites

Google Workspace/Cloud

- **Google Workspace Enterprise Account with Admin Privileges:** Required for device enrollment and management.
- **Chrome Device Reset to Factory Settings:** Essential if the device was previously enrolled or managed by another organization.
- **Access to Google Workspace Admin Console:** To configure and enable device enrollment.
- **Wi-Fi Network Connection:** Needed for device enrollment.
- **Project Creation and API Activation in Google Cloud:** Necessary for configuration and integration with Google Workspace.
- **Service Account Creation and Private Key:** For authentication and access to Google Workspace APIs.
- **API Scopes Addition to Domain-Wide Delegation:** Allows access to necessary APIs for integration.

OmniVista – Enabling IoT Devices on AOS Switches/APs

The IoT application can be configured to integrate with Google Workspace to collect information on devices. This feature enables network managers to obtain details on devices connected to AOS Switches and Access Points, including devices running Chrome OS.

- Google Workspace Integration is only supported on devices connected to AOS Switches running AOS 8.6R2 and later, or devices connected to APs connected to AOS Switches running AOS 8.6R2 and later.
- IoT is disabled on AOS Switches and APs by default. To enable IoT on a switch/AP, go to the Managed Devices Screen (Network – Discovery – Managed Devices), select the switch(es)/AP(s) in the Managed Devices List, click on the Features drop-down, and select Enable IoT. The switches/APs will appear in the “Enable IoT – Confirm” switch picker window. (Note that switches/APs that do not support IoT will not appear in the window.) Click OK to enable IoT. OmniVista will begin collecting IoT information for endpoints connected to the switches/APs.
- An NTP Server(s) is required for a consistent Inventory view of IoT devices. Switches/APs must be synced to the same time, for OmniVista to correctly display session start time/end time, and sort and filter of IoT Inventory data. Switches/APs must have access to at least one NTP Server, whether local or external.
- To utilize the IoT application effectively, OmniVista, rather than the switch or access point (AP), requires an internet connection. Additionally, if a firewall is in place, it must be configured to permit access to the Device Fingerprinting Service (api.fingerbank.org) to ensure seamless operation.

Google Workspace Device Enrollment

Enrollment

Preparation Steps:

1. Factory Reset Chrome Device (if necessary):

- A factory reset is only required if the Chrome device was previously enrolled or managed by a different organization. If the device is new or was never enrolled, you can skip the factory reset and proceed with enrollment.
- If a reset is required, turn off the device, perform a factory reset according to the manufacturer's instructions, and then power it on once it is complete.

2. Admin Console Access:

- Log in to the Google Workspace Admin Console (admin.google.com).
- Use an account with admin rights.

Configuration in Admin Console:

1. Navigate to Enrollment Settings:

Go to Devices > Chrome > Settings > User & browser settings.

2. Enable Device Enrollment:

- Verify or enable Enrollment & Access settings.
- Ensure settings apply to the correct organizational units.

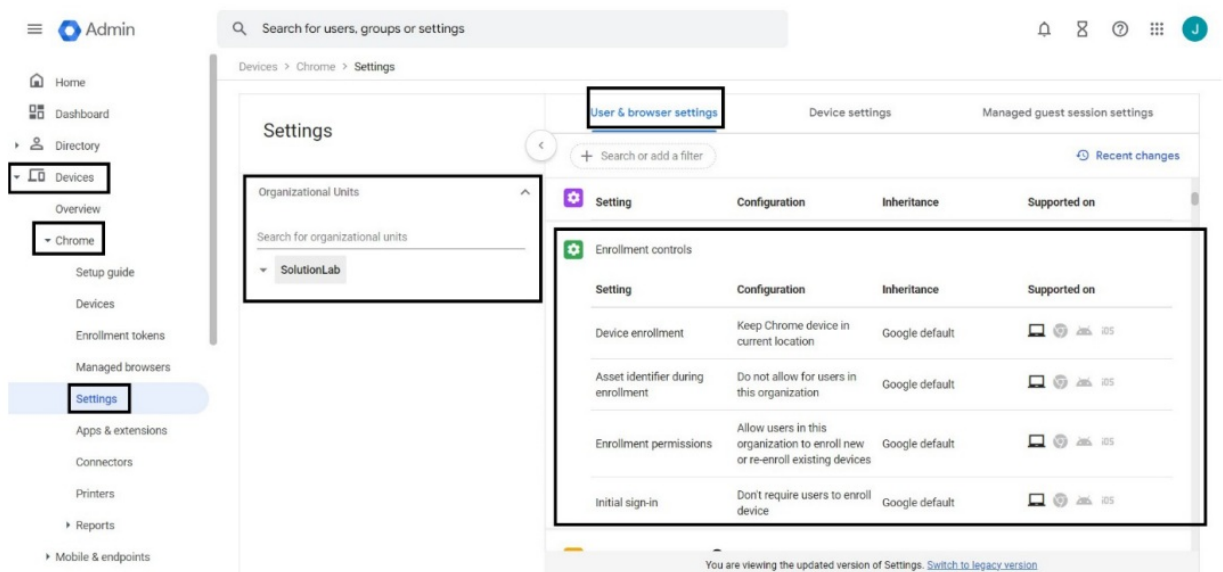


Figure 1: Enabling Device Enrollment

Enrollment Process:

1. Start Device & Connect to Wi-Fi:

- Power on the Chrome device.
- Connect to a Wi-Fi network if not automatically connected.

2. Access Enrollment Screen:

- At the initial login screen, do not sign in.
- Press Ctrl + Alt + E to go to the enrollment screen.

3. Sign In with Admin Account:

- Use a Google Workspace admin account to sign in.
- Follow on-screen instructions to enroll the device.

4. Complete Enrollment:

After enrollment, the device will apply configured policies from the Admin Console.

Post-Enrollment:

1. Verify Device Enrollment:

- Return to Devices > Chrome > Devices in the Admin Console.
- Check for the newly enrolled device in the list.

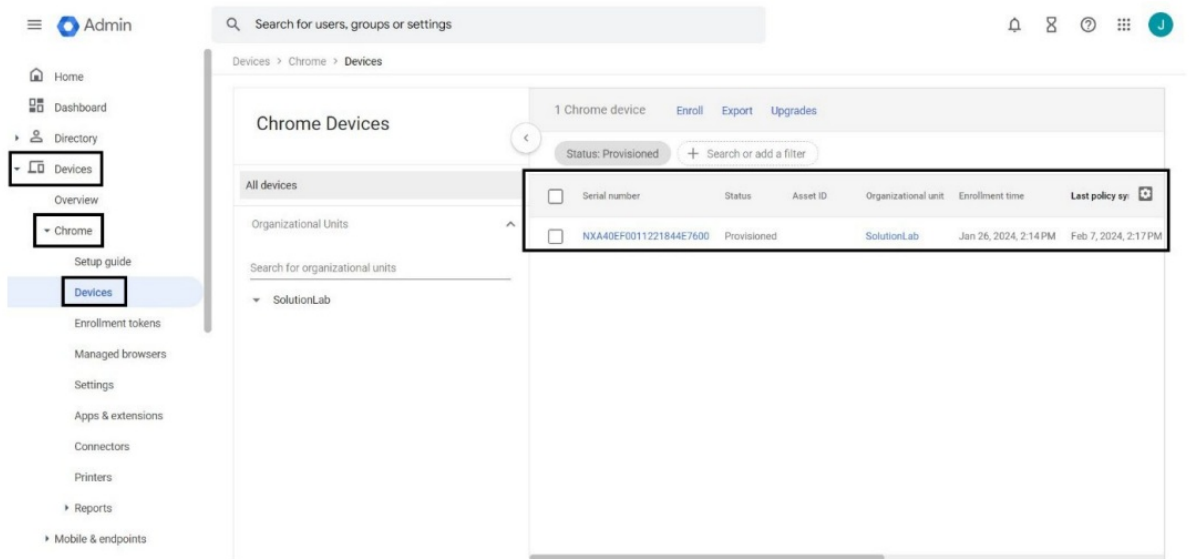


Figure 2: Device Enrollment Verification

The device should now be successfully enrolled and managed under your Google Workspace Enterprise account.

Google Cloud/Workspace Configuration

Project Creation and API enablement

Project Creation Steps:

1. Access Google Cloud Console:

Navigate to the Google Cloud Console (console.cloud.google.com) and log in with your Google account.

2. Create a New Project:

- Click on the project dropdown at the top of the dashboard.
- Name your New Project and select the Organization.

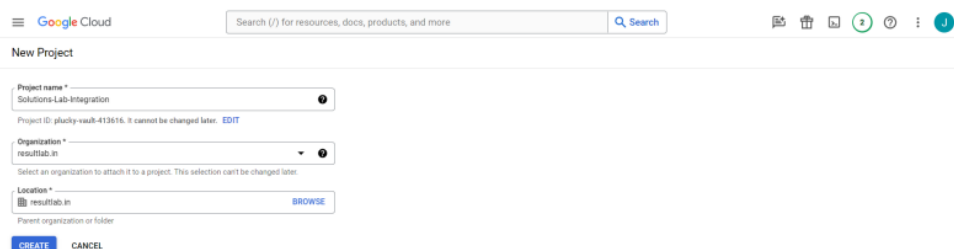


Figure 3: Creating New Project

API Enablement Steps:

1. Navigate to API & Services:

Once the project is created, navigate to API & Services > Dashboard from the main menu.

2. Enable APIs and Services:

Click on + ENABLE APIS AND SERVICES at the top of the page.

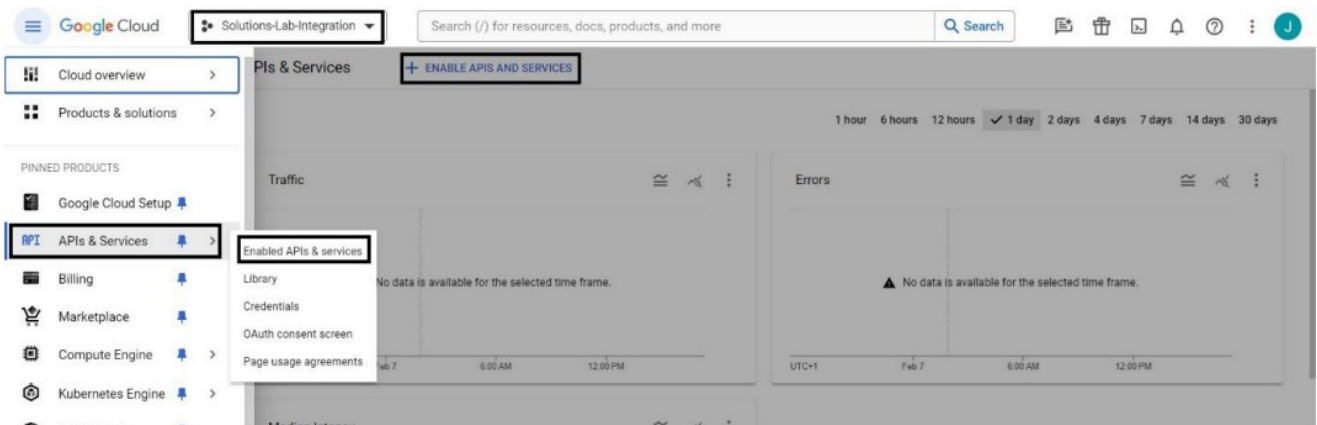


Figure 4: Enabling APIs and Services

3. Search for the Admin SDK API:

- In the API Library, use the search bar to find the Admin SDK API.
- Click on the Admin SDK API to open its details page.

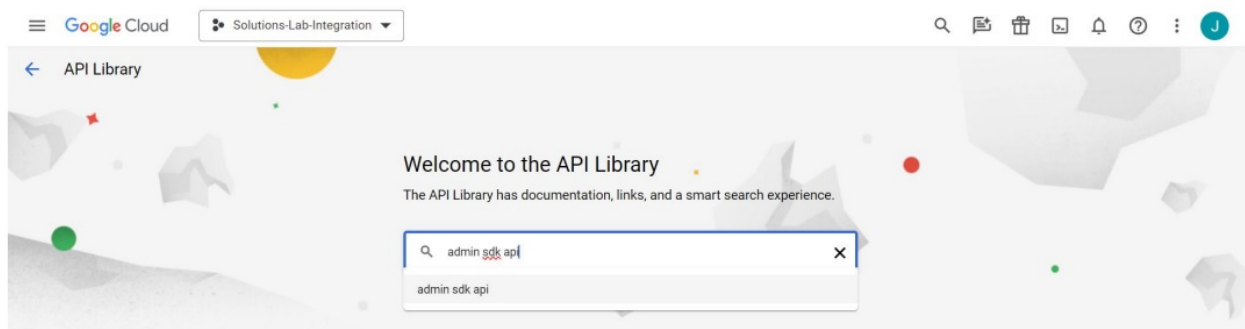


Figure 5: Adding Admin SDK API

4. Enable the API:

Click on the Enable button to activate the Admin SDK API for your project.

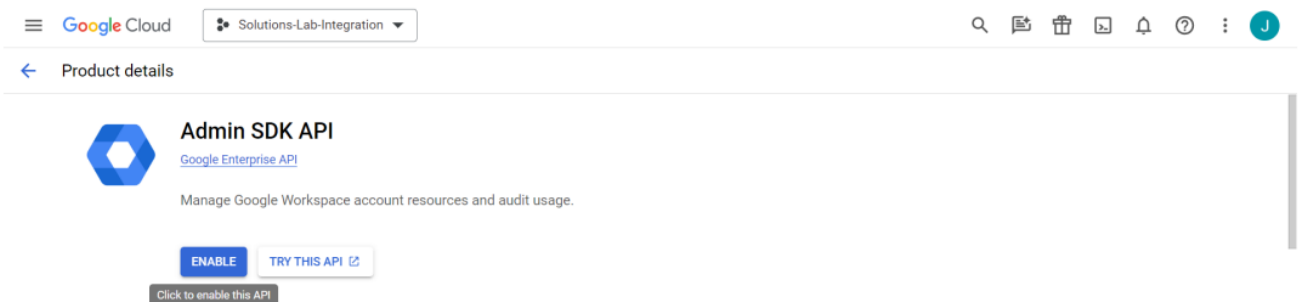


Figure 6: Enabling Admin SDK API

Service Account and Private Key Creation

Preparation Steps:

Access Google Cloud Console:

- Log in to Google Cloud Console (console.cloud.google.com).
- Select the project in which you want to create the service account.

Creating the Service Account:

1. Navigate to IAM & Admin > Service Accounts:

Click on + Create Service Account.

2. Configure the Service Account:

- Enter a Name and Description for the service account.
- Click on Create.
- Skip the optional fields.

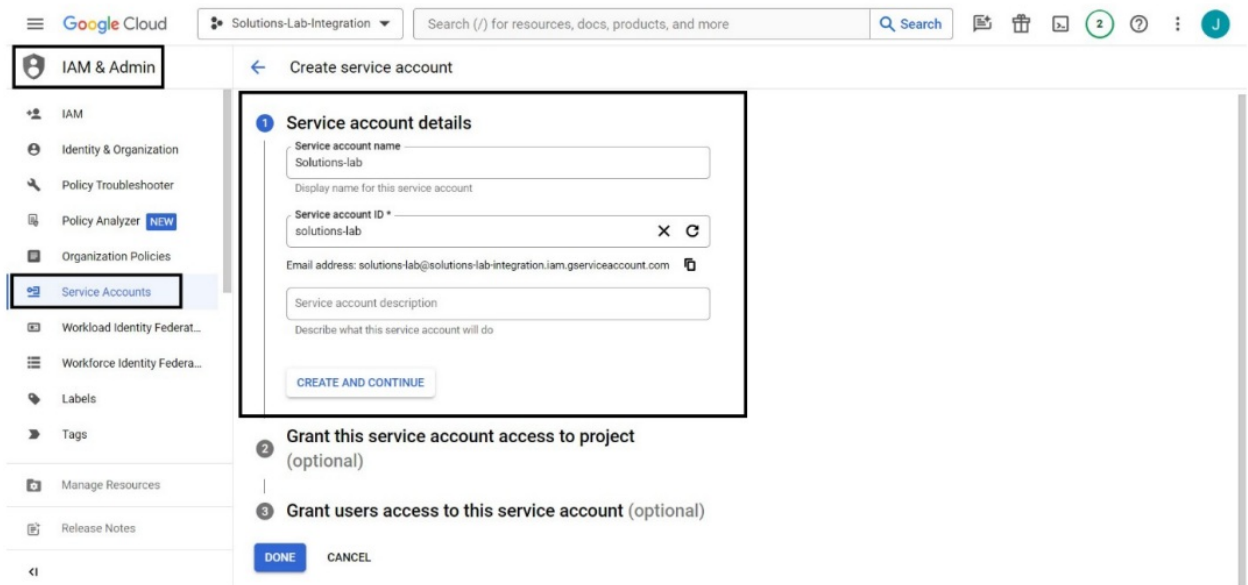


Figure 7: Service Account Creation

Generating the Private Key in P12 Format:

1. Select the Created Service Account:

In the service accounts tab, click on the newly created service account.

2. Add a Key:

- Click on the Keys tab.
- Choose Add Key, then Create new key.

3. Choose the Key Format:

- Select the P12 format.
- Click on Create.

4. Download and Secure the Key:

A .p12 file will be generated and downloaded to your machine.

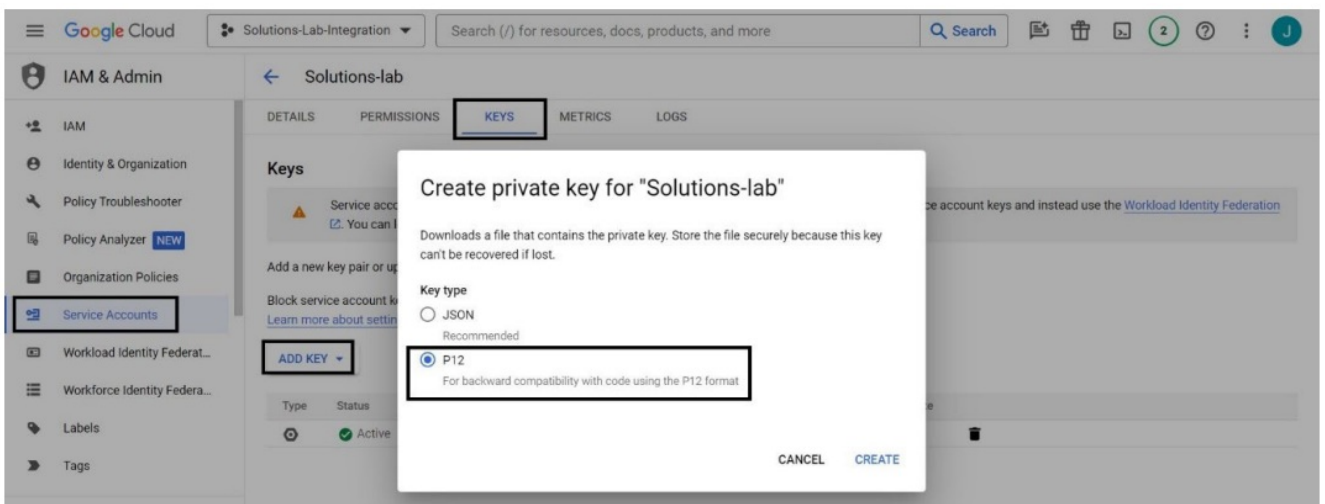


Figure 8: P12 Private Key Creation

Important: Keep this file secure, as it provides access to your service account.

Adding API scopes to Domain Wide Delegation

Steps for Adding API Scopes:

1. Identify Required API Scopes:

Determine which Google APIs your application will access and identify the corresponding scopes. Documentation for each Google API lists the available scopes.

2. Log into the Google Admin Console:

Navigate to the Google Admin Console (admin.google.com) and sign in using your Google Workspace admin account.

3. Access Security Settings:

- In the Admin Console, navigate to Security > API controls.
- In the API controls section, find the Domain-wide Delegation panel and click on Manage Domain Wide Delegation.

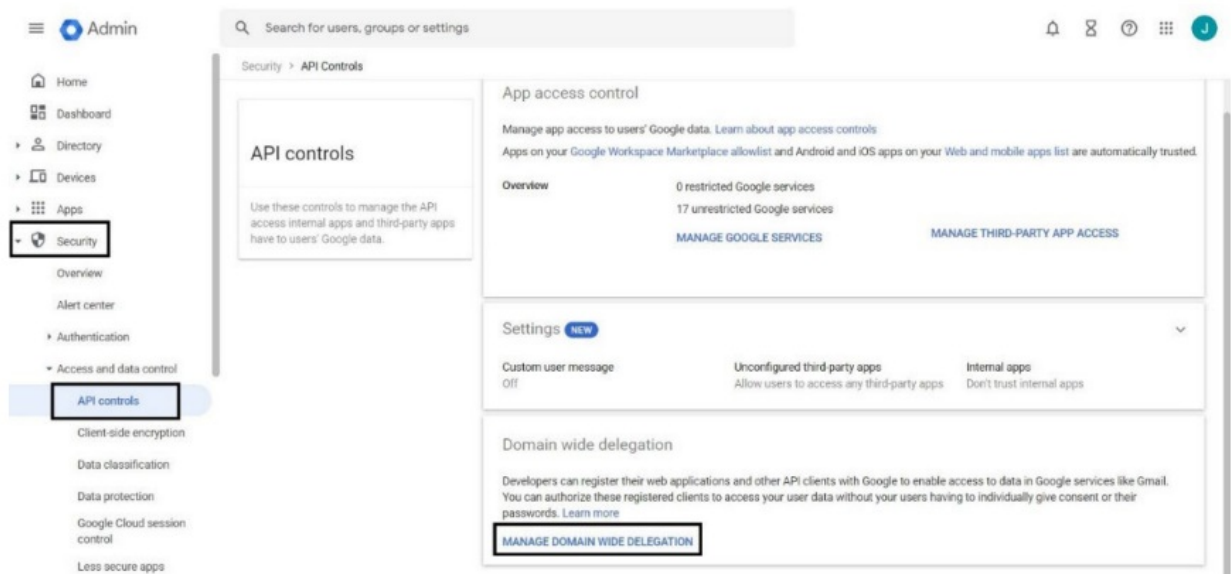


Figure 9: Access to Domain Wide Delegation

4. Add API Scopes to Your Service Account:

- Click on Add new.
- Enter the Client ID of your service account. You can find this in the Google Cloud Console under IAM & Admin > Service Accounts, by clicking on your service account and viewing its details.
- In the OAuth Scopes (comma-delimited) field, enter the API scopes your application requires, separated by commas:
 - <https://www.googleapis.com/auth/admin.directory.device.chromeos.readonly>
 - <https://www.googleapis.com/auth/admin.directory.device.mobile.readonly>
- Click on Authorize.

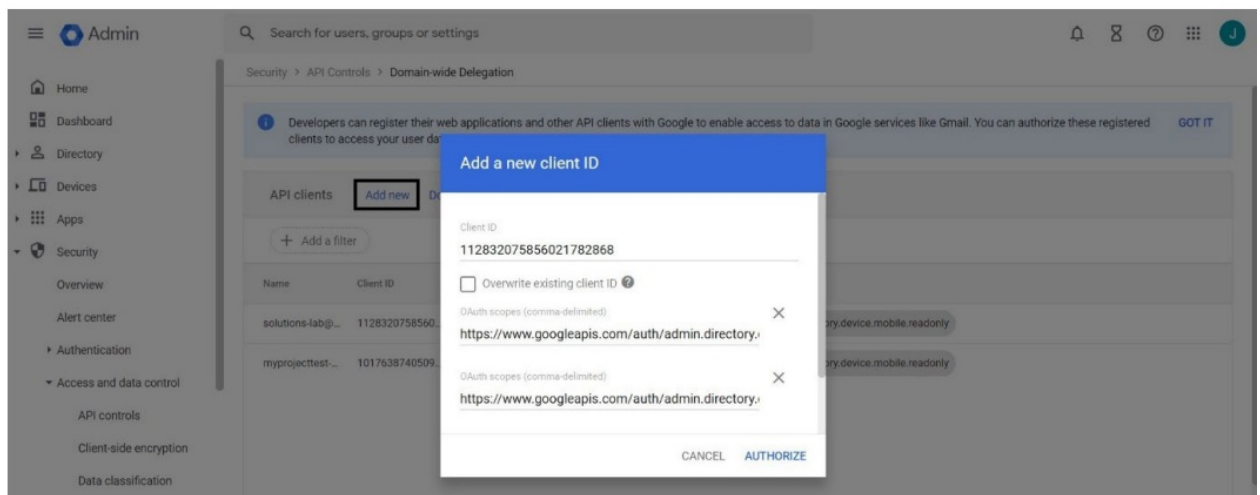


Figure 10: Adding new Client ID for APIs Scopes

Google Workspace on OmniVista

Setting up Google Workspace Account on OmniVista

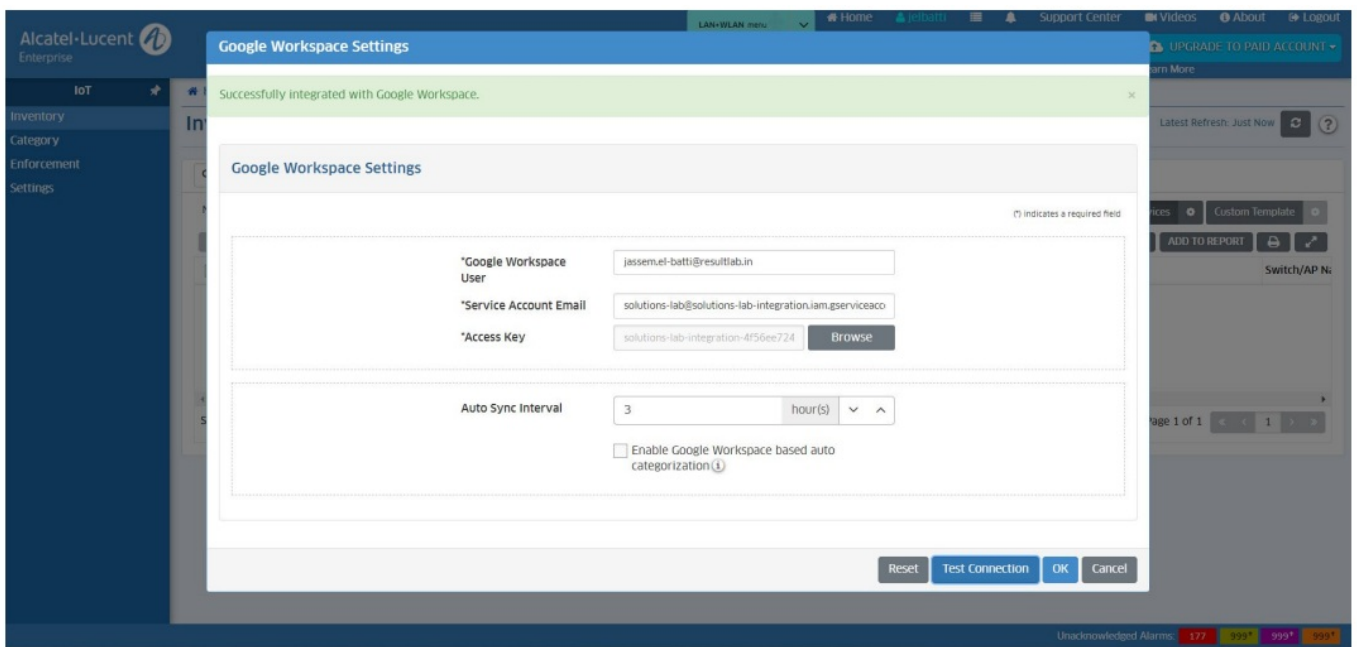


Figure 11: Setting Up Google Workspace into IoT Inventory

Setting up Google Workspace Account

Information Entry:

- **Google Workspace User:** Enter the email address of the Google Workspace administrator who has the necessary permissions.
- **Service Account Email:** Input the email address associated with your Google Cloud Platform service account.
- **Access Key:** Provide the previously downloaded private key corresponding to the service account. Click on Browse to select the key file .p12 format.
- **Setting the Automatic Synchronization Interval:** Set how frequently the application should automatically synchronize information with Google Workspace.
- **Test the Connection:** Before finalizing the settings, use the Test Connection feature to verify that the application can communicate with Google Workspace using the provided settings.
- **Validate the Settings:** If the connection test is successful, save the settings by clicking OK.

IoT Inventory View

- Upon connecting a client or endpoint to an AOS Switch/AP, it triggers the transmission of MQTT messages to OmniVista, providing immediate insights that include device MAC address, DHCP fingerprint, User-Agent, TCP signatures, and network behavior. This initial data set paves the way for OmniVista to utilize a sophisticated cloud-based Device Fingerprinting Service, ensuring accurate device categorization.
- The integration with Google Workspace significantly amplifies the scope of inventory visibility, extending well beyond basic connectivity details. It allows for a comprehensive view of each device, detailing aspects such as Endpoint MAC, IP, Status, Recent Users, OS Version, and Model.
- Importantly, this integration affords a deeper dive into specific Google Workspace data, alongside authentication, location, and other critical information, markedly enhancing the oversight capabilities within the OmniVista.

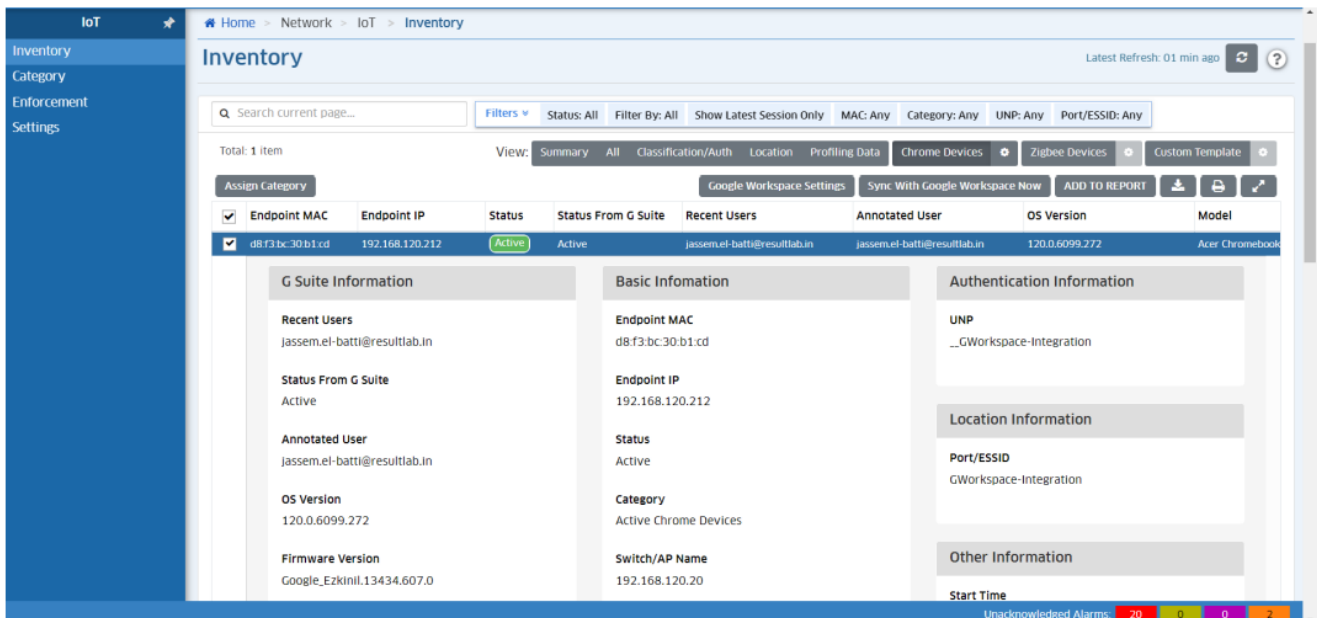


Figure 12: IoT Inventory View

IoT Enforcement

In OmniVista, Chromebook devices that are actively managed and connected appear under the 'Active Chrome Devices' section. Once you have identified the specific category these Chromebooks belong to, you can then navigate to the 'Enforcement' tab. Here, you have the option to apply Access Role Profile (ARP) directly to this category. By doing so, you can enforce consistent network policies across all active Chromebooks, ensuring that they conform to your organization's security standards and access privileges. This centralized approach simplifies the management of device policies.

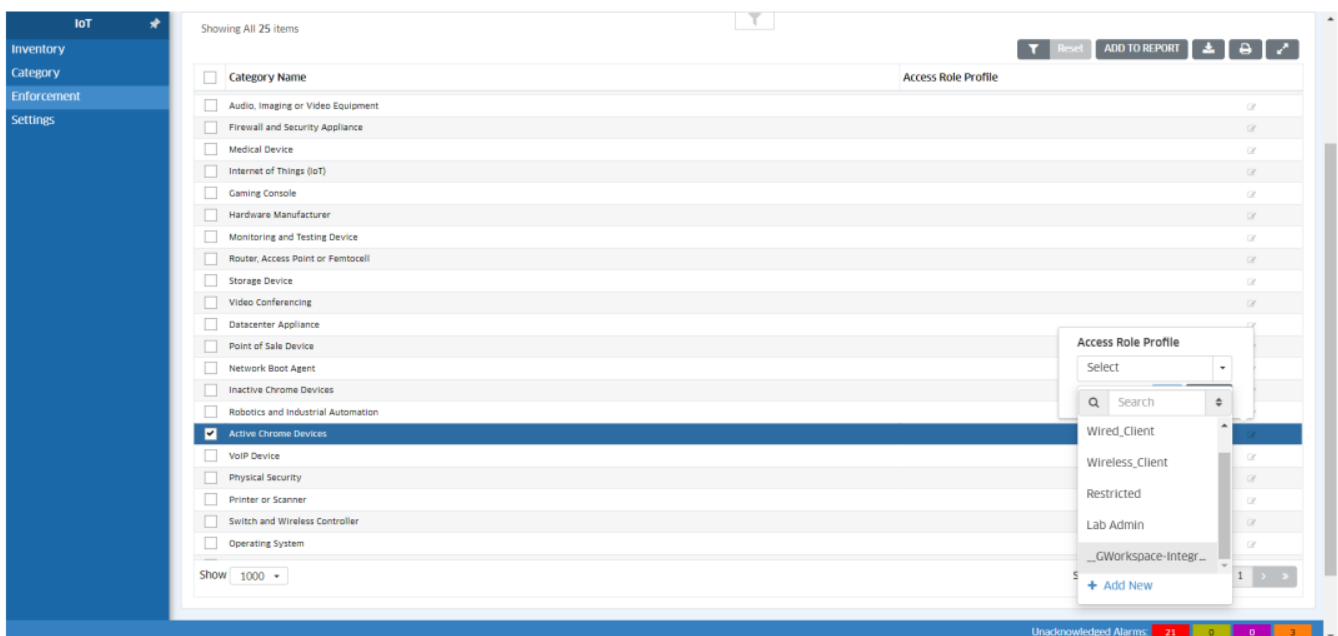


Figure 13: IoT Enforcement

Conclusion

In conclusion, this Application Note delves into leveraging OmniVista for efficient view of Chrome Devices, with a significant emphasis on inventory management. Aimed at IT professionals, it provides a comprehensive exploration of how OmniVista can streamline Chrome Device oversight, focusing on inventory accuracy. Through effective inventory management, organizations can enhance efficiency and gain a coherent understanding of their device landscape. Access Role Profiles (ARP) can be used as a feature to further refine management processes




as needed.

Documents / Resources



[Alcatel Lucent IoT Inventory Integration with Google Workspace](#) [pdf] User Guide
IoT Inventory Integration with Google Workspace, IoT Inventory Integration with Google Worksp
ace, Inventory Integration with Google Workspace, Integration with Google Workspace, with Go
ogle Workspace, Google Workspace, Workspace

References

-  [Fingerbank - Devices index](#)
-  googleapis.com/auth/admin.directory.device.chromeos.readonly
-  googleapis.com/auth/admin.directory.device.mobile.readonly
- [User Manual](#)

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.