New Rock Technologies, Inc.

Unified Management System
User Guide

Document Version: 2025-04

Release Date：2025-04-02

Amendment Records

Documentation Version 02 (Feb,2025)

Updated supported device models and new features based on UMS Version 1.1.112.

Document Rev. 01 (June, 2018)

Applied to UMS V1.1.2.

Copyright © 2025 New Rock Technologies, Inc. All Rights Reserved.

All or part of this document may not be excerpted, reproduced and transmitted in any form or by any means without prior written permission from the company.

Contents

1 Overview 3
1.1 Key features 3
1.2 Manageable device models 3
1.3 Typical application scenario 4
2 Install UMS server 5
2.1 Environment requirements for installation 5
2.2 Installation process 5
2.3 Manage UMS service and upgrade UMS 6
2.4 Replacement of UMS certificate 6
2.5 Cloud account 6
2.6 Security settings 7
3 Log in to UMS 8
4 Manage devices 9
4.1 Create domains and device groups 9
4.2 Add devices 10
4.3 Device list and device status 21
5 Configure devices 23
5.1 Parameters and templates 24
5.2 Back up parameters 29
5.3 Provision parameters 32
5.4 Back up configuration package 34
5.5 Provision configuration packages 36
5.6 Configuration management 37
5.7 Number resource 38
6 Upgrade devices 40
6.1 Manage upgrade packages 40
6.2 Upgrade manually 43
6.3 Upgrade automatically 45
6.4 View upgrade history 48
7 Logs of devices 49
7.1 Download logs of a single device 49
7.2 Download logs of multiple devices 50

 Copyright © New Rock Technologies, Inc

8 Monitor device alarms 52
8.1 Alarms 52
8.2 Monitor 56
8.3 Events 58
8.4 Monitoring group 58
8.5 Monitor website 59
9 Roles and privileges 60
9.1 Create administrators 60
9.2 Create users 61
9.3 User security settings 62
10 System settings 64
10.1 View system information 64
10.2 Upgrade 64
10.3 Maintenance 66

 Copyright © New Rock Technologies, Inc

1 Overview

Unified Management System (UMS), developed by New Rock Technology, Inc., is used to manage and control New Rock OM series IP-PBX and MX series voice gateway devices remotely. By using UMS, you can now seamlessly manage a large number of devices, obtain real-time devices' status information, configure or upgrade devices in batch to improve the management efficiency and reducing support costs.

1.1 Key features

- Browser-based access to the Web GUI, no need to install a client software
- Remote configuration and management for devices in batch
- Auto provisioning configuration packages to devices
- Automatically back up parameters, configurations, and log files for devices
- Upgrade devices easily: upgrade manually, upgrade automatically, or upgrade at a preset time
- Multi-level management: multi-level account with different permission for device amount and operation for a device
- Security event notifications are sent immediately to preset Emails, Mobile phones, and WeChat accounts
- Applicable to either a dedicated network or public network

1.2 Manageable device models

UMS can manage these models:

- Voice gateway: HX4G、MX8G、MX60E、MX120G、MX100G-S、HX4E、MX8A、MX60、MX100G
- IP-PBX: OM20G、OM50G、OM80E、OM200G、OM500、OM20、OM50
- NRP1202、NRP2002/P、NRP2013/P

The devices should meet the requirements shown in the following table:

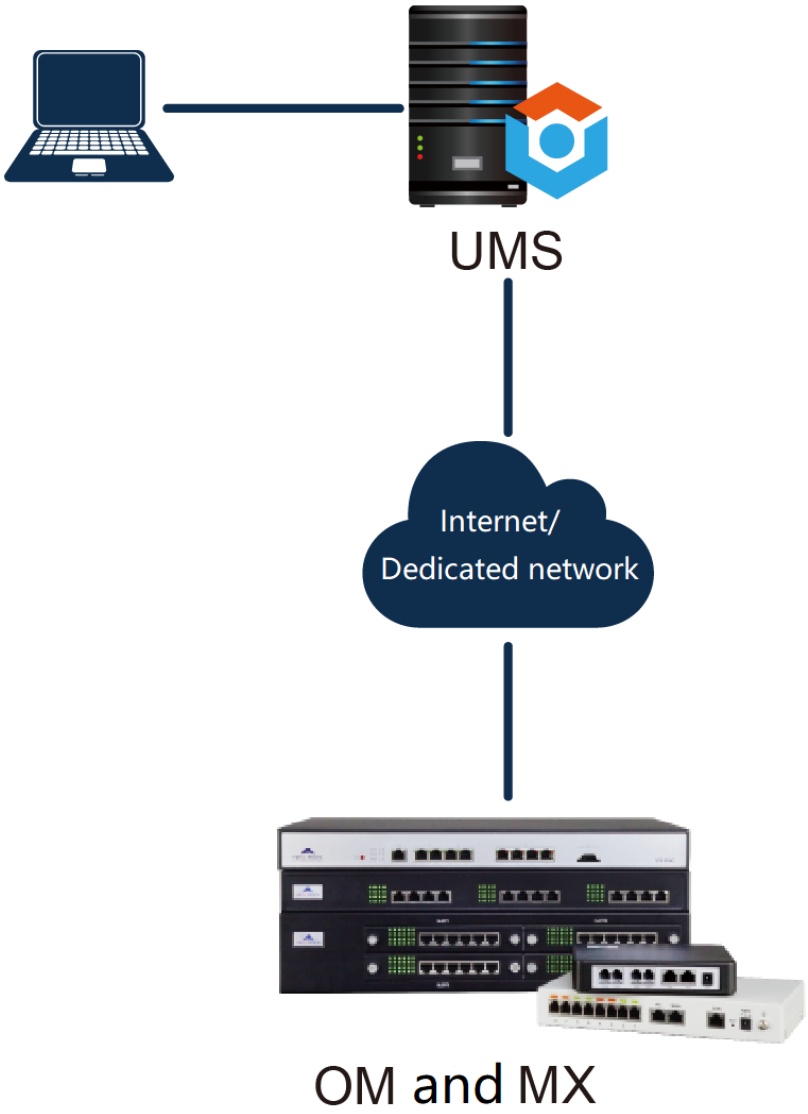
Components	Lowest version
cloud_basic	1.0.38
boa	2.4.58
autoupd	3.0.160

To make sure a device meets the requirements referred above, please do as follows:

1. Log on to the device's Web GUI.
2. Open the page of ***https://device's address/cloud/cloud.html.***
3. Upgrade the **cloud_basic** component to the version 1.0.38 or later.

 Copyright © New Rock Technologies, Inc

1.3 Typical application scenario



Copyright © New Rock Technologies, Inc

2 Install UMS server

The UMS server installation package will be provided to you after purchasing. It should be installed on a CentOS 64bit Linux operating system.
The installation package for the first installation is named as “ums_vx.x.x.tar.gz”, and that for upgrading is named as “umsUpgrade_vx.x.x.tar.gz”, where x.x.x indicates the version number.

2.1 Environment requirements for installation

Recommended configurations for hardware

CPU: Intel® Xeon® Processors, four cores, 2.5GHZ or higher clock speed
RAM: 8GB or more
Hard disk drive: 500GB or more

Running environment

Operating system: CentOS Linux 7.x 64 bit
Make sure the UMS server can access the Internet, because some system softwares need to be installed through Internet.

2.2 Installation process

1. Upload the installation package to the Linux server and run the following command to extract the package.

   tar -zxf ums_vx.x.x.tar.gz
2. Open the file folder after the package is extracted.
3. Run the following command to install.

   sudo ./install.sh -i eth0 --show –-domain=www.yourdomain.com

   Where “**-i**” is the UMS server’s network port (such as eth0), whose IP address is the adderss to access the UMS.

   “--show” means to print the installation process messages on the screen

   “--domain” is followed by the domain name of the UMS to be accessed, if there is no domain name, enter the IP address
4. After the installation is completed, reboot the server or use the command **/usr/local/ums/umsservice.sh start** to start the UMS.

 Copyright © New Rock Technologies, Inc

2.3 Manage UMS service and upgrade UMS

Management

To stop UMS service, run the command:
/usr/local/ums/umsservice.sh stop
To start UMS, run the command:
/usr/local/ums/umsservice.sh start

Upgrading

See Upgrade.

2.4 Replacement of UMS certificate

1. Perform the following steps in the directory where the new certificate is located:

```
cp -f cert.pem /usr/local/ums/ums/conf/

cp -f key.pem /usr/local/ums/ums/conf/

cp -f cert.pem /usr/local/ums/umsmaintenance/conf/

cp -f key.pem /usr/local/ums/umsmaintenance/conf/

cp -f cert.pem /usr/local/ums/mqtt/mosquitto_ca.crt

cp -f cert.pem /usr/local/ums/mqtt/mosquitto_srv.crt

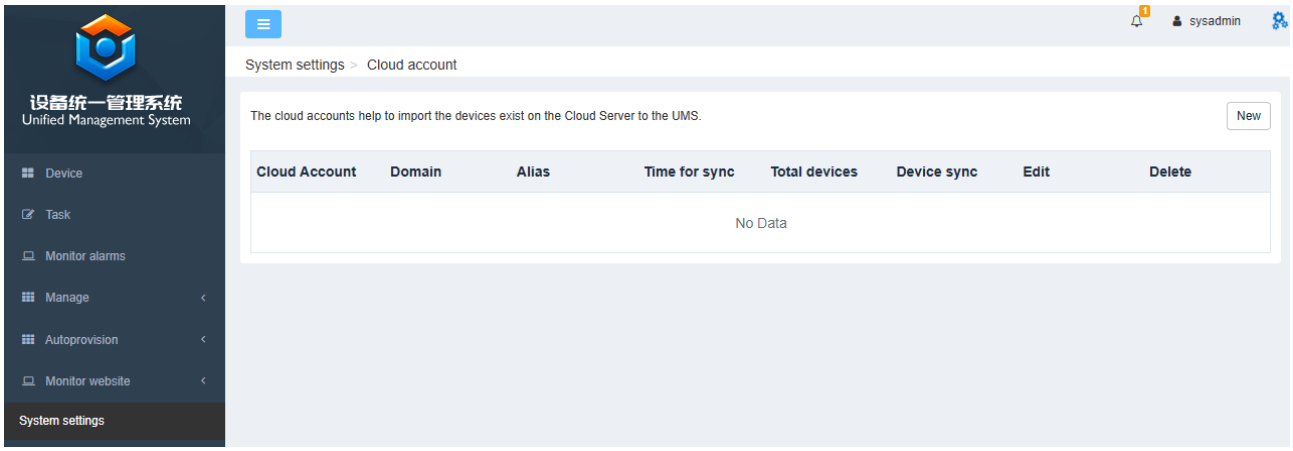
cp -f key.pem /usr/local/ums/mqtt/mosquitto_srv.key
```

2. Reboot UMS after replacement

2.5 Cloud account

Navigate to System Settings > Cloud Account to set up a cloud account, and the cloud platform devices can be synchronized and imported to the webmaster for management via your cloud account.

 Copyright © New Rock Technologies, Inc



2.6 Security settings

When UMS server is deployed in public network, the following security settings is required to avoid the network attacks.

- Turn off all unnecessary applications or services
- Modify the port 22 of SSH service to another port and add firewall rules for IP address to access the SSH service.
- Add firewall rules to deny all ports and protocols except for the necessary port for UMS service (443, 8883) and SSH service.
- Deny receiving ICMP packets to avoid Ping of Death.

Copyright © New Rock Technologies, Inc

3 Log in to UMS

On any computer connected with the UMS server, enter the UMS IP address or domain name (with the port number 443) in the browser to log in to UMS.
Default administrator: sysadmin
Default password: admin@123



4 Manage devices

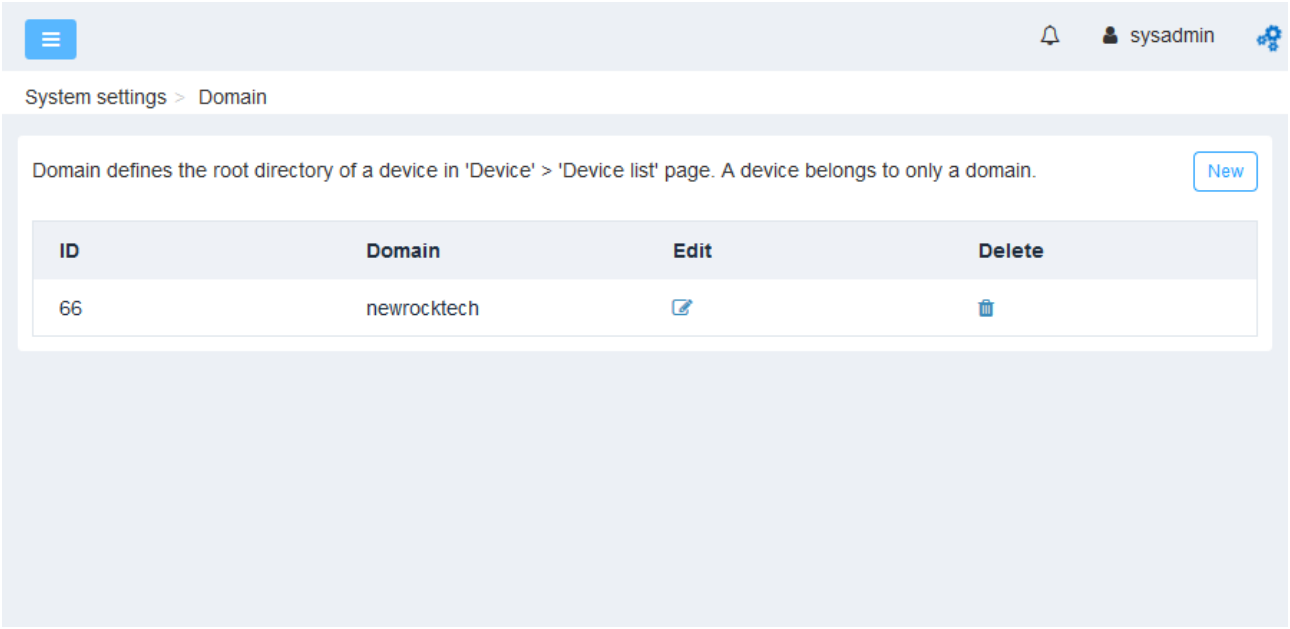
4.1 Create domains and device groups

Allocating New Rock devices into multiple domains and groups allows administrator (and other types of users) to manage and control devices more effectively.
Domain defines the root directory of a device in **Device** > **Device list** page. A domain is a collection of devices which contains many device groups, and a device group contains multiple sub-groups.
In short, you can create multiple device groups under one domain.

UMS has a default domain which contains those devices that do not specify specific ownership.

Add a new domain

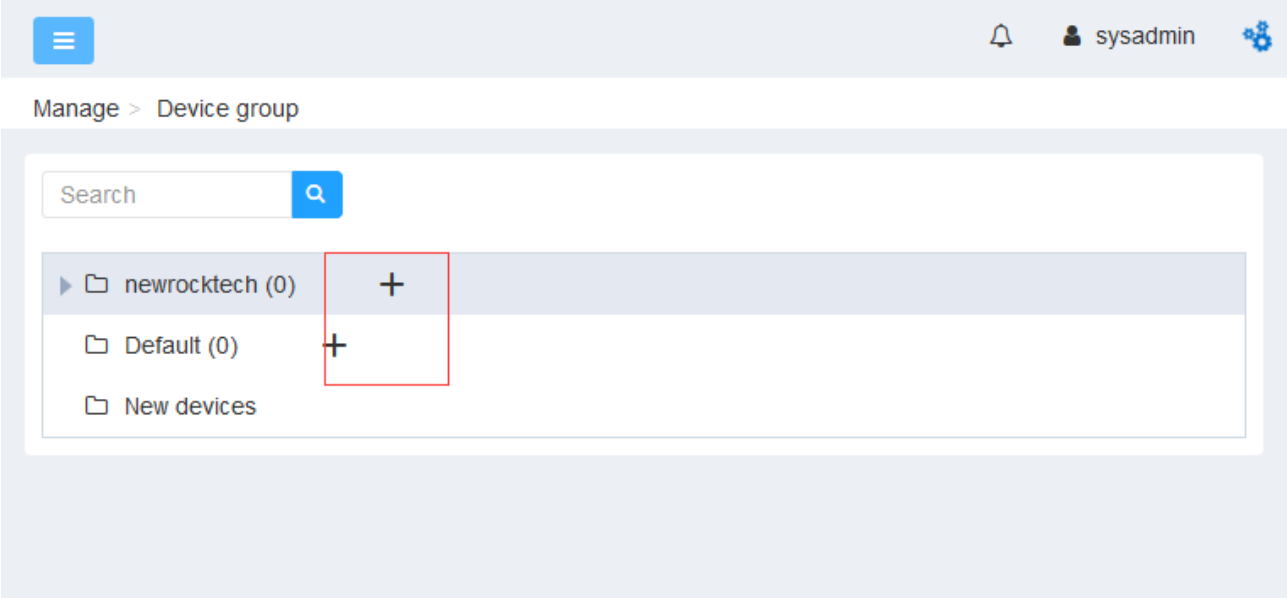
1. Go to **System settings** > **Domains**, click **New** to create and fill in domain information.



Add a new device group

1. Go to **Manage** > **Device groups**, click + to create a device group.

Copyright © New Rock Technologies, Inc



4.2 Add devices

To allow the UMS to manage a device, you need to add the device to the UMS.

There are three methods to add a device to UMS.

- If the device meets the requirements listed in Section 1.2, two methods are applicable:

  Method 1: Add the device through auto discovery by UMS

  Method 2: Add the device by using New Rock cloud plaform through your cloud account

- If the device does not meet the requirements listed in Section 1.2, only one method is applicable:

  Method 3: Manually add the devices one by one to UMS.

  Attention: in common, this method is not recommended to use, because UMS do not provide full management to the devices added through this method.

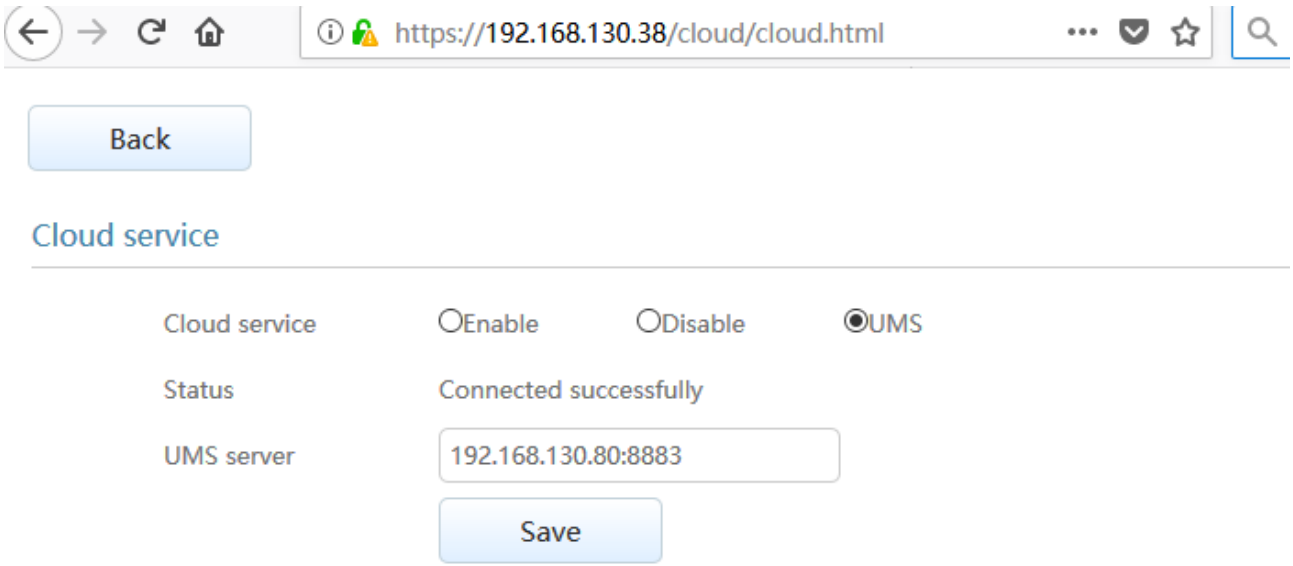
Add devices by auto-discovery

This method requires that the devices can access UMS, and is applicable to the scenario that the devices and UMS are deployed in the same dedicated network.

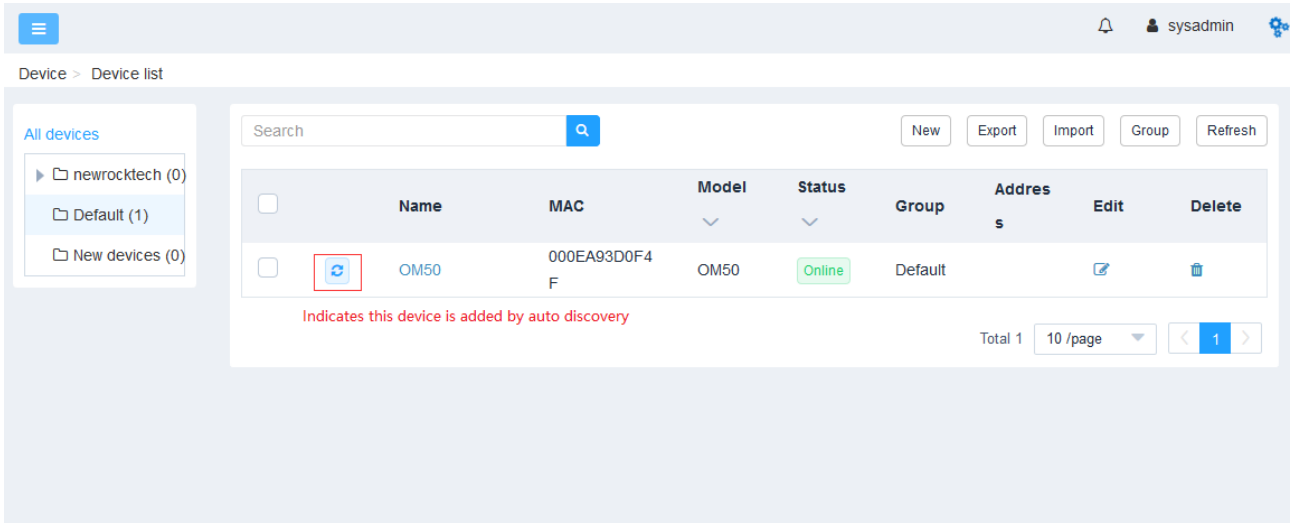
You need to preset all devices to be added as follows.

1. Log in to the Web GUI of the device.
2. Open the page of https://device's-IP-address/cloud/cloud.html.
3. Choose **UMS** for **Cloud service**. Enter the IP address or domain name of UMS server, with the port number 8883.
4. Click **Save**. Then this device can be discovered by UMS.

 Copyright © New Rock Technologies, Inc

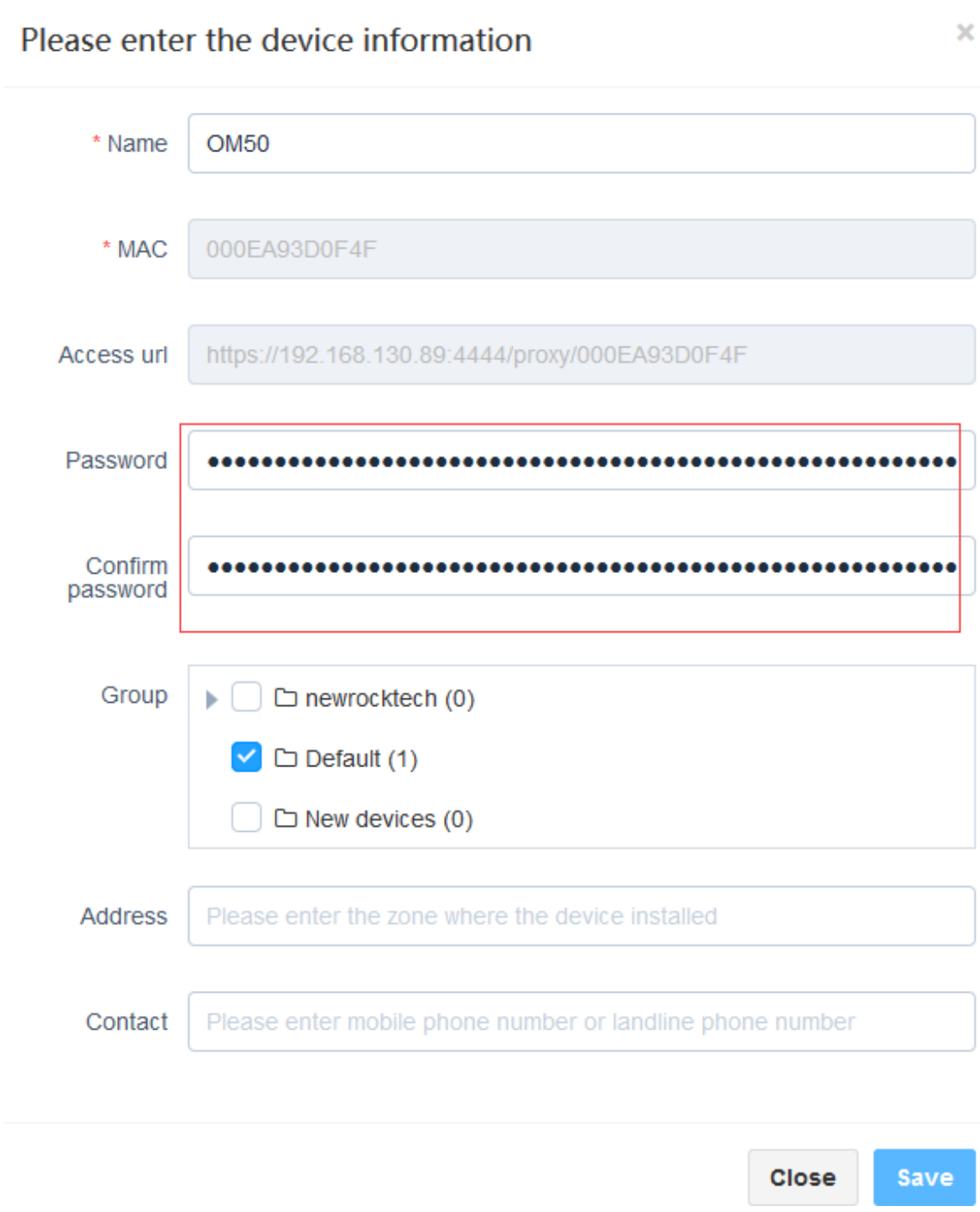


5. Log in to UMS, you may see the devices added by auto-discovery on **Device** > **Device list** page.



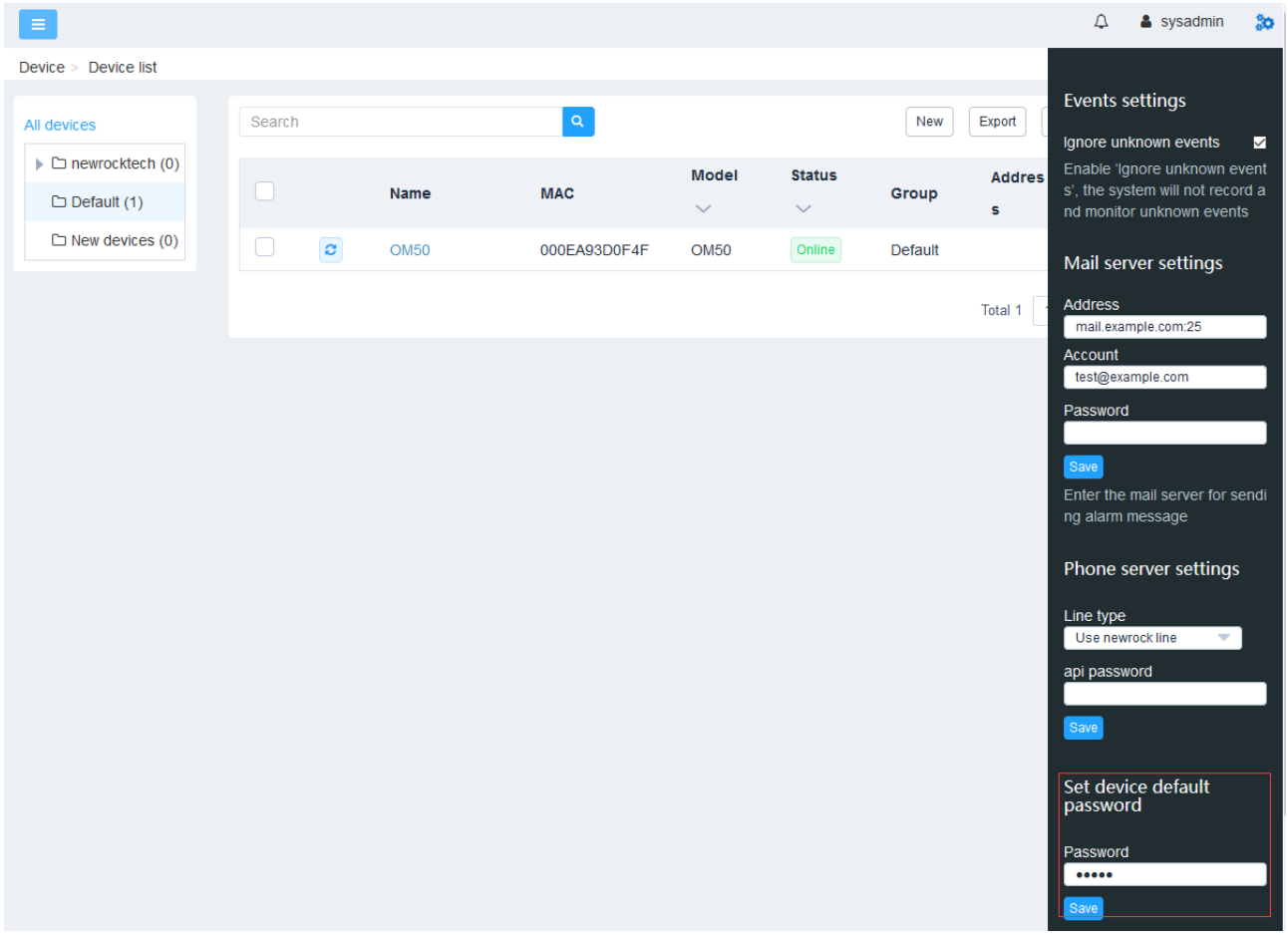
6. Click a specific device name, and input the password to log in to the device's Web GUI, now, the UMS has the permission to manage the device.

Copyright © New Rock Technologies, Inc



Note: If you did not input the password for the device, the UMS will use a default password to attempt to log in to the device. You can preset the default password by clicking the symbol at the upper right corner. The default password avoids that you input the password one by one when you add numerous devices with the same password.

Copyright © New Rock Technologies, Inc



Add devices by a New Rock Cloud Account ID

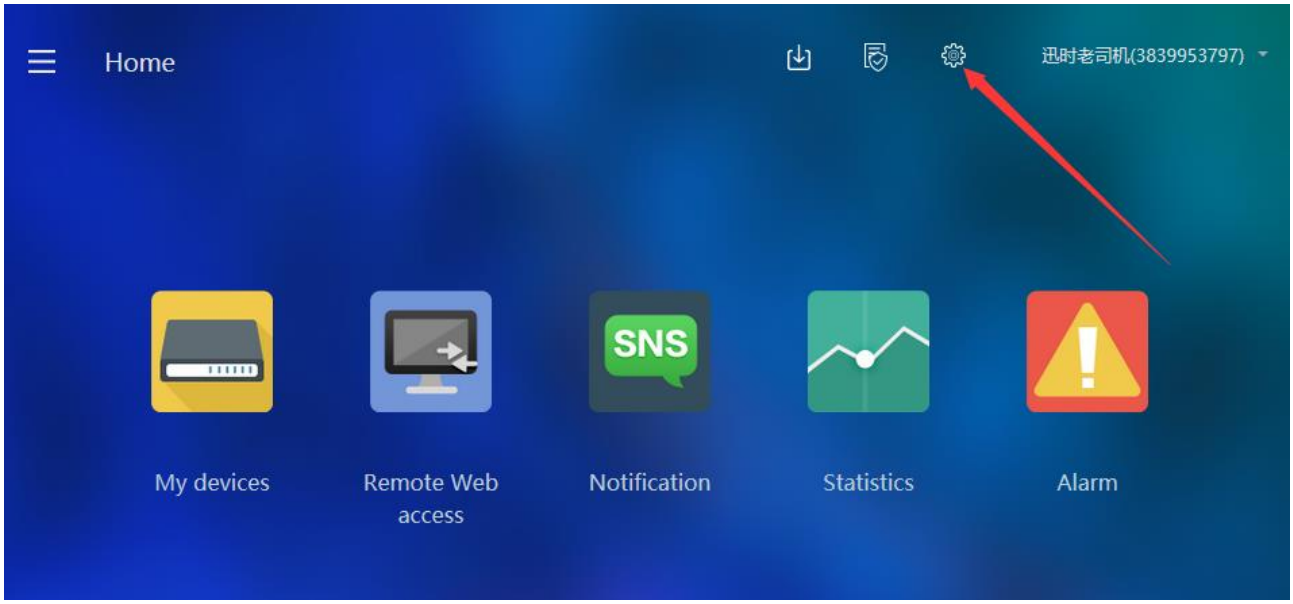
If the devices had been managed by New Rock Cloud, you can import all these devices to UMS by a New Rock Cloud Acoount ID.

This method requires all the devices and UMS can access Internet.

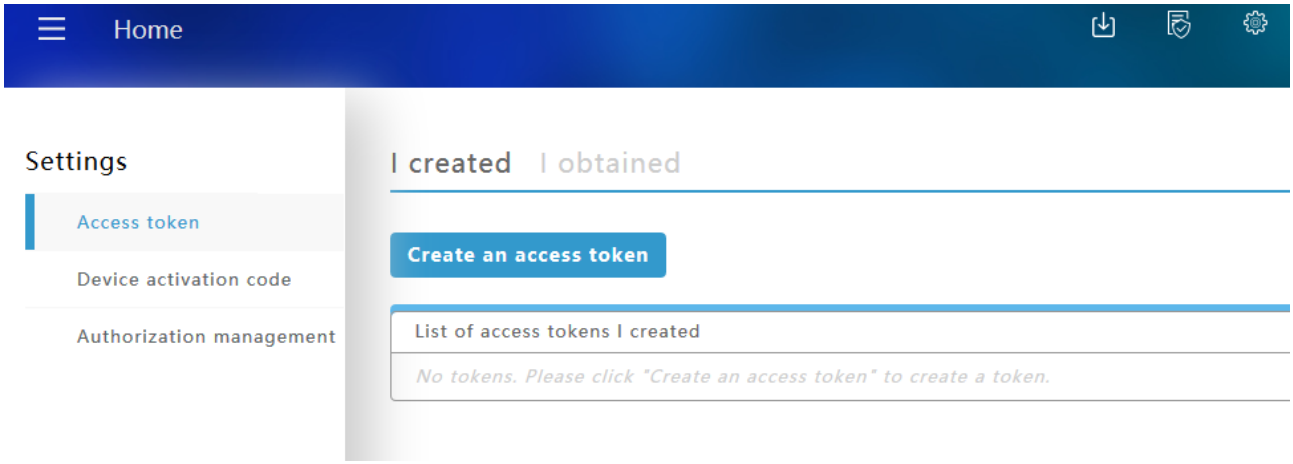
The process is as follows:

1. Log in to New Rock Cloud website https://i.newrocktech.com.
2. Click the symbol  on the upper right corner.

Copyright © New Rock Technologies, Inc



3. Click **Access Token** > **Create an access token**.



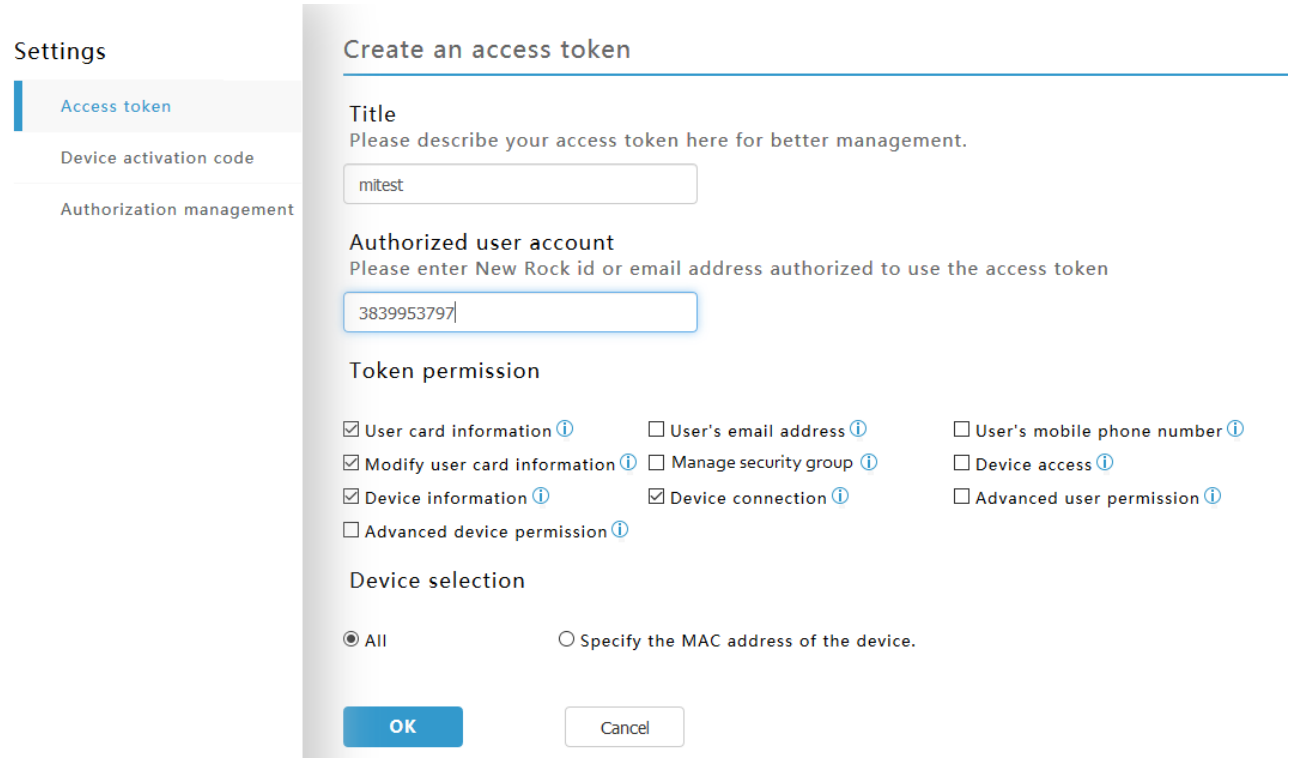
4. Input token information:

Authorized user account: Input the current logged-in New Rock Cloud ID.

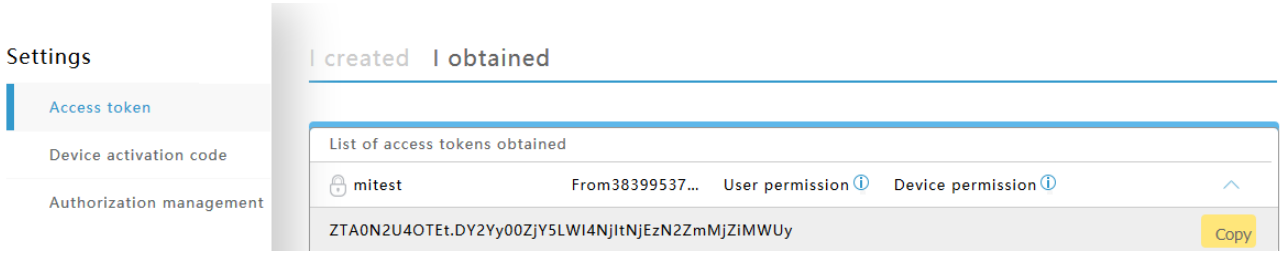
Token permission: Tick all the functions you want to authorize to this access token.

Then Click **OK**.

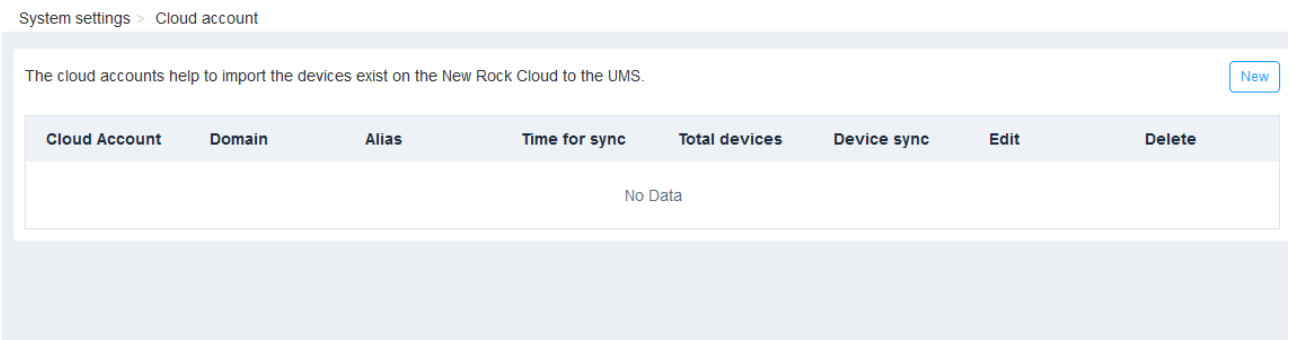
Copyright © New Rock Technologies, Inc



5. Click **Access token>I obtained** > **Copy** to copy the access token.

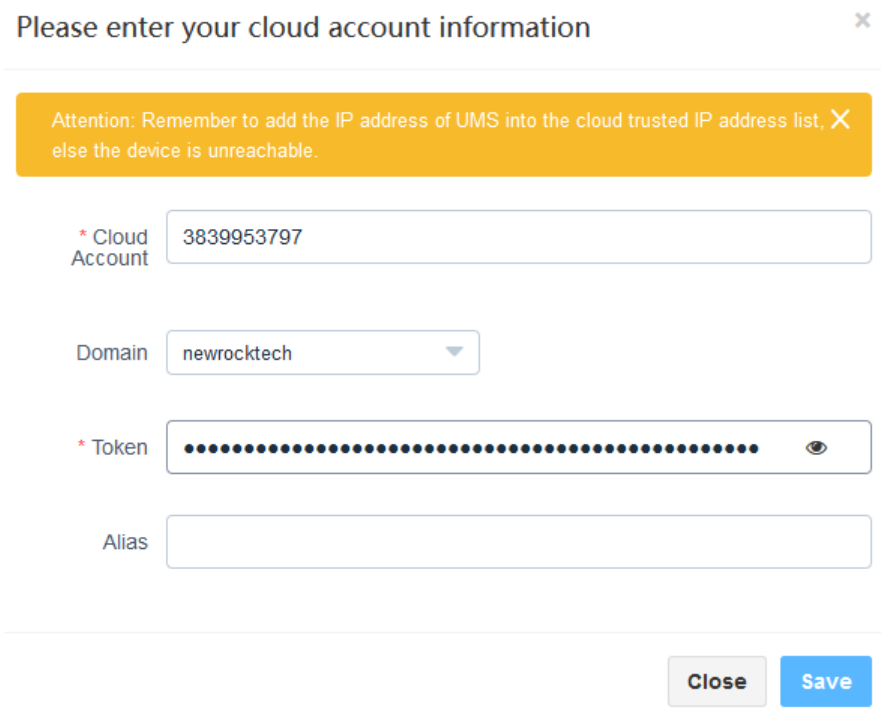


6. Now please log in to UMS, go to **System settings** > **Cloud account** page, and click **New**.

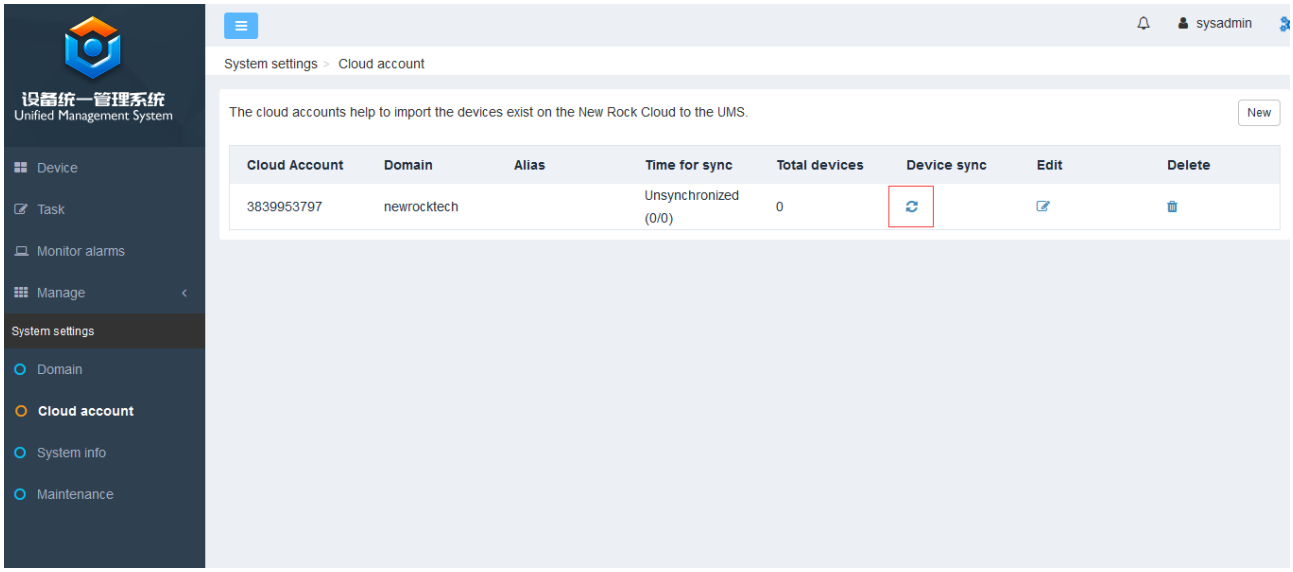


7. Input the New Rock Cloud Account ID and paste the access token, then click **Save**.

Copyright © New Rock Technologies, Inc

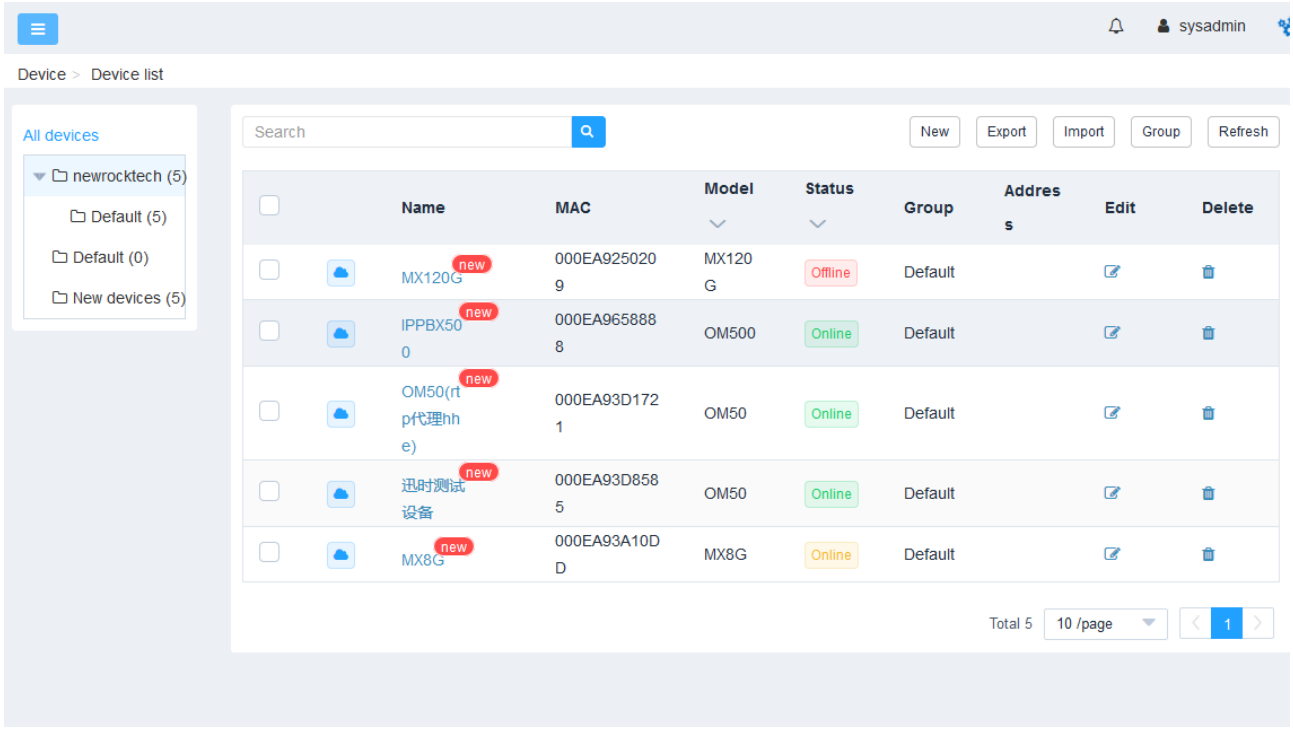


8. Click the symbol of **Device sync** to add all the devices to UMS. All the added devices belong to the default device group of the specific domain.



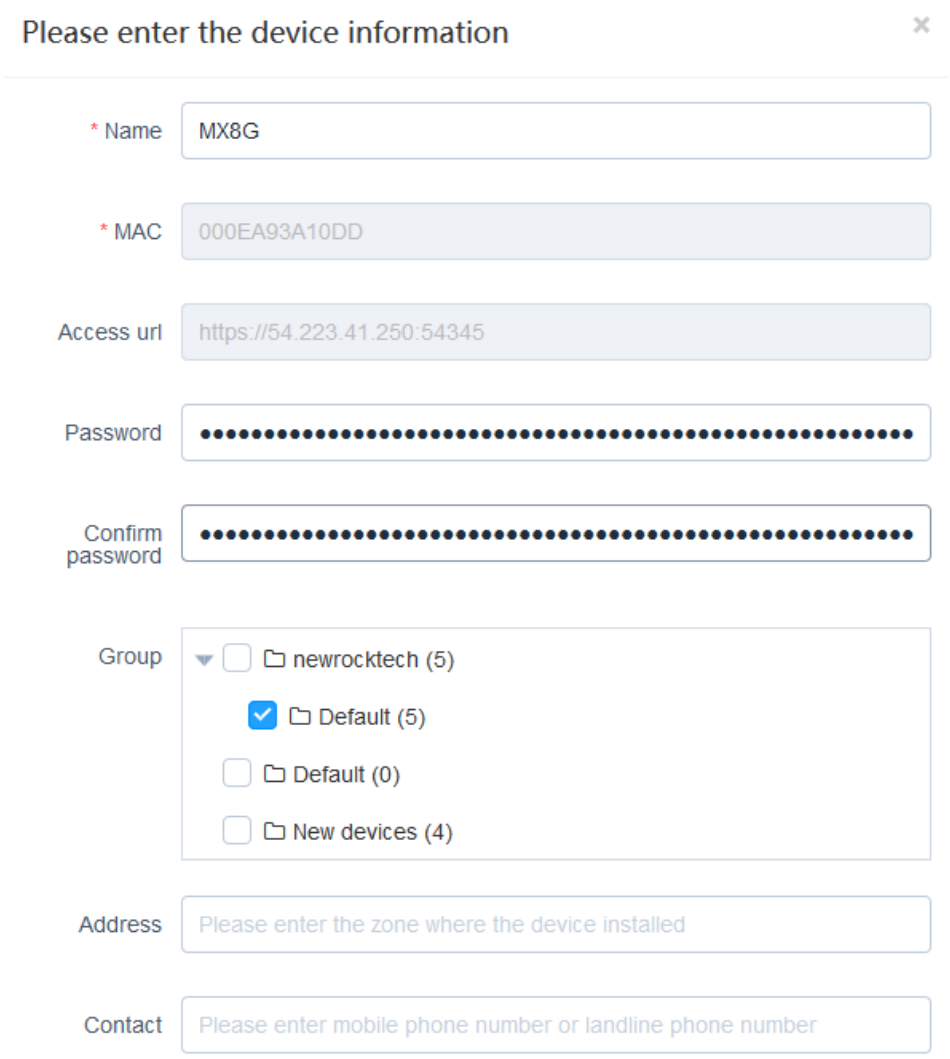
9. You can view the added devices on **Device** > **Device list** page. All the devices are marked with a symbol .

 Copyright © New Rock Technologies, Inc



7. Click a specific device name, and input the password for logging in to the device's Web GUI, now, the UMS has the permission to manage the device. If you keep the password empty, the UMS will use the default password. If the password is incorrect, the UMS is not allowed to manage the device.

Copyright © New Rock Technologies, Inc



 Copyright © New Rock Technologies, Inc

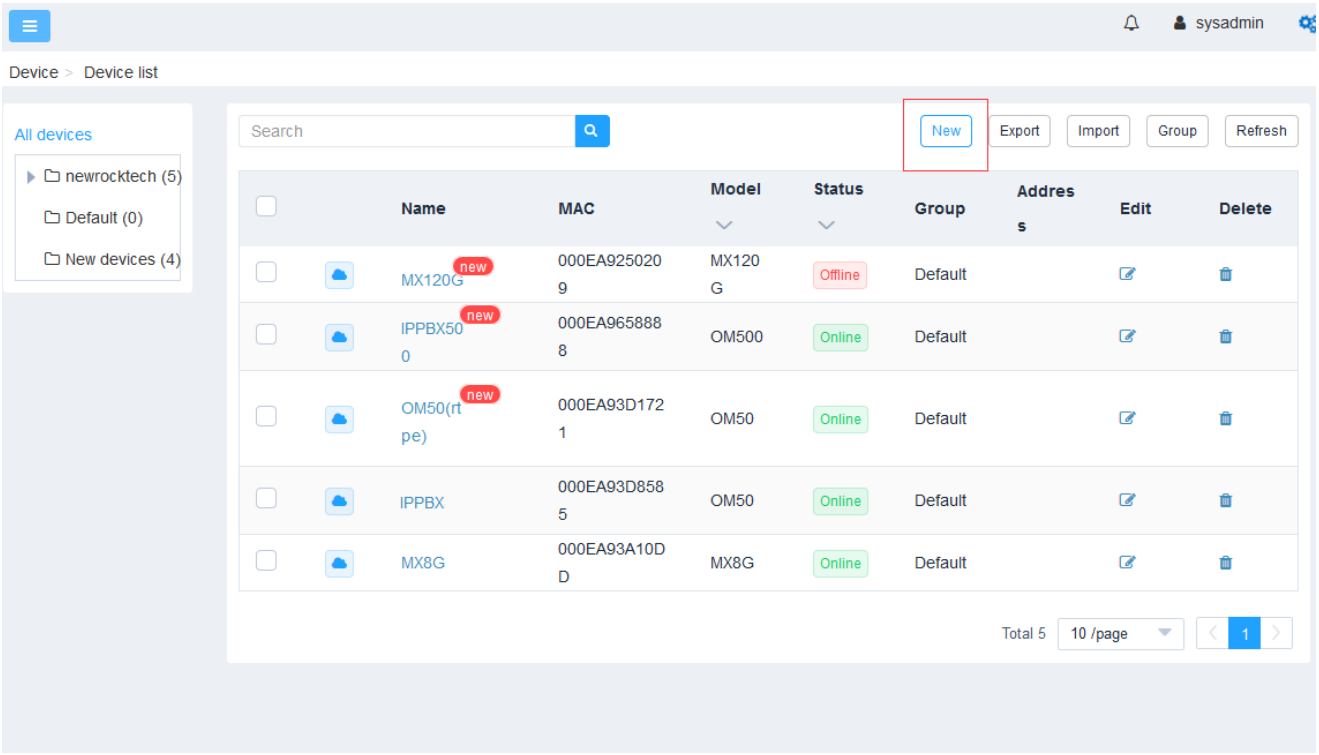
Add devices manually

When the device version does not meet the requirements listed in Section 1.2, you have to add the device manually. This method only requires the UMS server can access the device.

But UMS does not have full control to these devices, so this method is not recommended to use.

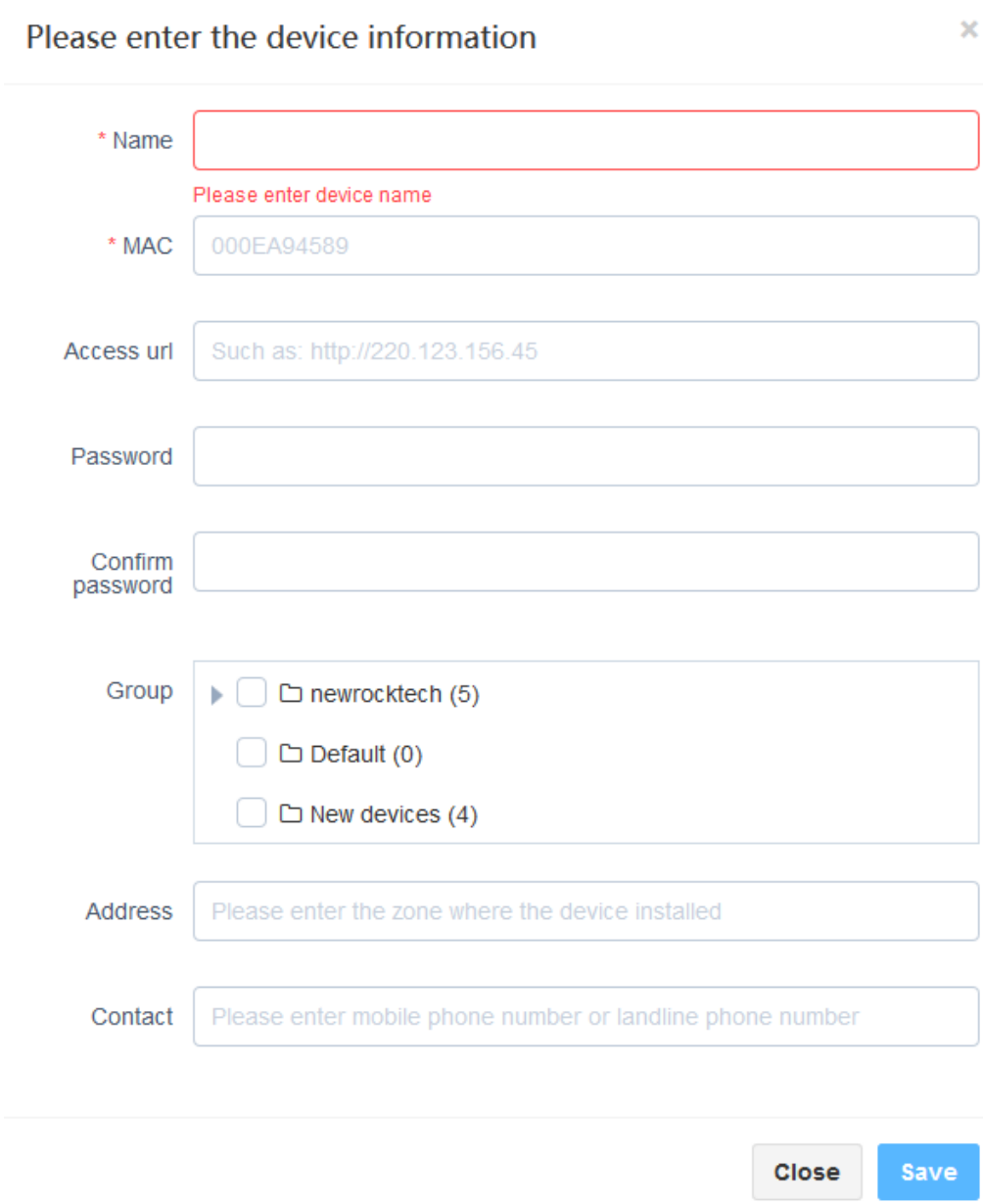
Do as the follows to implement this method.

1. Go to **Device** > **Device list**, and click **New** on the up right corner.



2. Input information as required, then click **Save**.

Copyright © New Rock Technologies, Inc

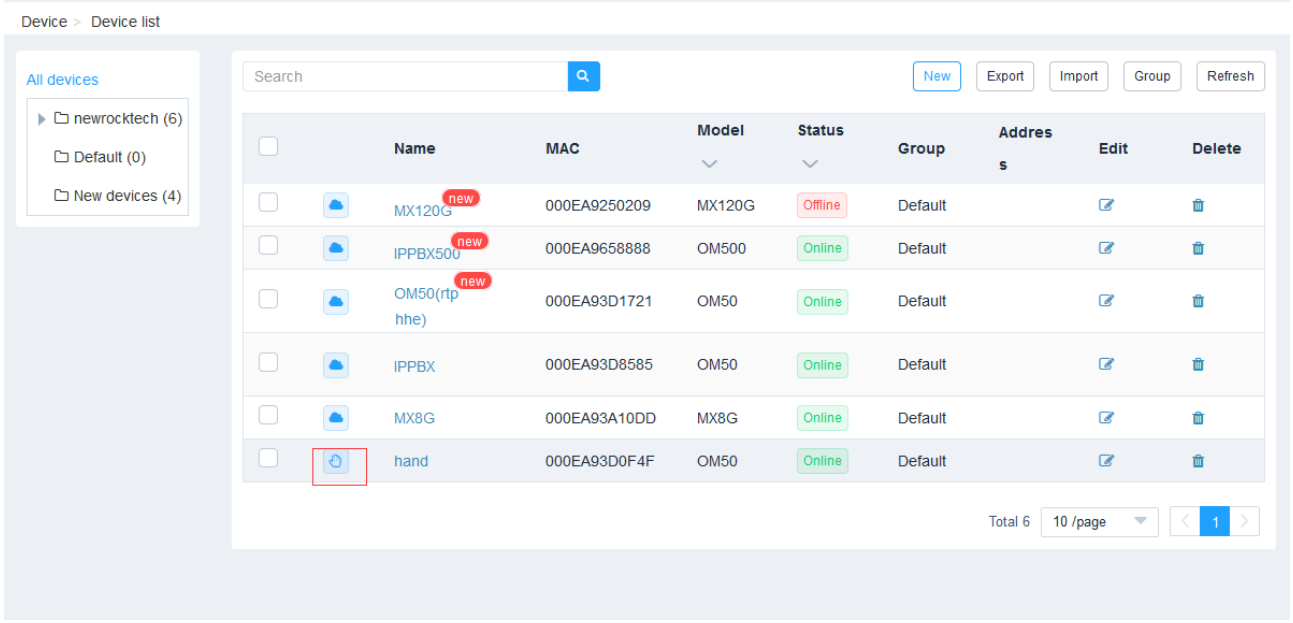


Description:

- Name: make a name for the device to allow you to search for it by its name.
- MAC: Input the MAC address of the device. The MAC address is the unique identifier for a device.
- Access URL: Input the address of the device, in the format of https://ip-address or https://domain-name. It should be a fixed address which can be accessed by UMS.
- Password: Input the password for logging in to the Web GUI of the device. Note that an incorrect password will block the UMS to obtain the configurations from the device and provision configurations to the device.
- Confirm password: Input the password again.
- Group: Choose a device group to which the device belongs.
- Address: Input the location where the device is installed. It is optional.
- Contact: Input a contact who is responsible for the device.

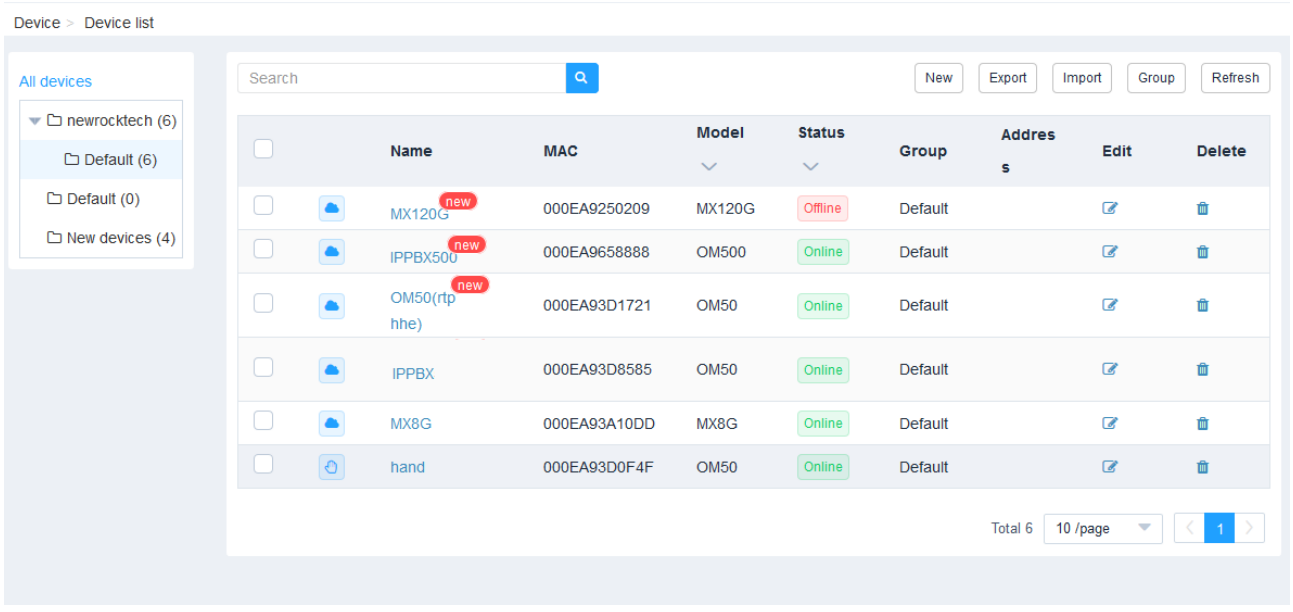
Copyright © New Rock Technologies, Inc

3. After the device is added successfully, you can see it in correspond device group on **Device>Device list** page. All devices added manually are marked by a symbol .



4.3 Device list and device status

All added devices are listed on **Device** > **Device list** page.



Description:

- The device list allows you to view and modify the device information, add or delete devices.
- Click the symbol in front of the device name, you may sync the device status.
- You can search the device by its name or MAC address.
- To change the device group to which the device belongs, choose the device and click **Group** to

 Copyright © New Rock Technologies, Inc

select another group.

- Support to import and export devices in batch.

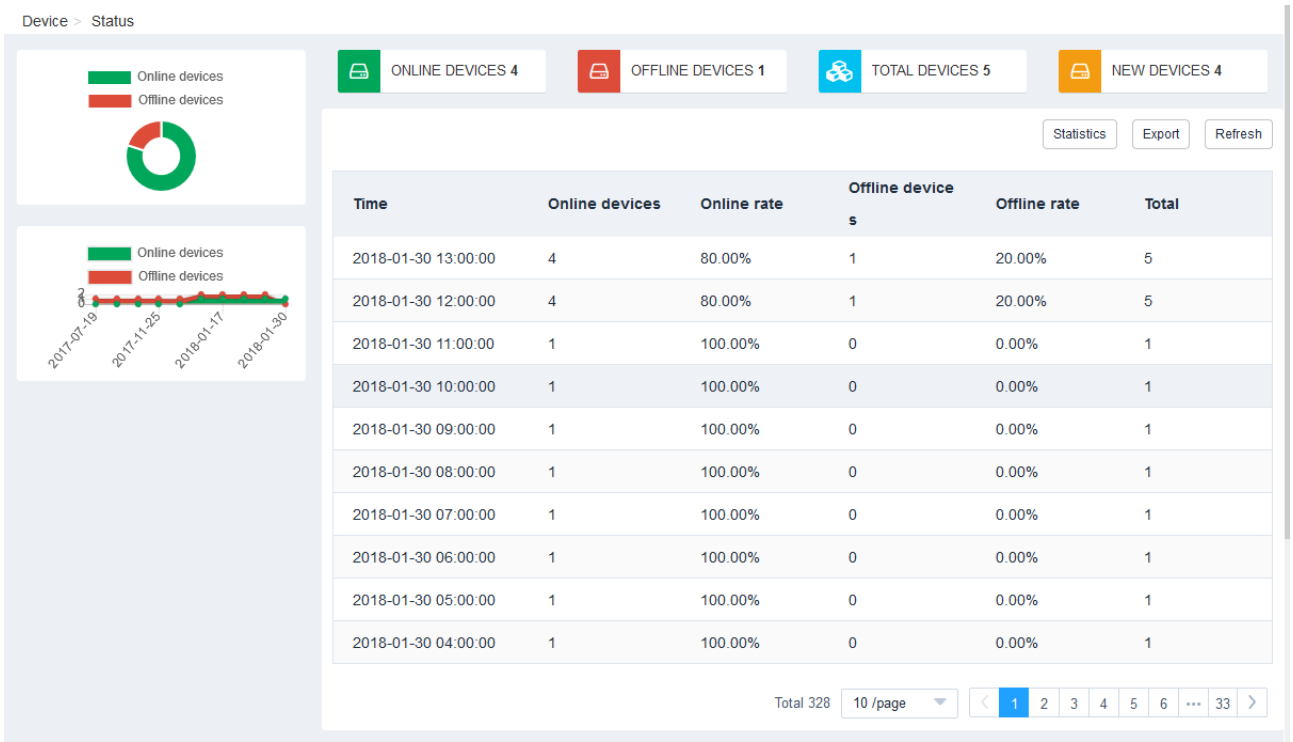
The exported device list is shown as below (The access URL and password cannot be exported):

MAC	Name	Access URL	Password	Address	Contact	Model	App version
000EA92D015B	Cxy_OM20			Shanghai	Lisa	OM20	5_121_3
000EA9611006	MX100G-S			Beijing	Michael	MX100G	5_115
000EA9050C31	Officium200G			Hangzhou	Alex	OM200G	2.1.5.108

Before importing, please fill in the table based on an exported list. The MAC address field is mandatory, the other fields can be omitted.

MAC	Name	Access URL	Password	Address	Contact	Model	App version
000EA92D015B	Cxy_OM20	https://222.2.111.118	2w3e4r	Shanghai	Lisa	OM20	5_121_3
000EA9611006	MX100G-S	https://32.8.11.111	tgbyh6	Beijing	Michael	MX100G	5_115
000EA9050C31	Officium200G	https://23.5.1.7	ujik89	Hangzhou	Alex	OM200G	2.1.5.108
000EA941DD34	MX60-VoIP	https://83.5.9.16	dfg567	Nanjing	James	MX60	1.9.82.344.2

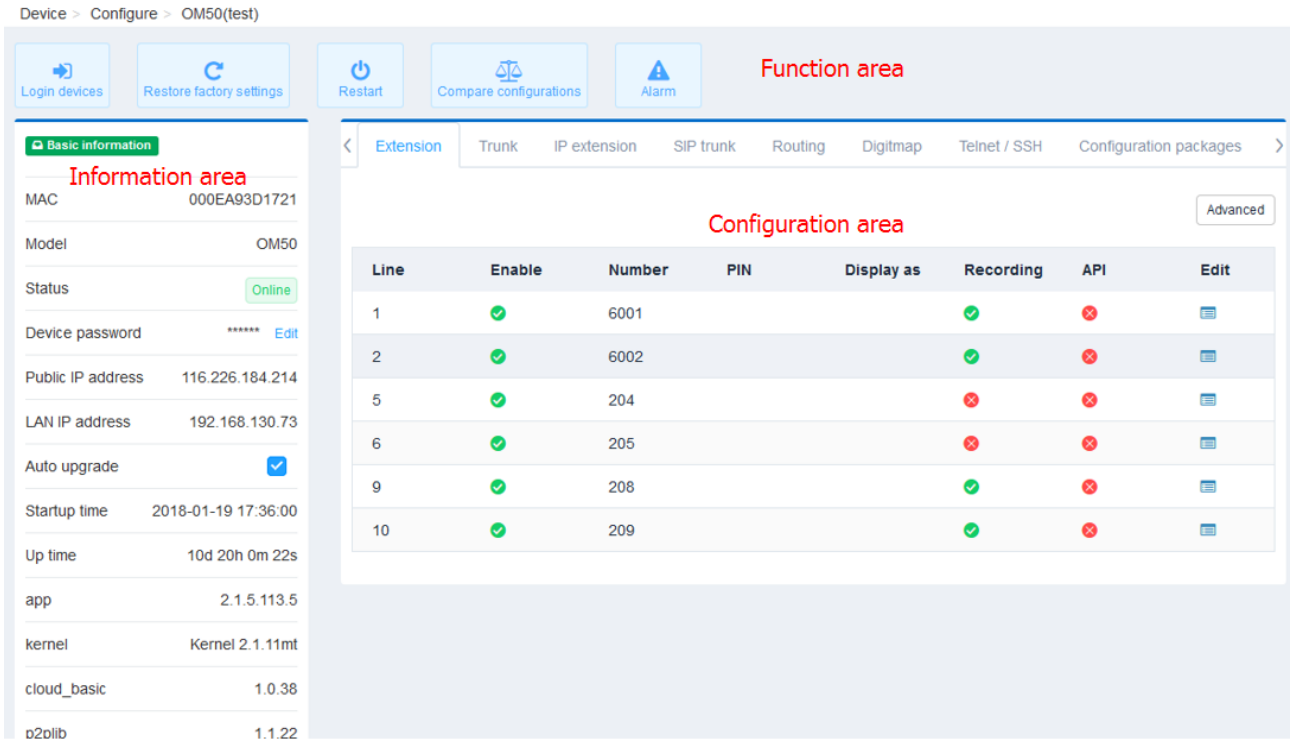
The **Device** > **Device status** page shows statistics which is updated per hour (set as default). To update the statistics real time, please click **Statistics**.



 Copyright © New Rock Technologies, Inc

5 Configure devices

Go to **Device** > **Configure**, and click a specific device name to open the device configuration page. This page shows the device's basic information and allows you to configure the device.



Description:

Function area: lists the most common functions for the device, such as log in to the device, reset to factory default settings, reboot, compare configurations, and alarms.

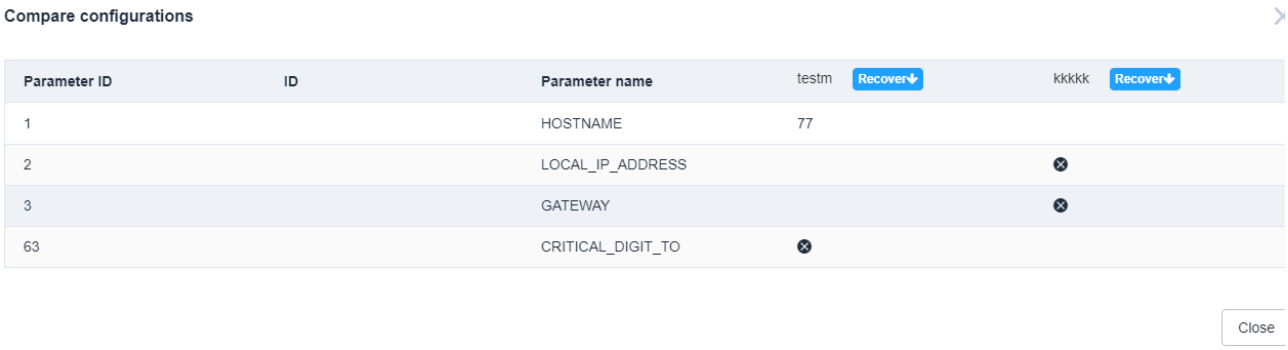
Information area: lists the device address and version information

Configuration area: allows you to configure the device.

Description for Some of the functions to configure the device:

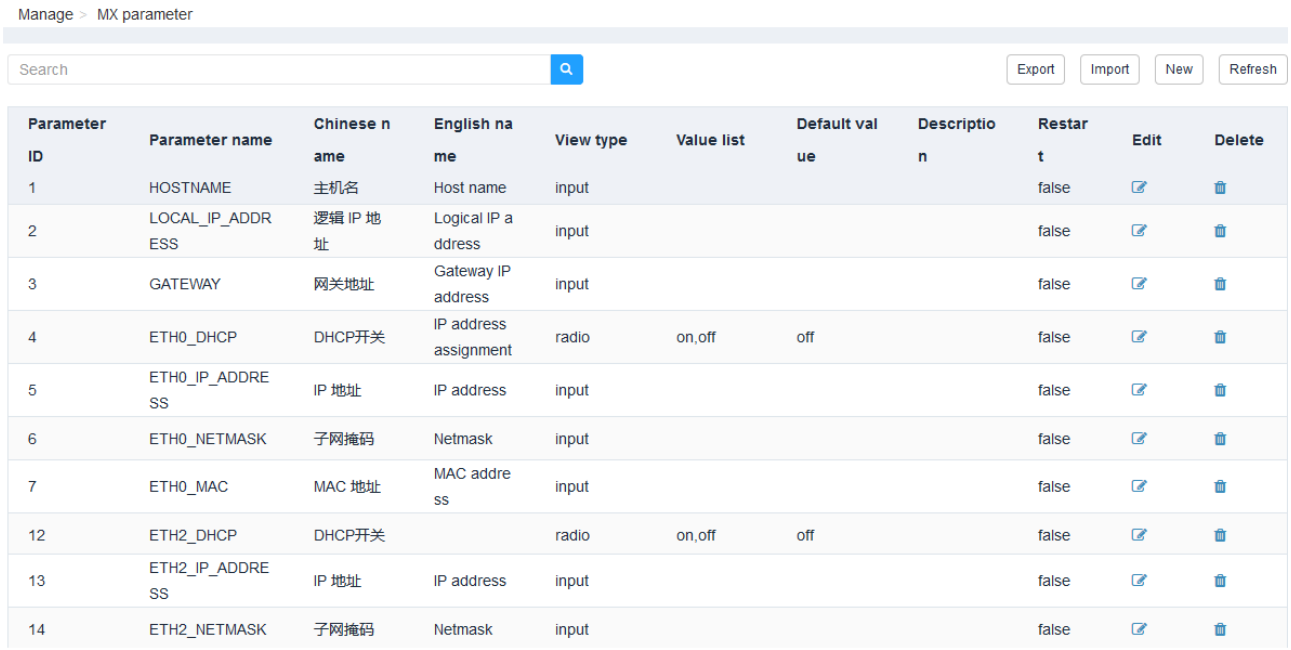
- Login devices: click it to open the login page for the device's Web GUI.
- Auto Upgrade: tick it to enable the auto upgrade for the device. For more details about auto upgrade, see Upgrade automatically.
- Compare configurations: click it to open the page for comparing any two configuration templates or backed up configurations.

Copyright © New Rock Technologies, Inc



5.1 Parameters and templates

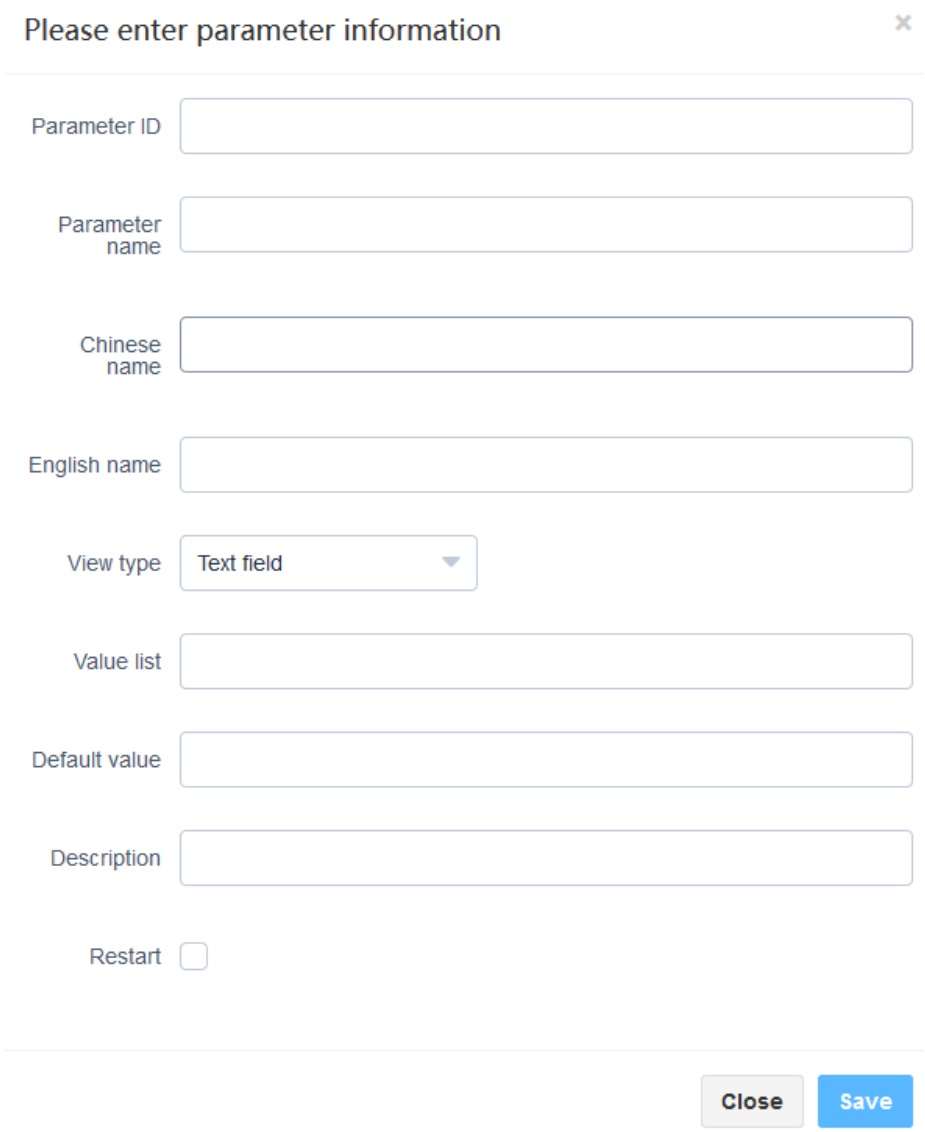
The most common parameters of OM and MX are listed On **Manage**> **MX parameters** and **Manage** > **OM parameters** pages. Of course, you can also add or delete the parameters.



Parameters

To add more parameters, click **New**.

Copyright © New Rock Technologies, Inc



Description for each field of a parameter:

- Parameter ID: Input the parameter ID which is defined by the device. Each parameter has a unique parameter ID. For example, the parameter ID of the parameter MAC address is 7.
- Parameter name: Input the parameter name which is defined by the device.
- Chinese name: Create a unique Chinese name for the parameter. It is optional.
- English name: Create a unique English name for the parameter. It is optional.
- View type: Choose the view type for the parameter. There are four view types to choose: Text field, Radio button, Drop-down list and Read-only parameter.
- Value list and Default value: Input the possible values and the default value. They vary with the **View type**:

1) If the **View type** is **Text field**, please input the value for the parameter, and keep the default value empty.

2) If the **View type** is **Radio button**, please input two values and separate them by a comma ",". Set the default value as either.

3) If the **View type** is **Drop-down list**, please input several values for the parameter, and keep the

 Copyright © New Rock Technologies, Inc

default value empty.

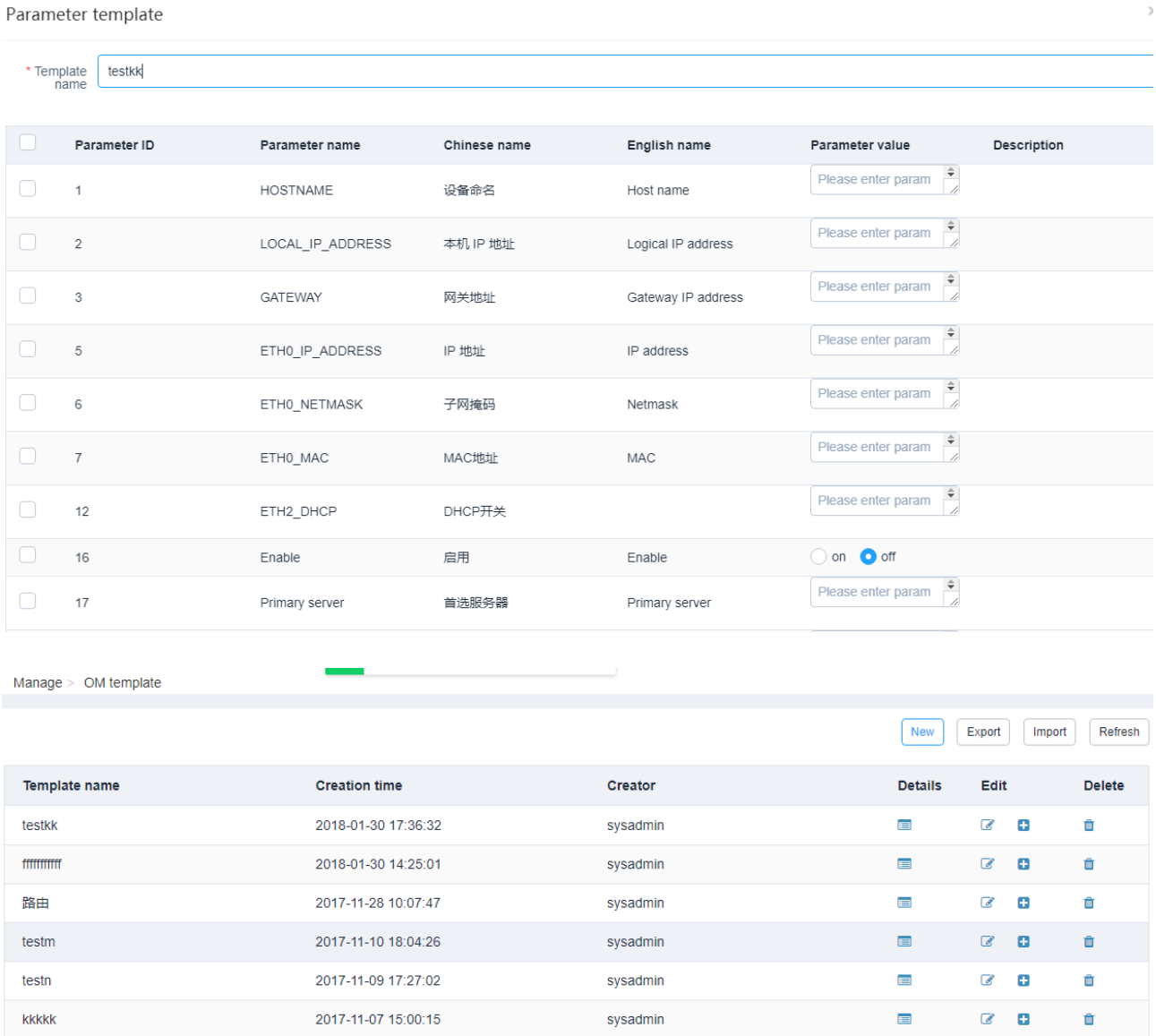
4) If the **View type** is **Read-only parameter**, keep both the value list and default value empty.

- Description: Input the description for the parameter, it is used to recognize the parameter and it is optional.
- Restart: Tick it if the configuration for the parameter will take effect after the device restarts.

Parameter template

A parameter template is a collection of many parameters. It will be helpful to maintain or manage a large number of devices to back up or provision configuration based on a parameter template.

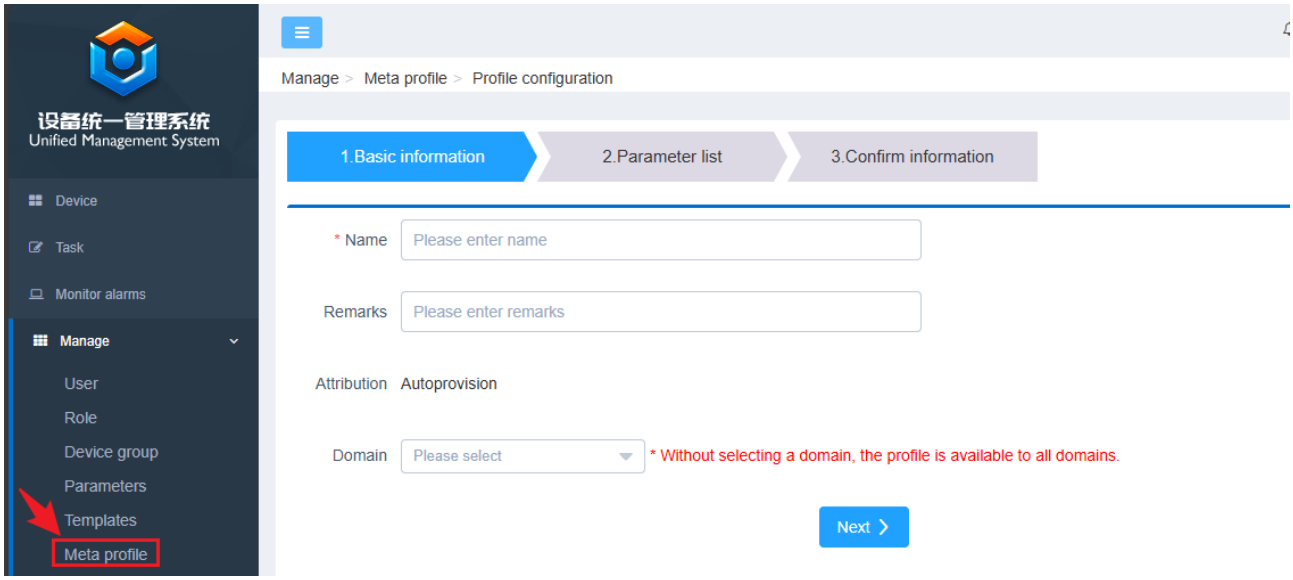
You can configure multiple parameter templates. The parameters contained in a template are derived from the preset parameter list on the **Manage** > **OM parameters** or **Manage** > **MX parameters** page. To add a parameter which is not listed on these pages to a template, you should add it on the **Manage** > **OM parameters** or **Manage** > **MX parameters** page first.



 Copyright © New Rock Technologies, Inc

Customized templates

Navigate to Manage> Meta profile> Profile configuration, a module for creating and managing device configuration templates for quick bulk application to multiple devices.

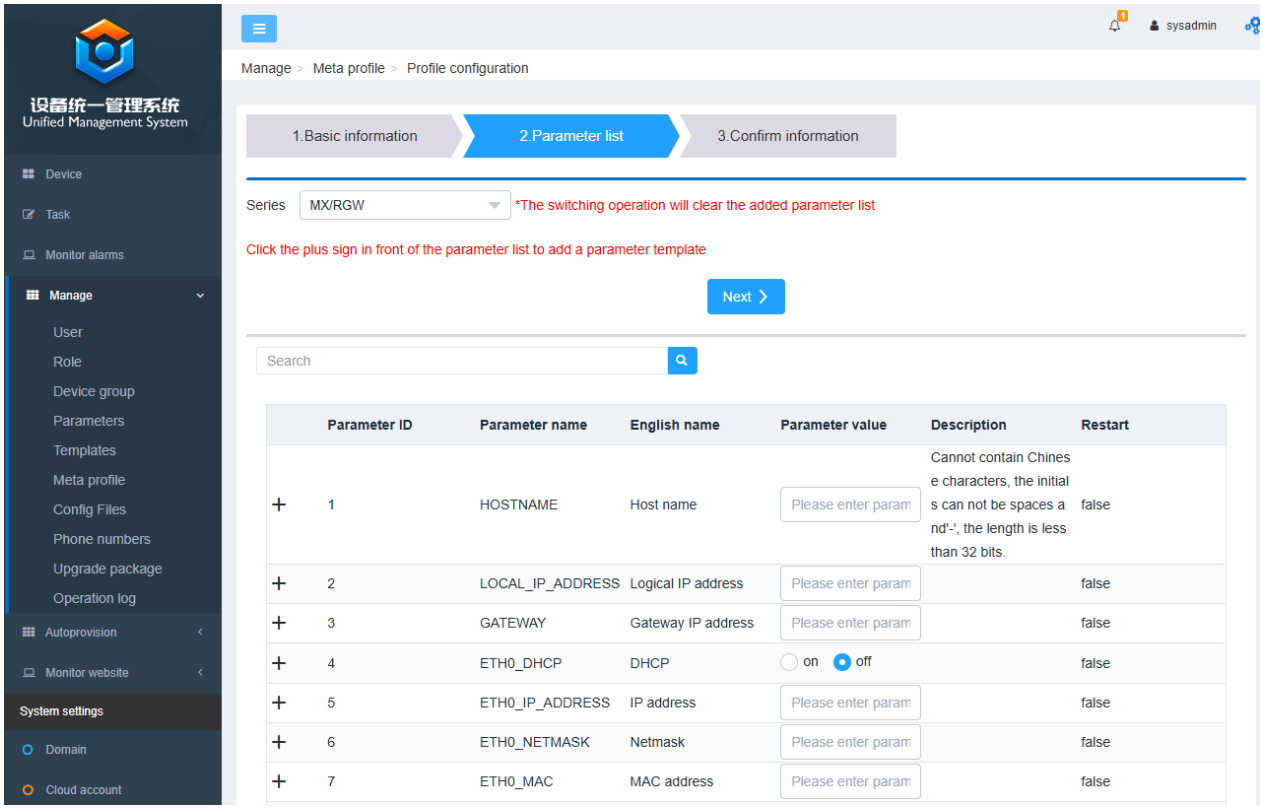


Step 1. Fill in the basic information

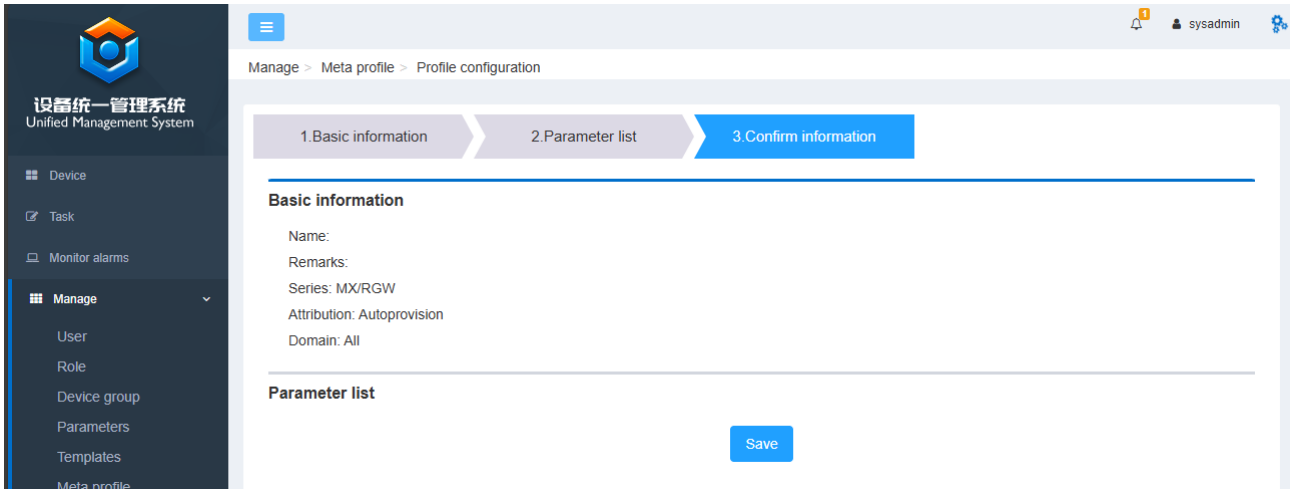
Item	Definition
Name	Enter a name for the template
Remarks	Additional instructions for entering templates
Domain	Selecting Managed Device Groups

Step 2. Configure the parameter list

Copyright © New Rock Technologies, Inc



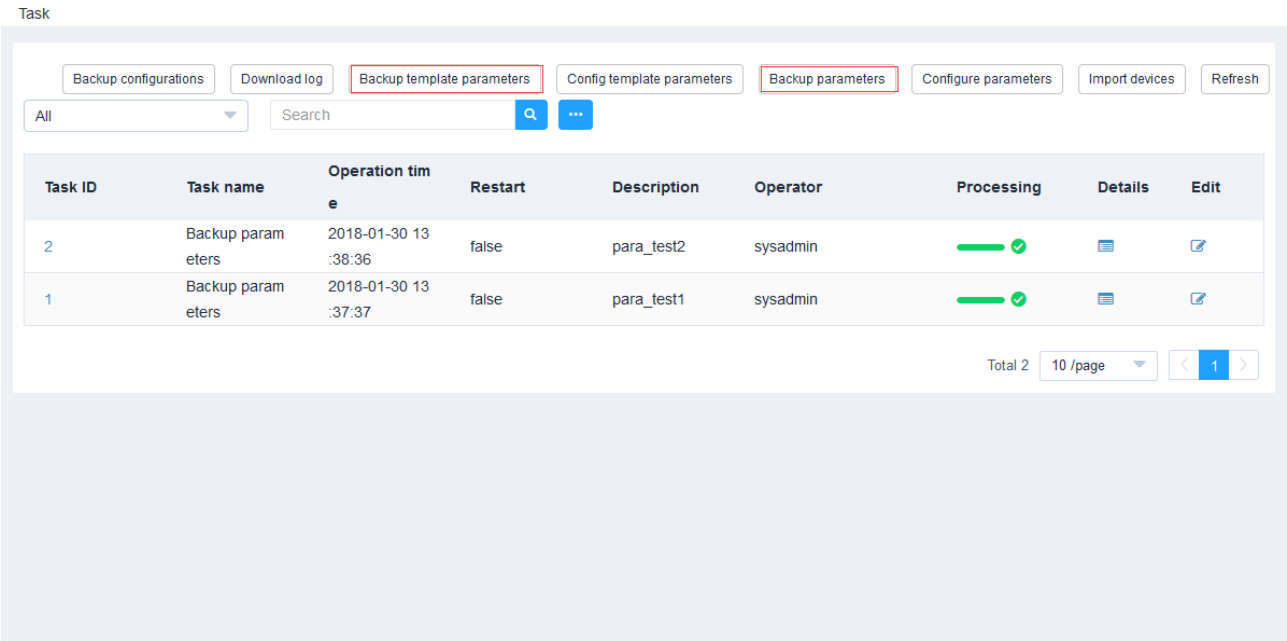
Step Three. Confirmation of information



 Copyright © New Rock Technologies, Inc

5.2 Back up parameters

This function allows you to quickly recover the configurations by provisioning the backup parameters when the device's configurations are modified.



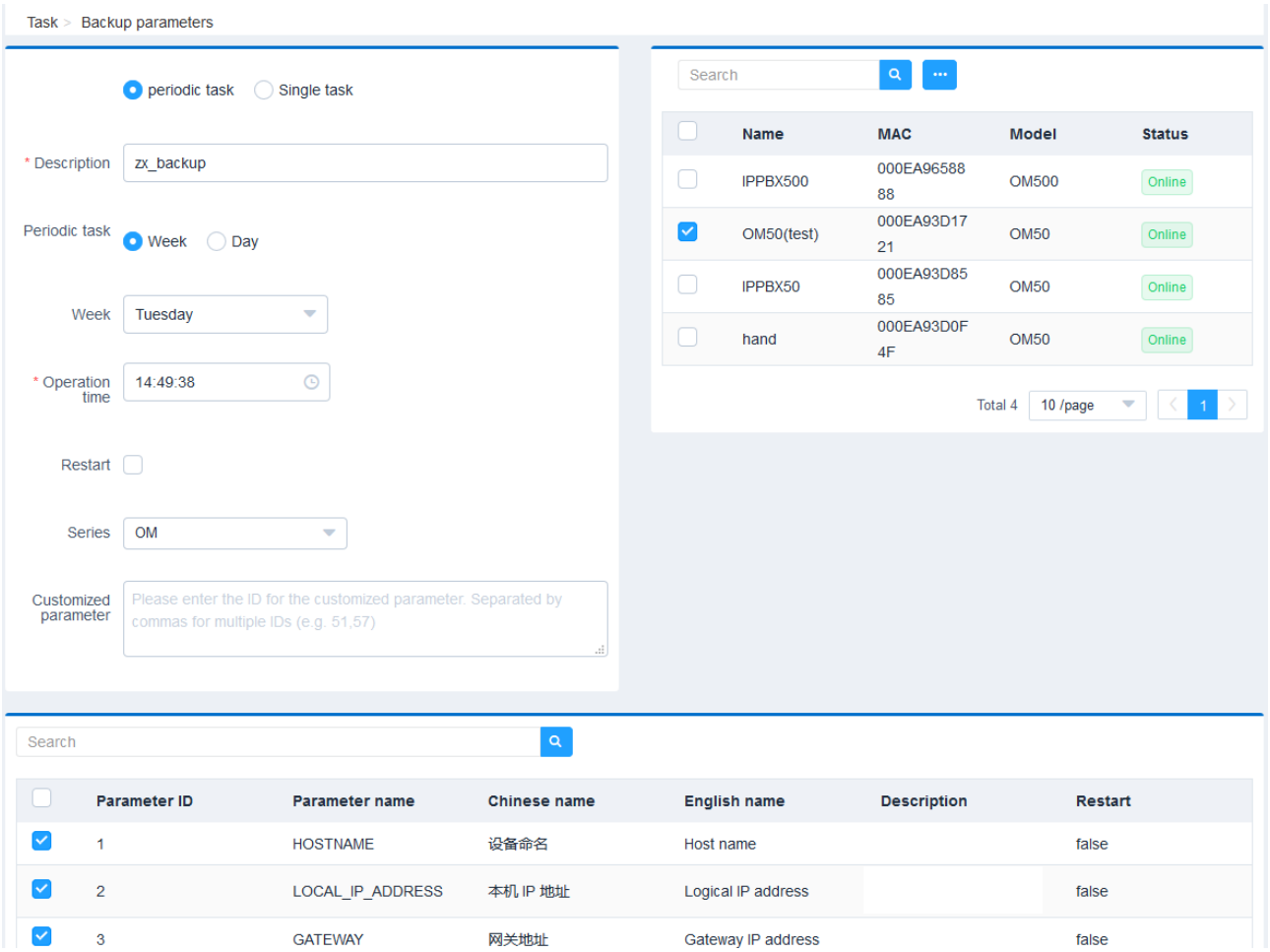
Back up parameters

Go to **Task** > **Backup parameters** page.

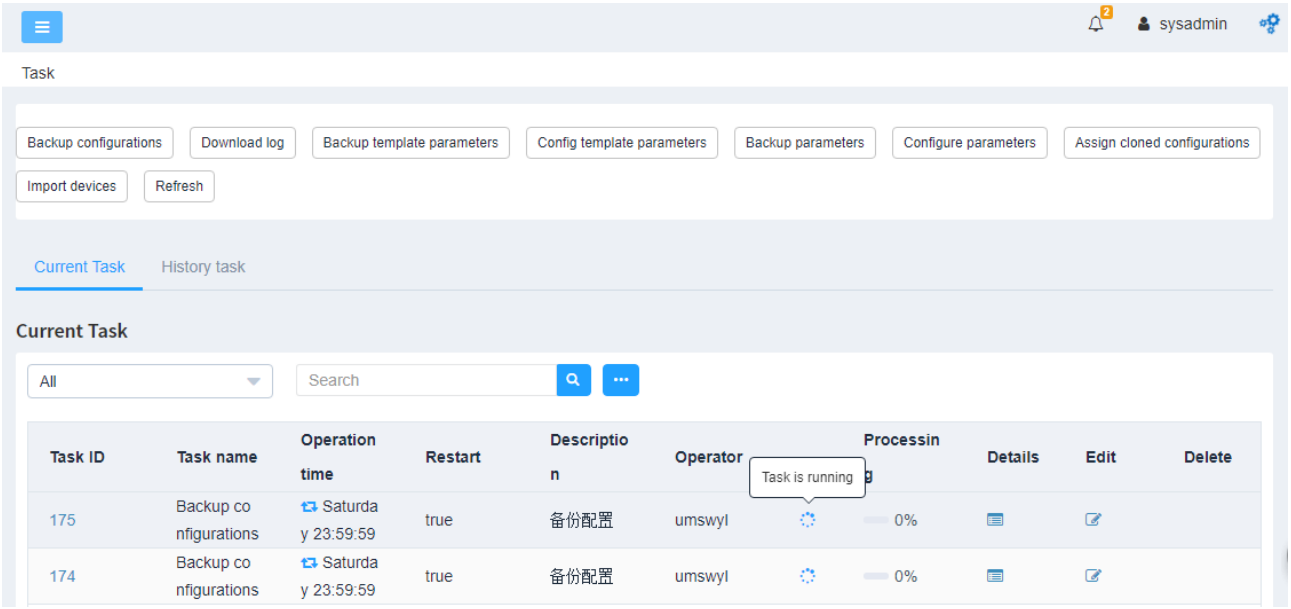
You can make a backup of the parameters as follows:

1. Input the description for the task to back up parameters.
2. From the list on right, choose the devices whose parameters will be backed up.
3. From the list on the bottom, choose the parameters to be backed up.
4. Click **Save**. Then a task to back up parameters has been created.

Copyright © New Rock Technologies, Inc



5. All tasks to back up parameters are contained in **Task** page. You can click the specific task ID to see details about the task, or click to start, stop or terminate the task. Once a task is terminated, it is removed from the task list and cannot be recovered.



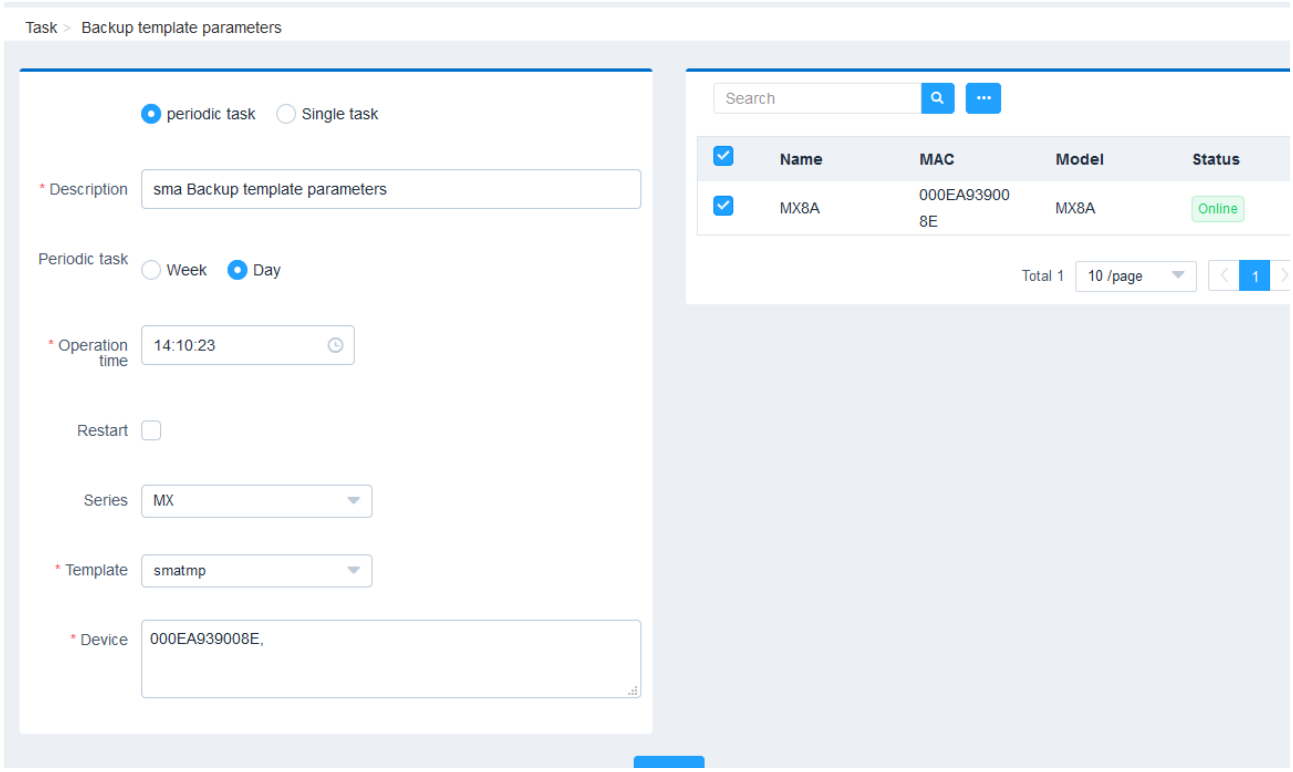
 Copyright © New Rock Technologies, Inc

Back up parameters by template

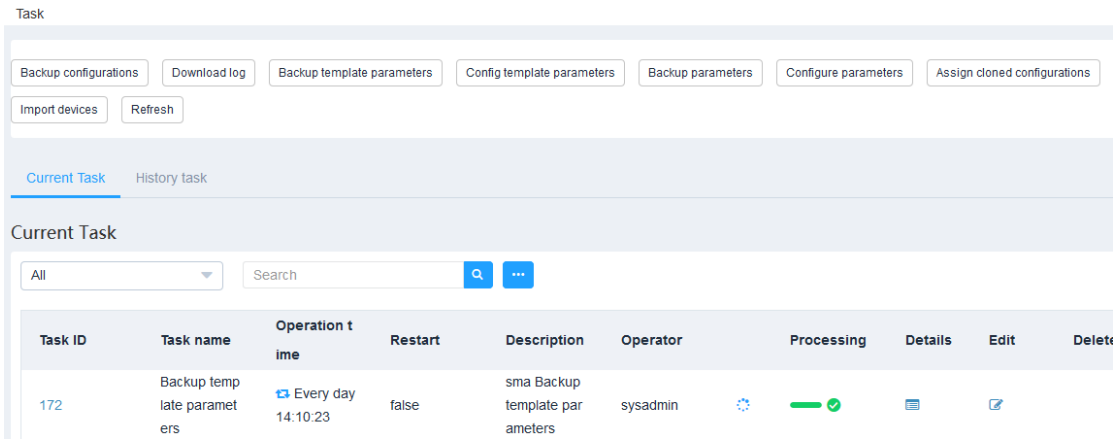
Go to **Task** > **Backup template parameters** page.

You can make a backup of the parameters as follows:

1. Input the description for the task to back up parameters.
2. Choose a template.
3. Choose the devices whose parameters will be backed up.
4. Click **Save**. Then a task to back up parameters by template has been created.

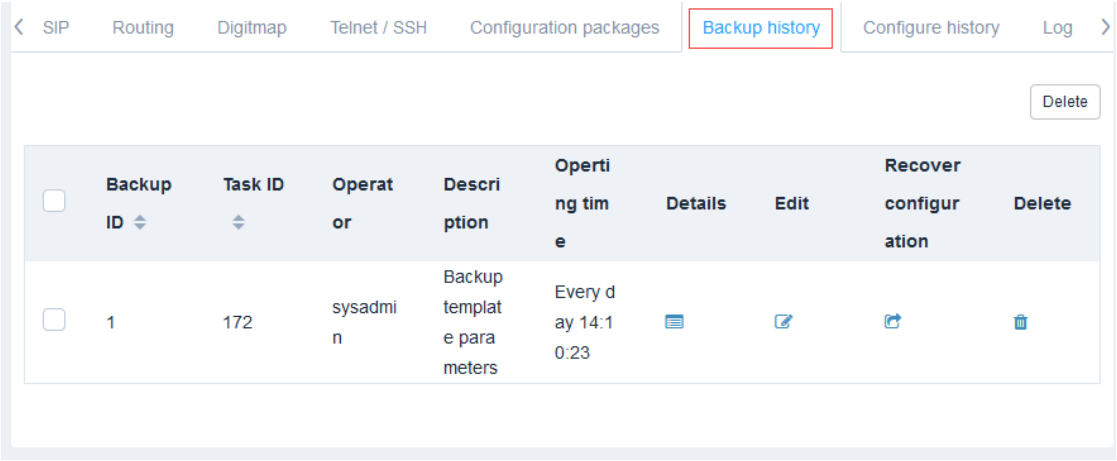


All tasks to back up parameters are listed in the **Task** page. You can click the task ID to see details about the task, or click to start, stop or terminate the task. Once a task is terminated, it is removed from the task list and cannot be recovered.



 Copyright © New Rock Technologies, Inc

To see parameter backup history, go to **Devices** > **Configure** page and click **Backup history**.



5.3 Provision parameters

You can modify multiple devices' configurations at the same time by provisioning parameters.

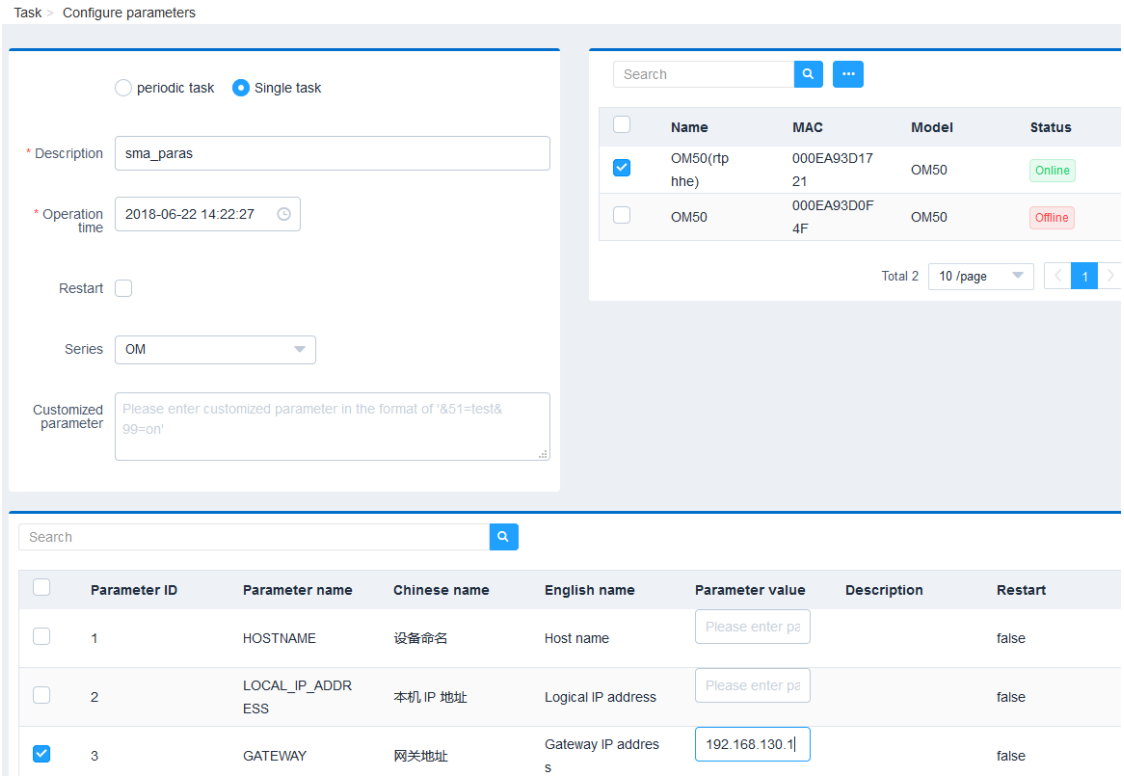
Provision parameters

Go to **Task** > **Provision parameters** page.

You can provision parameters as follows:

1. Input the description for the task to provision parameters.
2. Choose the devices to whom the parameters will be provisioned.
3. Choose the parameters to be provisioned. Remember to preset values for the parameters.
4. Click **Save**. Then a task to provision parameters has been created.

Copyright © New Rock Technologies, Inc



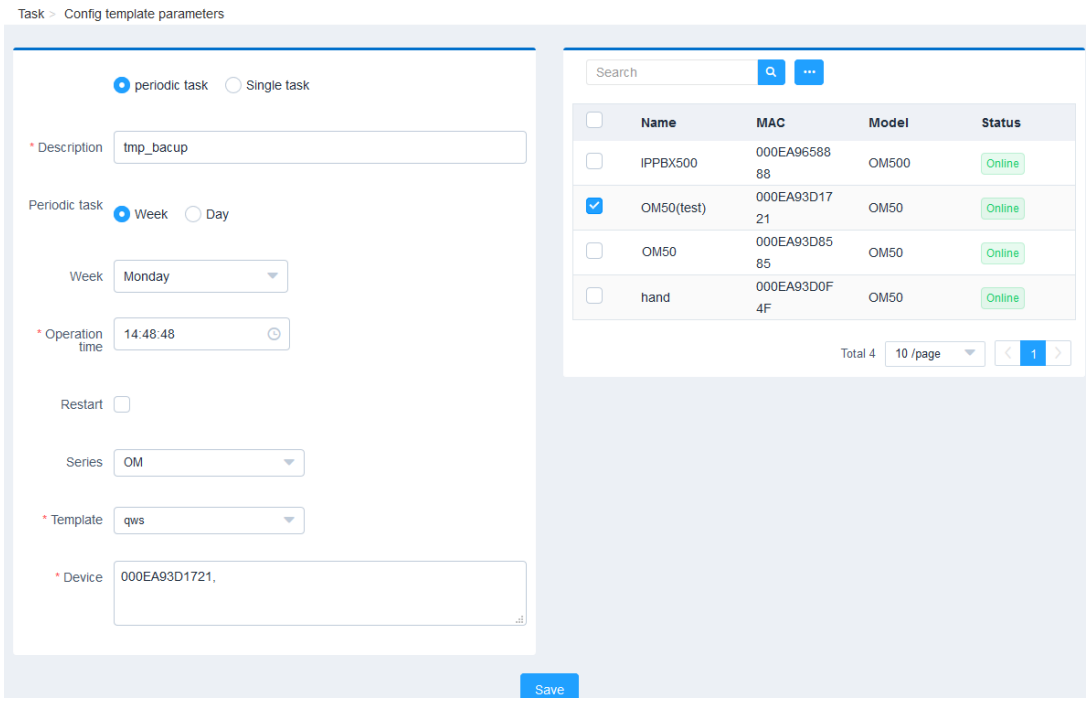
Provision parameters by template

Go to **Task** > **Config tempelate parameters** page.

You canprovision parameters as follows:

1. Input the description for the task to provision parameters.
2. Choose a template. Remember to preset values for the parameters in the template first.
3. Choose the devices to whom the parameters will be provisioned.
4. Click **Save**. Then a task to provision parameters of a specified template has been created.

Copyright © New Rock Technologies, Inc

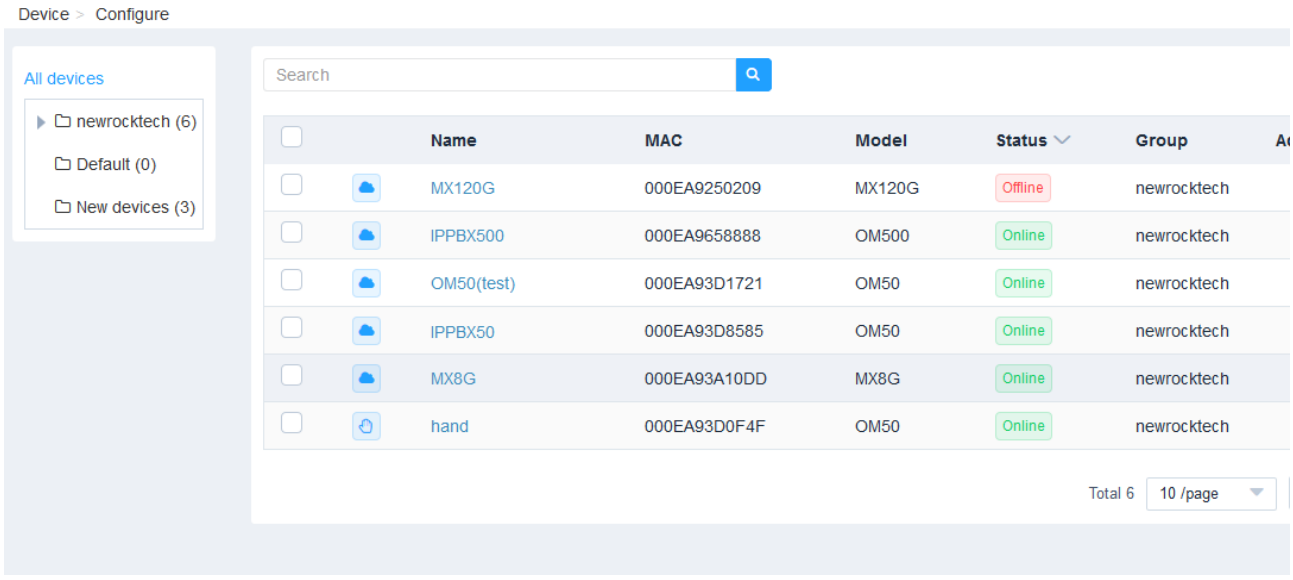


5.4 Back up configuration package

Note: a configuration package only contains voice related configurations (not contain network related configurations.)

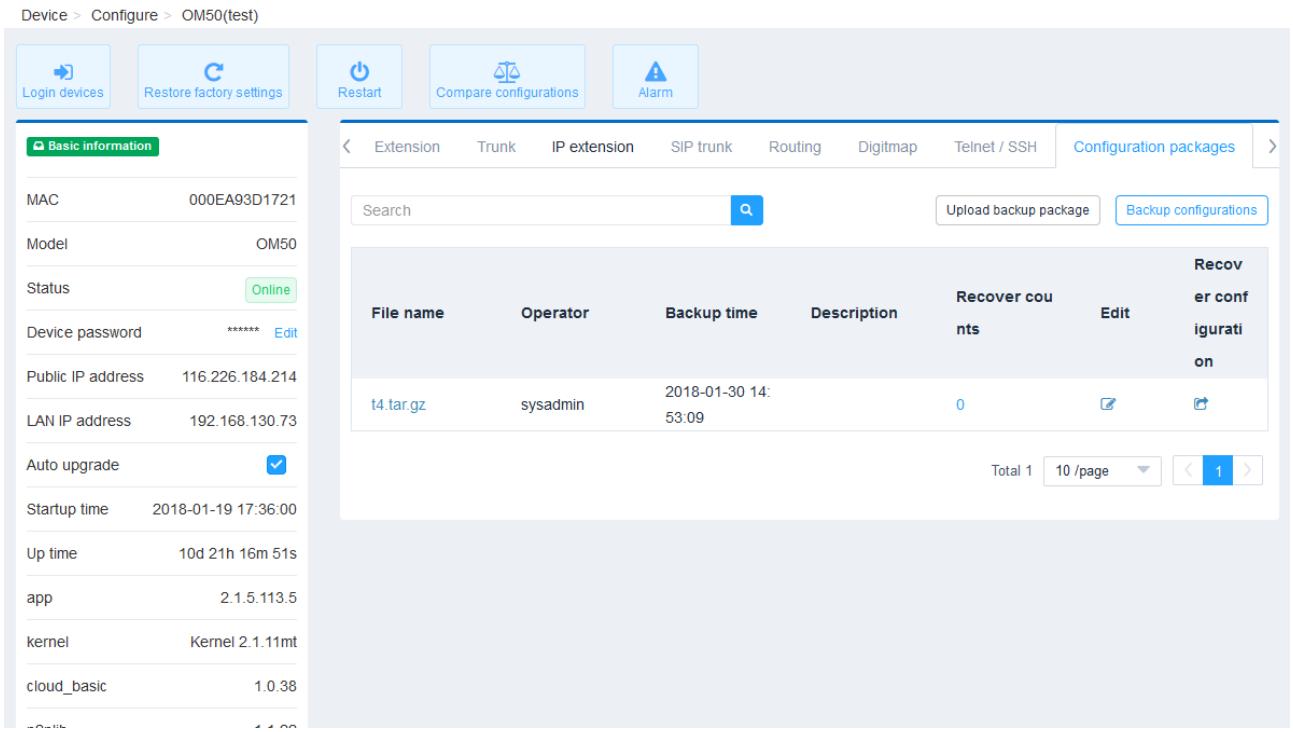
Back up the configuration package for a single device

1. Go to **Device>Configure** page, click a specific device name.



2. Open **Configuration packages**, then you can back up configurations, upload configuration packages, or provision configurations.

 Copyright © New Rock Technologies, Inc



- Click **Backup configurations** to back up the current configurations of the device to the UMS. The backed up configuration package will be listed below, and you can download the package by clicking the file name.
- Click **Upload backup package** to upload configuration packages to the UMS.

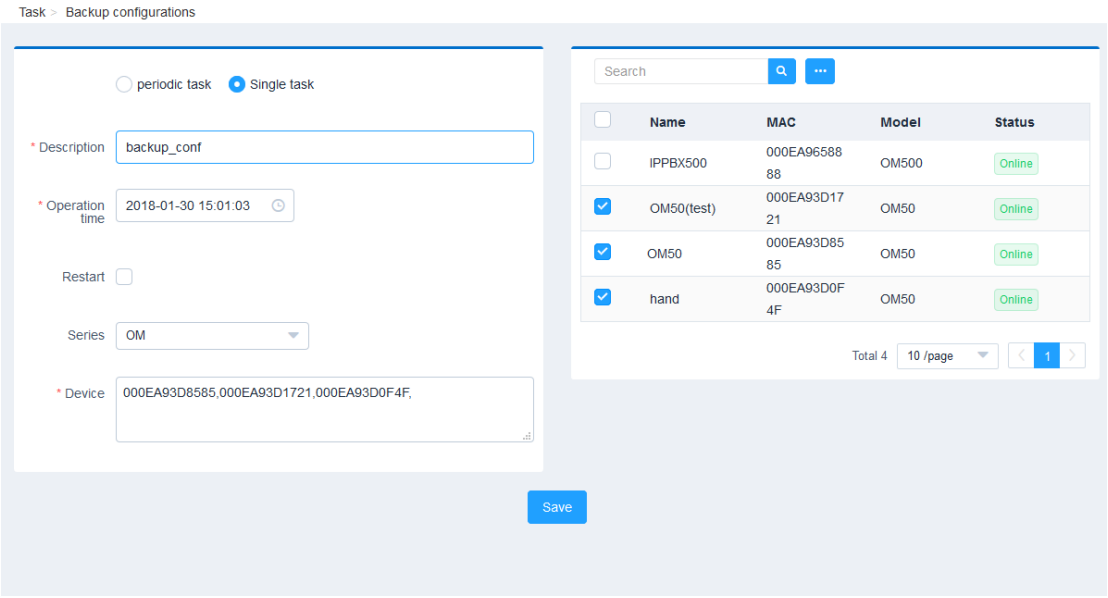
Back up configuration packages for multiple devices

Go to **Task** > **Backup configurations** page.

You can make a back up of the configuration packages as follows:

1. Input the information for the task to back up configuration packages.
2. Choose the devices whose configuration packages will be backed up.
3. Click **Save**. Then a task to back up configuration packages has been created.

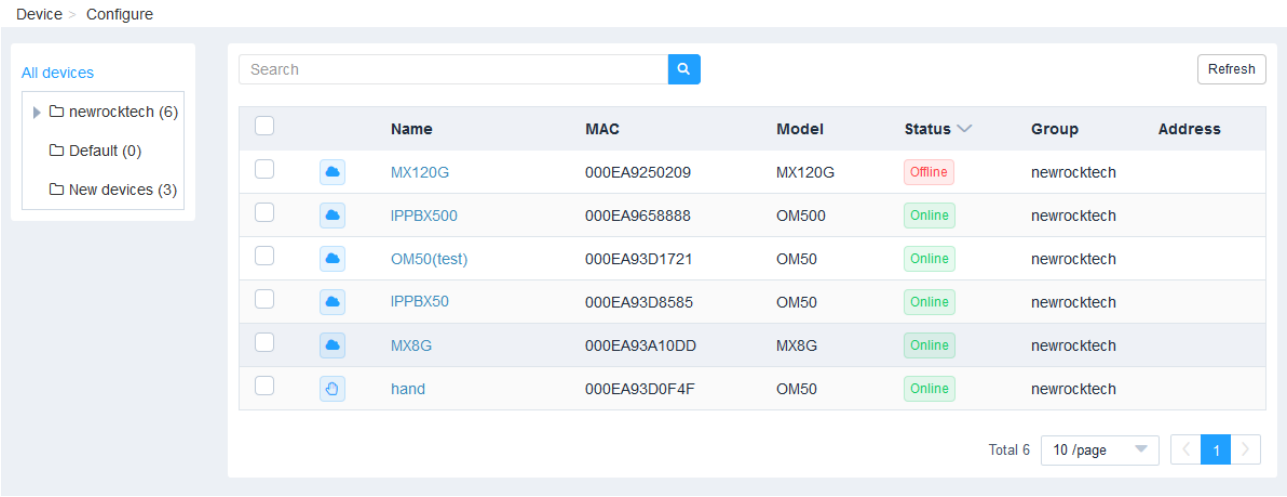
Copyright © New Rock Technologies, Inc



5.5 Provision configuration packages

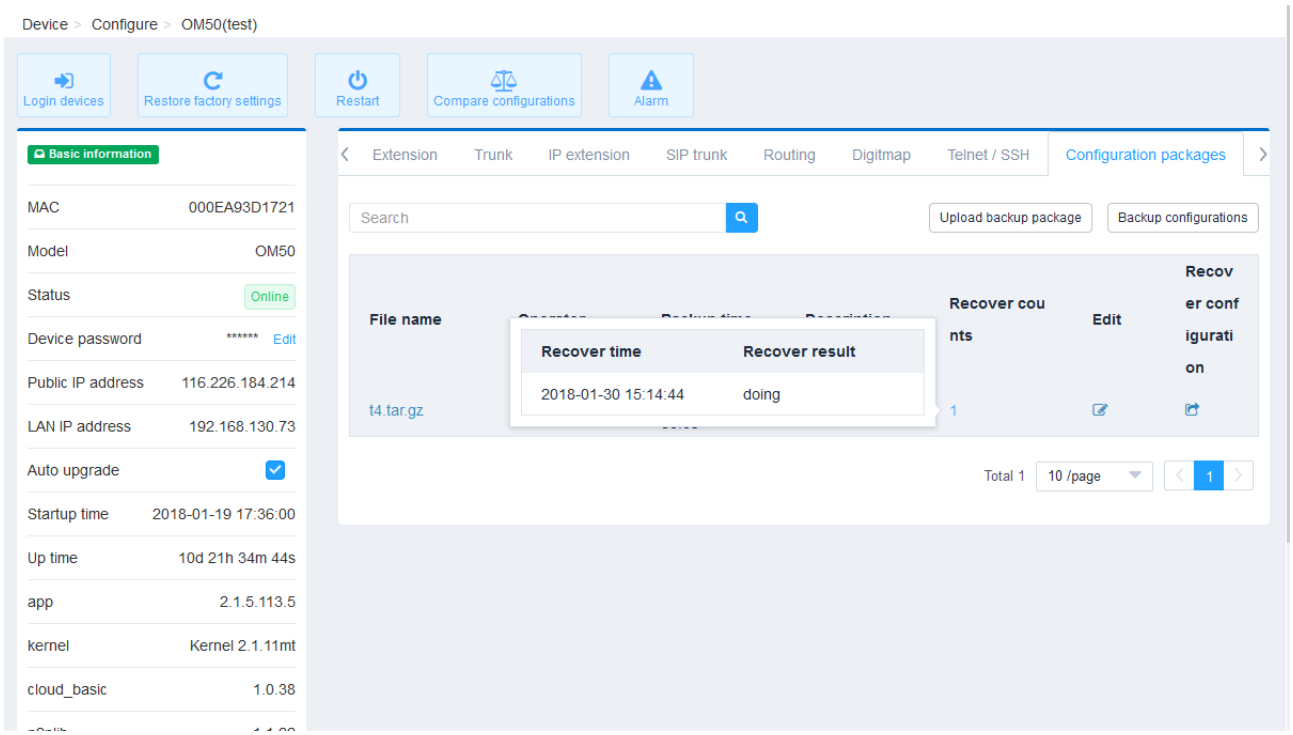
Attention: It is only allowed to provision the device's own configuration package.

Go to **Device** > **Configure** page, click the target device name to which the configuration package will be provisioned.



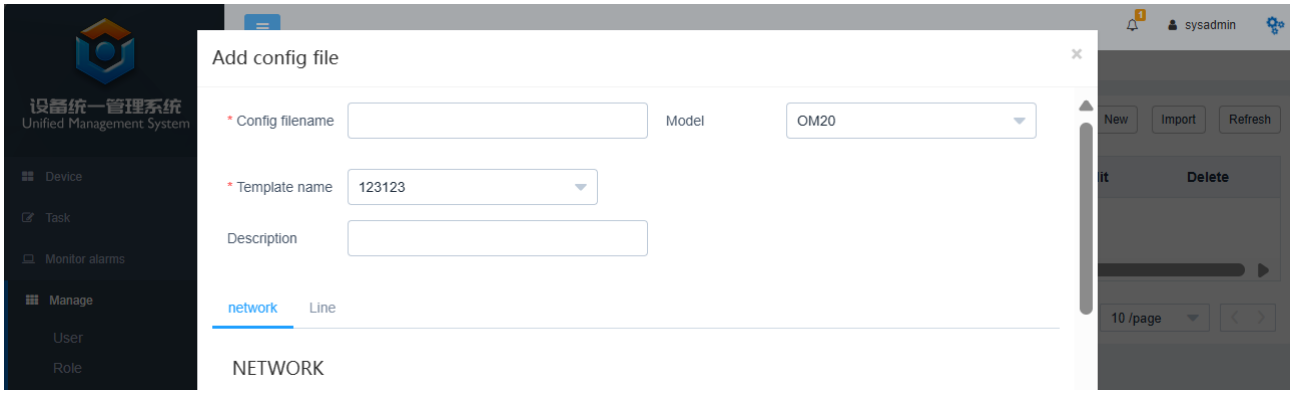
- Go to Configuration packages, and click to provision configurations. Then you can see the result by clicking the **Recover counts**.

Copyright © New Rock Technologies, Inc



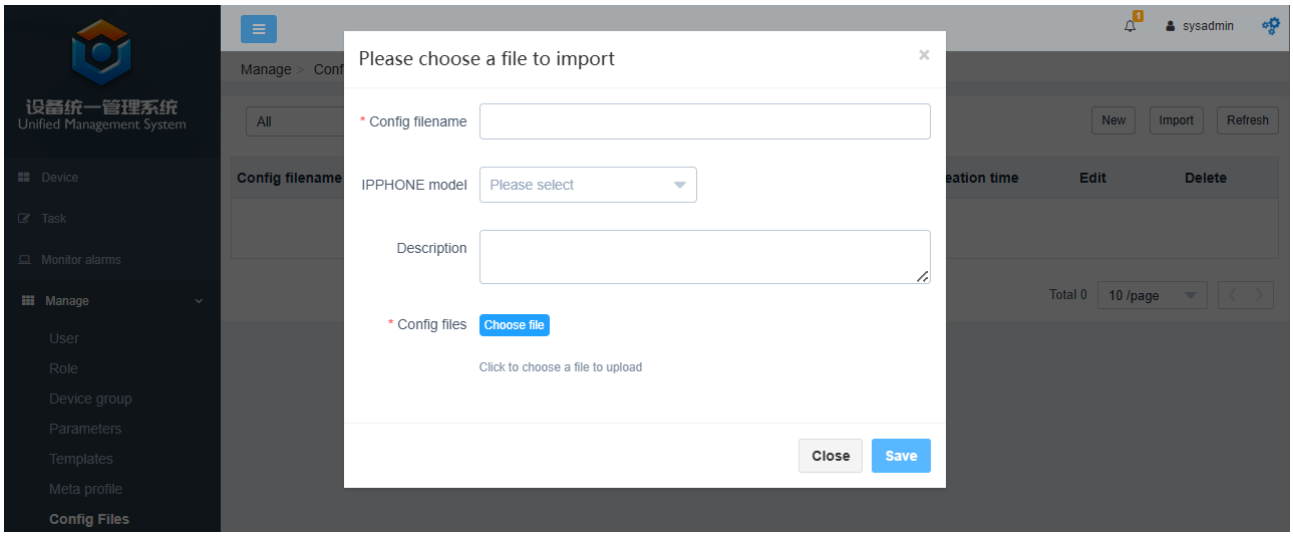
5.6 Configuration management

Navigate to Admin > Configuration Management, the Configuration Management module is used to create, manage and import configuration files for devices.



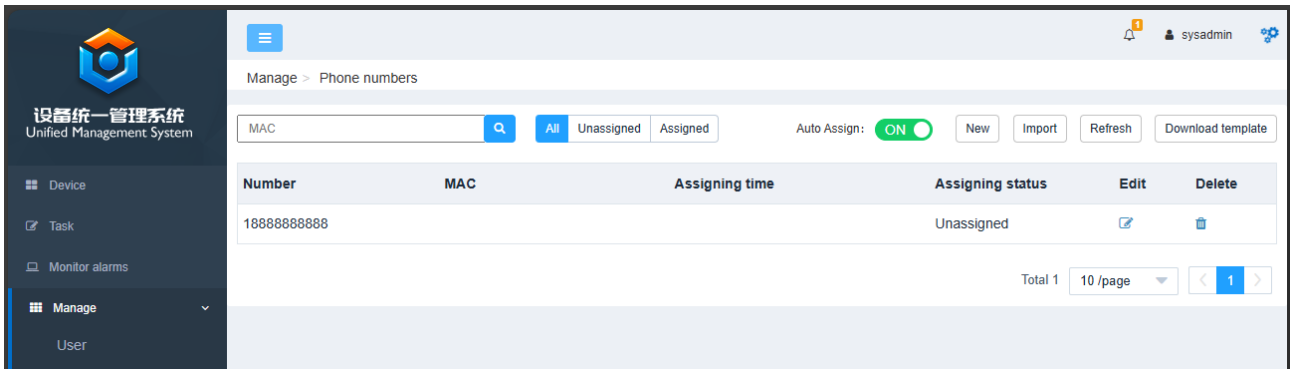
 Copyright © New Rock Technologies, Inc

Import file



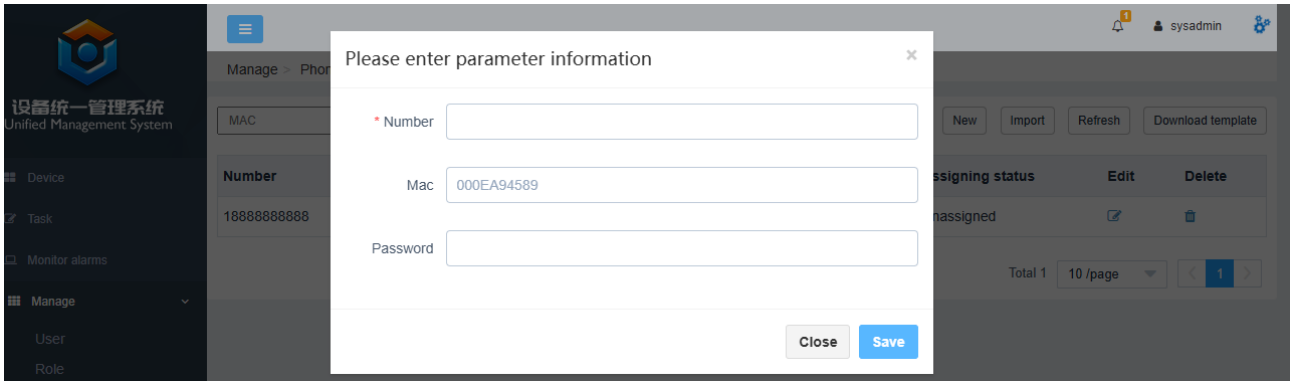
5.7 Number resource

Navigate to Manage > Phone numbers, the Number Resource Module is used to manage and allocate the phone number resources of the device, supporting manual and automatic allocation modes. The administrator can check the allocation status of numbers, search devices by MAC address, and batch import number data to improve the efficiency of device configuration.



 Copyright © New Rock Technologies, Inc

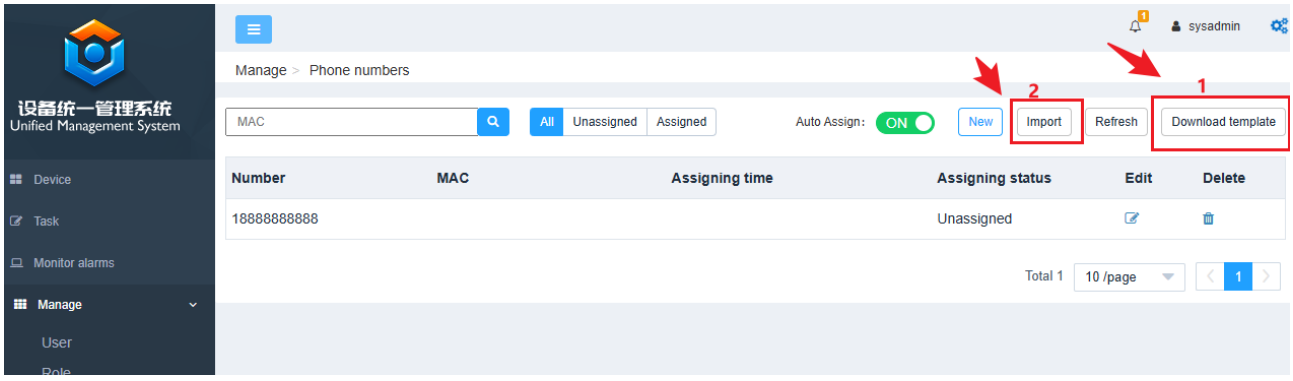
Add



Item	Definition
Number	Enter the phone number to be assigned
MAC Address	MAC address of the device
Password	Associated Passwords

Batch import

Click to download the template to support batch configuration of numbers, MAC addresses and passwords.



Copyright © New Rock Technologies, Inc

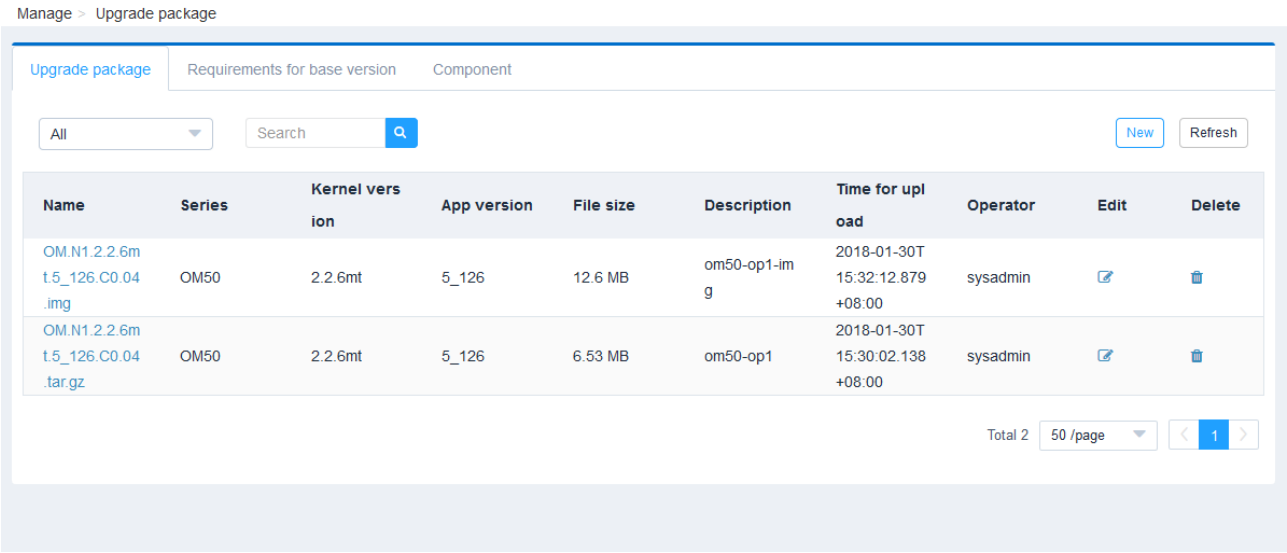
6 Upgrade devices

It will not modify the configurations of devices when you perform upgrades.

6.1 Manage upgrade packages

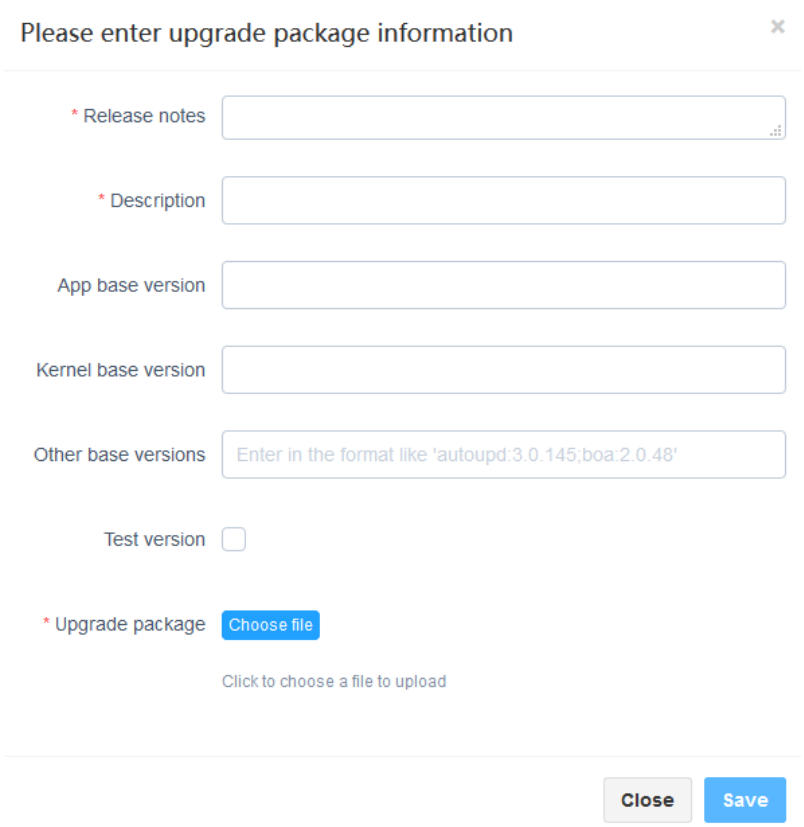
Upload upgrade packages

Go to **Manage**> **Upgrade package**, and click **New**.



Input necessary information for the upgrade package, and click **Choose file** to choose a configuration package and upload it to UMS.

 Copyright © New Rock Technologies, Inc



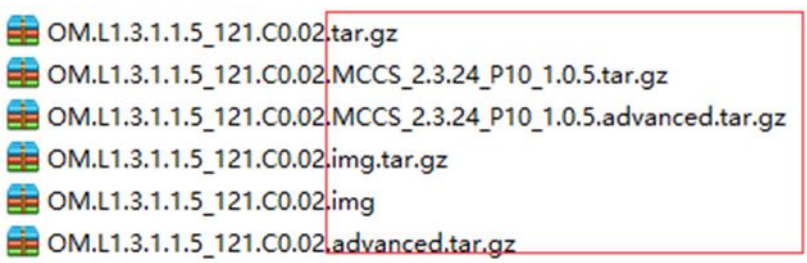
Description for some parameters:

- Base version: the lowest version from which the device can upgrade to the version of the upgrade package.

In addition, you can also set a base version for a device model on **Manage** > **Upgrade package** > **Requirements for base version** page.

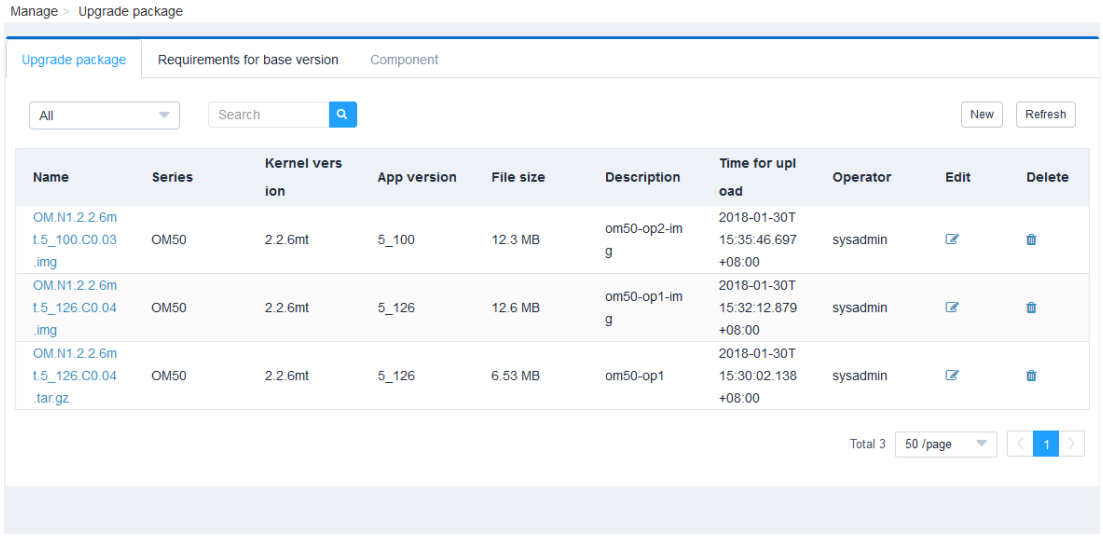
This higher version of these two base version will be take effect.

- Upgrade packages: the UMS supports six types of upgrade packages. Each type has its own file extension shown as below:



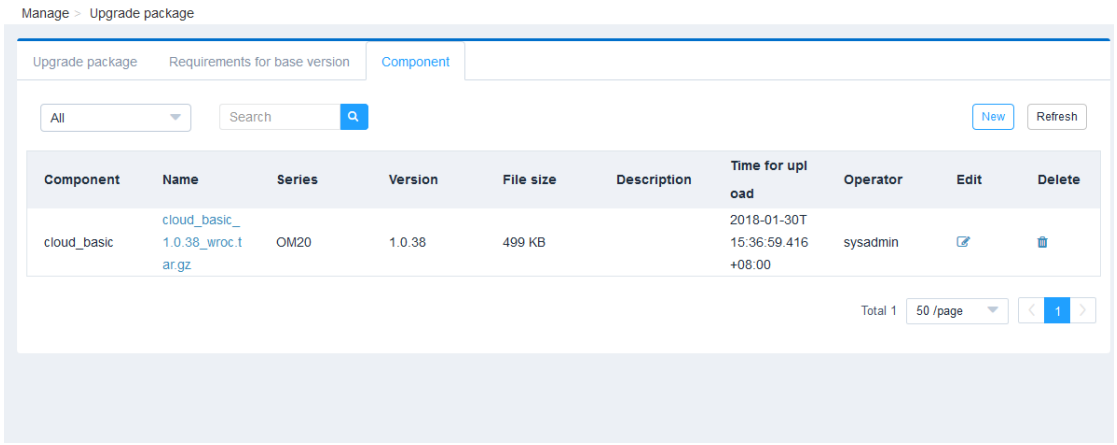
- Test version: Tick it if the upgrade package that you will upload is for test. In addition, you have to add the parameter TESTFLAG=1 to the autoupd.ini of the device.

 Copyright © New Rock Technologies, Inc



Upload upgrade packages for components

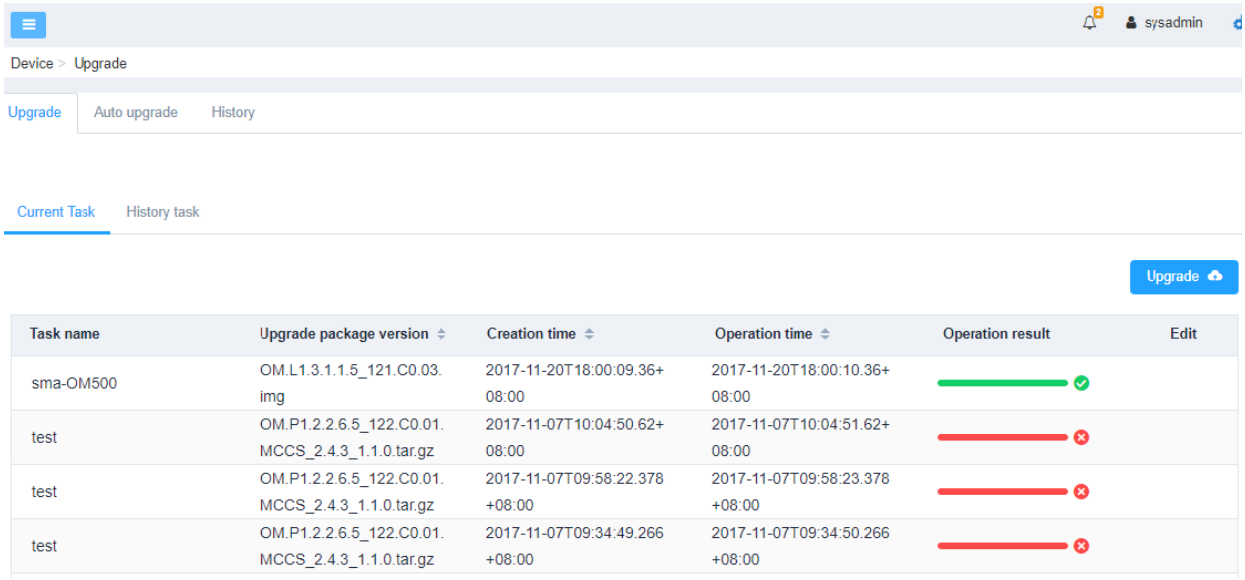
Go to **Manage**> **Upgrade package**>**Component**, and click **New** to upload upgrade package for components**.**



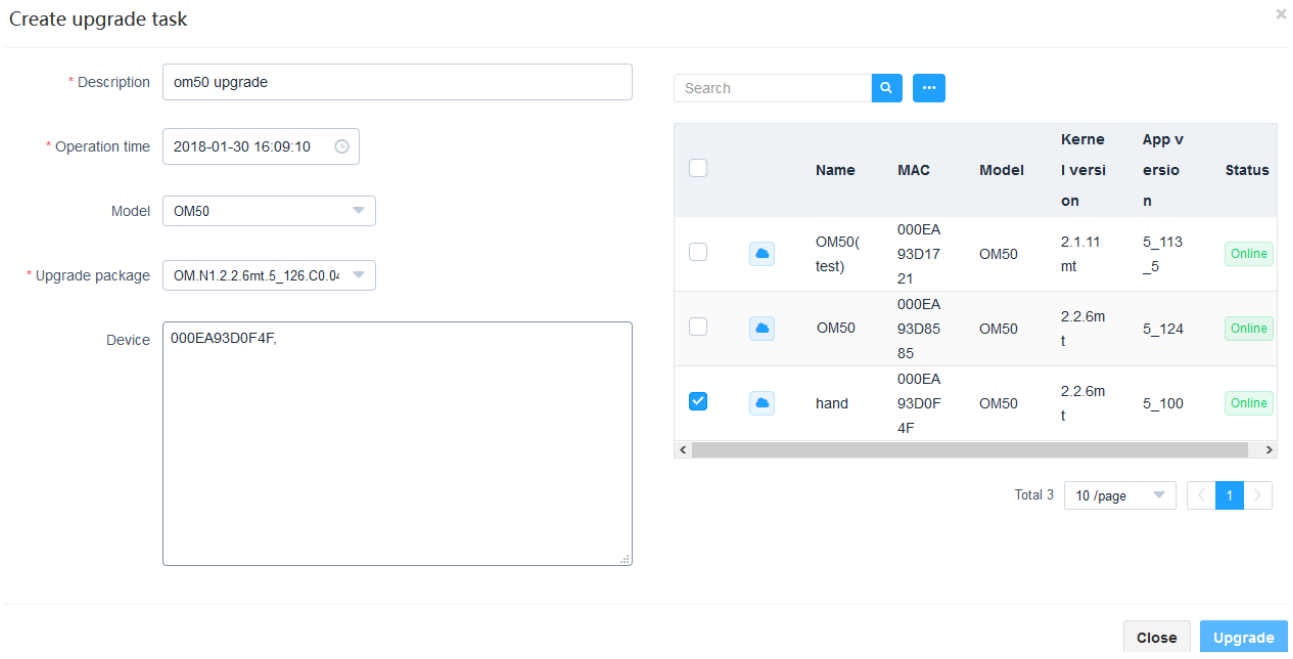
 Copyright © New Rock Technologies, Inc

6.2 Upgrade manually

1. Go to **Device** > **Upgrade** page, click Upgrade button to add an upgrading task.



2. Input necessary information for the task.

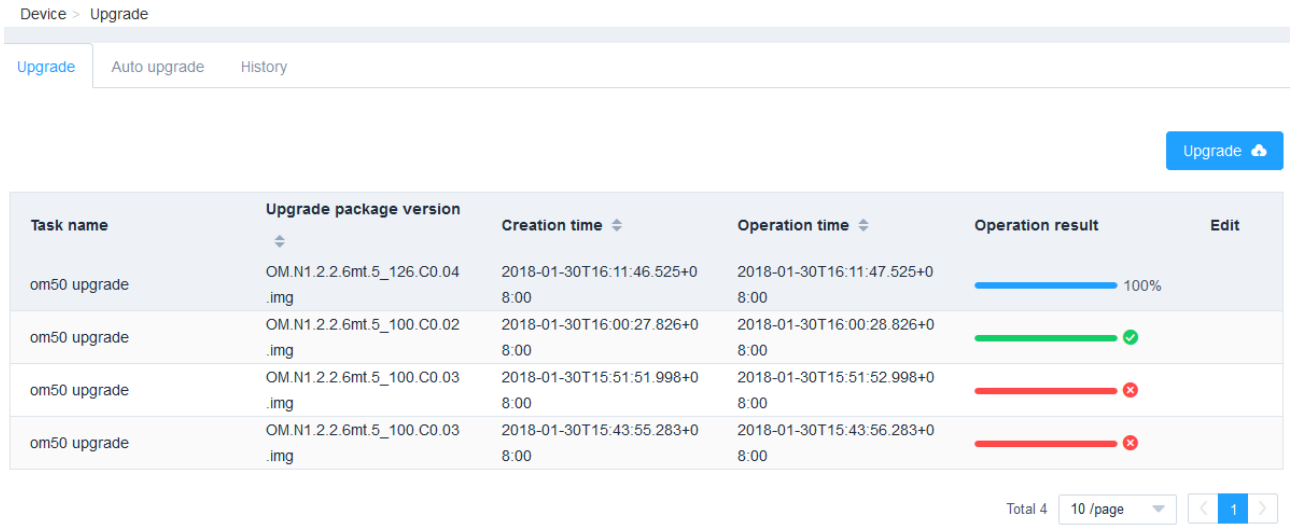


Description for a part of parameters:

- Operation time: It decides the time to perform the upgrading task.
- Model: Choose the device model to be upgraded.
- Device: choose from the list in the right side or enter the device's MAC address manually.

Copyright © New Rock Technologies, Inc

3. After the upgrade task is created, it will be displayed in the **Device** > **Upgrade** > **Upgrade** page.



Description for upgrading status:

- Green bar indicates that the upgrade is successful
- Red bar indicates that it failed to upgrade
- Blue bar 0% indicates that it is waiting to upgrade
- Blue bar (25%, 50% or 70%) indicates that the upgrade process is in progress
- Blue bar (100%) indicates that the upgrade task has been completed but there are several devices failed to upgrade.

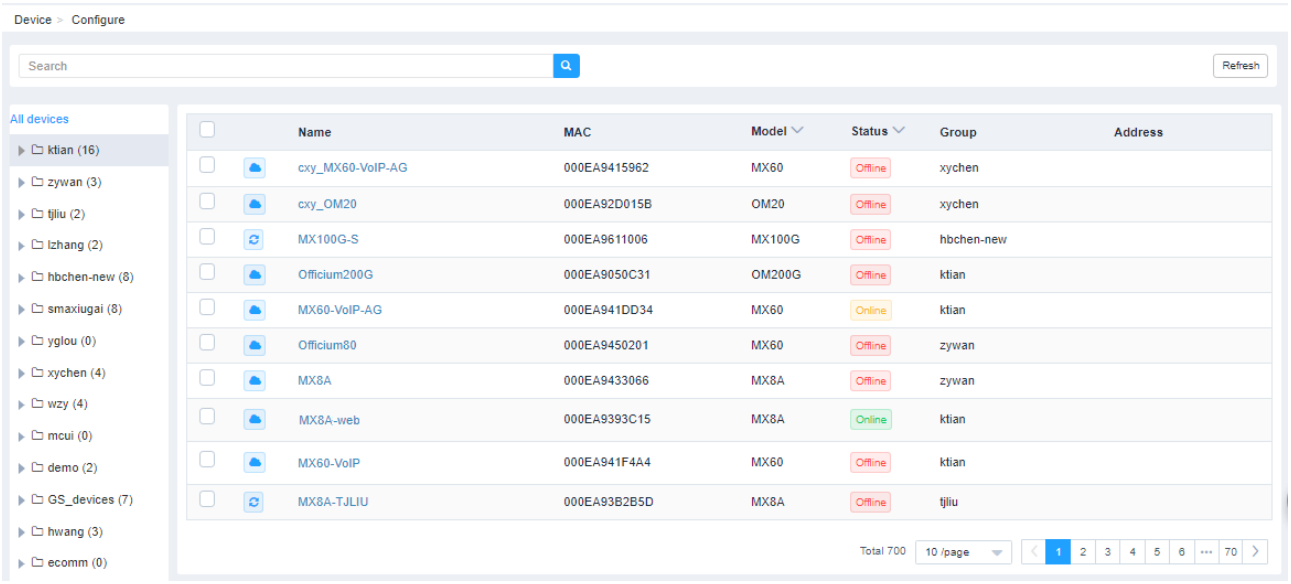
Copyright © New Rock Technologies, Inc

6.3 Upgrade automatically

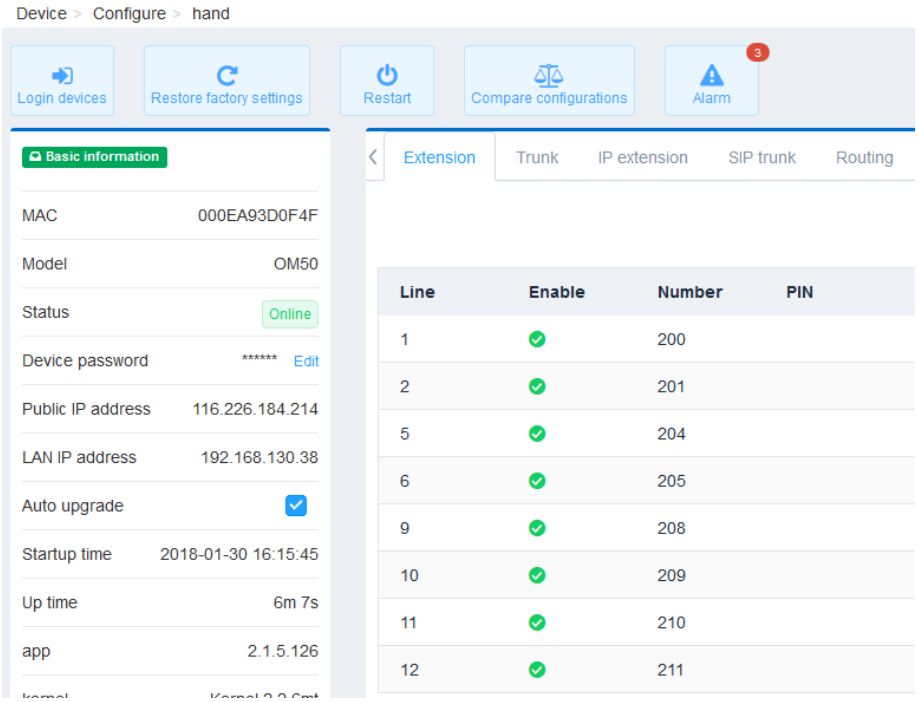
After you enable the auto upgrade function for the device, the device will automatically upgrade once the UMS has a later version compared to the device's current version.

Do as follows to enable auto upgrade for a device:

1. Go to **Devices>Configure** page, and click a specific device name.

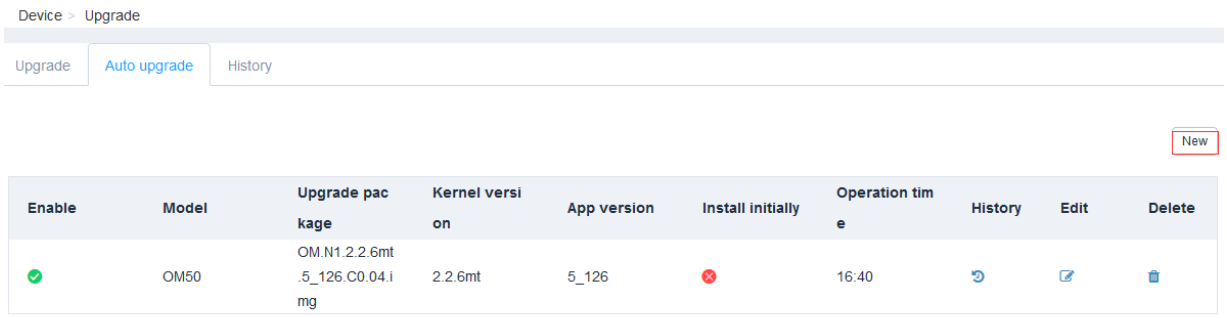


2. Tick the check box for **Auto upgrade**.

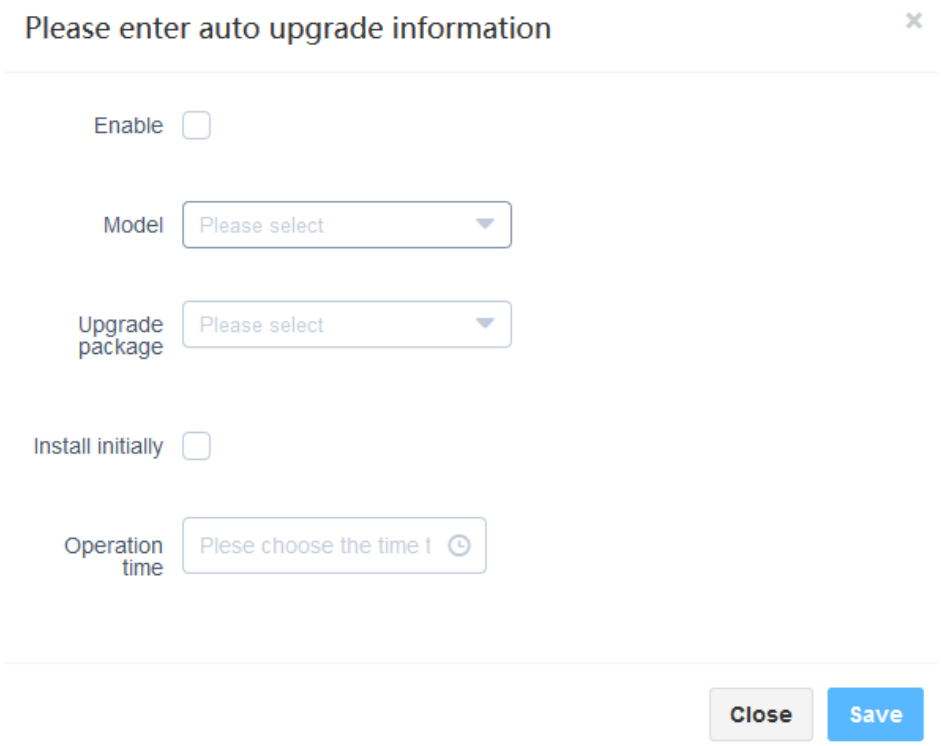


3. Go to **Device** > **Upgrade** > **Auto upgrade**, and click **New** to create an upgrading task.

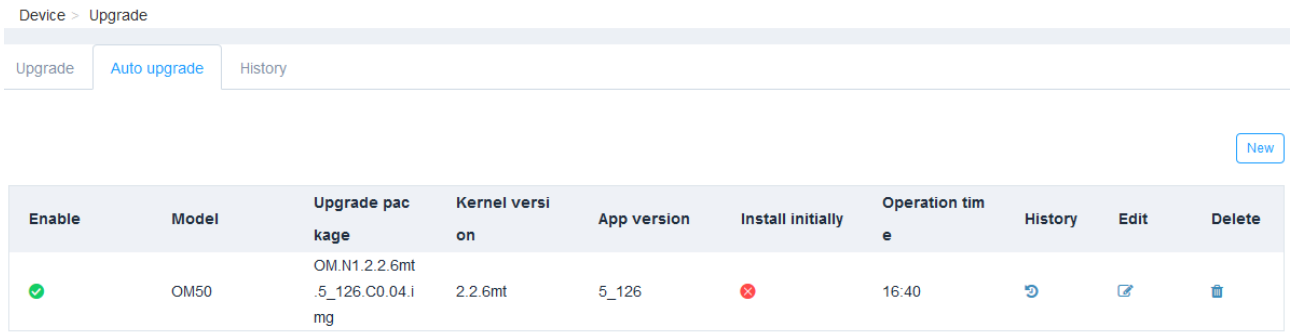
Copyright © New Rock Technologies, Inc



4. Input necessary information for the task, and click **Save**.



5. After the task is created, it will be listed in the page.



The device will periodically request UMS to upgrade. An auto upgrade will be activated when all the following three conditions happen:

 Copyright © New Rock Technologies, Inc

- The check box of **Auto upgrade** for the device is ticked and the upgrade task is enabled.
- The time preset for the auto upgrade is up.
- The component versions meet the lowest version requirements for Base version.

It is allowed to upload two types of upgrade packages for the same version. The device will use the package with the higher privilege:

- If the Kernel version of the device is lower than the one of the upgrade package, the six types are ordered from the highest privilege to the lowest privilege as follows:

OM.N2.xxx.xxx.xxx.img.tar.gz

OM.N2.xxx.xxx.xxx.img

OM.N2.xxx.xxx.xxx.MCCSxxx.advanced.tar.gz

OM.N2.xxx.xxx.xxx.advanced.tar.gz

OM.N2.xxx.xxx.xxx.MCCSxxx.tar.gz

OM.N2.xxx.xxx.xxx.tar.gz

- If the Kernel version of the device is the same as the one of the upgrade package, the six types are ordered from the highest privilege to the lowest privilege as follows:

OM.N2.xxx.xxx.xxx.MCCSxxx.advanced.tar.gz

OM.N2.xxx.xxx.xxx.advanced.tar.gz

OM.N2.xxx.xxx.xxx.MCCSxxx.tar.gz

OM.N2.xxx.xxx.xxx.tar.gz

OM.N2.xxx.xxx.xxx.img.tar.gz

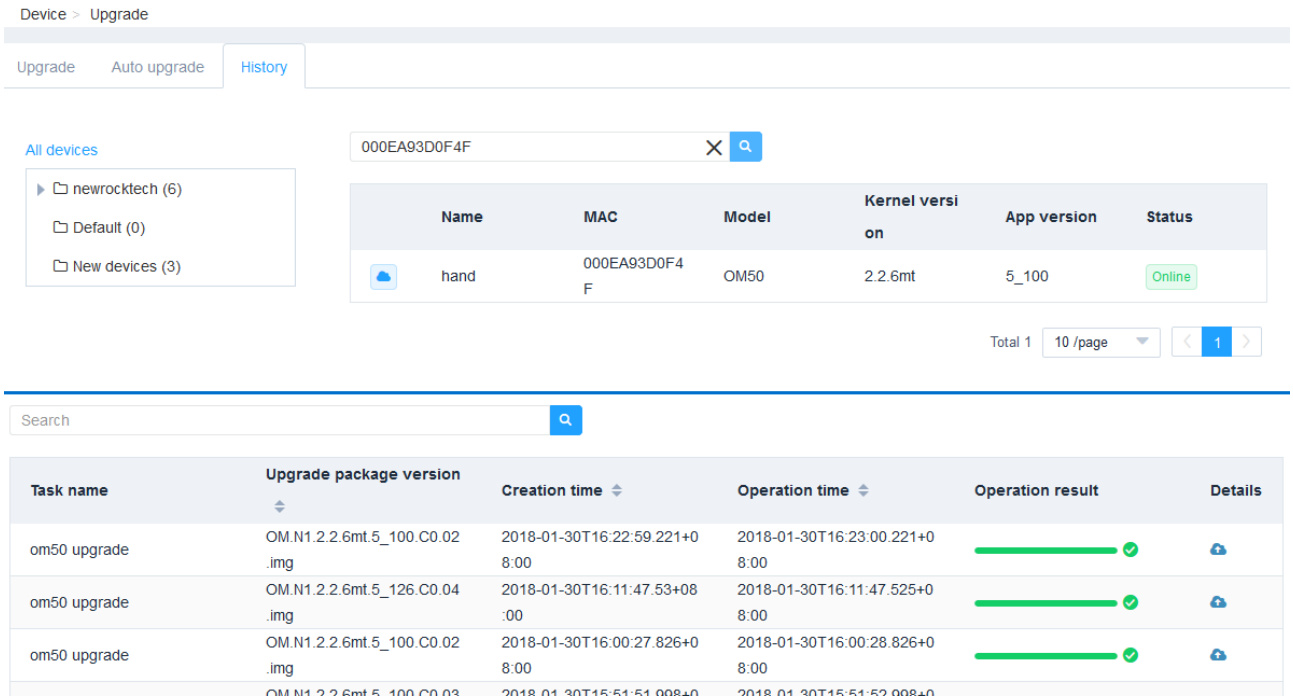
OM.N2.xxx.xxx.xxx.img

- If the Kernel version of the device is higher than the one of the upgrade package, the upgrade is forbidden.

 Copyright © New Rock Technologies, Inc

6.4 View upgrade history

Go to **Device** > **Upgrade** > **History** page, to view history of manual upgrade.

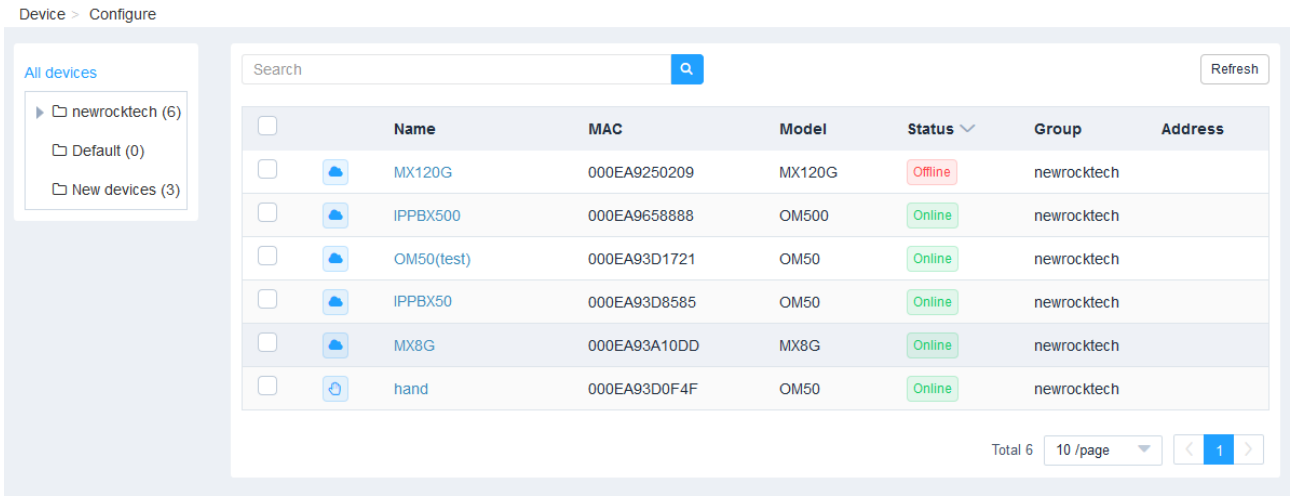


 Copyright © New Rock Technologies, Inc

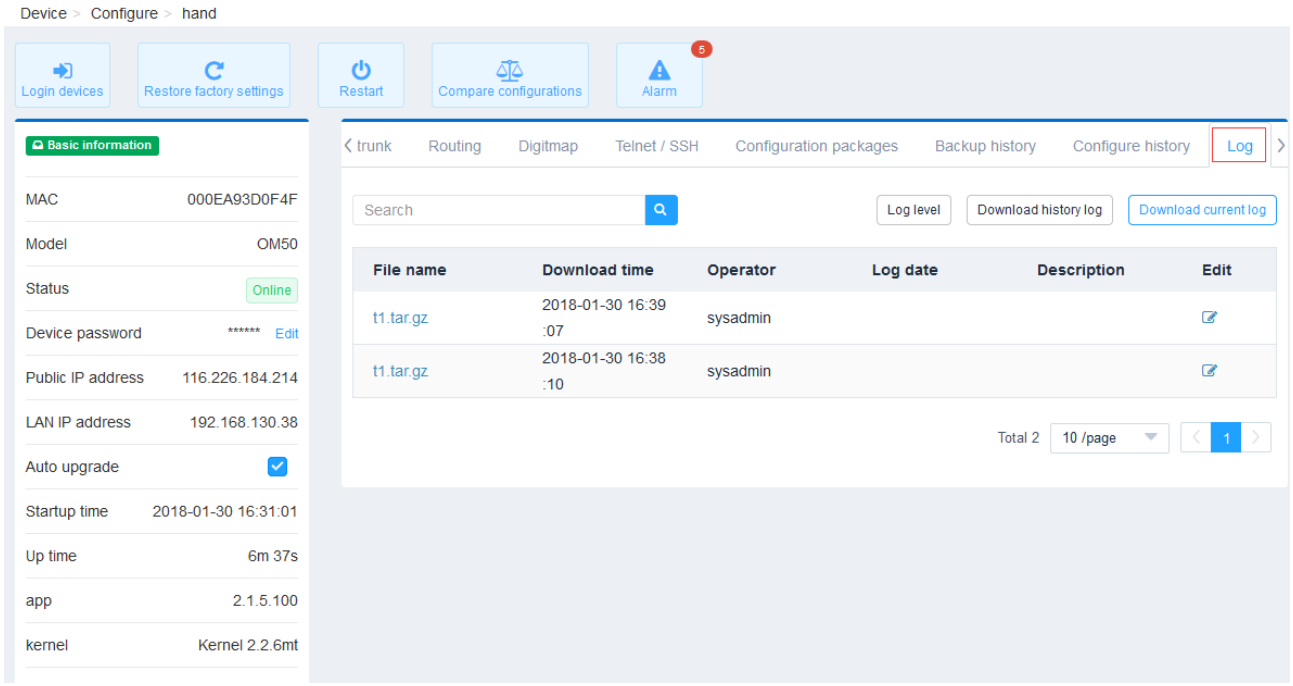
7 Logs of devices

7.1 Download logs of a single device

1. Go to **Device>Configure** page, click a specific device name.



2. Click **Log**, then click **Download history log** or **Download current log** to download logs from the device to UMS.

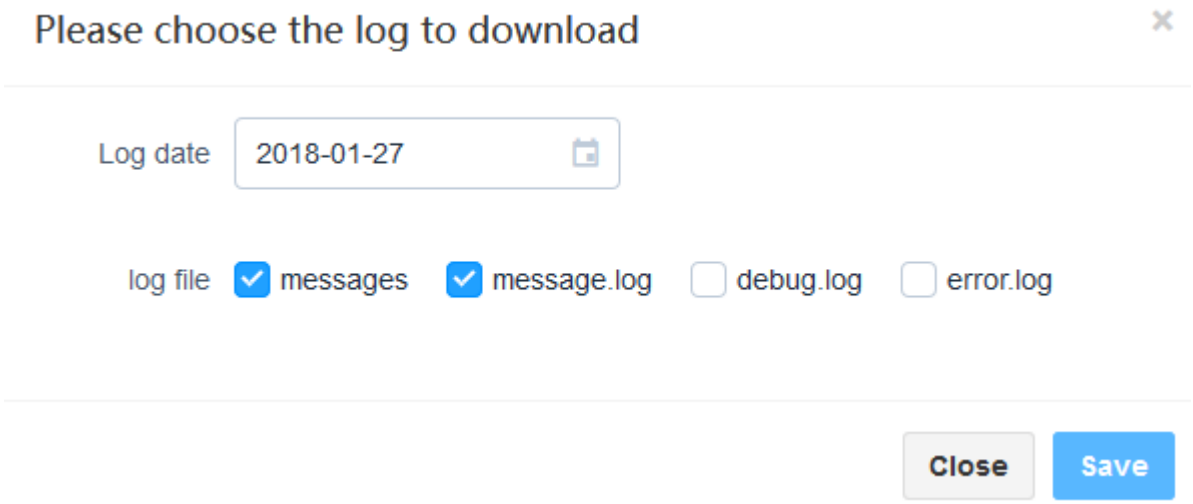


Description:

- Log level: set a level for logs, the higher the level is, the more detailed the logs will be.
- Download current log: click it to download the logs stored in the RAM of the device.

Copyright © New Rock Technologies, Inc

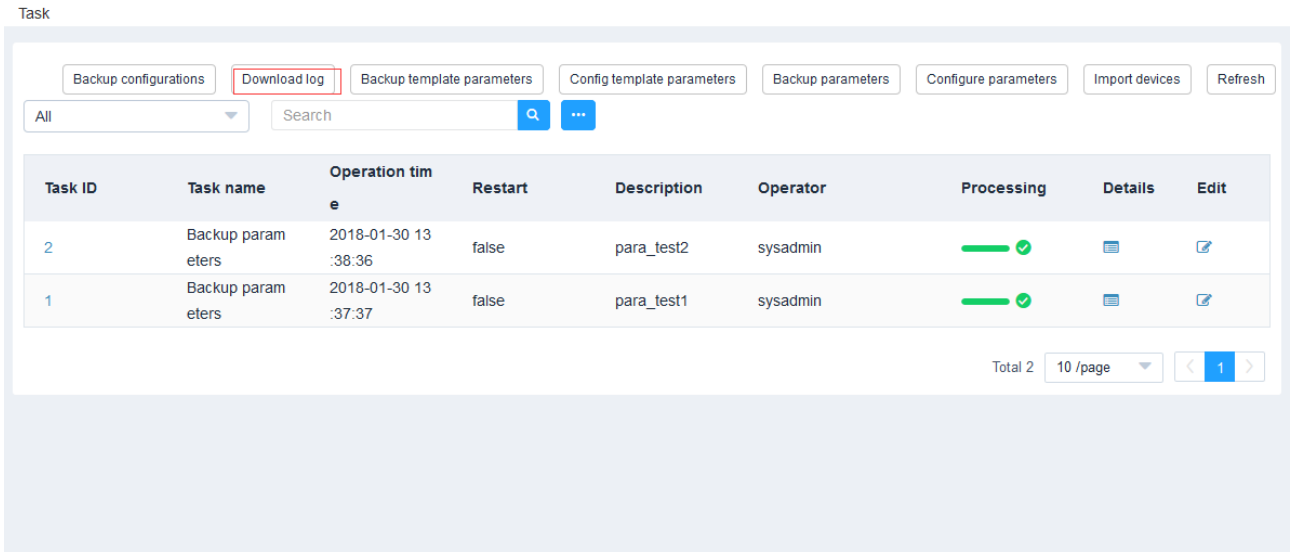
- Download history log: click it to download logs stored in the USB flash driver of the device. This function requires the device to be equipped with a USB flash driver and preset a script for auto backing up logs to the USB flash driver. To implement this, please contact our technical support.



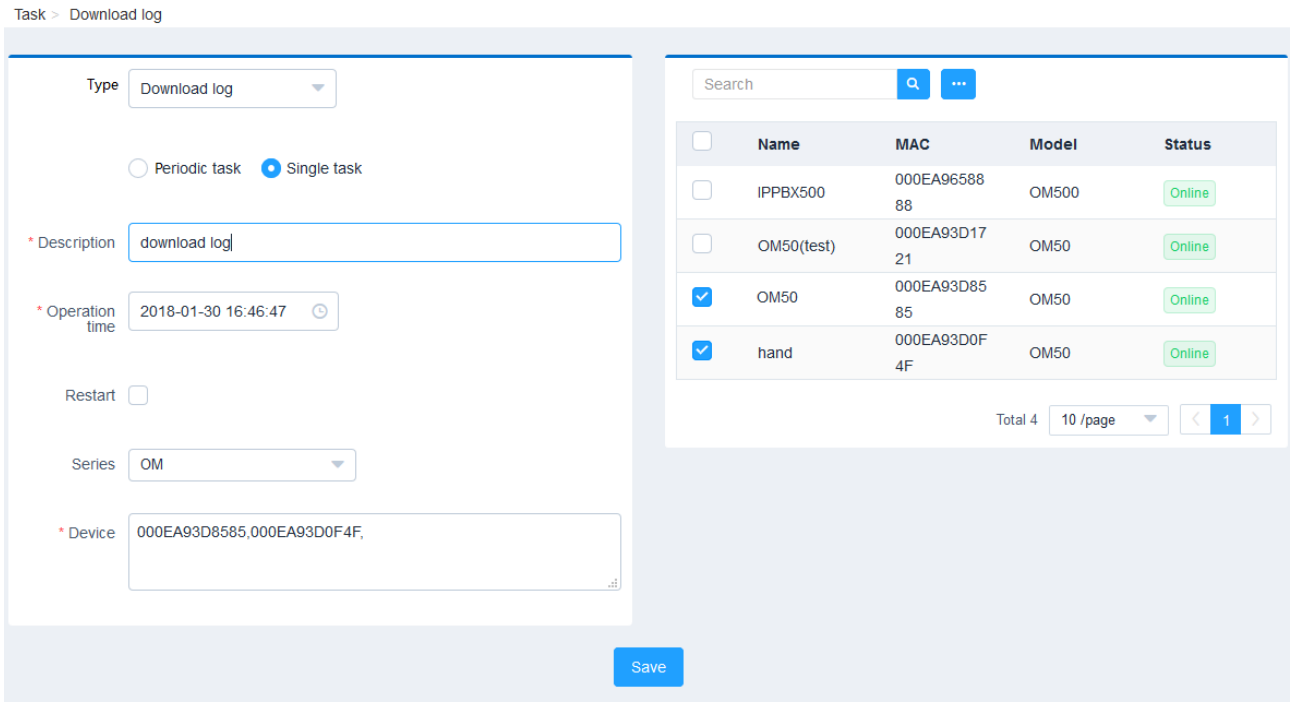
3. All downloaded logs can be found on the **Device** > **Configure** > **Device name**> **Log** page of the UMS. Then you can click the log file name to download it to your PC.

7.2 Download logs of multiple devices

1. Go to Task page, and click **Download log** to a task to down logs from devices to UMS.



 Copyright © New Rock Technologies, Inc



2. Input necessary information for the task, and click Save. Then the UMS will download logs from devices automatically.

Log type:

- Download log: Download the current logs.
- Download history log: Download the logs stored in the USB flash driver of the device.

 Copyright © New Rock Technologies, Inc

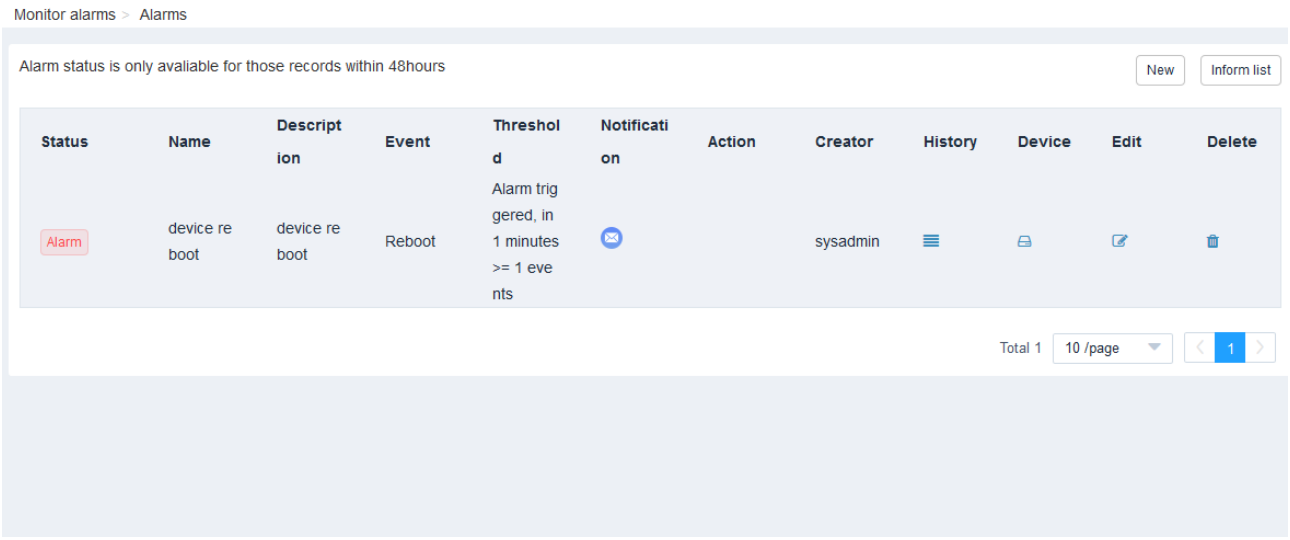
8 Monitor device alarms

8.1 Alarms

UMS can send security messages to preset mobile phones, WeChat IDs or Email addresses. You have to preset rules to define when the security messages will be sent.

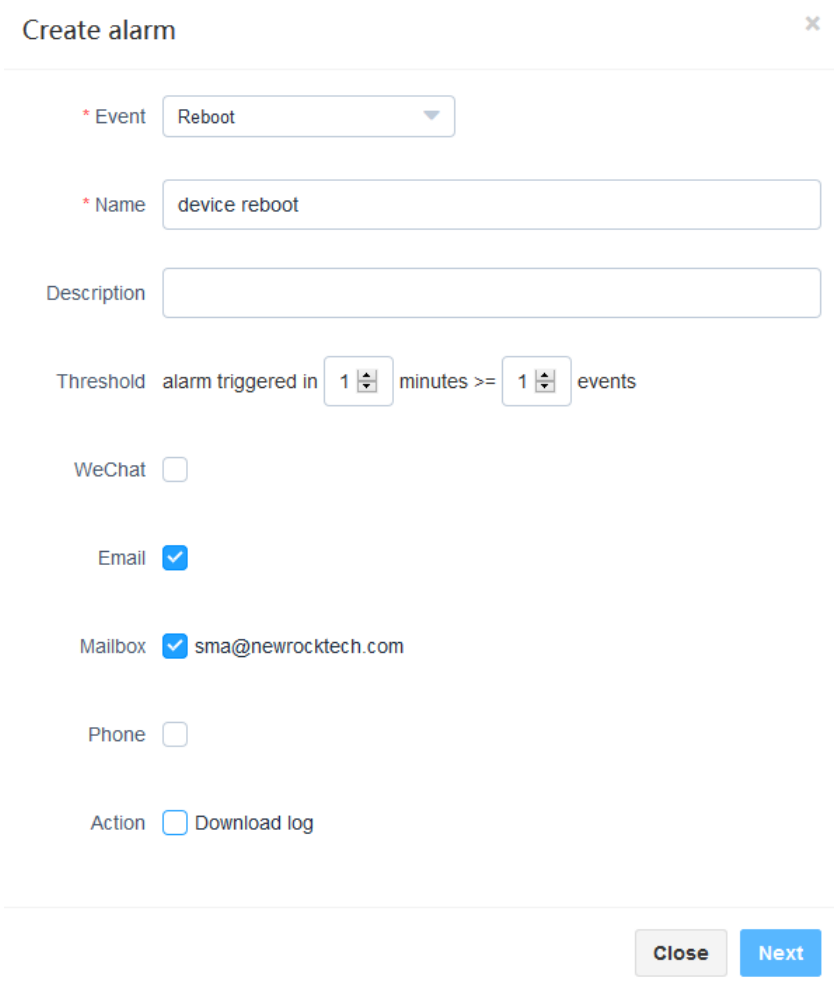
The procedure is as follows:

1. Go to **Monitor alarms** > **Alarms** page, and click **New**.



2. Create rules for an alarm.

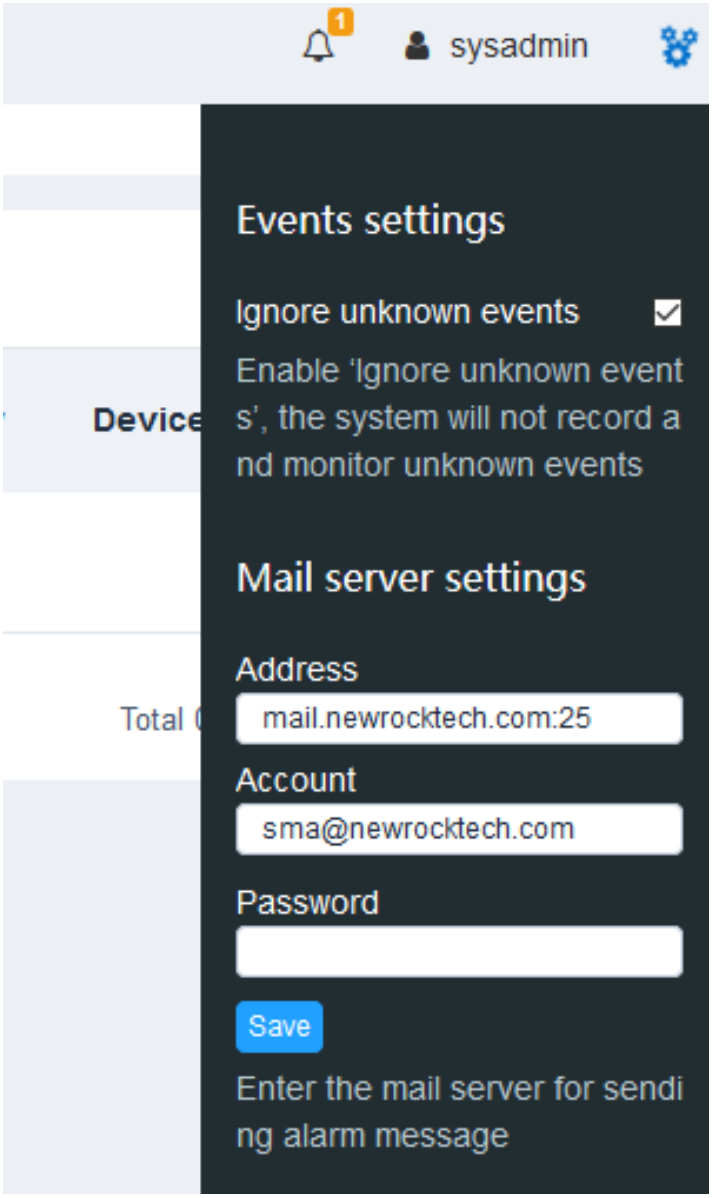
Copyright © New Rock Technologies, Inc



Description:

- Event: select the event to trigger an alarm. Only the events with the highest severity level can trigger alarms.
- Name: input a name for the alarm.
- Description: Input description for the alarm. It is optional.
- Threshold: the condition to trigger the alarm. For example: trigger an alarm if the reboot events take place more than 2 time within a minute.
- WeChat: tick it and choose WeChat IDs to receive the alarm messages. But you need to add the WeChat IDs on **Monitor alarms** > **Alarms** > **Inform list** page first.
- Email: Tick it and choose Emails addresses to receive the alarm messages. Note: First, you need to add the Emails address on **Monitor alarms** > **Alarms** > **Inform list** page, and set information for sending Email box by clicking .

 Copyright © New Rock Technologies, Inc



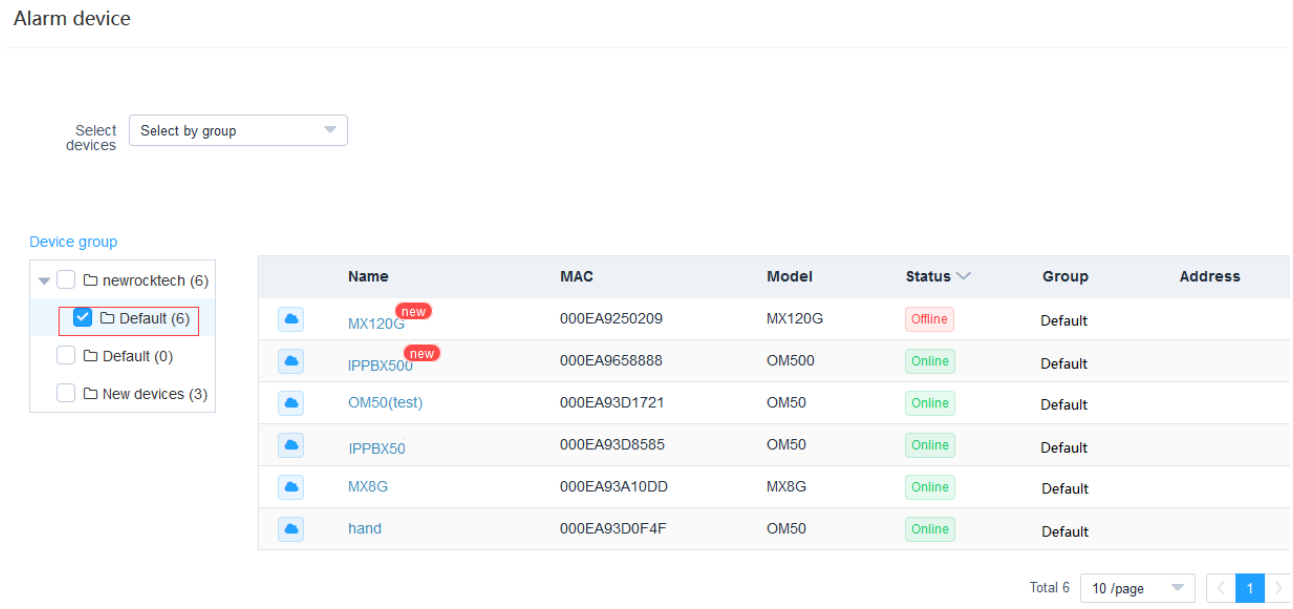
- Phone: Tick it and choose mobile phone numbers to receive the alarm messages. Note: First, you need to add the mobile phone numbers to be chose on **Monitor alarms** > **Alarms** > **Inform list** page**.**
- Action: Tick it, and the operation logs will be download upon an alarm is triggered.

3. Click **Next,** add devices for which the alarm rules are applicable.

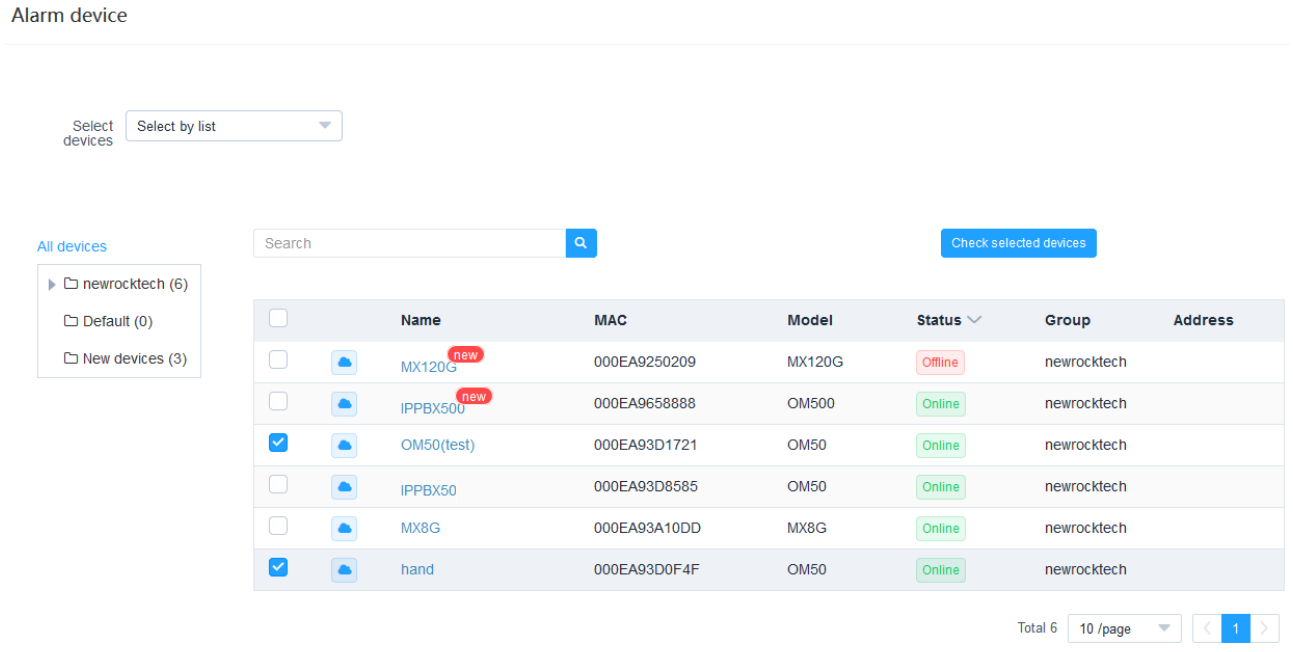
You have four choices:

- All device
- Select by device group

 Copyright © New Rock Technologies, Inc



- Select by device model
- Select user-defined devices

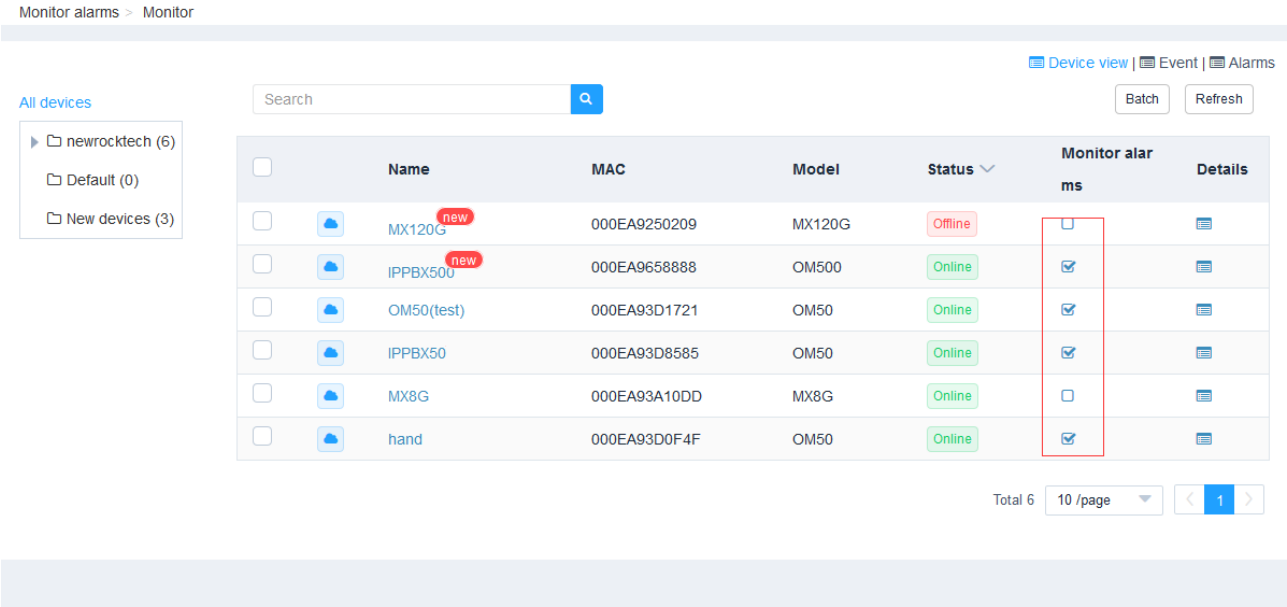


4. Click **save**.

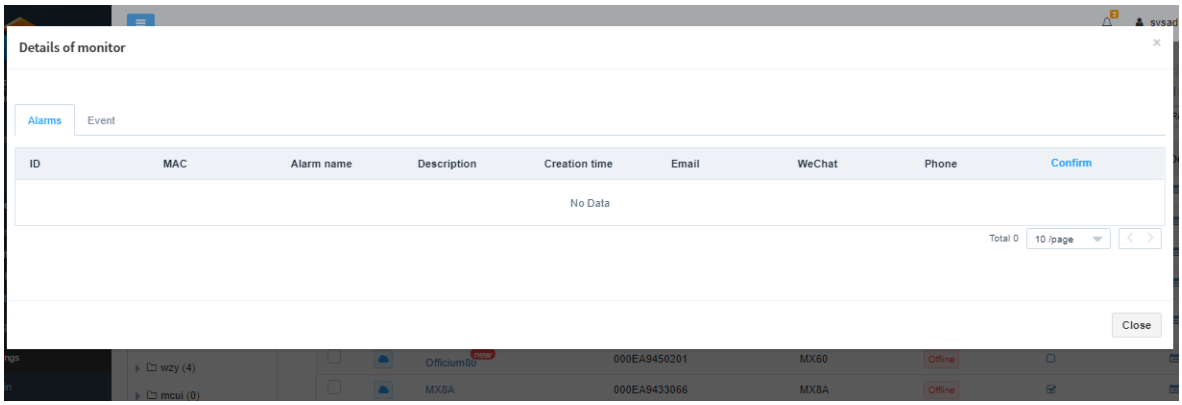
Copyright © New Rock Technologies, Inc

8.2 Monitor

1. Go to **Monitor alarms** > **Monitor** > **Device view** page, and tick the check boxes for the devices, to enable the UMS to monitor these devices.

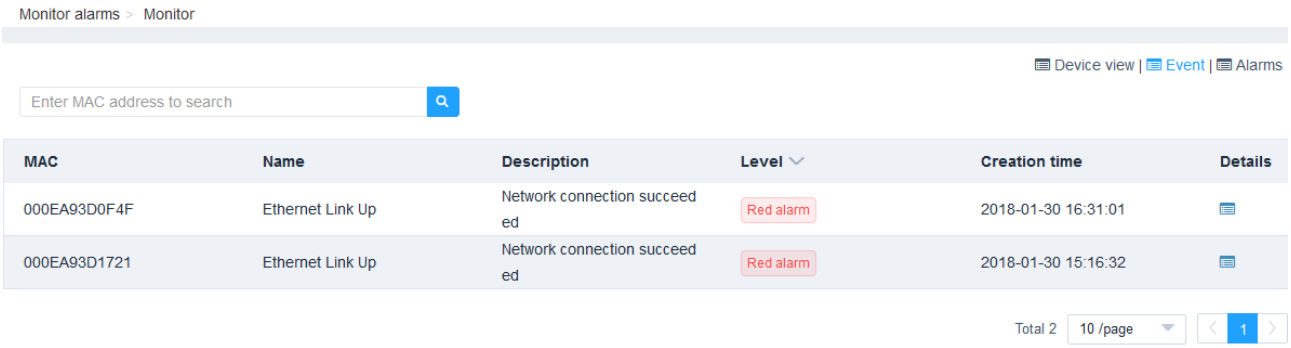


2. Click  to view alarms and events triggered by a specific device.

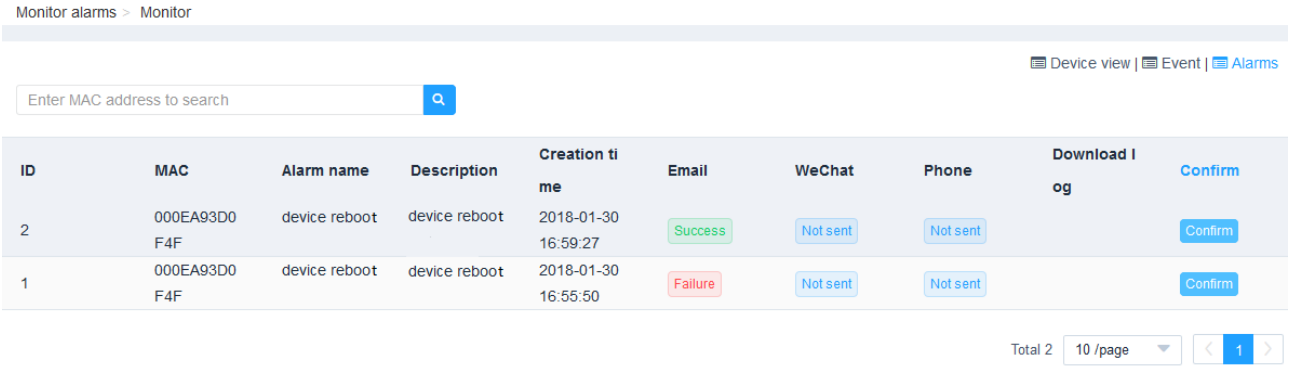


3. Go to **Monitor alarms** > **Monitor** > **Event** page to view all events triggered by all devices.

Copyright © New Rock Technologies, Inc



4. Go to **Monitor alarms** > **Monitor** > **Alarms** page to view all alarms triggered by all devices.



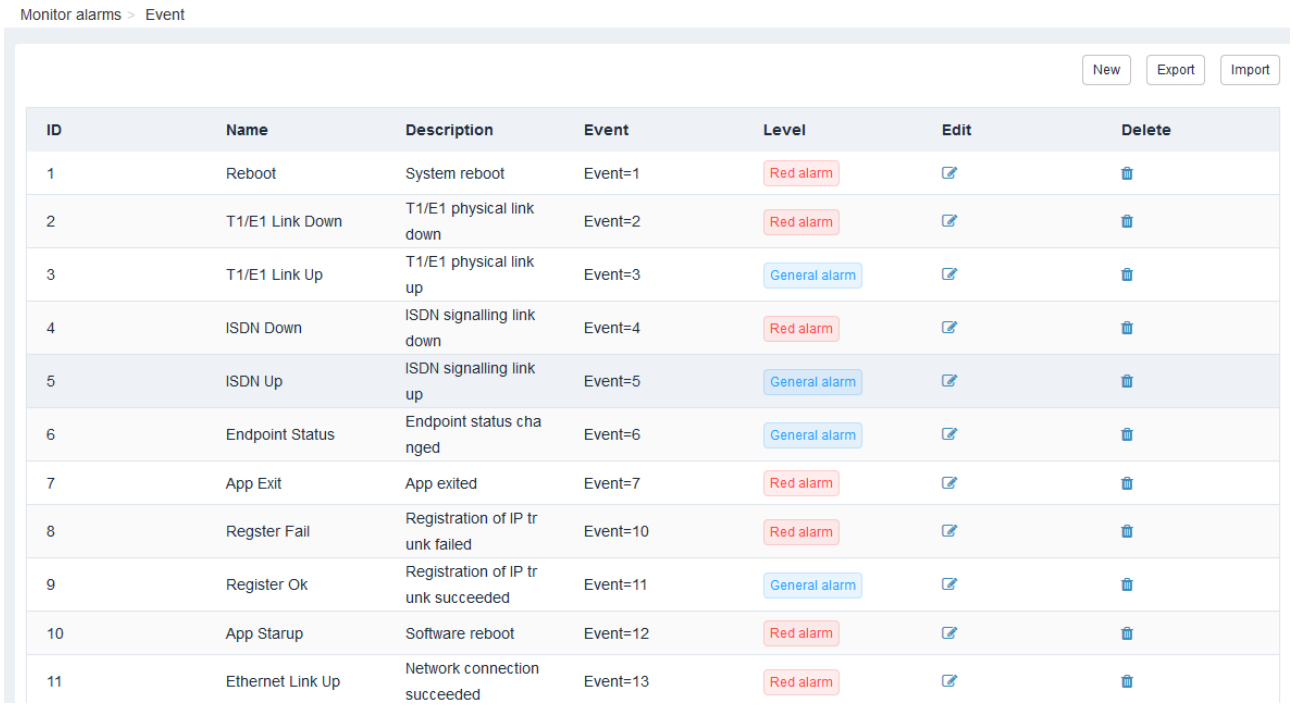
 Copyright © New Rock Technologies, Inc

8.3 Events

UMS can preset and monitor multiple events of devices.

These events are divided into three types based on the severity level, they are displayed with different color from highest to lowest: red, yellow, and black.

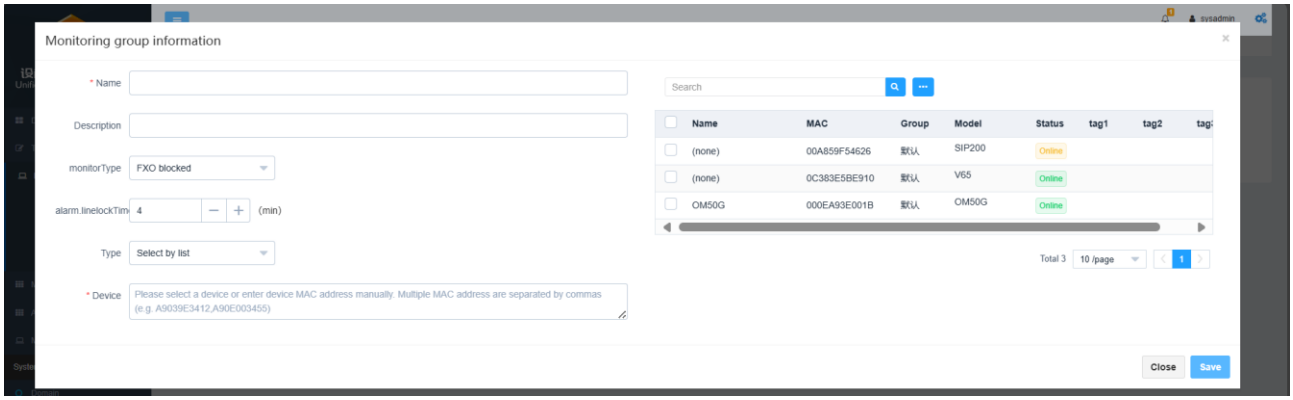
By default, there are 27 events. You can also add, import or modify events.



ID	Name	Description	Event	Level	Edit	Delete
1	Reboot	System reboot	Event=1	Red alarm		
2	T1/E1 Link Down	T1/E1 physical link down	Event=2	Red alarm		
3	T1/E1 Link Up	T1/E1 physical link up	Event=3	General alarm		
4	ISDN Down	ISDN signalling link down	Event=4	Red alarm		
5	ISDN Up	ISDN signalling link up	Event=5	General alarm		
6	Endpoint Status	Endpoint status changed	Event=6	General alarm		
7	App Exit	App exited	Event=7	Red alarm		
8	Regster Fail	Registration of IP trunk failed	Event=10	Red alarm		
9	Register Ok	Registration of IP trunk succeeded	Event=11	General alarm		
10	App Starup	Software reboot	Event=12	Red alarm		
11	Ethernet Link Up	Network connection succeeded	Event=13	Red alarm		

8.4 Monitoring group

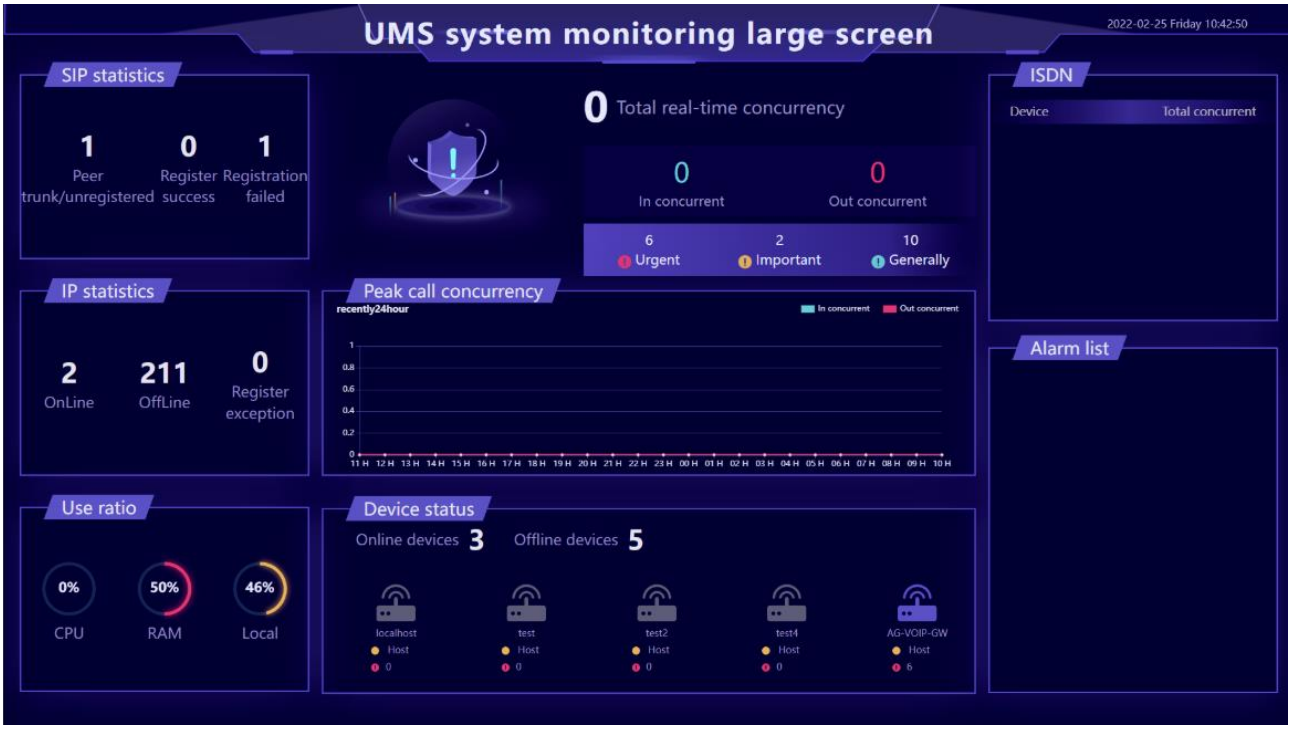
Navigate to Monitor Alarms, Monitor Groups, Monitor Groups are used for status monitoring and anomaly detection of devices, support selecting and setting monitoring types by multiple devices.



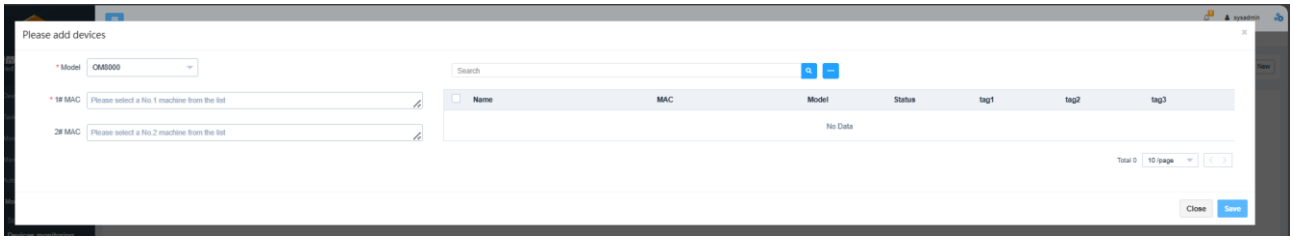
 Copyright © New Rock Technologies, Inc

8.5 Monitor website

Navigate to system settings> Big screen configuration, the Monitor Screen module is used to monitor the device status, call concurrency and system resource utilization of the UMS system in real time. The module provides visualized data display to help administrators quickly understand the system operation status, equipment online, alarm information, etc., and improve monitoring efficiency and fault response speed.



Additional monitoring equipment



 Copyright © New Rock Technologies, Inc

9 Roles and privileges

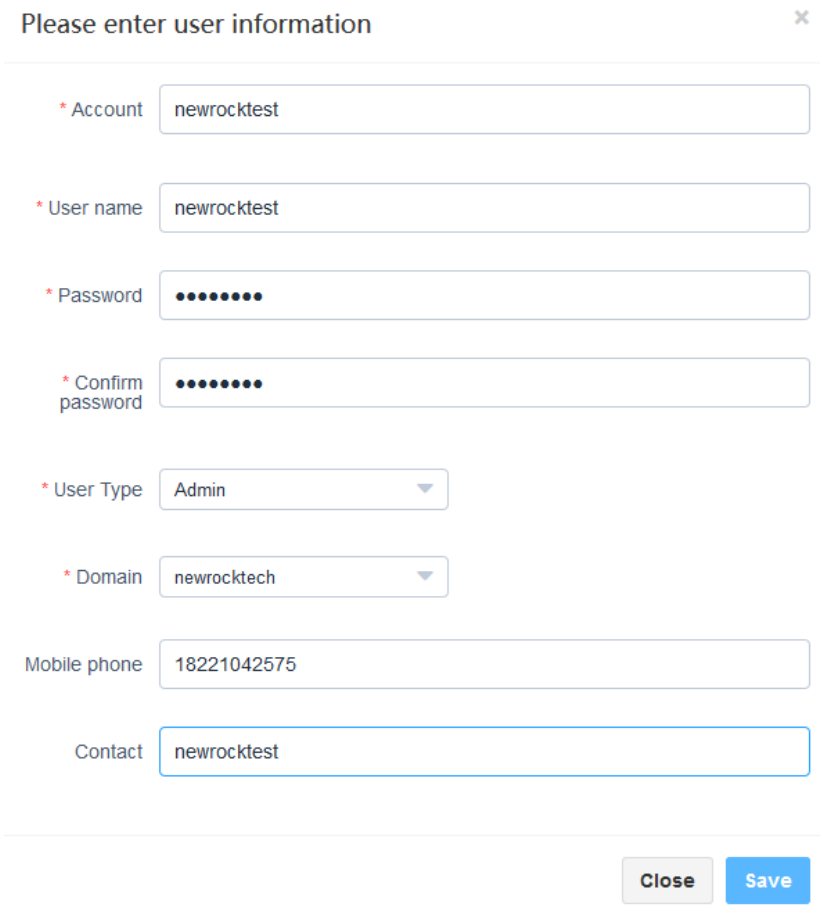
There are three types of account with different privilege:

- Super Administrator: There is only one super administrator who have whole permission to control the UMS. The account of the super administrator is **sysadmin** and it cannot be modified. The default password is **admin@123**.
- Administrators: They are created by the super administrator. Each one has the permission to manage the devices of a specified domain.
- Users: They are created by the super administrator or administrators. A user created by the super administrator may have permission to manager several domains while a user created by an administrator only has permission to manage one domain. And the permission details of a user depends its role, which are defined on **Manage > Roles** page.

9.1 Create administrators

Administrators are created by the super administrator. Each administrator has the whole permission to manage the devices of a specific domain.

Go to **Manage** > **User** page, click **New** to create an administrator. Please choose **Admin** for User Type. Account and password are used to login, the username is used for identification only.



 Copyright © New Rock Technologies, Inc

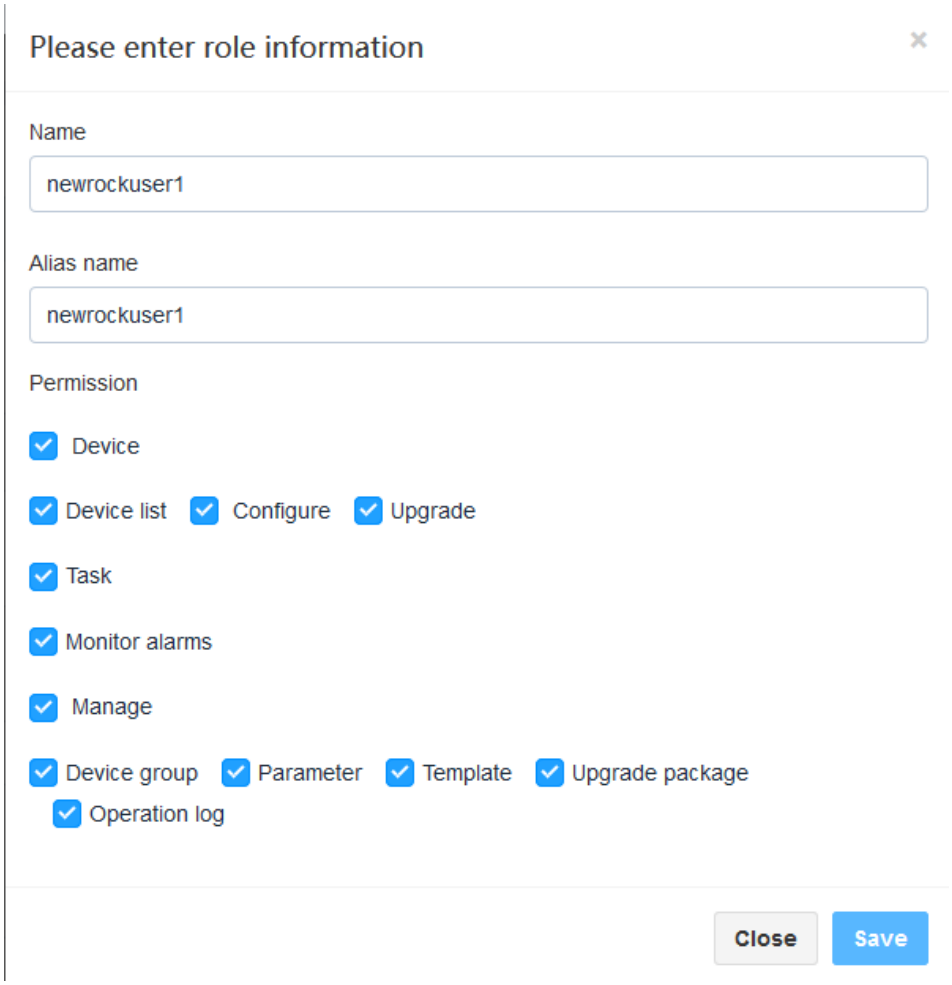
9.2 Create users

Before creating users, you have to create roles which decide privilege details for users.

Do as follows:

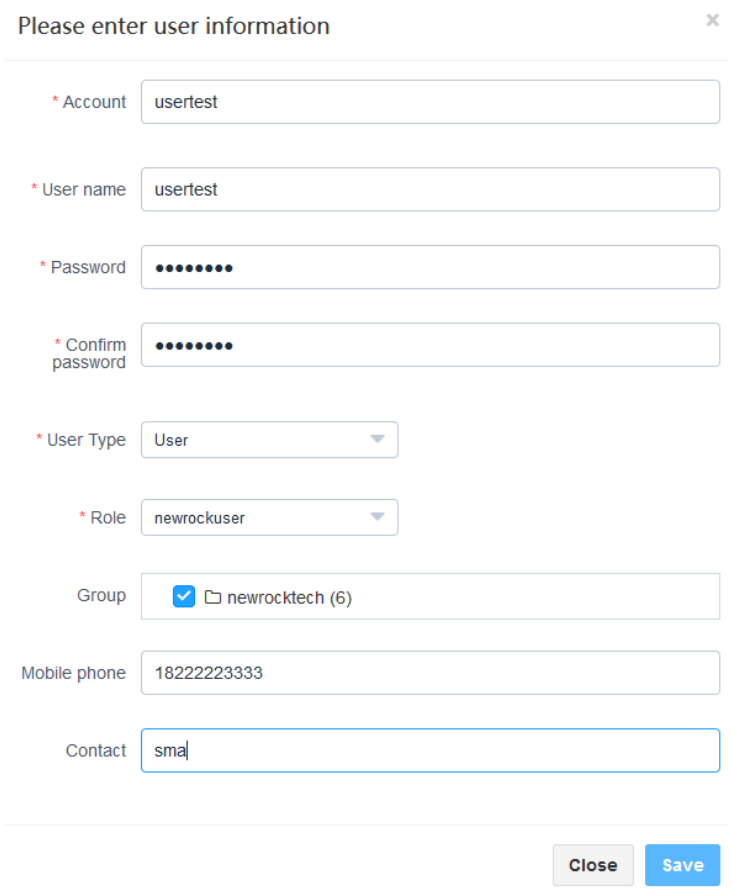
1. Go to **Manage > Roles** to create roles, and tick the privilege for specific functions.

   Note: All the privilege are less than that a super administrator or an administrator has.



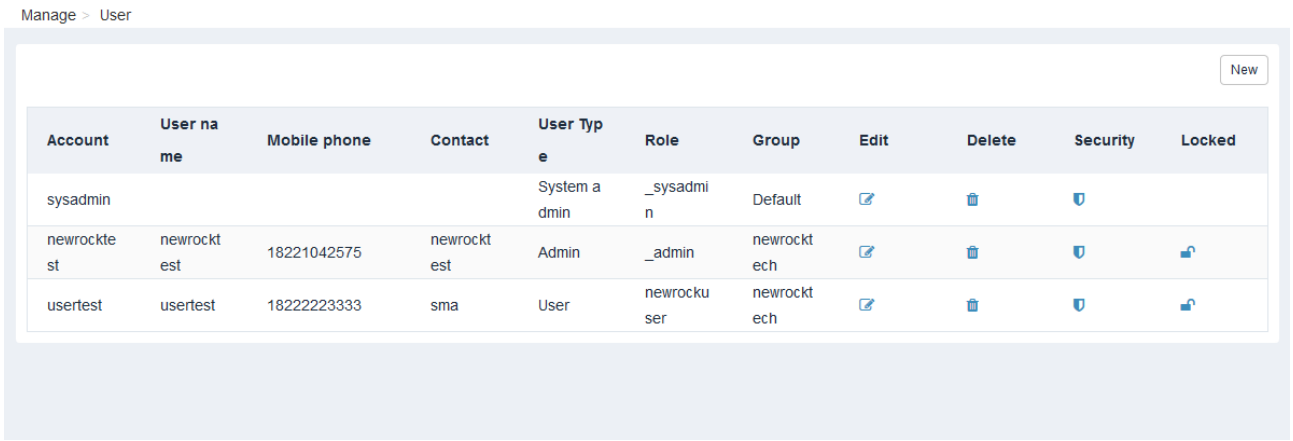
2. Go to **Manage** > **Users** to create users. Then choose a role for the user, and the device groups the user will manage.

Copyright © New Rock Technologies, Inc



9.3 User security settings

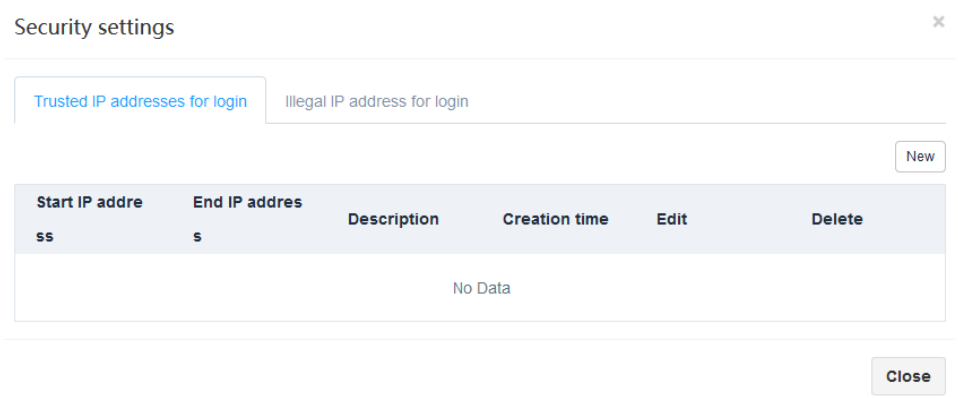
1. Go to **Manage** > **Users** page, click .

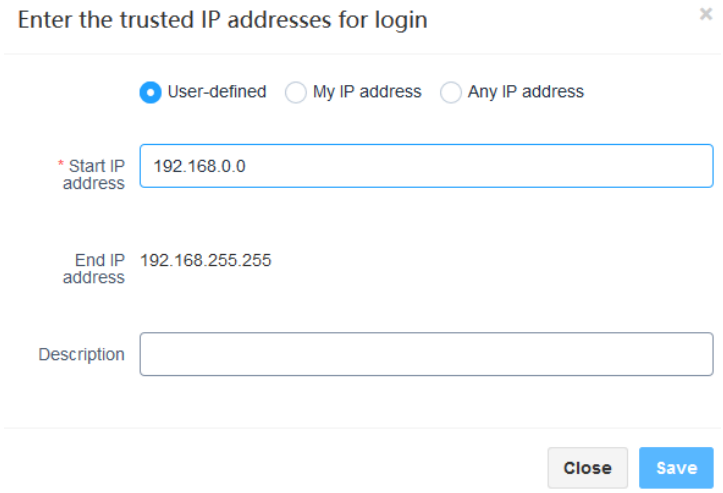


2. Click **New**, set the trusted IP addresses from which the user will log in to UMS. You may set several IP addresses for a user.

   If you keep the trusted IP address empty, that means the user can log into UMS from any IP addresses.

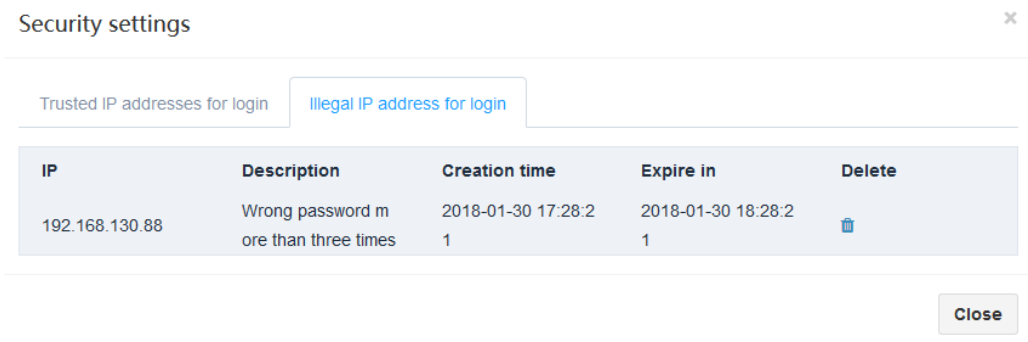
 Copyright © New Rock Technologies, Inc





- User-defined: Input an IP address or an IP address range, for example x.x.x.0 means the range of x.x.x.0 to x.x.x.255.
- My IP address: The IP address of the PC you log in to UMS will be added to the trusted address automatically.
- Any IP address: any IP address is a trusted IP address.

After three failed password login attempts, your IP address will be locked for an hour. You should request the administrator to remove the IP address from the untrusted IP address list or change your PC's IP address, if you want to log in UMS within one hour.

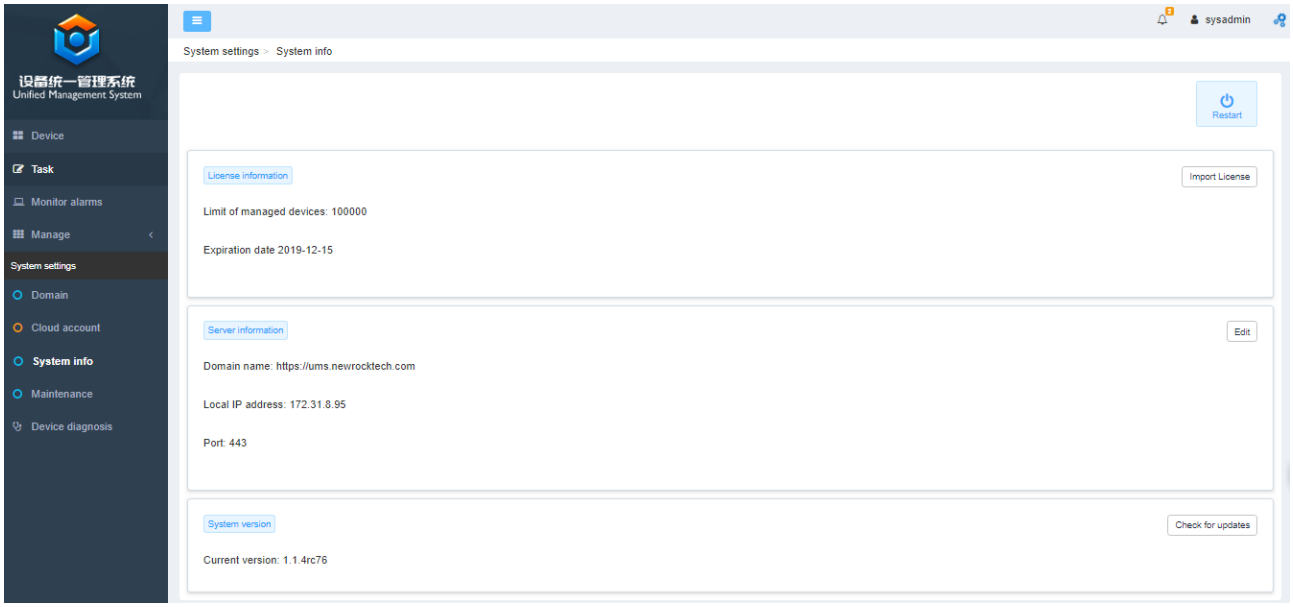


 Copyright © New Rock Technologies, Inc

10 System settings

10.1 View system information

Go to **System settings** > **System info** to view system information.

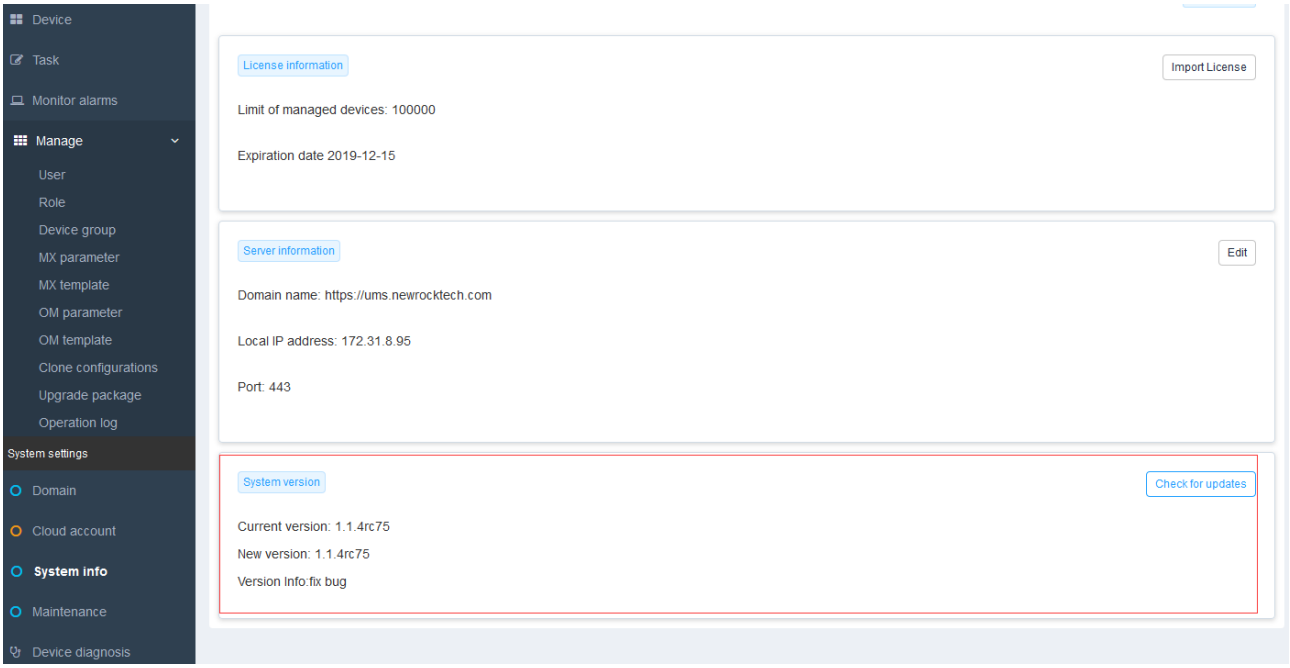


- License information: includes the limit of managed devices and expiration date. UMS has a free one month trial. At the end of your free trial, a code will be prompted, which is used to apply for a valid license from the seller. The new license need to be imported to UMS and need a reboot of UMS server to take effect.
- Server information: shows the domain name and IP address of the UMS server. You may modify them.
- System version: shows the version and allows you to upgrade UMS by clicking **Check for updates**.

10.2 Upgrade

- If UMS can access Internet, perform upgrading on **System settings** > **System info** > **System version** page.

 Copyright © New Rock Technologies, Inc

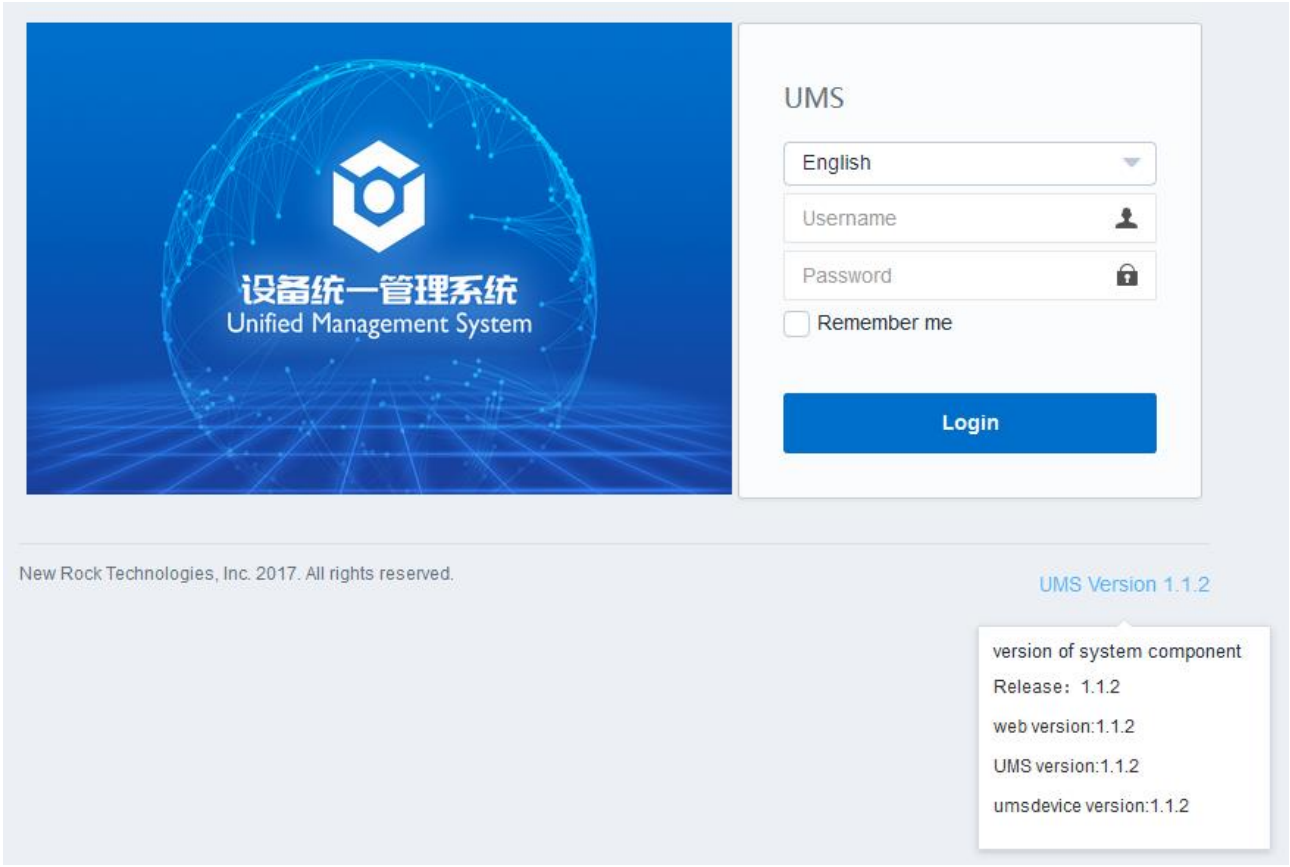


- If UMS cannot access Internet, do as follows to upgrade:

  1. Upload the upgrade package to the server, extract the package, and run the command below to install it:

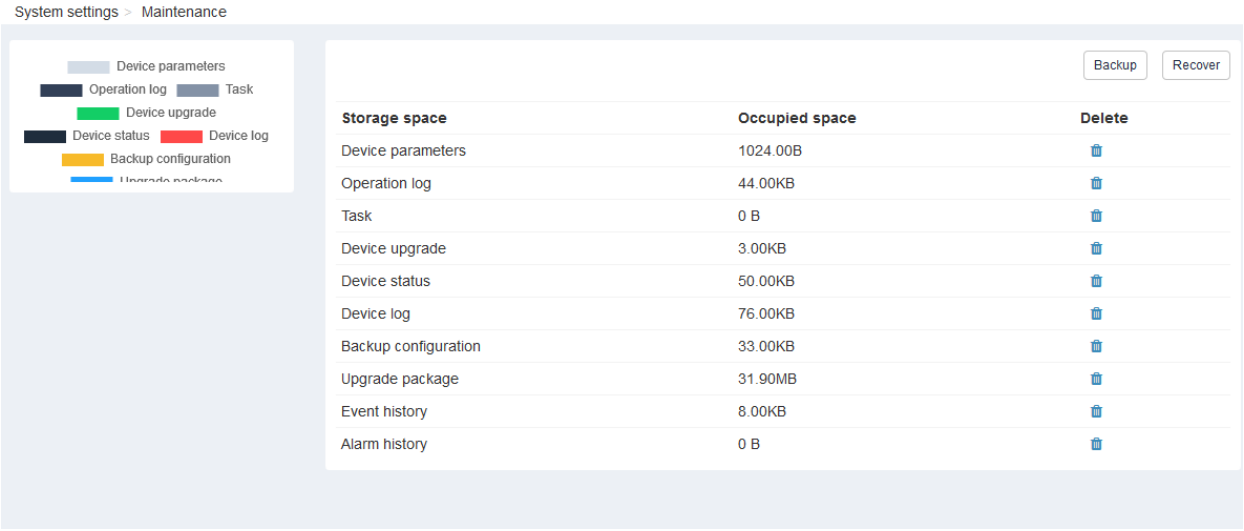
     sudo ./upgrade.sh

  2. Log in to UMS Web GUI to view the version information after upgrading.

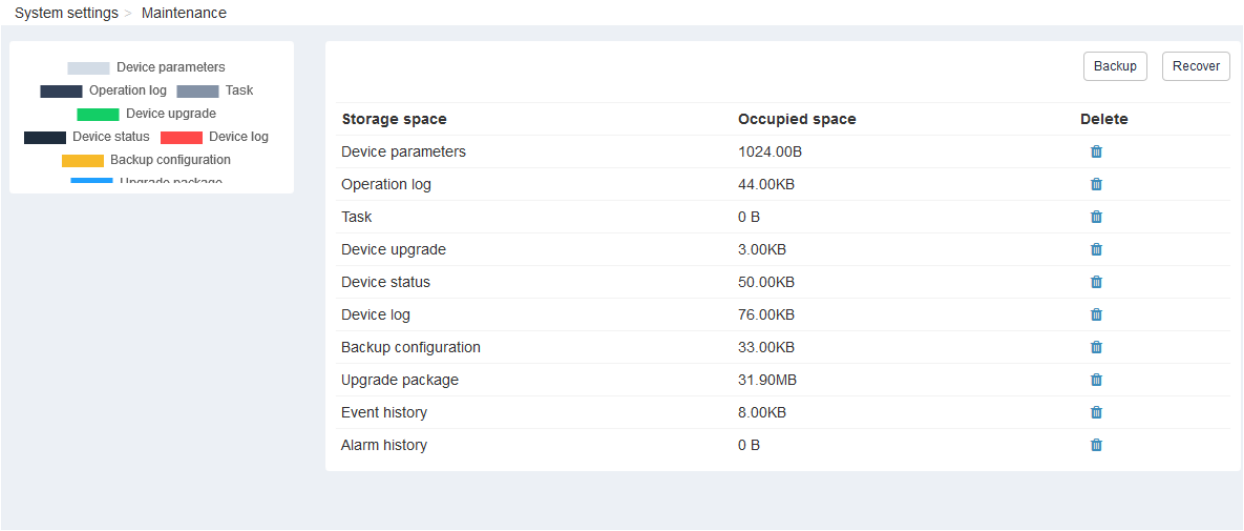


10.3 Maintenance

Go to **System settings** > **Maintenance** page, you may clear history data by clicking .



Click **Backup** to back up data to your PC or you can click **Recover** to recover the backed up data. Be sure to recover cautiously because it will override the current data.



- Device information
- System configurations
- Base version information for upgrading
- Role information
- Parameter and parameter template information
- User accounts
- Security settings
- Domain information
- Events and rules of alarms

 Copyright © New Rock Technologies, Inc