

APPLICATION NOTE

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

TABLE OF CONTENTS

TABLE OF CONTENTS	2
OVERVIEW.....	3
GETTING STARTED.....	4
Create a Meraki Credential.....	4
Install the Required Gluware Packages	5
Add the Required Meraki API Credentials in Gluware.....	6
DEVICE MANAGER.....	7
Add the API connection information in Device Manager	7
Hardware Inventory.....	8
Operating System	9
CONFIGURATION DRIFT.....	10
Configuration Drift Monitoring.....	10
CONFIGURATION AUDIT.....	12
Audit for Meraki Configs	12
REPORTING.....	14
Dashboard	14
Data Explorer.....	15
CONCLUSION	16
Additional Gluware Resources.....	16

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.

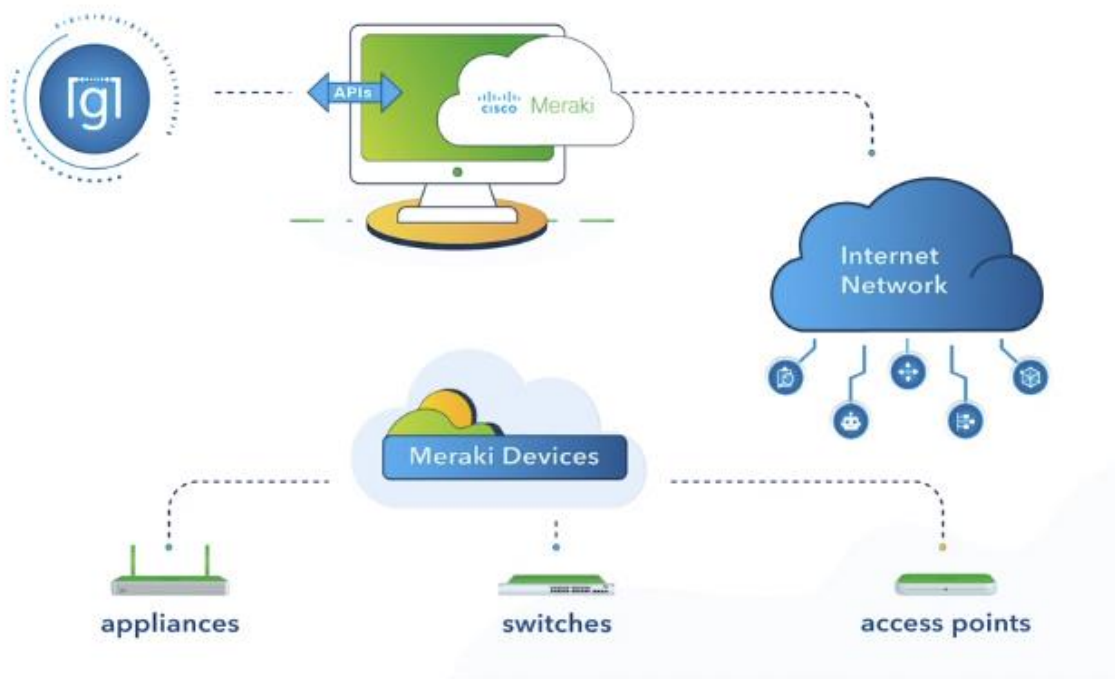


Figure 1 Gluware automating Meraki via API

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.

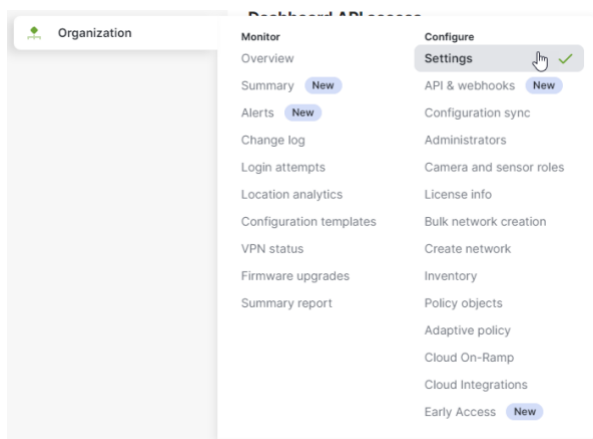
GETTING STARTED

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**.



Dashboard API access

API Access ⓘ

☒ Enable access to the Cisco Meraki Dashboard API

After enabling the API here, go to the [API & webhooks page](#) to generate an API key. The API will return 401 for requests with a missing or invalid API key.

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

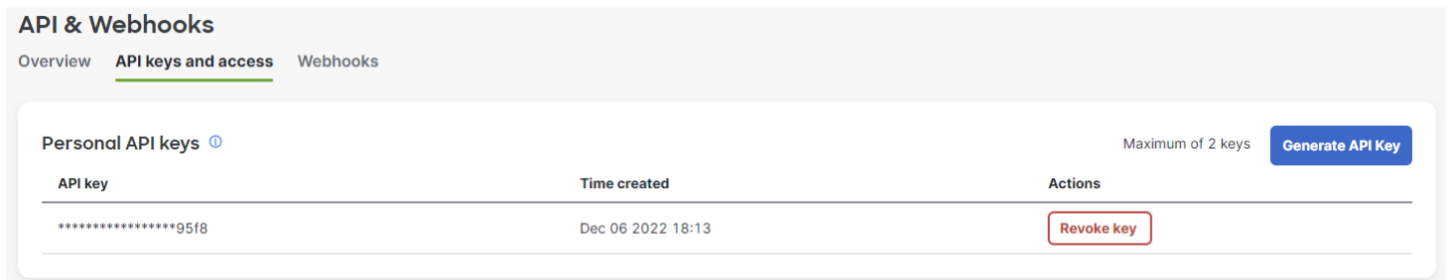
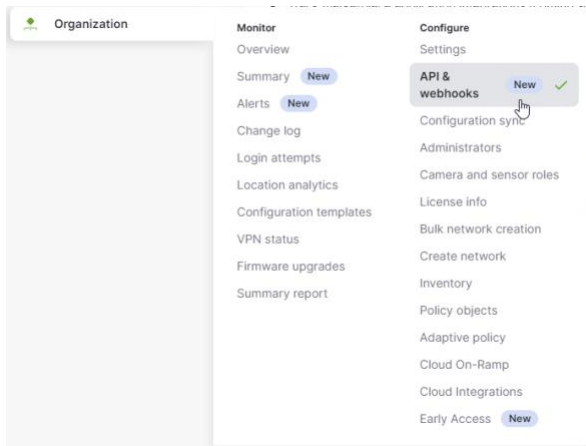


Figure 3 In the Meraki Org -> API & Webhooks generate the API key

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

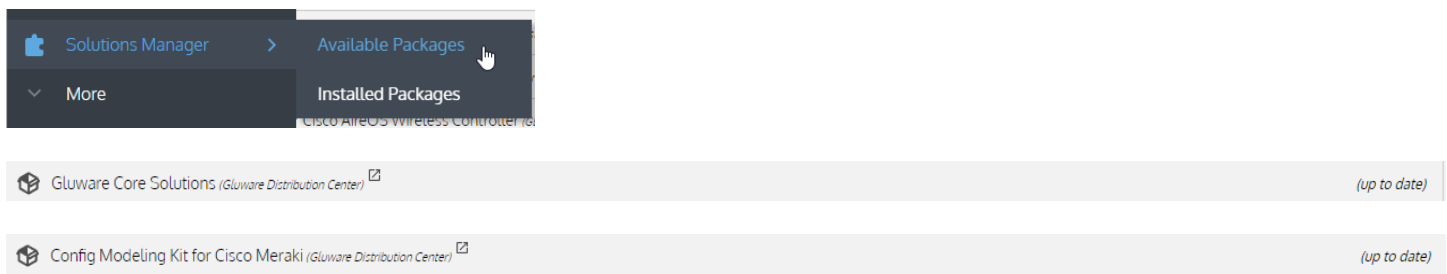


Figure 4 In the Gluware Solutions Manager, install/update the required packages

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

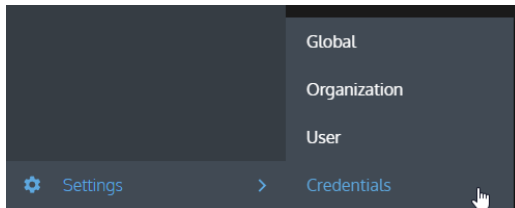
A screenshot of the Gluware Credentials Manager 'Edit Credential' form. The form is titled 'Credentials' and 'Credential Management'. It shows a table with columns 'Name', 'Description', 'Source', and 'Type'. The 'Meraki' credential is selected. The form fields are: Name (Meraki), Description (empty), Source (Gluware), Type (Device API Key), API Key (masked with dots and an eye icon), and Path (/secret/sys/credentials/deviceApiKey/Meraki.json). The 'Validate' button is highlighted.

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:

The screenshot shows the 'Device Details' form in the Gluware Device Manager. The form is titled 'Meraki Cloud Service'. It includes the following fields and options:

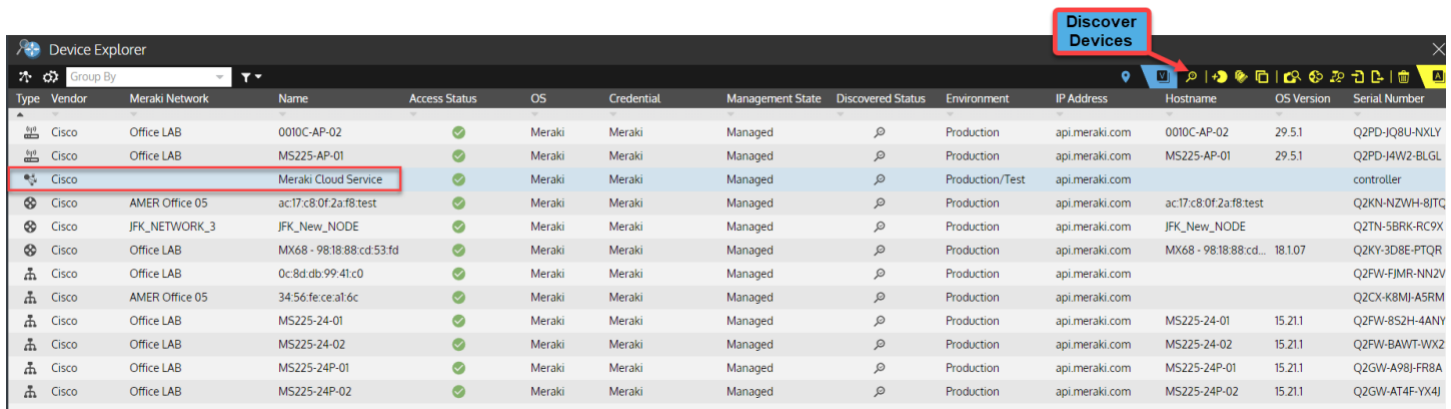
- Name:** Meraki Cloud Service (highlighted with 'Add the name')
- Description:** Description
- Site Path:** /
- Site Code Name:** ROOT
- Connection Method:** Meraki API connection (highlighted with 'Select Meraki API connection')
- End Point:** api.meraki.com (highlighted with 'add the URL')
- API version:** v1
- HTTP Headers:** X-Cisco-Meraki-API-Key Credential: Meraki (highlighted with 'Select the API credential')
- Discovery Level:** 3 - Neighbor
- Management State:** Managed
- Environment:** Production/Test
- HA Group:** Add
- File Server:**
- VRF:** VRF

The bottom right corner of the interface shows the 'Device Explorer' panel with a table of devices. The 'Add device' button is highlighted with 'First, Add Device'.

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



Type	Vendor	Meraki Network	Name	Access Status	OS	Credential	Management State	Discovered Status	Environment	IP Address	Hostname	OS Version	Serial Number
	Cisco	Office LAB	0010C-AP-02	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	0010C-AP-02	29.5.1	Q2PD-JQ8U-NXLY
	Cisco	Office LAB	MS225-AP-01	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	MS225-AP-01	29.5.1	Q2PD-J4W2-BLGL
	Cisco		Meraki Cloud Service	✓	Meraki	Meraki	Managed	⌚	Production/Test	api.meraki.com			controller
	Cisco	AMER Office 05	ac17:c8:0f:2a:f8:test	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	ac17:c8:0f:2a:f8:test		Q2KN-NZWH-8JTQ
	Cisco	JFK_NETWORK_3	JFK_New_NODE	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	JFK_New_NODE		Q2TN-5BRK-RC9X
	Cisco	Office LAB	MX68 - 98:18:88:cd:53:fd	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	MX68 - 98:18:88:cd...	18.1.07	Q2KY-3D8E-PTQR
	Cisco	Office LAB	0c8d:db:99:41:c0	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com			Q2FW-FJMR-NNZV
	Cisco	AMER Office 05	34:56:fe:ce:a1:6c	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com			Q2CX-K8MJ-A5RM
	Cisco	Office LAB	MS225-24-01	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	MS225-24-01	15.21.1	Q2FW-8S2H-4ANY
	Cisco	Office LAB	MS225-24-02	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	MS225-24-02	15.21.1	Q2FW-BAWT-WX2
	Cisco	Office LAB	MS225-24P-01	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	MS225-24P-01	15.21.1	Q2GW-A98J-FR8A
	Cisco	Office LAB	MS225-24P-02	✓	Meraki	Meraki	Managed	⌚	Production	api.meraki.com	MS225-24P-02	15.21.1	Q2GW-AT4F-YX4J

Figure 7 Select the Meraki Controller and execute a discovery

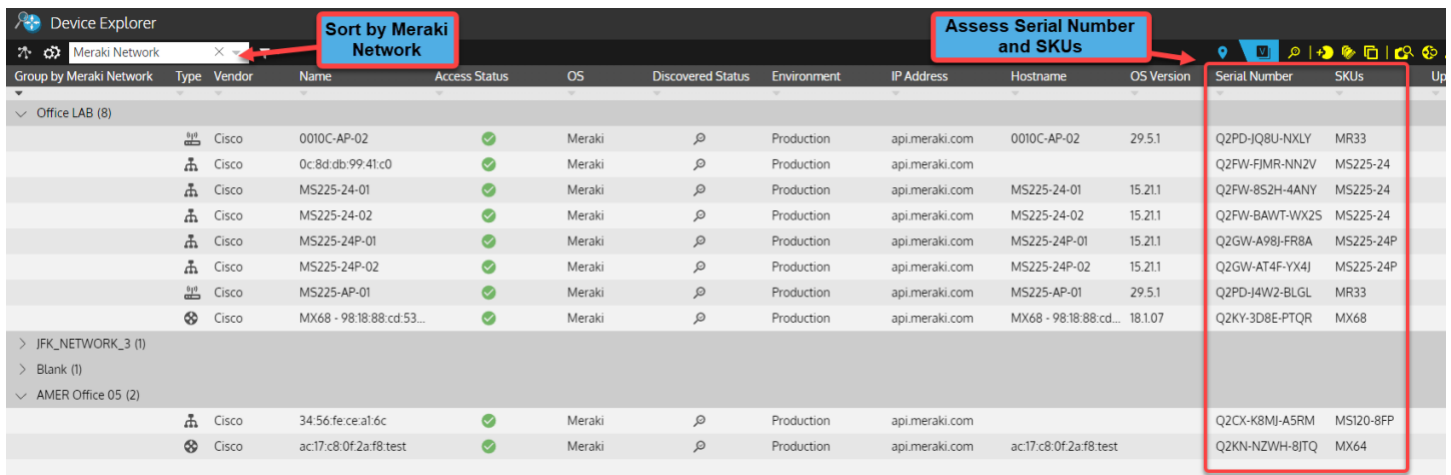
As shown in *Figure 7*, select the Meraki controller by clicking on it, then click the **Discovery devices** icon in the Device Explorer action bar menu. Gluware performs an API-based discovery to import the Meraki orgs, networks and devices, along with the configuration from the controller. The Device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

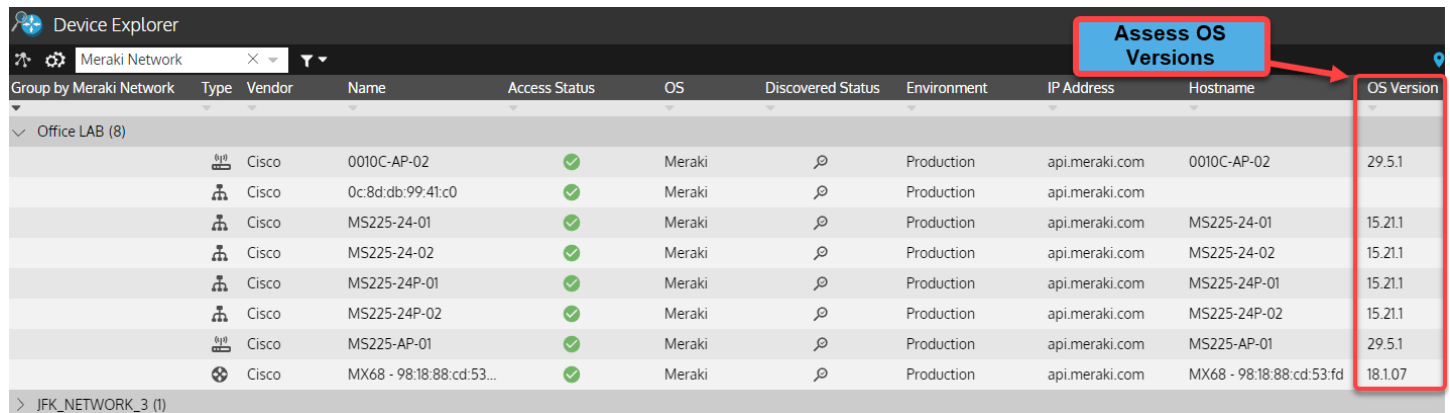


Group by Meraki Network	Type	Vendor	Name	Access Status	OS	Discovered Status	Environment	IP Address	Hostname	OS Version	Serial Number	SKUs
Office LAB (8)		Cisco	0010C-AP-02	✓	Meraki	⌚	Production	api.meraki.com	0010C-AP-02	29.5.1	Q2PD-JQ8U-NXLY	MR33
		Cisco	0c:8d:db:99:41:c0	✓	Meraki	⌚	Production	api.meraki.com			Q2FW-FJMR-NNZV	MS225-24
		Cisco	MS225-24-01	✓	Meraki	⌚	Production	api.meraki.com	MS225-24-01	15.21.1	Q2FW-8S2H-4ANY	MS225-24
		Cisco	MS225-24-02	✓	Meraki	⌚	Production	api.meraki.com	MS225-24-02	15.21.1	Q2FW-BAWT-WX2S	MS225-24
		Cisco	MS225-24P-01	✓	Meraki	⌚	Production	api.meraki.com	MS225-24P-01	15.21.1	Q2GW-A98J-FR8A	MS225-24P
		Cisco	MS225-24P-02	✓	Meraki	⌚	Production	api.meraki.com	MS225-24P-02	15.21.1	Q2GW-AT4F-YX4J	MS225-24P
		Cisco	MS225-AP-01	✓	Meraki	⌚	Production	api.meraki.com	MS225-AP-01	29.5.1	Q2PD-J4W2-BLGL	MR33
		Cisco	MX68 - 98:18:88:cd:53:fd	✓	Meraki	⌚	Production	api.meraki.com	MX68 - 98:18:88:cd...	18.1.07	Q2KY-3D8E-PTQR	MX68
JFK_NETWORK_3 (1)												
Blank (1)												
AMER Office 05 (2)		Cisco	34:56:fe:ce:a1:6c	✓	Meraki	⌚	Production	api.meraki.com			Q2CX-K8MJ-A5RM	MSI20-8FP
		Cisco	ac17:c8:0f:2a:f8:test	✓	Meraki	⌚	Production	api.meraki.com	ac17:c8:0f:2a:f8:test		Q2KN-NZWH-8JTQ	MX64

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.



Assess OS Versions

Group by Meraki Network	Type	Vendor	Name	Access Status	OS	Discovered Status	Environment	IP Address	Hostname	OS Version
Office LAB (8)										
		Cisco	0010C-AP-02	✓	Meraki	⌘	Production	api.meraki.com	0010C-AP-02	29.5.1
		Cisco	0c:8d:db:99:41:c0	✓	Meraki	⌘	Production	api.meraki.com		
		Cisco	MS225-24-01	✓	Meraki	⌘	Production	api.meraki.com	MS225-24-01	15.21.1
		Cisco	MS225-24-02	✓	Meraki	⌘	Production	api.meraki.com	MS225-24-02	15.21.1
		Cisco	MS225-24P-01	✓	Meraki	⌘	Production	api.meraki.com	MS225-24P-01	15.21.1
		Cisco	MS225-24P-02	✓	Meraki	⌘	Production	api.meraki.com	MS225-24P-02	15.21.1
		Cisco	MS225-AP-01	✓	Meraki	⌘	Production	api.meraki.com	MS225-AP-01	29.5.1
		Cisco	MX68 - 98:18:88:cd:53...	✓	Meraki	⌘	Production	api.meraki.com	MX68 - 98:18:88:cd:53:fd	18.1.07
> JFK_NETWORK_3 (1)										

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.

Type	Access Status	Vendor	Name	Environment	IP Address	Hostname	Captured Status	OS	OS Version	Serial Number	SKUs
Router	✓	Cisco	0010C-AP-02	Production	api.meraki.com	0010C-AP-02	⓪	Meraki	29.5.1	Q2PD-JQ8U-NXLY	MR33
Switch	✓	Cisco	0c:8d:db:99:41:c0	Production	api.meraki.com		⓪	Meraki		Q2FW-FJMR-NN2V	MS225-24
Switch	✓	Cisco	34:56:fe:ce:a1:6c	Production	api.meraki.com		⓪	Meraki		Q2CX-K8MJ-A5RM	MS120-8FP
Switch	✓	Cisco	ac:17:c8:0f:2a:f8:test	Production	api.meraki.com	ac:17:c8:0f:2a:f8:test	⓪	Meraki		Q2KN-NZWH-8JTQ	MX64
Switch	✓	Cisco	JFK_New_NODE	Production	api.meraki.com	JFK_New_NODE	⓪	Meraki		Q2TN-5BRK-RC9X	Z3
Switch	✓	Cisco	Meraki Cloud Service	Production/Test	api.meraki.com		?	Meraki		controller	
Switch	✓	Cisco	MS225-24-01	Production	api.meraki.com	MS225-24-01	⓪	Meraki	15.21.1	Q2FW-8S2H-4ANY	MS225-24
Switch	✓	Cisco	MS225-24-02	Production	api.meraki.com	MS225-24-02	⓪	Meraki	15.21.1	Q2FW-BAWT-WX2S	MS225-24
Switch	✓	Cisco	MS225-24P-01	Production	api.meraki.com	MS225-24P-01	⓪	Meraki	15.21.1	Q2GW-A98J-FR8A	MS225-24P
Switch	✓	Cisco	MS225-24P-02	Production	api.meraki.com	MS225-24P-02	⓪	Meraki	15.21.1	Q2GW-AT4F-YX4J	MS225-24P
Switch	✓	Cisco	MS225-AP-01	Production	api.meraki.com	MS225-AP-01	⓪	Meraki	29.5.1	Q2PD-J4W2-BLGL	MR33
Switch	✓	Cisco	MX68 - 98:18:88:cd:53:fd	Production	api.meraki.com	MX68 - 98:18:88:cd:53:fd	⓪	Meraki	18.1.07	Q2KY-3D8E-PTQR	MX68

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

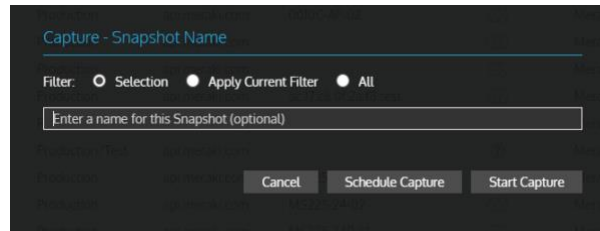


Figure 11 Schedule a periodic capture, or start the capture

Step through the detected changes

Select the config comparison view

Click on a device where drift has been detected

Type	Access Status	Vendor	Name	Environment	IP Address	Hostname	Captured Status	OS	OS Version	Serial Number	SKUs
AP	✓	Cisco	0010C-AP-02	Production	api.meraki.com	0010C-AP-02	📶	Meraki	29.5.1	Q2PD-JQ8U-NXLY	MR33
SW	✓	Cisco	0c8ddb9941c0	Production	api.meraki.com	0c8ddb9941c0	📶	Meraki		Q2FW-FJMR-NNZV	MS225-24
SW	✓	Cisco	3456feceal6c	Production	api.meraki.com	3456feceal6c	📶	Meraki		Q2CX-K8MJ-A5RM	MS120-8FP
SW	✓	Cisco	ac17c80f2af8test	Production	api.meraki.com	ac17c80f2af8test	📶	Meraki		Q2KN-NZWH-8JTO	MX64
SW	✓	Cisco	1F7 New N100E	Production	api.meraki.com	1F7 New N100E	📶	Meraki		Q2TN-5BRK-R00Y	73

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

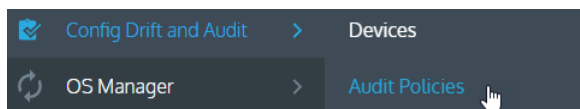
The Gluware Config Drift and Audit app enables users to execute multi-vendor, multi-platform audits without any coding required. Users easily define audits for company policy, ad-hoc policy and standards-based policies. Audit policies are comprised of multiple rules defining required or forbidden configuration 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.



Name	Description	Permission Level	Audit On	Audit By	Audit Status	Total Devices	Audited Devices	Passed Devices	Failed Devices	Skipped Devices	Device E
Meraki_SNMP_Audit		1	12/7/2022 1:10:06 PM	admin		7	7	7	0	0	0
Meraki_SNMP_v2_Audit	Checks to ensure SNMP v2 L...	1	12/7/2022 1:13:12 PM	admin		7	7	0	7	0	0

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

Policy Details										
Enabled	Severity	Name	Description	Source	OS	Command Set	Command Result	Query	Indy	Actions
<input checked="" type="checkbox"/>	Major	IsSNMPv3Enabled	Audit to Ensure SNMP v3 is en	Latest	All	All	Standard			

Figure 14 Use the details view to edit the audit policy

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

Device Explorer

Meraki Network

Group by Meraki Network

Type

Access Status

Vendor

Name

Environment

IP Address

Hostname

Captured Status

OS

OS V

> AMER Office 05 (2)

> Blank (1)

> JFK_NETWORK_3 (1)

> Office LAB (8)

		Cisco	0010C-AP-02	Production	api.meraki.com	0010C-AP-02		Meraki	29.5.1
		Cisco	0c:8d:db:99:41:c0	Production	api.meraki.com			Meraki	
		Cisco	MS225-24-01	Production	api.meraki.com	MS225-24-01		Meraki	15.21.7
		Cisco	MS225-24-02	Production	api.meraki.com	MS225-24-02		Meraki	15.21.7
		Cisco	MS225-24P-01	Production	api.meraki.com	MS225-24P-01		Meraki	15.21.7
		Cisco	MS225-24P-02	Production	api.meraki.com	MS225-24P-02		Meraki	15.21.7
		Cisco	MS225-AP-01	Production	api.meraki.com	MS225-AP-01		Meraki	29.5.1
		Cisco	MX68 - 98:18:88:cd:53:fd	Production	api.meraki.com	MX68 - 98:18:88:cd:53:fd		Meraki	18.1.0

Audit the configuration

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

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.

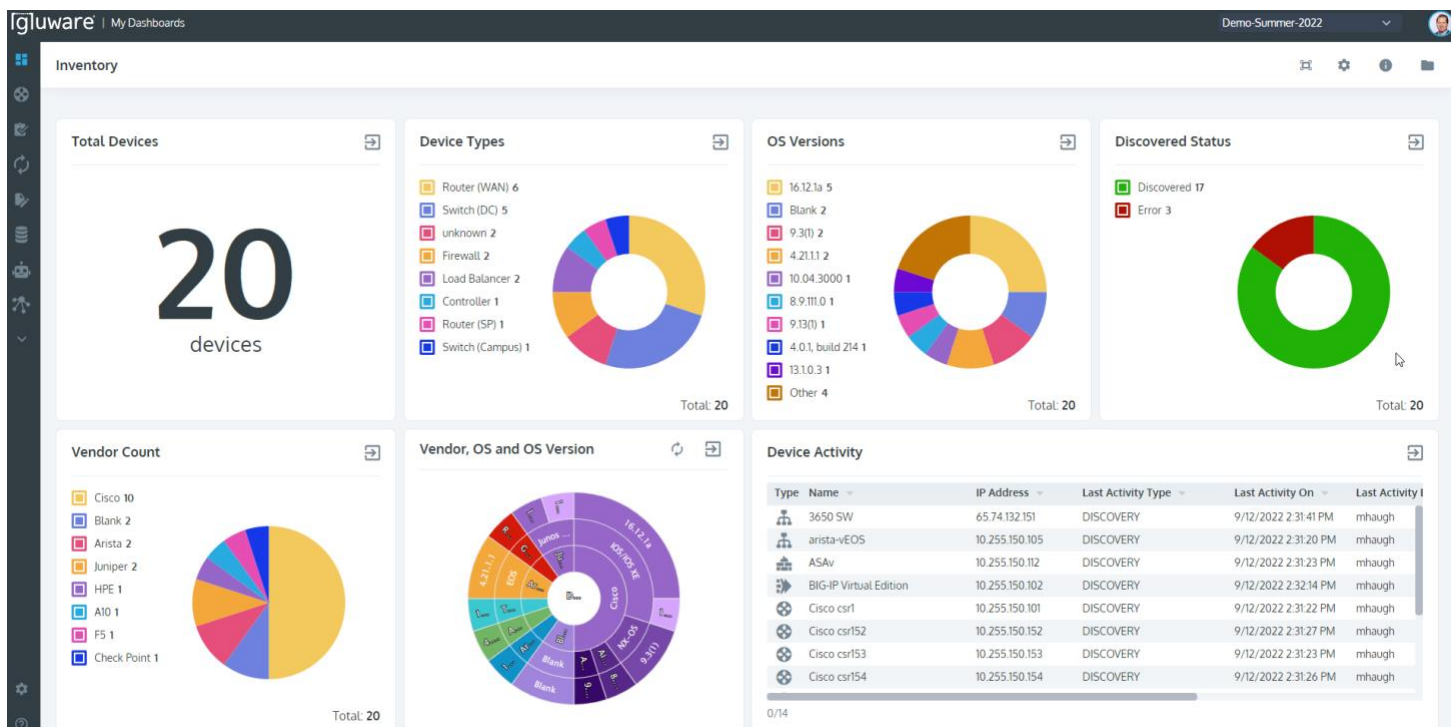


Figure 19 Use Gluware Dashboard to visualize the data from the network infrastructure

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

Name	Description	Immutable	Private	Created By	Created In	Created On	Modified By	Modified On
Shared Templates (12)								
Cisco Extended Inventory Device List	Contains a list of all Cisco devices for the cur...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:0...	mhaugh	9/7/2021 2:30:2...
Cisco Inventory License List	Contains a list of all Cisco devices for the cur...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:0...	mhaugh	9/7/2021 2:30:3...
Cisco PSIRT Summary	Contains a count device PSIRT advisories			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:15...	mhaugh	9/7/2021 2:30:3...
Cisco Support Data	Contains device EOX and SmartNet details			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:2...	mhaugh	9/7/2021 2:30:4...
Config Drift and Audit Device List	List of devices and details about its drift stat...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:3...	mhaugh	9/7/2021 2:30:4...
Device Inventory List	List of devices and their discovered details			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:5...	mhaugh	9/7/2021 2:30:5...
Device Inventory List with Components	List of devices and their discovered details i...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:3...	mhaugh	9/7/2021 2:31:02...
Device OSM Summary	List of devices and a summary of their last O...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:5...	mhaugh	9/7/2021 2:31:08...
L2 Port State	Contains Layer 2 configuration and operatio...			mhaugh	Test-Drive-4-POD-4	9/8/2021 4:08:0...	mhaugh	9/8/2021 4:08:16...
Network Discovery Result	Contains a list of all the network-discovered ...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:30:01...	mhaugh	9/7/2021 2:31:17...
Node List	Contains a list of all configured nodes in the ...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:30:0...	mhaugh	9/7/2021 2:31:23...
Node Provisioning Summary	A summary of node provisioning informatio...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:30:13...	mhaugh	9/7/2021 2:31:30...

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

Cisco PSIRT Summary

Example PSIRT Summary Report



















Data Explorer Results

Results: 9

Group by: None

Description: Contains a count device PSIRT advisories

Last Run: 9/13/2022, 12:51:07 PM

Name	Description	IP Address	SKU	OS	OS Version	Critical Advisories	High Advisories	Medium Advisories	Actions
POD-4-SPOKE-4		172.31.255.4	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	 
POD-4-SPOKE-3		172.31.255.3	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	 
POD-4-SPOKE-2		172.31.255.2	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	 
POD-4-SPOKE-1		172.31.255.1	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	 
POD-4-N9K1-1		172.31.255.14	N9K-9000v	NX-OS	9.3(1)	0	15	7	 
POD-4-HUB-2		172.31.255.12	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	 
POD-4-HUB-1		172.31.255.11	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	 
POD-4-ASAv-1		172.31.255.13	ASAv	ASA	9.8(4)10				 
POD-3-PHY-SWT-STACK		172.31.255.15	WS-C3650-24TS-L	IOS/IOS XE	16.6.7	1	32	19	 
Sum 19						Sum 335	Sum 254		

Assess Current State of PSIRT Exposure

Edit Data SelectionRun AgainEmailDownload

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](#)

