IP Maestro®

Version 2.1

Installation Guide

September 2024

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

Contents

Preface

This guide describes the steps for installing, configuring and logging in to IP Maestro. This preface includes the following sections:

Supported OcNOS Version

IP Maestro Release 2.1 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 2.1 release.

Document history

Date	Version	Description
January 2024	1.0	Final draft
May 2024	2.0	Final draft
September 2024	2.1	Final draft

Overview

IP Maestro streamlines element management processes, enhances visibility, and strengthens security. It features a user-friendly Graphical User Interface (GUI)-based Element Management System (EMS) that provides an intuitive display of network topology, faults, performance metrics, and inventory.

Key features include:

- **Centralized Log Repository**: The system gathers and stores logs centrally, simplifying log management and analysis.
- **Mass Device Configuration and Software Updates**: The system facilitates efficient and simultaneous configuration of multiple devices and allows for seamless software updates.
- **Role-Based User Management and Auditing Logs**: The system implements a role-based access control system for user management and maintains comprehensive auditing logs for accountability.
- **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.

Hardware and Software Requirements

Following are the software/hardware requirements to run the IP Maestro application efficiently.

Software/Hardware	Required/Version
Memory	32 GB 500GB disk space
Cores	4 CPUs
CPU Type	Support SSE 2.4 (Example: Westmere CPU Type)
Supported browsers • Google Chrome • Mozilla Firefox • Microsoft Edge • Opera • Safari • iOS • Android • Windows Mobile	 • 102.0.5005.63 (64 bit) • 99.0.1 (64 bit) • 103.0.1264.62 (64 bit) • 89.0.4447.51 • 15.5 (latest) • 9+ (or latest) • 4.4+ (or latest) • IE 11+ (or latest)
Operating System	Ubuntu 20.04.2 LTS
Docker	23.0.0 and above
Docker Compose	2.20.2 and above

Date and time on OcNOS Devices

- Ensure the OcNOS device date and time is in sync with IP Maestro and with the devices being monitored.
- Ensure the OcNOS device date and time is updated to the current date and time to get the license installed on the device.
- Execute `clock` command to set the device date and time on OcNOS.

Configure Host for IP Maestro

To prepare the host for IP Maestro deployment, you must have Docker and Docker Compose installed on it.

Docker Verification or Installation

To install or update Docker to the latest version on the deployment machine refer to Install Docker.

Prerequisites

- Ensure that Docker, Docker Compose plugin and Wget are installed.

  Note: If Wget & Unzip are not installed, install using the command `sudo apt-get install wget unzip -y`.
- Ensure that only one docker installation is running on the host.

Procedure

Ensure Docker Compose version is at least v2.20.2.

1. Install the latest version of Docker on the deployment machine. Refer to Install Docker.
2. Execute the following command to verify the docker version:

   ```
   docker version
   ```

   or

   ```
   docker -v
   ```
3. If the Docker compose version is not 2.20.2 or above, install the Docker Compose plugin. Refer to Uninstall Old Versions.

   Follow the instructions:

   - Setup Docker's apt repository (Ensure to copy and run all commands specified.)
   - Install the Docker packages.

   Note: It is recommended to add the host user to the docker group in a post-installation step.
4. Execute the `sudo usermod -aG docker $USER` command to eliminate the requirement to use `sudo` when executing docker commands and to add your user to the docker group.
5. Execute the following command to validate Docker and Docker Compose version:

   ```
   docker version
   ```

   ```
   docker compose version
   ```

To troubleshoot, refer to Remove Old Docker Installation, Remove Docker Snap Installation.

Deploy IP Maestro

If IP Maestro is currently running on your host and you want a fresh installation, you must shutdown the current deployment before installing the new version. For more information, refer to the chapter Shutdown IP Maestro.

If you want an upgrade of IP Maestro, refer to the chapter Upgrade IP Maestro.

Procedure

For a new installation, perform the following to deploy IP Maestro:

1. Login to Flexnet Operations with the user credentials.
2. Download the .zip file `IPMA-<VERSION>-<BUILD>.zip`
3. Copy the downloaded .zip file to the /home/user directory of your Linux server host, where you deploy IP Maestro.
4. Execute the following command to unpack the IP Maestro.zip file:

   ```
   unzip IPMA-<VERSION>-<BUILD>.zip
   ```
5. Execute the following command to navigate into the nsmo folder:

   ```
   cd nsmo
   ```
6. Execute the following command nsmo-init.sh script:

   ```
   ./nsmo-init.sh
   ```
7. Execute the following command to check if images are loaded:

   ```
   docker images
   ```

Example:

```
REPOSITORY                          TAG              IMAGE ID       CREATED      SIZE
nsmo-sdn                        2.0.0-263-ipma    4e40aff5c740   11 hours ago   761MB
nsmo-portal-server              2.0.0-263-ipma    72afdd578d12   11 hours ago  1.42GB
nsmo-portal-client              2.0.0-263-ipma    0c4a92dbe131   11 hours ago  1.24GB
nsmo-logstash                   2.0.0-1-ipma      e4e3f8655ba7     8 days ago  1.39GB
nsmo-proxy                      2.0.0-1-ipma      8a13baf756d7     8 days ago   398MB
nsmo-auth                       2.0.0-1-ipma      aa986f0ceac1     8 days ago   522MB
nsmo-dhcp                       latest            3561d119c5b5     6 weeks ago  218MB
nsmo-restconf-monitor           latest            a8fd5876afdc     6 weeks ago  202MB
nsmo-rabbitmq                   3.10-management   b53a052ad6ed    2 months ago  245MB
docker.elastic.co/elasticsearch 8.4.2             2f8a9577a31d   20 months ago 1.26GB
/elasticsearch
postgres                        14.4              e09e90144645   22 months ago   376MB
```

At this stage, IP Maestro is deployed with Docker images loaded into a local Docker repository.

Start IP Maestro

This section outlines the steps to initiate the IP Maestro deployment.

Prerequisites

- IP Maestro deployment is installed and Docker images loaded into the local Docker repository. Refer to the section Deploy IP Maestro.
- IP Maestro deployment requires certificates to guarantee SSL communication between Ocnos devices and IP Maestro stack (Shipping of OcNOS device logs to IP Maestro), and to expose the deployment through https protocol. The certificates should be placed/installed in the nsmo/certs folder. As part of the IP Maestro startup process, self-signed certificates will be generated and placed inside the nsmo/certs folder. This particular step will only be executed during the initial startup call.
- Signed certificates by a Trusted CA Authority, can be used in the deployment instead of self-signed ones. The certificates needs to be placed at nsmo/certs folder, and during the first start call, the user should type `false` in the following question: `Use self-signed certificate/key for Portal SSL settings.` The name of the certificate and key will be requested and checked from nsmo/certs folder.

Procedure

Perform the following to start IP Maestro:

Note: During startup, questions will be presented, and default values will be pre-set. To continue with default values, you can hit <CR>. Explanations on the options will be provided below.!! The user inputs will only be asked in the first nsmo-start.sh call.

1. Setup and start IP Maestro containers: `./nsmo_start.sh`

Note: This process creates the deployment, manages dependencies, and starts up containers (approximately 15 minutes).

2. Upon running the `nsmo_start.sh` script, user inputs are prompted. Press Enter to select defaults for most inputs.

Note: At this stage, IP Maestro is deployed and Docker image is loaded.

Here is an example of a sample run:

```
# ./nsmo-start.sh

:: Version 2.0.0 ::
[2024-05-29T15:10:43,709][INFO][host-validation] ---------- Executing Host Validation
[2024-05-29T15:10:43,744][INFO][validate-docker] Docker version: 24.0.7
[2024-05-29T15:10:43,886][INFO][validate-docker-compose] Docker Compose version: 2.23.3
[2024-05-29T15:10:43,902][WARN][validate-host-disk] Total Disk Space: 147GB
[2024-05-29T15:10:43,903][WARN][validate-host-disk] Host disk space 500GB or higher is
the minimum recommended, but found 147GB
[2024-05-29T15:10:43,904][INFO][validate-host-disk] Available Disk Space: 82GB
[2024-05-29T15:10:43,905][INFO][validate-host-disk] Used Disk Space: 42%
[2024-05-29T15:10:43,915][WARN][validate-host-memory] Total memory: 31GB
[2024-05-29T15:10:43,916][WARN][validate-host-memory] Host memory 32GB or higher is the
minimum recommended, but found 31GB


[2024-05-29T15:10:43,918][INFO][nsmo-start] ---------- Collecting Host Information
[2024-05-29T15:10:43,919][INFO][nsmo-start] Host IP:           10.12.104.22
```

```
[2024-05-29T15:10:43,920][INFO][nsmo-start] Hostname (--fqdn): QA-
22Server.ipinfusion.com


[2024-05-29T15:10:43,928][INFO][load-properties] ----------- Checking IP Maestro global
cfg
[2024-05-29T15:10:43,930][INFO][load-properties] Global cfg not present. Creating .cfg
and setting required properties

Image upgrade location []: http://10.12.104.22:8000/maestro_resources/images/
License installation path []: http://10.12.104.22:8000/maestro_resources/licenses/
push.configuration.for.LLDP <true/false> [true]: true
push.configuration.for.ALARMS <true/false> [true]: true
DHCP interface []:
OcNOS login [ocnos]: ocnos
OcNOS password [ocnos]: ocnos
OcNOS port [830]: 830


[2024-05-29T15:11:12,510][INFO][config-tls] ----------- Loading IP Maestro TLS/SSL
config
[2024-05-29T15:11:12,512][INFO][config-tls] Creating self-signed certificate/key. Files
will be available for ssl configuration

=====================================================
======== Generating IP MAESTRO Certificate(s) =======
=====================================================

Generating Certificate for host QA-22Server.ipinfusion.com and ip 10.12.104.22 ...
Using instances.yml file to create certificates...
# This file is used by elasticsearch-certutil to generate X.509 certificates
# for the Elasticsearch transport networking layer.
# see https://www.elastic.co/guide/en/elasticsearch/reference/current/certutil.html
#
# NOTE Remote connections based on IP is not a good aproach as IPs can change. DNS
should be prefered instead.
instances:
  - name: "CN=Self-Signed,C=US,ST=California,L=Santa Clara,O=IP Infusion,OU=NSMO"
    filename: "selfsigned"
    dns:
      - QA-22Server.ipinfusion.com
    ip:
      - 10.12.104.22


Unzipping Certificates...
Deleting /certs/certs.zip - If it exists...
Creating self-signed PKCS8 key for filebeat from /certs/selfsigned.key
ODL Keystore not found. Creating ODL PKCS12 keystore using self-signed cert and key...
Importing keystore /certs/selfsigned.p12 to /odl/etc/keystore/keystore.jks...
Entry for alias karaf successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or
cancelled
```

```
Applying Permissions...

=====================================================
Self-signed Certificate/Key generated successfully.
=====================================================

Use self-signed certificate/key for Portal SSL settings? [true]: no
[2024-05-29T15:11:17,719][INFO][config-tls] Use self-signed cert/key settings: no...
[2024-05-29T15:11:17,721][INFO][config-tls] Setting up external SSL certificate/key for
Portal. Files MUST be located at nsmo/certs ...
SSL Certificate Name: fullchain.pem
SSL Certificate Key Name: privkey.pem
[2024-05-29T15:11:37,138][INFO][config-tls] Verifying if certificates are present at
nsmo/certs ...
```

Execute the following command to check the status of the containers:

```
watch docker ps
```

Note: Ensure that containers that contain a health check have a `healthy` status.

Here is an example of the output:

```
*** The following is a short output to show the "healthy" STATUS expected

NAMES                   STATUS
ipi-dhcp                Up 2 hours
ipi-metricbeat          Up 2 hours
ipi-proxy               Up 2 hours (healthy)
ipi-keycloak            Up 2 hours (healthy)
ipi-portal-client       Up 2 hours (healthy)
ipi-portal-server       Up 2 hours (healthy)
ipi-odl                 Up 2 hours (healthy)
ipi-logstash            Up 2 hours (healthy)
ipi-elasticsearch       Up 2 hours (healthy)
ipi-rabbitmq            Up 2 hours (healthy)
ipi-postgresql          Up 2 hours (healthy)
ipi-restconf-monitor    Up 2 hours (healthy)
```

Log in to the IP Maestro Portal

For logging in to IP Maestro, you must ping the server as follows:

Prerequisites

- The containers are up and running.
- Login credentials.

Procedure

1. On any web browser, type the IP Maestro portal URL. For Example: https://[HOST_IP] for self-signed and https://[fqdn] for private CA certificate.
2. Enter the Username and Password.

   Note: The default username/password is admin/admin123.
3. Click **Sign In**.

   If the username and password are valid, the user is authenticated and redirected to the Portal home page.

Shutdown IP Maestro

This section describes the steps to shutdown IP Maestro.

Prerequisites

- IP Maestro must be up and running. Refer to the section Start IP Maestro for more information.

Procedure

Run the `./nsmo-shutdown.sh` script to shutdown IP Maestro services and to clean volumes/data (optional). When no option is specified, only a standard list of services will be terminated, and no volumes is removed to ensure data preservation.

Execute the following command to shutdown IP Maestro and remove containers and volumes:

```
./nsmo-shutdown.sh --all -v
```

Or

Execute the following command to stop and remove containers from the quick list:

```
./nsmo-shutdown.sh     Stop and remove containers from the quick list
./nsmo-shutdown.sh -v   Stop and remove containers from the quick list and delete volume
./nsmo-shutdown.sh --all  Stop and remove all containers
```

For more information, execute the `-help` command.

Cleanup IP Maestro Deployment

Cleaning up the IP Maestro process involves systematically shutting down of all IP Maestro components, removing associated directories, and purging any superfluous artifacts.

Prerequisites

- IP Maestro must be up and running.

Procedure

Perform the following to clean the IP Maestro:

1. Clean up all the IP Maestro created resources using the command `nsmo - shutdown.sh -- all -v` and execute the command `sudo rm -rf nsmo` to completely clean IP Maestro deployment from the host.

   Note: The `sudo rm -rf` command deletes all directories and its contents, including IP Maestro contents.

2. Execute the command `sudo docker system prune -a` to delete all Docker images from the host local repository.

Here is an example of the warning message displayed while performing the above steps:

```
WARNING! This will remove:
  - all stopped containers
  - all networks not used by at least one container
  - all images without at least one container associated to them
  - all build cache

Are you sure you want to continue? [y/N]
```

Upgrade IP Maestro

You can upgrade an existing installation of the IP Maestro Application (IPMA) without initiating a shutdown or performing a cleanup of the IP Maestro deployment.

Prerequisites

- IP Maestro must be up and running.

Procedure

Perform the following to upgrade IP Maestro:

1. Create a folder named **update** in the **nsmo** folder.
2. Place the new *.zip* file for deployment in the **nsmo/update** folder.
3. From the **nsmo** folder, run:

   ```
   unzip -o -j update/IPMA-<VERSION>-<BUILD>.zip -d . */nsmo-update.sh
   ```

4. From the **nsmo** folder, run:

   ```
   ./nsmo-update.sh -f IPMA-<VERSION>-<BUILD>.zip
   ```

The upgrade process will shutdown and remove containers from the old version, and initialize new ones using the new version loaded. Note that the previous configurations are retained.

Note: PostgreSQL and Elasticsearch databases will not be shut down in order to preserve the existing data.

Troubleshoot IP Maestro

IP Maestro Services Fail

When Maestro services are failing:

- Check Service Status: Execute the Docker commands to ensure all services are up and running:
  - `docker images` (Lists all images)
  - `docker ps` (Displays all running containers)

If any service appears inactive (life cycle phase of restart/ unhealthy/ exited), attempt to restart it by invoking the `nsmo-start.sh` script. If the service remains non-operational even after running the script again, then shut down the service and rerun `nsmo-start.sh`. This recreates the service container from scratch in an attempt to start it.

Unable to Access the Services Through the Specified Port

When you are unable to access services through specified port:

If any IP Maestro service is inaccessible through the assigned port, check the following:

- Ensure all necessary ports are open in the IP tables.
- Check for potential firewall restrictions or blocks.
- Check the logs of the service container which is failing or is unable to reach the service with docker commands:

  `docker logs -f containerid` or `docker logs -f container-name`

Remove Old Docker Installation

In case you have issues while installing Docker or getting Docker version up to the minimum requirement, uninstall all conflicting packages from the old version. Refer to Uninstall Old Versions.

Remove Docker Snap Installation

If Docker was previously installed with snap, it is recommended to remove it and have docker installation with apt only.

1. Execute the following command to check if Docker is installed with snap:

   ```
   snap list
   ```

2. If Docker is present in the snap list, execute the following command to remove:

   ```
   sudo snap remove --purge docker
   ```

Appendix

Start Options Description

This section describes the user configuration options during IP Maestro Startup:

1. Set up SSL Certificates: Select the SSL certificates model. Currently support self-signed certificates, but users also have the option to provide their own certificates from a Certificate Authority (CA). The default is set to 'true' for self-signed certificates.

   ```
   Use self-signed certificate/key for Portal SSL settings? [true]: <<<<< <CR>
   ```

   If false is provided, make sure external certificates are placed at nsmo/certs folder in advance. The startup will required the certificate and key names and check their existence at nsmo/certs folder.

   ```
   Use self-signed certificate/key for Portal SSL settings? [true]: false
   [2024-01-25T15:19:41,362][INFO][config-tls] Use self-signed cert/key settings: false...
   [2024-01-25T15:19:41,366][INFO][config-tls] Setting up external SSL certificate/key for Portal. Files MUST be located at nsmo/certs ...
   SSL Certificate Name: fullchain.pem     <<<< Type name of certificate
   SSL Certificate Key Name: privkey.key   <<<< Type name of key
   [2024-01-25T15:19:57,354][INFO][config-tls] Verifying if certificates are present at nsmo/certs ...
   ```

2. Provide local Image and License Repository: IP Maestro supports a local Image and License repository for OcNOS. Users can download images and licenses from this hosted repository, which can be located anywhere (not restricted to the IP Maestro server). The following prompts allow users to specify the repository details.

   ```
   Image upgrade location []: <<<<< <CR>
   License installation path []: <<<<< <CR>
   ```

3. Push Basic Configuration on Device Mount: When mounting devices, IP Maestro pushes basic configurations for LLDP, Beats monitoring, and enabling FMS for Alarms. Users have the option to disable any subset of these configurations. The default is to enable the push.

   ```
   push.configuration.for.ELK <true/false> [true]: <<<<< <CR>
   push.configuration.for.LLDP <true/false> [true]: <<<<< <CR>
   push.configuration.for.ALARMS <true/false> [true]: <<<<< <CR>
   ```

4. OcNOS credentials for SDN service usage and the Netconf port on the device. Default values are set.

   ```
   OcNOS login [ocnos]:      <<<<< <CR>
   OcNOS password [ocnos]:   <<<<< <CR>
   OcNOS port [830]:         <<<<< <CR>
   ```

Call Home Feature

IP Maestro supports the Call Home protocol defined in IETF RFC 8071. The Call-Home Server listens for incoming TCP connections and assumes that the other side of the connection is a device calling home through a NETCONF connection with SSH for management. The Maestro server uses port 4334 for all Call Home connections.

The following is an example which shows a configuration to enable Call Home on a device;

```
OcNOS(config)#netconf callhome
OcNOS(config)#feature netconf callhome enable
OcNOS(config)#reconnect enable
OcNOS(config)#retry-interval 20
OcNOS(config)#callhome server 10.12.104.25 10.12.104.25 port 4334
```

Configure External Databases (LDAP/AD)

In IP Maestro, you can provide users the access to external databases and directories, such as Lightweight Directory Access Protocol (LDAP) and Active Directory (AD). This is an alternate authentication service to the local user database wherein the user interface of IP Maestro utilizes the User Federation capabilities of authentication manager to integrate LDAP and AD.

This section provides a step-by-step guide on how to configure LDAP/AD provider in IP Maestro. A standard LDAP server typically contains an LDAP Data Interchange Format (LDIF) file that holds all the configurations.

The following configurations are demonstrated using the LDIF file shown below:

- 2 Groups: `ldap-admin` and `ldap-user`
- 2 Users:
  - `jbrown123` - part of '*ldap-admin*' and '*ldap-user*' groups.
  - `bwilson` - part of '*ldap-user*' group.

LDIF file

```
dn: dc=keycloak,dc=org
objectclass: dcObject
objectclass: organization
o: Keycloak
dc: Keycloak

dn: ou=People,dc=keycloak,dc=org
objectclass: top
objectclass: organizationalUnit
ou: People

dn: ou=RealmRoles,dc=keycloak,dc=org
objectclass: top
objectclass: organizationalUnit
ou: RealmRoles

dn: uid=jbrown123,ou=People,dc=keycloak,dc=org
objectclass: top
objectclass: person
objectclass: organizationalPerson
```

```
objectclass: inetOrgPerson
uid: jbrown123
cn: James
sn: Brown
mail: jbrown123@keycloak.org
postalCode: 88441
userPassword: password123

dn: uid=bwilson,ou=People,dc=keycloak,dc=org
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
uid: bwilson
cn: Bruce
sn: Wilson
mail: bwilson@keycloak.org
postalCode: 77332
street: Elm 5
userPassword: password123

dn: cn=ldap-admin,ou=RealmRoles,dc=keycloak,dc=org
objectclass: top
objectclass: groupOfNames
cn: ldap-admin
member: uid=jbrown123,ou=People,dc=keycloak,dc=org

dn: cn=ldap-user,ou=RealmRoles,dc=keycloak,dc=org
objectclass: top
objectclass: groupOfNames
cn: ldap-user
member: uid=jbrown123,ou=People,dc=keycloak,dc=org
member: uid=bwilson,ou=People,dc=keycloak,dc=org
```

For detailed information on adding and mapping providers to IP Maestro users, refer to the User Management section in *IP Maestro User Manual*.