gluware
Intelligent Network Automation

APPLICATION NOTE

Automate Meraki using Gluware
Part 1: Device Manager and Config Drift and Audit

TABLE OF CONTENTS

OVERVIEW

While the Meraki solution is feature-rich, the steps to configure and manage are more complicated, often requiring many clicks to navigate into network settings and device settings. As enterprises scale to hundreds or thousands of devices, the Meraki Cloud must be automated. Meraki does offer a rich Dashboard API users can leverage to enable 3rd party automation through Gluware.

Powered by API Modeling, Gluware expanded its automation capability of Meraki to enable Gluware applications to perform inventory, config drift, config audit, config management and process automation. Through integration with the Meraki REST API, and secure API keys, Gluware reads the inventory details along with all the configuration parameters available through the Meraki Dashboard. Meraki provides over 300 API calls Gluware leverages to provide automation and simplify operational tasks as enterprise users scale-out deployments. Performing a network assessment is a recommended starting point for any project that involves equipment refresh planning, lifecycle management planning, network automation or many other initiatives that make changes to the network infrastructure. Before making changes, it is critical to have current data regarding the inventory, configuration state and operational state.

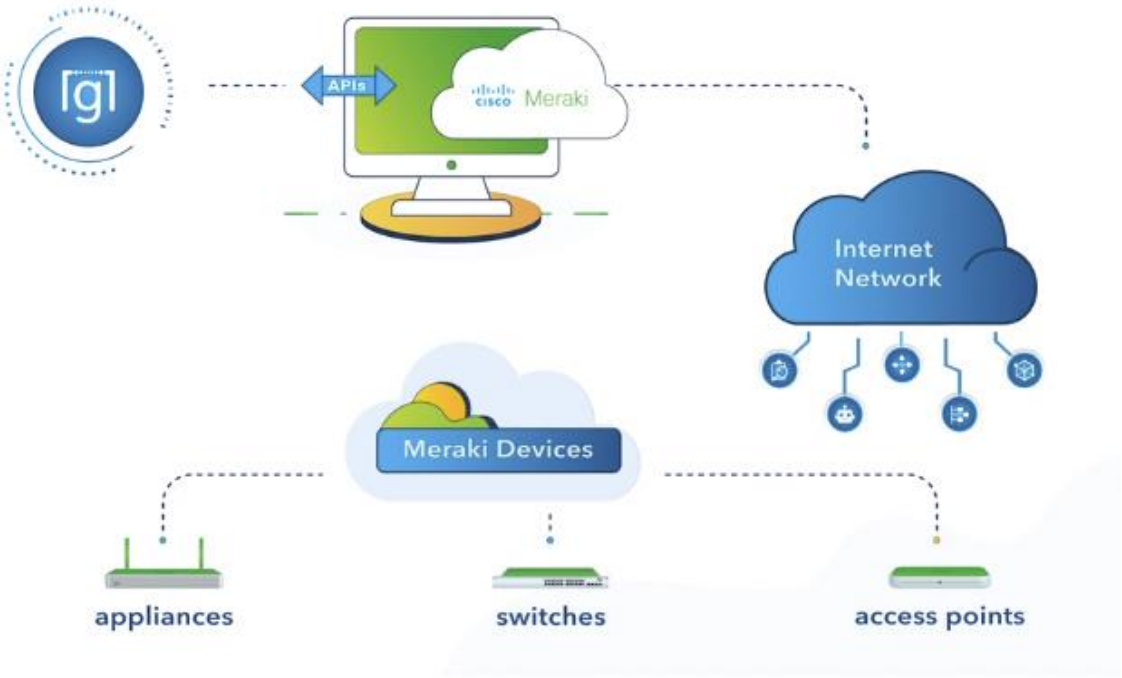


Figure 1 Gluware automating Meraki via API

Gluware provides automation through the Meraki Dashboard API using applications such as:

- **Device Manager** – View your inventory details across orgs and networks
- **Config Drift & Audit** – Identify config drift and execute no-code config audits
- **Config Model Editor** – Automate config changes across orgs, networks and devices
- **Network RPA** – Automate end-to-end processes with Gluware and 3rd party integrated tasks

Part 1 focuses on the Device Manager and Config Drift & Audit applications. Part 2 dives deeper into how Gluware provides simplicity and scale to automate adding new organizations, networks, devices, VLANs, and more, enabling users to configure thousands of network devices in minutes.

GETTING STARTED

Automating Meraki with Gluware requires two steps to set up the system. First, set up the Meraki Organization by obtaining a Meraki API key, including the credential and connection. Second, set up your Gluware Organization by installing the Meraki package. For more information, see the Meraki API Docs.

Create a Meraki Credential

To interact with the Meraki Dashboard via a 3rd party API, you must first obtain an API key.

- Open your Meraki dashboard: https://dashboard.meraki.com
- Once logged in, navigate to the **Organization > Settings** page.
- Ensure that API Access is set to **Enable access to the Cisco Meraki Dashboard API**.

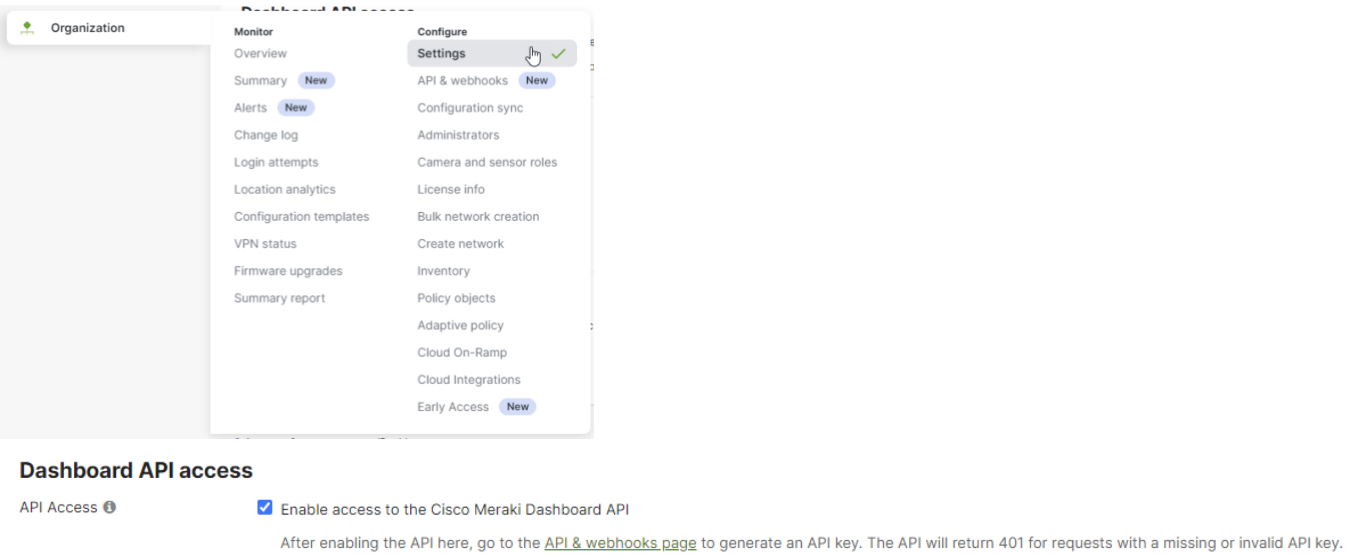


Figure 2 In the Meraki Org -> Settings enable API access

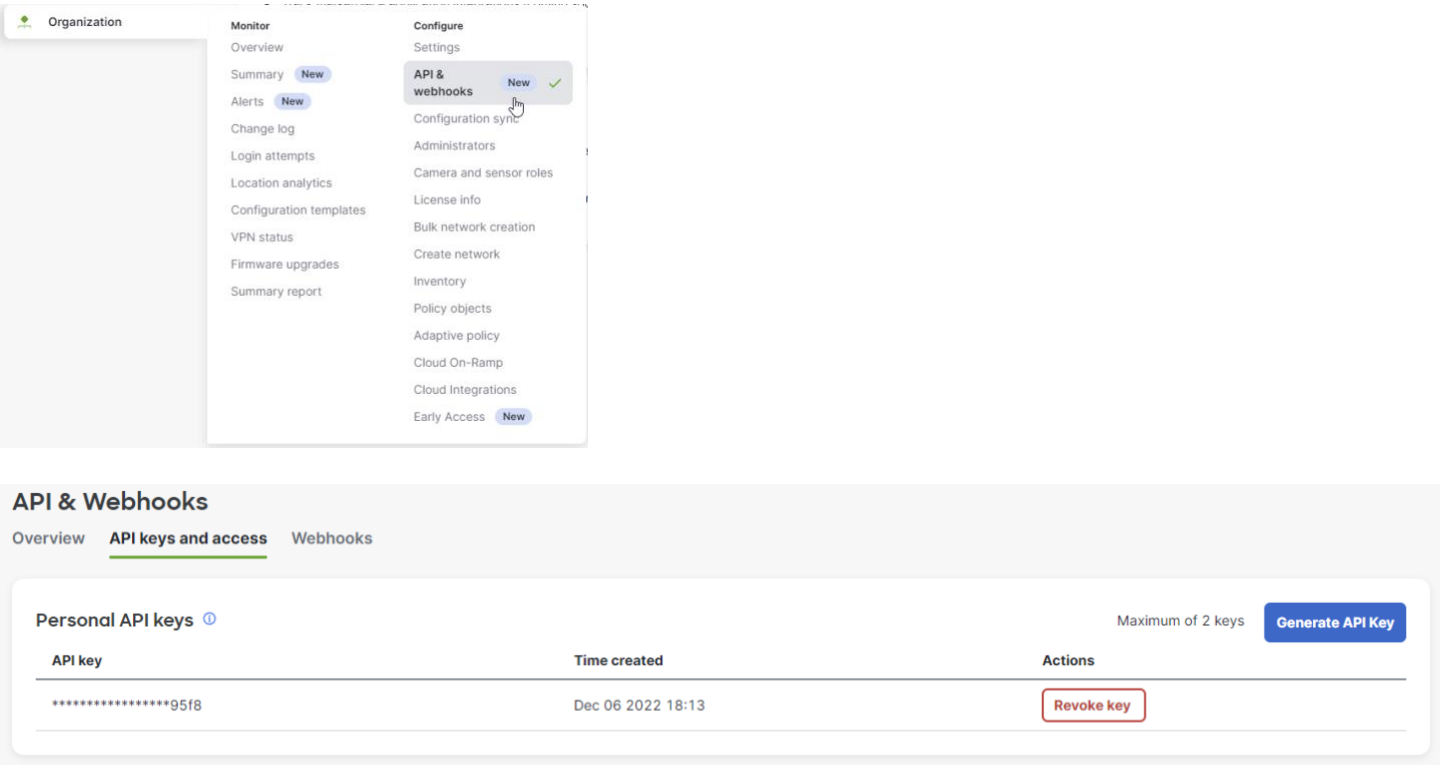


Figure 3 In the Meraki Org -> API & Webhooks generate the API key

Note: The key has the same permissions as the user and requires read/write access for full Gluware support.

Install the Required Gluware Packages

To automate Meraki using Gluware, you must have the required packages installed. In your Gluware instance, navigate to the Solutions Manager:

- Ensure the current Gluware Core Solutions package is installed
- Ensure the current Config Modeling Kit for Cisco Meraki is installed

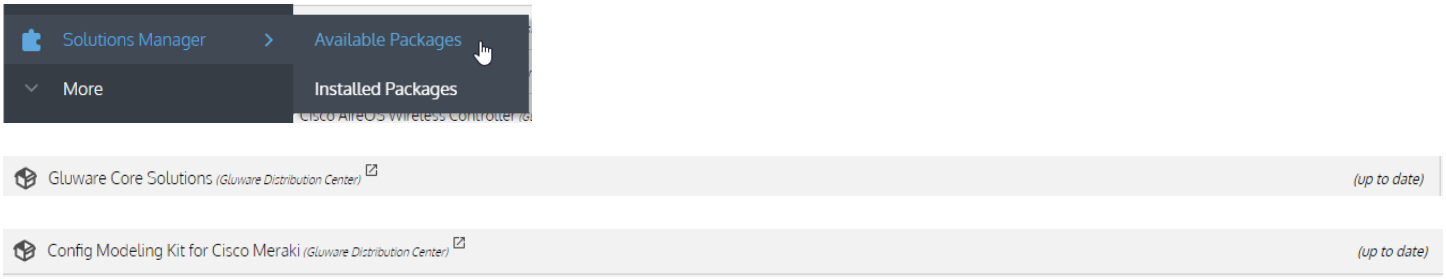
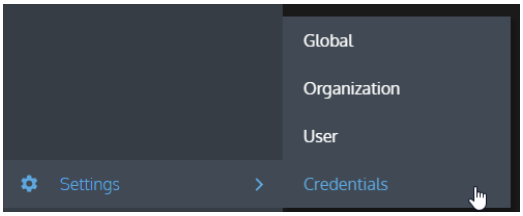


Figure 4 In the Gluware Solutions Manager, install/update the required packages

Add the Required Meraki API Credentials in Gluware

In your Gluware instance, navigate to the **Credentials Manager Settings -> Credentials**:

- Add the Meraki API credentials and validate the connection



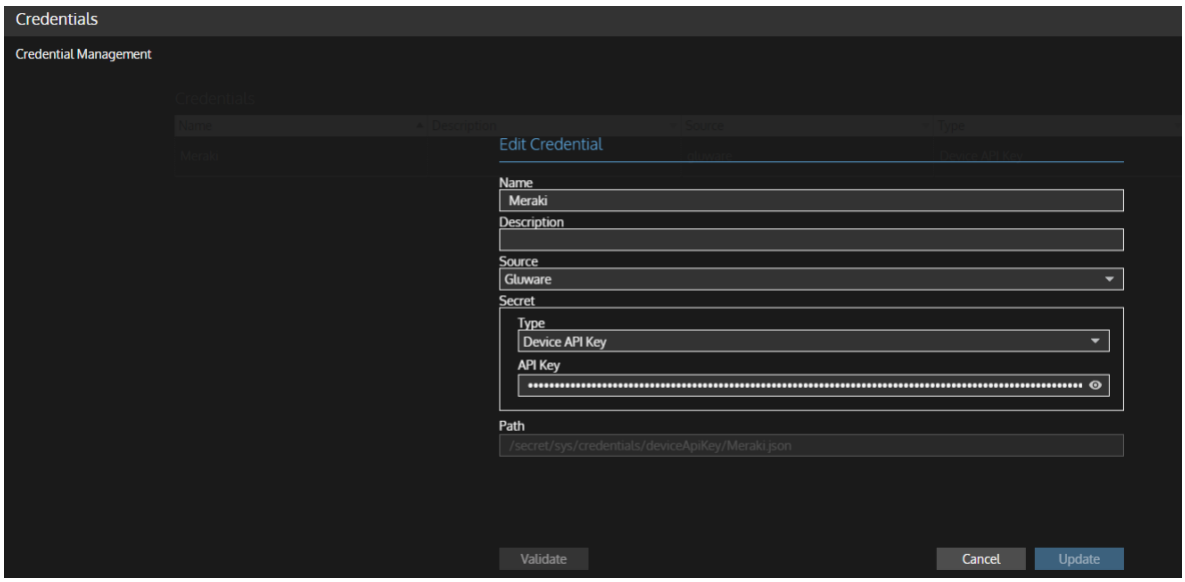


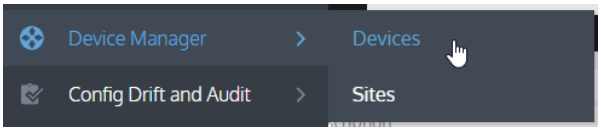
Figure 5 In the Gluware Credential Manager, add and validate the Meraki API key

DEVICE MANAGER

Use the Gluware Device Manager application to define the connection to the Meraki API and perform a discovery that imports the orgs, networks and devices into Gluware that the API credential has access to.

Add the API connection information in Device Manager

Configure the API connection by adding a device in Device Manager:



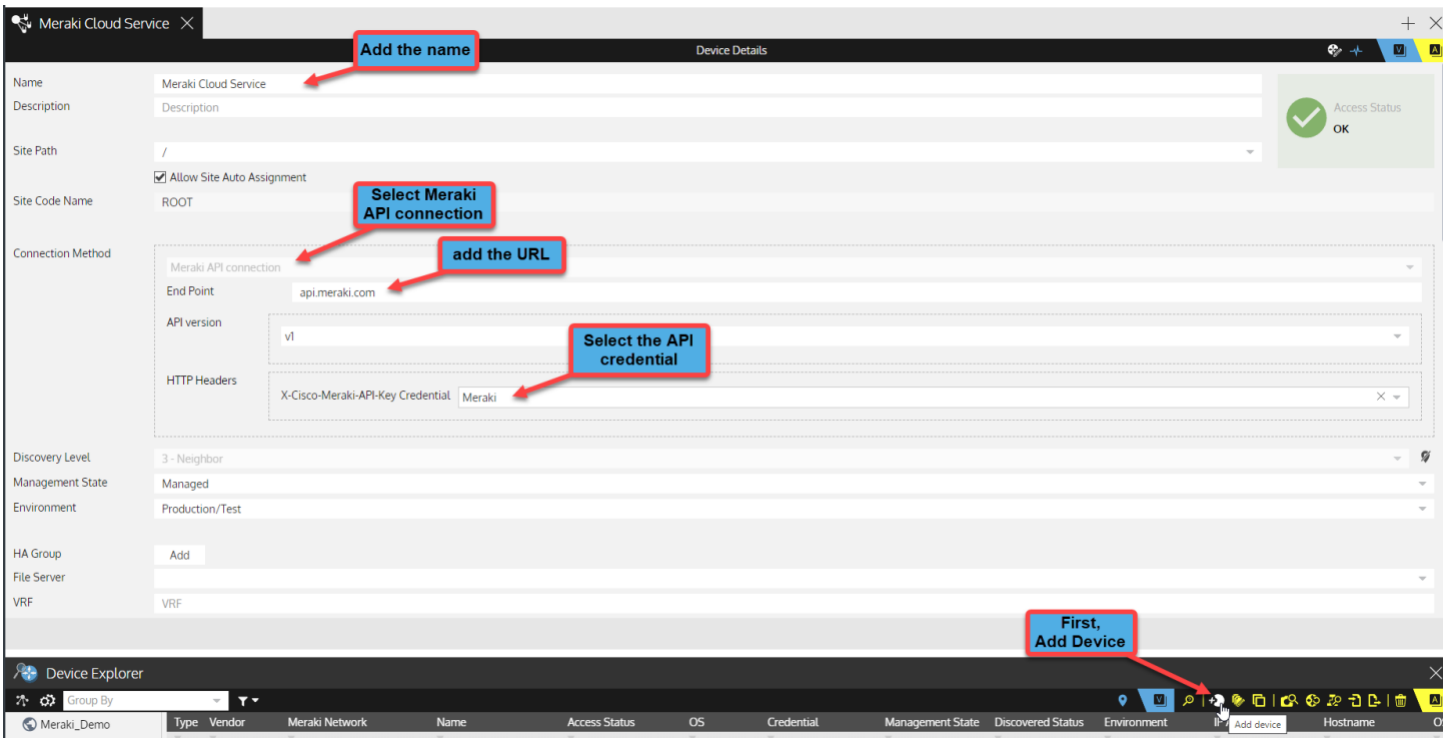


Figure 6 Add a device in Device Manager

In your Gluware instance, navigate to the **Device Manager** app:

- First, click the **Add device** icon on the Device Explorer action bar
- Next, use the dialog box to configure the device details including the connection method via API

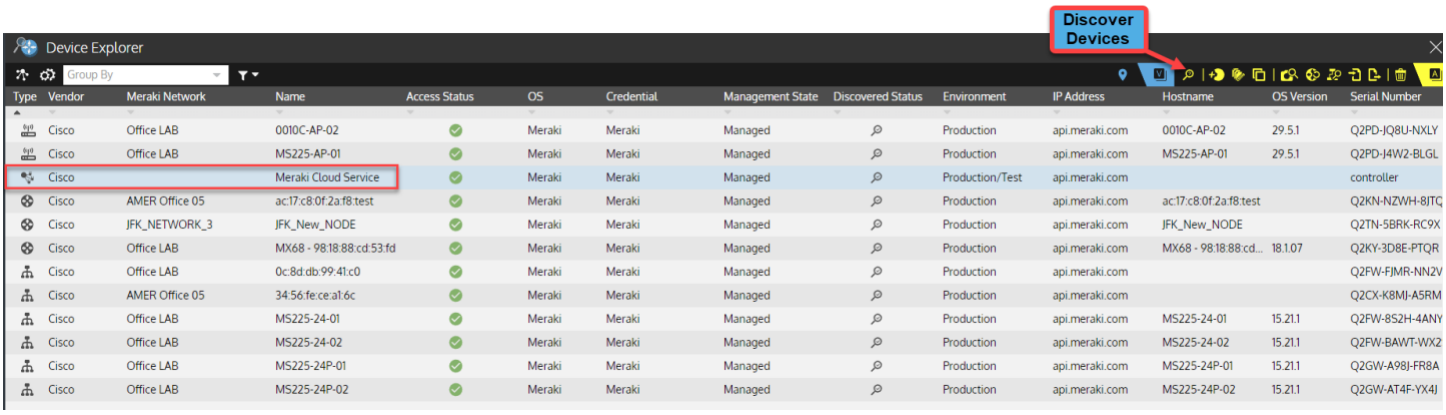


Figure 7 Select the Meraki Controller and execute a discovery

As shown in *Figure 7*, select the Meraki controller by clicking on it, then click the **Discovery devices** icon in the Device Explorer action bar menu. Gluware performs an API-based discovery to import the Meraki orgs, networks and devices, along with the configuration from the controller. The Device Explorer grid populates with all the discovered devices.

Use Device Manager to:

- ✓ Assess the hardware inventory including vendor model, SKUs, and components
- ✓ Assess the OS versions running in the network

Hardware Inventory

Use Device Manager to understand exactly what platforms are running in your network.

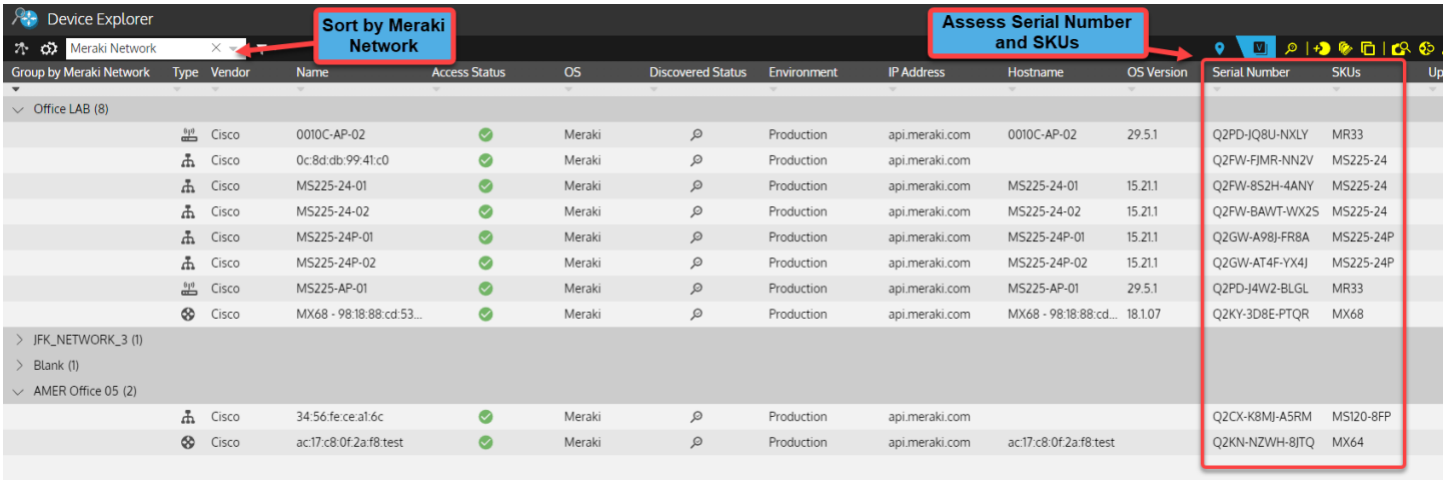


Figure 8 Use Device Explorer to sort, search and filter to assess device details

Operating System

Use Device Manager to assess operating system (OS) and assess if standards are implemented and enforced. Non-standard operating systems create security vulnerabilities and inconsistencies in features and performance.

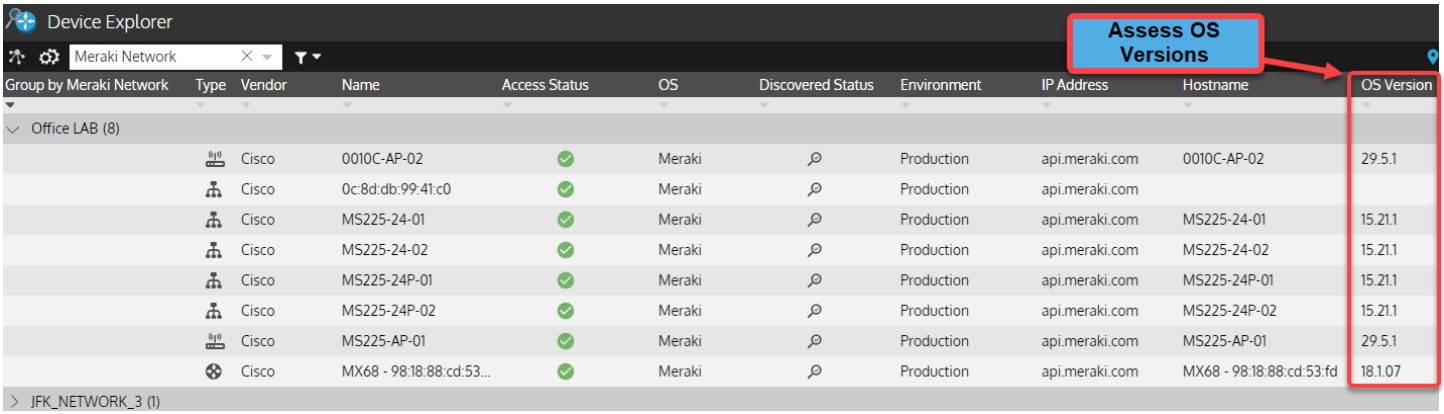


Figure 9 Use Device Manager to assess the Operating Systems

CONFIGURATION DRIFT

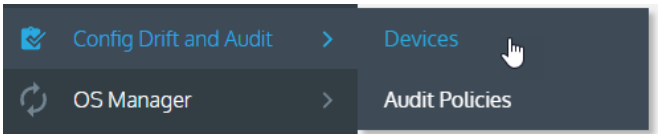
Using the Meraki Dashboard provides an intuitive user experience to configure orgs, networks and devices. However, if manually configuring through the dashboard UI, it can result in configuration mistakes and inconsistencies. Gluware Config Drift performs a “snapshot” to capture the configuration and provide comparisons of a current snapshot with a previously known snapshot, called the default. Users can also compare any previous snapshot to see configuration changes.

Use Config Drift to assess configuration changes for:

- ✓ Rapid troubleshooting to identify what changed
- ✓ Perform ad-hoc, scheduled or triggered drift detection
- ✓ Identify what changed for network remediation (manually or automatically)

Configuration Drift Monitoring

Navigate into the **Config Drift and Audit** app in the Devices view. From Device Explorer, users can execute a new capture snapshot. After the first capture, subsequent capture is available for comparison to see exactly how the config changed.



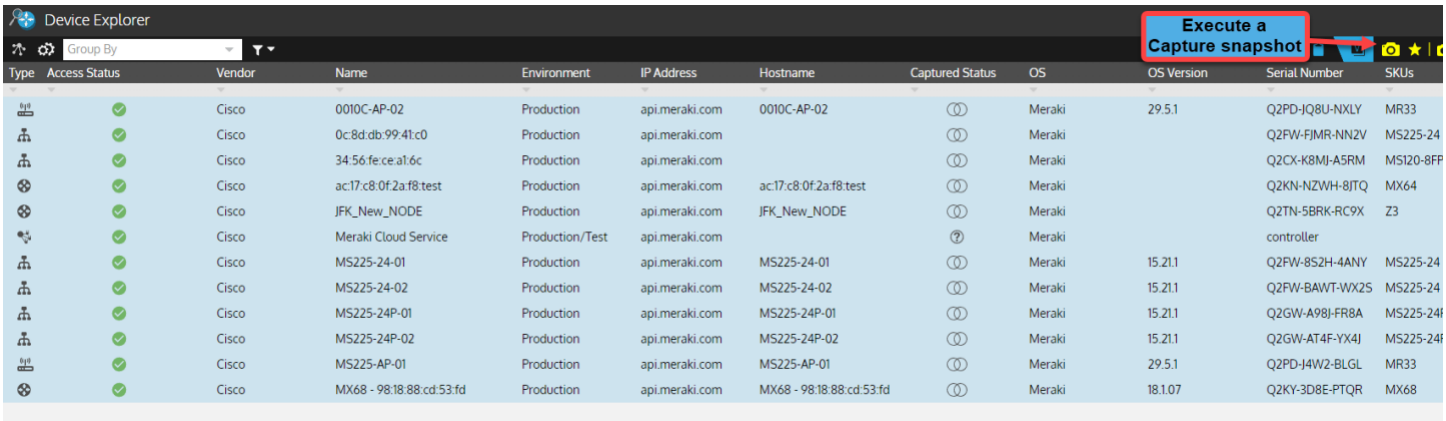


Figure 10 Navigate into the Config Drift Devices view, select devices and execute a capture snapshot

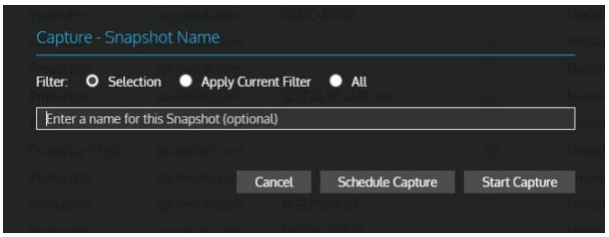


Figure 11 Schedule a periodic capture, or start the capture

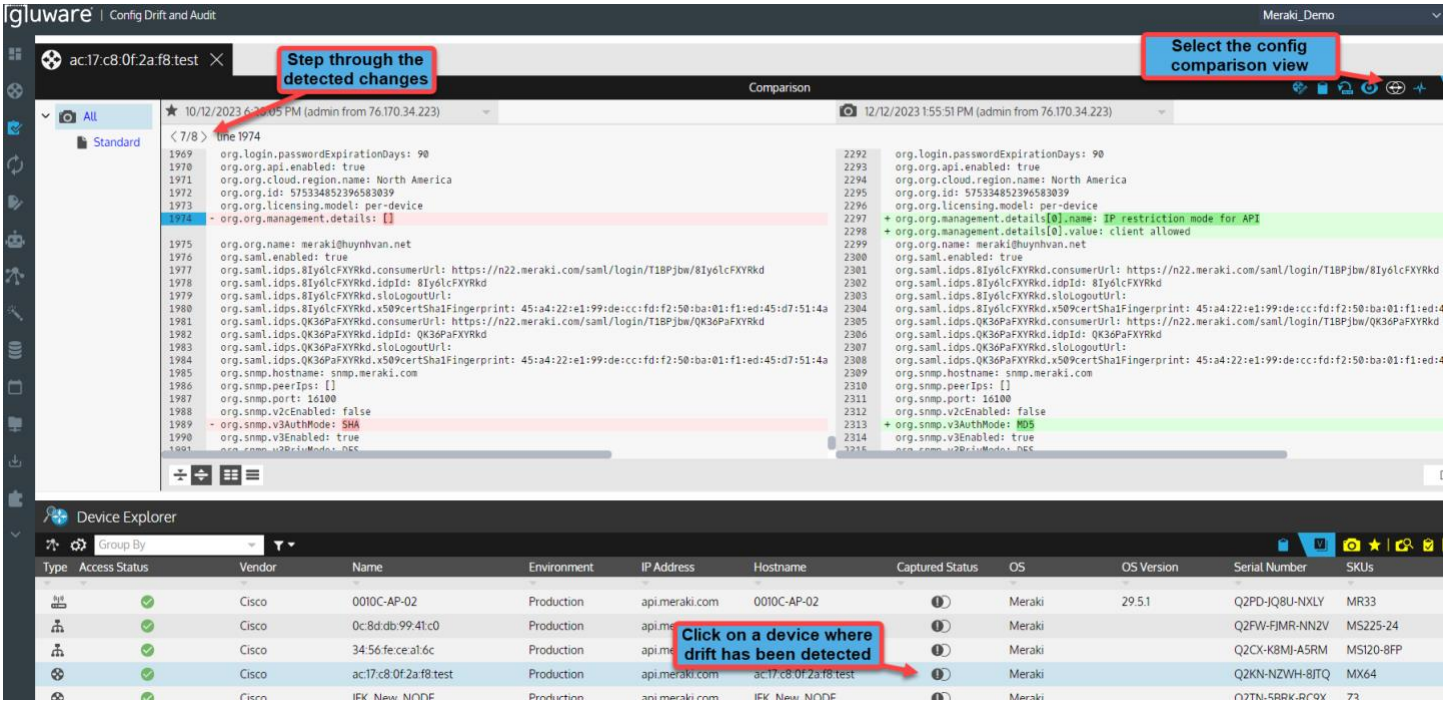


Figure 12 When drift is detected, use the comparison view to see what changed

If the configuration change is unexpected, it can be fixed using the Meraki Dashboard, or by automating the change using the Gluware Config Model Editor application.

CONFIGURATION AUDIT

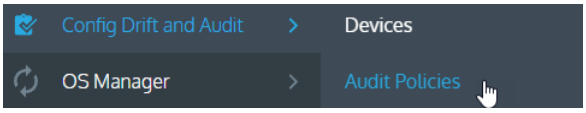
The Gluware Config Drift and Audit app enables users to execute multi-vendor, multi-platform audits without any coding required. Users easily define audits for company policy, ad-hoc policy and standards-based policies. Audit policies are comprised of multiple rules defining required or forbidden configuration statements. Build audit rules using native vendor CLI/API and RegEx supported for configuration policy. Run audits network-wide, or on a specific set of devices, either manually run, triggered, or scheduled. Results are available in the UI and can be downloaded in csv format.

Use Audits to assess configurations for:

- ✓ Standard company policies
- ✓ 3rd party compliance audits
- ✓ Security standard audits

Audit for Meraki Configs

Navigate into the **Config Drift and Audit** app in the Audit Policies view. From the Audit Policy Explorer, users can execute a new capture snapshot. After the first capture, subsequent capture is available for comparison to see exactly how the config changed.



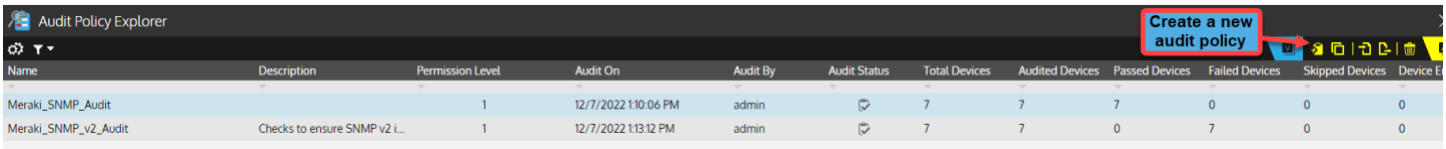


Figure 13 Users can select an existing audit policy or use the "Create policy" icon to create a new one

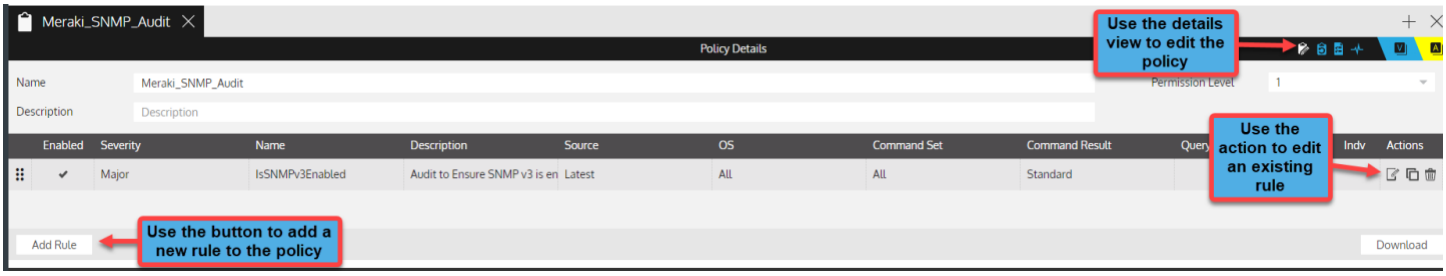


Figure 14 Use the details view to edit the audit policy

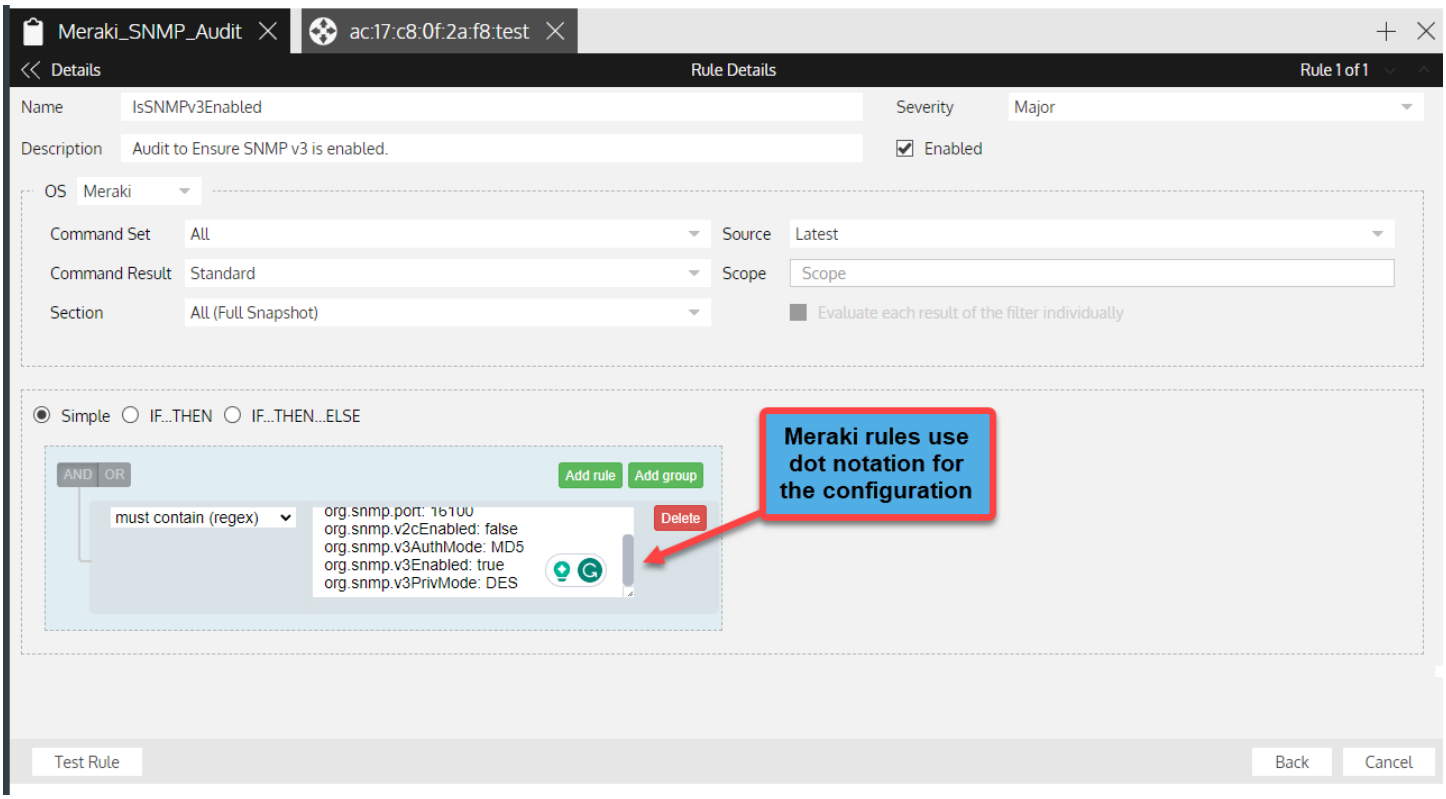


Figure 15 Create no-code audit rules to assess the Meraki configurations

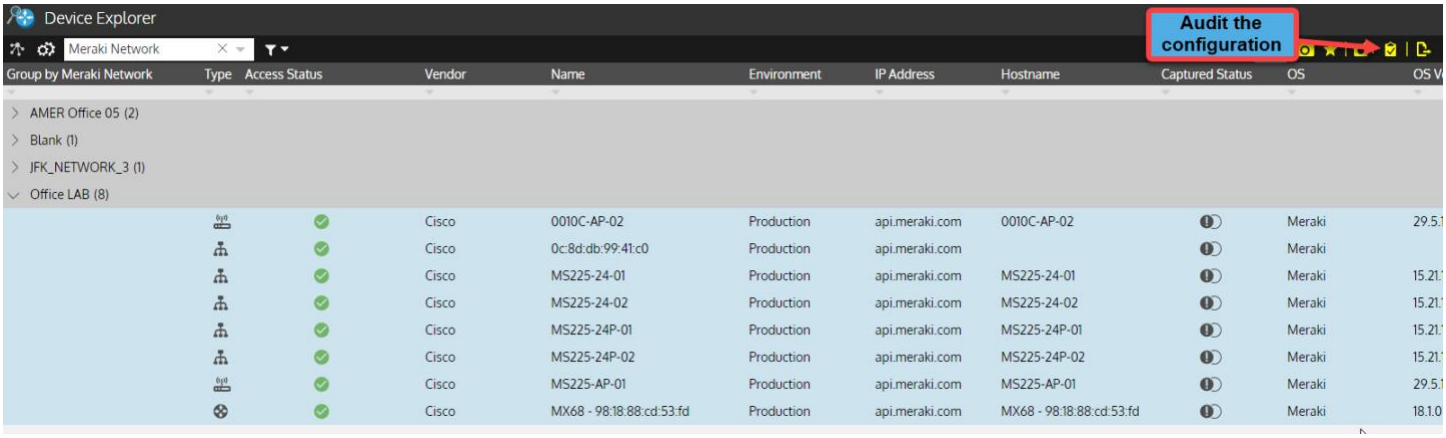


Figure 16 Select devices and click "Audit Configuration" to execute an audit

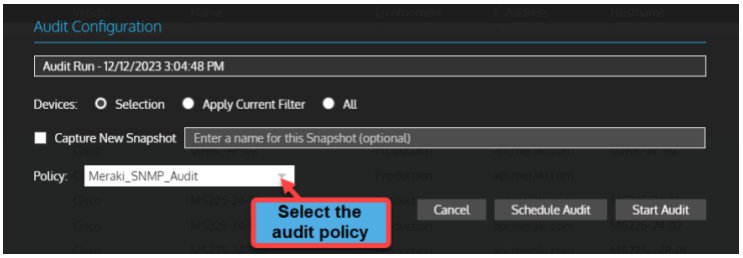


Figure 17 Select the audit policy and schedule or start the audit.

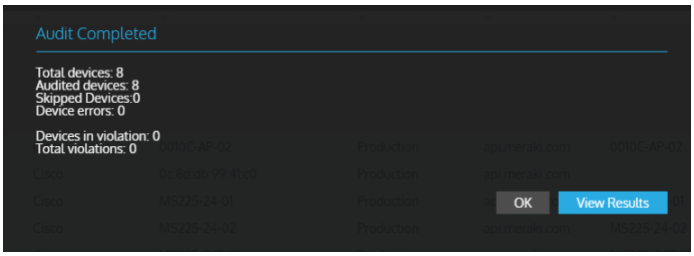


Figure 18 View audit summary results and click "View Results" to see the detailed results

REPORTING

Artifacts are a key deliverable for any automation project. This includes archiving the raw data, as well as processing the data to provide key insights and assessments based on that data. Gluware provides numerous ways to view, process and assess the data extracted from the network infrastructure. Beyond capabilities of the native applications previously mentioned, like Device Manager, Config Drift and Audit and Config Modeling, Gluware has two specific applications to provide data-driven insights.

Dashboard

The Gluware Dashboard app provides a rich graphical view of the underlying data captured from the network infrastructure. Numerous example dashboards provide administrative and app-specific views. Dashboards are fully customizable using a drag-and-drop editor and library of widgets. These include rich text notes, web pages, RSS feed, counts, tables schedules, user activity, and more.

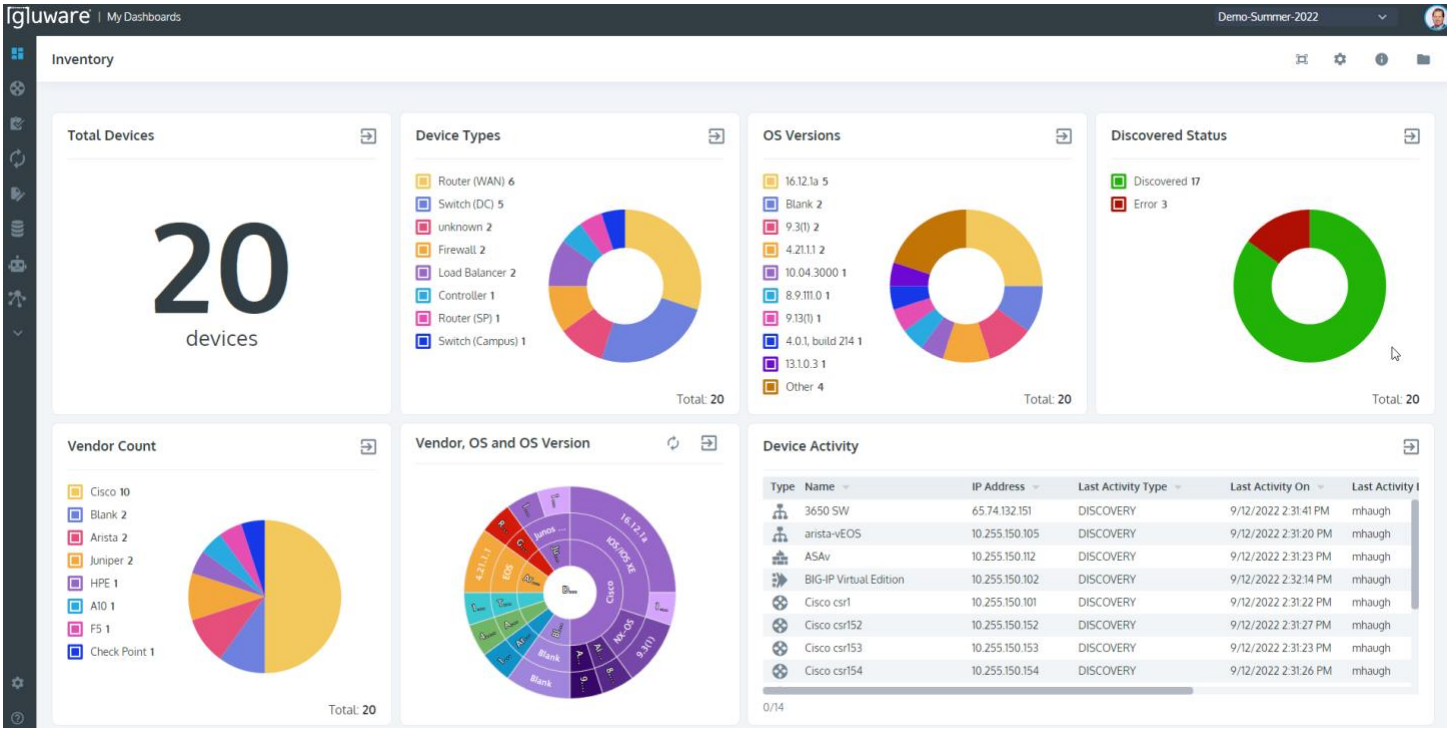


Figure 19 Use Gluware Dashboard to visualize the data from the network infrastructure

Data Explorer

Data Explorer offers unparalleled visibility into network data that enables NetOps teams to automate networks based on actionable, data-driven insights to enhance agility, performance, and security. The Data Explorer solution is powered by direct access to the underlying databases within the user's Gluware instance enabling users to assess network information faster.

Use Data Explorer to:

- ✓ Access to the data from each Gluware app
- ✓ Access platform, configuration and operational state data
- ✓ Create custom default reports for each app
- ✓ Leverage the created report templates from each app once created

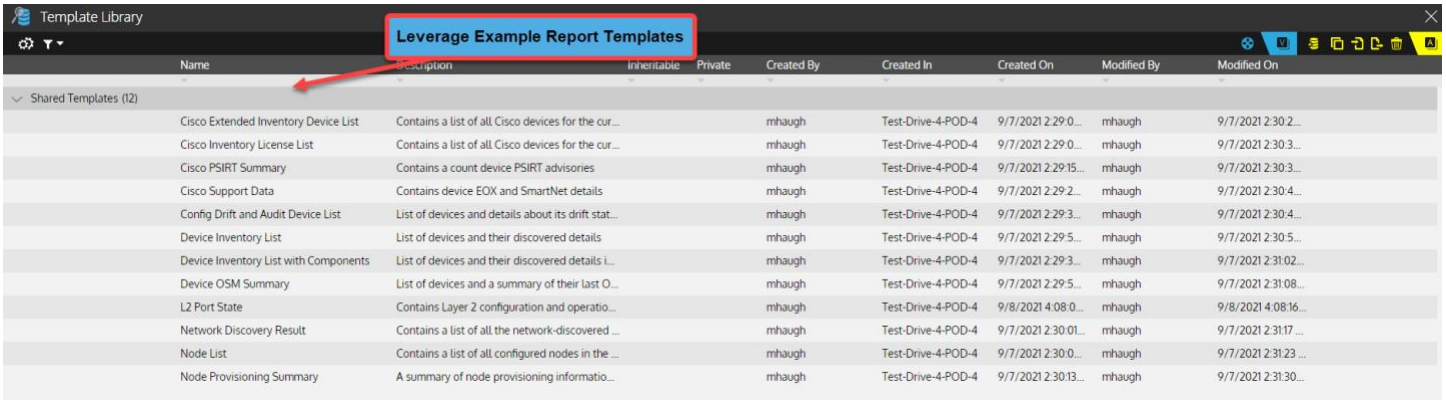


Figure 20 Use Gluware Data Explorer to generate reports leveraging example templates

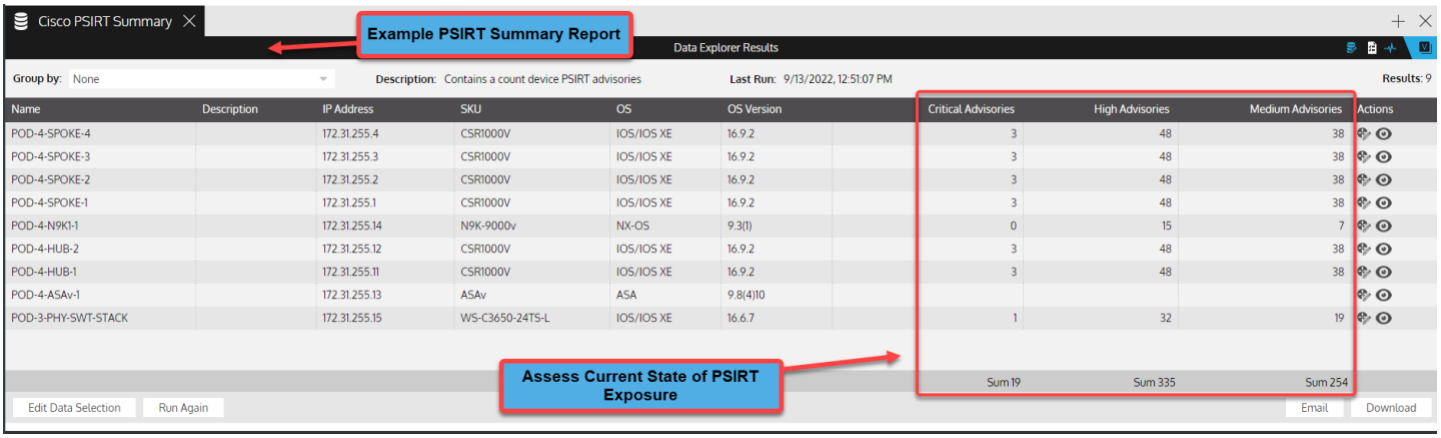


Figure 21 Gluware Data explorer example PSIRT summary r

CONCLUSION

While the Meraki Dashboard is easy to navigate and provides intuitive form-fill configuration pages, the difficulty comes when users make errors creating inconsistency in the configuration. As shown in this application note, Gluware provides a view of your full inventory and the ability to see config drift (what changed) along with no-code config audits (what is not standard) to keep the network in policy and compliant.

Part 2 of this series describes using the Config Model Editor application to automate configuration changes. Then, using no-code process automation with Network RPA, users build workflows to automate remediation and other use cases.

Additional Gluware Resources

Watch a demo of Gluware Automating Meraki Network Settings

Watch a demo of Gluware Automating Meraki Device IP Helpers

Watch a demo of Gluware Automating Meraki and ServiceNow

Watch a demo of Gluware Automating Meraki Deployments using Network RPA

Watch a demo of Gluware Automating Meraki Switch Stacks, SVIs and VLANs

gluware®
Intelligent Network Automation

2020 L Street, Suite 130, Sacramento, CA 95811 | www.gluware.com