



# **IRM**

## **(IEI Remote Management)**

### **Tutorials**

# Revision

---

Date	Version	Changes
August 14, 2023	1.00	Initial release

# Copyright

---

## **COPYRIGHT NOTICE**

The information in this document is subject to change without prior notice in order to improve reliability, design and function and does not represent a commitment on the part of the manufacturer.

In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages.

This document contains proprietary information protected by copyright. All rights are reserved. No part of this manual may be reproduced by any mechanical, electronic, or other means in any form without prior written permission of the manufacturer.

## **TRADEMARKS**

All registered trademarks and product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective owners.

# Table of Contents

---

<b>1 OVERVIEW .....</b>	<b>1</b>
1.1 HOW TO USE IRM TO MANAGE YOUR DEVICES.....	2
1.2 BROWSER SUPPORT .....	2
1.3 OS SUPPORT.....	2
1.4 REQUIREMENTS FOR INSTALLING IRM.....	3
1.5 INSTALLING CONTAINER STATION, IRMAGENTPACK AND IRM.....	3
<b>2 DEVICE DISCOVERY .....</b>	<b>6</b>
2.1 START SCAN .....	7
2.2 STOP SCANNING .....	11
2.3 RESETTING .....	11
2.4 STEPS TO ADD THE DEVICE TO IRM.....	12
2.4.1 <i>Windows Devices</i> .....	13
2.4.2 <i>Linux Devices</i> .....	18
2.5 ADD A DEVICE TO IRM DURING SCAN.....	21
2.6 SCAN HISTORY .....	21
<b>3 MAIN DASHBOARD .....</b>	<b>22</b>
3.1 ADD WIDGET .....	23
3.2 DELETE ALL WIDGETS IN THE DASHBOARD.....	26
3.3 REFRESH ALL WIDGETS IN THE DASHBOARD.....	27
3.4 SELECT THE LAYOUT MODE .....	28
3.5 EXPORT AS PDF FILE .....	28
3.6 EMAIL CURRENT VIEW.....	30
3.7 REAL-TIME AND HISTORICAL DATA PRESENTATION.....	31
<b>4 DEVICE MANAGEMENT.....</b>	<b>32</b>
4.1 DEVICE LIST.....	33
4.1.1 <i>Device Name</i> .....	33
4.1.2 <i>Status</i> .....	33
4.1.3 <i>Add Device</i> .....	33

4.1.3.1 Quickly add the specified device .....	35
1. Windows Devices.....	35
2. Linux Devices .....	36
4.1.3.2 Search the network to help you find the device to add.....	38
4.1.4 Remove Device.....	39
4.1.5 Reinstall .....	39
4.1.6 Power Control.....	39
4.2 NETWORK TOPOLOGY .....	40
<b>5 SINGLE DEVICE MANAGEMENT.....</b>	<b>41</b>
5.1 SINGLE DEVICE DASHBOARD.....	42
5.2 ADD WIDGET .....	42
5.3 DELETE ALL WIDGETS IN THE SINGLE DEVICE DASHBOARD .....	45
5.4 REFRESH ALL WIDGETS INFORMATION IN THE DASHBOARD .....	45
5.5 SELECT THE LAYOUT MODE .....	46
5.6 TOOLS - PING .....	47
5.7 TOOLS – TRACEROUTE.....	48
5.8 TOOLS - REMOTE DESKTOP .....	49
5.9 TOOLS - POWER CONTROL .....	53
<b>6 ALERT CONFIGURATION.....</b>	<b>54</b>
6.1 ADD ALERT .....	55
6.2 DELETE ALERT.....	57
6.3 ENABLE ALERT .....	58
6.4 DISABLE ALERT .....	59
6.5 EDIT ALERT.....	60
<b>7 LOGS .....</b>	<b>61</b>
7.1 ALERTS LOG.....	62
7.2 SYSTEM LOG .....	63
7.3 HISTORIC DATA LOG .....	65
<b>8 SETTINGS.....</b>	<b>67</b>
8.1 USER MANAGEMENT.....	68
8.1.1 Add User: .....	68
8.1.2 Deleting Users: .....	70

8.1.3 <i>Editing Permissions</i> .....	70
8.2 NOTIFICATION SETTINGS .....	72
8.3 APPLICATION SETTINGS.....	73
8.4 IRMAGENT INFORMATION .....	74

Chapter

1

# Overview

---

## 1.1 How to Use IRM to Manage Your Devices

IRM is a centralized remote device management solution from IEI designed for IT teams, home users, production line managers, or anyone who wants to monitor and manage computer devices (such as: computers, servers, etc).

IRM is a web-based solution that provides basic device management capabilities such as device discovery, monitoring, or management of all critical computing devices on the network, such as servers, computers, embedded computers, or compact computers.

Centralized management of IRM improves the manageability of IT infrastructure and computer equipment, and reduces the time required to troubleshoot and analyze system resource performance.

## 1.2 Browser Support

IRM supports most modern web browsers. For the best user experience, we recommend using the latest version of Google Chrome. IRM also supports the latest versions of:

- Safari
- Microsoft Edge
- Firefox

## 1.3 OS Support

The operating systems supported by IRM are listed below:

- **32-bit OS**
  - Windows 7
  - Windows 8/8.1
- **64-bit OS**
  - Windows 7
  - Windows 8/8.1
  - Windows 10
  - Window 11
  - Windows Server 2012
  - Windows Server 2016
  - Windows Server 2019
  - Window Server 2022
  - Ubuntu 16.x
  - Ubuntu 18.x
  - Ubuntu 20.x
  - Ubuntu 22.x
  - CentOS 7
  - Debian 8
  - Debian 9
  - Debian 10
  - Debian 11

## 1.4 Requirements for Installing IRM

Hardware:

- TS-i410X-8G2H

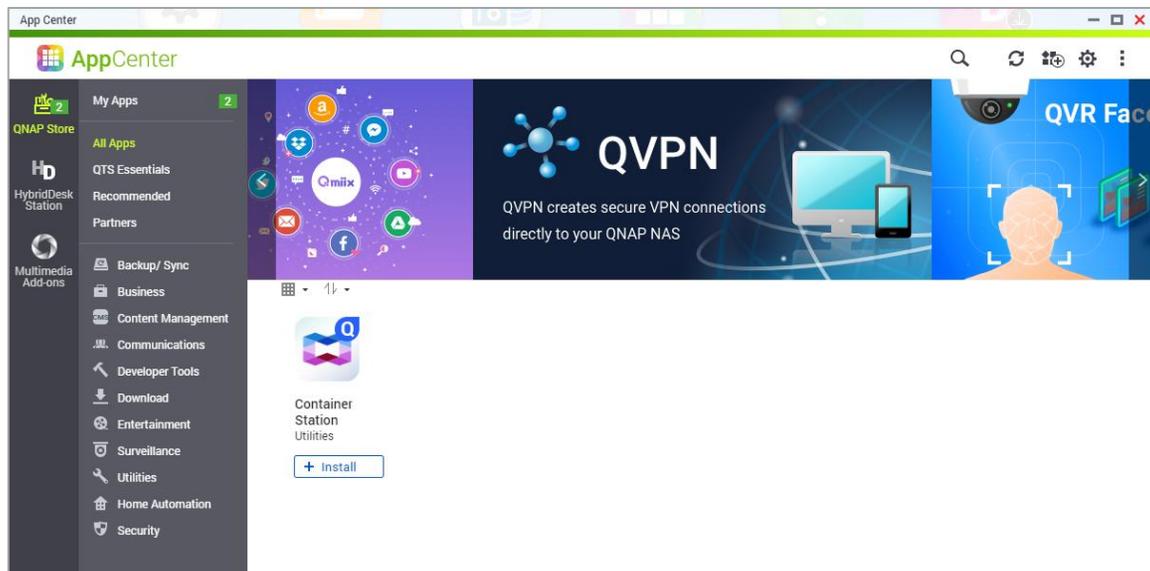
Software

- Container Station
- IRMAgent

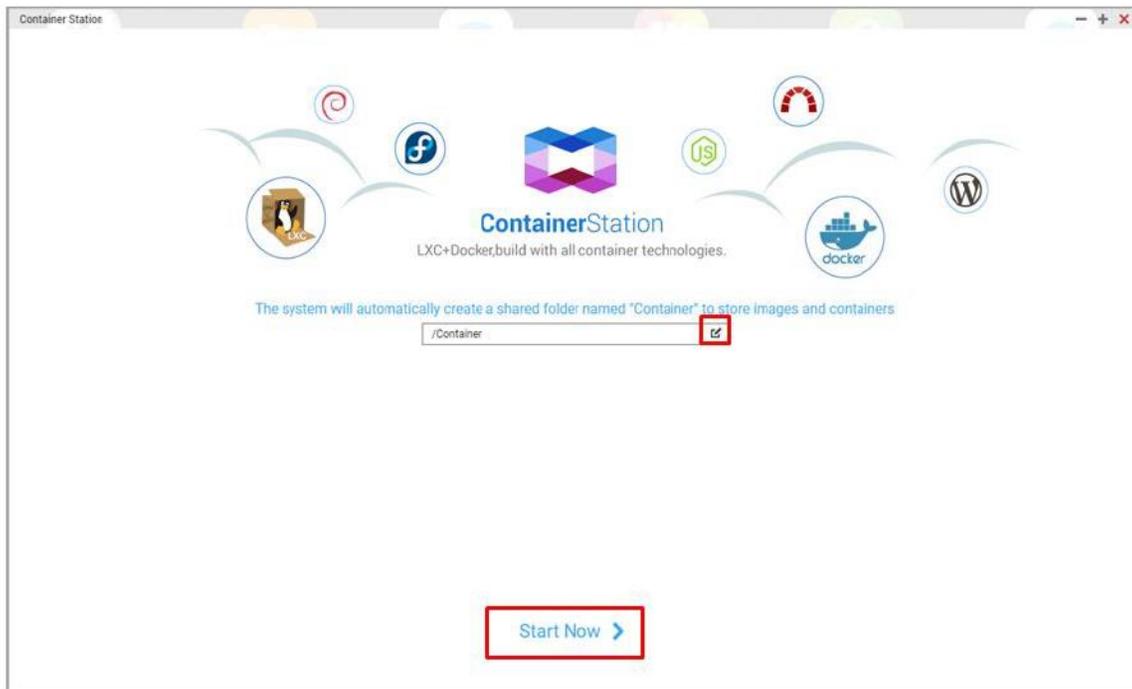
\*Container Station and IRMAgent must be installed before using IRM.

## 1.5 Installing Container Station, IRMAgentPack and IRM

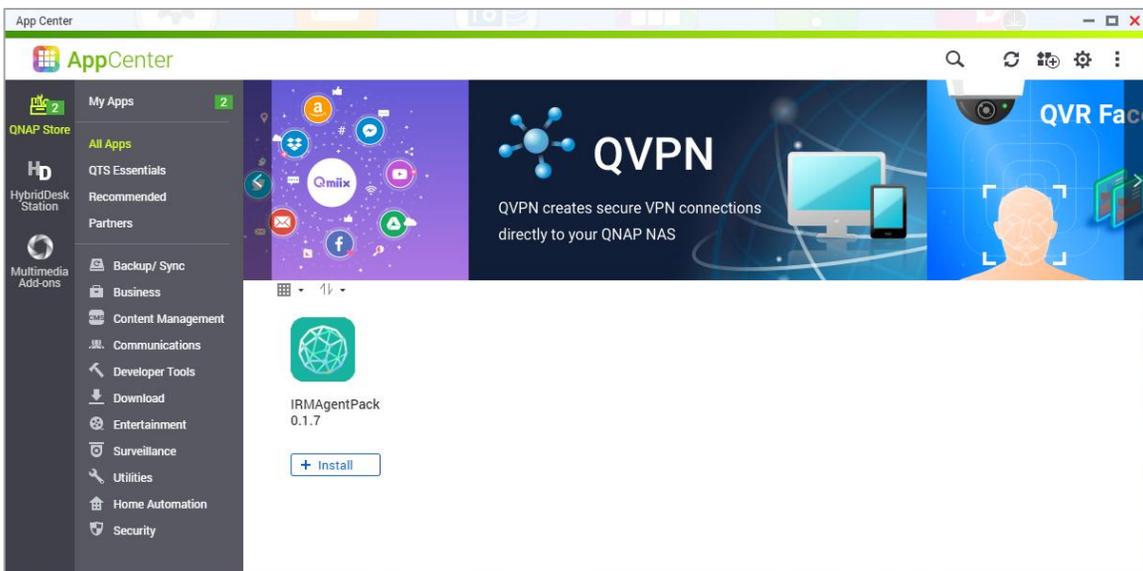
**Step 1:** Open QNAP's App Center and search for "Container Station". If you have not installed Container Station then an "+ Install" button will appear. Click the "+ Install button".



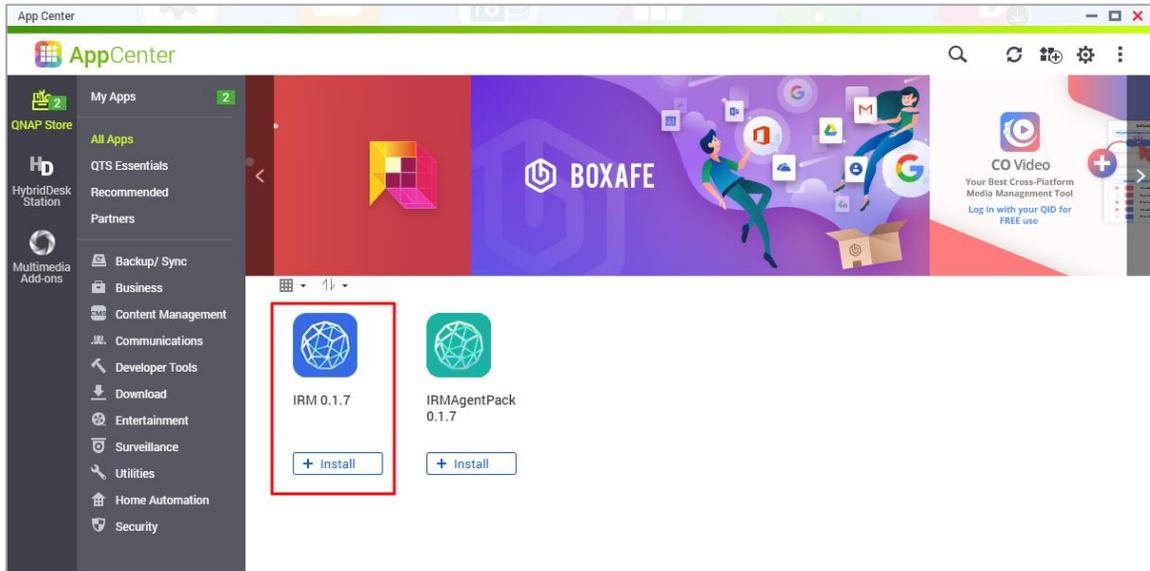
**Step 2:** Open Container Station and follow the installation wizard. After selecting a folder to store images and containers, click "Start Now".



**Step 3:** Return to the App Center and search for "IRMAgentPack". If you have not installed IRMAgentPack then an "+ Install" button will appear. Click the "+ Install button".



**Step 4:** Return to the App Center and search for "IRM". An app called "IRM " will be listed. If you have not installed IRM then an "+ Install" button will appear. Click the "+ Install button".



Chapter

2

# Device Discovery

---

With IRM, you can use the Device Discovery feature to discover the network you're in. Device Discovery allow users to discover computer devices on the current network based on the scan range they set up and quickly incorporate them into IRM Management. On the Device Discovery page, users can start scan, stop scan, reset, query scan history, filter scan results, add devices, generate scan result reports, and send current view as Email.

IRM supports the following two search types:

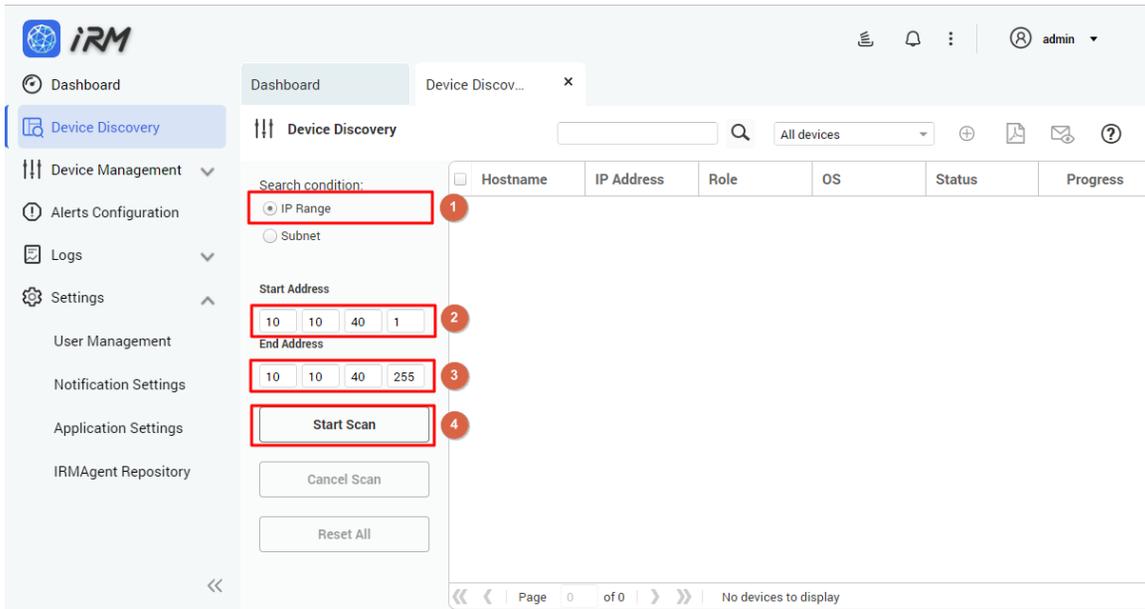
1. IP range
2. Subnet

## 2.1 Start Scan

If the user clicks the "Start Scan" button, IRM will start scanning all the devices within the IP range or in the subnet. During the scan, discovered devices are placed in order from the top down, and the user can add the discovered device to IRM without waiting for the scan to finish. Details are described in *Section 2.5 Add a Device to IRM During Scan*.

To scan a specific IP range, follow the steps below:

- Step 1:** Select the IP range.
- Step 2:** Enter the starting IP address.
- Step 3:** Enter the ending IP address.
- Step 4:** Click "Start Scan".

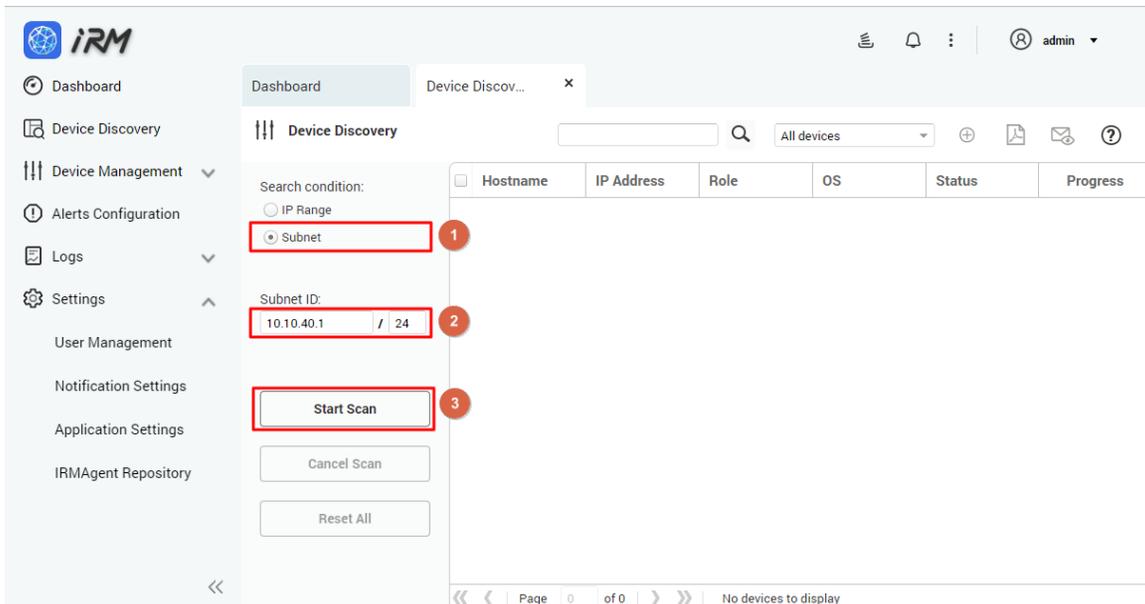


To scan a specific subnet range, follow the steps below:

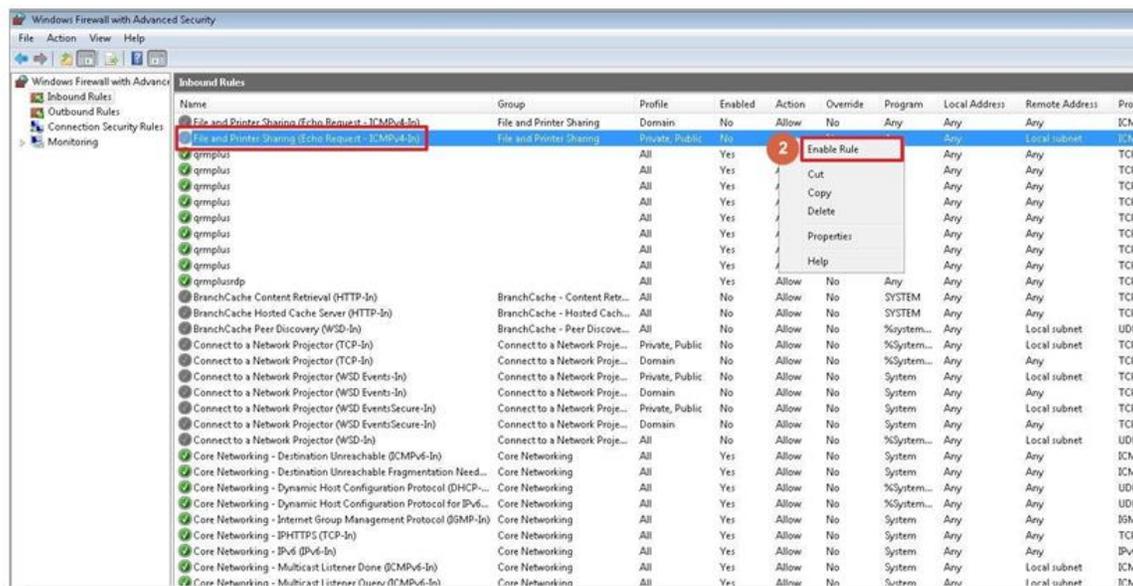
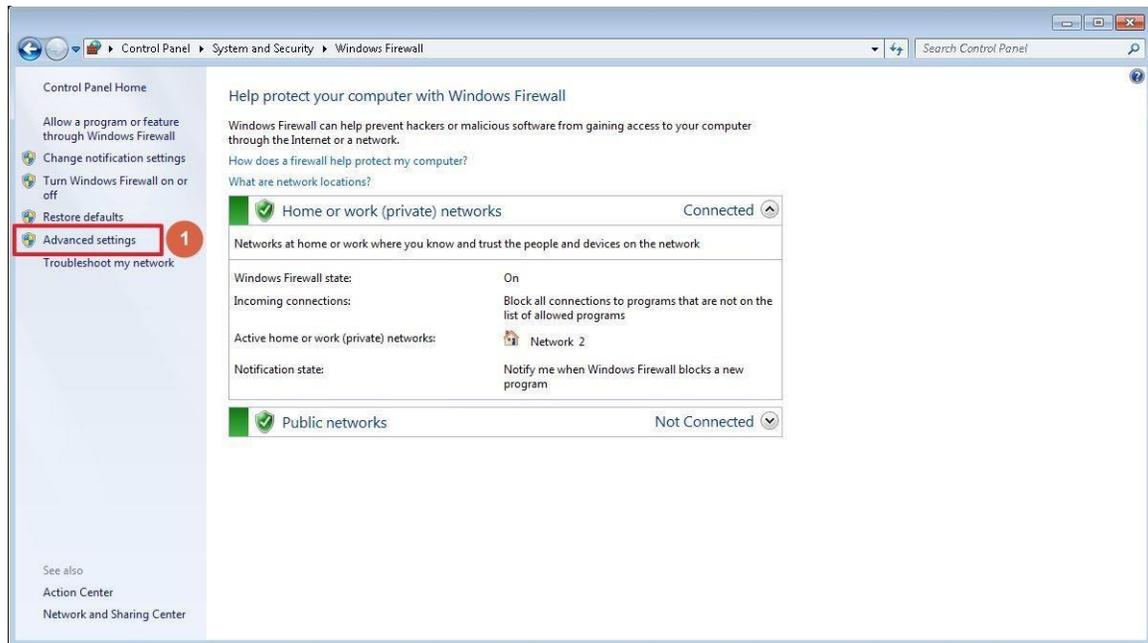
**Step 1:** Set the subnet.

**Step 2:** Enter the CIDR, default is 24.

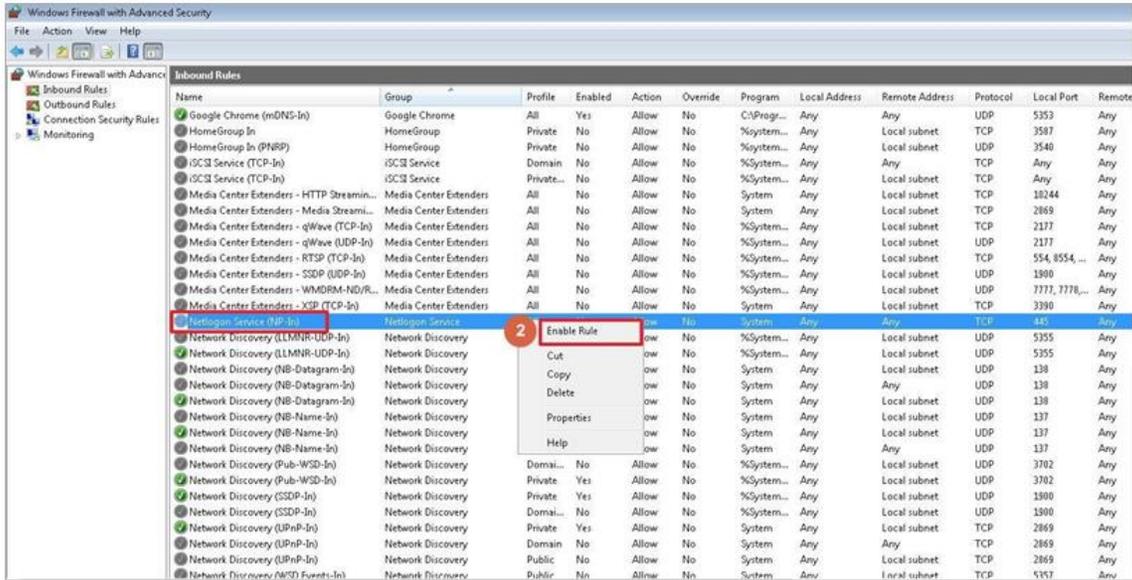
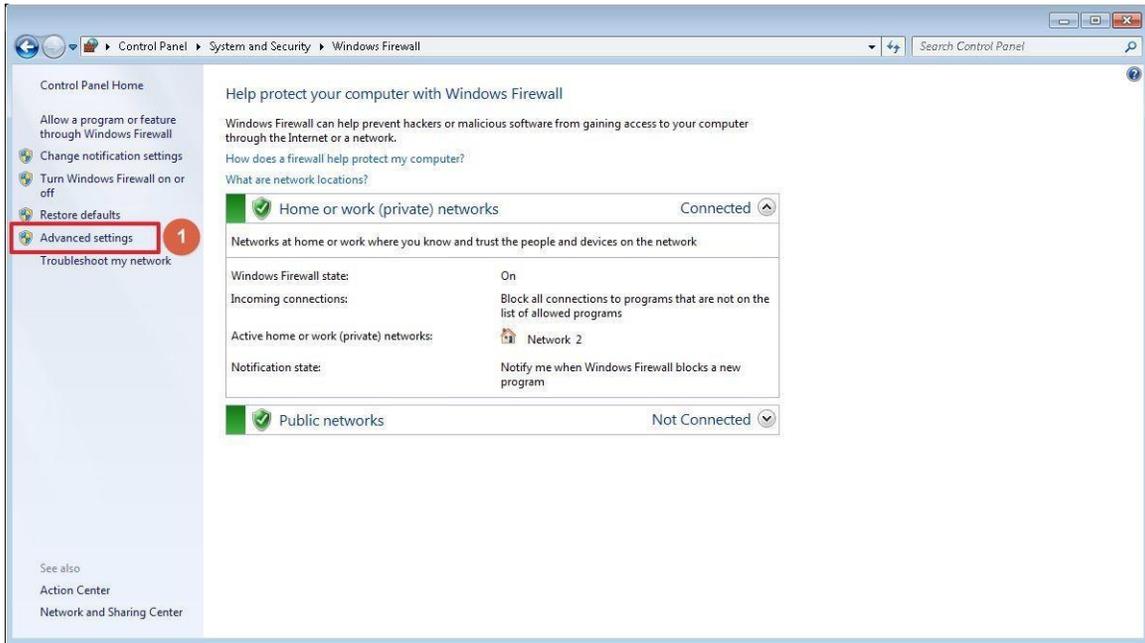
**Step 3:** Click "Start Scan".



**NOTE:** IRM uses ICMP protocol to search for devices within a specified IP address range. If the target device does not allow ICMP requests, IRM will not be able to find the target device. To support IRM search, enable ICMP requests on the target device.



**NOTE:** MS Windows firewall rules will also affect IRM and treat target device as unsupported device. To solve the problem, go to Control Panel> System & Security> Windows Firewall. Click the "Advanced Settings" button to set up (as shown below).



## 2.2 Stop Scanning

During a scan, the user can click the Cancel Scan button to stop the scan.

The screenshot shows the iRM interface with the 'Device Discovery' page active. The left sidebar contains navigation options: Dashboard, Device Discovery, Device Management, Alerts Configuration, Logs, Settings, User Management, Notification Settings, Application Settings, and IRMAgent Repository. The main content area shows search conditions (Subnet: 10.10.40.1 / 24) and a table of devices being scanned. The 'Cancel Scan' button is highlighted with a red box.

Hostname	IP Address	Role	OS	Status	Progress
B10802373-N	10.10.40.18				Scanning...
B10901419-N	10.10.40.20				Scanning...
B10801619-N	10.10.40.22				Scanning...
B11001086-P	10.10.40.25				Scanning...
B10801878-N	10.10.40.26				Scanning...
B11000025-P	10.10.40.38				Scanning...
SD-PETERLE...	10.10.40.43				Scanning...
NAS49103A-...	10.10.40.50				Scanning...

## 2.3 Resetting

The user can reset the settings after the scan is completed or after having clicked on the scan history. When the Reset All button is clicked, the contents of the table on the right side of the screen will be cleared.

The screenshot shows the iRM interface with the 'Device Discovery' page active. The left sidebar is the same as in the previous screenshot. The main content area shows search conditions (Subnet: 10.10.40.1 / 24) and a table of devices. The 'Reset All' button is highlighted with a red box.

Hostname	IP Address	Role	OS	Status	Progress
B10802373-N	10.10.40.18			Canceled	
B10901419-N	10.10.40.20			Canceled	
B10801619-N	10.10.40.22			Canceled	
B11001086-P	10.10.40.25			Canceled	
B10801878-N	10.10.40.26			Canceled	
B11000025-P	10.10.40.38			Canceled	
SD-PETERLE...	10.10.40.43			Canceled	
NAS49103A-...	10.10.40.50			Canceled	

## 2.4 Steps to Add the Device to IRM

Users can select a device from the list of discovered devices and click "Add Devices to IRM" button to add one or more devices to IRM. Different types of devices have different add methods:

1. Users of Linux device must provide administrator account and password to allow IRM to install the IRMAgent on the remote device. After successful installation, IRM will be able to monitor and manage the device.
2. Users of MS Windows device must download IRMAgent to the machine to be installed and extract the IRMAgent archive on the machine to run the installation program. After successful installation, IRM will be able to monitor and manage the device.

**Step 1:** Select the device you want to add from the list of discovered devices, you can select multiple devices.

**Step 2:** Click the "Add devices to IRM" button.

Hostname	IP Address ↑	Role	OS	Status	Progress
10.10.40.10	10.10.40.10	Router	Cisco	New Device	Completed
10.10.40.11	10.10.40.11	Router	Cisco	New Device	Completed
<input checked="" type="checkbox"/> B10802373-N	10.10.40.18	Device	Windows	New Device	Completed
<input type="checkbox"/> B10901419-N	10.10.40.20	Device	Windows	New Device	Completed

**Step 3:** Select the devices to be added in the device list screen.

 Add Devices to IRM ✕

**Add devices to IRM**

The devices you want to add by discovery are:

	Hostname	IP Address	OS	Status
<input checked="" type="checkbox"/>	B10802373-N	10.10.40.18	Windows	<span data-bbox="1154 457 1175 485">✖</span> Not Monitored

[Add selected devices](#)

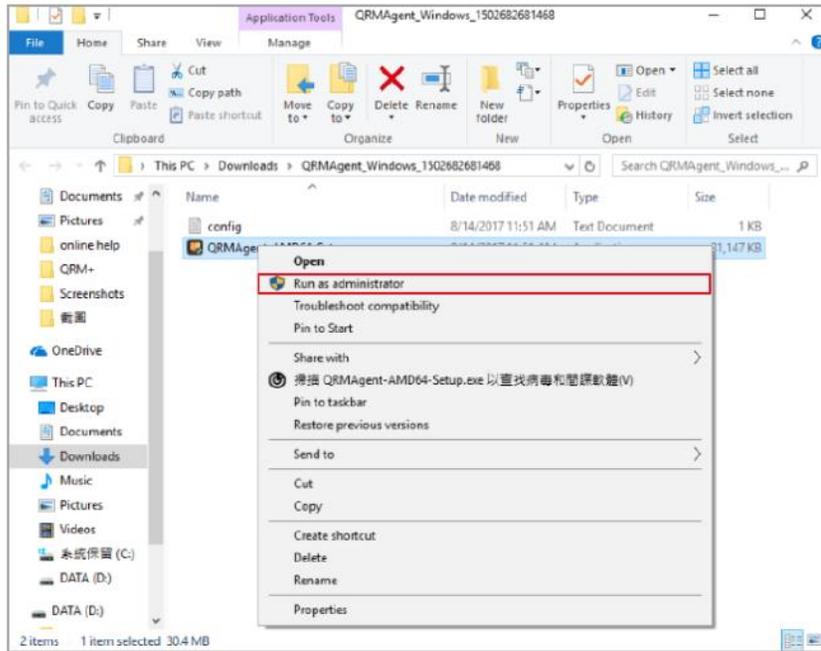
**Step 4:** Different device types (Windows device or Linux device) have different installation methods, which are described in the following sections.

### 2.4.1 Windows Devices

If a Windows device is selected in Step 3 of Section 2.4, you will be prompted to download IRMAgent for Windows. Click "Download" next to "Download Windows IRMAgent" to download the installation package.

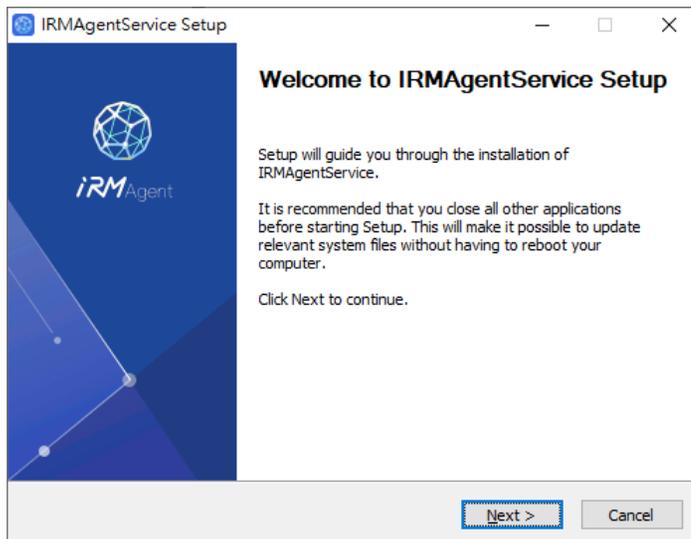


**Step 3:** Unzip the installer, right click on the installer and select "Run as administrator".

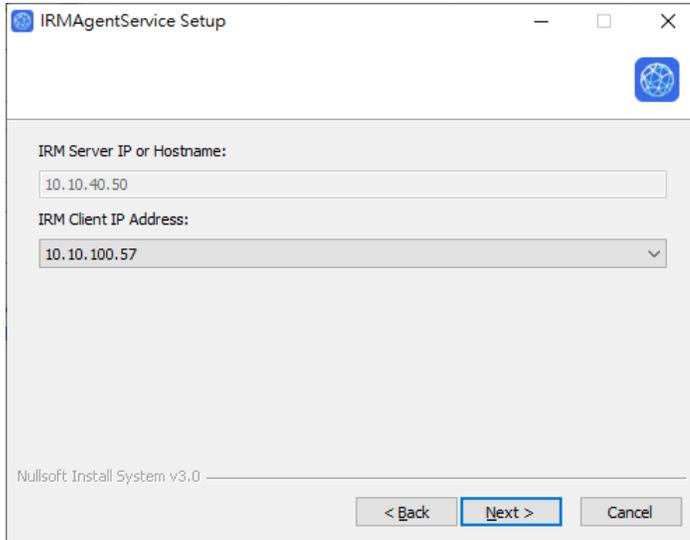


**Step 4:** Click "Yes" to allow the installer to make changes to your device.

**Step 5:** Click "Next".

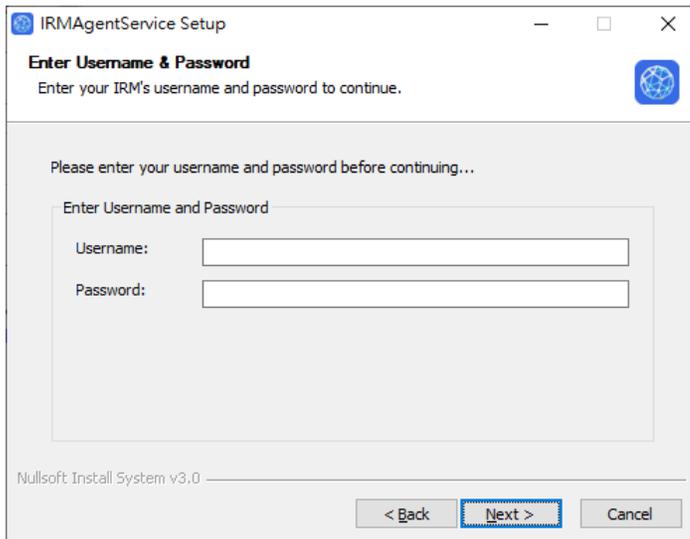


**Step 6:** Choose the IP address and click "Next".



The screenshot shows the 'IRMAgentService Setup' window. It has a title bar with a globe icon, a minimize button, a maximize button, and a close button. The main content area contains two input fields: 'IRM Server IP or Hostname:' with the value '10.10.40.50' and 'IRM Client IP Address:' with a dropdown menu showing '10.10.100.57'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The footer text reads 'Nullsoft Install System v3.0'.

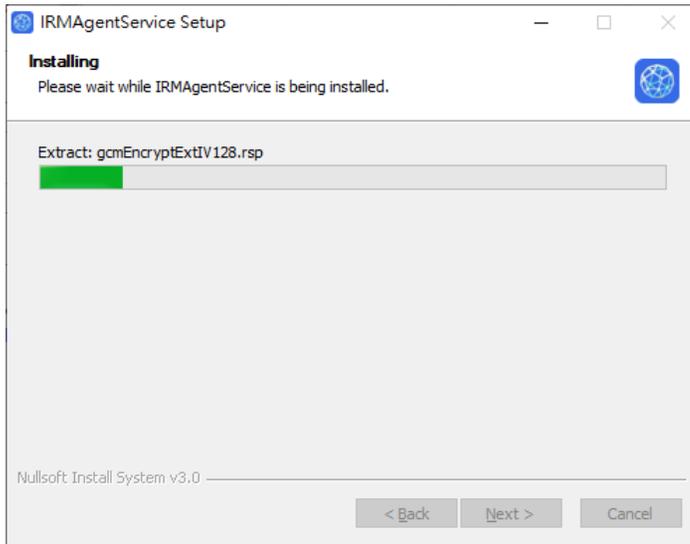
**Step 7:** Enter the Username and Password of IRM.



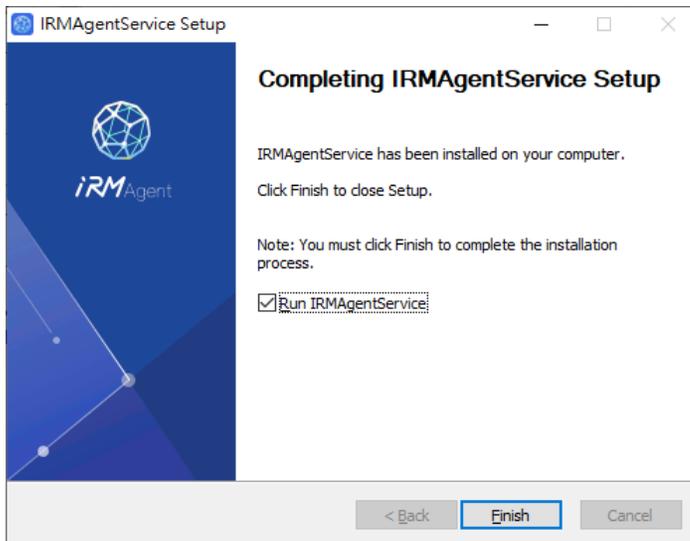
The screenshot shows the 'IRMAgentService Setup' window at the 'Enter Username & Password' step. The title bar is the same as in Step 6. The main content area has the heading 'Enter Username & Password' and the instruction 'Enter your IRM's username and password to continue.'. Below this is a sub-section titled 'Please enter your username and password before continuing...' containing two input fields: 'Username:' and 'Password:'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The footer text reads 'Nullsoft Install System v3.0'.

**Step 8:** If 2-step Verification is enabled then you must enter the security code.

**Step 9:** The IRMAgentService will be installed.

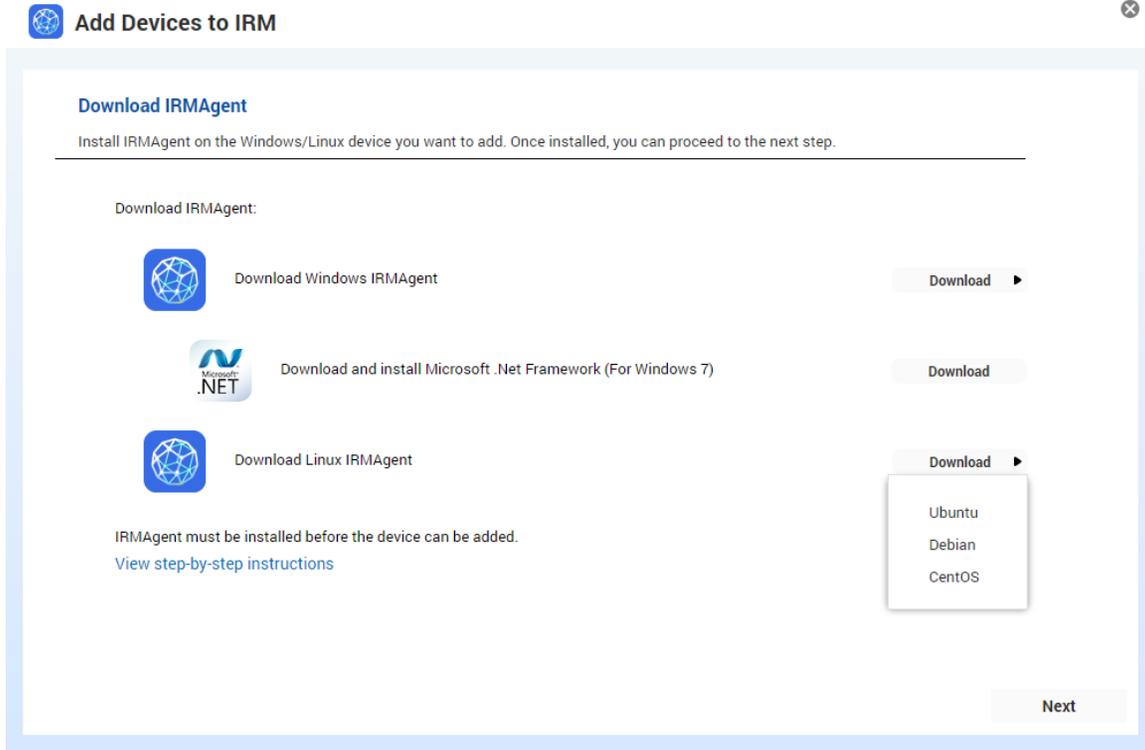


**Step 10:** Click "Finish" and you will see the installation status in the device list.



## 2.4.2 Linux Devices

If a Linux device is selected in Step 3 of Section 2.4, you will be prompted to download IRMAgent for Linux. Click "Download" next to "Download Linux IRMAgent".

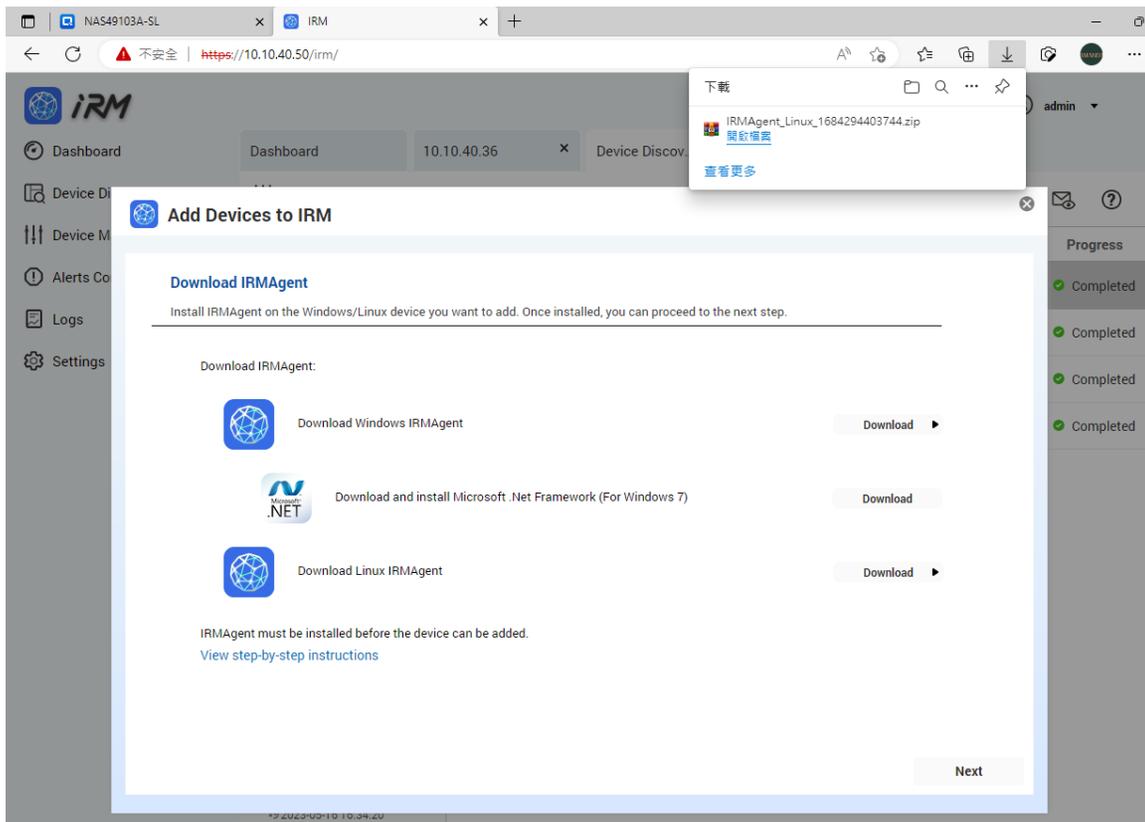


The screenshot shows a window titled "Add Devices to IRM" with a close button in the top right corner. Inside the window, there is a section titled "Download IRMAgent" with the instruction: "Install IRMAgent on the Windows/Linux device you want to add. Once installed, you can proceed to the next step." Below this, there are three download options, each with an icon and a "Download" button:

- Download Windows IRMAgent (with a globe icon) - Download button with a right-pointing arrow.
- Download and install Microsoft .Net Framework (For Windows 7) (with the Microsoft .NET logo) - Download button.
- Download Linux IRMAgent (with a globe icon) - Download button with a right-pointing arrow, which has a dropdown menu open showing "Ubuntu", "Debian", and "CentOS".

Below the download options, there is a note: "IRMAgent must be installed before the device can be added." followed by a link: "[View step-by-step instructions](#)". At the bottom right of the window is a "Next" button.

**Step 1:** After the IRMAgent installation package has been downloaded, copy it to the Linux device to be managed.



**Step 2:** In the Linux shell, unzip the IRM Agent installation package.

```

ubuntu@ubuntu14: ~
ubuntu@ubuntu14:~$
ubuntu@ubuntu14:~$
ubuntu@ubuntu14:~$
ubuntu@ubuntu14:~$ unzip QRMAgent_Linux_1504145467412.zip

```

Use the following command to run the IRM Agent installation program:  
 “sudo bash InstallUbuntuIRMAgent.sh <Client IP Address>”

```

ubuntu@ubuntu14: ~/QRMAgent_Linux_installer
ubuntu@ubuntu14:~/QRMAgent_Linux_installer$
ubuntu@ubuntu14:~/QRMAgent_Linux_installer$
ubuntu@ubuntu14:~/QRMAgent_Linux_installer$
ubuntu@ubuntu14:~/QRMAgent_Linux_installer$ sudo bash InstallUbuntuQRMAgent.sh 192.168.100.95

```

**Step 3:** Enter the IRM Username and Password.

```

ubuntu@ubuntu14: ~/QRMAgent_Linux_installer
ubuntu@ubuntu14:~/QRMAgent_Linux_installer$
ubuntu@ubuntu14:~/QRMAgent_Linux_installer$
ubuntu@ubuntu14:~/QRMAgent_Linux_installer$ sudo bash InstallUbuntuQRMAgent.sh 192.168.100.95
Please enter your QRM+'s username and password to continue.
Please enter your QRM+'s username:
test
Please enter your QRM+'s password:
test
    
```

**Step 4:** Confirm your sign in with 2-step Verification (if enabled).

```

ubuntu@ubuntu14: ~/QRMAgent_Linux_installer
--2017-09-11 17:14:45-- http://192.168.100.1:8080/qrmplusapi/api/v1/account/login
Connecting to 192.168.100.1:8080...connected.
HTTP request sent, awaiting response... 200 OK
Length: 105 [application/json]
Saving to: 'response.json'

100%[=====] 105      --.-K/s   in 0s

2017-09-11 17:14:45 (14.9 MB/s) - 'response.json' saved [105/105]

The first level of authentication is successfully completed. Please enter the security code to proceed.
1) Security Code
2) Lost phone
1
Please enter security code.
Security code:
123456
    
```

**Step 5:** The installation process will be displayed.

```

ubuntu@ubuntu14: ~/QRMAgent_Linux_installer
--2017-09-11 17:16:04-- http://192.168.100.1:8080/qrmplusapi/api/v1/account/login
Connecting to 192.168.100.1:8080...connected.
HTTP request sent, awaiting response... 200 OK
Length: 936 [application/json]
Saving to: 'sec_answer_response.json'

100%[=====] 936      --.-K/s   in 0s

2017-09-11 17:16:04 (133 MB/s) - 'sec_answer_response.json' saved [936/936]

Python 2.7.6
* INFO: PYTHON_PATH:      /usr/bin/python
* INFO: PYTHON_VERSION:   2.7.6

* INFO: System Information:
* INFO: CPU:               GenuineIntel
* INFO: CPU Arch:           x86_64
* INFO: OS Name:             Linux
* INFO: OS Version:         3.13.0-32-generic
* INFO: Distribution:      Ubuntu 14.04
    
```

**Step 6:** You will see the device status in the list.

## 2.5 Add a Device to IRM During Scan

**Step 1:** During the scanning process, select the device to be added as labeled 1 and click the button "Add devices to IRM" as labeled 2.

The screenshot shows the IRM Device Discovery interface. On the left, there are buttons for 'Cancel Scan' and 'Reset All', and a 'Scanning (15%)' progress indicator. Below that is a 'History' section. The main area is a table with columns: Hostname, IP Address, Role, OS, Status, and Progress. The table contains several rows of devices, all with 'Scanning...' in the progress column. The row with IP address 10.10.40.18 is selected, and its checkbox is highlighted with a red box labeled '1'. In the top right corner of the table area, there is a '+' button highlighted with a red box labeled '2'. The bottom of the interface shows pagination: 'Page 1 of 1' and '1 - 18 of 18'.

Hostname	IP Address	Role	OS	Status	Progress
<input type="checkbox"/>	10.10.40.5				🔦 Scanning...
<input type="checkbox"/>	10.10.40.6				🔦 Scanning...
<input type="checkbox"/>	10.10.40.7				🔦 Scanning...
<input type="checkbox"/>	10.10.40.8				🔦 Scanning...
<input type="checkbox"/>	10.10.40.9				🔦 Scanning...
<input type="checkbox"/>	10.10.40.10				🔦 Scanning...
<input type="checkbox"/>	10.10.40.11				🔦 Scanning...
<input checked="" type="checkbox"/>	B10802373-N				🔦 Scanning...

**Step 2:** Refer to *Section 2.4 Steps to Add the Device to IRM* to add devices.

## 2.6 Scan History

IRM maintains a scan history. Users can view the last 5 scans in the history pane of the left column and select the device to install in IRM from the list of discovered devices. Just follow the tutorial in *Section 2.4 Steps to Add the Device to IRM* to add devices to IRM.

Chapter

**3**

# Main Dashboard

---

The Dashboard is the main page of IRM. In the Dashboard, you can add multiple widgets to monitor the health of your device or server. This page allows users to add, remove, reorganize or choose layout, export as PDF, email current view and update widgets.

Note: Devices need to be added to IRM before they can be monitored using gadgets in the dashboard.

### 3.1 Add Widget

Users can add gadgets to the dashboard to continuously monitor the health of the device or server.

The following information can be monitored:

1. CPU usage
2. Memory usage
3. Disk usage
4. Network usage
5. General health status

Users can customize their own Dashboard to monitor multiple devices at the same time. Setup steps are described below:

**Step 1:** Go to the Dashboard page and click the "Add Widget" button.

The screenshot shows the IRM Dashboard interface. On the left is a navigation sidebar with options: Dashboard, Device Discovery, Device Management, Alerts Configuration, Logs, and Settings. The main content area is titled 'Dashboard' and contains several widgets:

- Device State Change Log:** A table with columns: Hostname, IP Address, State, St...
 

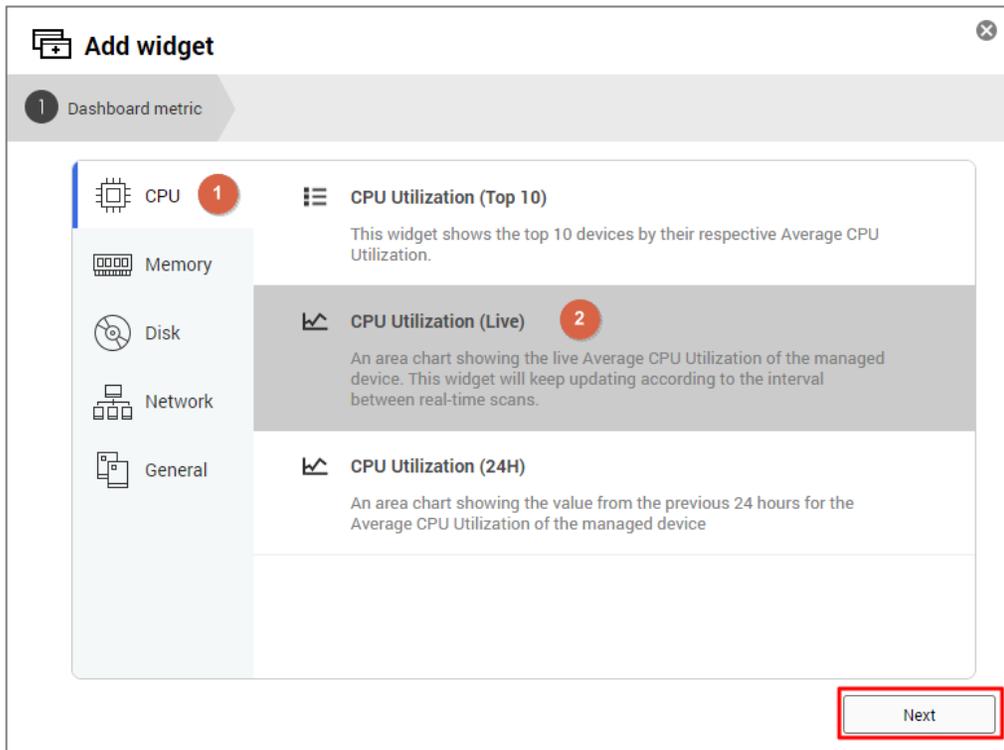
Hostname	IP Address	State	St...
<a href="#">B11100691-N</a>	10.10.100.225	UP	05/...
<a href="#">B11100695-N</a>	10.10.40.36	UP	05/...
- Server Health Overview:** A donut chart showing 2 Up (green), 0 Down (red), and 0 Not reachable (yellow).
- Memory Utilization (Top 10):** A table with columns: Hostname, IP Address, % Utilization
 

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	64.10 %
<a href="#">B11100691-N</a>	10.10.100.225	36.50 %
- Shutdown Devices (Recent 10):** A table with columns: Hostname, IP Address, Shutdown Time. Below the table, it says "No data could be shown."

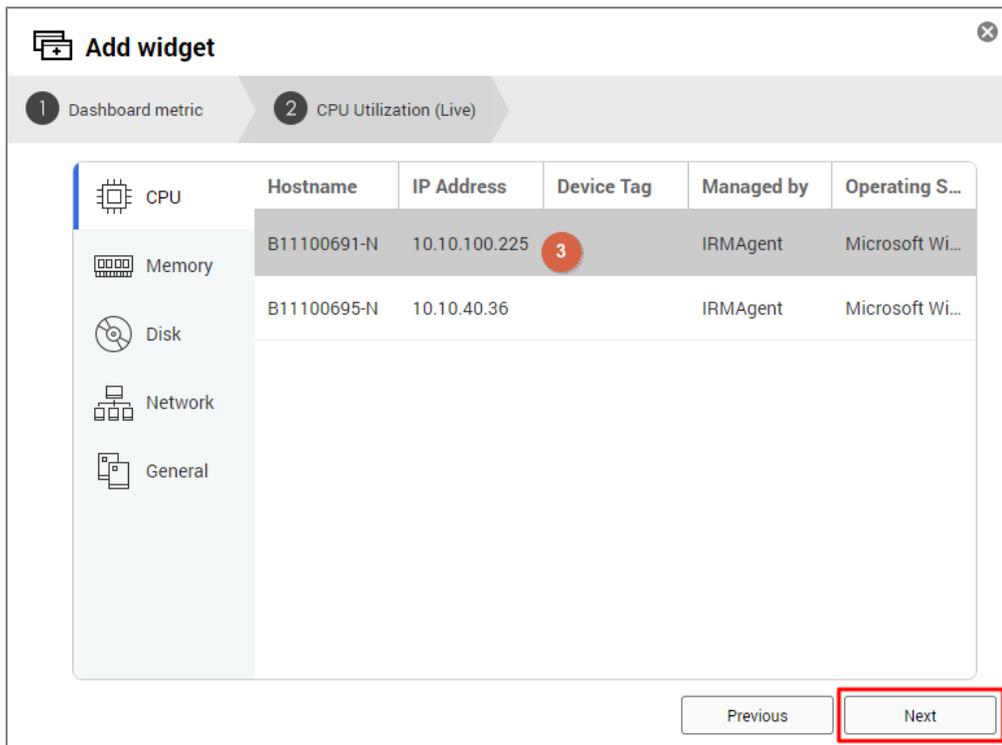
A red box highlights the '+' icon in the top right of the dashboard area, which is used to add new widgets.

**Step 2:** Select the type of data you want to monitor:

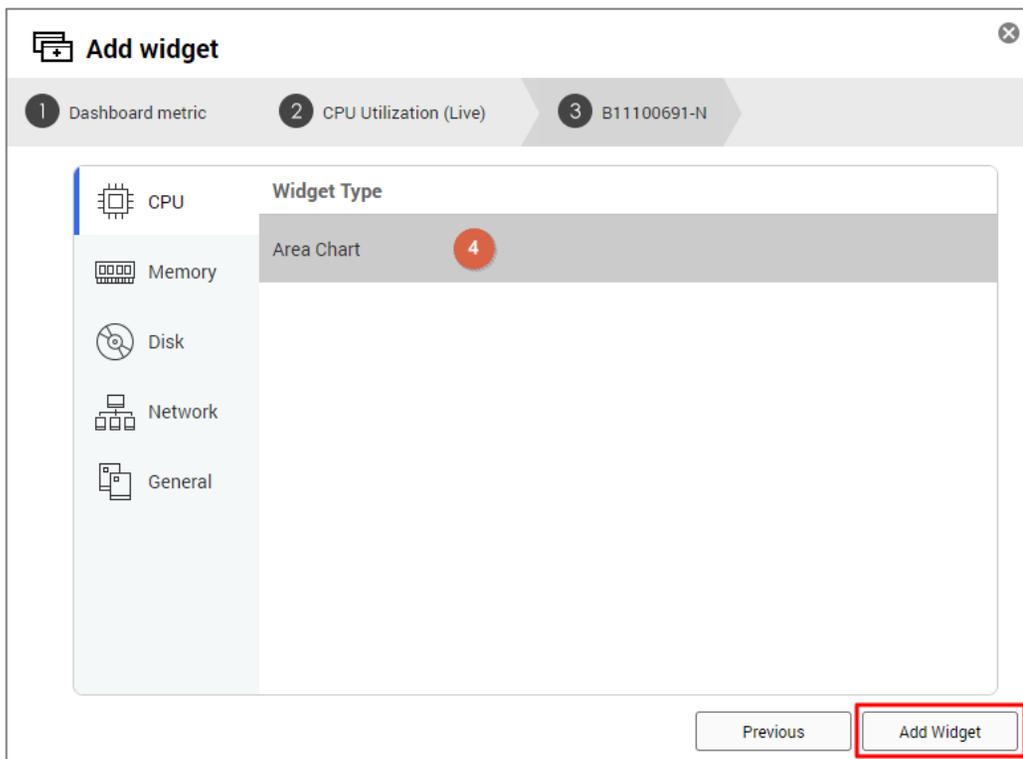
- (1) Select the data type you want to monitor in the left column. There are six types: CPU usage, memory usage, disk usage, network usage and general health status.
- (2) Select the method of data presentation that matches your needs.
- (3) Click "Next".



**Step 3:** After selecting the device you want to monitor, click "Next".



**Step 4:** After selecting the type of chart, click the "Add Widget" button to complete the operation.



**Step 5:** When the setup is complete, the widget will be added to the last position in the Dashboard

The screenshot shows the iRM dashboard interface. It features a top navigation bar with the iRM logo, a user profile for 'admin', and a 'Dashboard' breadcrumb. The main content area is divided into several widgets:

- Memory Utilization (Top 10):** A table showing memory usage for two hosts.
 

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	65.50 %
<a href="#">B11100691-N</a>	10.10.100.225	48.60 %
- Shutdown Devices (Recent 10):** A table with columns for Hostname, IP Address, and Shutdown Time. It currently displays "No data could be shown."
- Disk Utilization (Top 10):** A table showing disk usage for two hosts.
 

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	64.66 %
<a href="#">B11100691-N</a>	10.10.100.225	20.28 %
- CPU Utilization (Live):** A line graph for host B11100691-N showing CPU usage over time. The y-axis is labeled "% Utilization" (0-100) and the x-axis is labeled "Time" (13:10:02 to 13:11). The graph shows a very low, stable utilization level. This widget is highlighted with a red border.

### 3.2 Delete All Widgets in the Dashboard

Setup steps: Go to the Dashboard page and click the "Delete All Widgets" button.

The screenshot shows the iRM dashboard interface. At the top right, there is a user profile dropdown for 'admin'. Below the dashboard title, there are several icons: a refresh icon (circular arrow), a trash icon (highlighted with a red box), a print icon, an email icon, and a help icon. The dashboard contains four main widgets:

- Device State Change Log:** A table with columns: Hostname, IP Address, State, and State Change Ti...
 

Hostname	IP Address	State	State Change Ti...
<a href="#">B11100691-N</a>	10.10.100.225	UP	05/17/2023 01:08:...
<a href="#">B11100695-N</a>	10.10.40.36	UP	05/17/2023 01:02:...
- Server Health Overview:** A donut chart showing server health. A legend indicates: 2 Up (green), 0 Down (red), and 0 Not reachable (yellow).
- Disk Utilization (Top 10):** A table with columns: Hostname, IP Address, and % Utilization.
 

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	64.66 %
<a href="#">B11100691-N</a>	10.10.100.225	20.30 %
- Memory Utilization (Top 10):** A table with columns: Hostname, IP Address, and % Utilization.
 

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	66.00 %
<a href="#">B11100691-N</a>	10.10.100.225	50.60 %

### 3.3 Refresh All Widgets in the Dashboard

Setup steps: Go to the Dashboard page and click the Refresh button.

This screenshot is identical to the previous one, showing the iRM dashboard with the same widgets and data. In this version, the refresh icon (a circular arrow) in the top right of the dashboard area is highlighted with a red box, indicating the step to refresh all widgets.

### 3.4 Select the Layout Mode

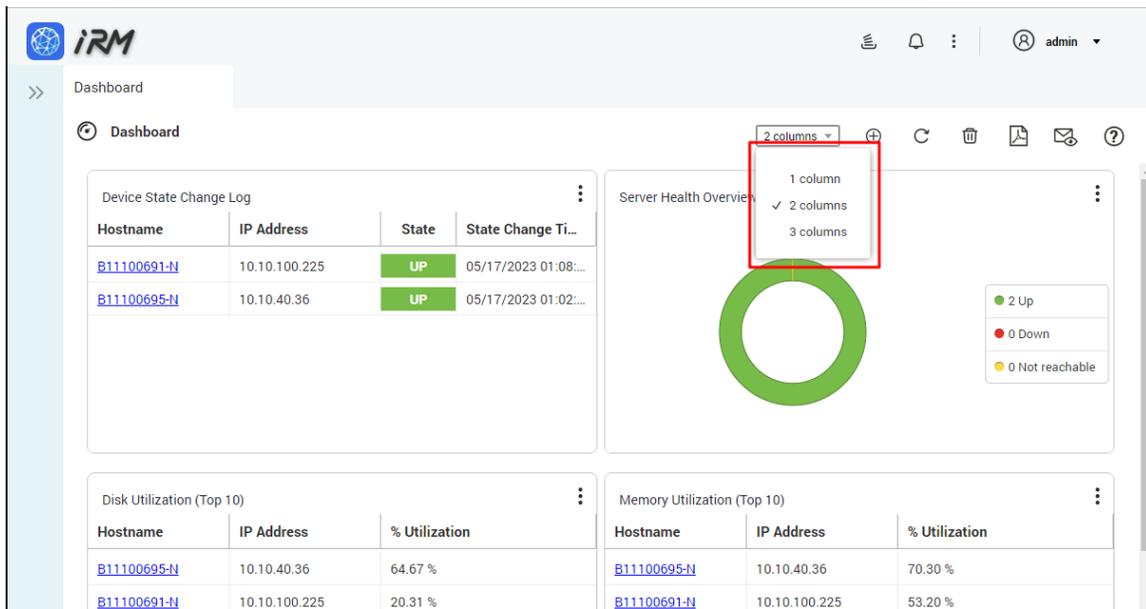
User can adjust the layout of the main Dashboard according to their requirements. IRM Dashboard provides:

- 1 column display
- 2 columns display
- 3 columns display

After selecting one of the three layout modes, all widgets will be adjusted accordingly. Setup steps are described below:

**Step 1:** Go to the Dashboard page and click the select layout menu.

**Step 2:** Select "1 column", "2 columns" or "3 columns" from the dropdown list.



The screenshot shows the IRM Dashboard interface. A dropdown menu is open over the 'Server Health Overview' widget, displaying three options: '1 column', '2 columns' (which is selected and has a checkmark), and '3 columns'. The dashboard contains several widgets: 'Device State Change Log' with a table of hostnames and states, 'Server Health Overview' with a donut chart, 'Disk Utilization (Top 10)', and 'Memory Utilization (Top 10)'. The user's profile 'admin' is visible in the top right corner.

Hostname	IP Address	State	State Change Ti...
<a href="#">B11100691-N</a>	10.10.100.225	UP	05/17/2023 01:08:...
<a href="#">B11100695-N</a>	10.10.40.36	UP	05/17/2023 01:02:...

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	64.67 %
<a href="#">B11100691-N</a>	10.10.100.225	20.31 %

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	70.30 %
<a href="#">B11100691-N</a>	10.10.100.225	53.20 %

### 3.5 Export as PDF File

You can export view from the current dashboard as PDF files and download them to your local computer. Setup steps are described below:

**Step 1:** Go to the Dashboard page and click the Export as PDF File button.

The screenshot shows the iRM dashboard with the following components:

- Device State Change Log:**

Hostname	IP Address	State	State Change Ti...
<a href="#">B11100691-N</a>	10.10.100.225	UP	05/17/2023 01:08:...
<a href="#">B11100695-N</a>	10.10.40.36	UP	05/17/2023 01:02:...
- Server Health Overview:** A donut chart showing 2 Up (green), 0 Down (red), and 0 Not reachable (yellow).
- Disk Utilization (Top 10):**

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	64.66 %
<a href="#">B11100691-N</a>	10.10.100.225	20.30 %
- Memory Utilization (Top 10):**

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	66.00 %
<a href="#">B11100691-N</a>	10.10.100.225	50.60 %

A red box highlights the 'Export as PDF' icon in the top right toolbar.

**Step 2:** Showing "Generating View as PDF".

**Step 3:** Download the view to the local computer.

The screenshot shows the iRM dashboard with the following components:

- Report generation in progress...** banner at the top.
- Device State Change Log:** (Same as in the previous screenshot)
- Server Health Overview:** Donut chart showing 2 Up, 0 Down, 0 Not reachable. A tooltip 'Export as PDF' is visible over the chart.
- Disk Utilization (Top 10):**

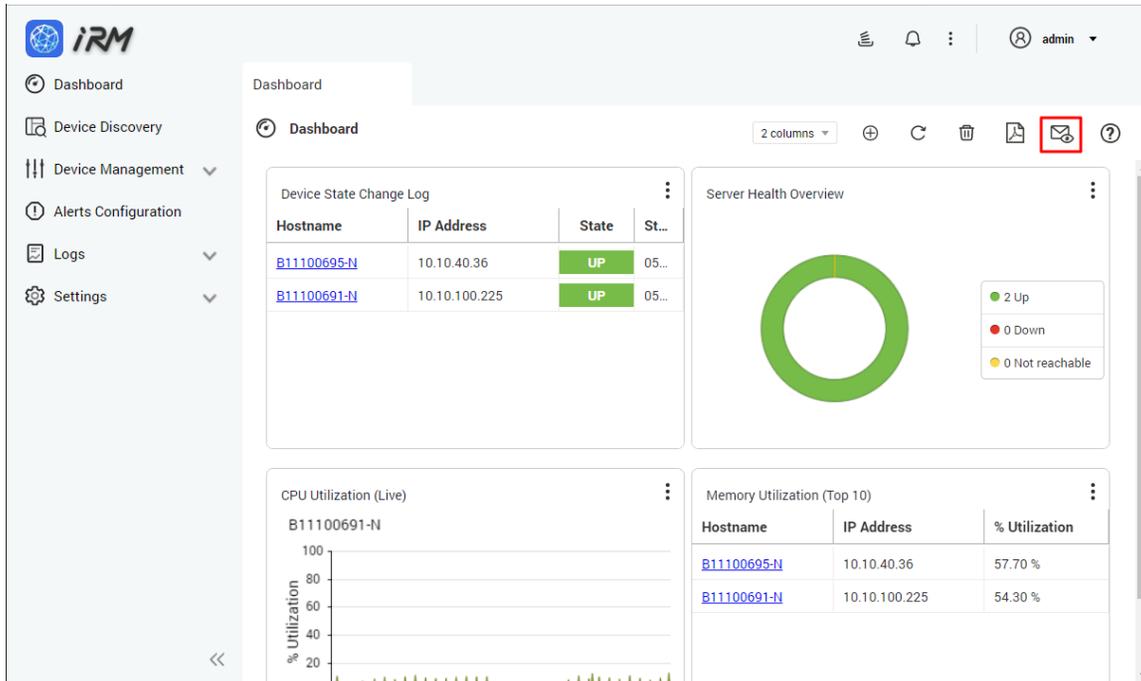
Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	64.65 %
<a href="#">B11100691-N</a>	10.10.100.225	20.32 %
- Memory Utilization (Top 10):**

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	68.40 %
<a href="#">B11100691-N</a>	10.10.100.225	55.20 %

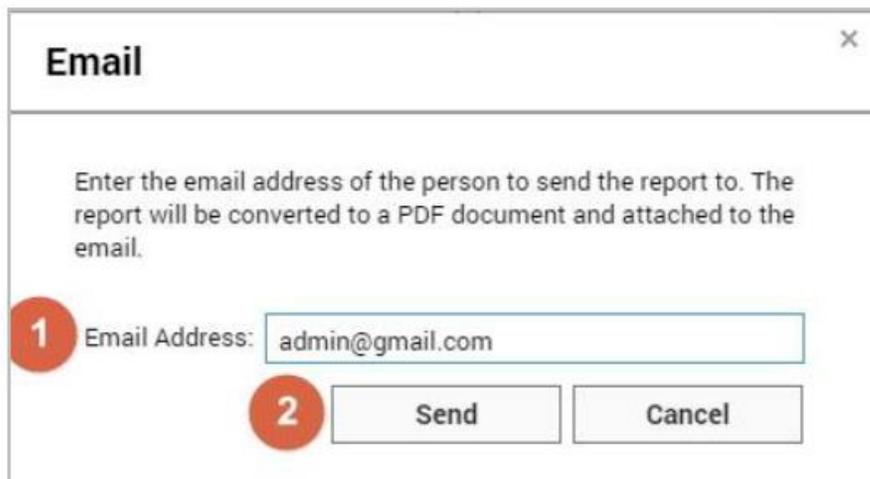
### 3.6 Email Current View

You can export the view from your current dashboard as PDF files and email them to a custom Email address. (Note: This function requires SMTP-related settings to be set up in the "Settings" page). Setup steps are described below:

**Step 1:** Go to the Dashboard page and click the "Email current view" button.



**Step 2:** After entering the mail address, click the "Send" button.



**Step 3:** When "Sending email..." message appears, the mail is being sent in the background.

The screenshot shows the iRM dashboard interface. At the top, a blue notification bar displays "Sending email to specified email address(s)...". The dashboard includes a left sidebar with navigation options: Dashboard, Device Discovery, Device Management, Alerts Configuration, Logs, and Settings. The main content area is titled "Dashboard" and contains several widgets:

- Device State Change Log:** A table with columns: Hostname, IP Address, State, and St...
 

Hostname	IP Address	State	St...
<a href="#">B11100695-N</a>	10.10.40.36	UP	05...
<a href="#">B11100691-N</a>	10.10.100.225	UP	05...
- Server Health Overview:** A donut chart showing server health. A legend indicates: 2 Up (green), 0 Down (red), and 0 Not reachable (yellow).
- CPU Utilization (Live):** A line graph for device B11100691-N showing % Utilization over time. The y-axis ranges from 0 to 100.
- Memory Utilization (Top 10):** A table with columns: Hostname, IP Address, and % Utilization.
 

Hostname	IP Address	% Utilization
<a href="#">B11100695-N</a>	10.10.40.36	57.70 %
<a href="#">B11100691-N</a>	10.10.100.225	54.30 %

### 3.7 Real-time and Historical Data Presentation

IRM provides both real-time and historical data presentation:

1. **Real-time Data Widget:** Updates your data every 10 seconds after you have added the widget.
2. **24 Hours Data Widget:** displays historical data trends of the last 24 hours at any time, updated once every 60 seconds.

Note: All widgets can be dragged and moved within the Dashboard.

Chapter

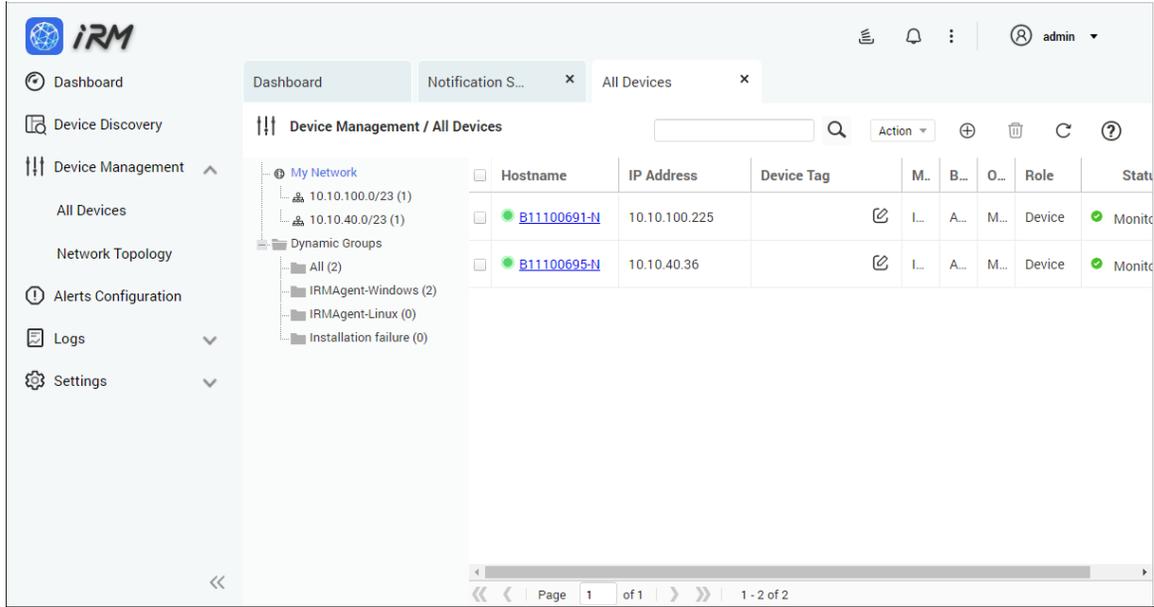
**4**

# Device Management

---

## 4.1 Device List

The Device Management page provides a list of all the devices currently managed by IRM, along with their brief information and associated status. Users can quickly find the device and find out their current status using the Device Management page.



The screenshot shows the IRM web interface. The left sidebar contains navigation options: Dashboard, Device Discovery, Device Management (expanded), Alerts Configuration, Logs, and Settings. The main content area is titled 'Device Management / All Devices' and displays a table of devices. The table has columns for Hostname, IP Address, Device Tag, M., B., O., Role, and Status. Two devices are listed, both with a green status indicator and 'Monit' in the status column.

Hostname	IP Address	Device Tag	M.	B.	O.	Role	Status
B11100691-N	10.10.100.225		I...	A...	M...	Device	Monit
B11100695-N	10.10.40.36		I...	A...	M...	Device	Monit

### 4.1.1 Device Name

Device Name not only differentiates the different devices, through different light colors, it also shows its current connection status with IRM.

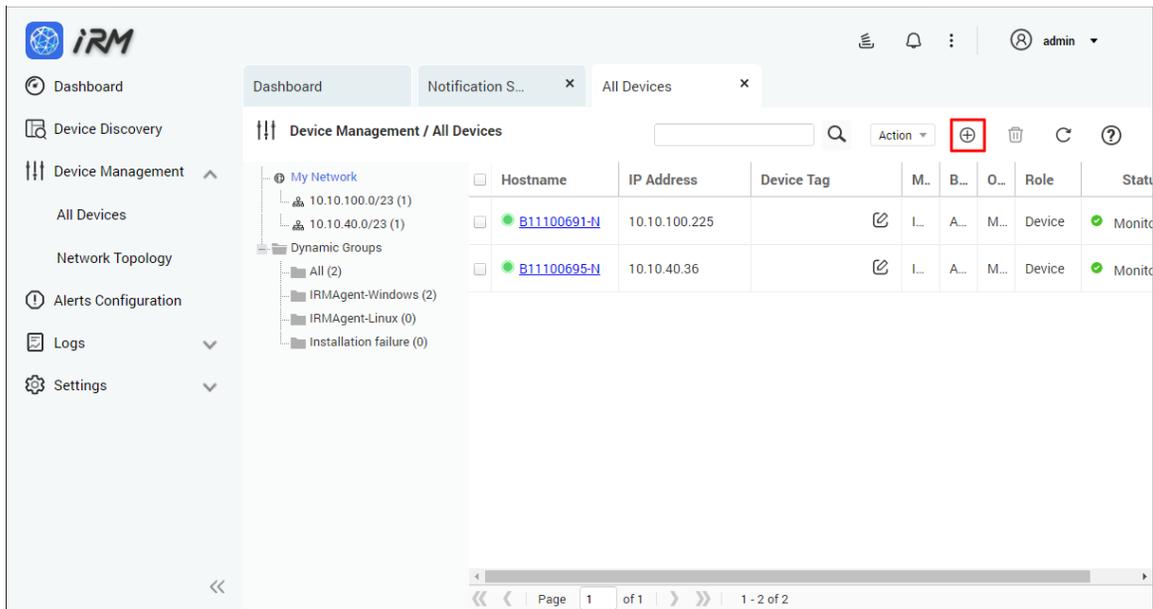
### 4.1.2 Status

Users will know whether the device is currently being monitored by IRM by looking at the Status column. Additional IRMAgent must be installed for it to be monitored via IRM.

### 4.1.3 Add Device

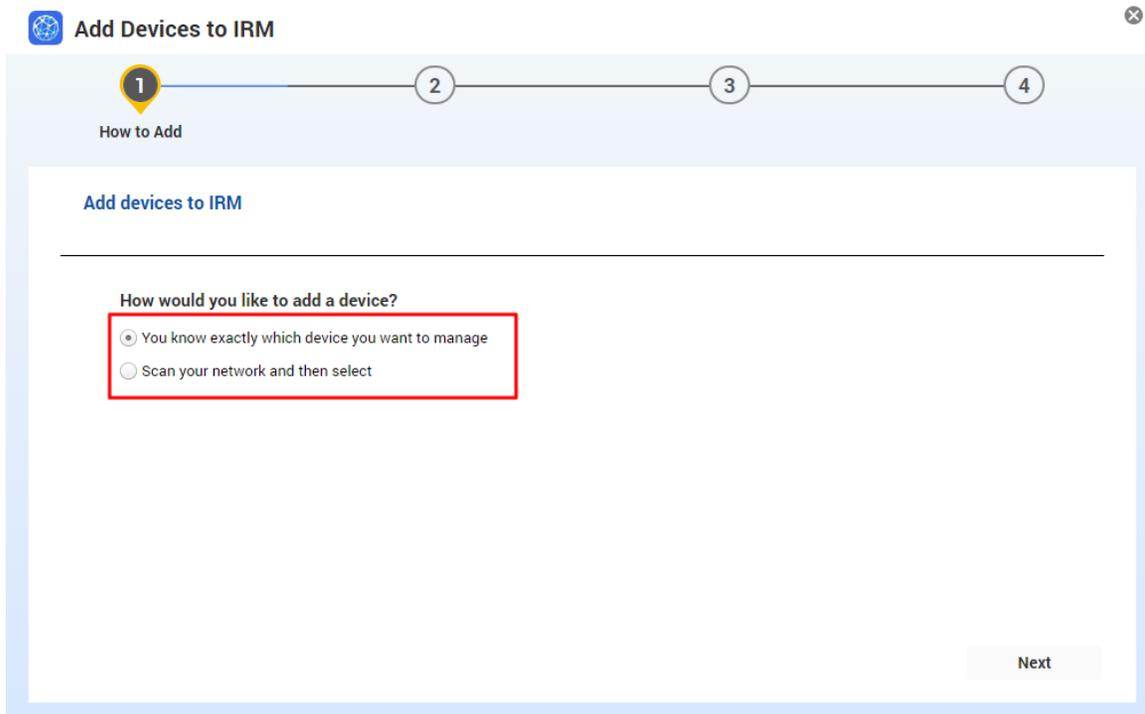
Users can add devices to IRM management via the Add Device feature. To add devices, follow the steps below:

**Step 1:** Click the "Add Device" button.



**Step 2:** Choose how you want to add the device.

1. Quickly add the specified device
2. Search the network to help you find the device to add



### 4.1.3.1 Quickly add the specified device

Select "You know exactly which device you want to manage", and click the "Next" button.

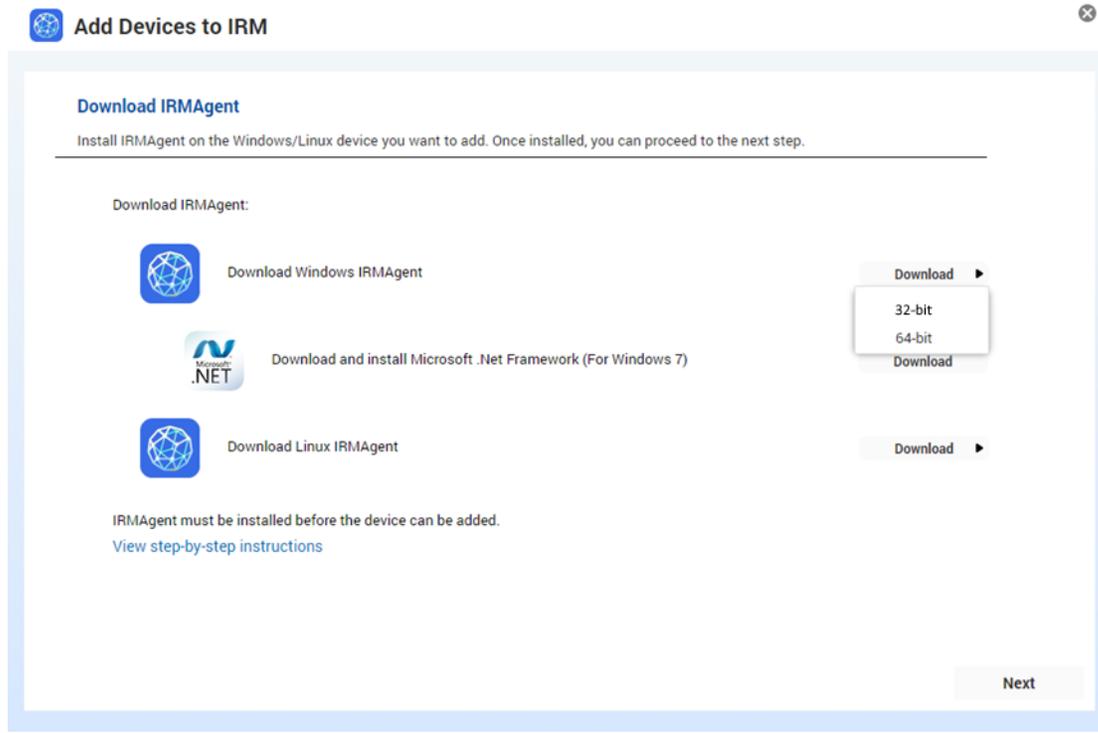
The screenshot shows a window titled "Add Devices to IRM" with a close button in the top right. A progress bar at the top has four steps: 1 (active, highlighted with a yellow circle), 2, 3, and 4. Below the progress bar, the text "How to Add" is displayed. The main content area is titled "Add devices to IRM" and contains the question "How would you like to add a device?". There are two radio button options: "You know exactly which device you want to manage" (which is selected and highlighted with a red box) and "Scan your network and then select". A "Next" button is located at the bottom right of the content area, also highlighted with a red box.

### 1. Windows Devices

**Step 1:** Select "Windows Device", and click the "Next" button.

The screenshot shows the same "Add Devices to IRM" window, now at Step 2. The progress bar shows Step 1 as completed (with a checkmark) and Step 2 as active (with a yellow circle). The text "How to Add" is replaced by "Select Device Type". The main content area is titled "Add devices to IRM" and contains the instruction "Select the device type to be added". Under the heading "Device type", there are two radio button options: "Windows Devices" (which is selected and highlighted with a red box) and "Linux Devices". At the bottom right, there are two buttons: "« Previous" and "Next" (highlighted with a red box).

**Step 2:** Click the "Download Windows IRMAgent" button to download the installation package.

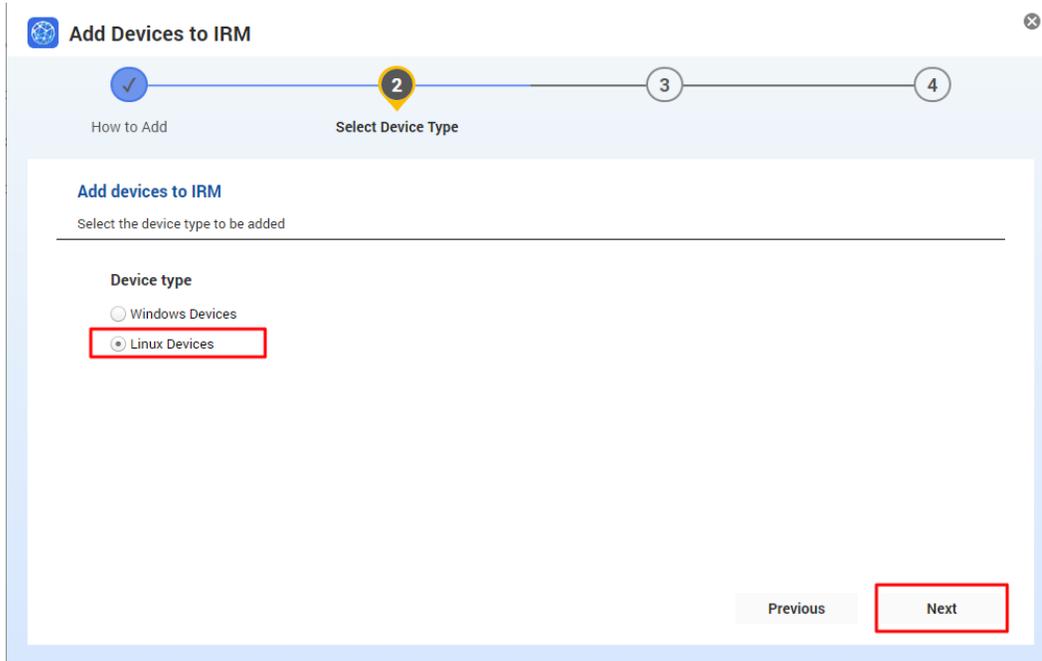


**Step 3:** Copy the installation package to the device you want to manage. After decompressing and running the installation program, you can check the installation status in the device list.

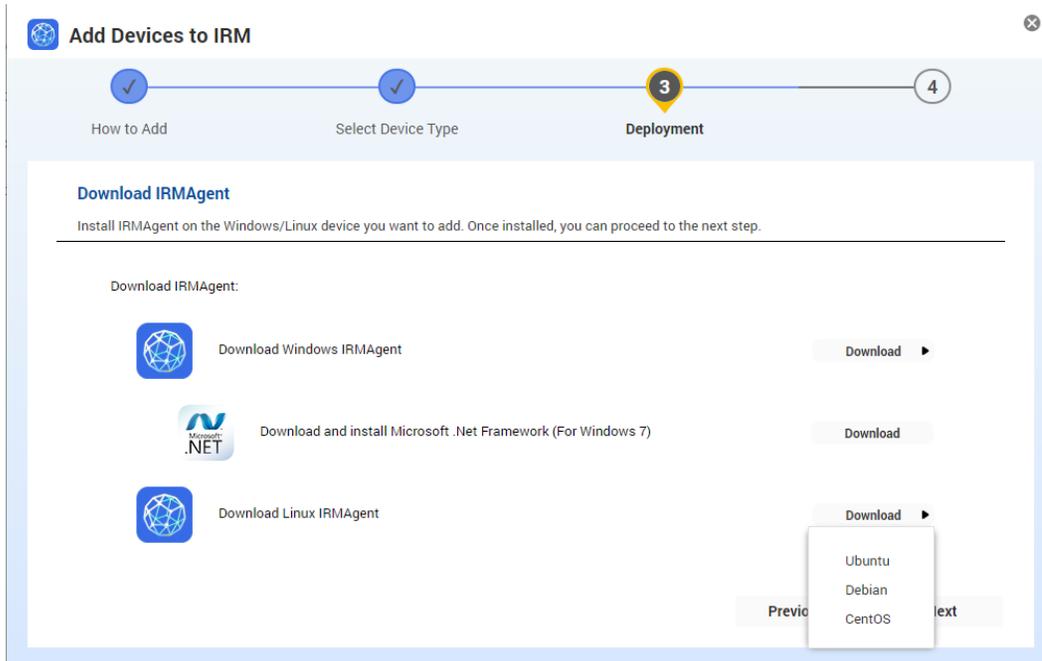
Refer to *Section 2.4 Steps to Add the Device to IRM* to know installation instructions.

## 2. Linux Devices

**Step 1:** Select "Linux Device", and click the "Next" button.



**Step 2:** You can view the progress of installation or press the "Finish" button to go to the device list page. Subsequent results of installation status will also be displayed in the device list screen.



Refer to "2.4 Steps to Add the Device to IRM" to know installation instructions.

### 4.1.3.2 Search the network to help you find the device to add

**Step 1:** Select "Scan your network and then select", and click the "Next" button.

**Add Devices to IRM** [Close]

1 How to Add 2 3 4

**Add devices to IRM**

---

How would you like to add a device?

You know exactly which device you want to manage

Scan your network and then select

**Next**

**Step 2:** Select to scan by IP Range or Subnet. Define the scan range and click "Start Scan" button to discover devices on the network.

**Add Devices to IRM** [Close]

1 How to Add 2 Device Discovery 3 4

**Select devices to add to IRM**

Allow users to discover computer devices on the current network based on their defined scan range and quickly incorporate them into IRM.

**Scan Devices**

IP Range: Start IP: 10 10 40 1 End IP: 10 10 40 255

Subnet: Subnet: 10.10.40.1 / 24

**Start Scan**

Search: [ ] All devices

Hostname	IP Address ↓	Role	OS	Status	Progress
No device found.					

Previous Add selected devices

**Step 3:** Select devices from the list of scan result and click “Add selected devices” button to add devices to IRM.

**Add Devices to IRM**

How to Add | Device Discovery | **Deployment** | 4

**Select devices to add to IRM**

Allow users to discover computer devices on the current network based on their defined scan range and quickly incorporate them into IRM.

Scan Devices

IP Range: Start IP 10 10 40 1 End IP 10 10 40 255 Scan Completed 100% Start Scan

Subnet: Subnet: 10.10.40.1 / 24

	Hostname	IP Address ↑	Role	OS	Status	Progress
<input type="checkbox"/>	10.10.40.39	10.10.40.39	Device	Linux	New Device	Completed
<input type="checkbox"/>	10.10.40.49	10.10.40.49	Unknown	Unknown	New Device	Completed
<input checked="" type="checkbox"/>	NAS49103A-SL	10.10.40.50	Unknown	Unknown	New Device	Completed
<input type="checkbox"/>	NAS49103A-SL	10.10.40.51	Unknown	Unknown	New Device	Completed
<input type="checkbox"/>	B10100813-P	10.10.40.52	Device	Windows	New Device	Completed

Previous **Add selected devices**

#### 4.1.4 Remove Device

Users can use the Delete Device button to remove devices from the list of IRM managed devices, and remove the related data as well.

#### 4.1.5 Reinstall

If a user's device fails during installation due to an unexpected error, such as a sudden network interruption, the user can click the "Action" button and select "Reinstall" to quickly reinstall it.

#### 4.1.6 Power Control

You can power control the remote unit, such as performing power-off or restart. Click the "Action" button and select "Power Control" to perform the action.

**NOTE:**

If all devices show turned off, the default gateway may have changed. Confirm the network

settings on the NAS.

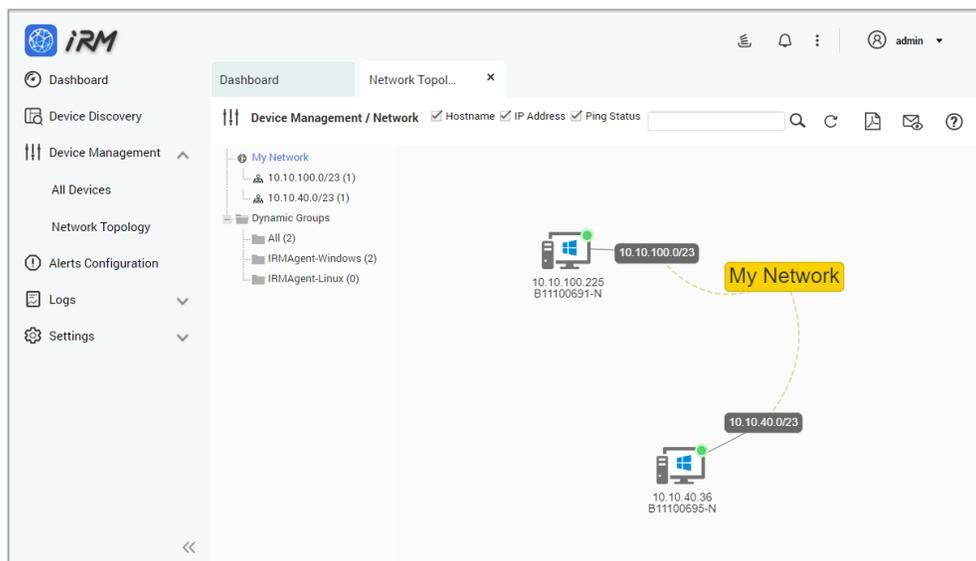
Step 1: Log in to QTS and open "Network & Virtual Switch".

Step 2: Check the network ports that can reach the Internet.

Step 3: Manually select the network port that can reach the Internet.

## 4.2 Network Topology

IRM provides visual network topology to quickly present the managed device's network structure, automatically groups devices based on device information, and changes status icons according to the current real-time status.



1. My network shows different subnet groups
2. Dynamic Groups will automatically sub-group according to subnet, operating system and other information
3. Device Name
4. IP address of the device
5. Current status of the managed device (Power On, Power Down, or network outage)
6. Device Discovery

Chapter

5

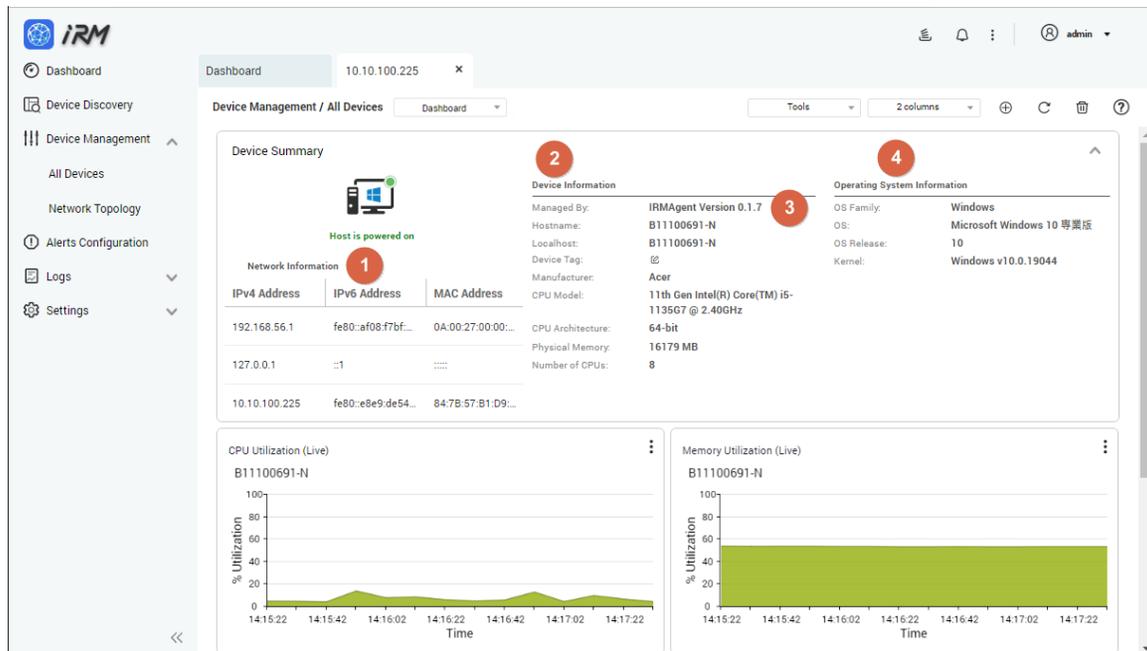
# Single Device Management

---

## 5.1 Single Device Dashboard

Single Device Dashboard provides detailed information about a specific managed device, including:

1. Network information
2. Device Information
3. IRMAgent version
4. Operating system information



In Single Device Dashboard, users can add or remove widgets, select layout modes, and use the tools in the tool set to manage IRMAgent devices.

## 5.2 Add Widget

Users can add multiple widgets to customize Single Device Dashboard to monitor CPU usage, memory usage, disk usage, network usage and more, there are also multiple chart types at the user's disposition. Setup steps are described below:

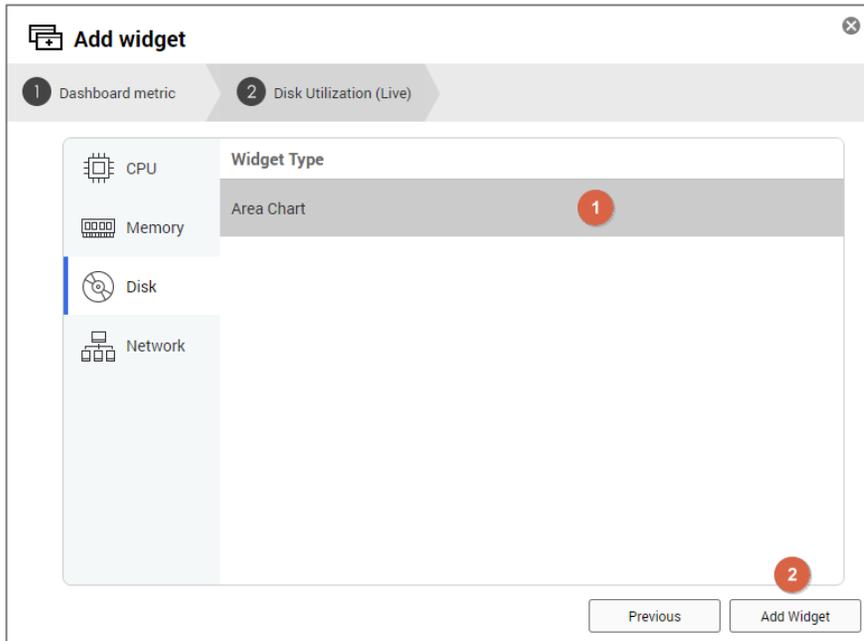
**Step 1:** Go to Single Device Dashboard page and click the "Add Widget" button.

**Step 2:** Complete the settings of data type and data range to be monitored:

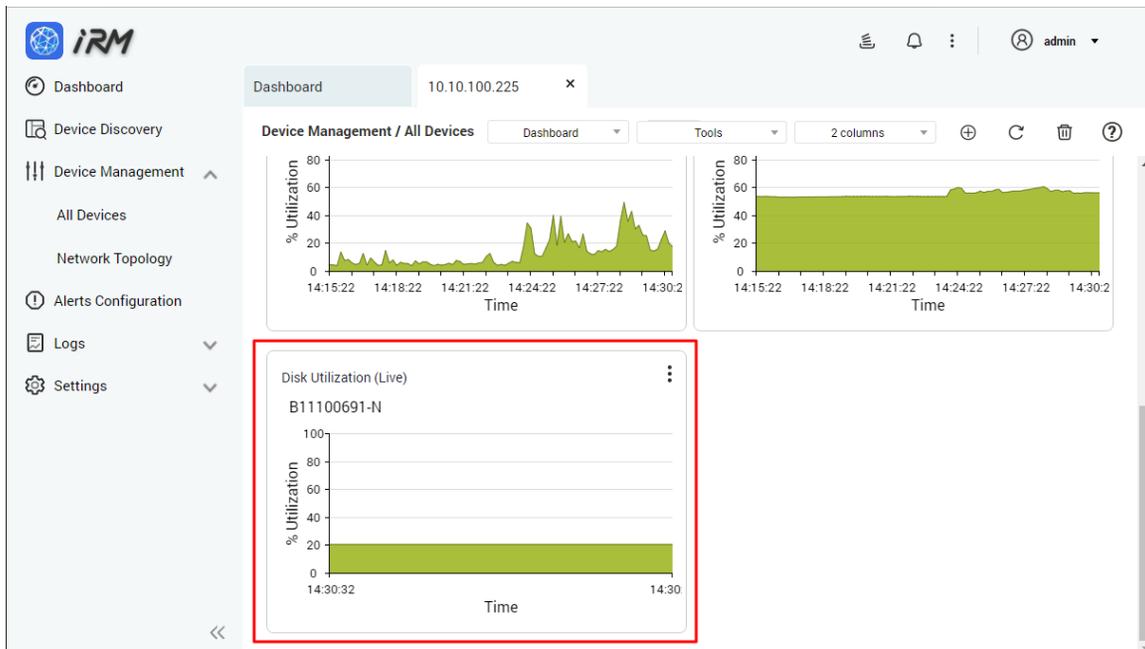
1. Select the type of data you want to monitor. There are four types: CPU usage, memory usage, disk usage, and network usage.
2. Select the data range (real-time data or last 24 hours of historical data).
3. Click "Next".

**Step 3:** Complete the chart type setting:

1. Select the type of chart.
2. Click the "Add Widget" button to complete the operation.

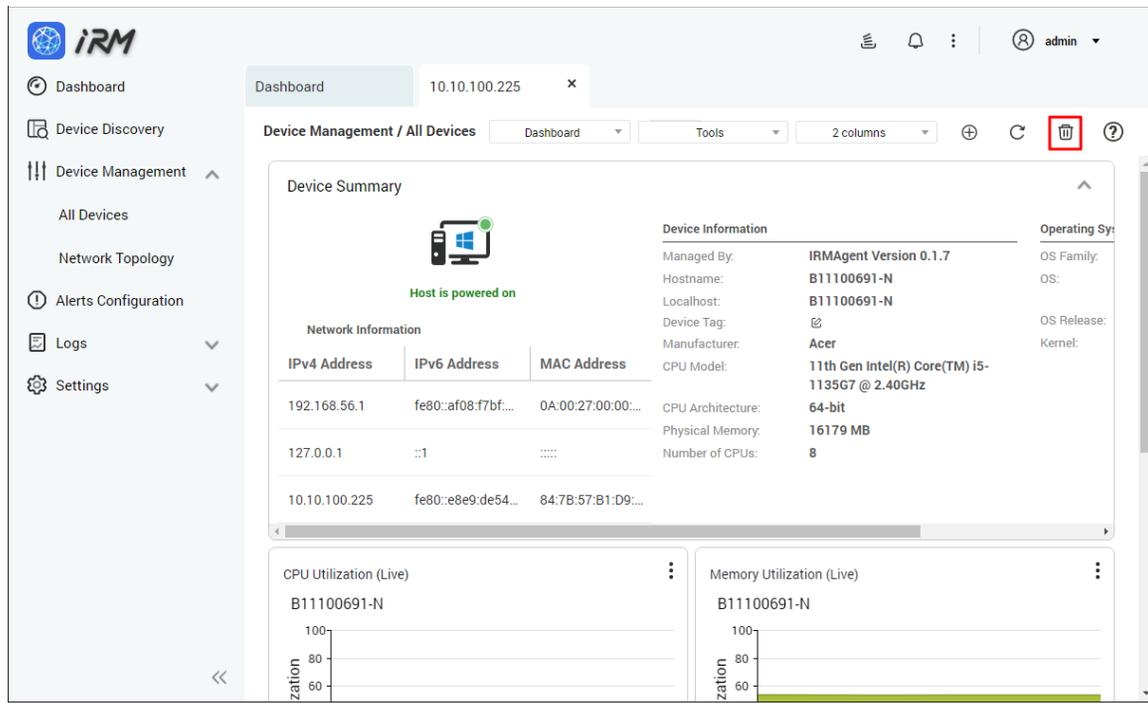


**Step 4:** When the setup is complete, the widget will be added to the last position in the Dashboard



### 5.3 Delete All Widgets in the Single Device Dashboard

Setup steps: Go to the Single Device Dashboard page and click the "Delete All Widgets" button.



### 5.4 Refresh All Widgets Information in the Dashboard

Setup steps: Go to the Single Device Dashboard page and click the "Refresh" button.

The screenshot shows the iRM web interface for a single device. The main content area is titled 'Device Management / All Devices' and shows details for the device with IP address 10.10.100.225. A red box highlights a refresh icon in the top right corner of the device management header.

**Device Summary**

Host is powered on

**Network Information**

IPv4 Address	IPv6 Address	MAC Address
192.168.56.1	fe80::af08:f7bf...	0A:00:27:00:00:...
127.0.0.1	::1	.....
10.10.100.225	fe80::e8e9:de54...	84:7B:57:B1:D9:...

**Device Information**

- Managed By: IRMAgent Version 0.1.7
- Hostname: B11100691-N
- Localhost: B11100691-N
- Device Tag: @
- Manufacturer: Acer
- CPU Model: 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
- CPU Architecture: 64-bit
- Physical Memory: 16179 MB
- Number of CPUs: 8

**Operating System Information**

- OS Family:
- OS:
- OS Release:
- Kernel:

**CPU Utilization (Live)**

B11100691-N

zation

**Memory Utilization (Live)**

B11100691-N

zation

## 5.5 Select the Layout Mode

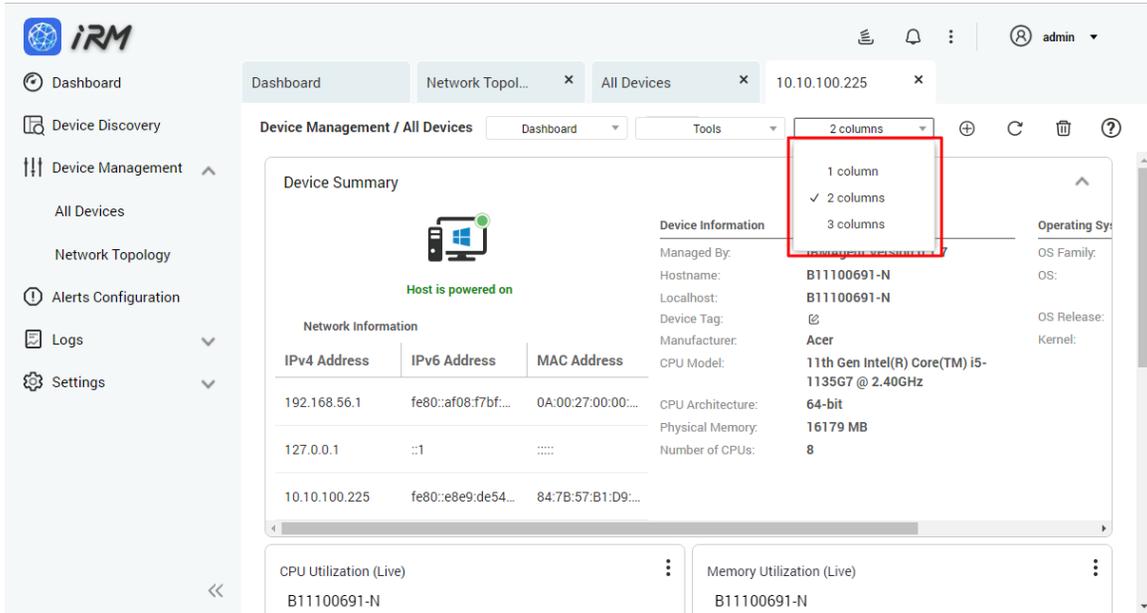
Users can customize the layout of Single Device Dashboard, and the widgets will re-arrange themselves accordingly.

- 1 column display
- 2 columns display
- 3 columns display

Setup steps are described below:

**Step 1:** Go to the Single Device Dashboard page and click the select layout menu.

**Step 2:** Select "1 column", "2 columns" or "3 columns" from the dropdown list.



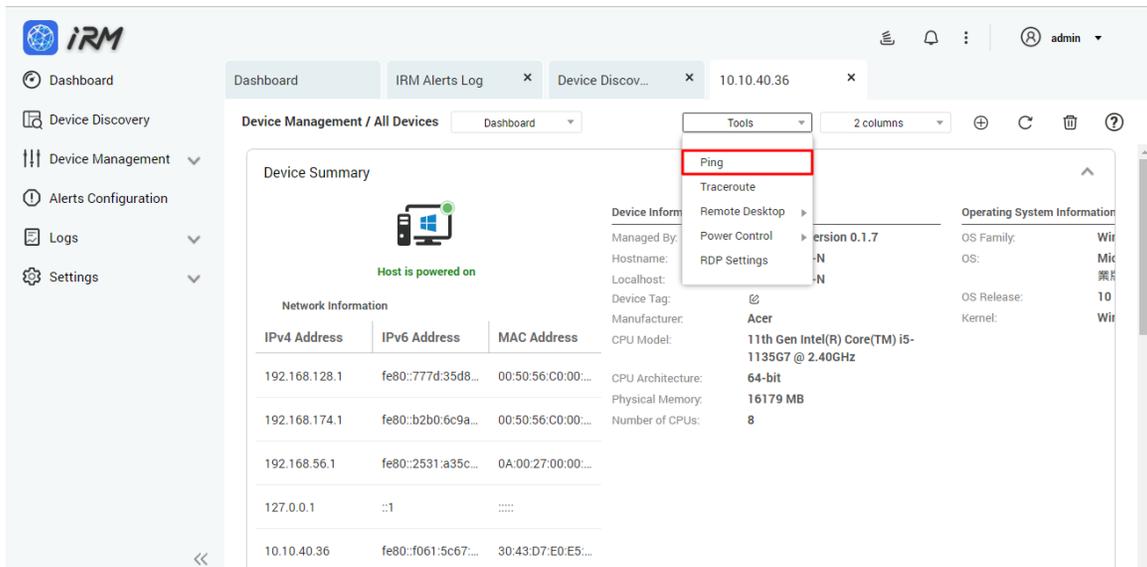
## 5.6 Tools - Ping

IRM provides Ping monitoring function to test whether a packet can reach a specific device through IP protocol and to view the connection status of IRM with the device

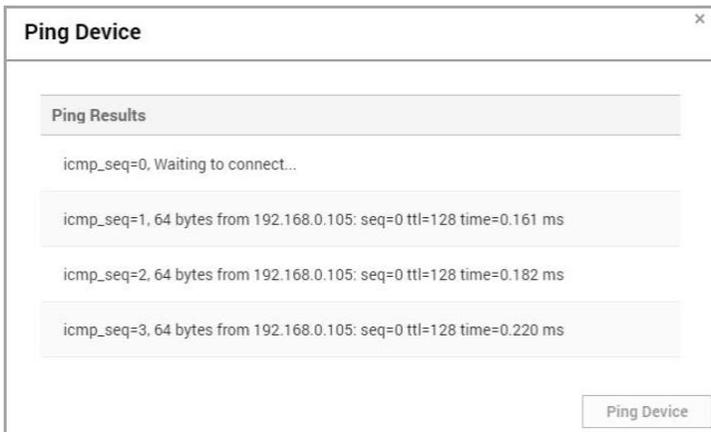
Setup steps are described below:

**Step 1:** Go to IRMAgent Single Device Dashboard page and click the "Tools" button.

**Step 2:** Select "Ping".



**Step 3:** A window pops up and displays the Ping command execution result.



**Step 4:** Click the Ping Device button to Ping again.

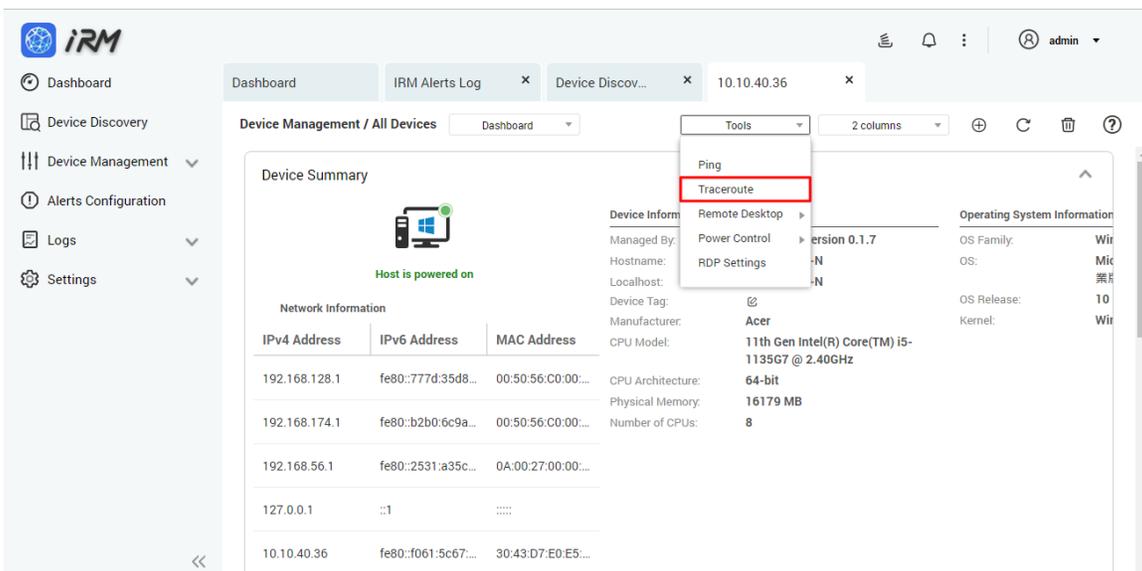
## 5.7 Tools – Traceroute

IRM provides Traceroute monitoring, which displays the IP addresses of the routers throughout the IP network in a new window.

Setup steps are described below:

**Step 1:** Go to IRMAgent Single Device Dashboard page and click the "Tools" button.

**Step 2:** Select "Traceroute".



**Step 3:** A window pops up and displays the Traceroute command execution result.



## 5.8 Tools - Remote Desktop

IRM provides integrated remote desktop functionality, you can select the appropriate remote access method according to different device types:

1. Windows device: RDP or VNC remote desktop
2. Linux device: VNC remote desktop or SSH connection (no need to install SSH client program)

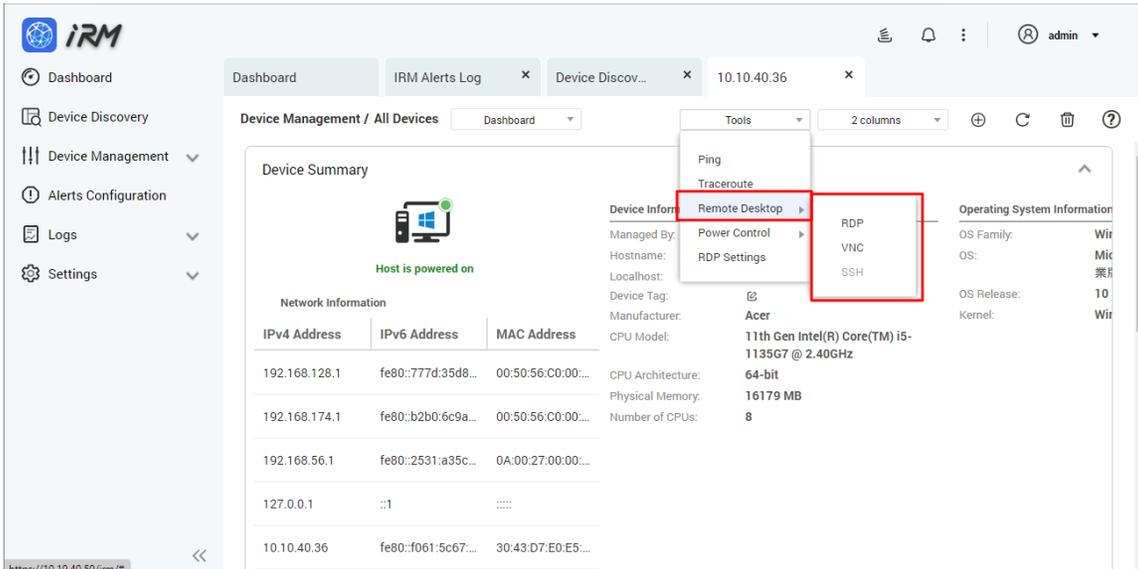
Note: The remote device must enable the option to allow users to connect to the computer Setup steps are described below:

**Step 1:** Go to IRMAgent Single Device Dashboard page and click the "Tools" button.

**Step 2:** Select "Remote Desktop".

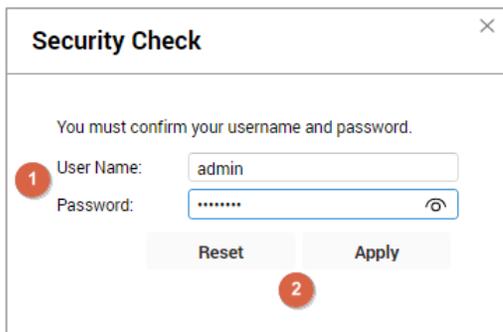
**Step 3:** Select the appropriate remote access method according to different device types.

1. Windows device: RDP or VNC Remote Desktop (users need to install VNC server program on Windows device)
2. Linux device: VNC remote desktop or SSH connection (no need to install SSH client program)



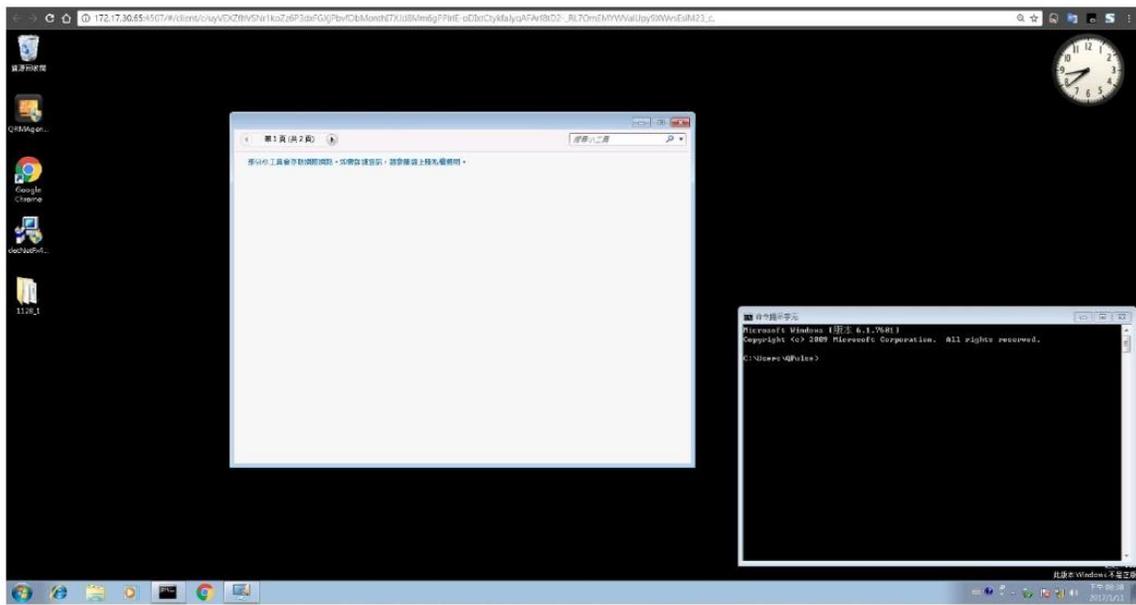
**Step 4:** A security check window will pop up, asking the user to enter the remote device account number and password.

**Step 5:** Select the "Apply" button, or click the "Reset" button to re-enter.

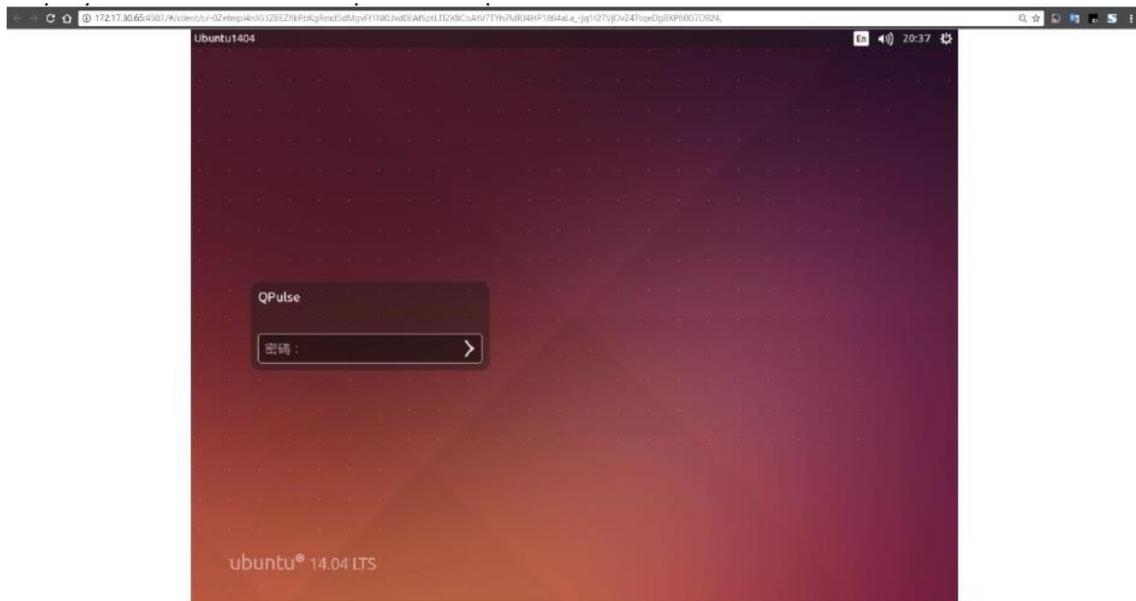


**Step 6:** The browser opens a new page to display the remote desktop. If the connection is successful, the remote desktop will be displayed. If the connection fails, an error message will be displayed and the user can try to reconnect.

Displays the remote desktop screen upon successful RDP connection



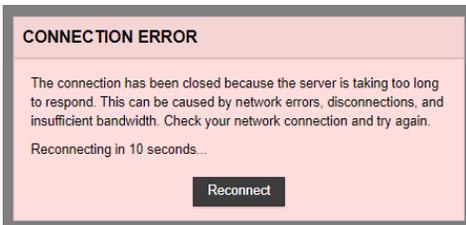
Displays the remote desktop screen upon successful VNC connection



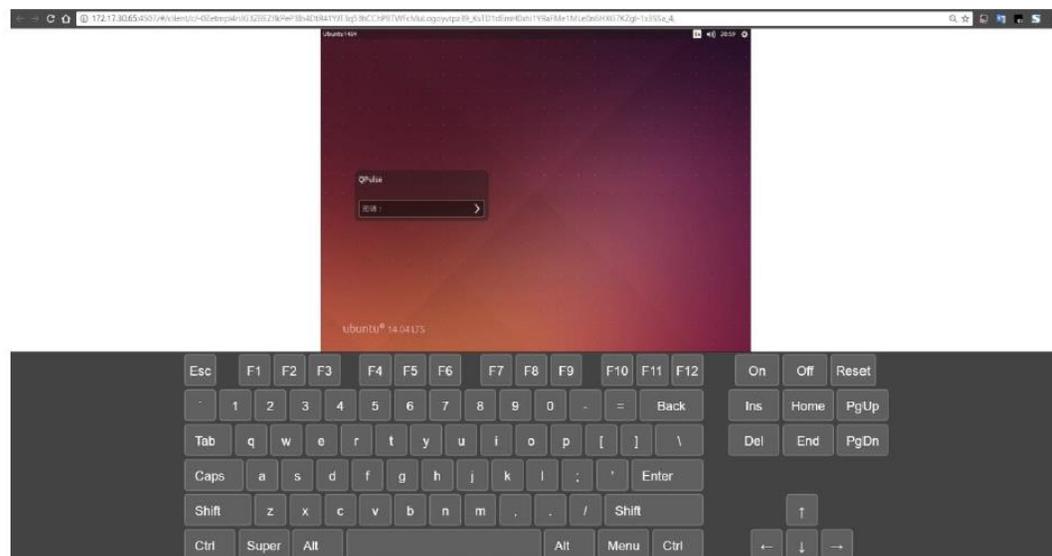
Displays the remote desktop screen upon successful SSH connection



If the connection fails, an error message will be displayed and the user can try to reconnect.



**Step 7:** Press CTRL + SHIFT + ALT in the new browser tab to open the on-screen keypad



## 5.9 Tools - Power Control

There are two control modes for device power control via IRMAgent:

1. Power Off
2. Restart

Setup steps are described below:

**Step 1:** Go to IRMAgent Single Device Dashboard page and click the "Tools" button

**Step 2:** Select "Power Control"

**Step 3:** Select "Power Off" or "Restart"

The screenshot shows the IRMAgent web interface. On the left is a navigation sidebar with options like Dashboard, Device Discovery, Device Management, Alerts Configuration, Logs, and Settings. The main content area is titled 'Device Management / All Devices' and shows a 'Device Summary' for a device with IP 10.10.40.36, which is 'Host is powered on'. Below this is a 'Network Information' table:

IPv4 Address	IPv6 Address	MAC Address
192.168.128.1	fe80::777d:35d8...	00:50:56:C0:00:...
192.168.174.1	fe80::b2b0:6c9a...	00:50:56:C0:00:...
192.168.56.1	fe80::2531:a35c...	0A:00:27:00:00:...
127.0.0.1	::1	.....
10.10.40.36	fe80::f061:5c67...	30:43:D7:E0:E5:...

To the right of the network table is 'Device Information' for an Acer laptop with a 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz processor, 64-bit architecture, 16179 MB physical memory, and 8 CPUs. Further right is 'Operating System Information' showing 'Windows' OS Family and 'Microsoft' OS.

A 'Tools' dropdown menu is open over the device information, listing 'Ping', 'Traceroute', 'Remote Desktop', 'Power Control', and 'RDP Settings'. The 'Power Control' option is highlighted with a red box, and its sub-menu is also open, showing 'Power Off' and 'Restart' options, both of which are also highlighted with red boxes.

Chapter

**6**

# Alert Configuration

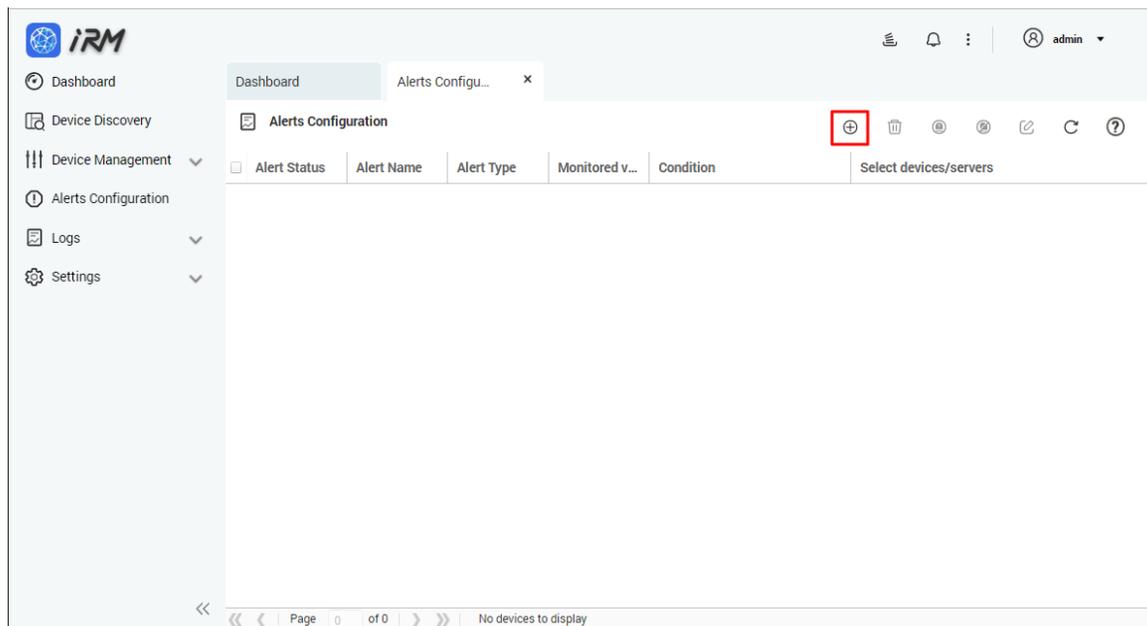
---

In IRM, you can set different alert configurations for different device types. When the set alert condition is met, an alert will appear in the upper right notification window of IRM management page, so that administrators will know the current situation and solve the problem immediately; you can set up SMTP in advanced settings / notification settings, and set up notification policy for alert to be sent via e-mail to administrators to facilitate problem solving. On this page, users can add, delete, edit, deactivate, and enable alert configurations.

## 6.1 Add Alert

Users can click the Add Alert button to add a new alert. Setup steps are described below:

**Step 1:** Enter the Alert Configuration page and click the "Add Alert" button.



**Step 2:** In the Add Alert window, complete the alert type setting:

1. Set Alert Name
2. Set Alert Type (There are four types of IRM alerts: CPU utilization, memory utilization, disk utilization and power status)
3. Click the Select Device button

### Add Alert ✕

Alert Name:  1

Alert Type:  2

Metric:  2

Condition:  3

Selected devices

<input type="checkbox"/>	Hostname	IP Address	Device Tag	Managed by	Brand	Model	Operating S...
No devices are selected.							

⏪ ⏩ | Page  of 0 | ⏪ ⏩ | No devices to display

**Step 3:** Select the device you want to set the alert, you can select one or multiple devices, then click the OK button.

### Selected devices ✕

<input type="checkbox"/>	Hostname	IP Address	Device Tag	Managed by	Brand	Model	Operating Syst...
<input type="checkbox"/>	B11100691-N	10.10.100.225		IRMAgent	Acer	11th Gen Intel(R...	Microsoft Wind...
<input checked="" type="checkbox"/>	B11100695-N	10.10.40.36		IRMAgent	Acer	11th Gen Intel(R...	Microsoft Wind...

⏪ ⏩ | Page  of 1 | ⏪ ⏩ | 1 - 2 of 2  Only list the selected servers or devices.

**Step 4:** Click the Save button to complete the new alert (Note: If the Save button is grayed out, it means that there are errors in alert name, alert type, or selected device).

**Add Alert** ✕

Alert Name:

Alert Type:

Metric:

Condition:

Selected devices ⊕ 🗑️

<input type="checkbox"/>	Hostname	IP Address	Device Tag	Managed by	Brand	Model	Operating S...
<input type="checkbox"/>	B11100695-N	10.10.40.36		IRMAgent	Acer	11th Gen Int...	Microsoft Wi...

⏪ ⏩ | Page  of 1 | ⏪ ⏩ | 1 - 1 of 1

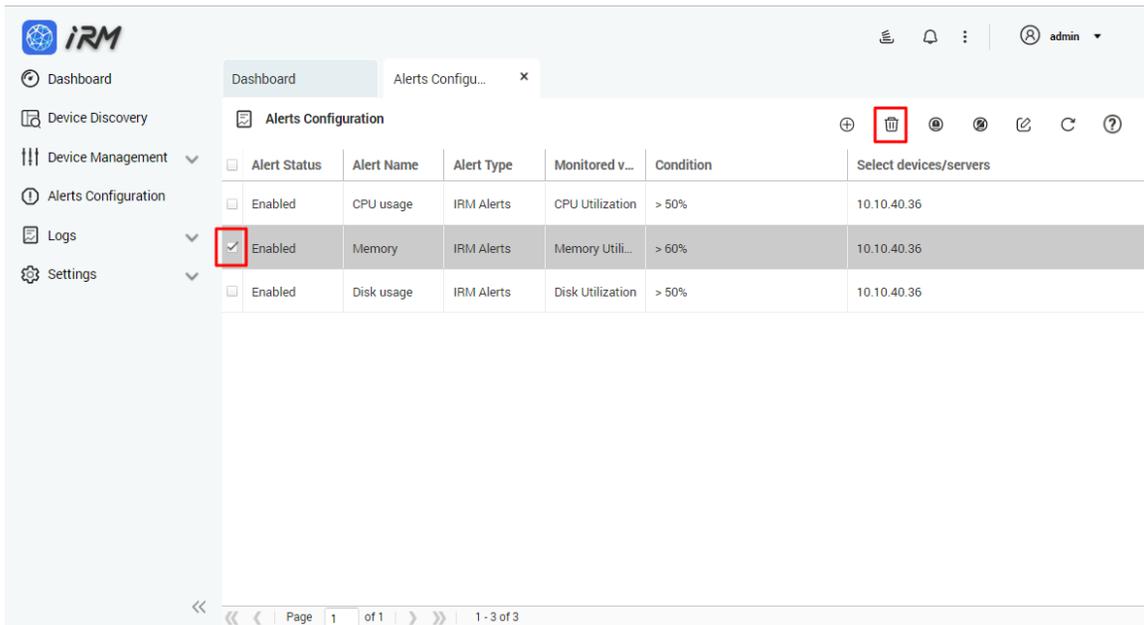
Save Cancel

## 6.2 Delete Alert

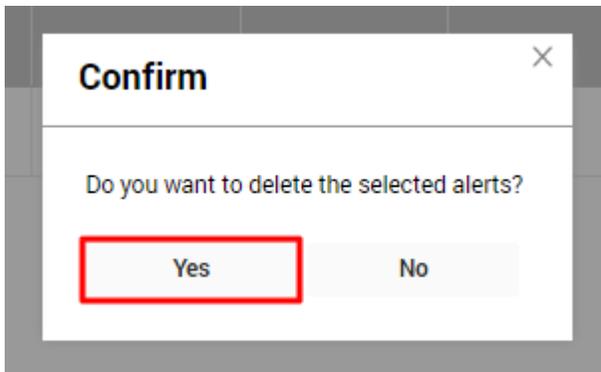
Users can click the "Delete Alert" button to remove one or more alerts at once. Setup steps are described below:

**Step 1:** Enter the Alert Configuration page and select the alert configuration you want to delete.

**Step 2:** Click the "Delete Alert" button.



**Step 3:** Click the "Yes" button to complete the operation.

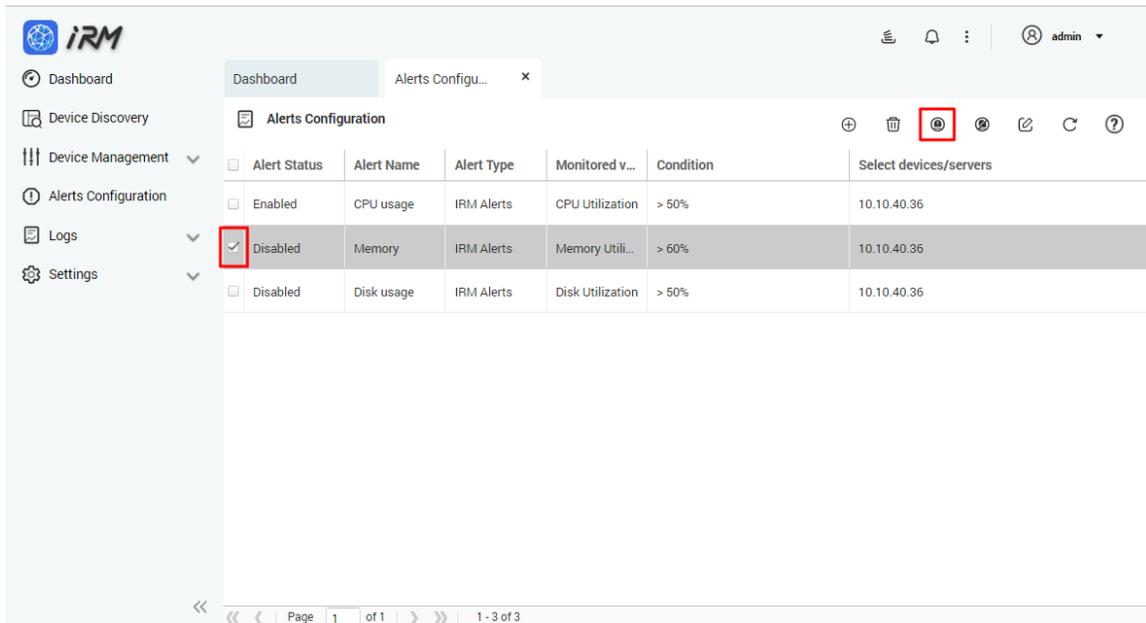


### 6.3 Enable Alert

Users can click the "Enable Alert" button to enable one or more alerts at once. Setup steps are described below:

**Step 1:** Enter the Alert Configuration page and select the alert configuration you want to enable.

**Step 2:** Click the "Enable Alert" button to complete the operation.

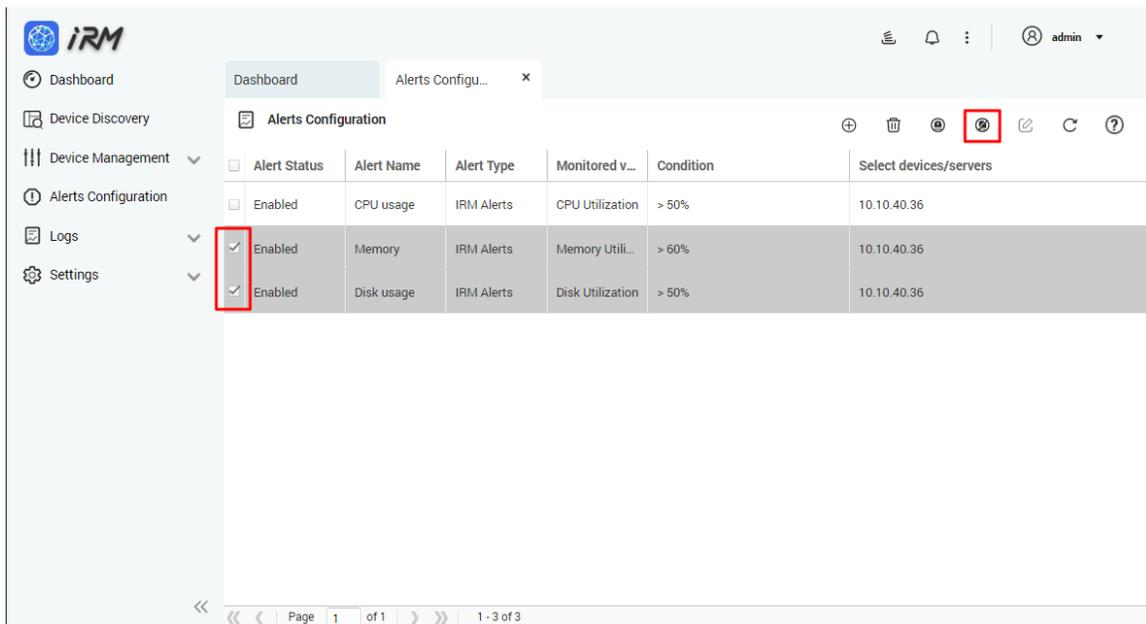


## 6.4 Disable Alert

Users can click the "Disable Alert" button to disable one or more alerts at once. Setup steps are described below:

**Step 1:** Enter the Alert Configuration page and select the alert configuration you want to disable.

**Step 2:** Click the "Disable Alert" button to disable the alert.



## 6.5 Edit Alert

The user can click the Edit Alert button to edit the alert. Only one alert can be edited at a time. Setup steps are described below:

**Step 1:** Enter the Alert Configuration page, select the alert you want to edit, and click the "Edit Alert" button.

Alert Status	Alert Name	Alert Type	Monitored v...	Condition	Select devices/servers
<input type="checkbox"/> Enabled	CPU usage	IRM Alerts	CPU Utilization	> 50%	10.10.40.36
<input checked="" type="checkbox"/> Disabled	Memory	IRM Alerts	Memory Utili...	> 60%	10.10.40.36
<input type="checkbox"/> Disabled	Disk usage	IRM Alerts	Disk Utilization	> 50%	10.10.40.36

**Step 2:** Edit the item you want to modify (please note: the alert type cannot be modified)

**Step 3:** Click the "Save" button to finish editing.

**Edit Alert**

Alert Name:

Alert Type:

Metric:

Condition:

Selected devices

Hostname	IP Address	Device Tag	Managed by	Brand	Model	Operating S...
<input type="checkbox"/> B11100695-N	10.10.40.36		IRMAgent	Acer	11th Gen Int...	Microsoft Wi...

Page 1 of 1 | 1 - 1 of 1

Chapter

7

**Logs**

---

IRM provides three types of logs: IRM alerts log, system log, and historic data log. This page is an advanced application. The user sets the corresponding alert type on the Alert Configuration page. Once an event occurs, you will be able to view the results in the Alert Log on the Logs page (the alert log generation time needs to be set in the Alert Notification setting in the Settings / Notification Settings).

## 7.1 Alerts Log

IRM Alerts Log page displays alerts for all Windows or Linux devices. Users need to select IRM Alerts from the Add Alert page and add one of the four types: CPU usage, memory usage, power status, or disk usage. Once an event occurs, you will be able to view the details of the alert on this page after the event has lasted for 5 minutes.

The basic steps are:

- Step 1:** Select IRM Alerts Log in the Logs page.
- Step 2:** View the alert info, including the Hostname, IP address, Device Tag, On Time and Off Time, etc.
- Step 3:** View the current number of alerts.
- Step 4:** Click the "Refresh" button at any time to get the latest alert message.

Hostname	IP Address	Device Tag	Description	Alert Status	On Time	Off Time
B11100695-N	10.10.40.36		Disk Utilization > 50%	Enabled	2023-05-17 17:...	N/A
B11100695-N	10.10.40.36		Memory Utilization > 60%	Enabled	2023-05-17 17:...	N/A
B11100695-N	10.10.40.36		Memory Utilization > 60%	Disabled	2023-05-17 17:...	2023-05-17 17:...

The Alerts Log has advanced search features:

**Step 1:** Click the "Search Device" button on the Alerts Log page

**Step 2:** Click Select Device and select a device (can only select one).

**Step 3:** Click the "Apply" button to search for all alerts on the target device.

The screenshot shows the IRM Alerts Log interface. On the left is a navigation menu with options like Dashboard, Device Discovery, Device Management, Alerts Configuration, Logs, and Settings. The main area is titled 'Logs / IRM Alerts Log' and includes a search bar with 'Refresh: 21' and a search icon. Below the search bar is an 'Advanced Search' section with fields for 'IP Address' and 'Period', and a 'Select device' button. An 'Apply' button is also present. Below the search section is a table with columns: Hostname, IP Address, Device Tag, Description, Alert Status, On Time, and Off Time. The table contains three rows of alert data.

Hostname	IP Address	Device Tag	Description	Alert Status	On Time	Off Time
B11100695-N	10.10.40.36		Disk Utilization > 50%	Enabled	2023-05-17 17:...	N/A
B11100695-N	10.10.40.36		Memory Utilization > 60%	Enabled	2023-05-17 17:...	N/A
B11100695-N	10.10.40.36		Memory Utilization > 60%	Disabled	2023-05-17 17:...	2023-05-17 17:...

IRM provides Log Retention Settings feature, which can be set for periodic viewing. The default alert log retention period is 1 week. Logs older than one week will be deleted by the system. Users can adjust the length of period according to their needs. See 0

Application Settings.

## 7.2 System Log

System Log shows the messages, alerts, errors, and other events logged by IRM as well as the user's activities.

How to access the System Log: In the Logs page, select "System Log".

The screenshot shows the iRM System Log interface. The left sidebar contains navigation options: Dashboard, Device Discovery, Device Management, Alerts Configuration, Logs (with IRM Alerts Log and System Log highlighted), Historic Data Logs, and Settings. The main content area displays a table of log entries under the heading 'Logs / System Log'. The table has columns for Type, Time, Category, Content, User Name, and Source IP. The entries include Authentication, Device Discovery, and RDP Control events. A search icon is visible in the top right corner of the log view.

Type	Time	Category	Content	User Name	Source IP
Authentication	2023-05-17 17:41...	Authentication	User Login Successful	admin	10.10.101.49
Device Discovery	2023-05-17 14:01...	Device Discovery	Device Discovery completed successfully for 10.10.40.1 to 10...	admin	10.10.100.57
Device Discovery	2023-05-17 13:58...	Device Discovery	Device Discovery started: 10.10.40.1~10.10.40.255	admin	10.10.100.57
RDP Control	2023-05-17 13:46...	RDP Control	Starting to get RDP configuration for 10.10.100.225	admin	10.10.100.57
RDP Control	2023-05-17 13:46...	RDP Control	Get device RDP started for 10.10.100.57	admin	10.10.100.57
Device Discovery	2023-05-17 11:42...	Device Discovery	Device Discovery completed successfully for 10.10.40.0 to 10...	admin	10.10.100.57
Device Discovery	2023-05-17 11:41...	Device Discovery	Device Discovery started: 10.10.40.0~10.10.40.50	admin	10.10.100.57
Device Discovery	2023-05-17 11:41...	Device Discovery	Device Discovery completed successfully for 10.10.40.0 to 10...	admin	10.10.100.57
Device Discovery	2023-05-17 11:40...	Device Discovery	Device Discovery started: 10.10.40.0~10.10.40.20	admin	10.10.100.57

System Log provides advanced search options that allow users to search according to different alert types:

**Step 1:** Select the alert type.

**Step 2:** After selecting the period, press "Apply" to complete the operation.

The screenshot shows the iRM System Log interface with the advanced search options visible. The 'Alert Type' dropdown is set to 'All events' and the 'Period' dropdown is empty. The 'Apply' button is highlighted. The table of log entries is visible below the search options.

Advanced Search:

Alert Type: All events  
 Period: [Empty]

Apply Reset

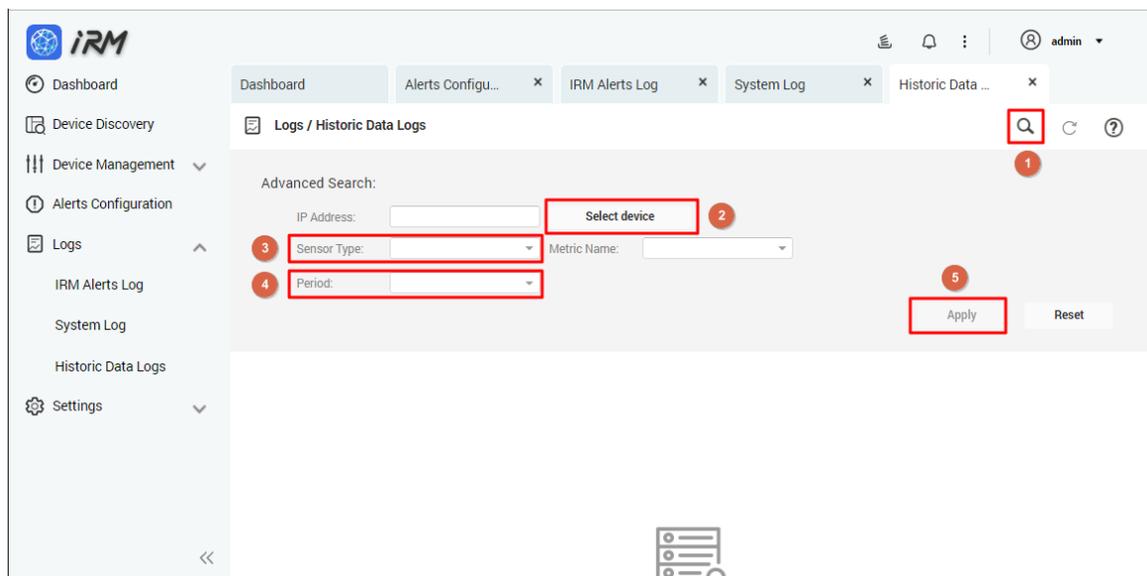
Type	Time	Category	Content	User Name	Source IP
Authentication	2023-05-17 17:41...	Authentication	User Login Successful	admin	10.10.101.49
Device Discovery	2023-05-17 14:01...	Device Discovery	Device Discovery completed successfully for 10.10.40.1 to 10...	admin	10.10.100.57
Device Discovery	2023-05-17 13:58...	Device Discovery	Device Discovery started: 10.10.40.1~10.10.40.255	admin	10.10.100.57
RDP Control	2023-05-17 13:46...	RDP Control	Starting to get RDP configuration for 10.10.100.225	admin	10.10.100.57
RDP Control	2023-05-17 13:46...	RDP Control	Get device RDP started for 10.10.100.57	admin	10.10.100.57

## 7.3 Historic Data Log

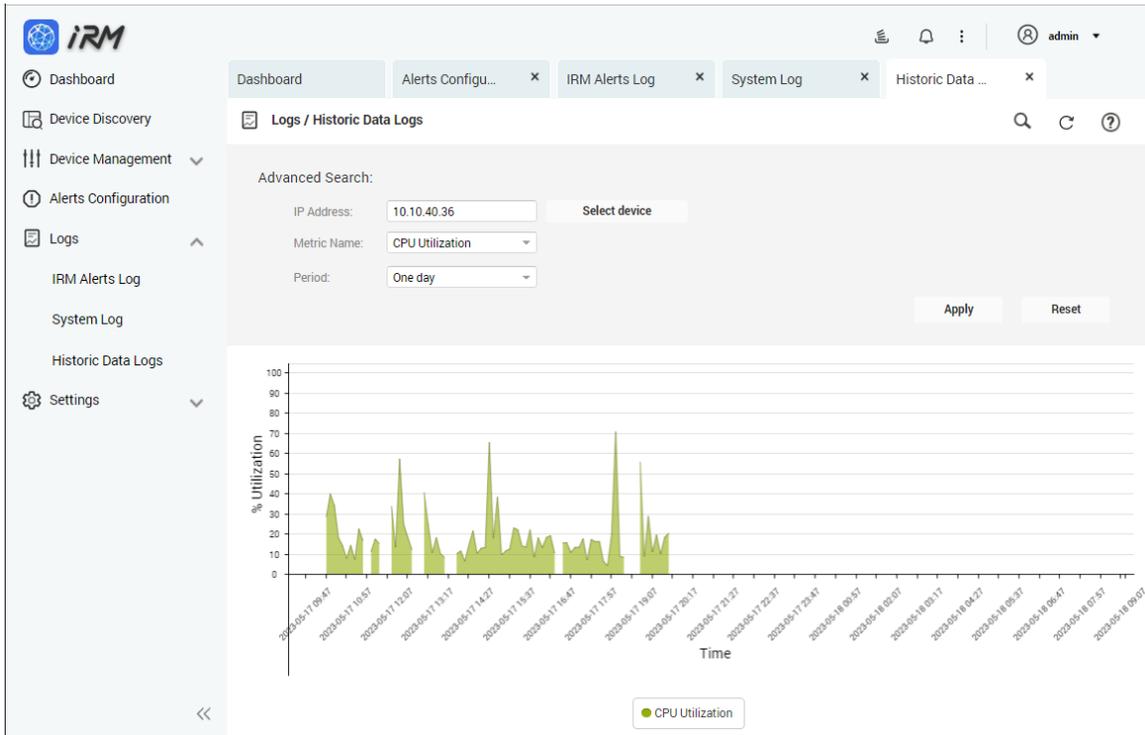
IRM provides historical data obtained by a specific sensor type of a specific device over a specific time frame. For example, a user can select a device, set the period as one day or one week, select the sensor type as CPU usage, then IRM will present the CPU Utilization as a line chart. This feature is useful for analyzing the values of different sensor types over a specific time frame in order to take actions for improvement.

To display the historical data as a line chart in IRM, follow the steps below:

- Step 1:** Click the “Search Device” button.
- Step 2:** Select the target device (required).
- Step 3:** Select Metric Name (required).
- Step 4:** Select the Period (required).
- Step 5:** Click “Apply” button to complete the operation.



The line chart for a specific device is shown below.



IRM provides Log Retention Settings feature, which can be set for periodic viewing. The default Historic Data Log retention period is 1 week. Logs older than one week will be deleted by the system. Users can adjust the length of period according to their needs. See 0

Application Settings.

Chapter

8

# Settings

---

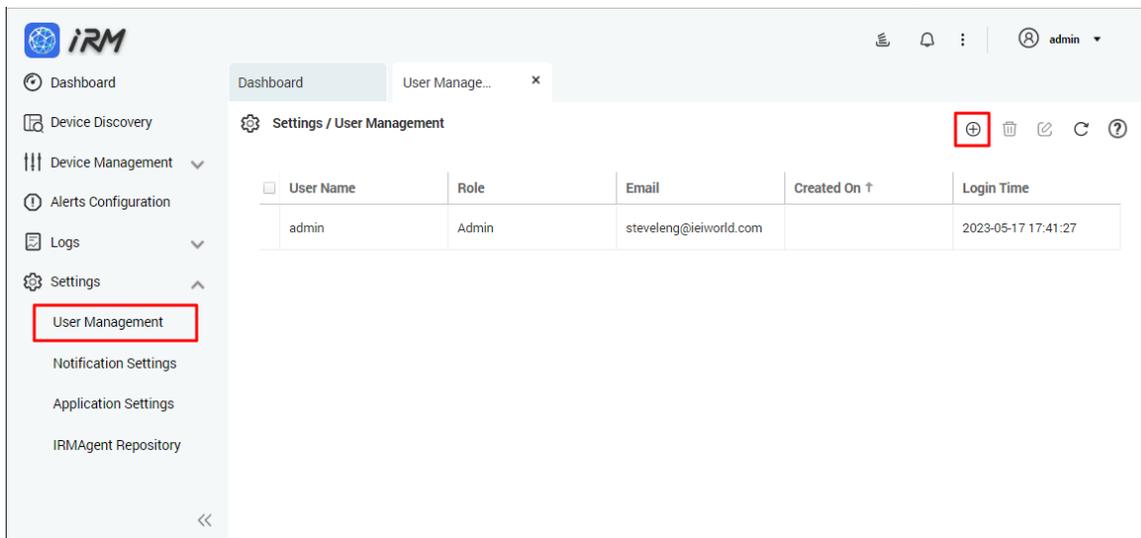
The Settings page contains the system user account and permissions management; **only the user with administrator permissions can enter this page.**

## 8.1 User Management

User Management provides the functions for setting up user permissions, adding or deleting users. IRM account must be bundled with a QTS account. Only QTS accounts can be added as IRM accounts. If a QTS account is deleted, the associated IRM will become unavailable.

### 8.1.1 Add User

**Step 1:** Select "User Management" from the Settings page and click the "Add User" button.

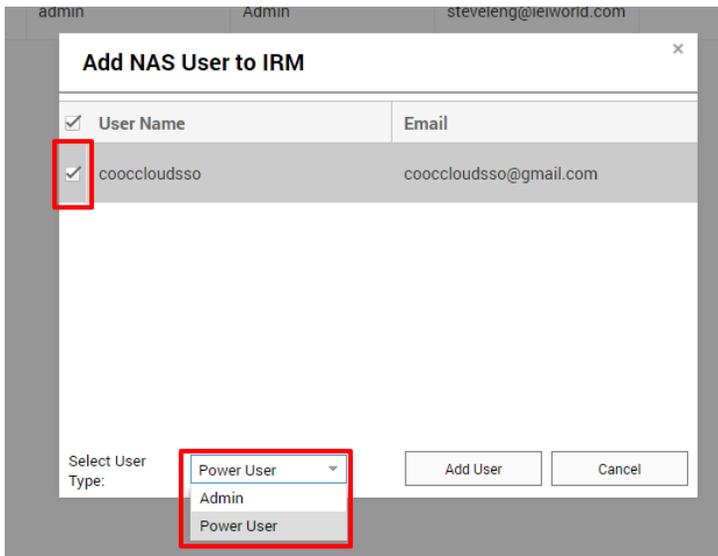


The screenshot shows the IRM web interface. On the left, a sidebar menu lists various settings, with 'User Management' highlighted in a red box. The main content area is titled 'Settings / User Management' and contains a table with the following data:

User Name	Role	Email	Created On ↑	Login Time
admin	Admin	steveleng@ieiworld.com		2023-05-17 17:41:27

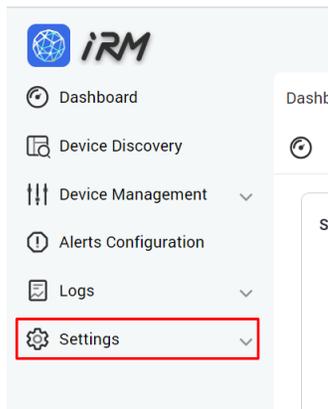
In the top right corner of the table area, there is a red box around a plus sign icon (+), which is the 'Add User' button.

**Step 2:** After select the user and the permissions that you want to add, click "Add User" to finish.

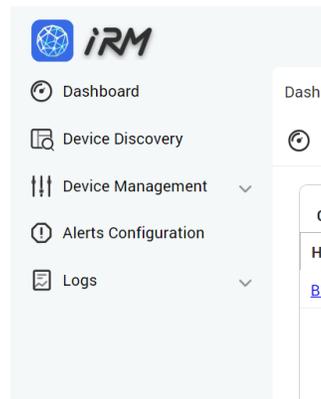


**NOTE:** The difference in permissions between Admin and Power User is that only Admin can access Settings. Power User has no authority to modify or change system settings.

**Administrator's UI**

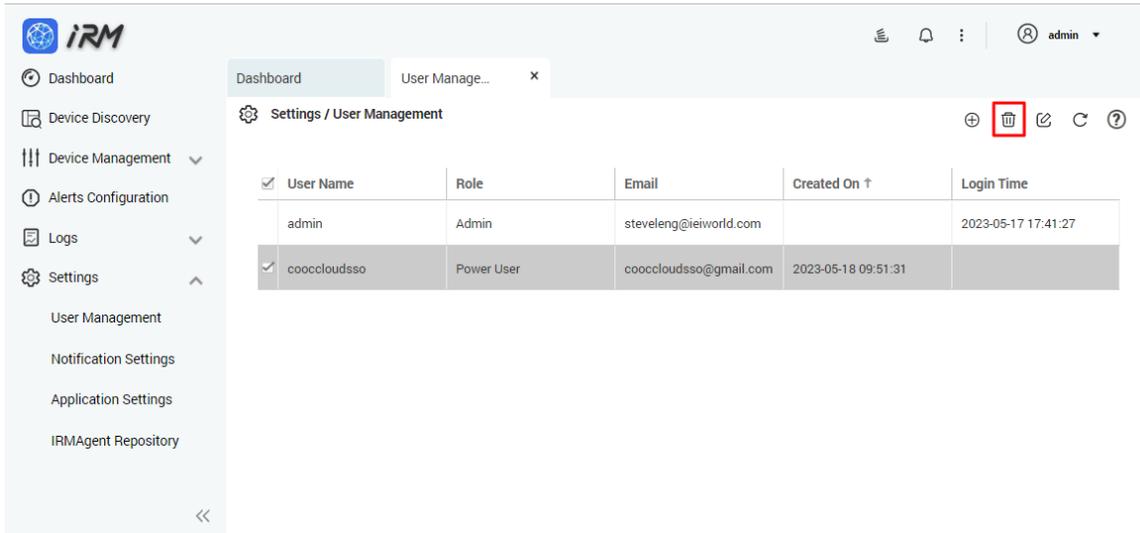


**Power User's UI**



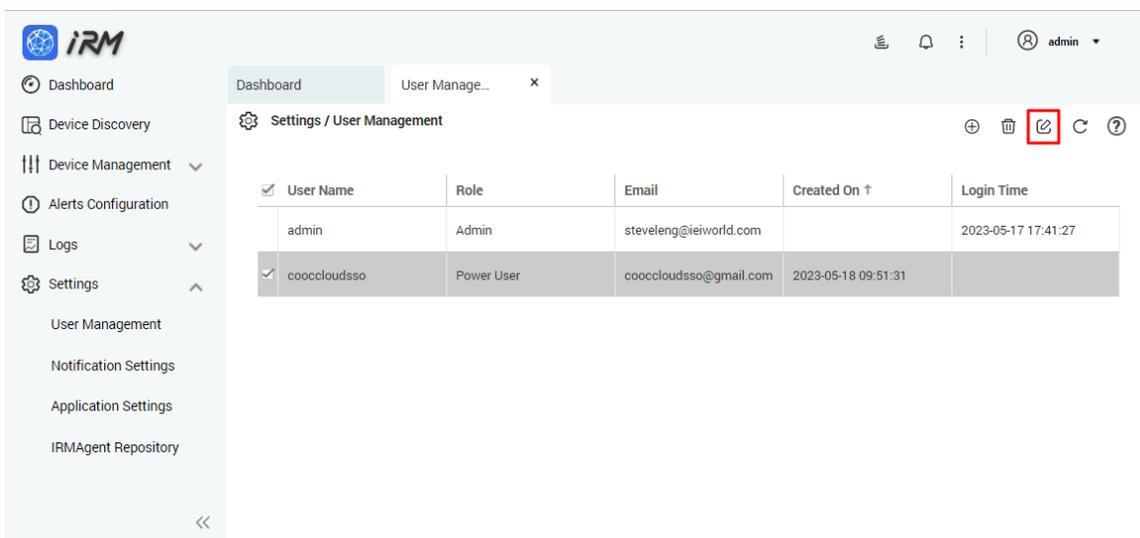
### 8.1.2 Deleting Users

Select "User Management" in the Settings page, select the user you want to delete and click the "Delete User" button.

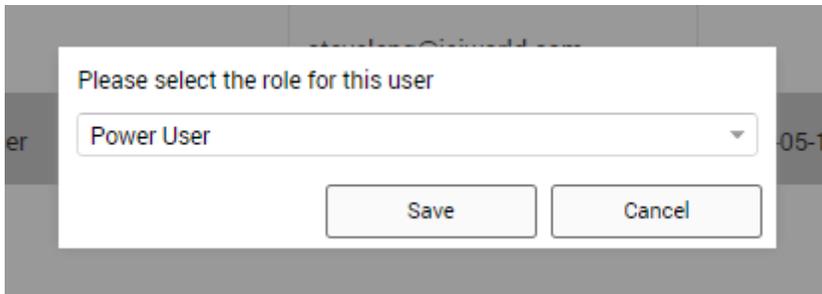


### 8.1.3 Editing Permissions

**Step 1:** Select "User Management" from the Settings page, select the user you want to edit and click the "Edit User" button.

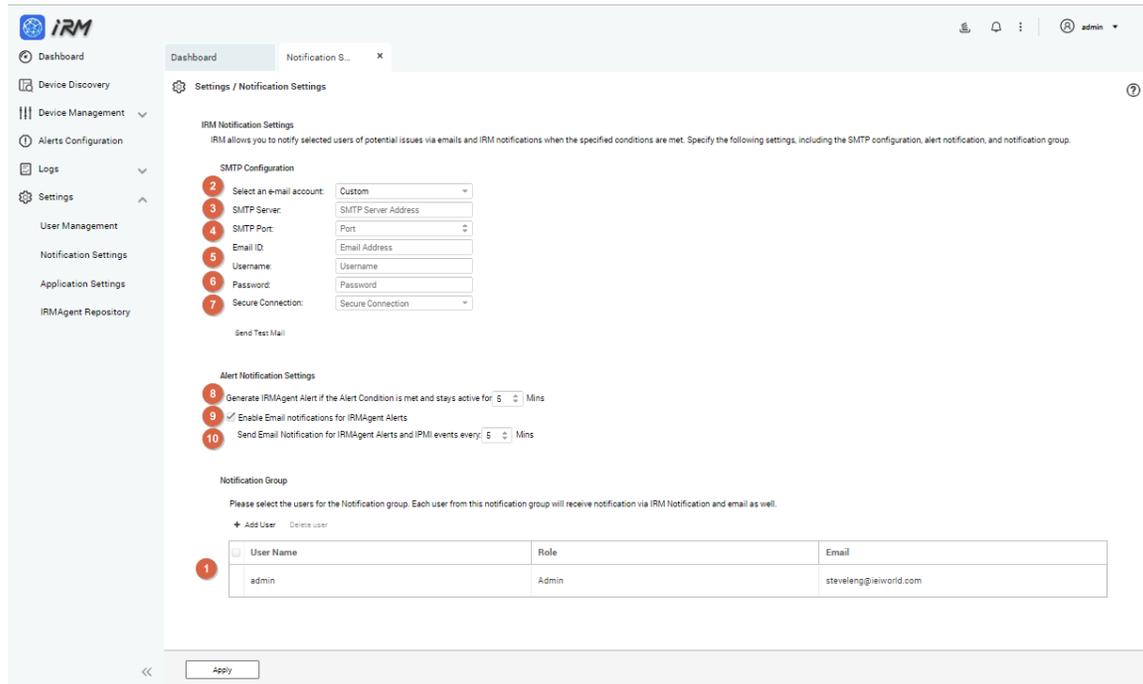


**Step 2:** Select the permission level you want to change from the drop-down menu and click the "Save" button to complete the operation.

A screenshot of a software dialog box. The dialog box has a white background and a grey border. At the top, it says "Please select the role for this user". Below this is a drop-down menu with "Power User" selected. At the bottom of the dialog box, there are two buttons: "Save" and "Cancel". The dialog box is overlaid on a grey background that shows some blurred text from the underlying application, including "er" on the left and "05-1" on the right.

## 8.2 Notification Settings

The notification settings allow users to be notified immediately when an event occurs, thus improving emergency response capabilities. Detailed setup instructions are as follows:



1. The list of accounts that need to be notified
2. SMTP type
3. SMTP server location
4. SMTP server port
5. E-mail account
6. E-mail password
7. Secure connection mode
8. How long after an alert condition has lasted before sending an alert
9. Whether to enable e-mail sent Agent alert
10. Time interval for sending repeat alerts

## 8.3 Application Settings

Application Settings let users adjust the system log files and video retention settings according to their needs, users can also adjust real-time data and automatic device scan period based on performance.

The screenshot displays the iRM Application Settings interface. The sidebar on the left lists various system components, with 'Settings' currently selected. The main panel shows configuration options for logs and device scans. The 'Log Retention Settings' section includes three dropdown menus, each set to '1 Week'. The 'Data collection on devices' section includes two dropdown menus: 'Interval between periodic scans on remote devices (minutes)' set to '1' and 'Interval between real-time scans on remote devices (seconds)' set to '10'. An 'Apply' button is positioned at the bottom of the settings area.

1. Alert log retention period
2. System logs retention period
3. Historical data log retention period
4. Device scan and automatic refresh period
5. Real-time data automatic refresh period

## 8.4 IRMAgent Information

Select "IRMAgent Repository" in the Settings page to list the currently supported operating system platforms and their Agent versions.

The screenshot shows the IRM web interface. On the left is a navigation sidebar with options: Dashboard, Device Discovery, Device Management, Alerts Configuration, Logs, Settings, User Management, Notification Settings, Application Settings, and IRMAgent Repository. The main content area is titled "Settings / IRMAgent Repository" and contains a table with the following data:

IRMAgent Pkg. Name	IRMAgent Ver...	Target OS	Download...
IRMAgent-Windows-x86_64-Setup (64-bit)	v0.1.7	Windows 7, Windows 8/8.1, Windows 10, Windows 11, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022	↓
IRMAgent-Ubuntu-x86_64-Setup (64-bit)	v0.1.7	Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04	↓
IRMAgent-Debian-x86_64-Setup (64-bit)	v0.1.7	Debian 8, Debian 9, Debian 10, Debian 11	↓
IRMAgent-CentOS-x86_64-Setup (64-bit)	v0.1.7	CentOS 7	↓