IP Maestro®

Version 2.0

User Manual

May 2024

Contents

Preface

This guide describes the steps for logging in to Network Service Mediation (IP Maestro) and describes the multiple dashboards of IP Maestro. This preface includes the following sections:

- Supported OcNOS Version

- Intended audience

- Product version

- Document history

Supported OcNOS Version

IP Maestro Release 2.0 software is designed to monitor devices running OcNOS-6.3.4-70 and above.

Intended audience

The intended audience for this guide is the end-user with access/role/permission to IP Maestro with valid roles that include Network Administrators, Engineers, Operators, and Users.

Product version

This document applies to the IP Maestro 2.0 release.

Document history

Date	Version	Description
April 2024	0.1	First draft
May 2024	0.2	Final draft

Introduction

IP Maestro is a Graphical User Interface (GUI)-based Element Management System (EMS) framework that allows operators to simplify device configuration, management, and automation operations.It is meticulously designed to streamline device management, enhance visibility, fortify security. The system offers an intuitive view of the network topology, performance metrics, faults, and inventory.

IP Maestro supports the following features:

- **Topology**: Discover the network topology effortlessly with a visual map, enabling an intuitive understanding of network elements' physical connectivity. The Topology Toolbar ensures easy manipulation, providing a graphical overview of device and connected link.

- **Inventory:** Gain a holistic view of physical and logical network resources, services, and topologies. The real-time network inventory, coupled with the filter functionality, allows users to navigate and select specific inventory types with ease.

- **Fault Management:** Capture and display alarms from network devices, links, and services. IP Maestro's Fault Management module efficiently processes NETCONF alarms and integrates with syslog for centralized management and alerts. IP Maestro also has the ability to send out email notification to users on occurrences of critical alarms.

- **Performance Monitoring:** Monitor network performance effortlessly with metrics (KPI) and calculated/complex metrics (KQI). Define measurement points, groups, collection intervals, and aggregations intervals for precise and periodic data analysis.

- **Configuration Management:** Manage device configurations with IP Maestro seamlessly. Perform tasks such as downloading software images, creating and deleting configuration files, syncing configurations with the database, and executing configurations on specific devices. Ability to take device configuration backups and then do a *config diff* to see the difference between two configurations

- **Audit and Logs:** Ensure transparency and accountability through historical logs, including syslog records and command history logs. IP Maestro maintains a detailed account of device activities for comprehensive auditing and implements a role-based user management system with comprehensive auditing logs for accountability.

Log in to IP Maestro

Logging in to IP Maestro involves accessing the system to perform network management, configuration, and monitoring tasks.

Prerequisites

- A valid SSO account.
- Ensure to install any of the following browser versions on your compute:

Browser	Version
Google Chrome	102.0.5005.63 (64-bit) (or latest)
Mozilla Firefox	100.0.1 (64-bit) (or latest)
Microsoft Edge	13+ (64-bit) (or latest)
Safari	15.5 (or latest)
Opera	89.0.4447.51

Procedure

To log in to the IP Maestro:

1. On any web browser, type the IP Maestro portal URL. For Example: https://[HOST_IP].

2. On the login page, enter user credentials, including a username and password.
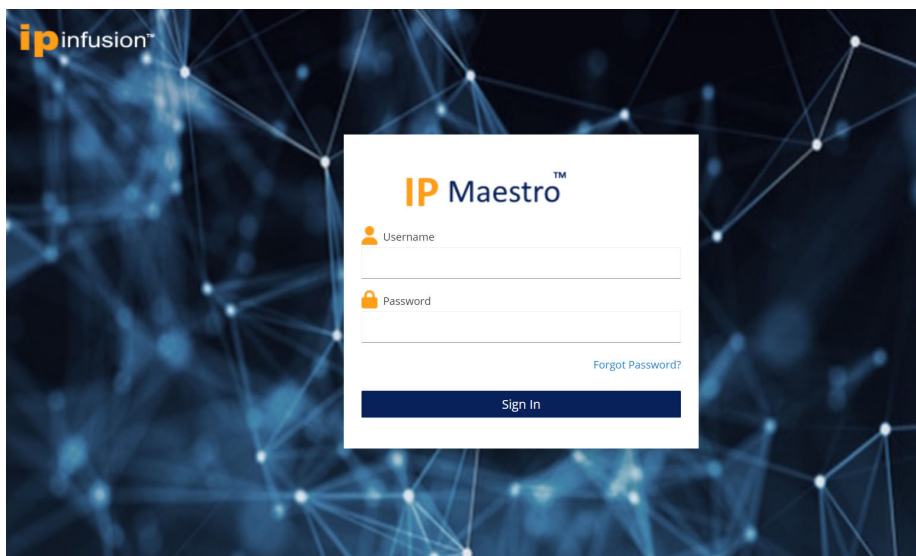
3. Click **Sign In**.

Note: For security reasons, it is advisable to log out of IP Maestro when the session is no longer needed.

Home Page

Upon successful login to IP Maestro, users are displayed with the IP Maestro home page, which serves as the central hub for accessing key information related to network management. The home page offers a high-level overview of the network status, presenting details about configured devices, network topologies, and device-specific information.

Key components:

- [Navigation Pane](#)
- [System Dashboards](#)

The IP Maestro Dashboard is the default home page displayed as below.
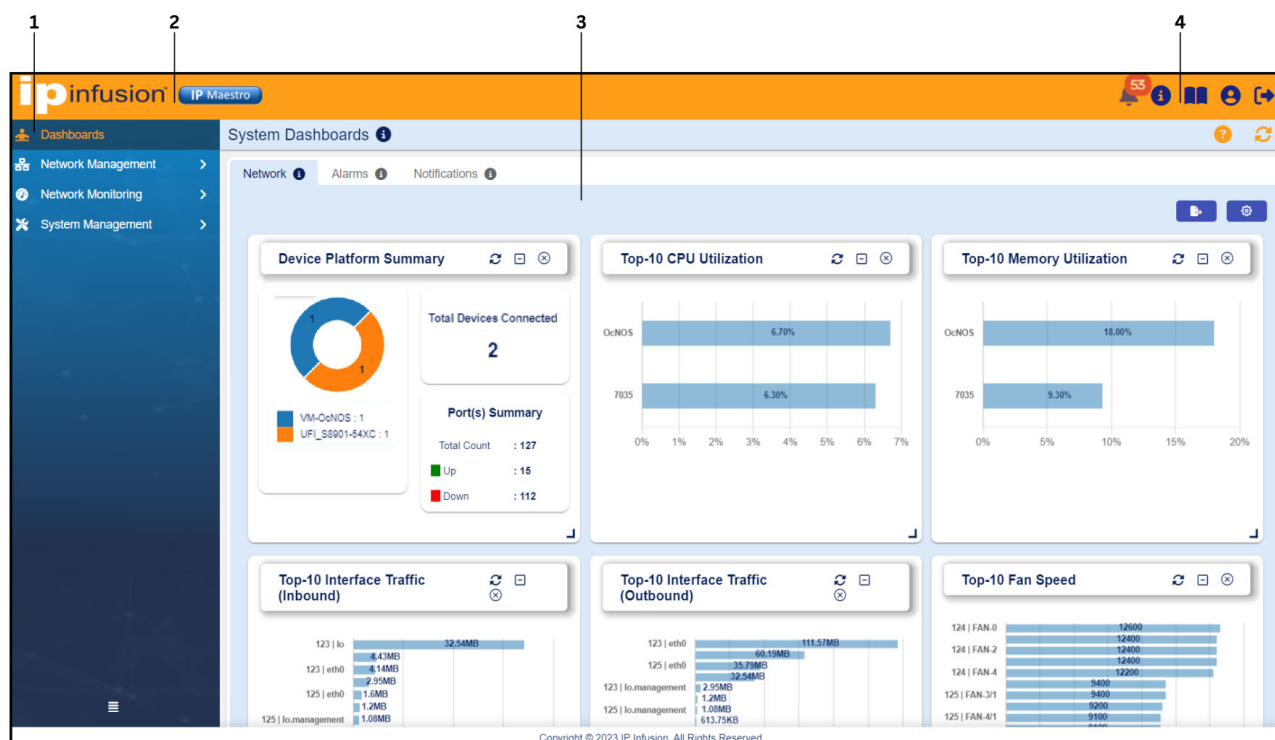
Figure 1: Home Page

Callouts	Description
1. Menu Bar	Facilitates navigation in the IP Maestro UI.This provides various informational panes to help users effectively monitor and manage network-related tasks.
2. Banner	Displays the global actions icon and redirects to IP Infusion web page for detailed information.
3. Home Page	Displays the system dashboard by default and provide an overview of the mounted devices.
4. Navigation Pane	Offers quick access to essential functions, information, and personalization options.

Navigation Pane

The navigation pane menu on the top right corner of the screen enhances user interaction with IP Maestro, offering quick access to essential functions, information, and personalization options. Users can efficiently navigate the system, manage alarms, check software details, adjust preferences, and securely log out as required.

The following menus are available:

- **Active Alarms**: The count and summary of the generated active alarms that are device-related. Click 🔔 menu to view the list of active alarms on the Alarms page under the **System Dashboards** menu. The following are the types of the severity of the active alarms:
  - Critical
  - Major
  - Minor
  - Warning

Click the alarm row in the table to render another Alarm details page.

>   Note: For more information on active alarms, refer to the View Alarms Dashboard section.

- **About IP Maestro**: Click the 🛈 icon to view the IP Maestro version details.
- **User Guide**: Click the 📖 icon to view or download the IP Maestro User Manual.
- **User Preferences:** Click the 👤 icon to view the user preferences and system settings like admin, theme, and dashboard color settings.
  - **Switch Theme**: Click to switch the entire application to dark mode or light mode.
  - **Dashboard Color Scheme**: Select a color scheme from a list of options for the dashboard.
- **Logout:** Click the 🔘 icon to log out.

System Dashboards

The System Dashboards serve as visual interfaces that deliver a comprehensive status overview of the critical elements monitored by the IP Maestro domain controller. Upon a successful login, users are directed to the IP Maestro dashboard, which functions as the primary landing page. To access specific dashboards, click the designated tab.

- View Network Dashboard
- View Alarms Dashboard
- View Notifications Dashboard

View Network Dashboard

The Network Dashboard comprises multiple network-related panels featuring key contributors to the network. These panels encompass a device-platform summary, CPU utilization, memory utilization, interface traffic (outbound and inbound), fan speed, power supply temperature, and sensor temperature. Each panel operates autonomously and supports data refreshment functionality.

The following list describes some of the key features and functionalities of the panels:

Field	Description
	Reloads the data in the widget.
	Collapses (minimizes) the details. Click again to show the details.
	Removes the widget from the dashboard.
	Exports the dashboard in PDF format.
	Allows to display data based on the following settings: • Dashboard color scheme - you can choose the color scheme to display the dashboard. • Manage Widgets - you can choose widgets to show/hide on the dashboard.

Prerequisites

The devices must be mounted as the dashboard displays data for the mounted devices only.

Procedure

1. In the IP Maestro home page, click **System Dashboards > Network**.

2. Click the appropriate widget to view the details as displayed:

Field	Description
Device Platform Summary	Summarizes the platform type mounted on the system.

Top-10 CPU Utilization	Displays the top 10 CPU utilization across all devices.
Top-10 RAM Utilization	Displays the top 10 memory utilization across all devices.
Top-10 Interface Traffic (Inbound)	Displays the top 10 inbound traffic across all devices.
Top-10 Interface Traffic (Outbound)	Displays the top 10 outbound traffic across all devices.
Top-10 Fan Speed	Displays the top 10 fan speed traffic across all devices.
Top-10 Power Supply Temperature	Displays the top 10 power supply temperature traffic across all devices.
Top-10 Sensor Temperature	Displays the top 10 sensor temperature traffic across all devices.

View Alarms Dashboard

The Alarms Dashboard facilitates the monitoring of active alarms associated with mounted devices. Use various filters to customize the alarm display according to your interests. These filters include Critical, Major, Minor, and Warning tabs.

The following are the details of the alarms that are displayed on the Alarms page:

Field	Description
All Alarms	Displays all active alarms.
Acknowledged	Active alarms that are acknowledged by the current user.
Unacknowledged	Active alarms that are not acknowledged by the current user.

Note:

- The active alarms table automatically updates as new alarms are raised.
- Click an alarm row to view the history (transitions) of the selected alarm.

Prerequisites

The devices must be mounted as the dashboard displays data for the mounted devices only.

Procedure

On the IP Maestro home page, click **System Dashboards > Alarms**. The following details of the active alarms are displayed:

Field	Description
Ack	Check box to acknowledge the alarm.
Alarm	Alarm type.
Device	IPv4 address of the device.
Severity	Alarm severity level.

Resource	Origin or source of the alarm.
Description	Description of the alarm.
Timestamp	Date and time in IST.
Action	Alarm history

View Notifications Dashboard

The Notifications dashboard allows to monitor notifications (events) for the system. Use various filter options including clicking on the **Error**, **Warning**, and **Info** tabs to filter notifications that you are interested in.

> Note: The notifications table automatically updates as new notifications are raised.

Prerequisites

The devices must be mounted as the dashboard displays data for the mounted devices only.

Procedure

On the IP Maestro home page, click **System Dashboards > Notifications**. The following details of the notifications are displayed:

Field	Description
Source	Origin or source of the notification.
Description	Event description of the notification.
Severity	Notification severity level.
Role	Details of the role.
User	Details of the user.
Timestamp	Date and time in IST.

Network Management

The Network Management menu allows to configure network devices and manage its performance. It shows data on network elements such as device information, image upgrade, license information, network configuration and so on.

This menu has the following sub-menus:

- Manage Inventory
- View Topology
- Manage Device Terminal Access

Manage Inventory

The Inventory page provides options used to administer the network devices. It displays all the known network devices for this controller and helps with the mounting of the devices on the domain controller.

Icons located at the top-right of the table are primarily used to mount network devices, monitor operational progress, and for bulk execution.

This page shows the devices that are configured on the domain controller. You can mount/connect or unmount/disconnect the registered devices.

Procedure

1. In the IP Maestro home page, click **Network Management** > **Inventory**.

The Inventory page is displayed with the following details:

Field	Description
Host Name	The assigned name or label generated by the system.
Device	Ipv4 address provided by the user.
Status	Operational connection status. The possible values are: • Connected • Unable to connect • Connecting • Unknown • Rebooting
Groups	Group in which the device is located
Device Type	Device description details generated by the system.
License	License type.
Image	Installed image details.
Action	A set of actions that can be performed on each device.

Mount a device

You can mount one or many devices on the domain controller. Each network device is known as a mount point and each mount point must be configured and registered to the controller.

Prerequisites

- Ensure that the device exists in the network.
- The Management IP must be reachable.

Procedure

1. Click the [Mount new device. +] icon at the top right.

2. In the **Device Mount** dialog box, add the required details in the following fields:

Field	Description
Device	The registered device to be updated.
Username	The username used to gain access to the device.
Password	Password used to gain access to the device.

3. In the **Device Mount** dialog box, click the [Device Groups Management +] icon to define the device groups.

4. In the Device Groups dialog box, add the required details in the following fields:

Field	Description
Group name	A user-defined name or label that can be used to group devices together.
Owner (username)	Originator and/or owner of the group.
Notes	Describes the general purpose of the group.

5. Click **Save**.

6. In the **Device Mount** dialog box, click **Apply** to save the changes on the device.

7. In the **Inventory** page, click the [Reload current view with latest information.] icon to check the status of the device.

The new device is configured.

Discover a Device

You can discover and mount several devices on the Inventory page by specifying the start range and the end range of the device IPs.

Prerequisites

- The device exists in the network.
- The Management IP is reachable.

Procedure

1. On the Inventory page, click the [Device Discovery 🔍] icon.

2. In the **Device Discovery** dialog box, add the required details in the following fields:

Field	Description
Device Range	
Start	The IPv4 address to begin the search with.
End	The IPv4 address to conclude the search. Note: The ending address must be within the same subnet (network ID).
Username	The username to gain access to the device.
Password	The password to gain access to the device.
Port	The port number of the device.

3. Click **Discover** to display the list of the devices within the range you have specified.

4. In the Device Discovery dialog box, select the devices that you want to mount, and then click **Mount** to add the devices to the Inventory page.

The selected devices are mounted on the Inventory page.

Unmount a Device

You can unmount one or many devices that are mounted.

Prerequisites

The device(s) must be mounted.

Procedure

1. Click the check-box on the device rows you want to unmount and click the [Umount selected devices ➖] icon.

2. In the Confirmation dialog box, click **Yes**.

Import Device Details

You can import the Comma Separated Value (CSV) files to the Inventory page. The **Import** and **Export** features allow you to save and restore your registered devices. This feature also allows offline customization through custom imports of CSV file.

Prerequisites

- Ensure that the device already exists and is configured on the domain controller.
- All devices mentioned in the CSV files are reachable.

Procedure

1. On the **Inventory** page, click the [Bulk device mount using CSV import →] icon.

2. Select the CSV files that you want to import to the **Inventory** page.

The selected CSV files are imported. This enables you to configure a large number of devices at once.

Export Device Details

You can export the current device details in a CSV format. The **Import** and **Export** features allow you to save and restore your registered devices. This feature also allows offline customization via custom imports. This file format is comma-separated values (CSV).

Prerequisite

Ensure that the device already exists and is configured on the domain controller.

Procedure

1. On the **Inventory** page, select the devices that you want to export.

2. Click the [Export selected devices data in CSV format →] icon.

The devices' details are exported as CSV files in Excel format. You can open these CSV files on Notepad for better representation.

Push Configuration for Devices

There is an option to push device configurations in JSON format using NETCONF for selected devices.

Note: *This is an experimental feature and subject to change*.

Procedure

To push configurations for the mounted devices, follow the steps mentioned below:

1. On the **Inventory** page, select the devices to push JSON configurations.

2. Click the [Bulk device JSON config push ≋] icon. The **Config Push** screen is opened displaying the selected devices on the left. You can select more devices from the drop-down, if required.
   The main window is a JSON formatted sensitive code editor. The initial editor contains an empty payload in the first line denoted by 1 {}.
   The code editor implements IntelliSense and validation including basic syntax checking and coloring.
   The intended payload consists of NETCONF YANG model segments in JSON format as shown in the following example images.
   If you select Delete action, a basic YANG-PATCH template is shown. Enter the REQUEST URL and complete the PAYLOAD.
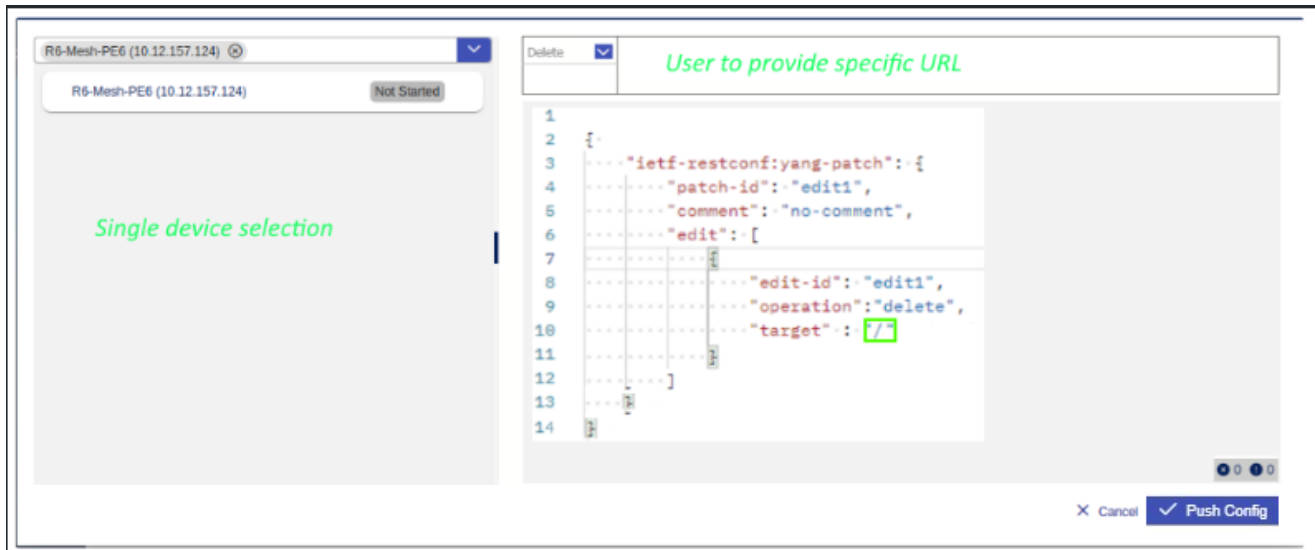
On selecting the operation and model, the code editor is populated with a delete template as shown below. The green highlighted text indicates the minimal input required.

REQUEST URL: Portal to iterate through selected devices and replace with appropriate <host> variable.

REQUEST URL: Selected model to likely have empty variables. Example, interface name in this case.

REQUEST BODY: The target attribute must be specified.
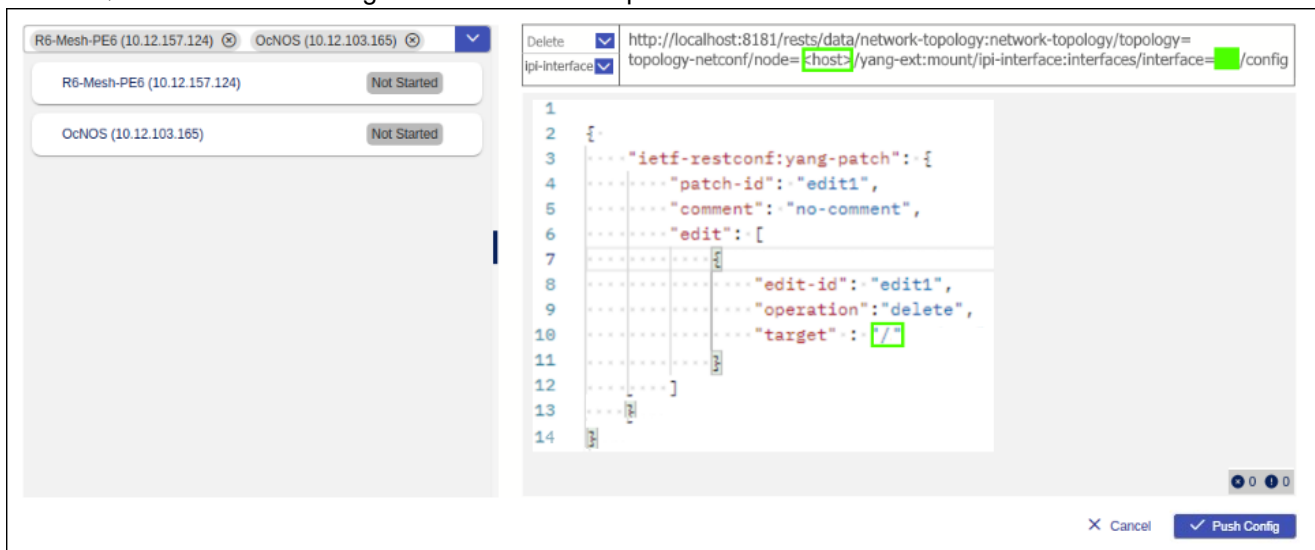
3. Click the **Push Config** button at the bottom.

4. Click **Yes** at the confirmation message that is displayed. The status of the operation is shown against the device on the screen.

HINT: You can use the CLI on a device to help you construct and format a payload using the "show json running-config" command.

Monitor Operation Progress on Device

You can monitor the operation progress on a device and administer the following:

Image Upgrade:

This supports a feature to upgrade the OcNOS image on a device being managed by IP Maestro. It provides a feature that enables IP maestro to download and upgrade the software on devices. The images are created and managed externally from IP Maestro and are made available via a published repository. The portal is then used to navigate through the public folder in search of the appropriate image. The user selects the image file for the targeted device. For more information, refer

Install License:

This provides a feature that enables IP Maestro to manage device node licenses. The binary license files are created and managed externally from IP Maestro and are made available via a published repository. The portal is then used to navigate through the public folder in search of the appropriate license. The user selects the license file based on its name, which is the serial number of the targeted device. Upon device and license selection, the portal is then used to notify the device as to where the license is located. The device will then retrieve and activate the license.

Config Backup:

This is used to back up Device Configuration for a single device or the entire network. A customized data table is used to define and manage the targeted devices.

The managed network devices are configured using YANG modules and each device contains its own modules. The Config Backup feature is used to store these device configurations (which can be restored at a later date). When a device is backed up, all the configurations are grouped and assigned a label. The label is then used to restore a specifically labeled backup.

Config Restore:

This is used to back up and restore Device Configuration for a single device or the entire network. A customized data table is used to define and manage the targeted devices.

The managed network devices are configured using YANG modules and each device contains its own modules. This feature is used to replace device configurations that were previously backed up.

Upgrade New Image

The image is a binary file that is installed on the OcNOS device. During the upgrade process, the image is first downloaded to the device. The actual installation however is performed according to the scheduled installation time. One or more registered devices can be selected for image upgrade at the same time. This two-step process is executed automatically.

Prerequisite

Ensure that the device already exists and is configured on the domain controller.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Inventory**.

2. Click the [Monitor operation progress on device] icon, and then click **Image Upgrade** to display the image upgrade status and configuration.

The following details are displayed for **Image Upgrade Progress**:

Field	Description
Host Name	The assigned name or label generated by the system.
Device	Ipv4 address provided by the user.
Status	The status of download operation, such as: • Pending • Scheduled • In-Progress • Failed • Done The status of image operation: • Started
Operation	Status in response (or notification). It is the current sequence of the two-step process. The operation status can be: • Download • Installation
Install Time (GMT)	The time scheduled to begin operation.
Current Version	Software version installed on the device.
Installed Version	The recently installed software version on the device.
Image Location	The fully qualified path name of the file.
Interface	The management interface used for file transfers.

1. Click the ⟨Add a new entry to table ⊞⟩ icon.

2. In the **Image Upgrade** dialog box, add the required details in the following fields:

Field	Description
Device	Registered device to update selected by the user from the dropdown.
Source Interface	Select an interface on the device used for data transfers (within the management VRF). The default is "eth0" interface. Note: The source interface is used for all selected interfaces.
Image Selection	
Published Images	The images that are available and hosted from an Image Repository. Note: The repository is defined in System Management > Preferences.
User Defined	Free- form field to enter a custom, fully-qualified path and image name.
Upgrade Now	Toggle to enable the input switch to execute the upgrade.

| Save Configuration | Toggle to copy the configuration to startup-config before the image upgrade. |
| Installation Time | Calendar to schedule an update. |

3. Click **Apply** to save and schedule the image upgrade for all selected devices.
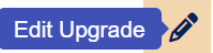
The new image upgrade is configured.

Edit the Image Upgrade Details

You can edit an image that is installed on the device.

Prerequisite

Ensure that the device already exists and is configured on the domain controller.

Procedure

1. On the **Inventory** page, in the **Image Upgrade Progress** menu, click the [Edit Upgrade ✏] icon at the end of device row.

2. In the **Image Upgrade** dialog box, add the required details in the following fields:

Field	Description
Device	Registered device to update from the dropdown.
Source Interface	Select an interface on the device used for data transfers (within the management VRF). The default is "eth0" interface. Note: The source interface is used for all selected interfaces
Image Selection	
Published Images	The images that are available and hosted from an Image Repository. Note: The repository is defined in System Management > Preferences.
User Defined	Free- form field to enter a custom, fully-qualified path and image name.
Upgrade Now	Toggle to enable the input switch to execute the upgrade.
Save Configuration	Toggle this to copy the configuration to startup-config before the image upgrade.
Installation Time	Calendar to schedule an update.

3. Click **Apply** to save and schedule image upgrade for all selected devices.

The image upgrade is edited.

Upgrade Image for all Selected Devices

You can perform bulk upgrade of images for selected devices.

Prerequisite

Ensure that the device already exists and is configured on the domain controller.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Inventory**.

2. Click the | Monitor operation progress on device | ☰ **i**con, and then click **Image Upgrade** to display the image upgrade status.

3. In the Image Upgrade Progress panel, click the | Upgrade image for all selected devices. | 🖼 icon.

4. In the **Image Upgrade** dialog box, add the required details in the following fields:

Field	Description
Device	Registered device to update selected by the user from the drop-down.
Source Interface	Select an interface on the device used for data transfers (within the management VRF). The default is "eth0" interface. Note: The source interface is used for all selected interfaces.
Image Selection	
Published Images	The images that are available and hosted from an Image Repository. Note: The repository is defined in System Management > Preferences.
User Defined	Free- form field to enter a custom, fully-qualified path and image name.
Upgrade Now	Toggle to enable the input switch to execute the upgrade.
Save Configuration	Toggle to copy the configuration to startup-config before the image upgrade.
Installation Time	Calendar to schedule an update.

5. Click **Apply** to save and schedule the image upgrade for all selected devices.

The image upgrade is configured for the selected device(s)

Import the Image Upgrade Details

You can import the CSV files to the Image Upgrade page. The **Import** and **Export** features allow you to save and restore your upgraded images. This feature also allows offline customization via custom imports. This file format is comma-separated values (CSV).

Prerequisites

*   The device already exists and is configured on the domain controller.

*   All devices mentioned in the CSV files are reachable.

Procedure

1. On the **Inventory** page,in the **Image Upgrade Progress** menu, click the **Import** 🔁 icon.

2. In the **Import Data** dialog box, **Select** or **Upload** the CSV files that you want to import to the **Image Upgrade Progress** menu.

The selected CSV files are imported on the **Image Upgrade Progress** menu. This enables you to configure a large number of images in one go.

Export the Image Upgrade Details

You can export the current device details in a CSV format. The **Import** and **Export** features allow you to save and restore your upgraded images. This feature also allows offline customization via custom imports. This file format is CSV.

Prerequisite

Ensure that the device already exists and is configured on the domain controller.

Procedure

1. On the **Inventory** page, in the **Image Upgrade Progress** menu, select the devices for which you want to export the images.

2. Click the **Export** ![icon] icon.

The devices' details are exported as CSV files in Excel format. You can open these CSV files in Notepad for a better representation.

Delete the Image Upgrade Details

To cancel the scheduled image upgrade for all selected devices, you must delete the details from the **Image Upgrade** page.

Prerequisite

The image upgrade details are applied on the mounted devices.

Procedure

1. In the **Image Upgrade Progress** menu, select the device row(s) to delete the image.

2. Click **Delete**.

The scheduled image upgrade gets canceled for all the selected devices.

Edit the License Installation Progress

To edit the available license, follow the steps mentioned below:
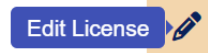
Prerequisites

- The devices are already mounted and registered on the domain controller.
- Licenses are externally available via a public URL.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Inventory**.

2. Click the **Monitor operation progress on device** ⚞☰ icon and click **Install License** to display the license status and configuration.

3. The Inventory page is displayed with the following details under the **License Installation Progress** menu:

Field	Description
Host Name	Assigned name or label generated by the system.
Device	Ipv4 address provided by the user.
Status	Operational status of the device.
Device ID	Serial number of the device.
Device SKU	Software capabilities installed on the device.
Software Type	License type of the device.
License Validity	License status of the device.
Interface	Management interface used for file transfers.
License Path	Fully qualified path name of the file.

4. Click the **Edit License** ✎ icon.

5. In the **Edit Table Entry** dialog box, add the required details in the following fields:

Field	Description
Device	Registered device to update.
Source Interface	Select an interface on the device used for data transfers (within the management VRF). The default is "eth0" interface. Note: The source interface is used for all selected interfaces.
License Selection	
Published Licenses	Licenses available and hosted from a License Repository. The repository is defined in System Management > Preferences.
User Defined	Free-form field to enter a custom fully-qualified path and name of license.
Device ID	Registered device to update.

6. Click **Save** at the bottom of the **License Installation Progress** menu to copy and save the license on the device.

The license installation progress details are edited.

Configure New Backup

Config Backup can be used to back up Device Configuration for a single device or the entire network.It is used to store the device configurations to be restored at a later date. When a device is backed up, all the configurations are grouped and assigned a label. The label is then used to restore a specifically labeled backup.

To define an immediate backup, click the **Action** icon to the right of the device row and click **Operations > Config Backup.** The **Config Backup** dialog box is displayed. Enter the appropriate information as follows:

Field	Description
Device	The device to backup.
Backup Label	A user-defined label to identify the configuration.

Prerequisites

Ensure that the devices are already mounted and registered on the domain controller.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Inventory**.

2. Click the [Monitor operation progress on device ≣] icon and click **Config Backup** to display the backup status and configuration.

The **Config Backup Progress** menu is displayed with the following information:

Field	Description
Host Name	The Host name or Label.
Device	The device to backup.
Status	Displays the status of the operation. The possible values are: • Pending • Scheduled • In-Progress • Failed • Done
Start Time	Date and time provided by the date-time picker.
Label	The name assigned to the host. The label is N/A if the type is network.

1. Click the [Add a new entry to table +] icon.

2. In the **New Config Backup** dialog box, add the required details in the following fields:

Field	Description
Device	The device to back up.
Backup Label	A user-defined label to isentify the configuration.

3. Click **Save**.

4. Click **Apply** at the bottom of the **Config Backup Progress** menu to apply and save the changes on the device.

The new backup is configured.

Create/Update Schedule for Backup of Registered Devices

You can schedule a backup of the registered devices.

Prerequisites

- The devices are already mounted and registered on the domain controller.

Procedure

1. In the **Config Backup Progress** menu, click the **Create/Update schedule for backup of registered devices** icon.

2. The **Save Backup Schedule** dialog box is displayed. Add the required details in the following fields:

Field	Description
Start Time	Use the calendar to schedule a backup.
Recurring	The frequency to schedule a backup. The possible values are: • Daily • Weekly • Monthly

3. Toggle the **Active** icon to schedule the backup. The icon changes to green color indicating the "Active" status

   Note: If there is an active schedule for any of the devices, the status line will display a green status icon.

4. Click **Save**.

5. In the Inventory page, click **Apply** to save the changes on the device.

6. In the Inventory page, click **Refresh** to check the status of the device.

The new schedule is updated.

View Backup History and Formatted Configuration

You can view the backup history and the formatted configuration of the already configured and created backup and backup schedules.

Prerequisites

- The devices are already mounted and registered on the domain controller.

Procedure

1. In the **Config Backup Progress** menu, click the **Actions** icon to the right of the device details and click **History**.

   The **Backup History** page is displayed showing the **Label** and the **Backup Time** of the already configured backup schedules.

2. Click the [Show Formatted Configuration] icon to view the configuration details of the specific module.

Compare Configuration

The comparing configuration process allows you to compare the configurations of the backup labels of the selected modules.

Prerequisites

• The devices are already mounted and registered on the domain controller.

Procedure

1. Under the **Config Backup Progress** menu, click the **Action** [Actions ⋮] icon and click **Compare**.

   The **Compare Configuration** page is displayed.

2. Select the backup labels from the drop-down to compare their configurations.

Configure Restore

Config Restore can be used to back up and restore images for a single device or the entire network.

Note:

When a device is restored, the previous configuration is removed and replaced with the new set of configurations.

To define a restore, in the **Inventory** screen, click the **Action** icon to the right of the device row and click **Operations > Config Restore.** In the **Config Restore** dialog box that is displayed, enter the appropriate information as follows:

Field	Description
Device	Registered device to update selected by the user from the drop-down.
Archive	The available labels to restore.

Click **Apply** to apply the changes.

Prerequisites

• The devices are mounted and registered on the domain controller.
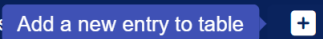
Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Inventory**.

2. Click the [Monitor operation progress on device ⋮≡] icon, and then click **Config Restore** to display the restore status and configuration.

   The Inventory page is displayed with the following details under the **Config Restore Progress** menu:

Field	Description
Host Name	The assigned name or label generated by the system.
Device	The host IP address.

Status	Displays the status of the operation. The possible values are: • Pending • Scheduled • In-Progress • Failed • Done
Start Time	Date and time provided by the date-time picker.
Label	The name assigned to the host. The label is N/A if the type is network.

3. Click the **Add a new entry to table** ⊕ icon.

4. In the **New Config Restore** dialog, add the required details in the following fields:

Field	Description
Device	Registered device to update.
Archive	The available labels to restore.

5. Click **Save**.

6. Click **Apply** at the bottom of the **Config Restore Progress** menu to apply and save the changes on the device.

7. In the Inventory page, click **Refresh** to check the status of the device.

The new restore is configured.

Action

In the **Inventory** home page, every device row contains the **Actions** ⋮ icon to the right which enables the following actions:

Field	Description
Device information	Contains the basic information about the device such as operational status, port speed, fan, temperature, power, transceiver details etc.
Device Terminal Access	Redirects to the Device Terminal Access page to gain direct access to a shell on any device on the network using a secure connection.
Interfaces	Interface details of the device. The assigned name or label generated by the system.

Operations	
• Unmount Device	• To unmount the device
• Image Upgrade	• To add a published or user defined image
• Install License	• To install published or user defined license
• Config Backup	• To apply backup for the device
• Config Restore	• To apply config restore using the available labels on the device
• Device Groups	• To assign the device to a group
Monitoring	
• Device Metric	• Allows to monitor the resources for the device
• Chassis Monitoring	• Visualization of the hardware metrics for the device
• Interface Statistics	• Visualization of the interface for the device
• Device Logs	• Displays the device log details.

View Topology

This menu is used to represent a topology view of the network based on Link Layer Discovery Protocol (LLDP). The map consists of nodes and edges where each node represents a registered network device and shows connections between each node using bidirectional edges.

The devices that are configured can be viewed in the topology. The LLDP topology is a vendor-neutral link layer protocol used by network devices. It is used for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally, wired Ethernet. The LLDP topology is configured on the domain controller.

Note: The nodes are initially positioned based on a d3-force algorithm, but each node can be dragged to improve visibility.

The following list describes some of the key features and functionalities:

Field	Description
Toolbar	
	Displays device link details on an information panel.
	Provides options to customize the graph.
	Provides access to User Manual.
	Manual topology refresh.
Node mouse events	
	Shift-click to show device details.
	Shift-click to show an enlarged view of the nodes.
	Right-click to show the sub-menu containing device links.

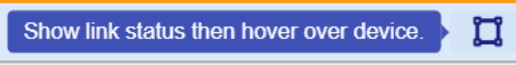| Node legend	
●	Normal operation.
◼	Fault detected.

View Devices on the Topology Menu

The configured devices are shown on the Topology page as follows:

Prerequisite

Ensure that the configured devices (through the device registration process) are available and connected.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Topology.** The Topology page is displayed. You can view the nodes according to the **Alarm** and **Groups**.

2. Click the [Show link status then hover over device.] icon and then hover over the node icon to view the device details. The following details of the selected device are displayed:

Field	Description
Details	
Host Name	Network node name defined for the topology.
Node ID	Unique identifier for the node.
Software Version	OcNOS version installed on the device.
Software Build	Build details of software installed on the device.
Boot Time	Device boot time.
Time Zone	Time zone for the device boot time.
License Type	License type.
License Status	License status.
License Remaining Days	Number of days for license validity.
Active Alarm Severity	Severity of the active alarm.
Groups	
Groups	Shows the group for the selected node, if any.

Customize Nodes and Links of Configured Devices

You can customize nodes and links of the configured devices as follows:

Prerequisite

Ensure that the configured devices (through the device registration process) are available.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Topology**.The Topology page is displayed.

2. Click the [Open the toolbox to customize the graph.] icon, which allows you to customize the **Nodes** and **Links** of the configured devices.

3. Navigate and customize the following details:

- Nodes:

    - Show Node Labels: The names of the nodes in the configured devices. The node labels are shown by default.

    - Node Label: Sets the node label in topology to Host Name or Node ID.

- Links:

    - Link Thickness (px): Drag to set the stroke-width property to define the thickness of the links or edges.

    - Curved Lines: Select the checkbox to display links as curved lines.

    - Link Curve Size: Drag to adjust the shape of the curved lines.

    - Bidirectional links: Select the checkbox to display the bidirectional links.

    - Arrow Size: Drag to adjust the size of the arrows.

    - Arrow Position: Drag to adjust the position of arrows in the links.

4. Click **Reset** to restore the changes back to default or click **Close** to apply the changes.

View the Device-level Dashboards

You can view the dashboards from a device level by right-clicking the configured device in the Topology menu.

Prerequisite

Ensure that the configured devices are available.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Topology**.The Topology page is displayed.

2. Right-click the configured device, for which you want to see the device-level information. The following details of the device are displayed:

Field	Description

Network Management	
• Inventory	• Redirects to the Inventory page for information on the devices' mount transaction.
• Device Terminal Access	• Redirects to the Device Terminal Access page to gain direct access to a shell on any device on the network using a secure connection.
Network Monitoring	
• Device Metrics	• Allows to monitor the resources for the device
• Chassis Monitoring	• Visualization of the hardware metrics for the device
• Active Alarms	• Displays the active alarms for the device.
• Interface Statistics	• Visualization of the interface for the device
• Device Logs	• Displays the device log details.

Manage Device Terminal Access

Terminals are web-based command-line applications to access the devices from which you can directly connect to the OcNOS device over Secure Shell Protocol (SSH). This is a fully-featured terminal emulator that can be used to gain direct access to a shell on any device on the network using an SSH connection.

Prerequisite

Ensure that the configured devices (through the device registration process) are available.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Device Terminal Access**. The Device Terminal Access page is displayed.

2. Click the [Add new terminal. +] icon. This allows you to manage the **New Connection** and **Registered Devices** as follows:

   • **New Connection**:

      • Host: IP Address/hostname for connecting to the terminal over SSH.

      • Username: Username for connecting the terminal to a host/device over SSH.

   • **Registered Devices**: Select a host from the drop-down menu.

3. Click **Connect** to view the running configuration.

   The OcNOS device is connected. To terminate a session, type exit in the **terminal>_** or just click the **Close** icon on the terminal tab.

Network Monitoring

The Network Monitoring menu contains submenus that display system-configured dashboards. These dashboards are tailored to provide comprehensive visual representations of network data and performance metrics. Users can access detailed insights into devices configured for distinct time periods, including 15 minutes, 30 minutes,1 hour, 12 hours, 24 hours, 7 days, 30 days, 90 days or 1 year. Users can utilize these submenus to track historical trends, analyze patterns, and assess the performance of network devices across different durations.

This chapter describes the following sections:

- View Device Metrics
- View Interface Statistics
- View Chassis Monitoring
- Manage Device Logs
- Manage System Audit

View Device Metrics

The Device Metrics dashboard allows you to monitor resources for mounted devices. Using RESTCONF monitoring capabilities, the dashboard presents comprehensive information encompassing CPU, disk, memory, and host-related metrics.

The following list provides details on key features of device metrics:

Field	Description
⟳	Reloads the data in the widget.
⊟	Collapses (minimizes) the widget. Click again to show the details.
⊗	Removes the widget from the dashboard.
⮕	Exports the Dashboard in PDF format. You can choose the panels to include/exclude from the file.
🗓 Last 12 Hours(s)	Displays data according to the date range.
⚙	Allows to display data based on the following settings: • Date range - displays data according to the specified date range. • Auto refresh - If enabled, data is refreshed as per the specified time interval. • Dashboard color scheme - you can choose the color scheme to display the dashboard. • Manage Widgets - you can choose widgets to be shown on the dashboard.

Note: This dashboard currently shows data from polling the device using RESTCONF. The data is not real-time, causing a 3-minute delay in fetching information based on the polling interval. To instantly update the page, click the reload icon in the toolbar.

Prerequisites

Ensure that the configured devices (through the device registration process) are available.

Procedure

1. In the IP Maestro home page, navigate to **Network Monitoring** > **Device Metrics**.

2. Click the **Device** dropdown to select a device from the available list of registered devices.

    The following list provides details on key features of device metrics:

Field	Description
CPU Information	
CPU Usage	Percentage of CPU usage.
1 min Load	Percentage of load to the CPU over 1 minute for the selected device.
5 min Load	Percentage of load to the CPU over 5 minutes for the selected device.
15 min Load	Percentage of load to the CPU over 15 minutes for the selected device.
RAM Information	
RAM Usage	Percentage of RAM usage.
RAM Details	Details of Total, Used and Available RAM in megabytes.
Other Details	Details about Shared memory, Buffers and number of processes running currently.
Swap Memory	The total, used and available swap space in megabytes.
High Memory	The total, used and available high memory in the RAM in megabytes.
CPU Usage Chart - Historical	Chart showing the percentage of CPU utilization, and load details for different time intervals.
RAM Usage Chart - Historical	Chart showing the Total, Used and Available memory with respect to RAM usage.
Hard Disk Information	Detailed information about the hard disk and disk activity.

View Interface Statistics

The Interface Statistics dashboard gives a visual representation of the interface specific to the selected device.

The dashboard displays a data table containing a comprehensive list of all interfaces, displaying the administrative and operational statuses, alongside additional miscellaneous statistics (such as Speed, MAC, and so on.). It also includes the timestamp of the last change made to each interface.

In conjunction with the data table, the dashboard provides aggregated metrics reflecting inbound and outbound traffic for these interfaces. These metrics offer a summarized view of traffic flow and activity on the selected device's interfaces.

The following list describes some of the key features and functionalities of the interface statistics details:

Field	Description
	Reloads the data in the widget.
	Collapses (minimizes) the widget. Click again to show the details.
	Removes the widget from the dashboard.
	Exports the Dashboard in PDF format. You can choose the panels to include/exclude from the file.
Last 12 Hours(s)	Displays data according to the date range,
	Allows to display data based on the following settings: • Date range - displays data according to the specified date range. • Auto refresh - If enabled, data is refreshed as per the specified time interval. • Dashboard color scheme - you can choose the color scheme to display the dashboard. • Manage Widgets - you can choose widgets to be shown on the dashboard.

Note: This dashboard currently shows data from polling the device using RESTCONF. The data is not real-time, causing a 3-minute delay in fetching information based on the polling interval. To instantly update the page, click the reload icon in the toolbar.

Prerequisites

Ensure that the configured devices are available through the device registration process.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Interface Statistics**.

2. Click the **Device** dropdown to select a device from the available list of registered devices

3. Click the **Interface(s)** dropdown to select a particular interface(s) (this is optional).

Field	Description
Interface Statistics	Represents the data in tabular view and provides the following information for the selected interface: • Admin Status • Oper Status • LastChange-Flapped • Speed (MBs) • Index • MAC • Inbound Traffic • Outbound Traffic • Inbound Packets • Outbound Packets • Action
Network Traffic Bandwidth	Displays the network traffic bandwidth in bytes per second.
Network Traffic (Bytes)	Displays the network traffic in bytes.
Network Traffic (Packets)	Displays the network traffic in packets.
Errors and Discards	Displays the errors and discards in packets.

Note: The traffic data represented indicates the total aggregate traffic through the port.

Clear Interface Counters

The Interface Statistics table provides a wide range of information on the traffic and inbound/outbound packets for the selected interface. There is an option to clear the information and reset the values for one or more interfaces.

Procedure

1. In the IP Maestro home page, navigate to **Network Management** > **Interface Statistics**.

2. Click the **Device** drop-down to select a device from the available list of registered devices.

3. In the Interface Statistics table, click the **Clear Interface Counters** icon at the end of the interface row for which you want to clear the counter.

4. At the confirmation dialog, click **Yes** to confirm.

    The counters are cleared and all the values are reset to zero.

Alternatively, you can follow the below steps to clear the counters for more than one interface at a time:

1. Select the check-box at the start of the required interface rows.

2. Click the **Bulk Clear Interface Counters** icon that is enabled above the statistics table.

3. Click **Yes** at the confirmation dialog that is displayed.

View Chassis Monitoring

Chassis Monitoring dashboard allows you to retrieve the device-specific information concerning device type, power supply, fan, and sensors for the selected device. This dashboard offers a visual representation of hardware metrics associated with mounted devices.

There are two sections of the dashboard.

- **Top Section**: It presents a summary and detailed information for the selected device. When a physical device is selected, this section displays the following information:

  - **Summary Fieldset:** Displays fundamental parameters pertinent to the device.

  - **Details Fieldset:** Provides miscellaneous values retrieved from the device.

  However, if a Virtual Machine is selected, only its summary is visible.

- **Bottom Section:** It offers an aggregate perspective on hardware-specific metrics, focusing on the hardware chassis. It includes details concerning:

  - Power Supplies

  - System Sensors

  - Fans

The following list provides details on key features of chassis monitoring:

Field	Description
⟳	Reloads the data in the widget.
⊟	Collapses (minimizes) the widget. Click again to show the details.
⊗	Removes the widget from the dashboard.
▶	Exports the Dashboard in PDF format. You can choose the panels to include/exclude from the file.
🗓 Last 12 Hours(s)	Displays data according to the date range,
⚙	Allows to display data based on the following settings: • Date range - displays data according to the specified date range. • Auto refresh - If enabled, data is refreshed as per the specified time interval. • Dashboard color scheme - you can choose the color scheme to display the dashboard. • Manage Widgets - you can choose widgets to be shown on the dashboard.

Note: This dashboard currently shows data from polling the device using RESTCONF. The data is not real-time, causing a 3-minute delay in fetching information based on the polling interval. To instantly update the page, click the reload icon in the toolbar.

Prerequisites

Ensure that the configured devices (through the device registration process) are available.

Procedure

1. In the IP Maestro home page, navigate to **Network Monitoring** > **Chassis Monitoring**.

2. Click the **Device** dropdown to select a device from the available list of registered devices:

.

| Field	Description
Device Details	Displays the following data of the OcNOS device: • Host Name • IP Address • Software Version • Software Build • Boot Time • Device Model
Device Summary	Displays a device summary for the OcNOS device, with details on the power supply, the total number of installed fans, fan cards, and system sensors on the devices.
Power Supply Summary	Displays the summary of the power supply units.
Power Supply Temperature Chart	Displays the temperature of the individual sensors installed on the devices.
Sensors Summary	Displays the summary of the sensors installed on the hardware devices.
Fan Summary	Displays the fan summary in Rotation Per Minute (RPM).
Fan Speed Chart	Displays the data of the all the fans represented in the chart.
Sensor(s) Temperature Chart	Displays data on the temperature of all the installed sensors.
Fan Card Summary	Displays data of the fan cards.
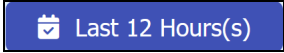
Manage Device Logs

The Device Logs page helps you view logs, such as application logs, for the selected host. When a device is mounted, a remote syslog configuration is pushed into OcNOS to set up IP Maestro remote syslog server that will receive OcNOS device logs.

This dashboard provides a visualization of the logs for the selected devices. The logs can be filtered by Log Level, Protocol, and Description.

Note: This dashboard currently shows data from polling the device using RESTCONF. The data is not real-time, causing a 3-minute delay in fetching information based on the polling interval. To instantly update the page, click the reload icon in the toolbar.

The following list describes some of the key features and functionalities of the device log details:

Field	Description
⟳	Reloads the data.
▸	Exports the data in PDF format.
📅 Last 12 Hours(s)	Displays data according to the date range.
⟳ 10 s	Auto refresh every 10 seconds
⚙	Allows to display data based on the following settings: • Date range - displays data according to the specified date range. • Auto refresh - If enabled, data is refreshed as per the specified time interval.

View Device Logs

Prerequisite

• Ensure that the configured devices (through the device registration process) are available.

Procedure

1. In the IP Maestro home page, click **Network Monitoring** > **Device Logs**.

2. In the **Monitored** tab, select a device from the available list of registered devices.

Field	Description
Device • Device IP • Host name	Select a device from the available list of registered devices. • Ipv4 address of the device • Assigned name or label
Log Level	Select the severity of the log.
Protocol	Select the protocol module name.

The device logs for the selected device is displayed with the following details:

Field	Description
Host Name	Assigned name or label
Device	IP address of the device
Timestamp	Date and time in Indian Standard Time (IST) format

Field	Description
Log Level	Severity of the log.
Protocol	Protocol module name.
Description	Operator logs with severity.
Details	Details of the log.

Upload Device Logs

You can import or load a previously saved device log file. The content is added to the database to provide persistent storage and retrieval capabilities.

Prerequisite

- Ensure that the configured devices (through the device registration process) are available.

- The device log file must be available for upload.

Procedure

1. In the IP Maestro home page, click **Network Monitoring** > **Device Logs**.

2. In the **Uploaded** tab, click **Upload Log File(s)** button. Click **+Choose** to select the file or drag and drop the file to upload.

Manage System Audit

The System Audit page provides audit logging of configuration changes to all the registered devices. It is a read-only menu where no write or delete capabilities are provided. It provides the ability to expand and view payload contents in a user-friendly format.

The System Audit page provides a group of tabbed panels used to display and filter various logs throughout IP Maestro and the network.

The following tabs can be used to display, filter, and inspect the following information:

- **Configuration Logs**: Modifications applied to the network devices.

- **Administrative**: User actions or operational (such as mounting/unmounting devices).

View Configuration Logs

This table provides a configuration history for all the devices in the network. Each log shows the device and its associated operation.

In addition to providing the details for each operation, most operations contain a configuration (or payload). When a payload is available for inspection, click the icon within the desired row under the **Action** column.

Prerequisite

The device already exists and is configured on the domain controller.

Procedure

1. In the IP Maestro page, click **Network Monitoring > Config Audit Logs.**

2. Click the **Configuration Logs** tab to display the log status and configuration as follows:

Field	Device IP
Device IP	Ipv4 address.
Status	Command execution status. The possible values are: • Success • Failed
Operation	The execution type to configure the device.
Timestamp	The execution date and time logged by the system in IST.
User	The user that applied the configuration.
Browser	The originating address of the client.
Origin	The servicing component responsible for command execution.
Payload	The payload identifier in JSON format.

3. Click the **Action** expansion icon to show the entire payload of the existing entries in a JSON-friendly format.

4. Click **Close** to close the **JSON Formatted Payload** window.

View Administrative Logs

This table provides a configuration history for all other non-device configurations or operations.

In addition to providing the details for each operation, most operations will contain a configuration (or payload). When a payload is available for inspection, click the icon within the desired row under the **Action** column.

Prerequisite

The device already exists and is configured on the domain controller.

Procedure

1. In the IP Maestro home page, click **Network Monitoring > Config Audit Logs.**

2. Click the **Administrative** tab to display all the non-device configurations and operations with the following details:

Field	Device IP
Device IP	Ipv4 address.
Status	Command execution status. The possible values are: • Success • Failed
Operation	The execution type to configure the device.

Field	Device IP
Timestamp	The execution date and time logged by the system in IST.
User	The user that applied the configuration.
Browser	The originating address of the client.
Origin	The servicing component responsible for command execution.
Payload	The payload identifier in JSON format.

3. Click the **Action** expansion icon to show the entire payload of the existing entries in a JSON-friendly format.

4. Click **Close** to close the **JSON Formatted Payload** window.

System Management

The System Management menu in the IP Maestro banner serves as a comprehensive tool for overseeing various aspects of the system. It facilitates the management of key components, including the IP Maestro portal, user activity, user accounts, sessions, user preferences, and DHCP & SMTP configuration.

This chapter describes the following sections:

- User Management
- Manage Preferences
- View IP Maestro Health

User Management

The User Management page allows you to manage users and sessions.

Accounts

The Accounts dashboard allows you to create, read, delete, and update user accounts. You will be able to access the Accounts screen and create multiple users with similar access. You can also create, delete, and update all user profiles. The data of all the users are shown in table format. Multiple users can be created, updated, and deleted by selecting table rows.

Add a New User

The addition process allows you to add new users to the Accounts page.

Prerequisite

You have the permissions/roles to add a new user.

Procedure

1. In the IP Maestro home page, click **System Management** > **User Management**.

2. In the **Accounts** tab, click the Create new user + icon.

3. In the **Create new user** dialog box, add the following field details:

Field	Description
Username	The username to authenticate provided by the user.
Email	Email address of the user.
Role	The user role. The following are the user roles: • IP Maestro Administrator - Complete read and write access to entire system. • IP Maestro Engineer - Read access to entire system. Read and write access to fabric interconnect infrastructure and network security operations. • IP Maestro Operator - Read access to entire system. Read and write access to all the logs. • IP Maestro User - Read only access to the entire system.

First Name	First name of the user.
Last Name	Last name of the user.
Password	Provide the credentials for the user to access.

4. Click **Create** to add the new user.

The new user is added in the **Accounts** tab.

Edit an Existing User

The editing process allows you to edit existing users on the Accounts page.

Prerequisites

*   The user is already added to the user accounts.
*   You have the permissions/roles to edit an existing user.

Procedure

1. In the IP Maestro home page, click **System Management** > **User Management**.

2. In the Account tab, select the checkbox of the user accounts row to edit the selected users.

3. Click **Action** > **Edit User** for the user that you want to edit or update.

4. Edit the required fields in the dialog box that is displayed:

Field	Description
Username	The username to authenticate provided by the user.
Email	Email address of the user.
Role	The user role. The following are the user roles: • IP Maestro Administrator - Complete read and write access to entire system. • IP Maestro Engineer - Read access to entire system. Read and write access to fabric interconnect infrastructure and network security operations. • IP Maestro Operator - Read access to entire system. Read and write access to all the logs. • IP Maestro User - Read only access to the entire system.
First Name	First name of the user.
Last Name	Last name of the user.
Password	Provide the credentials for the user to access.

5. Click **Update** to incorporate your changes.

6. In the Accounts page, click **Refresh** to check the status of the user.

The existing user is updated.

Delete an Existing User

When you want to remove the user from its physical location, you must delete the user details from the Accounts page.

Prerequisites

- The user is already added to the user accounts.

- You have the permissions/roles to delete an existing user.

Procedure

1. Select the row containing the user account to delete the selected users.

2. In the **Action** tab, click **Delete User** for the user that you want to delete.

3. In the **User Deletion Confirmation** dialog box, click **Yes** to delete the user.

The selected users are deleted from the Accounts page.

Note: The default admin user cannot be deleted. This default admin user can be used to create other admin users

Sessions

The sessions page allows the user to view and manage all the active sessions.

View Sessions

Allows you to view which users are active and when they are logged in.

Prerequisite

The users must be active to be viewed.

Procedure

In the IP Maestro home page, click **System Management** > **User Management > Sessions**. The Sessions page is displayed with the details related to the **Username**, IP address (**From IP**), **Session Start**, and **Last Access** details.

Note: To log out a user from the session, select the user and click the **Logout** icon.

Email Notifications

This tab allows you to subscribe to email alerts by selecting the alert type and the severity. You can select the alert type as alarm or notification.

As an Admin, you can choose an user from the list of registered users in the drop-down, and select the type of alarm or notification that you want to enable for that user.

Procedure

1. In the IP Maestro home page, click **System Management** > **User Management > Email Notifications.** The page is displayed with the list of registered users.

2. From the drop-down list, select the user that you want to subscribe to email alerts.

3. Click the check-box for the desired **Alarm** type - Critical, Major, Warning, Minor.

4. Click the check-box for the **Notification** type.

5. Click **Save** to save the changes. A pop-up message is displayed to confirm the preferences are saved successfully.

Note: As a non-admin user, you can go to the **Email Notifications** tab and check if your email ID is correct. You can select the severity type check-box for which you want to be notified on email.

User Federation

This tab provides support for role-based access control using Lightweight Directory Access Protocol (LDAP) Authentication and Active Directory (AD). IP Maestro user interface leverages the User Federation capabilities of authentication manager to integrate LDAP and AD.

For detailed information on configuration, refer to Appendix section in the *IP Maestro Installation Guide*.

Create and Manage Providers

The **User Federation** tab on IP Maestro interface enables administrators to create and manage providers.

To add a new provider, follow the steps mentioned below:

1. In the IP Maestro home page, click **System Management** > **User Management** > **User Federation**.

2. In the User Federation page, click the **Add Provider** button.

In the **Provider Details** page that is displayed, enter the details as follows:

Field	Description	Mock LDAP server settings	Comments
General Options			
Provider Name	Enter a display name for the provider.	Test LDAP server	Any name to identify the provider.
Vendor	Type of the LDAP vendor.	Other	Mock LDAP server is not a part of AD, hence use "Other".
Connection and Authentication Settings			
Connection URL	URL to connect to the LDAP server	ldap://<ip-of-server>:port	For example: ldap://1.1.1.1:10381
Enable StartTLS	Encrypts the connection to LDAP using StartTLS	Off	Mock LDAP server does not support TLS.
Connection Pooling	Check box to determine if IP Maestro must use connection pooling for accessing LDAP server.	Off	Connection pooling is not required to access mock LDAP server.
Connection Timeout	LDAP connection timeout in milliseconds	Off	No connection timeout is specified.
Test Connection	Button to test the connection		
Bind Type	Type of authentication method used during LDAP bind operation.	Simple	If the LDAP server allows anonymous requests, select 'none'. The mock LDAP server will not accept anonymous requests hence select 'simple' and pass authentication details.

Bind DN	Distinguished name of the LDAP admin for IP Maestro to access LDAP server.	`uid=jbrown123,ou=People,dc=keycloak,dc=org`	Complete DN of the admin user
Bind Credentials	Password of LDAP admin.	`password123`	Password is encrypted and only used to check authentication with LDAP server.
Test Authentication	Button to test the authentication		
LDAP Searching and Updating			
Edit Mode	READ_ONLY - Read-only LDAP store. UNSYNCED - Imports User data without syncing back to LDAP.	UNSYNCED	Recommended to select edit mode as UNSYNCED so that the basic information of users will be imported to IP Maestro and cached.
Users DN	Parent distinguished name of LDAP users. It is the name of the LDAP tree where the users are stored.	`ou=People,dc=keycloak,dc=org`	Name of the LDAP tree where users are present.
Username LDAP Attribute	LDAP attribute that is stored as IP Maestro user name	`uid`	The attribute in the mock LDAP server which defines the username of the users.
RDN LDAP Attribute	Name of LDAP attribute used as Relative Distinguished Name (RDN) of typical user	`uid`	Same as user name attribute.
UUID LDAP Attribute	LDAP attribute used as unique object identifier for objects in LDAP.	`uid`	Same as user name attribute.
User Object Classes	LDAP object class attribute values for users, separated by commas	`top, person, organizationalPerson, inetOrgPerson`	Object classes defined for users in the mock server.
Read Timeout	LDAP read timeout in milliseconds that apply to read operations		Read timeout values not configured.
Pagination	Check-box to determine if LDAP server supports pagination	Off	The mock server does not support pagination.
Group Mapper Settings			
Create Group Mapper	Check-box to create LDAP mapper	On	Group-mapper will be created
LDAP Groups DN	Distinguished name of LDAP where the groups of the tree are saved.	`ou=RealmRoles,dc=keycloak,dc=org`	Tree where groups are defined in the mock server.
Group Name LDAP Attribute	Name of LDAP attribute in group objects and Relative Distinguished Name (RDN) of group	`cn`	This defines the name of the group in the mock LDAP server.

Group Object Classes	LDAP object class of the group object, separated by commas	`top, groupOfNames`	These are the 2 object classes defined in the server.
Membership LDAP Attribute	Name of LDAP attribute on group used for membership mappings	`member`	
Membership Attribute Type	• DN - The LDAP group has members declared in the form of full distinguished name. • UID - The LDAP group has members declared in the form of user ID.	`DN`	
Membership User LDAP Attribute	Enter if the membership attribute type is UID	`uid`	
User Groups Retrieve Strategy	Specifies how to retrieve groups of users: • LOAD_Groups_BY_MEMBER_ATTRIBUTE - Roles of users are retrieved by sending LDAP query for all groups where 'member' is our user. • GET_GROUPS_FROM_USER_MEMBEROF_ATTRIBUTE - Groups of users are retrieved from 'memberOf' attribute of our user.	LOAD_Groups_BY_MEMBER_ATTRIBUTE	
Member-of LDAP Attribute	Used only when the User Roles Retireve Strategy is GET_GROUPS_FROM_USER_MEMBEROF_ATTRIBUTE. The default value is 'memberOf'.	memberOf	This is default value as it is not needed for mock LDAP server since retrieve strategy is LOAD_Groups_BY_MEMBER_ATTRIBUTE

The configurations that are provided enable IP Maestro to connect to the LDAP server, allowing users from the LDAP server to log in to Maestro upon successful authentication.

Here are a few images of the mock LDAP server configurations that have been added in the IP Maestro user interface.

General Options

Provider Name * ❓   Test LDAP Server

Vendor * ❓   Other ⌄

Connection and Authentication Settings

Connection URL * ❓   ldap://1.1.1.1:10381

Enable StartTLS ❓   ☐ Off

Connection Pooling ❓ ☐ Off

Connection Timeout ❓

Test Connection

Bind Type * ❓   simple ⌄

Bind DN * ❓   uid=jbrown123,ou=People,dc=keycloak,dc=org

Bind Credentials * ❓ •••••••••••   👁

LDAP Searching and Updating

Edit Mode * ❓   UNSYNCED ⌄

Users DN * ❓   ou=People,dc=keycloak,dc=org

Username LDAP Attribute * ❓   uid

RDN LDAP Attribute * ❓   uid

UUID LDAP Attribute * ❓   uid

User Object Classes * ❓   top,person,organizationalPerson,inetOrgPerson

Read Timeout ❓

Pagination ❓   ☐ Off

It is recommended to retain the Synchronization and Advanced Settings as provided below:

Map Roles

To map LDAP group/user role to a relevant role in IP Maestro, follow the procedure mentioned below:

1. In the IP Maestro home page, click **System Management** > **User Management** > **User Federation**.

2. In the User Federation page, click the **Map Role(s)** button.

3. In the **Role Mapping** page that is displayed, follow the steps shown below:

    Note: If group mapper is created, the groups/roles from the LDAP server will be imported to IP Maestro as per configurations and will be available to map.

    •   In the **LDAP Synced Role/Group** drop-down menu, select the groups/roles that are needed to be mapped to IP Maestro role.

- From the **IP Maestro Role** drop-down menu, select IP Maestro role.

- After selecting the appropriate roles, the mapping details are displayed.

- Click the **Map Role(s)** button to confirm the mapping.

  The mapped roles are displayed in the **Mapped Group(s)/Role(s)** table and can be modified or deleted using the **Action** button.

After successful authentication, users from the configured provider will be granted access to IP Maestro and their roles will be assigned based on the role mappings. The user roles can also be validates under **System Management** > **User Management** > **Accounts** tab.

Note: If no mappings are done, the LDAP users are allowed to login with the default IP Maestro User role assigned to them.

Manage Preferences

The Preferences page helps you to define system-wide parameters like license repository and image repository. These global parameters are initially configured during the deployment of IP Maestro.

Note:

- The image and license repository path names can be modified to accommodate field requirements.
- The Configuration Push Parameters are defined during initial installation and cannot be modified using the portal.

Configure System Preferences

The configuration process allows you to define the location of the repository of the licenses and images for managing the system in the **Licenses** and **Image Upgrade** sections under the **Device Management** menu.

Note:

For more information on licenses and images, refer to the Edit the License Installation Progress and Upgrade New Image sections.

Procedure

1. In the IP Maestro home page, click **System Management** > **Preferences > System**.

2. Specify the URL details in the **License Repository**, and the **Image Repository** fields.

Field	Description
License Repository	Fully qualified path name used to access the licenses repository provided by the user.
Image Repository	Fully qualified path name used to access the image repository provided by the user.

3. Click **Save** to save your changes.

Configuration Push Parameters

The Configuration Push Parameters that are defined during initial installation are displayed. Note that the parameters cannot be modified here.

Field	Description
Push Configuration for LLDP	Allows IP Maestro to push the LLDP configuration.
Push Configuration for Alarms	Allows IP Maestro to enable Fault Management Services on a device.

Database Management

The Backup Database feature allows to export the backup of the entire IP Maestro database. It provides a solution to restore the Maestro network configuration in the event of hardware failure or corrupted database.

To download the backup zip file, follow the steps mentioned below:

1. In the IP Maestro home page, click **System Management** > **Preferences > System**.

2. In **Database Management** section, click the **Backup** button.

    This opens the **Database Archive File** dialog box which displays the newly backed up zip file that is ready to be downloaded.

3. Click **Submit** to download the files. The archive is generated with the date-time stamp and then downloaded into the Downloads folder.

Restoration

Restoration is a script based feature with a set of steps to be followed by an admin user with Linux privileges.

WARNING: Perform the Restore operation only when absolutely necessary.

Note: These instructions require that you essentially 'down/stop' IP Maestro for a short period of time.

1. Log in to the Maestro controller via Linux shell into the NSMO directory. You can reinstall Maestro, if necessary.

2. Copy the associated archive file (from the Downloads folder) to the local NSMO directory.

3. In the script file `postgresRestoreFromZip.sh` (located in *./bin dir*) enter the command:

    `sudo bash ./postgresRestoreFromZip.sh  <path_to_zip_file>` to repopulate the Maestro database.

The Restore script takes the archive file name as an input parameter and populates the Maestro database from its contents.

Note: While performing a restore, to prevent database locking you must ensure all docker containers are stopped except the postgres server (ipi-postgres). This is to ensure no database contention is caused by other docker containers.

Configure DHCP

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

Procedure

1. In the IP Maestro home page, click **System Management** > **Preferences > DHCP**.

2. In the DHCP tab, enter the following details:

Field	Description
• Form View • File Editor	• Displays the form view with the options mentioned below. • Displays the file editor.
Interface	The physical interface of the server on which the DHCP server needs to listen when serving DHCP requests.
DHCP Configuration	
Default Lease Time	Specifies the duration in seconds for which DHCP clients will retain the assigned IP address (e.g., default-lease-time 86400 sets the lease time for 24 hours).
Maximum Lease Time	Specifies the maximum duration in seconds for which DHCP clients can retain the assigned IP address before they must renew the lease or request a new IP address (e.g., max-lease-time 7200 sets the maximum lease time to 7200 seconds or 2 hours).
Subnet	Defines a subnet with its network address pool.

Subnet Mask (or netmask)	Specifies the subnet mask, which determines the network portion and host portion of an IP address within the subnet.
Range Start	Start IP for the IP address range within the subnet that can be assigned to DHCP clients.
Range End	End IP for the IP address range within the subnet that can be assigned to DHCP clients.
Routers	Specifies the IP address of the default gateway (router) that DHCP clients must use for internet access.
Domain Name Server	Sets the IP address of the Domain Name System (DNS) server that DHCP clients must use for domain name resolution.
License Server	Specifies the URL to obtain a valid software license file for the device.
License Folder	Specifies the URL of the software license folder to obtain a valid software license file for the device.
Image Location	Specifies the URL to obtain a valid OcNOS image to be loaded to the device.
Day Zero Configuration	Specifies the URL to obtain a valid day-0 configuration file to be applied to the device.

3. Click **Save** to save your changes.

You can click **Restart** if you want to restart the server.

Configure SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard communication protocol for e-mail transmission. In order to have email notifications enabled on IP Maestro, the SMTP server must be configured.

Procedure

To configure SMTP server, follow the steps below:

1. In the IP Maestro home page, click **System Management** > **Preferences > SMTP**.

    In the SMTP tab, enter the following details:

Field	Description
From	From address email ID
From Display Name	A user-friendly name for the 'From' address
Reply to Display Name	A user-friendly name for the 'Reply to' address
SMTP host	SMTP Mail server host IP
SMTP Port	SMTP Mail server port

2. Click the **Test Connection** button to test the SMTP connection. A pop-up message is displayed to show if the connection is successful or not. This also triggers a test mail to the e-mail address of the logged-in admin user.

3. Click **Save** to save the SMTP configuration.

This configuration is necessary for enabling e-mail alerts to users. As an admin, you can configure subscription to e-mail alerts, notifications and alarms for other users. For more details, refer the section Email Notifications.

Configure Dashboard Level Preferences

The user persistence feature in IP Maestro provides the ability to render the dashboards and other settings, based on the assigned preferences data. This feature also detects the changes to the dashboards or other preferences and these changes are persisted in the database.

The **Dashboards** tab allows you to configure dashboard level preferences for different types of roles.

Configure Preferences

As an administrator, you can assign default preferences to user accounts based on particular roles in IP Maestro as follows:

1. In the IP Maestro home page, click **System Management** > **Preferences > Dashboards**.

2. In the **Role** drop-down field, select the role for which you want to assign the preferences.

3. Select the check-boxes for the desired features you want to be displayed for each dashboard.

4. Click **Update** to save the preferences.

Note: Whenever an user account is deleted from IP Maestro, the preferences are also removed.

View IP Maestro Health

The IP Maestro Health page allows you to monitor the system health of the overall IP Maestro domain controller

The following list provides details on key features of IP Maestro Health:

Field	Description
⟳	Reloads the data in the Health tab.
⊟	Collapses (minimizes) the details. Click again to show the details.
⊗	Removes the widget from the screen.
⊳	Exports the data in PDF format.
📅 Last 12 Hours(s)	Displays data according to the date range,
⚙	Allows to display data based on the following settings: • Date range - displays data according to the specified date range. • Auto refresh - If enabled, data is refreshed at the specified time interval. • Dashboard color scheme - you can choose the color scheme for display. • Manage Widgets - you can choose widgets to be shown on the dashboard.

Prerequisites

Ensure that the configured devices (through the device registration process) are available.

Procedure

In the IP Maestro home page, navigate to **System Management** > **IP Maestro Health**

The Health dashboard is displayed with the following information:

Field	Description
Status Summary	Provides an overview of the internal IP Maestro applications as a container. It shows the container name, image specification, and its running time.
Statistics	Lists the internal IP Maestro applications as containers along with the statistics for each container. It displays the following information: • Container Name • CPU Usage • Memory Usage (%) • Memory Usage • Max Memory Used • Memory Limit • Total Disk IO • Total Net Inbound • Total Net Outbound
Memory Usage	Displays the overall Memory usage for the IP Maestro system.

Field	Description
CPU Usage	Displays the overall CPU usage for the IP Maestro system.