infoblox.

DEPLOYMENT GUIDE

INFOBLOX UNIVERSAL ASSET INSIGHTS™ CISCO MERAKI INTEGRATION

DISCOVERY JOB CONFIGURATION

TABLE OF CONTENTS

INTRODUCTION

Infoblox Universal Asset Insights™, a powerful product within the **Infoblox Universal DDI™ Product Suite**, automates the discovery and analysis of assets across major public clouds, on-premises networks, and third-party solutions, such as Cisco Meraki, providing detailed and continuous visibility into network assets, giving organizations a unified, accurate view of all their IT assets.

Cisco Meraki is a cloud-managed IT solution that simplifies the management of wired, wireless, and security devices across distributed networks. Organizations can remotely configure, monitor, and troubleshoot infrastructure without the need for complicated on-premises controllers thanks to its centralized dashboard. Meraki has features like network security, real-time device visibility, analytics, and automatic updates that make operations run smoothly.

As enterprises increasingly adopt cloud-managed infrastructures, including distributed branch offices, wireless networks, on-premises data centers and edge environments, it becomes essential to keep accurate and continuous visibility of these assets not only to keep IT operations running smoothly, but also to meet governance, audit, and compliance requirements.

CISCO MERAKI INTEGRATION

Universal Asset Insights addresses the above challenge by integrating with Cisco Meraki through a secure REST API-based connection configured within the Infoblox Portal. It retrieves comprehensive asset information such as organizations, networks, VLANs, subnets, and device metadata, by using Meraki's cloud APIs. And it organizes this data into a centralized asset inventory. This eliminates data silos, ensures consistency across environments, and provides NetOps, CloudOps, and IT service management (ITSM) teams with a unified view of all Meraki-managed network assets in a single pane of glass.

Universal Asset Insights retrieves data from Cisco Meraki, including network details, device types, hostnames, IP and MAC addresses, and first- and last-seen discovery information. Further, this data goes through a process of normalization and consolidation where it is correlated with asset information gathered from cloud platforms, on-premises environments, and other third-party integrations such as ServiceNow and CrowdStrike. This ensures data consistency, eliminates duplicates, and provides a unified view of assets across hybrid environments.

The unified Meraki asset data is then presented within the Asset Inventory, accessible under the *Network > Assets Workspace* in the Monitor section of the Infoblox Portal, giving NetOps and CloudOps teams complete visibility into their cloud-managed infrastructure.

Type of Assets Discovered

The Cisco Meraki integration with Infoblox Universal Asset Insights discovers a wide range of asset types across different categories:

- **Organization Assets:** Devices, device availability, and networks within the Meraki-managed environment.
- **Network Assets:** Appliance VLANs, connected clients, VLAN profiles, cellular gateway subnet pools, subnets, and site-to-site VPN configurations.
- **Device Assets:** Associated clients providing details on connectivity and addressing.

KEY CAPABILITIES

Comprehensive Asset Visibility

By combining Cisco Meraki data with Infoblox Universal Asset Insights, organizations gain full visibility into every device across cloud-managed, on-premises, and third-party environments. This unified inventory consolidates information from multiple sources such as public clouds, on-premises environments, and third-party vendors like CrowdStrike and ServiceNow, getting rid of silos and making operations more transparent. NetOps and SecOps teams benefit from a single source of truth for network assets, enabling better tracking, improved operational efficiency, and stronger security governance.

IPAM Synchronization for Accuracy and Compliance

IP address records stay accurate as devices are added, moved, or removed because Meraki-managed networks and Infoblox IP Address Management™ are always in sync. The integration eliminates manual updates, lowers the chances of configuration errors, and makes sure that IP address management (IPAM) is complete across hybrid infrastructures. As a result, organizations have more reliable networks, consistent IP address allocation, and enhanced compliance readiness.

DISCOVERY JOB: PERMISSIONS REQUIRED AND CONFIGURATION ANALYSIS

PERMISSIONS REQUIRED FOR CISCO MERAKI

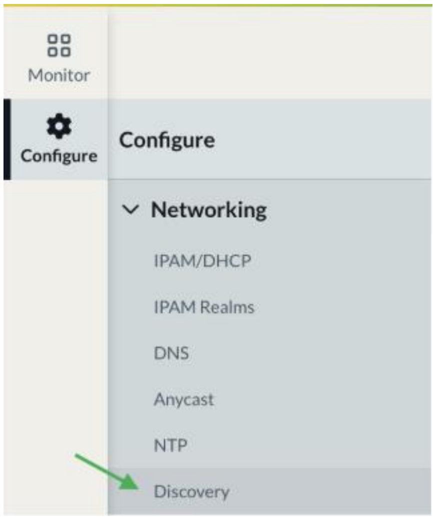
The integration uses API key authentication, which you can generate in your Meraki Dashboard under your account profile, to securely provide Universal Asset Insights with read-only access to the necessary data. It should be linked to organizations that let you see the networks and devices you want to find. To get configuration and asset data, the integration will need all “**config:read**” scopes. If you don’t have the right API key or scopes, the discovery job might not be able to connect or get all the asset information, which would leave gaps in visibility. Contact your IT or Meraki admin to ensure the API key you get for configuring the discovery job has been set up correctly.

CONFIGURE CISCO MERAKI DISCOVERY JOB IN INFOBLOX PORTAL

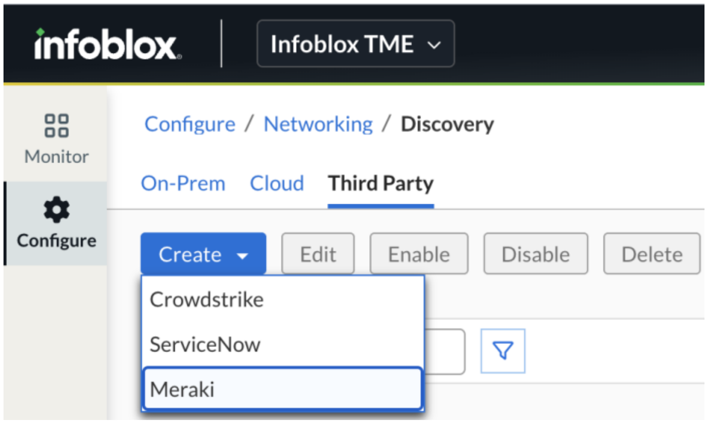
Configuring a discovery job to integrate Universal Asset Insights with Cisco Meraki involves setting up a secure connection using the Meraki API key. This configuration is done through the Infoblox Portal on the **Configure -> Networking -> Discovery -> Third Party** page.

General

1. Log in to Infoblox Portal with an administrator account.
2. Navigate to **Configure -> Networking -> Discovery.**



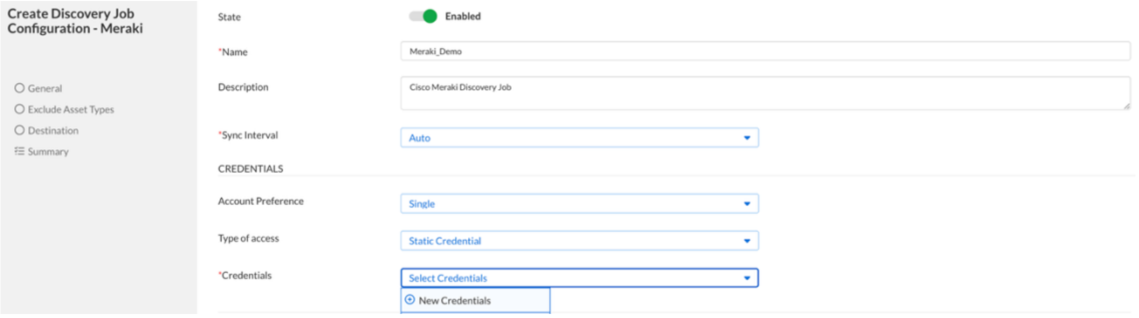
3. Click on **Third Party -> Create -> Meraki**.



4. **Name:** Assign a name to the discovery job.
5. **Description**: This is optional. Write an appropriate description for this job.
6. **Sync Interval:** Select the time interval that you'd like to set for your discovery job or leave it to default.
7. **Account Preference:** Select between **Single** or **Auto-Discover Multiple**.

*Note: If you need to discover assets across multiple organizations, select **Auto-Discover Multiple**.*

8. **Type of Access**: Leave this to default, **Static Credentials**.
9. **Credentials:** Click on **Select Credentials** and from the dropdown, click on **New Credentials**.



State: Enabled

*Name: Meraki_Demo

Description: Cisco Meraki Discovery Job

*Sync Interval: Auto

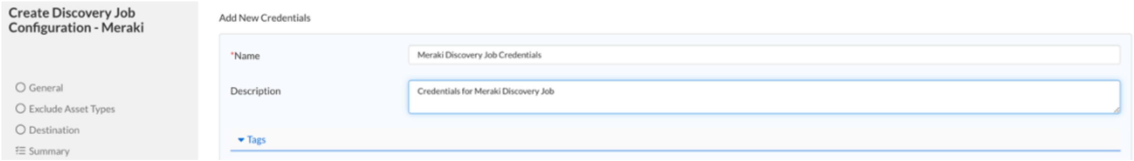
CREDENTIALS

Account Preference: Single

Type of access: Static Credential

*Credentials: Select Credentials

9.1. Provide the credential **Name** and **Description.**



Add New Credentials

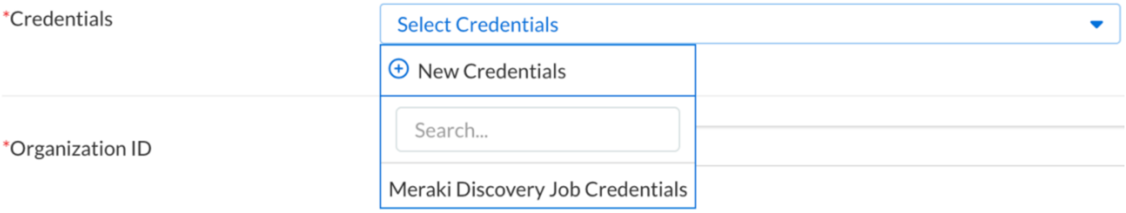
*Name: Meraki Discovery Job Credentials

Description: Credentials for Meraki Discovery Job

9.2. Tags are optional. Click **Next**.

9.3. Under the **MERAKI CREDENTIALS** section, provide the **API key**, click **Next** and click **Save**.

*Note: This will return you to the General section, where you can select the credentials you just created. Select the credentials and click **Next**.*



*Credentials: Select Credentials

*Organization ID

10. **Organization ID:** Enter the organization ID.

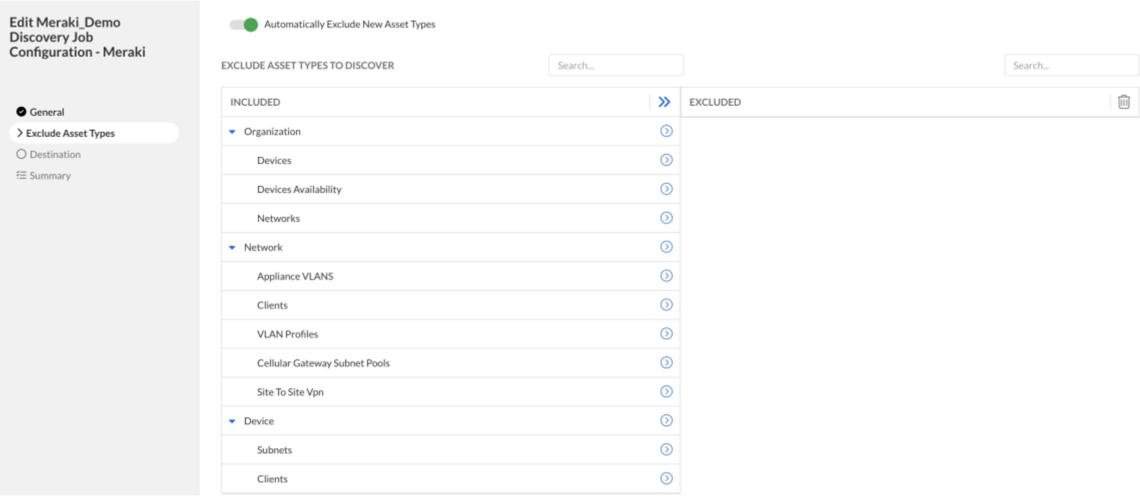
*Note: The **Organization ID** is required only when configuring the discovery job for a **single account**.*

11. Tags are optional. Click **Next**.

Exclude Asset Types

- **Automatically Exclude New Asset Types:** This is on by default. You can turn off the toggle feature if you'd like to discover newly added asset types.

1. **Exclude Asset Types to Discover:** This shows all the asset types that will be discovered. You can exclude asset types that you do not want to discover.



Edit Meraki_Demo Discovery Job Configuration - Meraki

Automatically Exclude New Asset Types

EXCLUDE ASSET TYPES TO DISCOVER

INCLUDED	EXCLUDED
Organization	
Devices	
Devices Availability	
Networks	
Network	
Appliance VLANS	
Clients	
VLAN Profiles	
Cellular Gateway Subnet Pools	
Site To Site Vpn	
Device	
Subnets	
Clients	

2. Click **Next.**

Destination

- **IPAM Discovery:** This is off by default. You can turn on the toggle feature if you'd like to discover IPAM data.

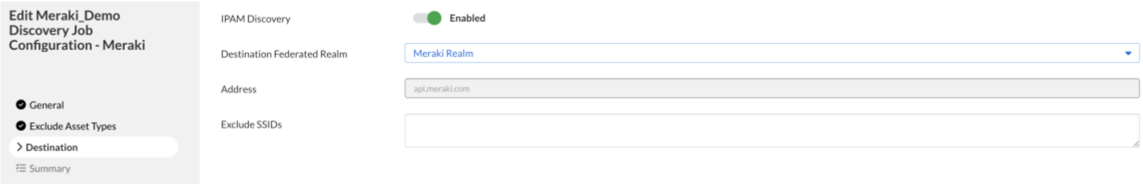
  *Note: If the **IPAM Discovery** toggle is turned off, the job will not sync any IPAM data. It will only discover the assets listed above and display them under Asset Inventory.*

- **Destination Federated Realm:** This option becomes available once the **IPAM Discovery** toggle is enabled. Select the **Realm** where you want to manage address spaces from Meraki-managed networks.

  Note: Federated Realm is a unified framework within Infoblox Universal DDI designed to streamline the planning and enforcement of IP address usage across multiple IPAM platforms, including on-premises and cloud environments like AWS, Azure, and Google. It provides a single hierarchical view of an enterprise's network, enabling administrators to manage IP address blocks, apply policies, and maintain consistency across diverse infrastructure sources. This model simplifies operations by abstracting backend complexities and offering a user-centric interface for managing IPAM. For additional details on IPAM Federation, refer to https://docs.infoblox.com/space/BloxOneDDI/684884521/Configuring+IPAM+Federation

1. **Exclude SSIDs:** The **Exclude SSIDs** option allows you to filter out specific wireless SSIDs from the discovery process. Click **Next**.

   Note: *You can enter multiple SSIDs using a comma-separated format to exclude several at once.*



IPAM Discovery: Enabled

Destination Federated Realm: Meraki Realm

Address: api.meraki.com

Exclude SSIDs:

Summary

1. Review the summary for complete configuration and click **Save & Close**.

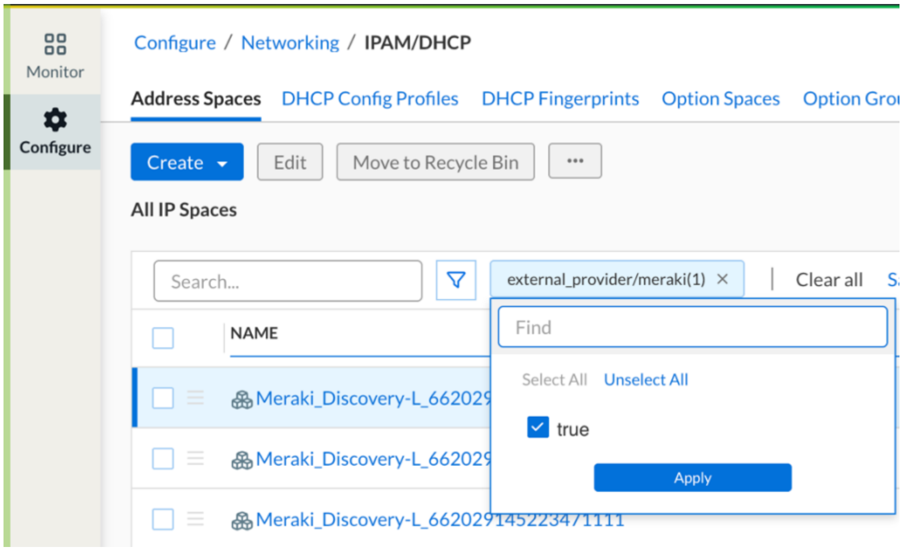
VIEW THE DISCOVERED DATA IN INFOBLOX PORTAL

Once the discovery job is created and sync is successful, follow these steps to view the discovered data under Infoblox Portal.

IPAM Data

1. Click on **Configure -> Networking -> IPAM/DHCP**.

- From the search bar, search for “Meraki” (case insensitive), or click the filter icon. Scroll down to the **External Provider** section and select “external_provider/meraki”. Then select the **true** checkbox and click **Apply**.

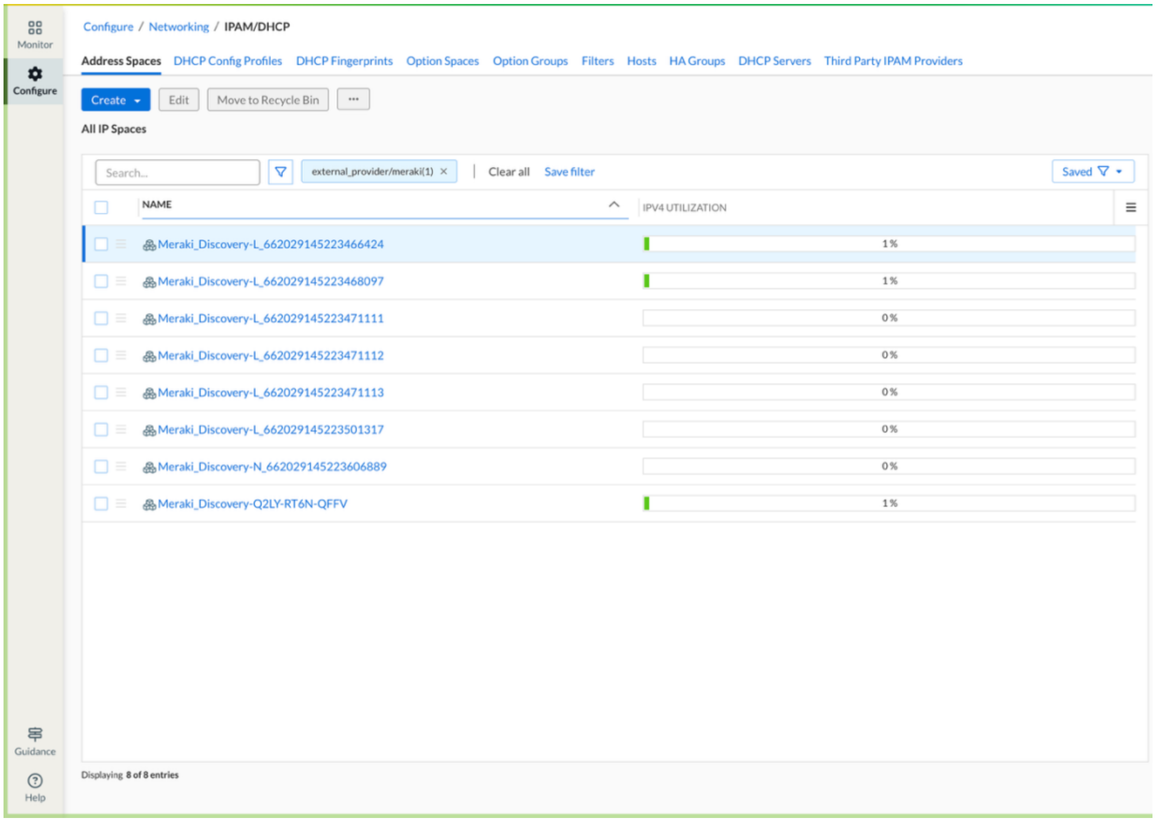


external_provider/meraki(1) ×

☑ true

□	NAME
□	Meraki_Discovery-L_662029
□	Meraki_Discovery-L_662029
□	Meraki_Discovery-L_66202914522347111

- This will display all the Meraki networks.



All IP Spaces

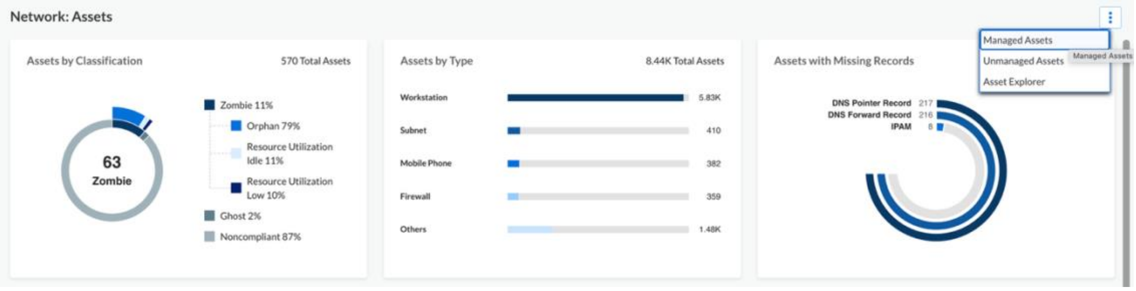
external_provider/meraki(1)

NAME	IPV4 UTILIZATION
Meraki_Discovery-L_662029145223466424	1%
Meraki_Discovery-L_662029145223468097	1%
Meraki_Discovery-L_662029145223471111	0%
Meraki_Discovery-L_662029145223471112	0%
Meraki_Discovery-L_662029145223471113	0%
Meraki_Discovery-L_662029145223501317	0%
Meraki_Discovery-N_662029145223606889	0%
Meraki_Discovery-Q2LY-RT6N-QFFV	1%

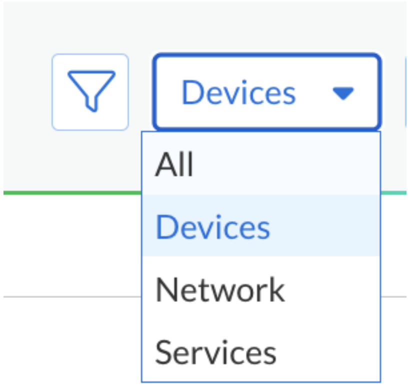
Displaying 8 of 8 entries

Asset Inventory Data

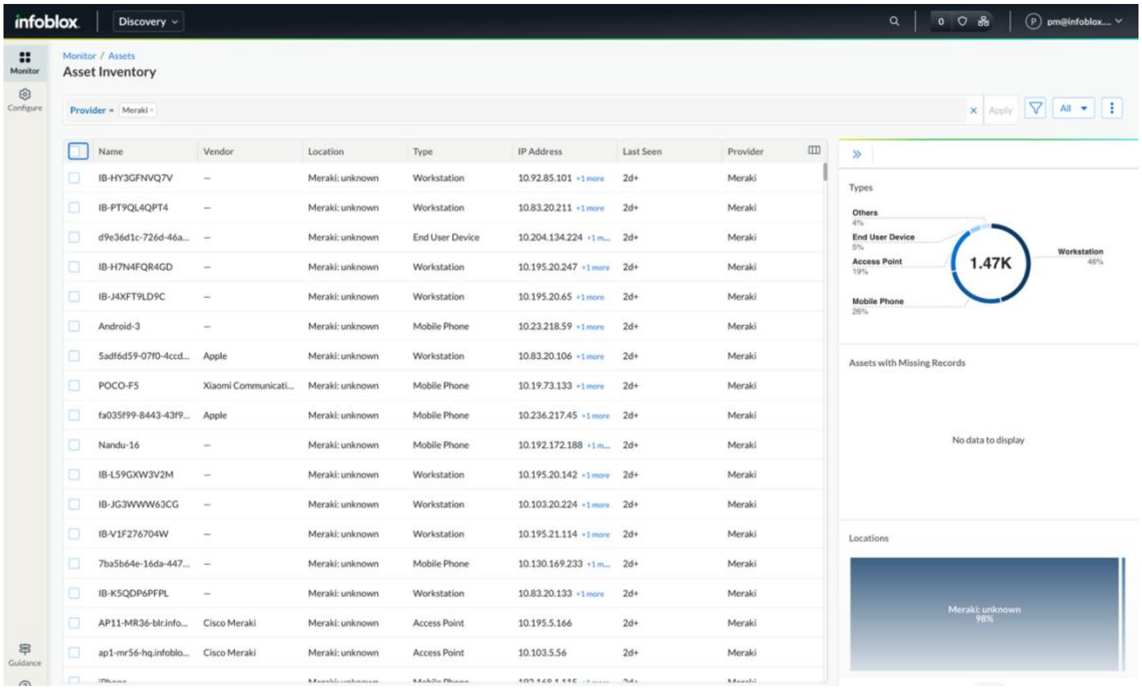
- Click on **Monitor**, which takes you to the **Network -> DDI** workspace by default. Click **Assets** to switch to **Network -> Assets** workspace.
- From the ellipses, click **Managed Assets**.



It opens **Devices** by default. Select **All**.



- Click on the filter button and select the provider as **Meraki**. Click **Apply**. This will present the Asset Inventory for Meraki assets.



Asset Inventory

Provider = Meraki

Name	Vendor	Location	Type	IP Address	Last Seen	Provider
IB-HY3GFNVQ7V	–	Meraki: unknown	Workstation	10.92.85.101 +1 more	2d+	Meraki
IB-PT9QL4QPT4	–	Meraki: unknown	Workstation	10.83.20.211 +1 more	2d+	Meraki
d9e36d1c-726d-46a...	–	Meraki: unknown	End User Device	10.204.134.224 +1 m...	2d+	Meraki
IB-H7N4FQR4GD	–	Meraki: unknown	Workstation	10.195.20.247 +1 more	2d+	Meraki
IB-J4XFT9LD9C	–	Meraki: unknown	Workstation	10.195.20.65 +1 more	2d+	Meraki
Android-3	–	Meraki: unknown	Mobile Phone	10.23.218.59 +1 more	2d+	Meraki
5adf6d59-07f0-4ccd...	Apple	Meraki: unknown	Workstation	10.83.20.106 +1 more	2d+	Meraki
POCO-F5	Xiaomi Communicati...	Meraki: unknown	Mobile Phone	10.19.73.133 +1 more	2d+	Meraki
fa035f99-8443-43f9...	Apple	Meraki: unknown	Mobile Phone	10.236.217.45 +1 more	2d+	Meraki
Nandu-16	–	Meraki: unknown	Mobile Phone	10.192.172.188 +1 m...	2d+	Meraki
IB-L59GXW3V2M	–	Meraki: unknown	Workstation	10.195.20.142 +1 more	2d+	Meraki
IB-JG3WWW63CG	–	Meraki: unknown	Workstation	10.103.20.224 +1 more	2d+	Meraki
IB-V1F276704W	–	Meraki: unknown	Workstation	10.195.21.114 +1 more	2d+	Meraki
7ba5b64e-16da-447...	–	Meraki: unknown	Mobile Phone	10.130.169.233 +1 m...	2d+	Meraki
IB-K5QDP6PFPL	–	Meraki: unknown	Workstation	10.83.20.133 +1 more	2d+	Meraki
AP11-MR36-blr.info...	Cisco Meraki	Meraki: unknown	Access Point	10.195.5.166	2d+	Meraki
ap1-mr56-hq.infoblo...	Cisco Meraki	Meraki: unknown	Access Point	10.103.5.56	2d+	Meraki

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste.
501 Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com

Version: YYYYMMDDvX