

Magma
NMS Installation & Configuration

PUBLICATION DATE :
MARCH 2020

VERSION 1.0



NMS Guide

Network Management System

PURPOSE:

Step by step instructions on how to install, setup and configure the Magma Network Management System



Disclaimer & Confidentiality

The content of this presentation is proprietary and confidential information of Facebook, Inc. It is not intended to be distributed to any third party without the written consent of Facebook, Inc.

This presentation is provided for informational purposes only and constitutes Facebook's confidential information, subject to the non-disclosure agreement and/or confidentiality terms in place between your company and Facebook. This presentation (and any information from it) may only be used for your company's internal purposes in connection with work on Magma and cannot be shared with any unauthorized third party. Facebook has made efforts to ensure that this course is accurate and does not make any representation or warranty regarding accuracy or completeness. Facebook reserves the right to update and otherwise modify the information included in this presentation without notice. If you find information that is incorrect or incomplete, we would appreciate your comments and suggestions.

Table of Contents

Network Management System (NMS)

1. Introduction	4
Purpose	
Scope & Audience	
Resources	
2. NMS Prerequisites & Hardware Recommendations	5
3. NMS Setup	6
Runnng NMS Setup 1	
Runnng NMS Setup 2	
Running the NMS	
4. Map	8
5. Metrics	9
Viewing Network Status & Health	
6. Alerts	10
How to Create an Alert Rule	
7. Subscribers.....	11
Viewing Subscribers List	
Adding Subscribers	
Adding Subscribers from a File Upload	
8. Gateways	13
Adding a Gateway (AGW)	
Editing a Gateway (AGW)	
Verrifying Gateway Configuration	
9. eNodeB Devices.....	16
To Add an eNodeB	
10. Configure	17
Data Plans	
Adding a Data Plan	
Editing a Data Plan	
Removing a Data Plan	
Network Configuration	
Upgrades	
Policies	
To Add and a Base Name	
11. Administrative Tools	22
Adding NMS Administrators	
Removing Admins	

1. Introduction

The Network Management System (**NMS**) is the UI for managing, configuring, viewing health status and monitoring networks.

At a high level, Magma is comprised of a set of Access Gateways (AGW) or LTE base stations managed by a centralized controller called the Orchestrator. The Network Management System (NMS) receives network metrics via RESTful API's.

Magma is an open source platform for building access networks (LTE, 2G, Wifi, etc.). Magma gives network operators an open, flexible and extendable mobile core network solution. It's a distributed core and extends mobile data services and wireless access networks. Magma provides network services as pluggable modules for building such networks. Network services in this context can be authentication, metering, subscriber management, IP allocation, mobile edge computing services, etc.

Purpose

The purpose of this document is to provide step by step instructions on how to install, setup and configure the Magma Network Management System (NMS) onto a Linux server environment.

- High level architecture diagram
- Prerequisites for NMS Installation
- Explanation of the Key Components
- Configuration of Devices

Scope & Audience

Scope of this document is limited to describe Magma's NMS installation and device configuration process. This document is intended for Magma Business Partners, Mobile Network Operators, System Integrators, Mobile Network Engineers and or anyone wanting to deploy a Magma Fixed Wireless Access (FWA) network.

Resources

- [Introduction to Magma](#)
- [GitHub Open Source Code](#)

2. NMS Prerequisites & Hardware Recommendations

Magma Network Management System (NMS) prerequisites and recommended hardware is as follows:

- An installed and running Magma Network; Orchestrator, eNodeB, AGW
Once the NMS is up and running, adding, configuring and monitoring of eNodeB's and AGW's is enabled.
- Install Docker <https://docs.docker.com/install/>
Docker compose is used to run the Magma container and configure application services
- Add xplat to hg sparse profiles (tools/scm/sparse/xplat/base)
- The NMS and the E2E must be IP reachable from each other.
- The NMS must be IP reachable from each of the nodes.
- The NMS must be capable of being deployed as a private cloud solution within an ISP network.



3. NMS Setup

To setup access to the Magma NMS, enter the following commands in a Terminal window on your laptop. Firefox or Chrome is recommended. Unlike the GitHub repo where the NMS is located in the `magma` directory, internally the Magma NMS lives in `fbsource/xplat/fbc/fbcnms-projects/magmalte`



Runnng NMS Setup 1

```
git clone git@github.com:facebookexternal/magma.git
cd magma/nms/fbcnms-projects/magmalte/
docker-compose build magmalte
docker-compose up
docker-compose exec magmalte yarn run setAdminPassword
testuser@mydomain.com password1234
```

Runnng NMS Setup 2

1. Run `setup_nms.sh` within `magma/fb/cloud`. This will automatically set up the `.env` file for `magmalte` using `magma` certs.

```
$ cd ~/fbsource/fbcode/magma/fb/cloud
$ ./setup_nms.sh
```

2. If your `magma` or `magmalte` directories live somewhere else other than `~/fbsource/fbcode/magma` and `~/fbsource/xplat/fbc/fbcnms-projects/magmalte`, you can run `setup_nms.sh` with flags `-m` and `-n` respectively to specify different directories.

Running the NMS

In the `magmalte` directory, start docker containers and create a test user:

```
$ cd ~/fbsource/xplat/fbc/fbcnms-projects/magmalte
$ docker-compose build magmalte
$ docker-compose up -d
$ ./scripts/dev_setup.sh
```

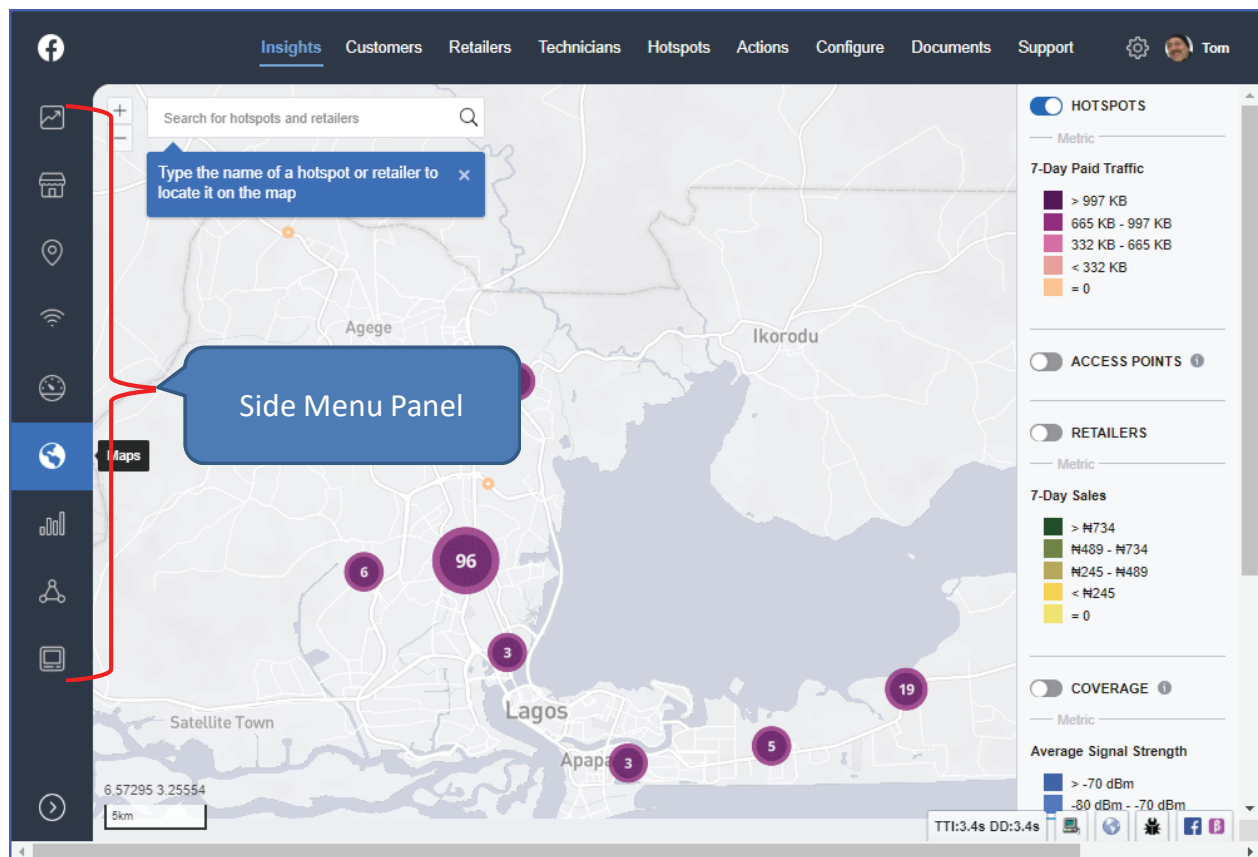
You may get an error if you run `dev_setup.sh` immediately after `docker-compose up -d`. To resolve this, wait a bit before running the script to let migrations run.

Once you have started the docker containers and created a test user, go to <https://localhost> and login with test credentials `admin@magma.test` and `password1234`.

Note: if you want to name a user other than `admin@magma.test`, you can run `setAdminPassword`, like so:
`$ docker-compose run magmalte yarn run setAdminPassword admin@magma.test password1234`

The Magma NMS opens to the Maps screen. The left side menu panel provides tabs to the following management and configuration pages:

- Map
- Metrics
- Alerts
- Subscribers
- Gateways
- eNodeB Devices
- Configure

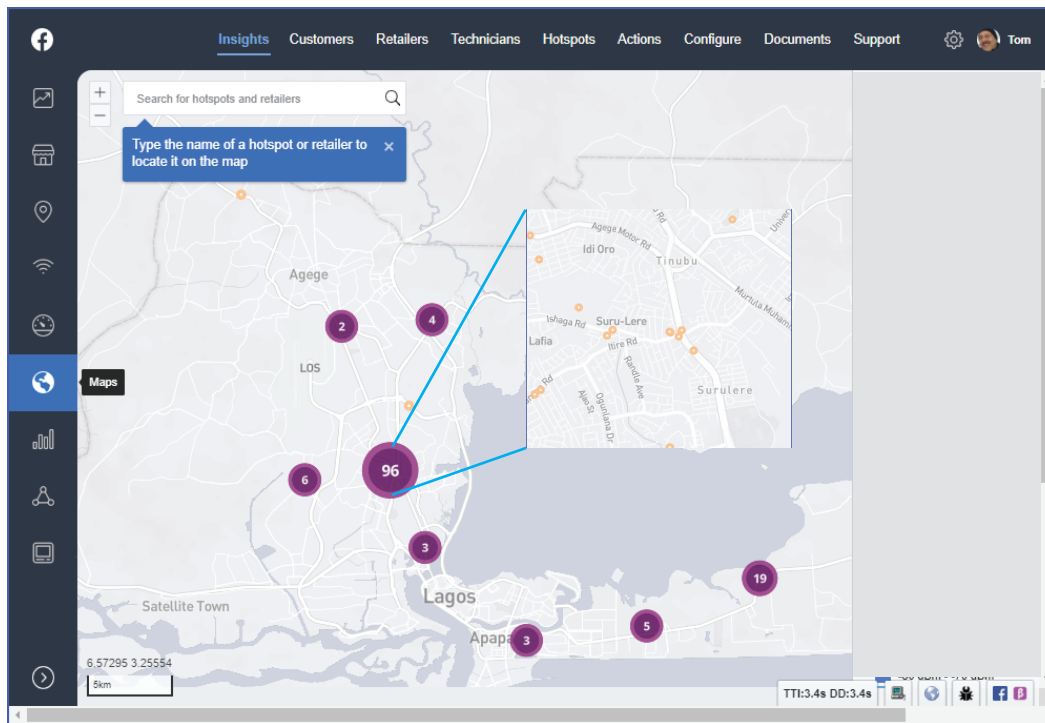


resource: <https://our.internmc.facebook.com/intern/wiki/MagmaGuide/setup-magmalte-nms/>

4. Map

The Map page displays a map of the Magma network with all active devices shown at their specific GPS location. Devices include; Access Gateways and eNodeB's. The NMS captures the End-to-End (E2E) controller input file for the Global Positioning Satellite (GPS) coordinate information of the radios and leverages [OpenStreetMap](#) to show the locations of the radio nodes.

1. With the map zoomed out, circles indicate AGW loactions and the number within that area.
2. Zoom in for more location detail



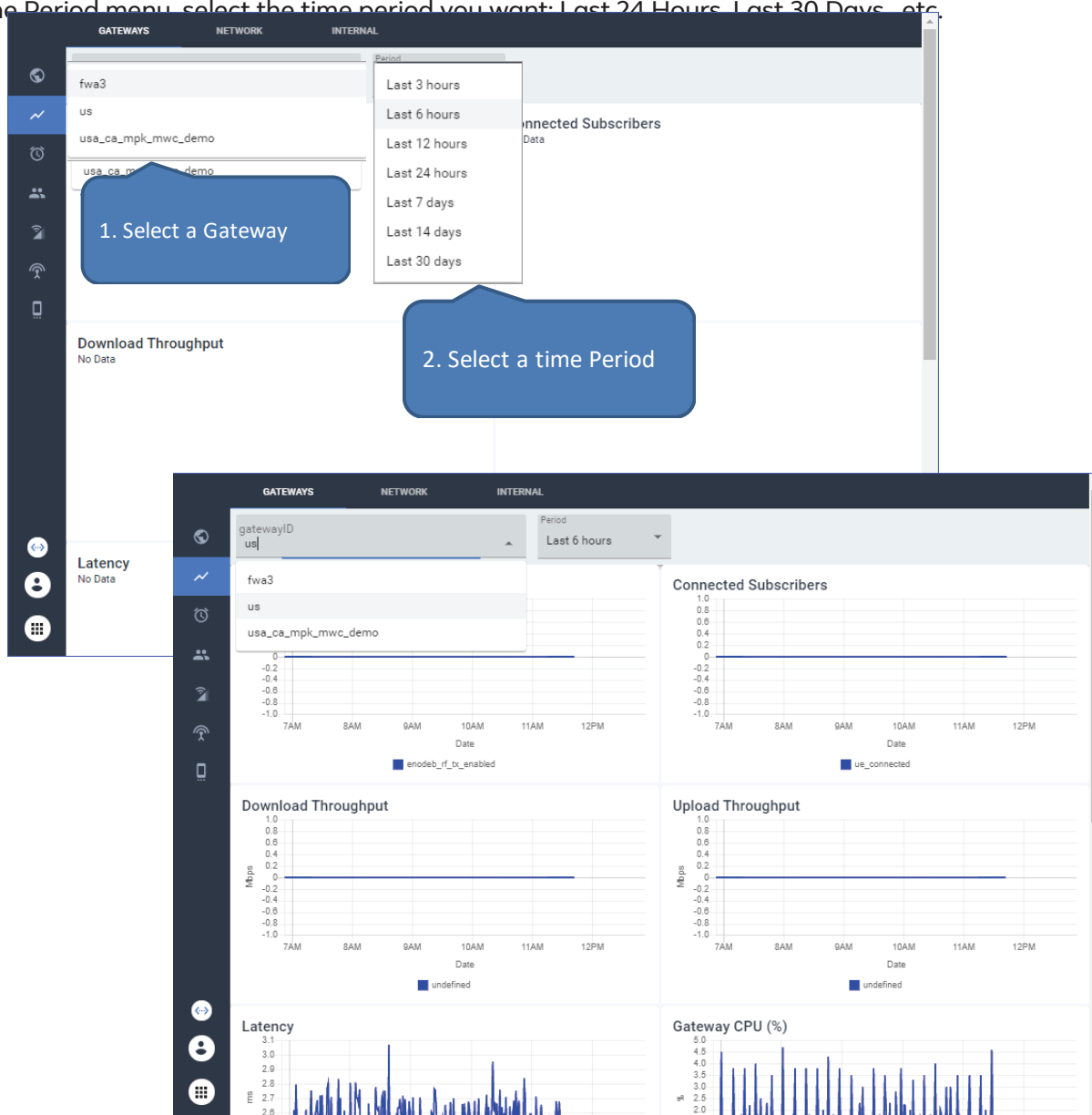
5. Metrics

The Metrics page shows information about the Magma Gateways, this includes:

- eNodeB Status
- Connected Subscribers
- Download & Upload Throughput
- Latency
- Gateway CPU (%)
- Temperature (°C)
- Disk (%)
- s6a Auth Access & Failure

Viewing Network Status & Health

1. From the Device menu, select GATEWAYS to view status of a specific AGW
2. From the Period menu, select the time period you want: Last 24 Hours, Last 30 Days, etc.



6. Alerts

The Alerts Page allows the Magma NMS Administrator or Mobile Network Operator to create and establish alerts or events. Alerts help Operators respond to degraded network conditions faster and improve overall service availability as well as network availability.

A selection of Events can be set by the Operator to trigger an Alert or Alarm. An Alert is set by the Operator for its level of severity (Warning, Alarm, and Critical), which may lead to an automatic email/message sent to the Operator.

How to Create an Alert Rule

1. Begin from the Alerts Page
2. From the top tab bar, select **ALERT RULES**
3. In the lower left of screen, click the **blue plus sign (+)**
4. Complete the required information
 - a. Enter a **Rule Name** (example: Service Down)
 - b. Create an **Advanced Expression** (optional)
*Switch the toggle on to write an arbitrary alerting expression in PromQL.
 To learn more about how to write alert expressions, click on the help icon to open the prometheus querying basics guide.*
 - c. Create a built-in **Expression** (example: backhaul latency is greater than .5 seconds)
 Select an IF Metric Name, select an Expression and an expected result
 - d. Create a **Filter**
 Select a Label (gateway or service), select a Value (the network name)
 - e. Select a **Severity** (CRITICAL, MAJOR, MINOR, WARNING, INFO, NOTICE)
 - f. Select a **Duration** and **Unit** (seconds, minutes, hours)
 - g. Enter a **Description** and click **Add**

The screenshot shows the 'ALERT RULES' configuration page. The top navigation bar has 'ALERTS' and 'ALERT RULES' tabs. The left sidebar contains various navigation icons. The main content area is a form for creating an alert rule. It includes a 'Rule Name' field, an 'Advanced Expression' toggle with a help icon, an 'IF Metric Name' dropdown, an 'IS' operator dropdown, and a value input field. There is an 'Add Filter' button. Below these are 'Severity', 'Duration', and 'Unit' fields, followed by a 'Description' field. At the bottom are 'Close' and 'Add' buttons. Red callout numbers 1, 2, and 3 highlight the sidebar, the 'ALERT RULES' tab, and the bottom right plus icon respectively.

7. Subscribers

The Subscribers Page allows the following functions:

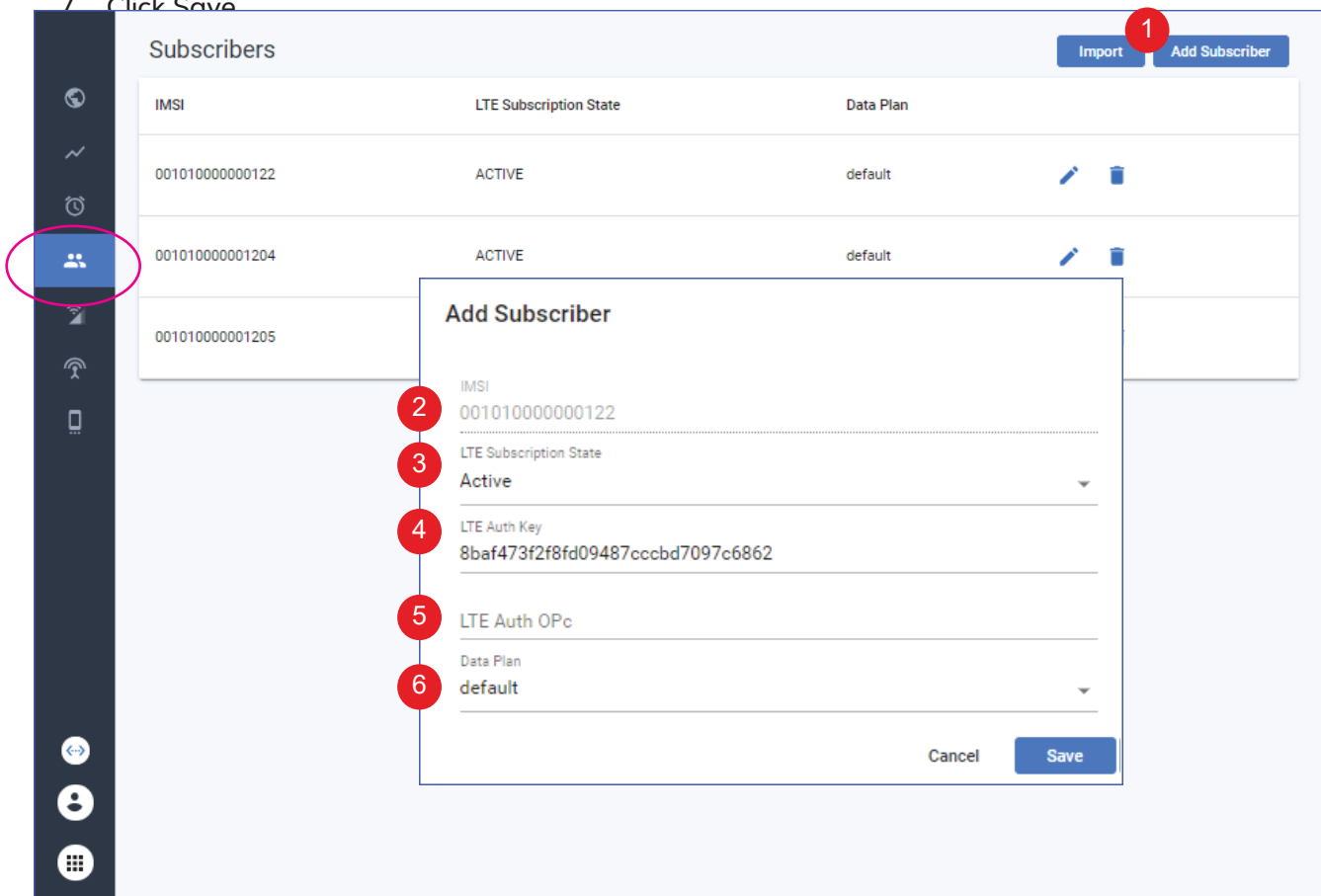
- View all system Subscribers (Users)
- Add & Delete Subscribers
- Upload Subscriber File

Viewing Subscribers List

1. From the side menu panel, click the Subscribers icon to view the System list.

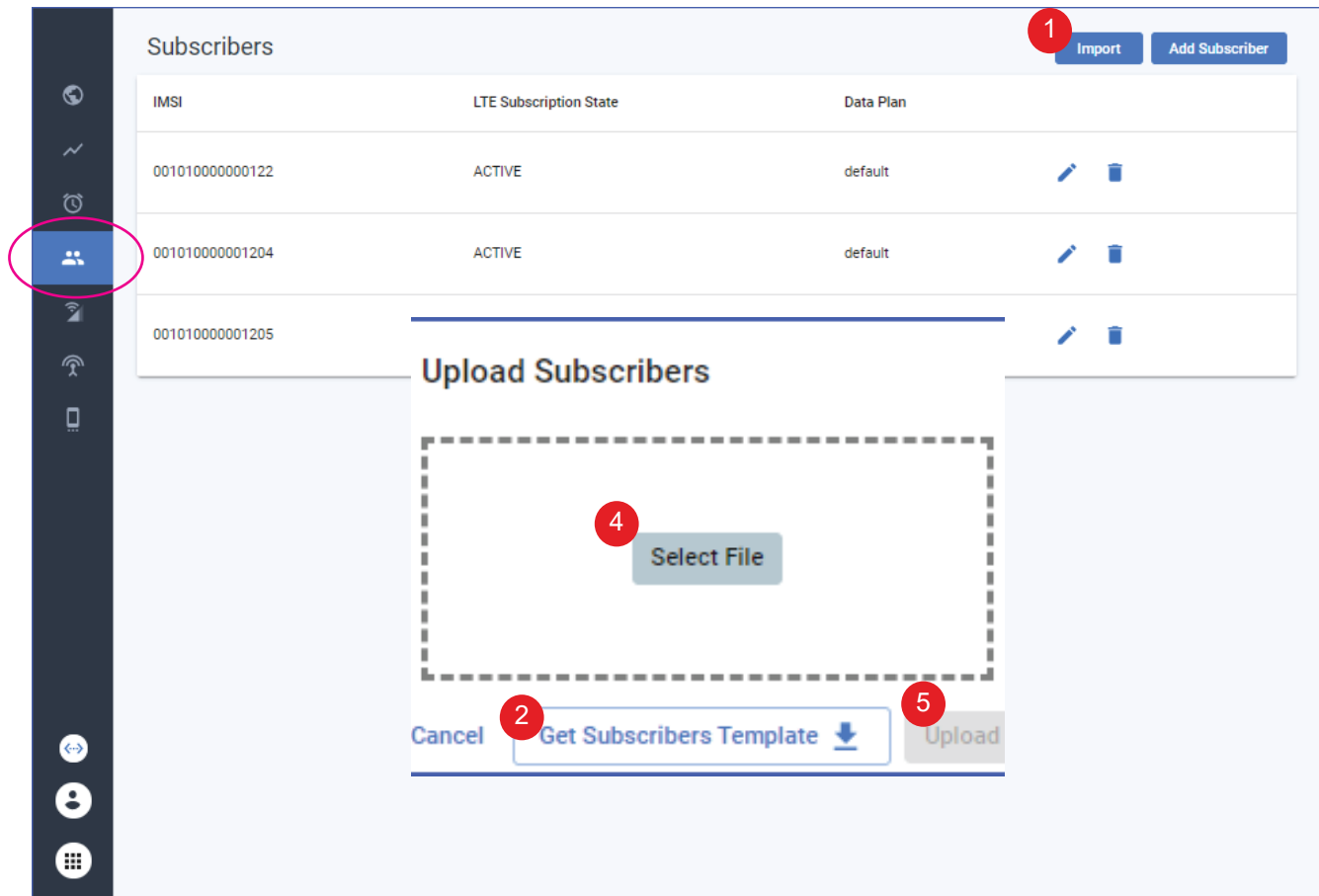
Adding Subscribers

1. From the Subscribers page, click [Add Subscriber](#)
2. Enter an IMSI, the International Mobile Subscriber Identity (IMSI) ID number
3. Enter the LTE Subscription State, select Active.
4. Enter the LTE Auth Key, the LTE Authentication key.
5. For LTE Auth OPc, select LTE Auth OPc. If OP is used instead of OPc, this field should be left blank, OP is set in Network Configurations.
6. Select a Data Plan, or select default.
7. Click Save



Adding Subscribers from a File Upload

1. From the Subscribers page, click [Import](#)
2. Click on [Get Subscribers Template](#) to download the sample CSV file of the expected layout to upload
3. Enter Subscribers into the CSV file in the format shown
4. Save the file and click [Select File](#) to upload
5. Click Upload



	A	B	C	D	E	F	G
1	imsi	lte_state	lte_auth_key	lte_auth_opc	sub_profile		
2	"200056789012345"	ACTIVE	20000000001234567890ABCDEFABCDEF	21111111111234567890ABCDEFABCDEF	low rate 1		
3	"200056789012346"	INACTIVE	20000000001234567890ABCDEFABCDEF	21111111111234567890ABCDEFABCDEF	default		
4							
5							
6							
7							
8							

8. Gateways

The Gateways Page allows the following functions:

- Add Access Gateways (AGW)
- Configure
- Sit gateways.

From the side menu panel, select the Gateways icon. The Configure Gateways page appears.

Adding a Gateway (AGW)



Prerequisites:

The Hardware ID and the Public Key from the gateway are required. To obtain the ID and Key open a Terminal window and run: `show_gateway_info.py`

1. From the Gateways page, click [Add Gateway](#). The Add Gateway screen appears.
2. Complete the required information:
Enter a **Gateway Name**, a meaningful name that describes the gateway.
 - Enter a **Gateway Description**
 - Enter a **Hardware UUID**, the Hardware ID for your gateway.
Use the Hardware ID you received using `show_gateway_info.py`
 - Enter the **Gateway ID**, the gateway ID you want. Choose a meaningful name, such as country, organization, location, or site number.
 - Enter a **Challenge Key**, the gateway Public Key.
Use the Public Key you received using `show_gateway_info.py`
3. Verify that the new AGW appears on the Configure Gateways page.

The screenshot shows the 'Configure Gateways' interface. On the left is a sidebar with navigation icons. The main area has a table with columns 'Name' and 'Hardware UUID'. The table contains several rows, some with 'N/A' and others with specific gateway names like 'fwa3', 'fwalkia1', and 'mwc_demo'. In the top right corner, there is a blue button labeled 'Add Gateway'. A red circle with the number '1' points to this button. An 'Add Gateway' modal is open in the center, with a red circle and the number '2' pointing to it. The modal has input fields for 'Gateway Name', 'Gateway Description', 'Hardware UUID', 'Gateway ID', 'Challenge Key', and a dropdown for 'Upgrade Tier'. At the bottom of the modal are 'Cancel' and 'Save' buttons. A red line connects the 'Add Gateway' button to the modal.

Editing a Gateway (AGW)

To Edit, Change or Update an Access Gateways settings, use the following steps.

1. From Gateways Page, click the Edit icon to open the configuration dialog.
2. Select the LTE tab
3. Under EPC Configs:
 - Set NAT enabled to Enabled
 - Set IP Block to the IP address and mask you want, for example: 192.168.128.0/24

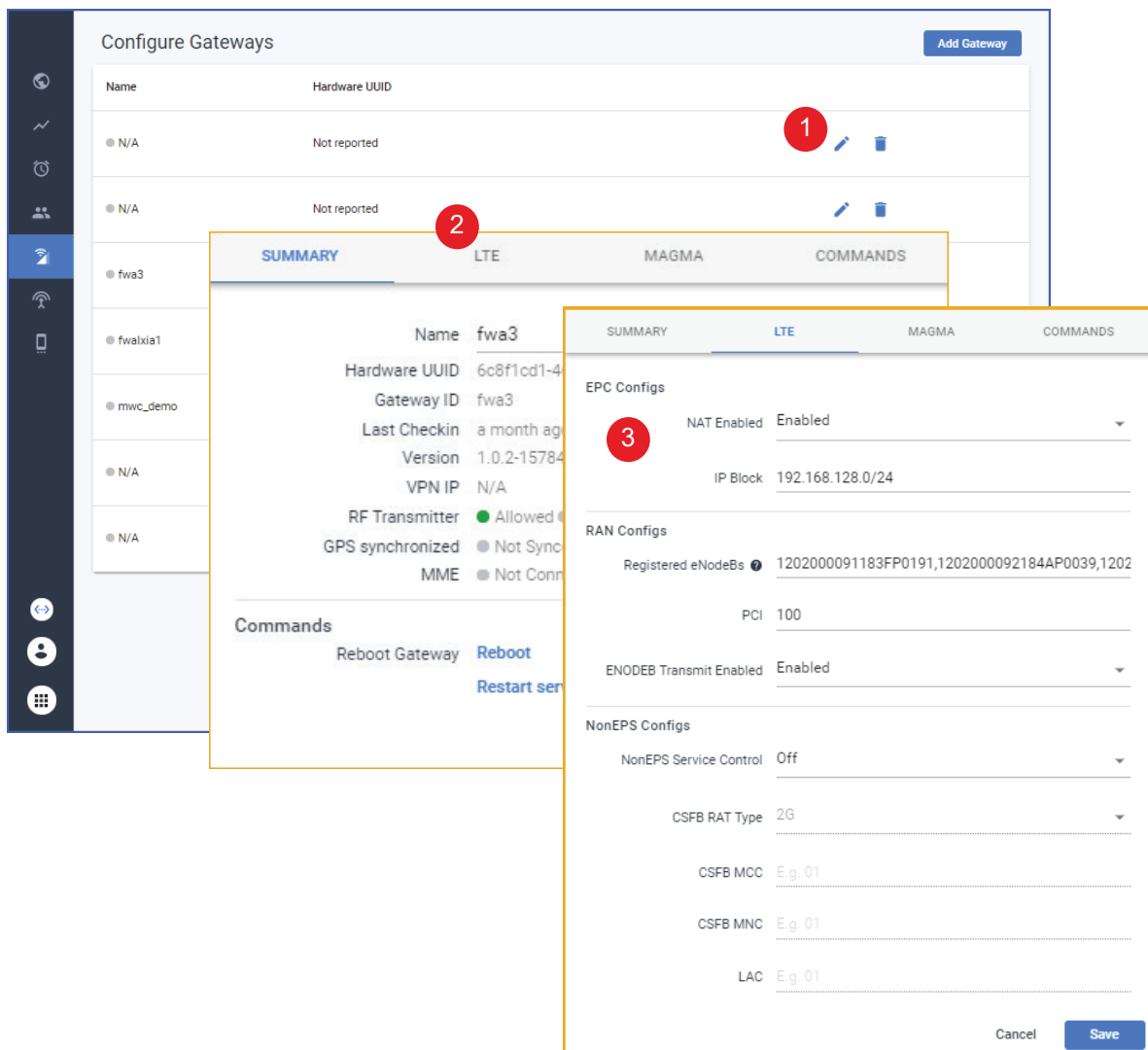
Under RAN Configs:

- Set PCI to 260.
- Set Enodeb Transmit Enabled to Enabled.

Under NonEPS Configs:

- Set NonEPS Service Control to Off

4. Click [Save](#)



Verrifying Gateway Configuration

To verify a Gateway Configuration and CheckIn.

1. Click the Summary tab.
2. Verify the AGW checks in to Orchestrator
Verify the **Last Checkin** time was in the last few minutes
Note: This may take up to 10 minutes to update.
3. If the AGW does not check in to Orchestrator

Run `checkin_cli.py` on the gateway to debug
4. Click on the Magma tab
Verify that the Autoupgrade fields and the Checkin fields are set as you want them.

1 SUMMARY LTE MAGMA COMMANDS

Name	N/A
Hardware UUID	Not reported
Gateway ID	
Last Checkin	Invalid date
Version	Not Reported
VPN IP	Not Reported
RF Transmitter	<input checked="" type="radio"/> Not Allowed <input type="radio"/> Not Connected
GPS synchronized	<input type="radio"/> Not Synced
MME	<input type="radio"/> Not Connected

2

Commands

Reboot Gateway [Reboot](#)

[Restart services](#)

Cancel [Save](#)

SUMMARY LTE **3** MAGMA COMMANDS

Autoupgrade Enabled

Enabled

Autoupgrade Poll Interval (seconds)

300

Checkin Interval (seconds)

60

Checkin Timeout (seconds)

10

Cancel [Save](#)

9. eNodeB Devices

The Magma system is comprised of AGW's connecting to eNodeB's. The NMS can monitor the eNodeB's when they are registered by adding to the NMS.

Adding an eNodeB

1. From the eNodeB Devices page, click on [Add eNodeB](#)
2. Enter a **eNodeB Name**: a unique name
3. Enter the **eNodeB Serial ID** or Serial Number - a unique number
4. Select the **eNodeB DL/UL Bandwidth (MHz)**
A list of tested and Magma proven eNodeB's appears
5. Enter the **EARFCNDL** (E-UTRA Absolute Radio Frequency Channel Number Down Link)
The range is 0 to 65535
6. Enter the **Subframe Assignment** - The range is 0 to 6
7. Enter the **Special Subframe Pattern** - The range is 0 to 9
8. Enter the **Physical Cell Identifier** - The range is 0 to 504
9. Select the **eNodeB DL/UL Bandwidth (MHz)** - The range is 3, 5, 10, 15, or 20
10. Enter the **Tracking Area Code** - The range is 0 to 65535
11. Enter the **eNodeB ID** - a unique number
12. The **Cell Number** is displayed, a numerical counter
13. Select **Transmit Enabled** if the device is configured, tested and prepared to make active.

Baicells Nova-233 G2 OD FDD

Baicells Nova-243 OD TDD

Baicells ID TDD/FDD

NuRAN Cavium OC-LTE

The screenshot displays the 'Configure eNodeB Devices' interface. It features a table with columns for 'Serial ID' and 'Device Class'. The table lists five eNodeB devices, all of which are 'Baicells ID TDD/FDD'. To the right of the table is an 'Add eNodeB' button. Below the table, a modal form titled 'Add eNodeB' is open, showing fields for: eNodeB Name, eNodeB Serial ID, eNodeB DL/UL Bandwidth (MHz) (set to Baicells ID TDD/FDD), EARFCNDL, Subframe Assignment, Special Subframe Pattern, Physical Cell Identifier, eNodeB DL/UL Bandwidth (MHz) (set to 20), Tracking Area Code, eNodeB ID (set to 0), Cell Number (set to 1), and a 'Transmit Enabled' checkbox. The modal has 'Cancel' and 'Save' buttons at the bottom right.

Serial ID	Device Class
1202000091183FP0191	Baicells ID TDD/FDD
1202000092184AP0039	Baicells ID TDD/FDD
120200010717CJP0063	Baicells ID TDD/FDD
120200020718CJP0003	Baicells ID TDD/FDD
120200020718CJP0007	Baicells ID TDD/FDD

10. Configure

The Configure Page allow for setting up and managing Data Plans, Speeds, Policies, Upgrades and more. It consists of four tabs:

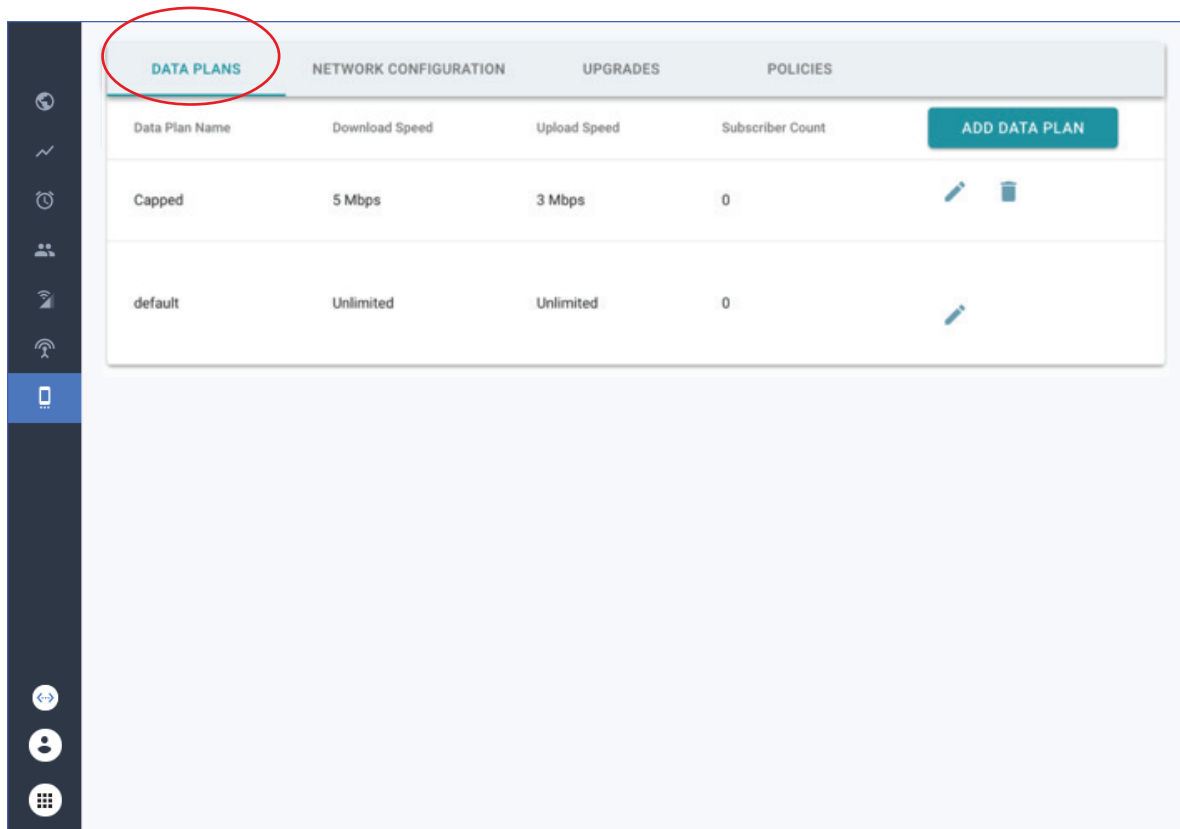
- Data Plans
- Network Configuration
- Updates
- Policies

From the side menu panel, select the Configure icon. The Configure Page appears.

Data Plans

A Data Plan is used to specify the rate limits for download and upload data transfers for subscribers.

- Users with administration level privileges can create and modify Data Plans, and can assign Subscribers to existing data plans.
- The Download Limit (Mbps) and the Upload Limit (Mbps) fields specify the maximum data transfer rates for the Subscriber that is assigned to the Data Plan.

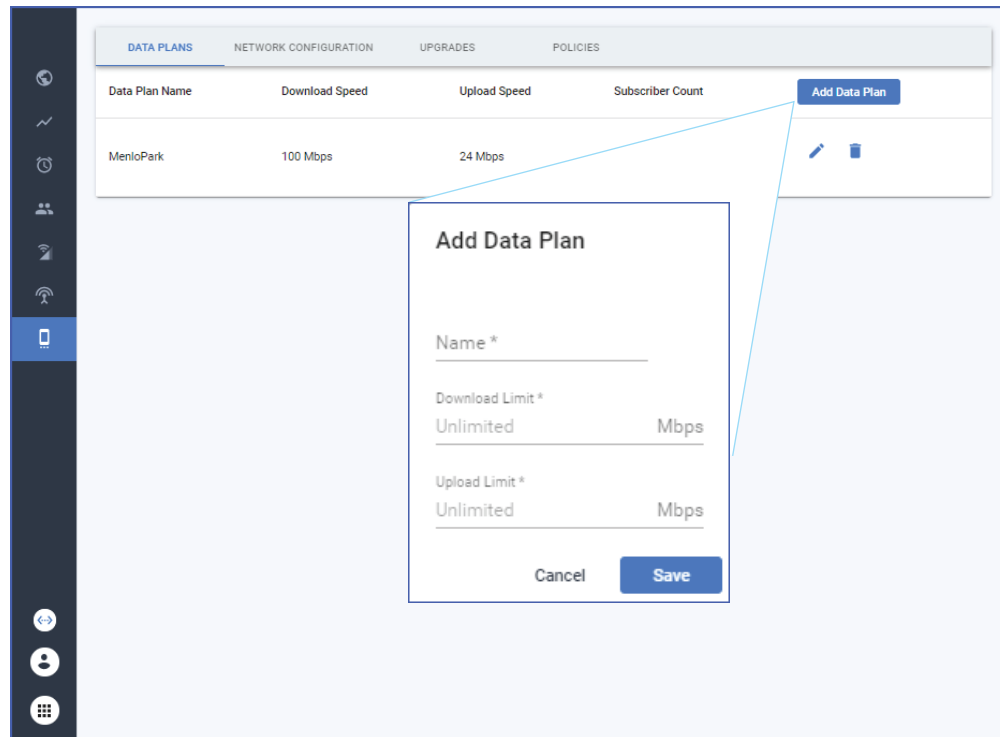


DATA PLANS	NETWORK CONFIGURATION	UPGRADES	POLICIES
Data Plan Name	Download Speed	Upload Speed	Subscriber Count
Capped	5 Mbps	3 Mbps	0
default	Unlimited	Unlimited	0

Adding a Data Plan

To Add a Data Plan:

1. From the Data Plan page, click **Add Data Plan**. The Add Data Plan screen appears.
2. Enter a Name, the name you want for the Data Plan.
3. Enter a Download Limit, the maximum transfer rate (in Mbps) for downloads that you want a UE to have under this plan. Zero (0) equals unlimited.
4. Enter an Upload Limit, the maximum transfer rate (in Mbps) for uploads that you want a UE to have under this plan. Zero (0) equals unlimited.



Editing a Data Plan

To Edit a Data Plan:

1. On the Data Plan page, click the edit icon for the Data Plan you want to edit.
2. Enter the new values that you want.

Removing a Data Plan

To Remove a Data Plan:

1. Click the trash icon for the Data Plan you want to delete.

Network Configuration

The Network Configure Page, allows for configuring the network settings for a Magma network.

To configure a network, proceed as follows:

1. Enter the MCC, the Mobile Country Code (MCC)for the network
Enter the MNC, the Mobile Network Code (MNC) for the network

To view a complete list of MCC and MNC go to <https://www.mcc-mnc.com/>

2. Enter the TAC (Tracking Area Code) for the network
3. Enter the Auth OP (Authentication Operation Code)
4. Select the bandwidth MHz block you want
The range is 3Mhz - 20Mhz
5. Select the Band Selection
Choose TDD (Time Division Duplex) or FDD (Frequency Division Duplex)
6. Enter the EARFCNDL (E-UTRA Absolute Radio Frequency Channel Number Down Link)
The range is 0 to 65535
7. Enter a Special Subframe Pattern
The range is 0 - 9
8. Enter the Subframe Assignment
The range is 0 - 6

The screenshot displays the 'Network Configuration' page within the Magma Network Management interface. The 'NETWORK CONFIGURATION' tab is highlighted with a red circle. The form contains the following fields and values:

Field	Value
MCC *	001
MNC *	01
TAC *	1
Auth OP	[Dotted line with eye icon]
Bandwidth (Mhz)	20
Band Selection	TDD
EARFCNDL *	44590
Special Subframe Pattern *	7
Subframe Assignment *	2

A 'Save' button is located at the bottom of the form. The URL at the bottom of the page is https://nms.fb magma.ninja/nms/pelican_agw/configure/network.

Upgrades

The Gateway Upgrade Status page displays information about currently supported releases and upgrade tiers. Upgrade tiers allows Mobile Operators, System Integrators and Wireless Internet Service Providers to offer different levels of service to customers.

To Add a new Tier:

1. Click the Add Tier button
2. Enter a Tier ID; numbers, letters or any combination
3. Enter a Tier Name; any descriptive title
4. Enter a Tier Version; example 1.0.0

To Assign a Tier to a network:

1. From the Tier ID dropdown, select the Tier ID you want for that gateway.

The screenshot displays the 'Gateway Upgrade Status' page in the Magma Network Management interface. The page has a sidebar with navigation icons and a top navigation bar with tabs for DATA PLANS, NETWORK CONFIGURATION, UPGRADES (selected), and POLICIES. The main content area shows a table of gateways with columns: Name, Hardware UUID, Tier ID, and Current Version. The table lists three gateways: fwa3, fwatxia1, and mwc_demo, all currently assigned 'Default Tier'. Below the table, there is a section for 'Current Supported Versions' and 'Upgrade Tiers'. An 'Add Upgrade Tier' modal is open, showing fields for Tier ID *, Tier Name *, and Tier Version *, with 'Add Tier' and 'Save' buttons.

Name	Hardware UUID	Tier ID	Current Version
fwa3	6c8f1cd1-46bf-4b2f-891b-b5693f1fd317	Default Tier	1.0.2-1578404680-fd918f7b
fwatxia1	bac13735-d318-46da-acbf-d2b6f4dfea9e	Default Tier	1.0.1-1580860031-33a94e98
mwc_demo	34da8b85-959f-4d03-85b0-667eaac1dfb6	Default Tier	1.0.1-1580860031-33a94e98

Tier ID	Tier Name	Software Version
default	Default Tier	0.0.0-0

Policies

The Policies Page lets you add and define network flow policies for the gateway.

To Add and Configure new Policy:

1. Click [Add Rule](#). The Add Rule screen appears.
2. Enter an ID for the rule.
3. Set the **Precedence** (priority) for the rule.
4. Enter the **Monitoring Key**
5. Enter the **Tracking Type**
Select Only OCS, Only PCRF, OCS and PCRF or No Tracking
6. Click the plus sign to the right of **Flows**
7. Click the dropdown for Flow 1 and select parameters:
Action: select Permit or Deny
Direction: select Uplink or Downlink.
8. Select a Protocol; IP, UDP, TCP, or ICMP.
9. Enter the IPv4 Source and IPv4 Destination addresses.
10. Click **SAVE**.

The screenshot shows the 'Policies' tab in the Magma Network Management interface. A modal window titled 'Add Rule' is open, allowing configuration of a new policy rule. The modal includes fields for 'ID *', 'Precedence *' (set to 1), 'Monitoring Key *', and 'Tracking Type' (set to 'No Tracking'). Below these is a 'Flows' section with a plus icon to add more flows. 'Flow 1' is configured with 'Action' set to 'Deny', 'Direction' set to 'Uplink', and 'Protocol' set to 'IP'. There are also input fields for 'IPv4 Source' and 'IPv4 Destination'. The modal has 'Cancel' and 'Save' buttons at the bottom.

To Add and a Base Name

1. Click [Add Base Name](#).
2. Enter a **Base Name**
3. Enter a **Rules Name** commas separated file (.csv)

The screenshot shows the 'Add Base Name' modal. It contains two input fields: 'Base Name *' and 'Rule Names (CSV) *'. At the bottom, there are 'Cancel' and 'Save' buttons.

11. Administrative Tools

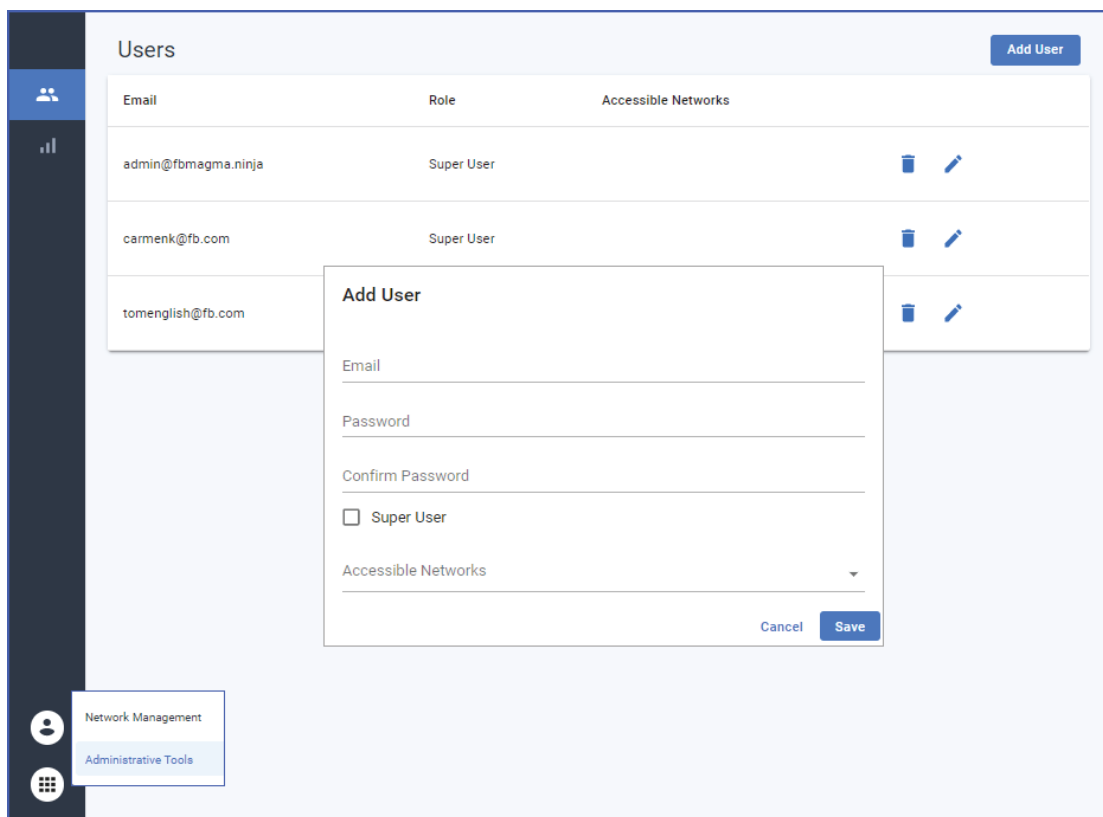
To enter Administrative tools or to switch back to the NMS, click the tools icon in the lower left side menu panel. Select Administrative Tools or Network Management.

Adding NMS Administrators

1. Click [Add User](#). The Add User screen appears.
2. Enter the Users Email address.
3. Enter a Password for the User.
4. Select **Super User** if the user is to have full control of the system.
Super Users have access to all networks by default
5. Select **Accessible Networks** and choose the network accessible to the User.

Removing Admins

1. Click the [Trash Can](#) to remove a User.





FACEBOOK CONNECTIVITY