



IRM (IEI Remote Management) Tutorials

Revision

Date	Version	Changes
March 5, 2026	1.02	Add: All new features of IRM 1.4.* 3. Add Device 3.2 IPMI Device (iRIS2) 7 Redundancy 8 Recovery 10.3 iVEC Management Delete: Device Discovery
February 16, 2024	1.01	Updated: 1.4 Requirements for Using IRM 1.5 Updating IRMAgentPack and IRM Added: 8.1.1 Default User 8.1.2 Create New User 9 Licenses
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

Content

REVISION	II
COPYRIGHT	III
TABLE OF CONTENTS	IV
1 OVERVIEW	8
1.1 HOW TO USE IRM TO MANAGE YOUR DEVICES.....	9
1.2 BROWSER SUPPORT	9
1.3 OS SUPPORT	9
1.4 REQUIREMENTS FOR USING IRM.....	10
1.5 UPDATING IRMAGENTPACK AND IRM.....	10
1.6 GLOBAL TOOLBAR.....	13
1.6.1 <i>User Account Menu</i>	13
1.6.2 <i>More Options Menu</i>	14
1.6.3 <i>Notification Center</i>	15
1.6.4 <i>Background Task Status</i>	19
2 MAIN DASHBOARD	21
2.1 ADD WIDGET	22
2.2 DELETE ALL WIDGETS IN THE DASHBOARD	25
2.3 REFRESH ALL WIDGETS IN THE DASHBOARD	26
2.4 SELECT THE LAYOUT MODE.....	27
2.5 EXPORT AS PDF FILE	28
2.6 EMAIL CURRENT VIEW	30
2.7 REAL-TIME AND HISTORICAL DATA PRESENTATION.....	32
3 ADD DEVICE	33
3.1 ADD WINDOWS DEVICES	35
3.1.1 <i>Windows Devices</i>	36
3.1.2 <i>Linux Devices</i>	42

3.2	IEI OUT-OF-BAND MANAGEMENT DEVICE	48
3.3	IVEC DEVICES	51
4	DEVICE MANAGEMENT	59
4.1	ALL DEVICES	60
4.1.1	<i>Host Name</i>	60
4.1.2	<i>Tag</i>	60
4.1.3	<i>Status</i>	60
4.1.4	<i>Add Device</i>	61
4.1.5	<i>Remove Device</i>	62
4.1.6	<i>Refresh</i>	62
4.1.7	<i>Help</i>	62
4.1.8	<i>Search</i>	63
4.1.9	<i>Action</i>	63
4.1.10	<i>Quick Menu</i>	64
4.1.11	<i>IEI System Monitoring Module</i>	67
4.2	NETWORK TOPOLOGY	73
4.2.1	<i>Start Scan</i>	74
4.2.2	<i>Stop Scanning</i>	78
4.2.3	<i>Resetting</i>	78
4.2.4	<i>Scan History</i>	79
4.4	IPMI KVM.....	79
4.4.1	<i>KVM Manager</i>	79
4.4.2	<i>KVM Dashboard</i>	82
4.4.3	<i>IPMI Add Widget</i>	88
5	SINGLE DEVICE MANAGEMENT	92
5.1	SINGLE DEVICE DASHBOARD.....	93
5.2	ADD WIDGET	93
5.3	DELETE ALL WIDGETS IN THE SINGLE DEVICE DASHBOARD	95
5.4	REFRESH ALL WIDGETS INFORMATION IN THE DASHBOARD.....	96
5.5	SELECT THE LAYOUT MODE.....	96
5.6	TOOLS - PING	97
5.7	TOOLS – TRACEROUTE	98
5.8	TOOLS - HARDWARE SETTING (WATCHDOG TIMER).....	99

5.9	TOOLS - REMOTE DESKTOP	100
5.10	TOOLS - POWER CONTROL	104
5.11	TOOLS - REMOTE RDP CONFIGURATIONS.....	105
6	ALERT CONFIGURATION.....	106
6.1	ADD AGENT ALERT.....	107
6.2	ADD HARDWARE SENSORS ALERT	110
6.3	ADD IPMI(iRIS2) ALERT	113
6.4	DELETE ALERT.....	117
6.5	ENABLE ALERT	117
6.6	DISABLE ALERT.....	118
6.7	EDIT ALERT	119
7	REDUNDANCY	121
7.1	DEVICE PAIR	122
7.2	POLICY.....	127
7.3	PLAN.....	129
7.4	REDUNDANCY LOG.....	134
8	RECOVERY.....	136
8.1	REMOTE RECOVERY.....	137
8.2	RECOVERY LOG	143
9	LOGS.....	144
9.1	SYSTEM LOG	145
9.2	HARDWARE & DEVICE.....	146
9.2.1	<i>Agent Alerts Log</i>	146
9.2.2	<i>IPMI Alert Log</i>	148
9.2.3	<i>IPMI Event List</i>	149
9.2.4	<i>Historic Data Log</i>	150
10	SETTINGS	152
10.1	NOTIFICATION SETTINGS.....	153
10.1	APPLICATION SETTINGS	160
10.1.1	<i>Log Retention Period</i>	161
10.1.2	<i>Data Collection Period</i>	161

10.1.3	<i>Agent Setting</i>	162
10.1.4	<i>Recovery Setting</i>	162
10.2	USER MANAGEMENT	163
10.2.1	<i>Default User</i>	163
10.2.2	<i>Create New User</i>	164
10.2.3	<i>Add User</i>	167
10.2.4	<i>Deleting Users</i>	169
10.2.5	<i>Editing Permissions</i>	169
10.3	IVEC MANAGEMENT	170
11	REPOSITORY	173
11.1	IRAGENT DOWNLOAD	174
12	LICENSES	175
12.1	LICENSE PORTALS AND UTILITY	176
12.2	IRM PERPETUAL LICENSE	176
12.3	LICENSE ACTIVATION	177
12.3.1	<i>Activation Methods</i>	178
12.3.2	<i>Setting up myQNAPcloud for Your IRM Mini Server</i>	179
12.3.3	<i>Activating a License Using a Product Key</i>	182
12.3.4	<i>Activating a License Using a License Key</i>	186
12.3.5	<i>Activating a License Using QNAP ID</i>	189
12.3.6	<i>License Activation Email</i>	193
12.3.7	<i>How to Check Your Activated IRM License</i>	194
12.3.8	<i>Activation Failed</i>	195
12.4	CHECKING AND BUY LICENSE	195
12.5	DEACTIVATING A LICENSE FOR LICENSE MIGRATION	196
12.5.1	<i>Migrating an Activated License</i>	196
12.5.2	<i>License Deactivation</i>	196

Chapter

1

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.

IRM is a web-based solution that provides basic device management capabilities such as device management, 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
 - Windows Server 2022
 - Ubuntu 16.x
 - Ubuntu 18.x
 - Ubuntu 20.x
 - Ubuntu 22.x
 - Ubuntu 24.x
 - CentOS 7
 - Debian 8
 - Debian 9
 - Debian 10
 - Debian 11
 - Debian 12

1.4 Requirements for Using IRM

Hardware:

- TS-i410X-8G2H

Software (App)

- Container Station
- IRMAgentPack
- IRM

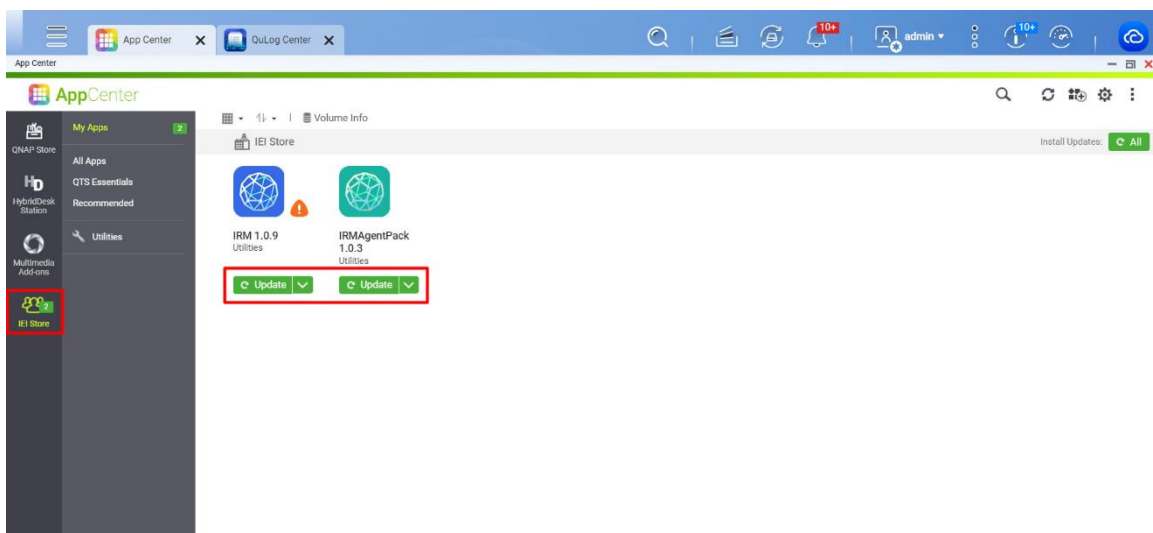
*Container Station, IRMAgentPack and IRM are pre-installed in TS-i410X-8G2H. To locate these apps in the App Center, find Container Station in the QNAP Store, and IRMAgentPack and IRM in the IEI Store. If these apps are not installed, please contact IEI for further instructions.

1.5 Updating IRMAgentPack and IRM

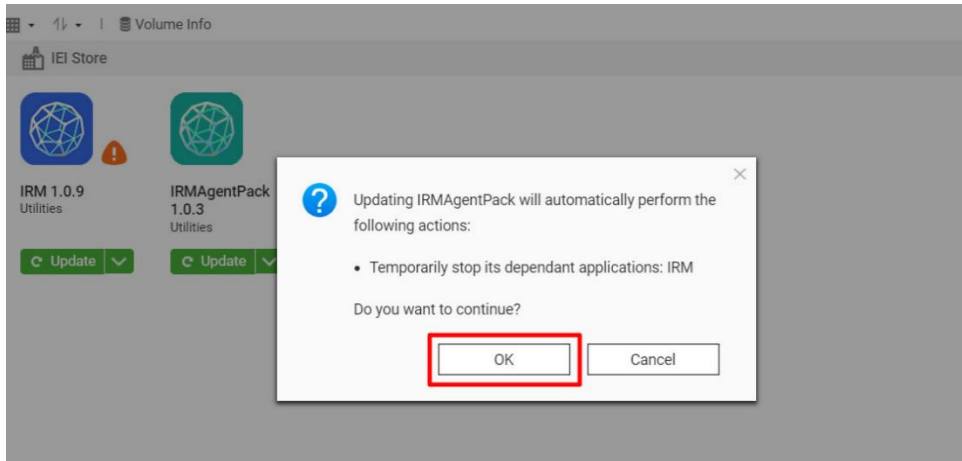
Before using IRM, connect the device to the internet and check if your IRM and IRMAgentPack apps are up-to-date. You must perform required updates to ensure the functionality, compatibility, and data security of your apps.

Step 1: Open **App Center** and click **IEI Store**. Locate the IRMAgentPack and IRM apps. Click the **Update** button.

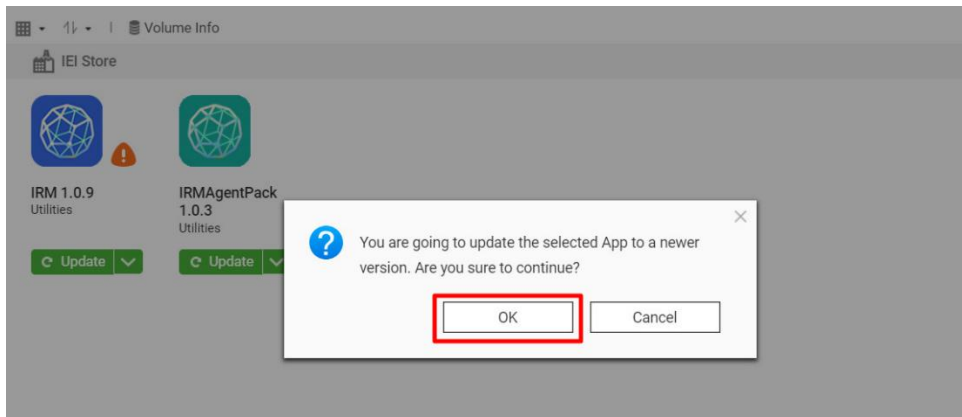
Note: Update the IRMAgentPack before IRM if both require an update.



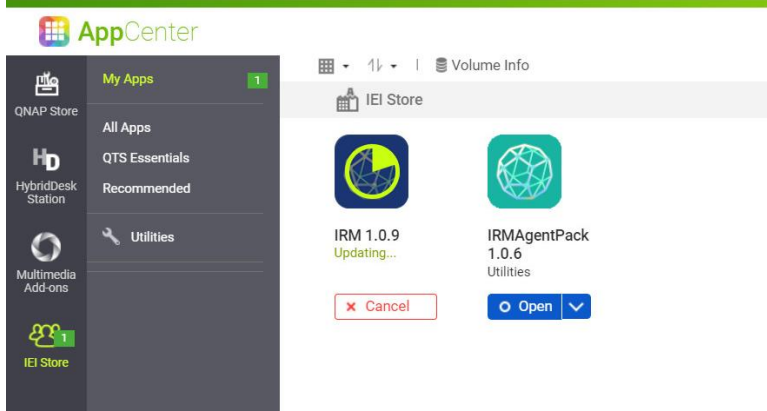
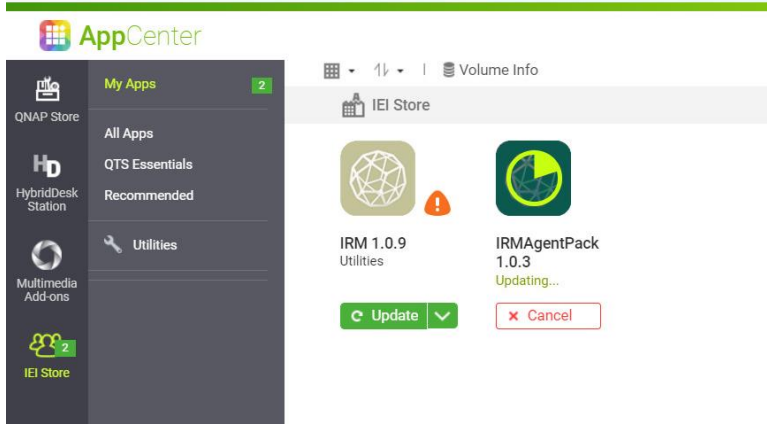
Step 2: The following warning message appears before updating the IRMAgentPack. Click **OK** to continue.



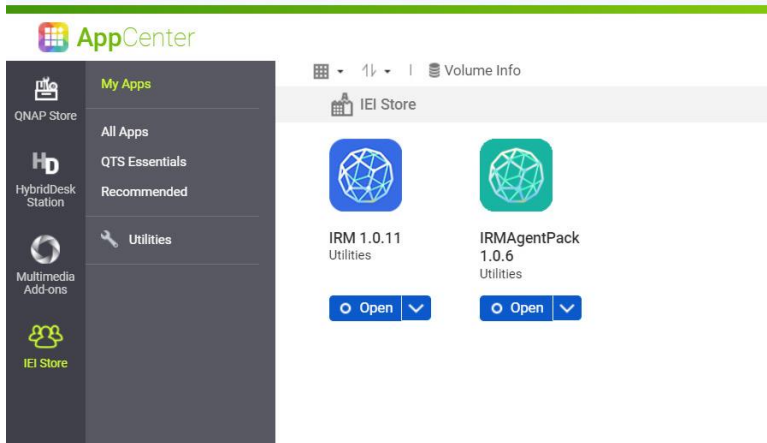
Step 3: The following confirmation message appears. Click **OK** to start update.



Step 4: The system starts updating the app.



Step 5: Update is finished.



1.6 Global Toolbar

The upper-right corner of the IRM interface provides four global function icons that are available on every page, allowing users to easily view system status and account information.

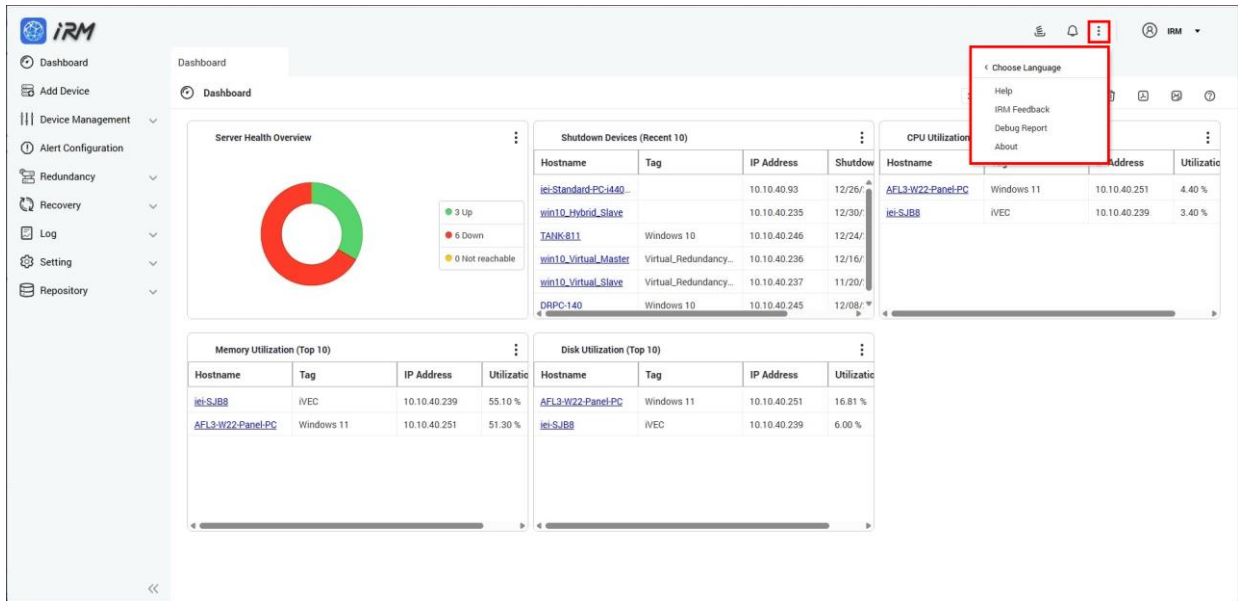
1.6.1 User Account Menu


The screenshot shows the IRM dashboard interface. In the top right corner, the user account 'IRM' is displayed with a drop-down arrow. The account menu is open, showing the 'Login Time' as '2025-12-31 10:11:47' and a 'Logout' button. The dashboard content includes a 'Server Health Overview' with a donut chart showing 3 Up, 6 Down, and 0 Not reachable. There are also tables for 'Shutdown Devices (Recent 10)', 'CPU Utilization (Top 10)', 'Memory Utilization (Top 10)', and 'Disk Utilization (Top 10)'.

In the upper-right corner of the page, the currently signed-in account name (e.g., IRM) and a drop-down arrow (▼) are displayed.

- Click the drop-down arrow (▼) to the right of the account name to open the user account menu.
- The menu includes the following items:
 - **Login Time**
Displays the date and time of the current IRM login session (e.g., 2025-12-23 09:22:53), allowing administrators to check when the session started.
 - **Logout**
Click **Logout** to end the current session and sign out of IRM. The system will return to the login page. It is recommended to log out after completing operations to enhance account and system security.

1.6.2 More Options Menu



When you click the  icon in the upper-right corner of the iRM interface, an extended options menu is displayed, as shown in the figure below.

The menu provides the following items:

- **Choose Language**

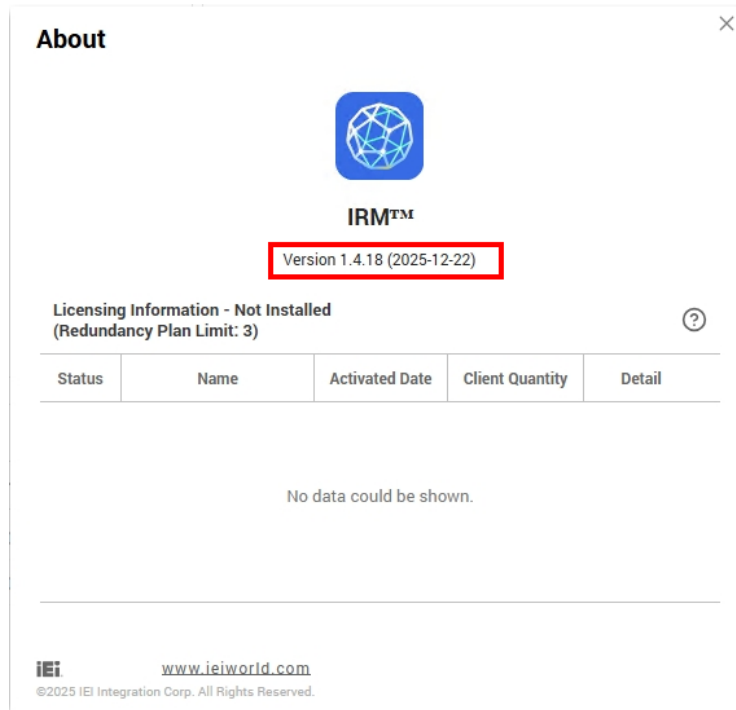
Opens the language selection window, where users can switch the display language of the iRM web interface. ◦
- **Help**

Opens iRM online help or the user guide, providing instructions and descriptions for each feature.
- **iRM Feedback**

Opens the feedback window, where users can submit issues, suggestions, or requests encountered while using iRM to IEI technical support or the development team.
- **Debug Report**

Generates and downloads iRM debugging/diagnostic information (such as system status and log files) to provide more complete details for troubleshooting or technical support.
- **About**

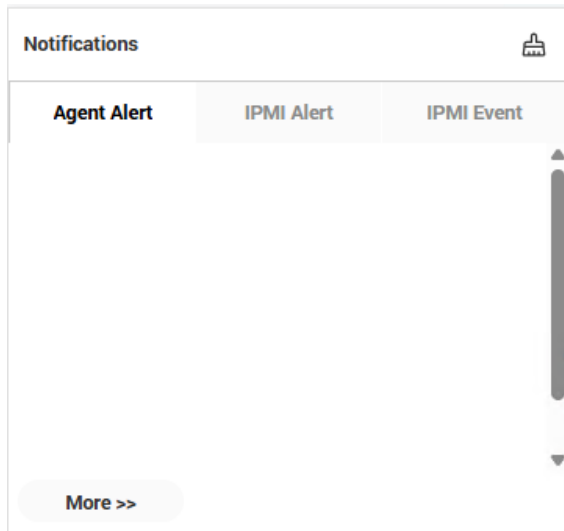
Displays iRM product information, including the version number, copyright information, and related details, useful for issue reporting and version management.



Note: The available options may vary slightly depending on the iRM version or the user's access permissions.

1.6.3 Notification Center

The Notification Center is located at the upper-right corner of the iRM management page, represented by the **notification bell (🔔) icon**. It is used to centrally display system events and various alert notifications. When a device triggers an alert condition or the system generates a related event, administrators can use the Notification Center to quickly understand the current status and take follow-up actions.

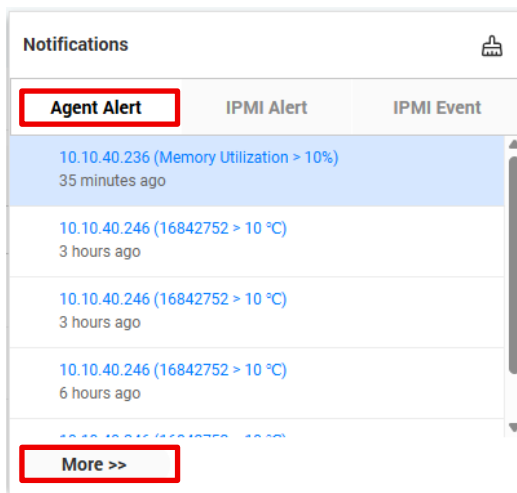


The Notification Center is divided into three tabs by source type:

- **Agent Alert**

Displays alert messages reported by the IRM Agent, for example:

- Abnormal operating system power on/off status
- Disk, memory, or CPU usage too high
- Agent not responding and other events



The “**More >>**” button at the bottom of the window opens the full notification/event list page, allowing users to further review, filter, and analyze historical records.

Agent Alert Log

Log / Agent Alert Log

Hostname	Tag	Description	Alert Status	IP Address	Trigger Time	Clear
win10_Virtual_Mas...	Virtual_Redundanc...	Memory Utilization > 10%	On	10.10.40.236	2026-01-05 16:36:16	N
TANK-811	Windows 10	over temperature 10 °C [name:1...	Off	10.10.40.246	2026-01-05 14:02:12	20
TANK-811	Windows 10	over temperature 10 °C [name:1...	Off	10.10.40.246	2026-01-05 13:42:12	20
TANK-811	Windows 10	over temperature 10 °C [name:1...	Off	10.10.40.246	2026-01-05 11:37:12	20
TANK-811	Windows 10	over temperature 10 °C [name:1...	Off	10.10.40.246	2026-01-05 11:27:12	20
AFL3-W22-Panel-PC	Windows 11	CPU Utilization > 10%	Off	10.10.40.251	2026-01-03 15:07:00	20
AFL3-W22-Panel-PC	Windows 11	CPU Utilization > 10%	Off	10.10.40.251	2026-01-03 11:07:00	20

Page 1 of 2 | 1 - 50 of 64

- IPMI Alert**

Displays hardware alerts reported by IPMI devices, such as power abnormalities, excessive temperature, or fan failures (data is shown only when IPMI devices are being monitored).

Notifications

Agent Alert | **IPMI Alert** | IPMI Event

SYS Temp1
10.10.40.250 (SYS TEMP1 > 10 °C)
5 days ago

More >>

The **More >>** button at the bottom of the window opens the full **Notifications/Events** list page, allowing users to further **view**, **filter**, and **analyze** historical records.

IPMI Alert Log

Log / IPMI Alert Log

Hostname	Tag	Description	IP Address	Sensor T...	Metric N...	Trigger T...	Clear Time
10.10.40.250	iRIS Device	CPU TEMP0 over 10.0°C	10.10.40.250	Temperat...	CPU TEM...	2025-12-...	2025-12-...
10.10.40.250	iRIS Device	SYS TEMP1 over 10.0°C	10.10.40.250	Temperat...	SYS TEM...	2025-12-...	2025-12-...
10.10.40.250	iRIS Device	SYS TEMP1 over 10.0°C	10.10.40.250	Temperat...	SYS TEM...	2025-12-...	N/A

Page 1 of 1 | 1 - 3 of 3

- **IPMI Event**

Displays general event logs reported by the IPMI device, such as power on/off, reboot operations, or sensor reading changes.

The More >> button at the bottom of the window opens the full Notifications/Events list page, allowing users to further view, filter, and analyze historical records.

IPMI Event List

Log / IPMI Event List

Advanced Search:

IP Address:

Sensor Type: Metric Name:

Period:

No log data found

1.6.4 Background Task Status

In the upper-right corner of the IRM interface, click to open the Background Tasks window. This window shows whether any background tasks are currently running in IRM.

Hostname ↑	Tag	IP Address	Operating System	Category	Brand	Status
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	Microsoft Windows	Agent	IEi	Monitored
DRPC-140	Windows 10	10.10.40.245	Microsoft Windows	Agent	IEi	Monitored
TANK-811	Windows 10	10.10.40.246	Microsoft Windows	Agent	IEi	Monitored
win10_Hybrid_Slave		10.10.40.235	Microsoft Windows	Agent	QEMU	Monitored
win10_Virtual_Master	Virtual_Redundancy_Ma...	10.10.40.236	Microsoft Windows	Agent	QEMU	Monitored
win10_Virtual_Slave	Virtual_Redundancy_Slave	10.10.40.237	Microsoft Windows	Agent	QEMU	Monitored

Status indicators:

- If a red number badge appears in the upper-right corner of the icon, it indicates that one or more background tasks are currently running.
- If no number badge is displayed, it indicates that there are no background tasks running.

Viewing Background Tasks

- Click the Background Tasks icon to open the Background Tasks window in the upper-right corner of the page.
- The window lists all running or recently triggered background tasks, for example:
 - *Recovering – TANK-811 (10.10.40.246)* :
Indicates that IRM is performing a remote recovery operation on host TANK-811 (IP: 10.10.40.246).
- Users can click a task item (for example, the host name link) to open the corresponding function page—such as Remote Recovery—to view real-time task details, including progress and partition recovery status.

Remote Recovery

Processing Recovery Task

Selected Device: TANR-811

Hostname: TANR-811 Recovery Image: Use image 1
 Tag: Windows 10 Scheduled on 2025-12-23 15:31:28

3% of 146.48 GB

Disk Label	/dev/sda	/dev/sdb	/dev/sdc	/dev/sdd
100%	100%	3%	0%	
sda1	sdb2	sdc3	sdd4	
100.00 MB	16.00 MB	145.86 GB	522.00 MB	

Close

Chapter

2

2 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.

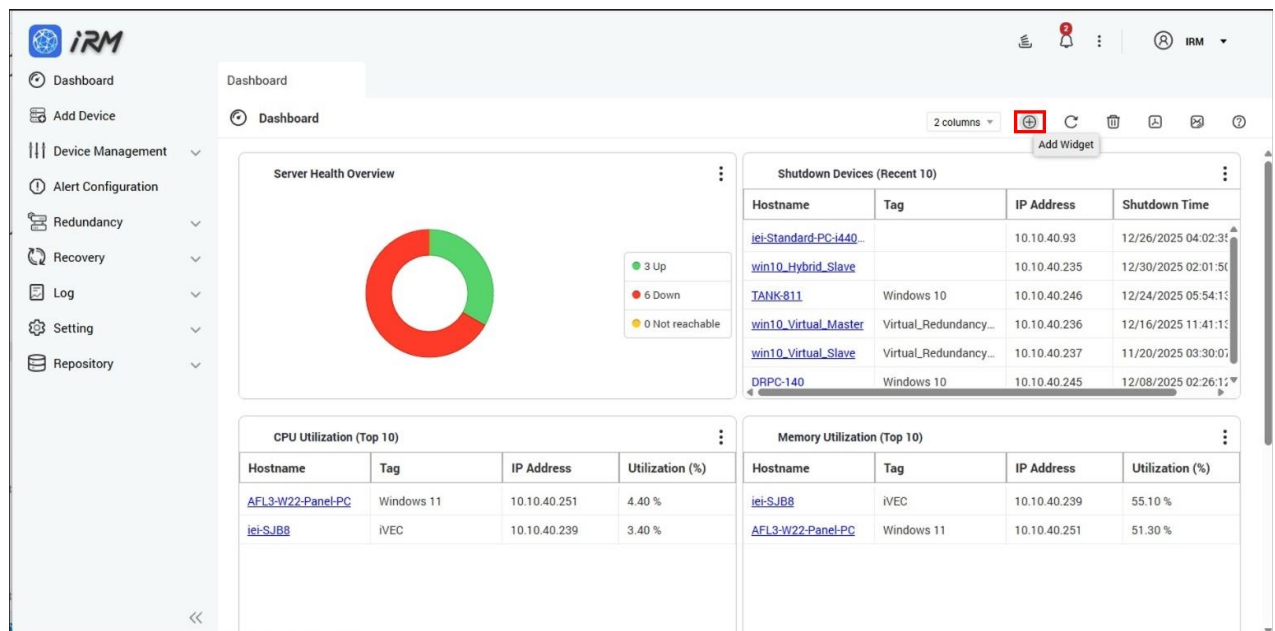
2.1 Add Widget

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
6. IPMI monitor
7. Hardware sensor

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 menu with options like Dashboard, Add Device, Device Management, Alert Configuration, Redundancy, Recovery, Log, Setting, and Repository. The main area contains several widgets: a 'Server Health Overview' donut chart showing 3 Up (green), 6 Down (red), and 0 Not reachable (yellow); a 'Shutdown Devices (Recent 10)' table; a 'CPU Utilization (Top 10)' table; and a 'Memory Utilization (Top 10)' table. In the top right corner of the dashboard area, there is a toolbar with icons for settings, notifications, and a red-bordered 'Add Widget' button.

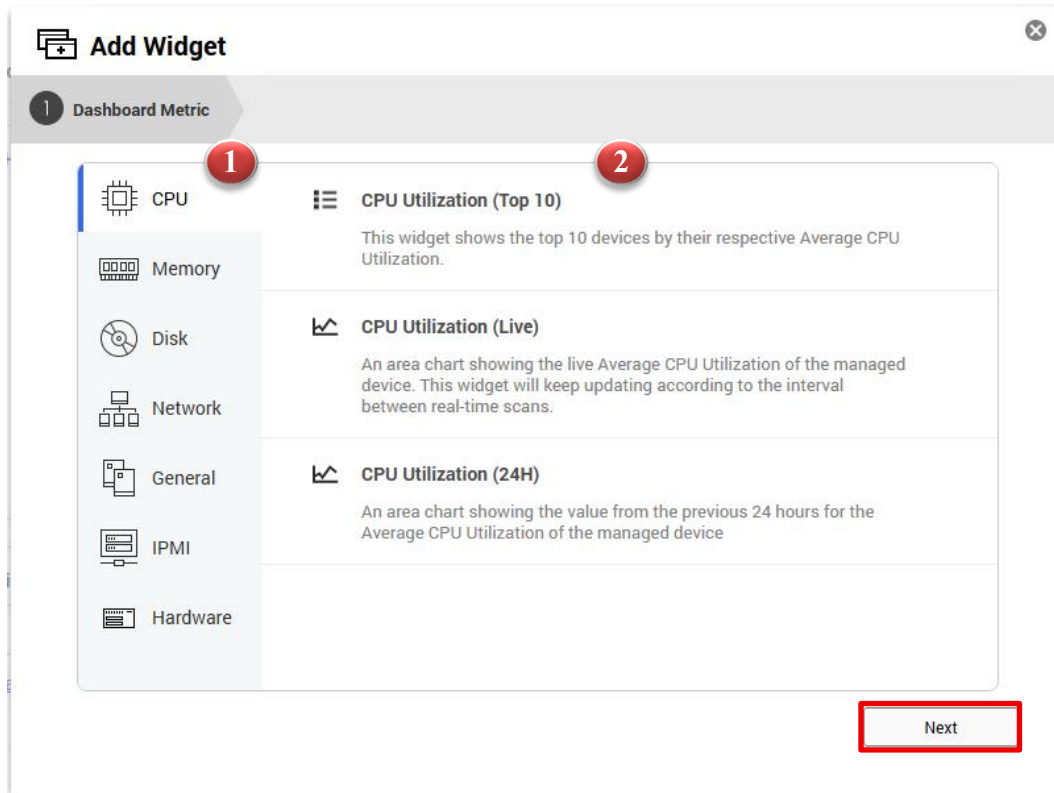
Hostname	Tag	IP Address	Shutdown Time
iei-Standard-PC-i440...		10.10.40.93	12/26/2025 04:02:31
win10_Hybrid_Slave		10.10.40.235	12/30/2025 02:01:50
TANK811	Windows 10	10.10.40.246	12/24/2025 05:54:13
win10_Virtual_Master	Virtual_Redundancy...	10.10.40.236	12/16/2025 11:41:13
win10_Virtual_Slave	Virtual_Redundancy...	10.10.40.237	11/20/2025 03:30:01
DRPC-140	Windows 10	10.10.40.245	12/08/2025 02:26:17

Hostname	Tag	IP Address	Utilization (%)
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	4.40 %
iei-SJB8	IVEC	10.10.40.239	3.40 %

Hostname	Tag	IP Address	Utilization (%)
iei-SJB8	IVEC	10.10.40.239	55.10 %
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	51.30 %

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 seven types: CPU usage, memory usage, disk usage, network usage, general health status, IPMI monitor and Hardware Sensor.
- (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".

Add Widget

1 Dashboard Metric 2 CPU Utilization (Live)

Category	Hostname ↑	IP Address	Tag	Manag...	Operati...
CPU	AFL3-W22-Panel-PC	10.10.40.251	Window...	IRMAgent	Microsof...
Memory	DRPC-140	10.10.40.245	Window...	IRMAgent	Microsof...
Disk	TANK-811	10.10.40.246	Window...	IRMAgent	Microsof...
Network	iei-SJB8	10.10.40.239	iVEC	IRMAgent	Ubuntu
General	iei-Standard-PC-i440FX...	10.10.40.93		IRMAgent	Ubuntu
IPMI	win10_Hybrid_Slave	10.10.40.235		IRMAgent	Microsof...
Hardware	win10_Virtual_Master	10.10.40.236	Virtual_R...	IRMAgent	Microsof...

Previous **Next**

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

Add Widget

1 Dashboard Metric 2 CPU Utilization (Live) 3 AFL3-W22-Panel-PC

Category	Widget Type
CPU	Area Chart 4
Memory	
Disk	
Network	
General	
IPMI	
Hardware	

Previous **Add Widget**

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. On the left is a navigation menu with items like Dashboard, Add Device, Device Management, Alert Configuration, Redundancy, Recovery, Log, Setting, and Repository. The main dashboard area contains several widgets:

- Server Health Overview:** A donut chart showing 3 Up (green), 6 Down (red), and 0 Not reachable (yellow).
- Shutdown Devices (Recent 10):** A table listing recently shutdown devices with columns for Hostname, Tag, IP Address, and Shutdown Time.
- CPU Utilization (Top 10):** A table listing the top 10 CPU-utilizing devices with columns for Hostname, Tag, IP Address, and Utilization (%).
- CPU Utilization (Live):** A line graph for 'AFL3-W22-Panel-PC' showing utilization percentage over time. This widget is highlighted with a red border in the image.

Step 6: IPMI Monitor

To display IPMI monitoring information on the Main Dashboard, refer to Section 4.4.3, IPMI Add Widget.

Step 7: Hardware Sensor

To display Hardware Sensor monitoring information on the Main Dashboard, refer to Section 4.1.11.1, Hardware Sensor Add Widget.

2.2 Delete All Widgets in the Dashboard

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

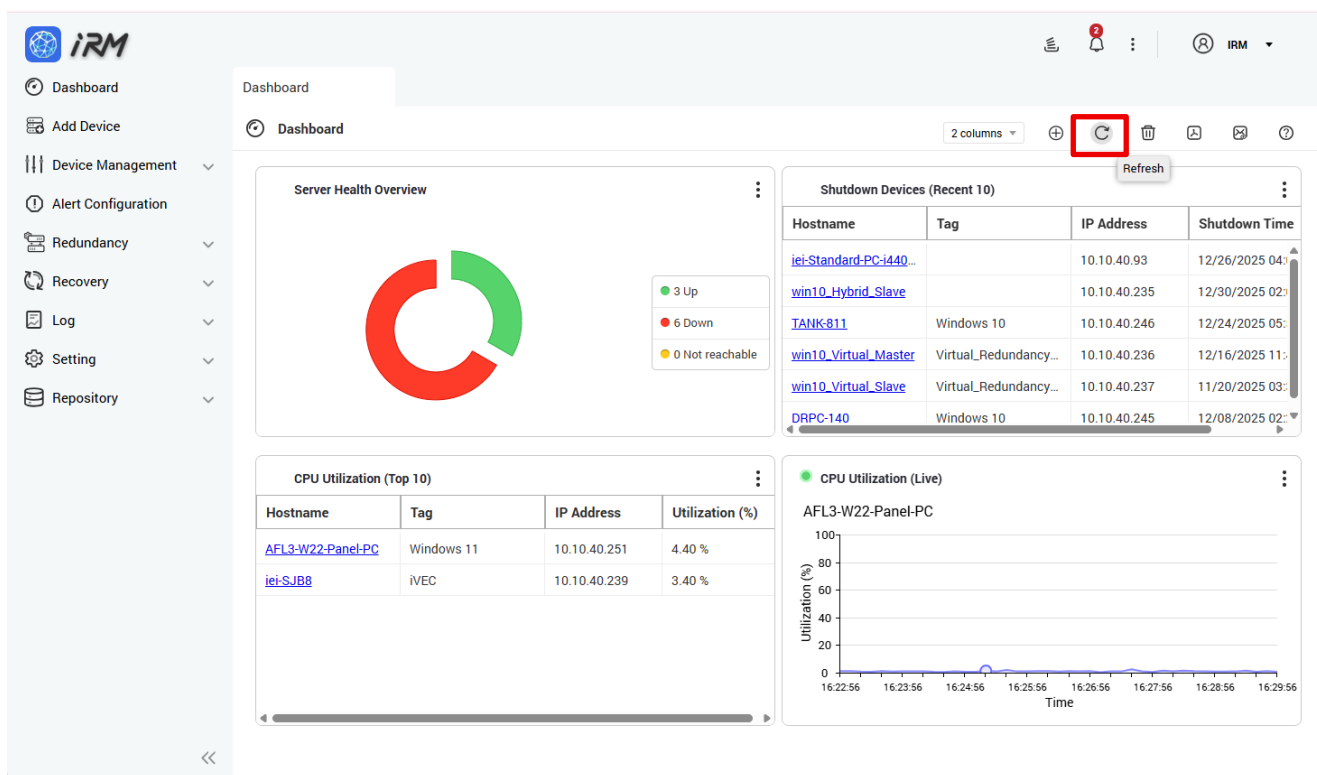
The screenshot shows the iRM dashboard with a sidebar on the left containing navigation options: Dashboard, Add Device, Device Management, Alert Configuration, Redundancy, Recovery, Log, Setting, and Repository. The main dashboard area contains several widgets:

- Server Health Overview:** A donut chart showing 3 Up (green), 6 Down (red), and 0 Not reachable (yellow).
- Shutdown Devices (Recent 10):** A table listing recently shutdown devices with columns for Hostname, Tag, IP Address, and Shutdown Time.
- CPU Utilization (Top 10):** A table listing the top 10 CPU-utilizing devices with columns for Hostname, Tag, IP Address, and Utilization (%).
- CPU Utilization (Live):** A line graph showing the live CPU utilization for the device AFL3-W22-Panel-PC over time.

In the top right corner of the dashboard area, there is a toolbar with icons for settings, notifications, and a refresh button (circular arrow icon) which is highlighted with a red box. Other icons include a trash can, a share icon, and a help icon.

2.3 Refresh All Widgets in the Dashboard

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



2.4 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. On the left is a navigation menu with items like Dashboard, Add Device, Device Management, Alert Configuration, Redundancy, Recovery, Log, Setting, and Repository. The main area contains several widgets:

- Server Health Overview:** A donut chart showing 3 Up (green), 6 Down (red), and 0 Not reachable (yellow).
- Shutdown Devices (Table):** A table with columns: Hostname, IP Address, and Shutdown Time. A dropdown menu is open above the table, showing options for 1 column, 2 columns (checked), and 3 columns.
- CPU Utilization (Top 10):** A table listing top CPU users.
- CPU Utilization (Live):** A line graph for device AFL3-W22-Panel-PC showing utilization percentage over time.

Hostname	Tag	IP Address	Utilization (%)
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	4.40 %
iei-SJB8	IVEC	10.10.40.239	3.40 %

2.5 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.

Dashboard

Server Health Overview

- 3 Up
- 6 Down
- 0 Not reachable

Shutdown Devices (Recent 10)

Hostname	Tag	IP Address	Shutdown Time
iei-Standard-PC-i440...		10.10.40.93	12/26/2025 04:...
win10_Hybrid_Slave		10.10.40.235	12/30/2025 02:...
TANK811	Windows 10	10.10.40.246	12/24/2025 05:...
win10_Virtual_Master	Virtual_Redundancy...	10.10.40.236	12/16/2025 11:...
win10_Virtual_Slave	Virtual_Redundancy...	10.10.40.237	11/20/2025 03:...
DRPC-140	Windows 10	10.10.40.245	12/08/2025 02:...

CPU Utilization (Top 10)

Hostname	Tag	IP Address	Utilization (%)
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	4.40 %
iei-SJB8	iVEC	10.10.40.239	3.40 %

CPU Utilization (Live)

AFL3-W22-Panel-PC

Utilization (%)

Time

Step 2: Showing "Generating View as PDF".

Step 3: Download the view to the local computer.

Report generation in progress...

IRM Report - Dashboard_2025-123 1.pdf
已封鎖不安全的下載內容

Dashboard

Server Health Overview

- 3 Up
- 6 Down
- 0 Not reachable

Shutdown Devices (Recent 10)

Hostname	Tag	IP Address	Shutdown Time
iei-Standard-PC-i440...		10.10.40.93	12/26/2025 04:...
win10_Hybrid_Slave		10.10.40.235	12/30/2025 02:...
TANK811	Windows 10	10.10.40.246	12/24/2025 05:...
win10_Virtual_Master	Virtual_Redundancy...	10.10.40.236	12/16/2025 11:...
win10_Virtual_Slave	Virtual_Redundancy...	10.10.40.237	11/20/2025 03:...
DRPC-140	Windows 10	10.10.40.245	12/08/2025 02:...

CPU Utilization (Top 10)

Hostname	Tag	IP Address	Utilization (%)
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	4.40 %
iei-SJB8	iVEC	10.10.40.239	3.40 %

CPU Utilization (Live)

AFL3-W22-Panel-PC

Utilization (%)

Time

2.6 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.

The screenshot shows the iRM Dashboard interface. On the left is a navigation menu with items like Dashboard, Add Device, Device Management, Alert Configuration, Redundancy, Recovery, Log, Setting, and Repository. The main content area is titled 'Dashboard' and contains several widgets:

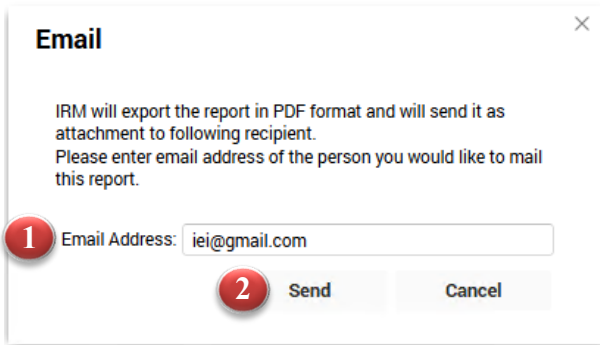
- Server Health Overview:** A donut chart showing 3 Up (green), 6 Down (red), and 0 Not reachable (yellow).
- Shutdown Devices (Recent 10):** A table listing devices with columns for Hostname, Tag, IP Address, and Shutdown Time.
- CPU Utilization (Top 10):** A table listing top CPU utilization devices with columns for Hostname, Tag, IP Address, and Utilization (%).
- CPU Utilization (Live):** A line graph showing live CPU utilization for 'AFL3-W22-Panel-PC' over time.

 In the top right corner of the dashboard, there is a toolbar with icons for settings, refresh, and a red-bordered button labeled 'Email', which is highlighted by a red box. A tooltip above this button reads 'Export and send email with PDF file'.

Hostname	Tag	IP Address	Shutdown Time
iei-Standard-PC-1440		10.10.40.93	12/26/2025 04:02:35 PM
win10_Hybrid_Slave		10.10.40.235	12/30/2025 02:01:50 PM
TANK811	Windows 10	10.10.40.246	12/24/2025 05:54:13 PM
win10_Virtual_Master	Virtual_Redundancy...	10.10.40.236	12/16/2025 11:41:13 AM
win10_Virtual_Slave	Virtual_Redundancy...	10.10.40.237	11/20/2025 03:30:07 PM
DRPC-140	Windows 10	10.10.40.245	12/08/2025 02:26:12 PM

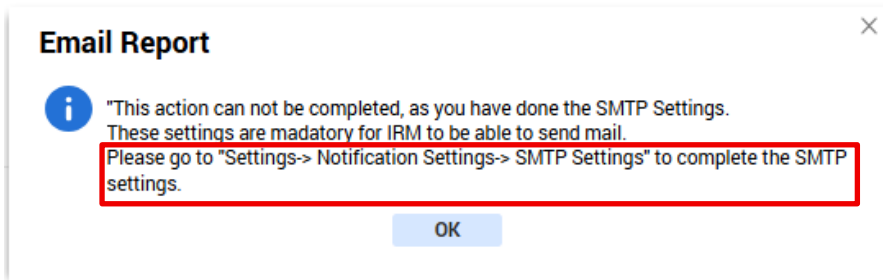
Hostname	Tag	IP Address	Utilization (%)
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	4.40 %
iei-SJB8	IVEC	10.10.40.239	3.40 %

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



If the SMTP settings have not been configured, the system displays an Email Report pop-up indicating that the email cannot be sent, and guides you to the SMTP configuration path. Click OK to close the message.

Please refer to Section 10.2, "Notification Settings," for setup instructions.



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

The screenshot shows the iRM dashboard interface. A notification banner at the top reads "Sending email to specified email address(s)..." and "The report has been successfully sent to specified mail." Below the notification, the dashboard displays several widgets:

- Server Health Overview:** A donut chart showing 3 Up (green), 6 Down (red), and 0 Not reachable (yellow).
- Shutdown Devices (Recent 10):** A table listing devices and their shutdown times.
- CPU Utilization (Top 10):** A table listing the top 10 CPU-utilizing devices.
- CPU Utilization (Live):** A line graph showing real-time CPU utilization for device AFL3-W22-Panel-PC.

Hostname	Tag	IP Address	Shutdown Time
iei-Standard-PC-i440		10.10.40.93	12/26/2025 04:02:35 PM
win10_Hybrid_Slave		10.10.40.235	12/30/2025 02:01:50 PM
TANK811	Windows 10	10.10.40.246	12/24/2025 05:54:13 PM
win10_Virtual_Master	Virtual_Redundancy...	10.10.40.236	12/16/2025 11:41:13 AM
win10_Virtual_Slave	Virtual_Redundancy...	10.10.40.237	11/20/2025 03:30:07 PM
DRPC-140	Windows 10	10.10.40.245	12/08/2025 02:26:12 PM

Hostname	Tag	IP Address	Utilization (%)
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	4.40 %
iei-SJBS	IVEC	10.10.40.239	3.40 %

2.7 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.

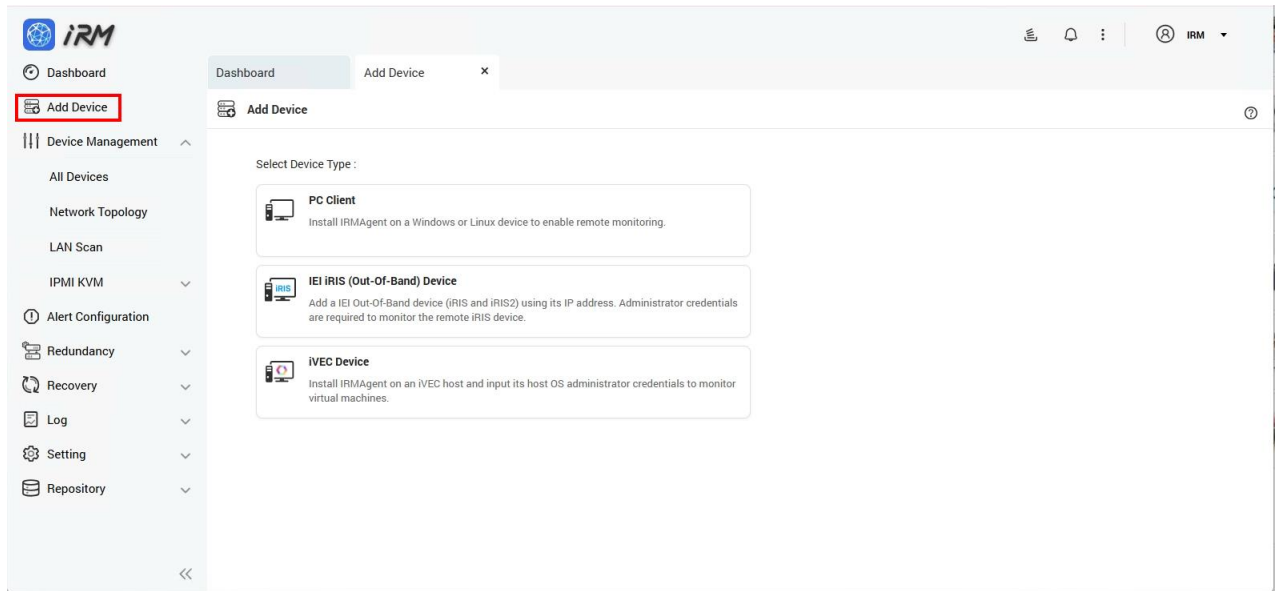
Note: All widgets can be dragged and moved within the Dashboard.

Chapter

3

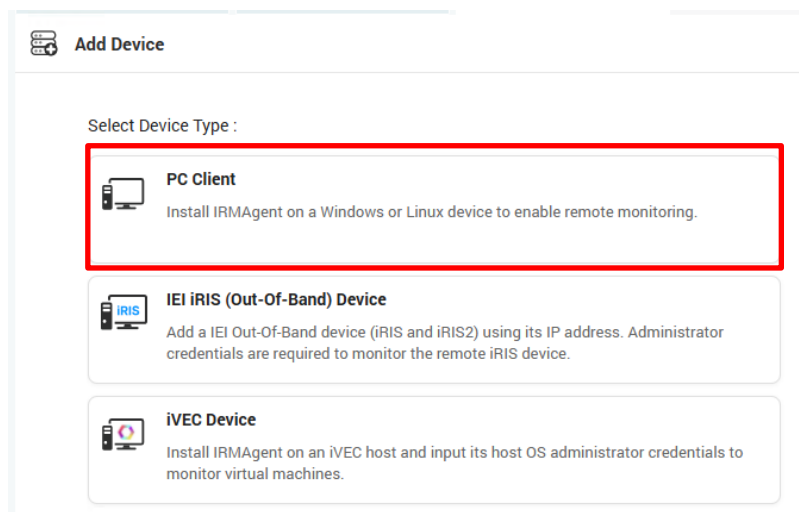
3 Add Device

The **Add Device** function is used to add devices to IRM for subsequent monitoring, alert notifications, and remote management. IRM provides different add methods and required settings depending on the device type. After a device is added, administrators can view its status in the device list and use the related management functions.



IRM supports three device types that can be added for management. On the **Add Device** page, first select the device type you want to add:

1. **PC Client:** Install the **IRM Agent** on a Windows or Linux device to enable endpoint monitoring.



3.1 Add Windows Devices

Add Windows Devices to the IRM Workflow

Hostname	Tag	IP Address	Operating System	Category	Brand	Status
AFL3-W22-Panel-PC	Windows 11	10.10.40.251	Microsoft Windows 11 Pro	Agent	IEI	Monitored
DRPC-140	Windows 10	10.10.40.245	Microsoft Windows 10 Pro	Agent	IEI	Monitored
TANK-811	Windows 10	10.10.40.246	Microsoft Windows 10 Pro	Agent	IEI	Monitored
win10_Hybrid_Slave	Hybrid_Slave_OS	10.10.40.235	Microsoft Windows 10 專業版	Agent	QEMU	Monitored
win10_Virtual_Master	Virtual_Redundancy_Master	10.10.40.236	Microsoft Windows 10 專業版	Agent	QEMU	Monitored
win10_Virtual_Slave	Virtual_Redundancy_Slave	10.10.40.237	Microsoft Windows 10 專業版	Agent	QEMU	Monitored

Install the **IRM Agent** on a Windows or Linux device to enable remote monitoring. After you click this option, the system displays the “**Add Device to IRM (PC Client)**” window.

Download IRM Agent: You must install the IRM Agent before the device can be added.

If the download and installation are not completed within **10 minutes**, the operation will time out.

- (1). Download Windows IRM Agent: Click Download, then select 32-bit or 64-bit to download the installer to your local computer.
- (2). Download and install Microsoft .NET Framework (for Windows 7): Click Download to open the official Microsoft .NET Framework 4 (Standalone Installer) page, then select the appropriate language version and download it to your local computer.
- (3). Download Linux IRM Agent: Click Download, then select Ubuntu, Debian, or CentOS to download the package to your local computer.

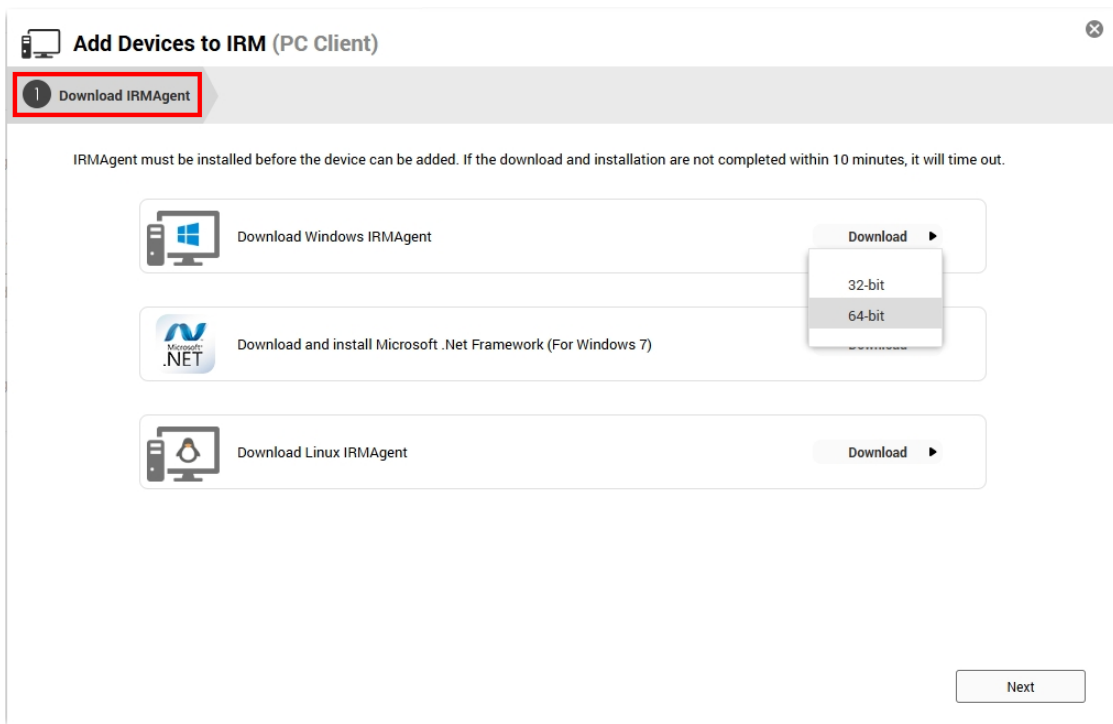
Copy the IRM Agent package to the device you want to manage. After extracting and running the installer, you can view the installation status in the device list.

3.1.1 Windows Devices

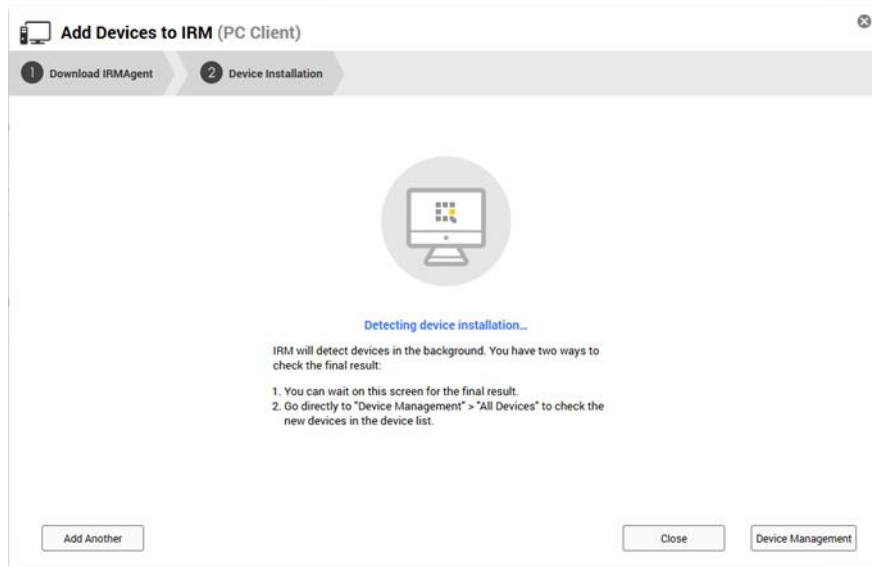
Users of MS Windows device must download IRMAgent to the machine to be installed and extract the IRMAgent archive on the machine to run the installation program. After successful installation, IRM will be able to monitor and manage the device.

Step 1: Download IRM Agent

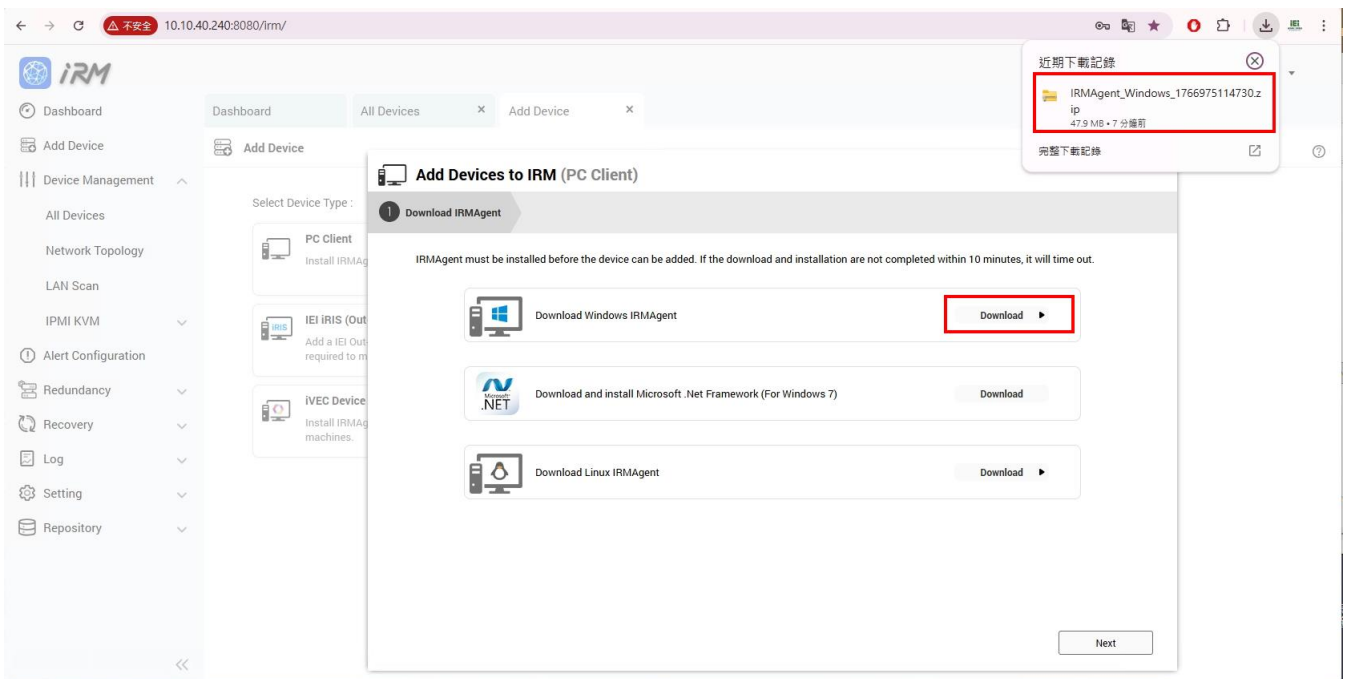
1). Users can select the appropriate IRMAgent installation package.



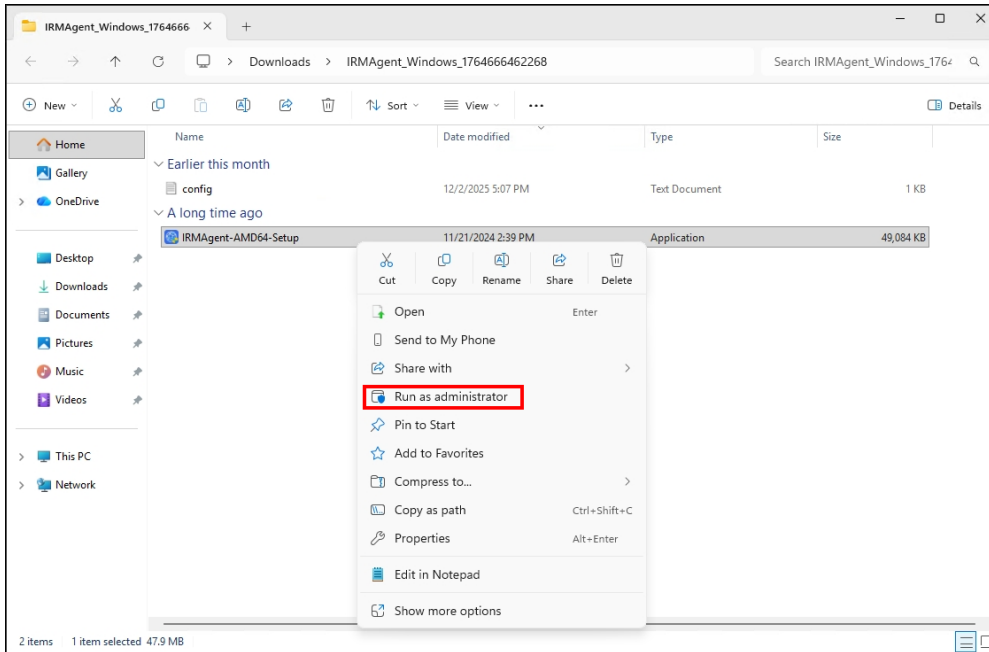
Step 2: Device Installation



1). Copy the installation package to the device to be managed.

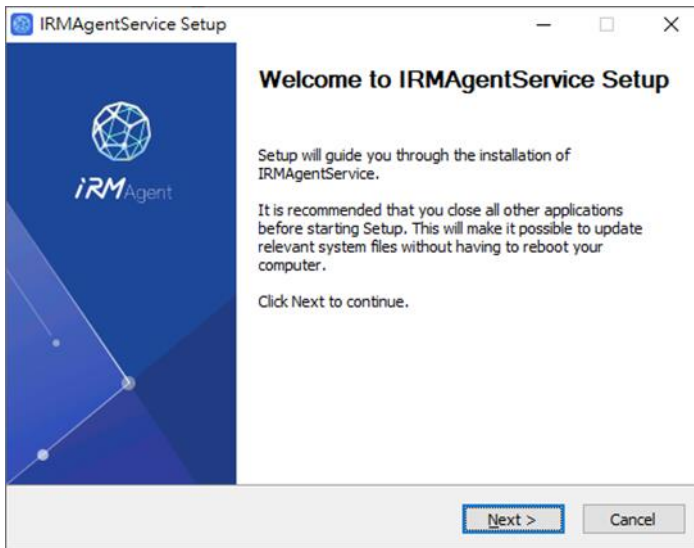


2). Unzip the installer, right click on the installer and select "Run as administrator".



3). Click "Yes" to allow the installer to make changes to your device.

4). Click "Next".



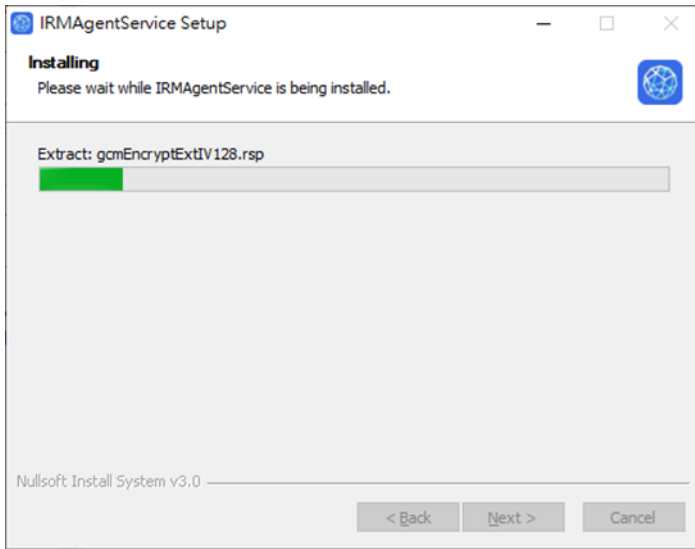
5). Choose the IP address and click "Next".

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'.

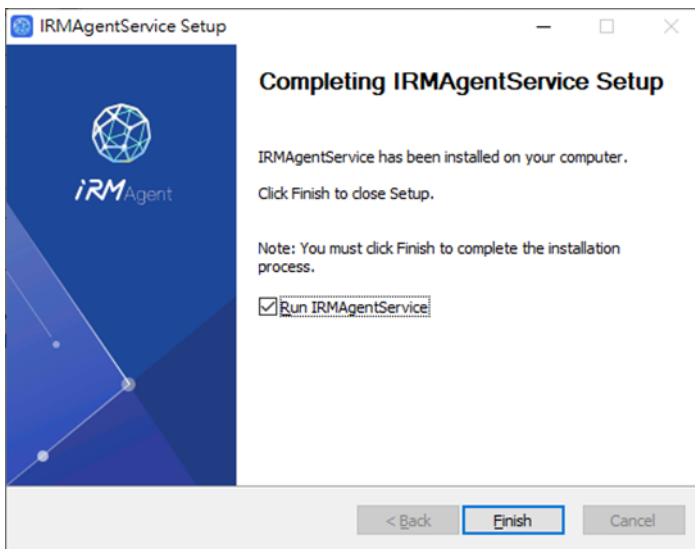
6). Enter the Username and Password of IRM.

The screenshot shows the 'IRMAgentService Setup' window at the 'Enter Username & Password' step. The title bar is the same as in the previous screenshot. 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-heading 'Please enter your username and password before continuing...' and a box 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'.

7). The IRMAgentService will be installed.



8). Click "Finish" and you will see the installation status in the device list.




Step 3: Installation Summary

Device added successfully. The device has been successfully added to IRM. You can find it in the device list under [Device Management] > [All Devices].

Add Devices to IRM (PC Client)
✕

1 Download IRMAgent
2 Device Installation
3 Installation Summary




Device added successfully.

The device has been successfully added to IRM. You can check it in the device list under "Device Management" > "All Devices".

Add Another
Close
Device Management

Step 4: Windows Device added successfully.

The device has been successfully added to IRM. You can check it in the device list under "Device Management" > "All Devices" or "IRMAgent-Windows".


Dashboard
IRM

- Dashboard
- Add Device
- Device Management
 - All Devices
 - Network Topology
 - LAN Scan
 - IPMI KVM
 - Alert Configuration
 - Redundancy
 - Recovery
 - Log
 - Setting
 - Repository

Dashboard
All Devices
✕

Device Management / All Devices

Action
+
✕
↻
ⓘ

My Network
ALL
4
5
0

Hostname ↑	Tag	IP Address	Operating System	Category	Brand	Status
<input type="checkbox"/> AFL3-W22-Panel-PC	Windows 11	10.10.40.251	Microsoft Window...	Agent	IEI	Monitored
<input type="checkbox"/> DRPC-140	Windows 10	10.10.40.245	Microsoft Window...	Agent	IEI	Monitored
<input type="checkbox"/> TANK-811	Windows 10	10.10.40.246	Microsoft Window...	Agent	IEI	Monitored
<input type="checkbox"/> win10_Hybrid_Slave		10.10.40.235	Microsoft Window...	Agent	QEMU	Monitored
<input type="checkbox"/> win10_Virtual_Master	Virtual_Redundancy_Ma...	10.10.40.236	Microsoft Window...	Agent	QEMU	Monitored
<input type="checkbox"/> win10_Virtual_Slave	Virtual_Redundancy_Slave	10.10.40.237	Microsoft Window...	Agent	QEMU	Monitored

Page 41

3.1.2 Linux Devices

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.

Add Linux Devices to the IRM Workflow

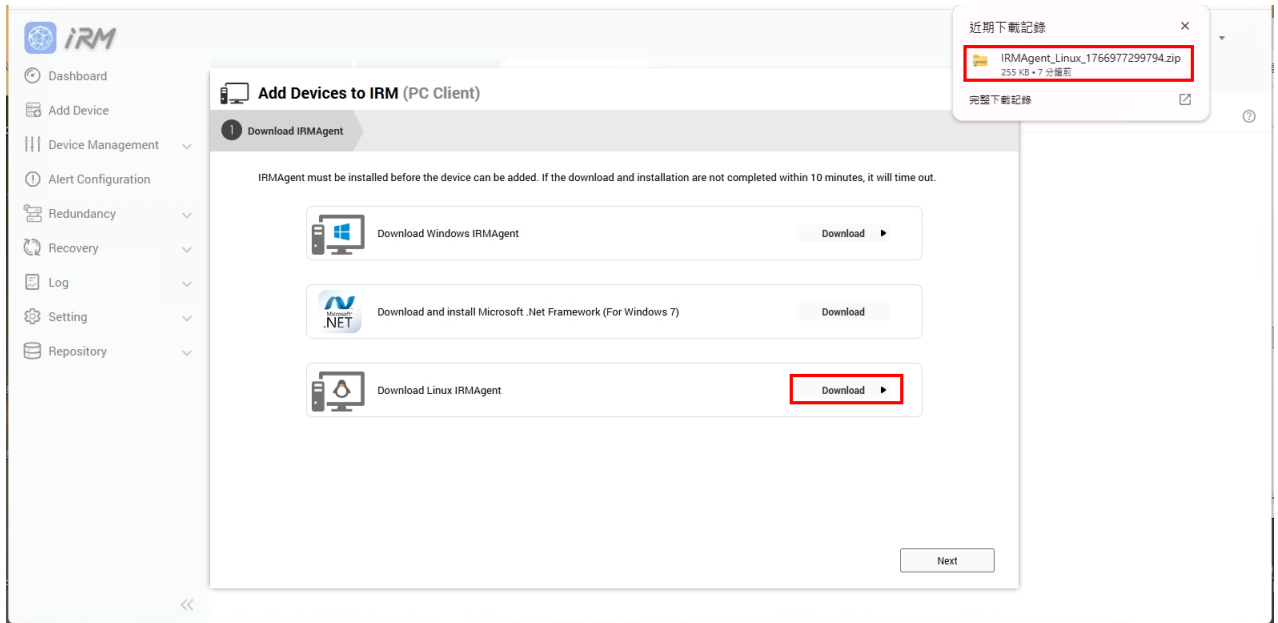
Hostname	Tag	IP Address	Operating System	Brand	Status
iei-SJBB	IVEC Platform	10.10.40.239	Ubuntu	IEI	Monitored
iei-Standard-PC-I440FX-PIIX-1996		10.10.40.93	Ubuntu	QEMU	Monitored

Step 1: Download IRM Agent

1). Users can select the appropriate IRMAgent installation package.

Step 2: Device Installation

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



2). In the Linux shell, unzip the IRMAgent installation package.

```
iei@iei-SJB8:~$ unzip IRMAgent_Linux_1766977299794.zip
Archive: IRMAgent_Linux_1766977299794.zip
extracting: config.txt
extracting: InstallUbuntuIRMAgent.sh
extracting: UninstallUbuntuIRMAgent.sh
extracting: ReinstallUbuntuIRMAgent.sh
extracting: RedirectUbuntuIRMAgent.sh
extracting: data/CreateRemoveUbuntuIRMAgentService.sh
extracting: data/RemoveUbuntuIRMAgent.sh
extracting: data/CreateRedirectUbuntuIRMAgentService.sh
extracting: data/RedirectUbuntuIRMAgentRegister.sh
```

3). Use the following command to run the IRMAgent installation program:
 “sudo ./InstallUbuntuIRMAgent.sh <Client IP Address>”

```
iei@iei-SJB8:~$
iei@iei-SJB8:~$ sudo ./InstallUbuntuIRMAgent.sh 10.10.40.239
* INFO: PYTHON_PATH: /usr/bin/python3
* INFO: PYTHON_VERSION: 3.10.12

* INFO: System Information:
* INFO: CPU: GenuineIntel
* INFO: CPU Arch: x86_64
* INFO: OS Name: Linux
* INFO: OS Version: 5.15.0-1075-intel-iotg
* INFO: Distribution: Ubuntu 22.04

* INFO: DISTRO_MAJOR_VERSION: 22
* INFO: DISTRO_MINOR_VERSION: 04
* INFO: DISTRO_CODENAME: jammy
The following NEW packages will be installed on system:
salt-common-iei_1.0.1
salt-minion-iei_1.0.0
Do you want to continue? [Y/n]
y
```

4). Enter the IRM Username and Password.

```
Please enter your IRM's username and password to continue.
Please enter your IRM's username:
IRM
Please enter your IRM's password:
1234qwer
```

5). The installation process will be displayed.

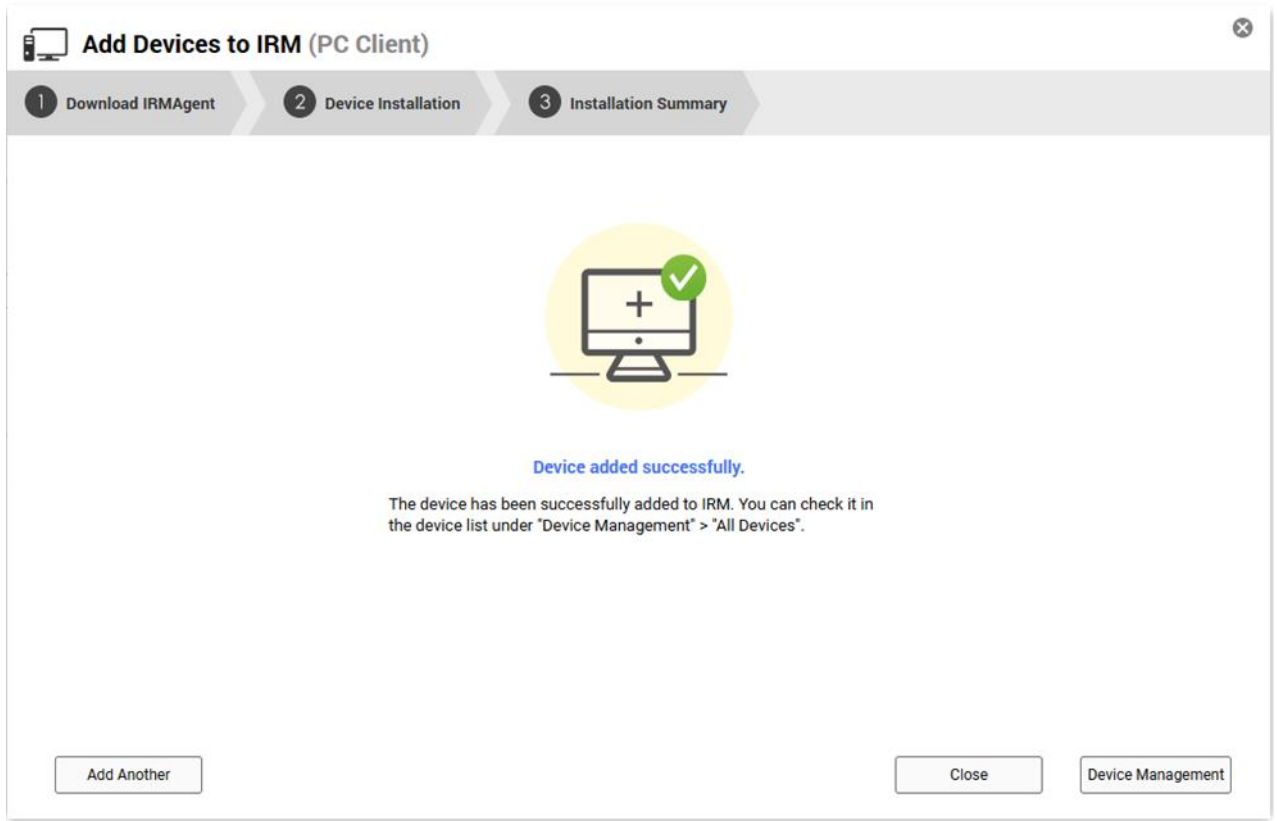
```
kill: (223923): No such process
http://10.10.40.240:8080/irm/resources/IRMAgentPack/Ubuntu/22/IRMAgent-Ubuntu-22-64.tgz
download 0Agent and copy files
--2025-12-29 11:27:22-- http://10.10.40.240:8080/irm/resources/IRMAgentPack/Ubuntu/22/IRMAgent-Ubuntu-22-64.tgz
Connecting to 10.10.40.240:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 12247040 (12M) [application/x-tar]
Saving to: 'IRMAgent-Ubuntu-22-64.tgz'

IRMAgent-Ubuntu-22-64.tgz      100%[=====] 11.68M  --.-KB/s  in 0.1s
2025-12-29 11:27:22 (107 MB/s) - 'IRMAgent-Ubuntu-22-64.tgz' saved [12247040/12247040]

copy file
set version config success
disabled
Created symlink /etc/systemd/system/multi-user.target.wants/salt-minion.service → /lib/systemd/system/salt-minion.service.
kill: (224298): No such process
```

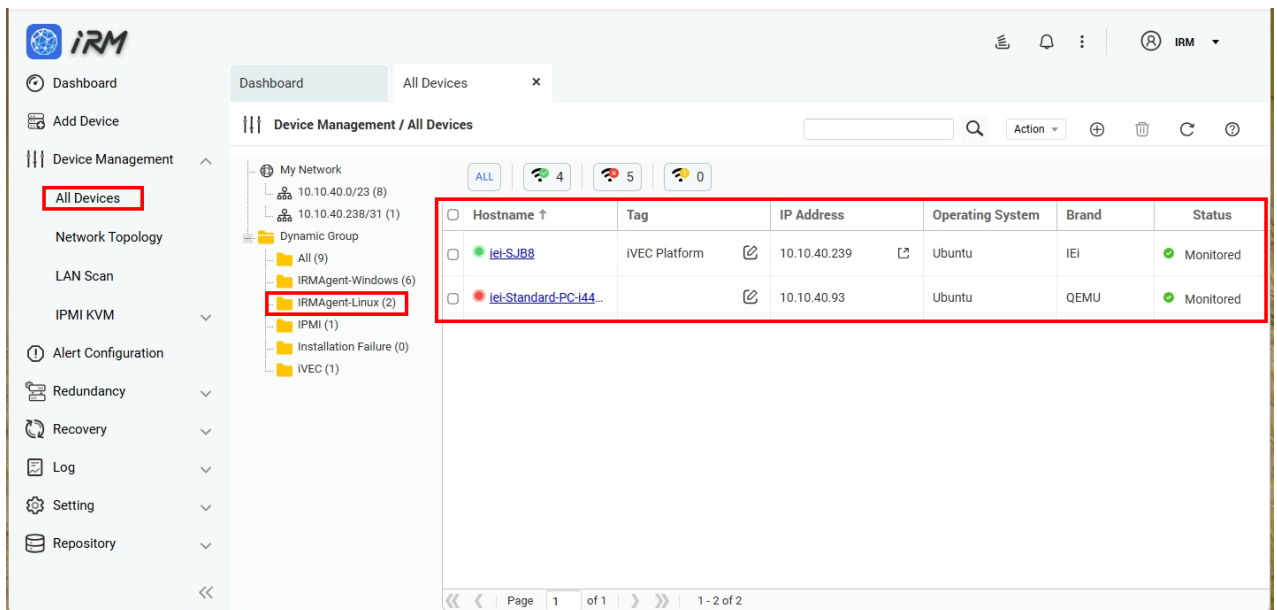
Step 3: Installation Summary

Device added successfully. The device has been successfully added to IRM. You can find it in the device list under [Device Management] > [All Devices].

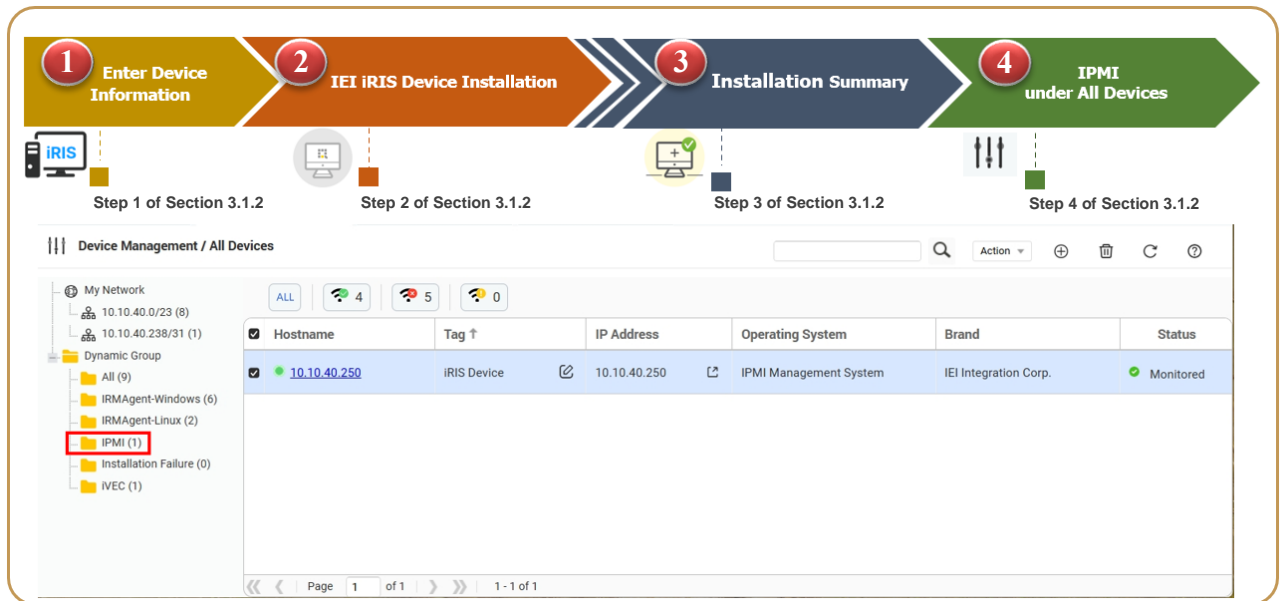
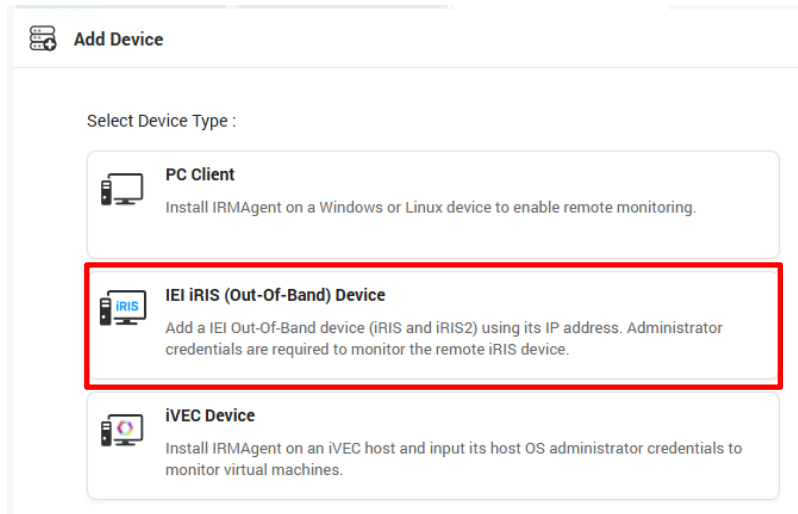


Step 4: Linux Device added successfully.

The device has been successfully added to IRM. You can check it in the device list under "Device Management" > "All Devices" or "IRMAgent-Linux".



2. **IEI iRIS (Out-of-Band Management) Device:** Add an IEI out-of-band management device (iRIS / iRIS2) using its IP address, and provide an account with administrative privileges for monitoring.



3. **iVEC Device:** Install the **IRM Agent** on the iVEC host and enter an account with administrative privileges to monitor **iVEC devices**.

Add Device

Select Device Type :

PC Client
Install IRMAgent on a Windows or Linux device to enable remote monitoring.

IEI iRIS (Out-Of-Band) Device
Add a IEI Out-Of-Band device (iRIS and iRIS2) using its IP address. Administrator credentials are required to monitor the remote iRIS device.

iVEC Device
Install IRMAgent on an iVEC host and input its host OS administrator credentials to monitor virtual machines.

Add iVEC Devices to the iVEC Workflow

1 Enter Device Information

2 Download IRMAgent

3 Linux IRMAgentService Installation

4 Installation Summary

5 iVEC under All Devices

Step 1 of Section 3.1.3 Step 2 of Section 3.1.3 Step 3 of Section 3.1.3 Step 4 of Section 3.1.3 Step 4 of Section 3.1.3

Device Management / All Devices

Hostname	Tag ↑	iVEC VM(s)	IP Address	Operating System	Category	Brand	Status
iei-S_IB8	iVEC		10.10.40.239	Ubuntu	Agent	IEI	Monitored

Page 1 of 1

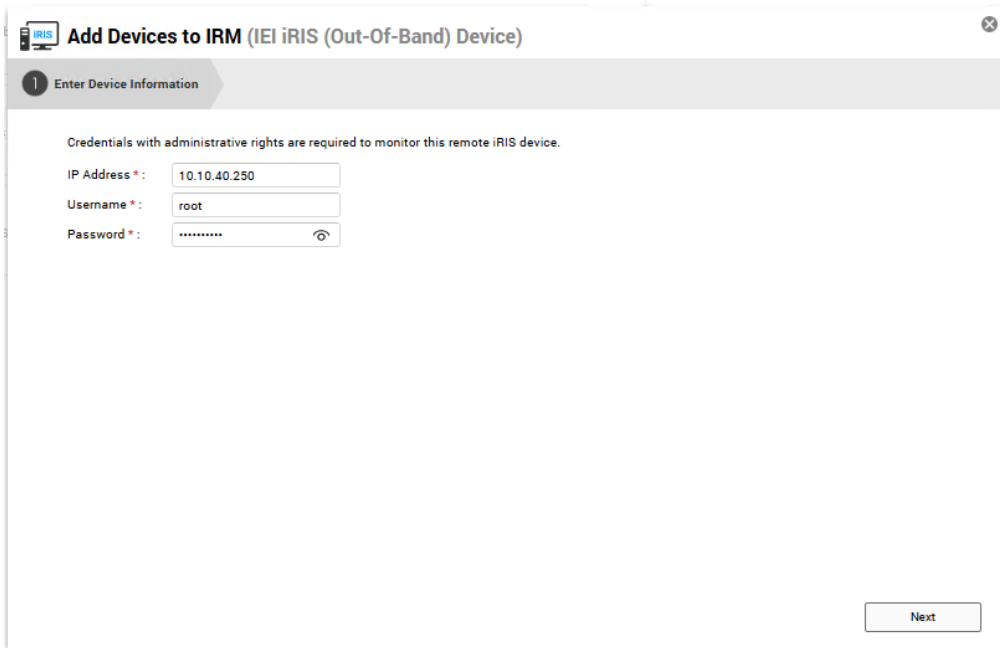
3.2 IEI out-of-band management device

Add an IEI out-of-band management device (**iRIS / iRIS2**) using its IP address. You must provide an account and password with administrative privileges to monitor the remote iRIS device. After you click this option, the system displays the “**Add Device to IEI iRIS (Out-of-Band Management) Device**” window.

Step 1: Enter Device Information

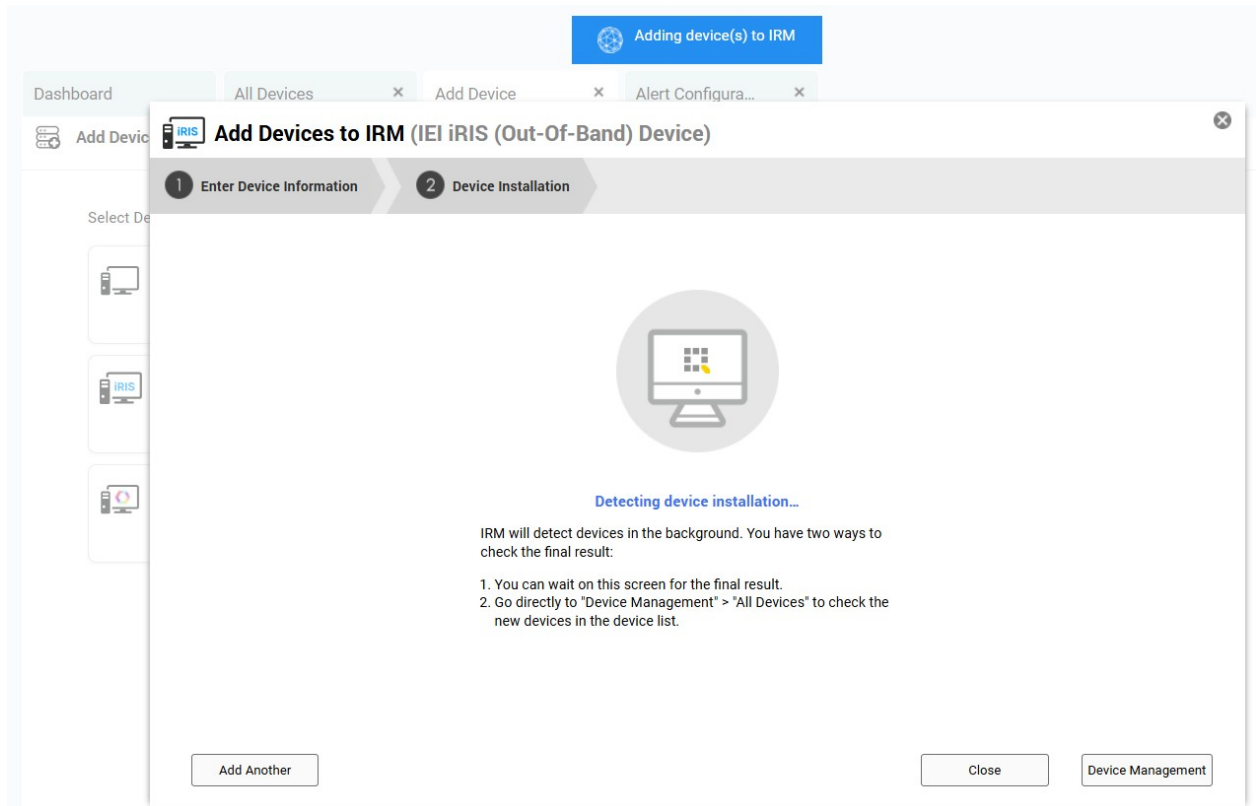
You must have administrator privileges to monitor a remote iRIS device.

- (1). **IP Address***: Enter the iRIS IP address.
- (2). **Username***: Enter the iRIS user account.
- (3). **Password***: Enter the iRIS user password.

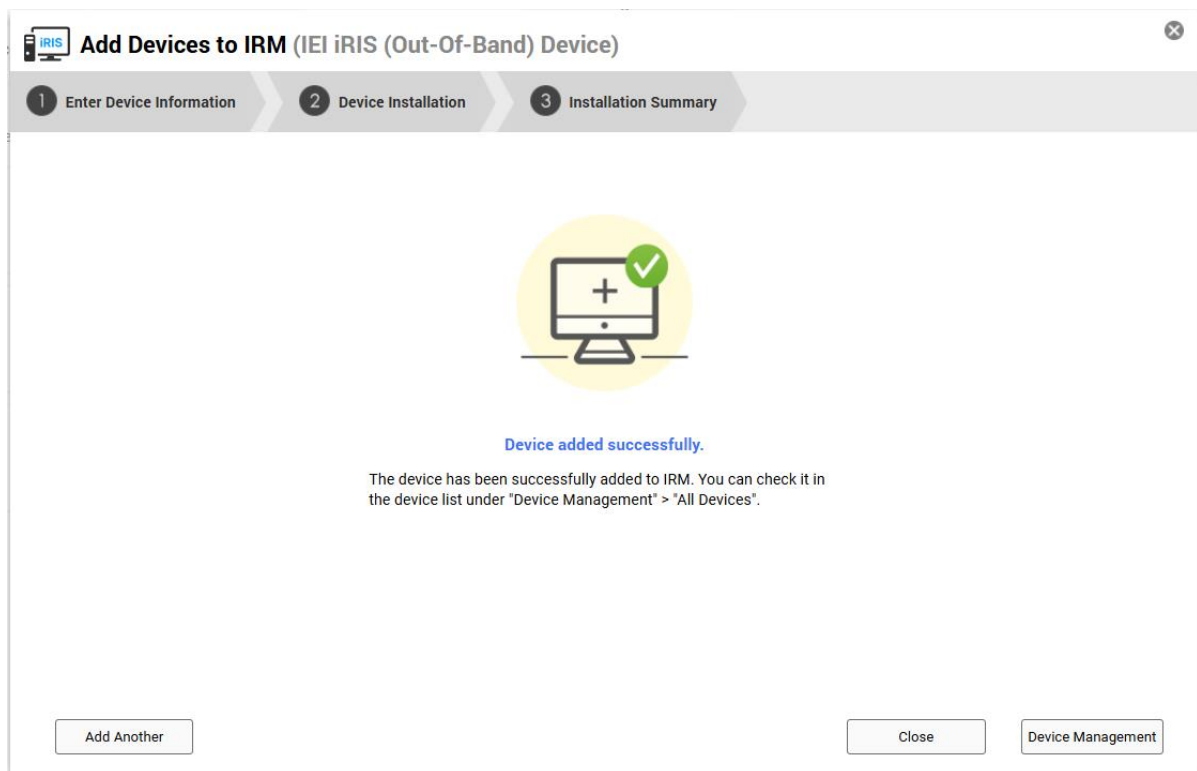


The screenshot shows a web application window titled "Add Devices to IRM (IEI iRIS (Out-Of-Band) Device)". The window has a close button in the top right corner. Below the title bar, there is a tab labeled "1 Enter Device Information". A message states: "Credentials with administrative rights are required to monitor this remote iRIS device." Below this message are three input fields: "IP Address *" with the value "10.10.40.250", "Username *" with the value "root", and "Password *" with masked characters "*****" and a visibility icon. A "Next" button is located at the bottom right of the form area.

Step 2: Device Installation

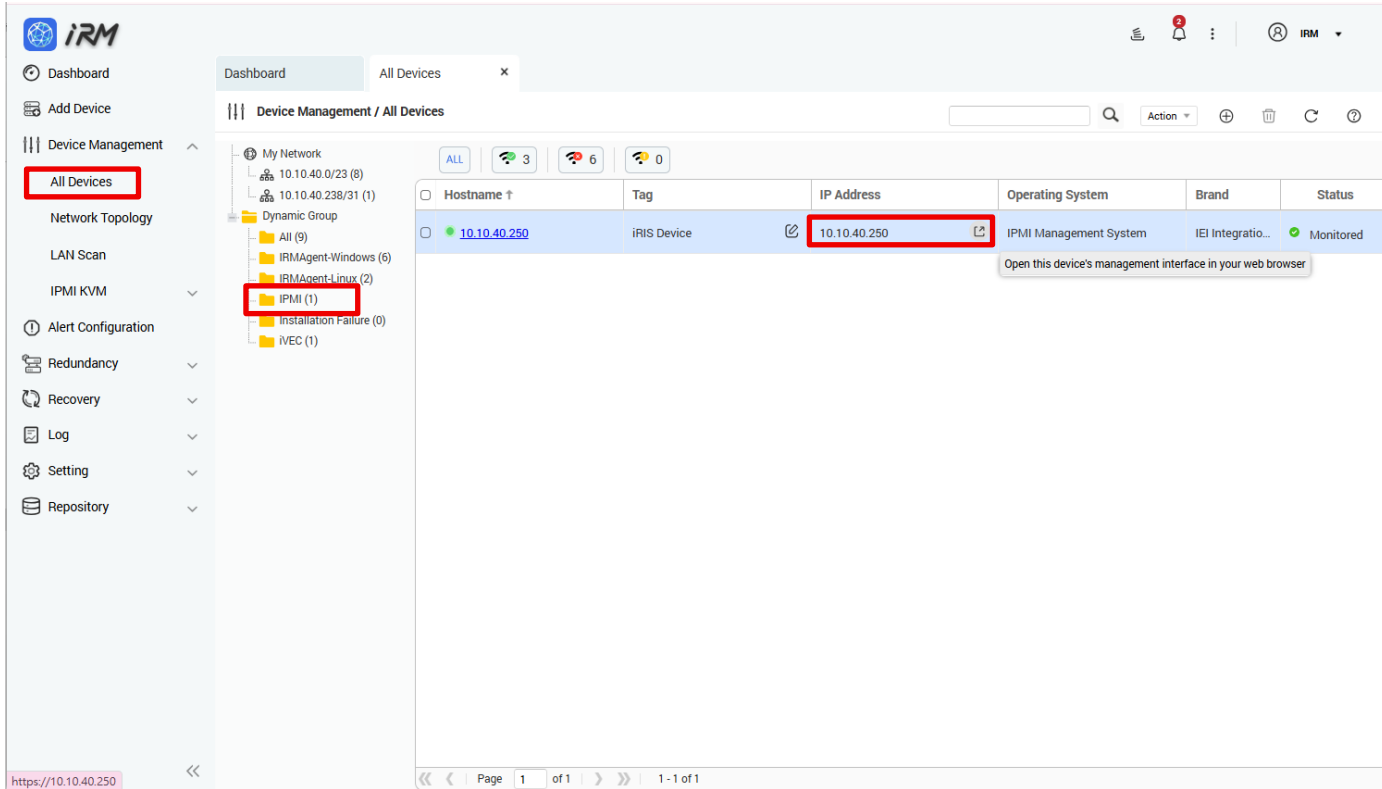


Step 3: Installation Summary



Step 4: IEI iRIS Device added successfully.


The device has been successfully added to IRM. You can check it in the device list under "Device Management" > "All Devices" or "IPMI".

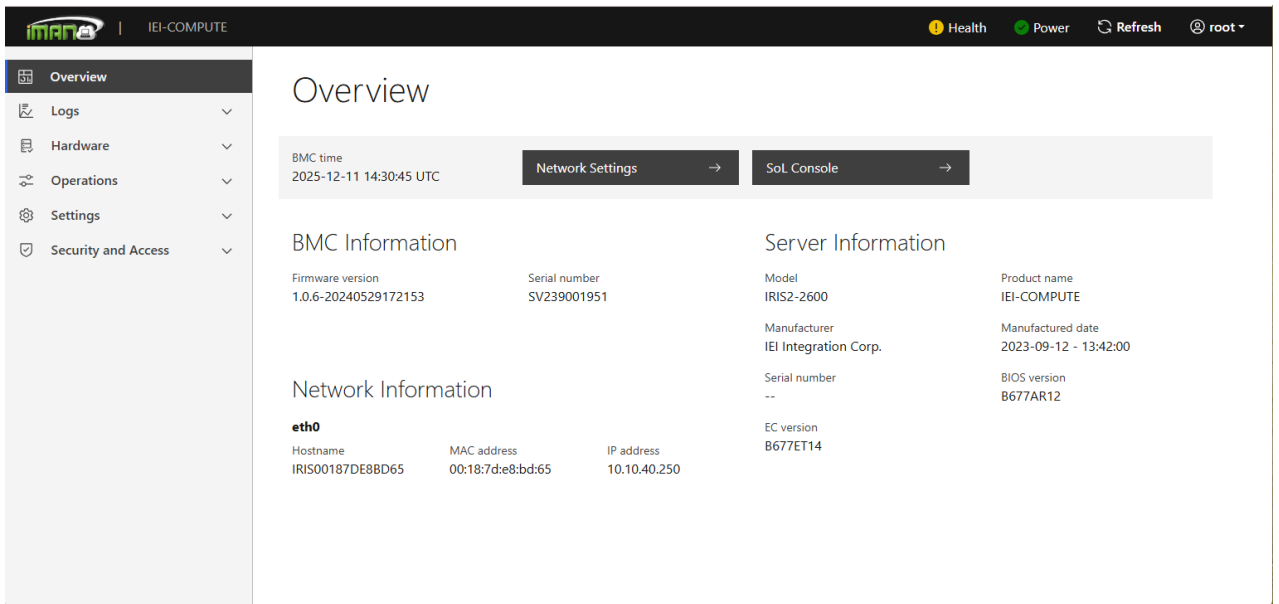
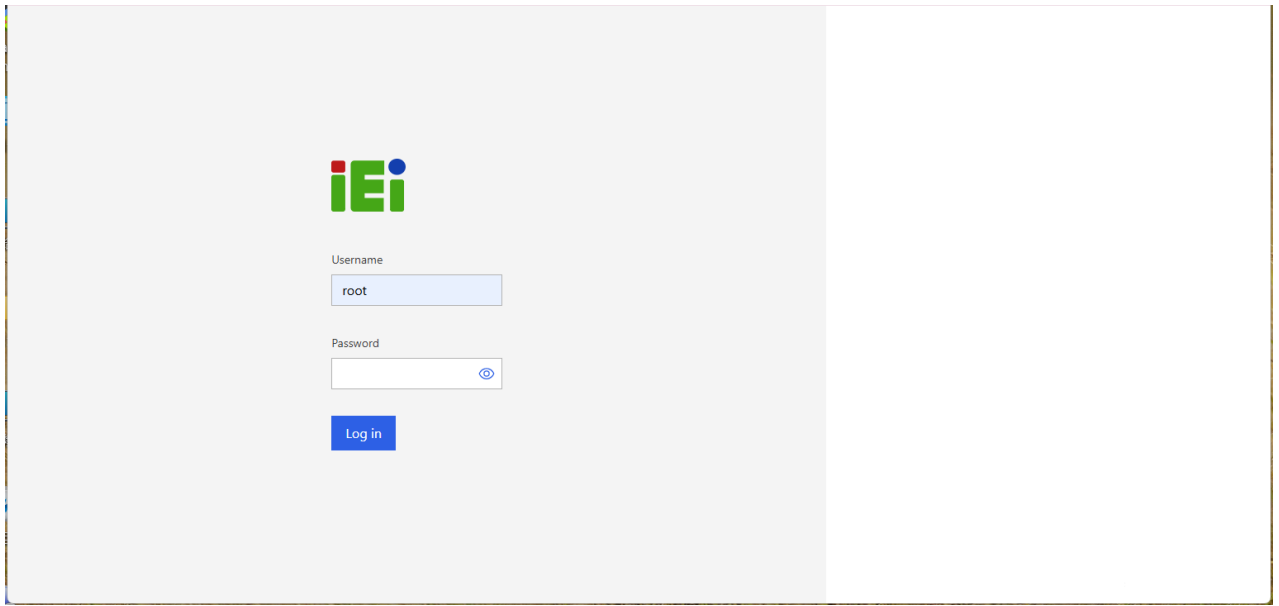


IPMI Device List

The **IPMI Device List** is the main entry point in IRM for managing IPMI (out-of-band management) devices. From this list, administrators can centrally view information for IPMI devices that have been added to IRM (such as **Hostname**, **IP address**, **Tag**, **Brand/Model**, and **Status**) and quickly open the device's **IPMI Web UI** for further operations.

Step 1:

- Open this IPMI device's management interface in your web browser
Click  icon, it will go to IPMI management interface.



3.3 iVEC devices

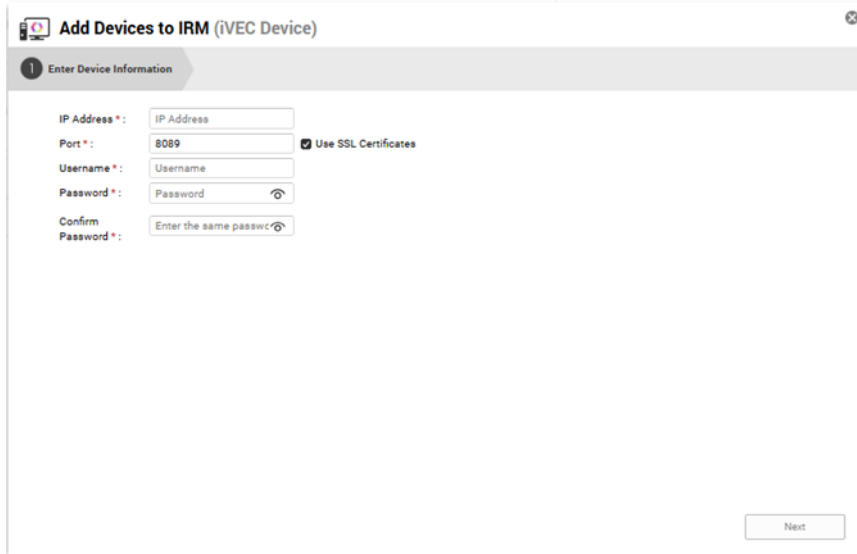
Install the **IRM Agent** on the iVEC host, then enter the **port** and an account/password with administrative privileges to monitor **iVEC devices**. After you click this option, the system displays the “**Add Device to IRM (iVEC Device)**” window.

Step 1: Enter Device Information

You must have administrator privileges to monitor a remote iVEC device.

- (1). **IP Address***: Enter the iVEC IP address.
- (2). **Port***: The default port for the iVEC host is 8089, using an SSL certificate.
- (3). **Username***: Enter the login username for the iVEC host.
- (4). **Password***: Enter the login password for the iVEC host.
- (5). **Confirm Password***: Re-enter the login password for the iVEC host.

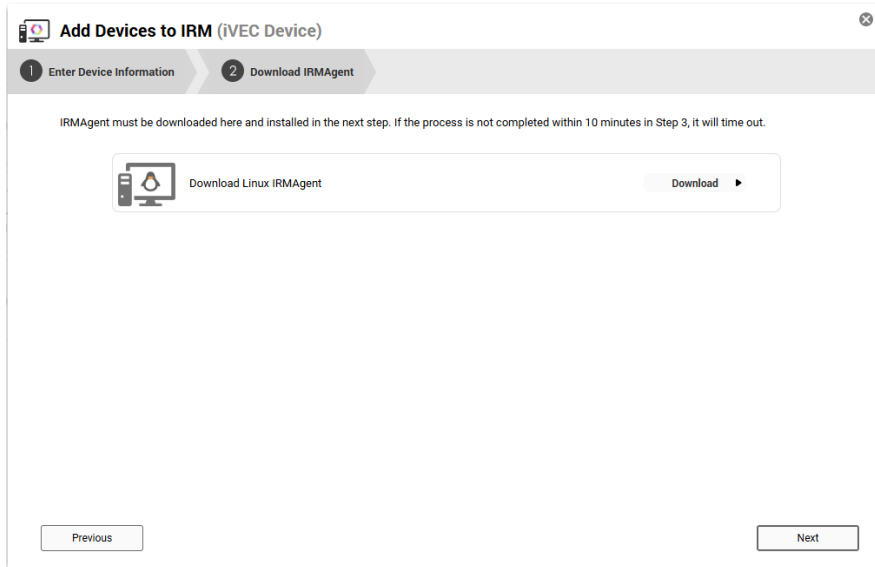
After verifying the information is correct, click **Next**.



Step 2: Download IRMAgent

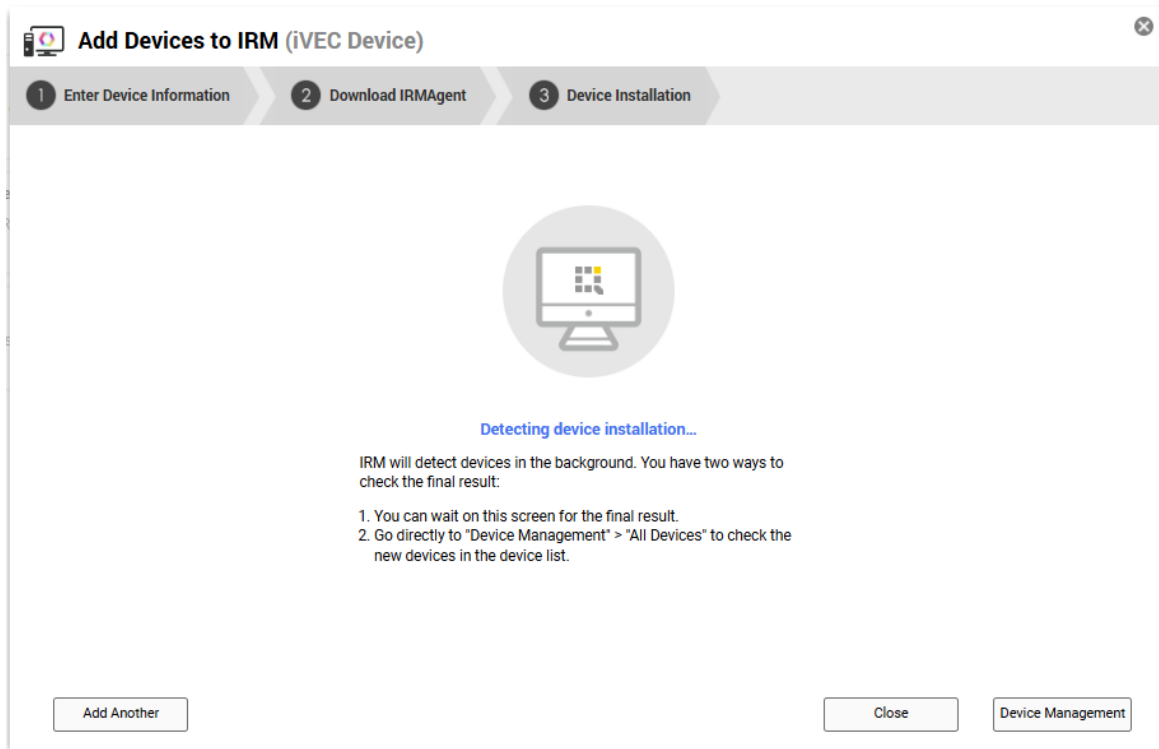
IRMAgent must be downloaded here and installed in the next step. If the process is not completed within 10 minutes in Step 3, it will time out.

Please refer to **Step 1 in Section 3.1.1.2, “Device Installation of Linux Devices,”** for installation instructions.

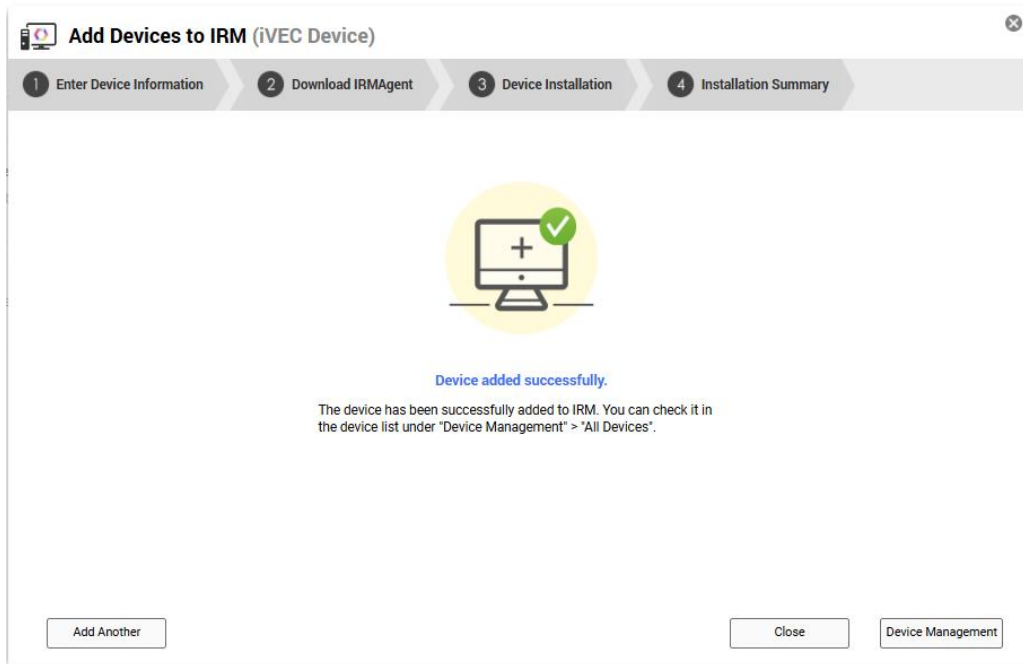


Step 3: Device Installation

Please refer to Step 2 in Section 4.1.1.2, "Device Installation of Linux Devices," for installation instructions.

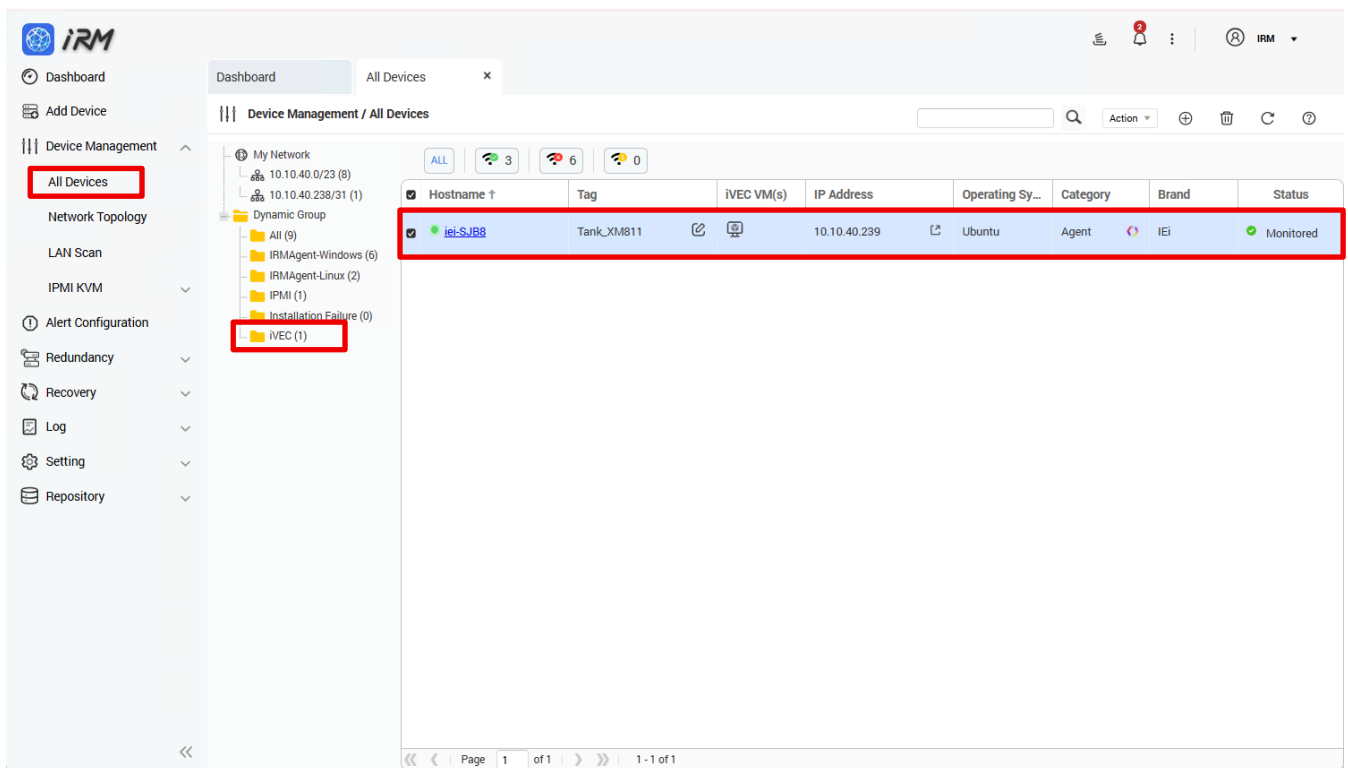


Step 4: Installation Summary



Step 5: iVEC Device added successfully

The device has been successfully added to IRM. You can check it in the device list under "Device Management" > "All Devices" or "iVEC".

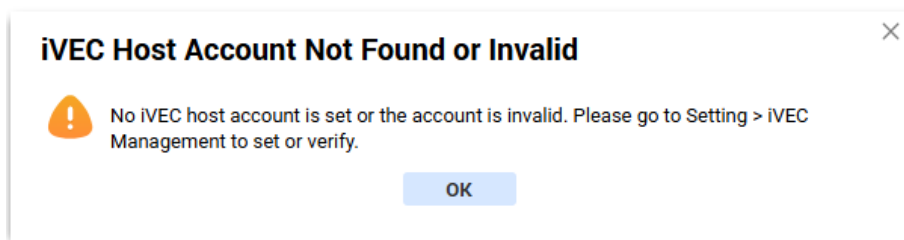


Step 6: iVEC VM List

The **iVEC VM List** provides a centralized view of virtual machines managed by the iVEC host. On this page, administrators can view basic VM information such as **power status**, **VM Name**, **Tag**, and **MAC Address**, and quickly open the VM management interface via the available entry points in the list.

Note: To use the iVEC VM List, go to **Settings > iVEC Management** to configure or verify the iVEC host account.

If no account has been configured or the account information is invalid, the system will display a prompt message:




Please refer to Section 10.5, “iVEC Management,” for setup instructions.

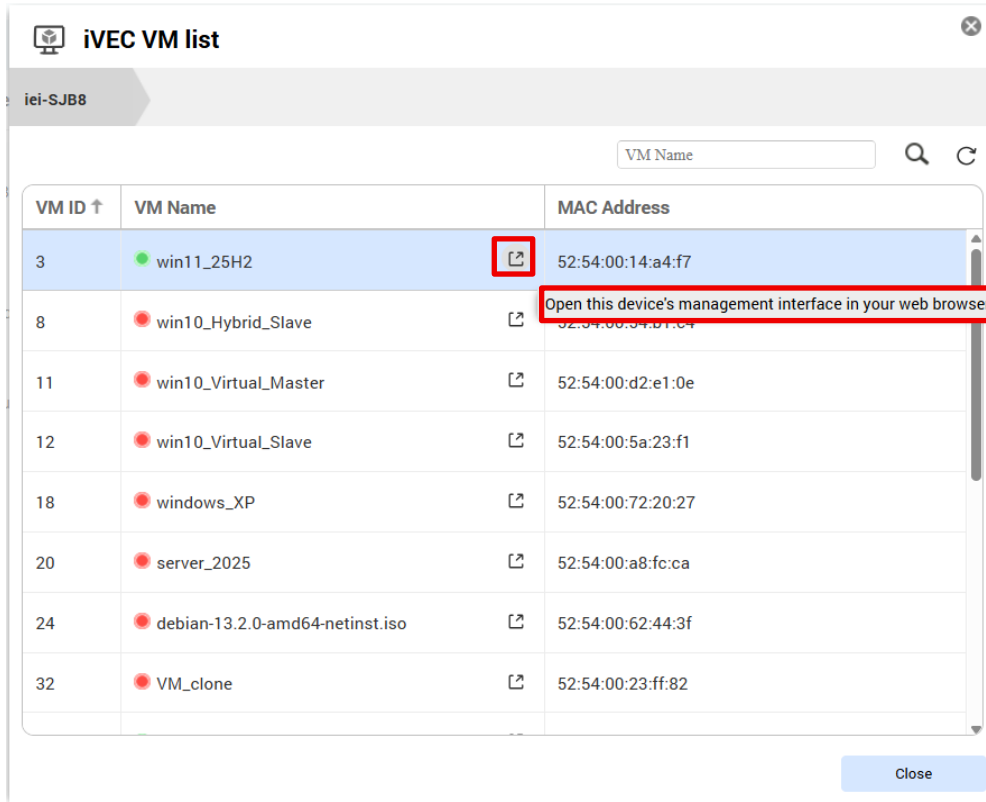



Steps:

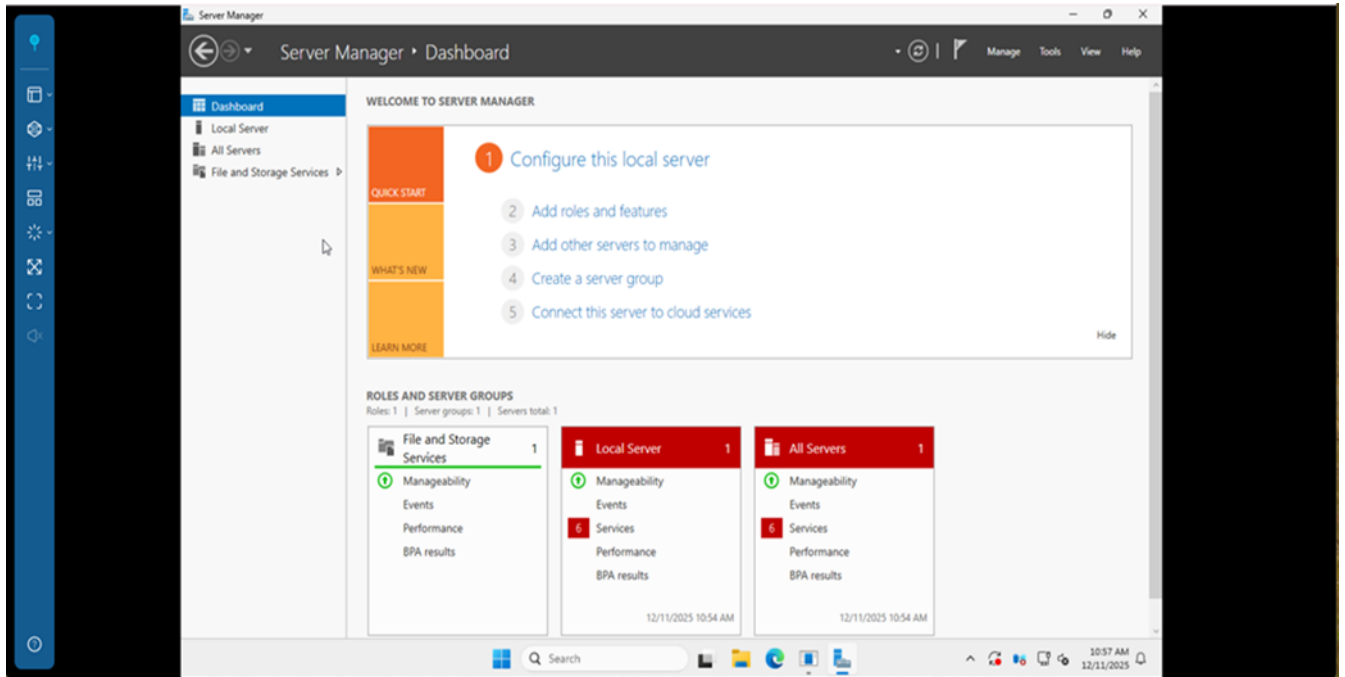
Click the **iVEC VM(s)** icon to open the **iVEC VM List** window. This window lists the VMs under the iVEC host, including **VM ID**, **VM Name**, and **MAC Address**.

To access the management interface for a specific VM, click the **external link** icon () on the right side of the VM (tooltip: “Open this device’s management interface in your web browser”). The system will open

the VM's **VM Console** in your web browser, allowing the administrator to log in and operate the VM.



Open this VM interface in your web browser: Click  icon, it go to VM Console.

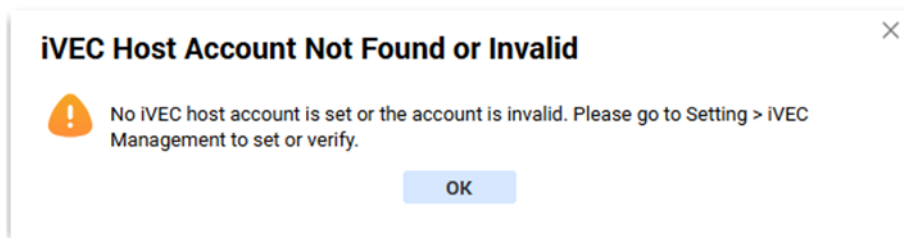


Step 7: iVEC management console.

The **iVEC Management Console** is the web-based management console of the iVEC host, providing a centralized entry point for VM management. From this entry point, users can log in directly to the iVEC Management Console and centrally manage and operate all VMs under the iVEC host.

Note: To use the iVEC Management Console, go to **Settings > iVEC Management** to configure or verify the iVEC host account.

If no account has been configured or the account information is invalid, the system will display a prompt message:



Hostname ↑	Tag	iVEC VM(s)	IP Address	Operating S...	Category	Brand	Status	
<input type="checkbox"/> iei-SJB8	Tank_XM811		10.10.40.239		Ubuntu	Agent	IEi	Monitored

Open this device's management interface in your web browser

Steps:

Open this device's management interface in your web browser: Click icon, it go to iVEC management console.

IEI VirtualizationEdgeComputer

[+ Create Virtual Machine](#)
🔍
📄
🔔
👤 iei

Overview

Virtual Machines (9)

- server_2025
- ubuntu-22.04.5-deskt...
- win10_Hybrid_Slave
- win10_Virtual_Master
- win10_Virtual_Slave
- win11_25H2

Data Protection

Images


Management

Preferences

Log

Overview

Virtual Machines (9)



Running: **3**

Suspended: **0**

Powered off: **6**

Status Change Logs (Recent 10 Activities)

Virtual Machines	Status	OS Version	Status Change Time
win11_25H2	Running	Microsoft Windo...	2025/12/11 09:55:10
win10_Virtual_Master	Running	Microsoft Windo...	2025/12/11 09:55:04
win10_Hybrid_Slave	Running	Microsoft Windo...	2025/12/11 09:55:01
VM	Powered off	Generic	2025/12/11 09:42:44
win10_Virtual_Slave	Powered off	Microsoft Windo...	2025/12/09 13:08:42
server_2025	Powered off	Microsoft Windo...	2025/12/02 09:47:11
ubuntu-22.04.5-deskto...	Powered off	Ubuntu 22.04 (Ja...	2025/11/28 16:15:51
debian-13.2.0-amd64-n...	Powered off	Generic	2025/11/27 17:51:11

CPU

Logical Cores: **24**

Allocated vCPUs: **12**

Top 5 VMs by CPU Utilization

Virtual Machines	Utilization (%)
win10_Virtual_Master	8.46%
win10_Hybrid_Slave	8.29%
win11_25H2	7.04%

Memory

Provisioned Memory: **27.0 GB**

Allocated Memory: **20 GB**

Top 5 VMs by Memory Utilization

Virtual Machines	Utilization (%)
win11_25H2	26.39%
win10_Virtual_Master	26.34%
win10_Hybrid_Slave	13.46%

Network

Received Data Rate (Top 5)

Virtual Machines	KB/s

Transmitted Data Rate (Top 5)

Virtual Machines	KB/s

Storage

Read Data Rate (Top 5)

Virtual Machines	KB/s

Write Data Rate (Top 5)

Virtual Machines	KB/s

Chapter

4

4 Device Management

4.1 All Devices

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. On the left is a navigation menu with 'All Devices' highlighted. The main area displays a tree view of network devices and a table of device details. The table has three columns: Hostname, Tag, and Status. Red callouts 1, 2, and 3 point to these columns respectively.

Hostname	Tag	Status
10.10.40.250	iRIS Device	Monitored
AFL3-W22-Panel-PC	Windows 11	Monitored
DRPC-140	Windows 10	Monitored
TANK-811	Windows 10	Monitored
iei-SJB8	Tank_XM811	Monitored
iei-Standard-PC-i440FX-PIIX-1996		Monitored
win10_Hybrid_Slave		Monitored
win10_Virtual_Master	Virtual_Redundancy_Master	Monitored
win10_Virtual_Slave	Virtual_Redundancy_Slave	Monitored

4.1.1 Host Name

The Host name not only distinguishes different devices through Dynamic Group, but also displays the current connection status with the IRM through different indicator light colors.

4.1.2 Tag

The Tag column displays device classification information to help users quickly identify device.

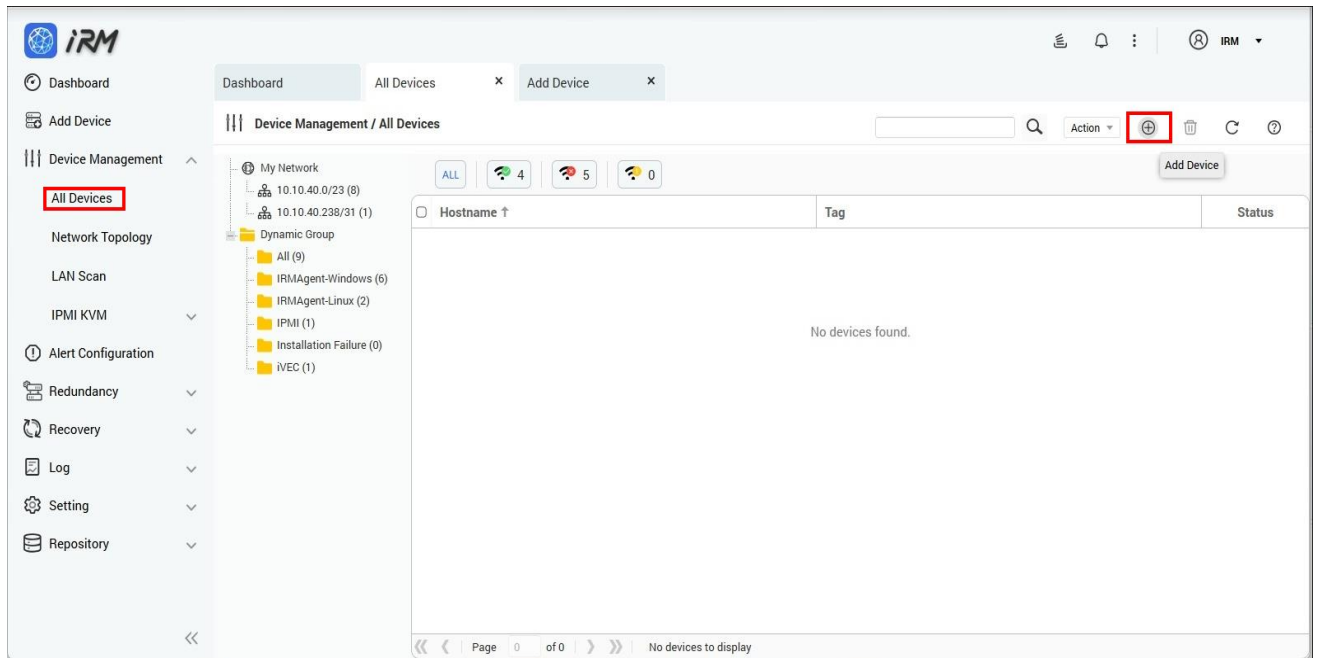
4.1.3 Status

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

4.1.4 Add Device

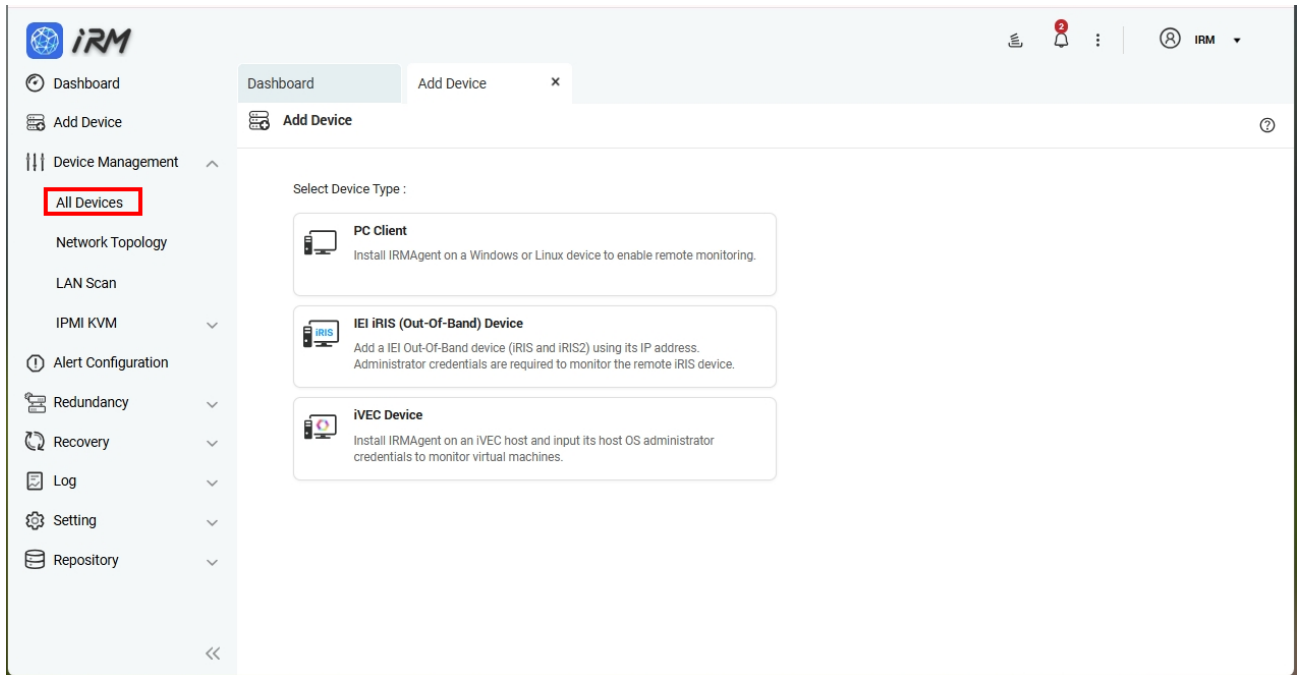
Users can add devices to IRM management via the Add Device feature. To add devices, follow the steps below:

Step 1: Click the "Add Device" button.



Step 2: IRM will redirect you to the Add Device Page.

Refer to [Section 3.1](#) 錯誤! 找不到參照來源。.



4.1.5 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.

4.1.6 Refresh

Refresh is used to update the device list and displayed information on the All Devices page. When device status changes (e.g., connection or monitoring status) or after adding/removing devices, users can click Refresh to retrieve the latest data.

4.1.7 Help

Click the Help (?) icon in the upper right corner of the All Devices page. The system will automatically open the online user manual and redirect you to the corresponding instruction page to help you quickly understand how to use the functions.

4.1.8 Search

The Search field at the top-right of the All-Devices page allows users to quickly filter the device list by keywords. Supported search keys include Hostname, IP address, and Device tag.

(Placeholder: Hostname, IP address, Device tag)

4.1.9 Action

The Action dropdown (top-right of All Devices) provides operations for the selected device(s). Select one or more devices in the list, then choose an operation from Action. Available actions may vary depending on device type, current status, and user permissions.

4.1.9.1 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.

- **Power Off** : Shuts down the selected device.
- **Restart** : Restarts the selected device.

4.1.9.2 Remote Access:

Provides remote access entry points for the selected device(s) (options depend on device capability and system configuration).

- **RDP**: Connect to a Windows device via Remote Desktop (requires device support/enabled).
- **VNC**: Connect via VNC (requires device support/enabled).
- **SSH**: Connect to a Linux device via SSH (requires device support/enabled).

Note: If an option is grayed out, it indicates the device does not support it or it is not enabled.

4.1.9.3 Export as PDF:

Exports the selected devices/list information as a PDF for archiving and sharing.

4.1.9.4 Email as PDF:

Sends the PDF report via email (SMTP/notification settings are required).

NOTE:

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

Step 1: Log in to IRM Server Management Console and open "Network & Virtual Switch".

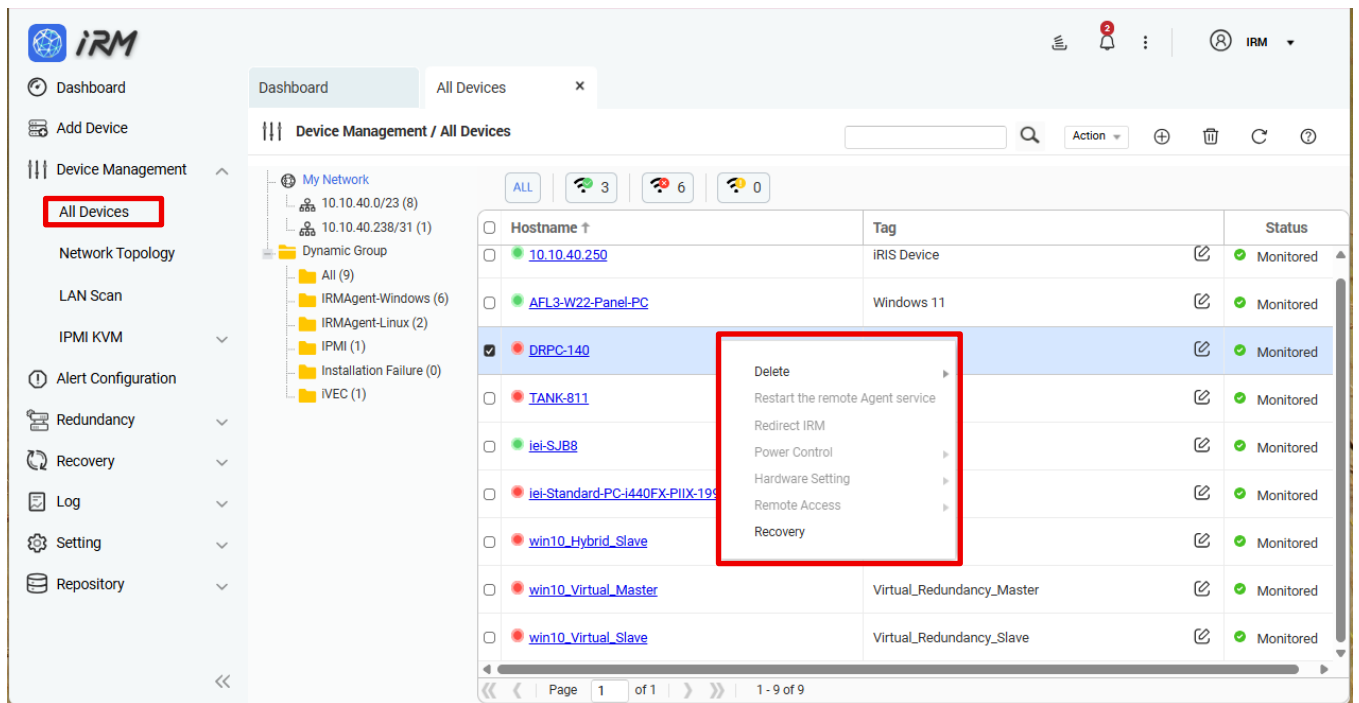
Step 2: Check the network ports that can reach the Internet.

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

4.1.10 Quick Menu

On the Device Management page, users can select a target host in the device list and right-click to open the quick menu.

The context menu provides multiple actions, including Delete, Restart Remote Agent Service, Redirect to IRM, Power Control, Hardware Settings, Remote Login Control, and Recovery.



4.1.10.1 Delete

User can use the quick menu to delete any device and remove it from management, or delete the remote Agent and remove the device from management.

4.1.10.2 Restart the remote Agent service

Users can use the quick menu to restart the remote Agent service (**Linux devices only**).

4.1.10.3 Redirect

Users can use the quick menu to redirect to IRM (**Linux devices only**).

Redirect IRM

Username *
IRM

Password *
.....

IP Address FQDN

IP Address *
10 10 40 80

Transport Protocol *
http

Port Number *
8080

OK

1. Username*: Enter the IRM username for redirection.
2. Password*: Enter the password for the IRM username.
3. IP Address or FQDN*: Enter the target IRM IP address or FQDN.
4. Transport Protocol*: The default protocol is HTTP. You can select HTTPS if needed.
5. Port Number*: Enter the port number (HTTP: 8080, HTTPS: 443).

After verifying the information, click Confirm. The device will be redirected to the specified IRM host and added for management.

4.1.10.4 Power Control

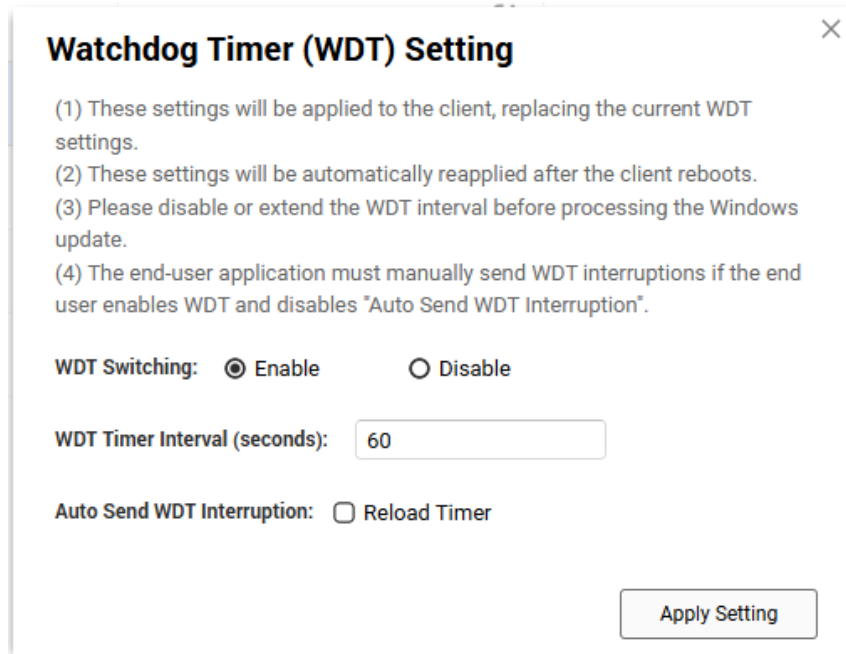
Users can use the quick menu to power off or reboot any device.

4.1.10.5 Hardware Setting (Watchdog Timer)

Hardware Setting (Watchdog Timer) is used to configure the device Watchdog Timer. A watchdog timer is a hardware/system protection mechanism that can automatically trigger a recovery action (such as a reboot)

when the system becomes abnormal or unresponsive, improving device stability and availability. user can configure watchdog-related parameters here and apply them to target devices.

Note: Watchdog Timer (Physical Windows devices only), Users can configure it through the quickt menu.



WDT Switch:

- **Enable:** Enables the Watchdog Timer. Enable it only when you need to test system stability or prevent the system from hanging without automatically rebooting.
- **Disable:** Disables the Watchdog Timer. For general testing or while performing OS/driver installation or updates, it is recommended to temporarily disable it.

WDT Timer Interval (seconds): In WDT Timer Interval (seconds), enter the time value. The range 0 ~ xx specifies the allowed watchdog timeout period. If no “reload timer” signal is received within the specified seconds, the Watchdog will determine that the system is unresponsive and trigger the default action (usually a reboot). Click Apply Settings to start the countdown.

Auto Send WDT Interruption: Automatically sends WDT interrupts.

Enable: Select **Reload Timer**. The Agent will periodically send WDT signals to automatically reload the timer.

Disable: Clear Reload Timer. The Agent will not send WDT signals automatically. In this case, your application must send WDT interruptions periodically; otherwise, the WDT will reboot the system when the timer expires.

4.1.10.6 Remote Access

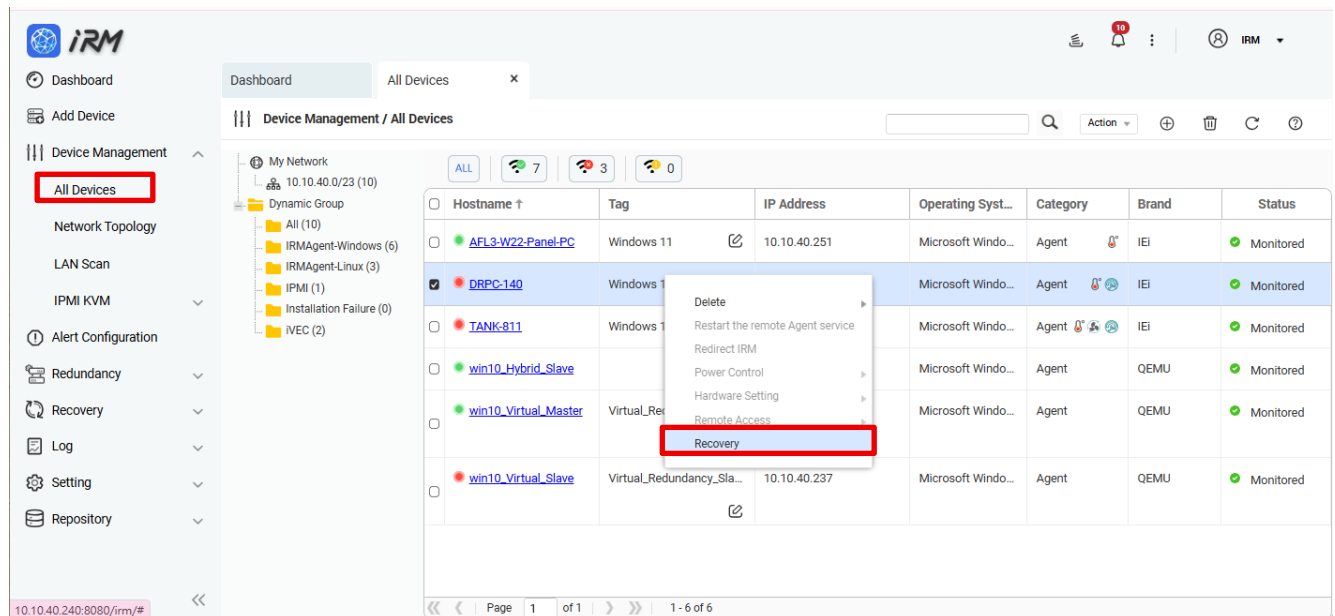
Users can use the quick menu to remotely access Windows devices (supports RDP and VNC) and Linux devices (supports VNC and SSH).

Note: VNC software must be installed separately.

4.1.10.7 Recovery

IRM supports recovery for IEI physical hosts. The host to be recovered must have **OKR2** installed in advance.

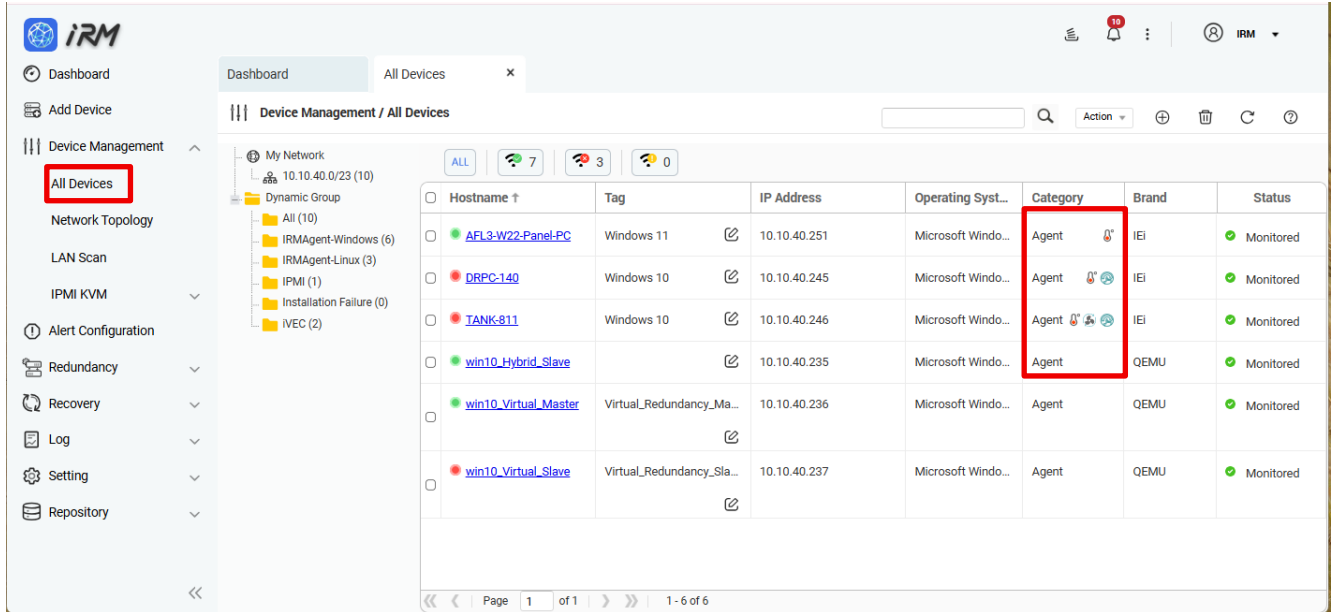
Please refer to **Section 8.1, “Remote Recovery,”** for installation instructions.



4.1.11 IEI System Monitoring Module

The IEI Intelligent System Management Module (iSMM) is a system health supervision application which utilizes sensor chips on IEI motherboards to track CPU and system temperatures, fan speed, watchdog timer, digital I/O status and system event.

Users can add gadgets to the dashboard to continuously monitor the health of the H/W device.



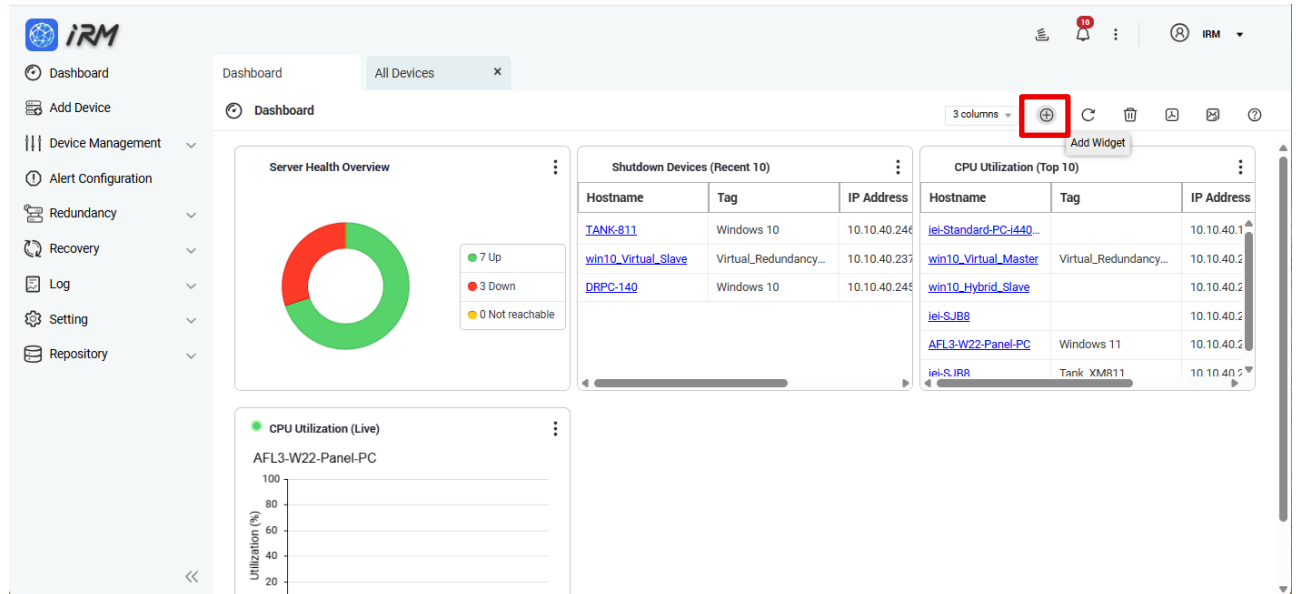
Go to Sensor ICO

Go to Device Management > All Devices > Dynamic Group > IRMAgent-Windows.

Icon	Module Name	Description	H/W Monitoring	Notes
	Temperature Sensor	Indicates that this IEI physical host supports hardware temperature sensor monitoring by IRM. The actual available items vary by model, but CPU Temp and SYS Temp are common items.	<ul style="list-style-type: none"> - CPU temperature - System temperature - Power temperature 	only support IEI PCs for Windows system
	Fan Speed Monitoring	Indicates that this IEI physical host supports fan speed monitoring by IRM, which can be used to observe cooling performance and verify whether the fans are operating properly.	<ul style="list-style-type: none"> - CPU Fan - Sys Fan 	only support IEI PCs for Windows system
	OKR2 Remote Recovery	Indicates that OKR2 has been installed and enabled on this IEI physical host. Remote recovery can be performed via IRM → Remote Recovery.	<ul style="list-style-type: none"> - OKR2 installed and enabled on the host 	only support IEI PCs for Windows system

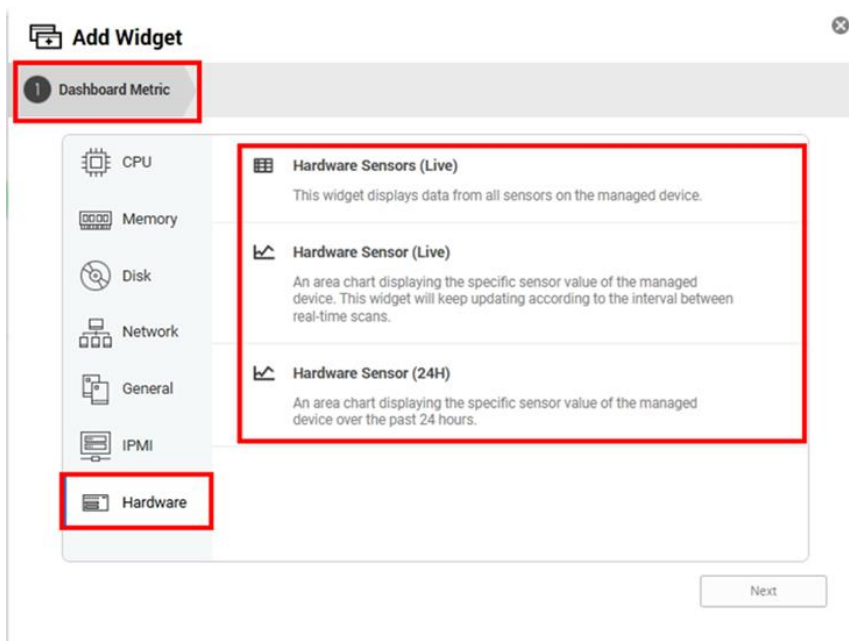
4.1.11.1 Hardware Sensor Add Widget

Go to the Dashboard page and click the "Add Widget" button.



4.1.11.2 Dashboard Metric

After adding the widget, you can use Dashboard Metrics to configure which hardware sensor metrics to display on the dashboard. In the Dashboard Metrics window, click Hardware on the left side.



4.1.11.3 Hardware Sensors (Live)

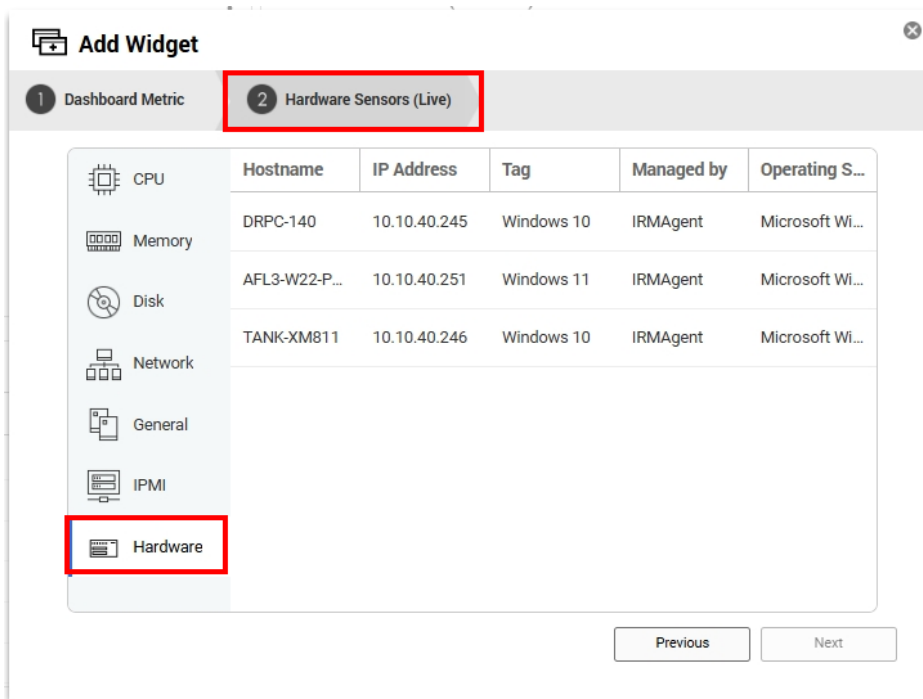
Step 1: In the **Add Widget** window, after selecting the **Hardware** category, you can choose one of the following three **H/W Sensor** widgets as needed: :

- **Hardware Sensors (Live):** Displays real-time values of all supported hardware sensors on the managed device in a table view. By default, all supported sensors and the layout are preloaded, and users cannot customize which sensors (information) are displayed.
- **Hardware Sensor (Live):** Displays the real-time value of a single hardware sensor in an area chart and updates automatically based on the scan interval.
Users must customize the sensor (information) to be displayed and the layout.
- **Hardware Sensor (24H):** Displays the historical trend of a single hardware sensor over the past 24 hours in an area chart. Users must customize the sensor (information) to be displayed and the layout.

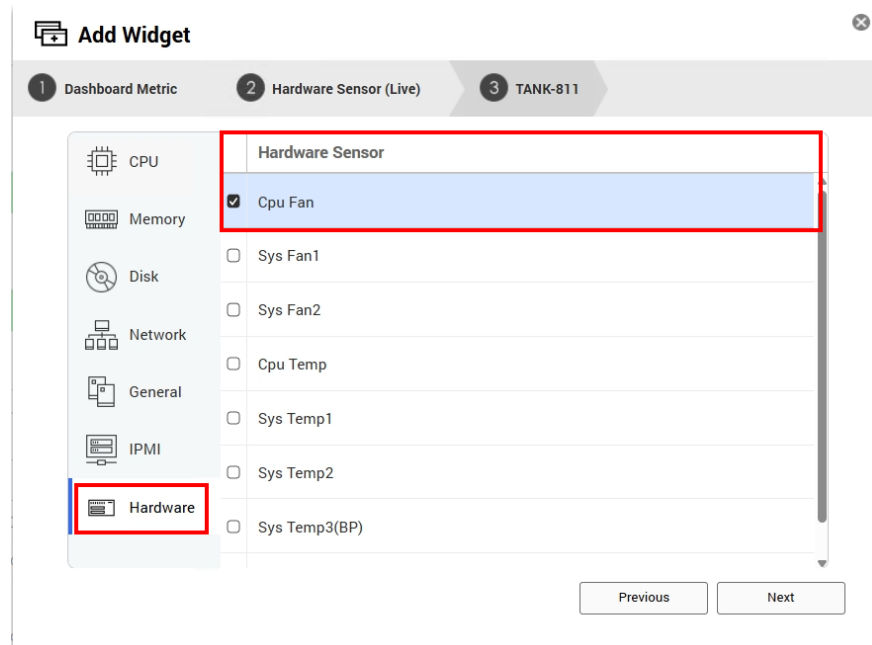
Note 1:

The hardware sensors supported by **Hardware Sensor** may vary across different IEI IPC models. However, the **CPU Temp** and **SYS Temp** sensors are common to all supported models. These sensors are available **only on IEI physical IPC hosts; virtual machines (VMs) do not support hardware sensor display.**

The system lists IEI physical hosts that support iSMM. Select the host you want to monitor, and then click Next.

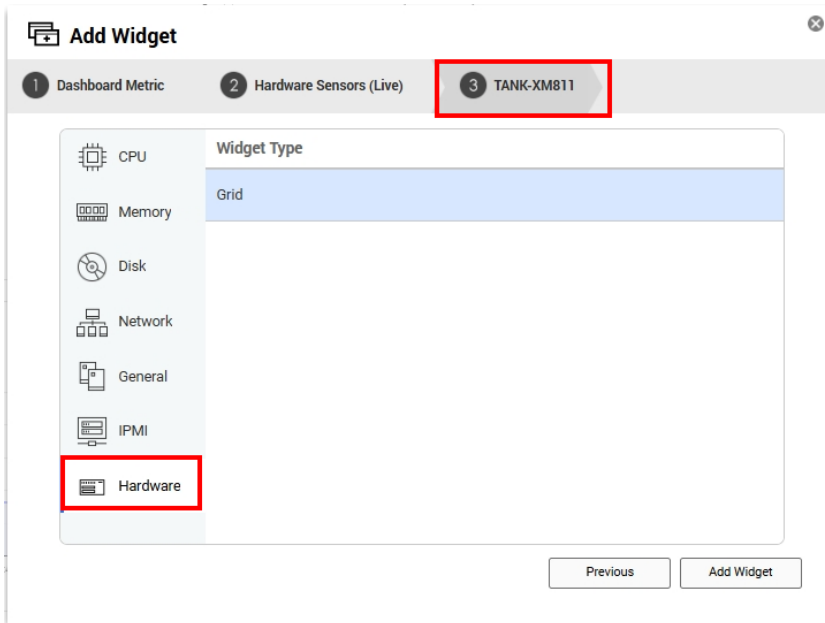


4.1.11.4 IPC Hardware Sensors (specific sensor)



1. After entering the Hardware Sensor list, the system automatically displays all hardware sensors reported by iSMM for the selected host.
2. Select a single sensor item to monitor from the list, for example, "CPU Fan".
3. After confirming your selection, click Next to continue with the layout configuration and complete the addition.

4.1.11.5 Widget Type

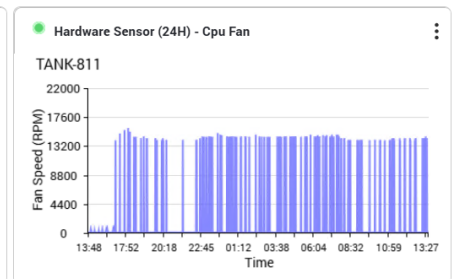
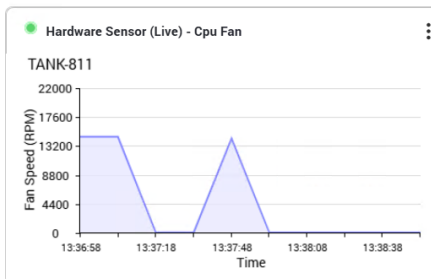


After selecting the type of chart, click the "Add Widget" button to complete the operation.

This section describes the available widget types for iSMM.

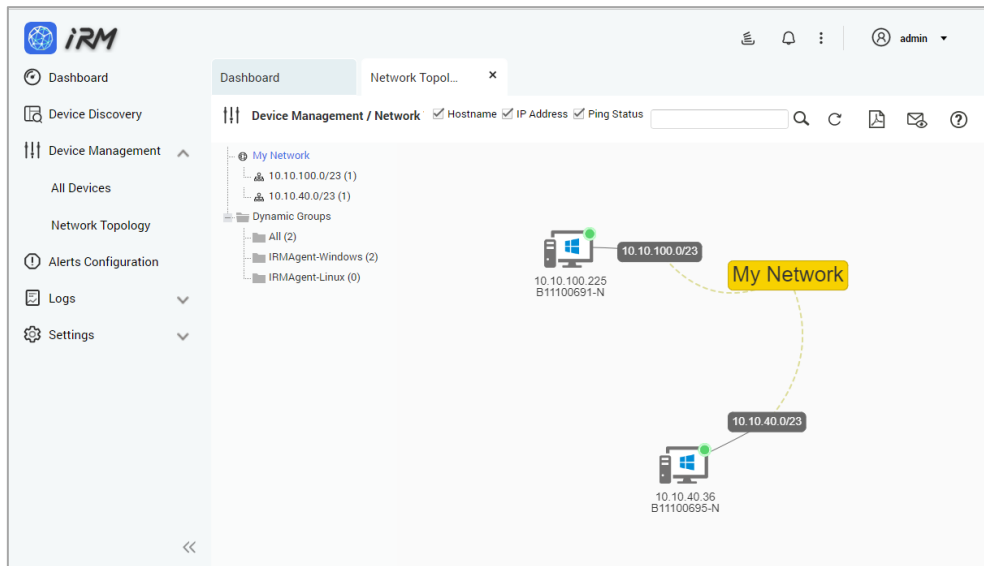
Type	Description	Scenario	Limitation
Hardware Sensors (Live) – Table	Displays real-time values and status of all supported hardware sensors on the device in a table.	Routine inspection of multiple sensors (CPU/system temperature, fans, voltage, etc.).	No trend chart and no historical data
Hardware Sensor (Live) – Single-line Area Chart	Plots a real-time trend chart for a single sensor.	Observing short-term fluctuations of a single sensor and early warning signs before an alert.	Supports only one sensor at a time
Hardware Sensor (Last 24 Hours) – Single-line Area Chart	Displays the historical trend of a single sensor over the past 24 hours.	Reviewing daily peaks/lows, offline periods, and cooling effectiveness.	Single sensor only; the time window is fixed at 24 hours.

Sensor Name	Value
Cpu Fan	0 RPM
Sys Fan1	0 RPM
Sys Fan2	0 RPM
Cpu Temp	0 °C
Sys Temp1	52 °C
Sys Temp2	53 °C



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.

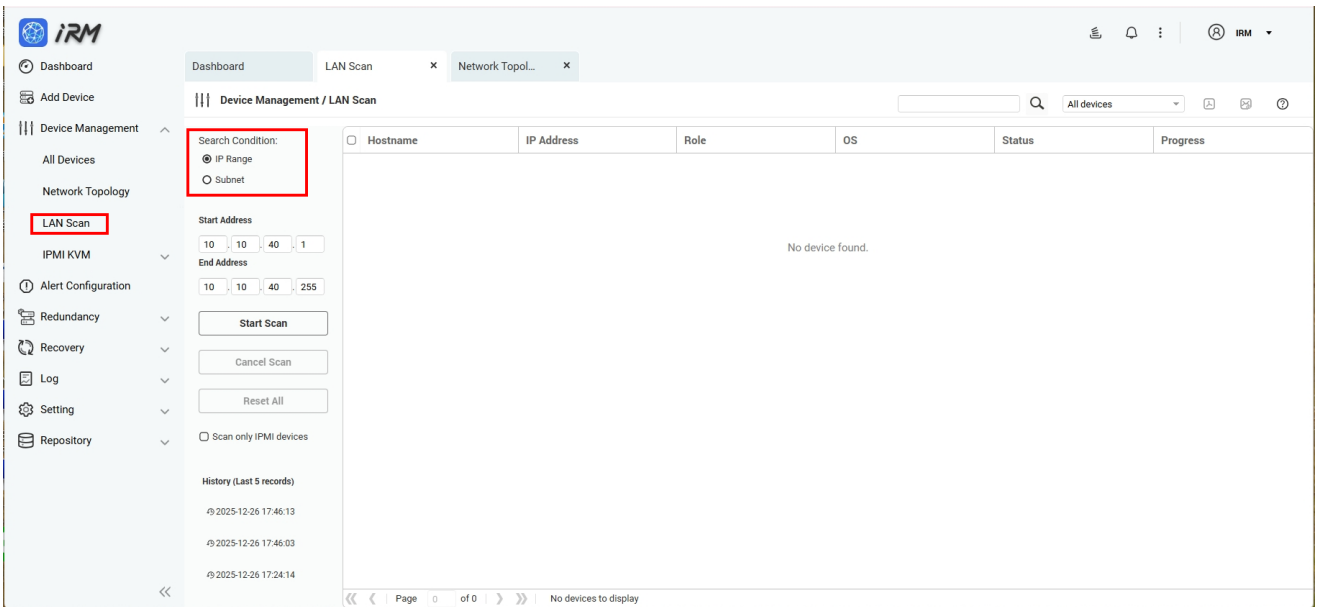


1. My network shows different subnet groups
2. Dynamic Groups will automatically sub-group according to subnet, operating system and other information
3. Device Name
4. IP address of the device
5. Current status of the managed device (Power On, Power Down, or network outage)
6. Device Discovery

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

IRM supports the following two search types:

1. IP range
2. Subnet

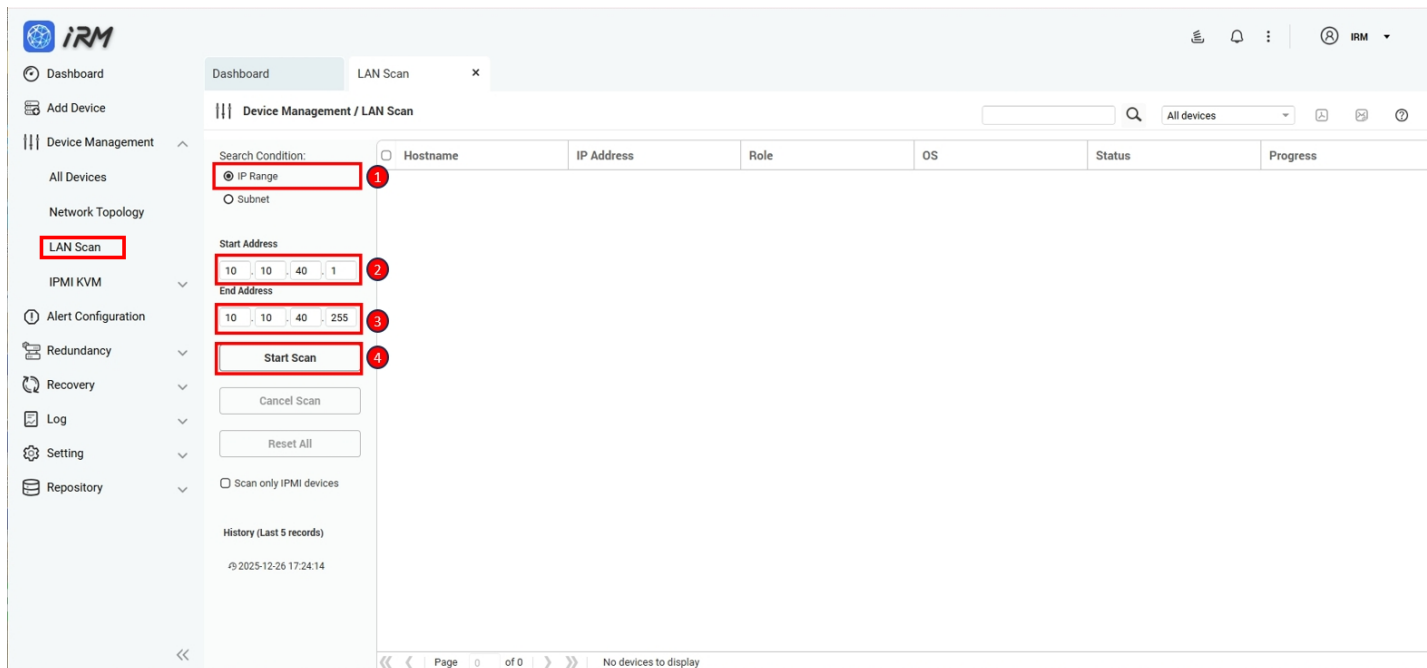


4.2.1 Start Scan

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.

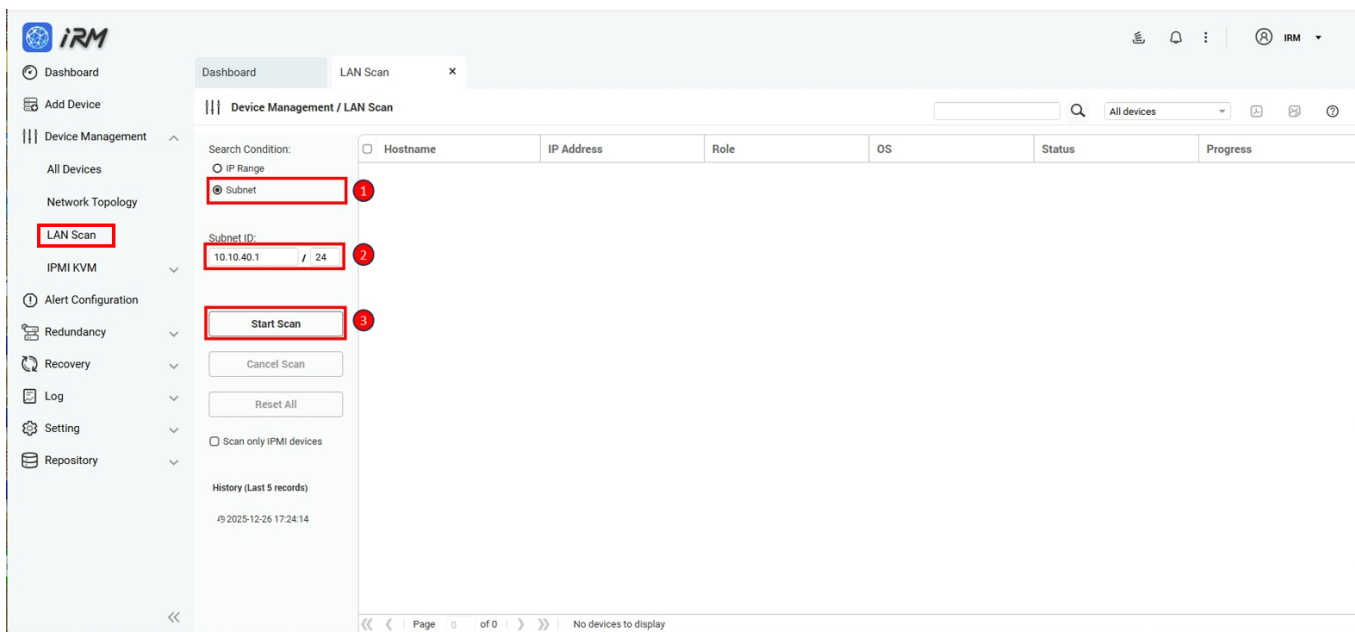
To scan a specific IP range, follow the steps below:

- 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".



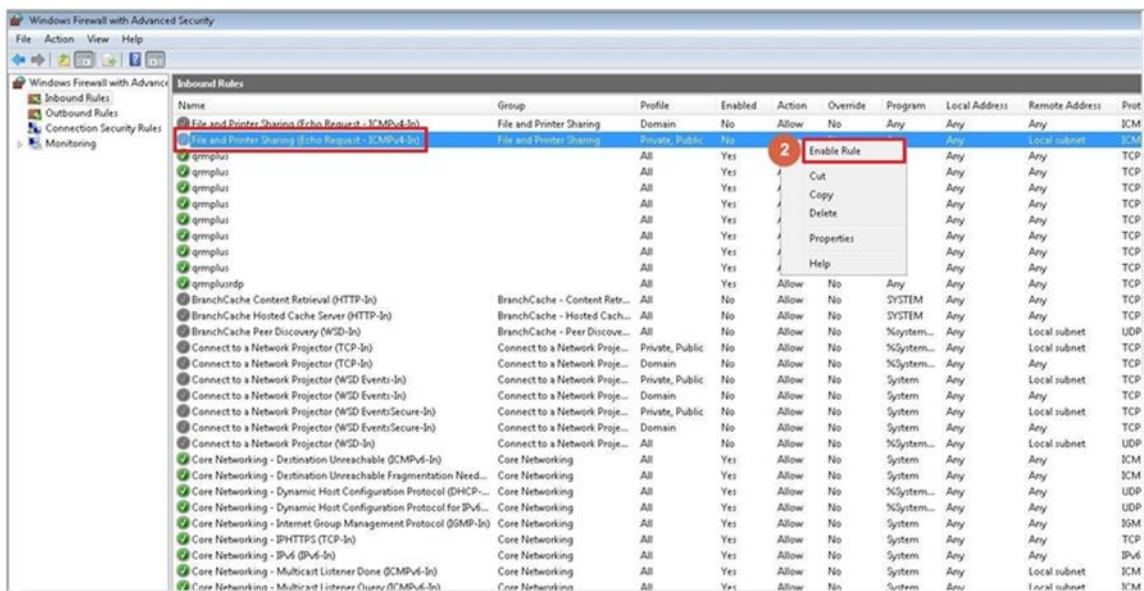
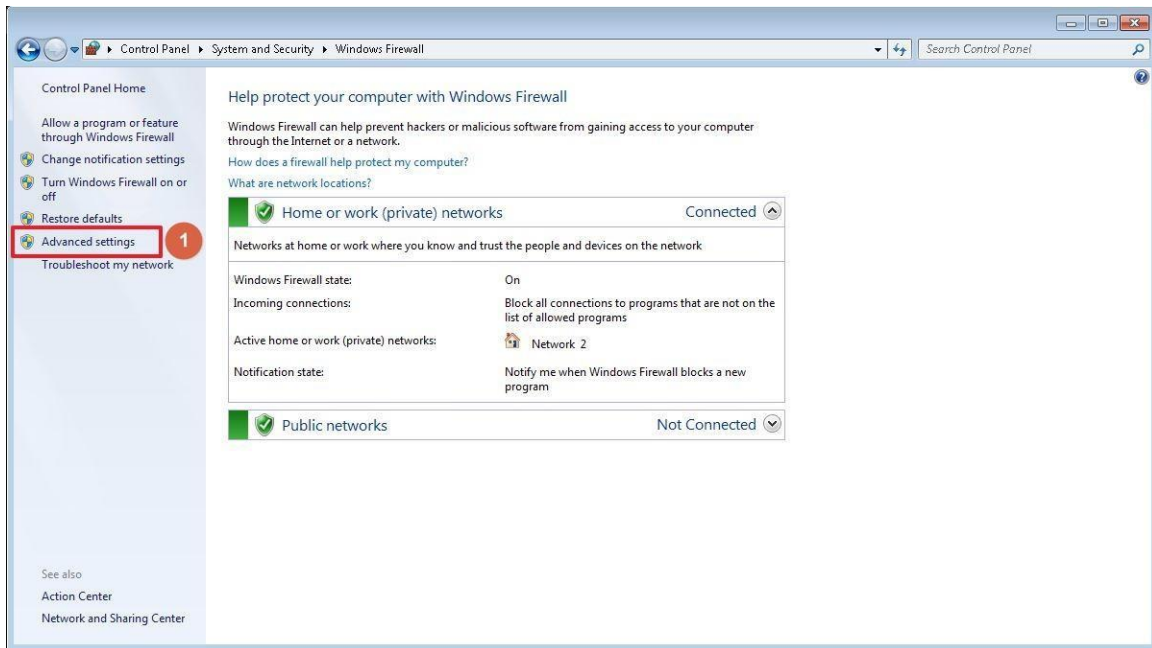
To scan a specific subnet range, follow the steps below:

- Step 1:** Set the subnet.
- Step 2:** Enter the CIDR, default is 24.
- Step 3:** Click "Start Scan".

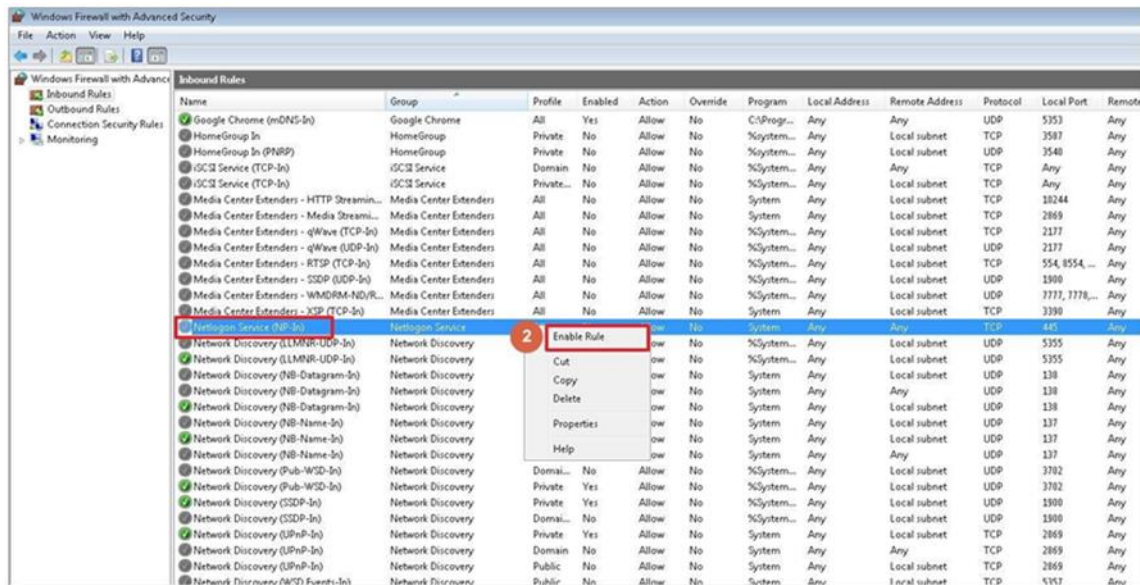
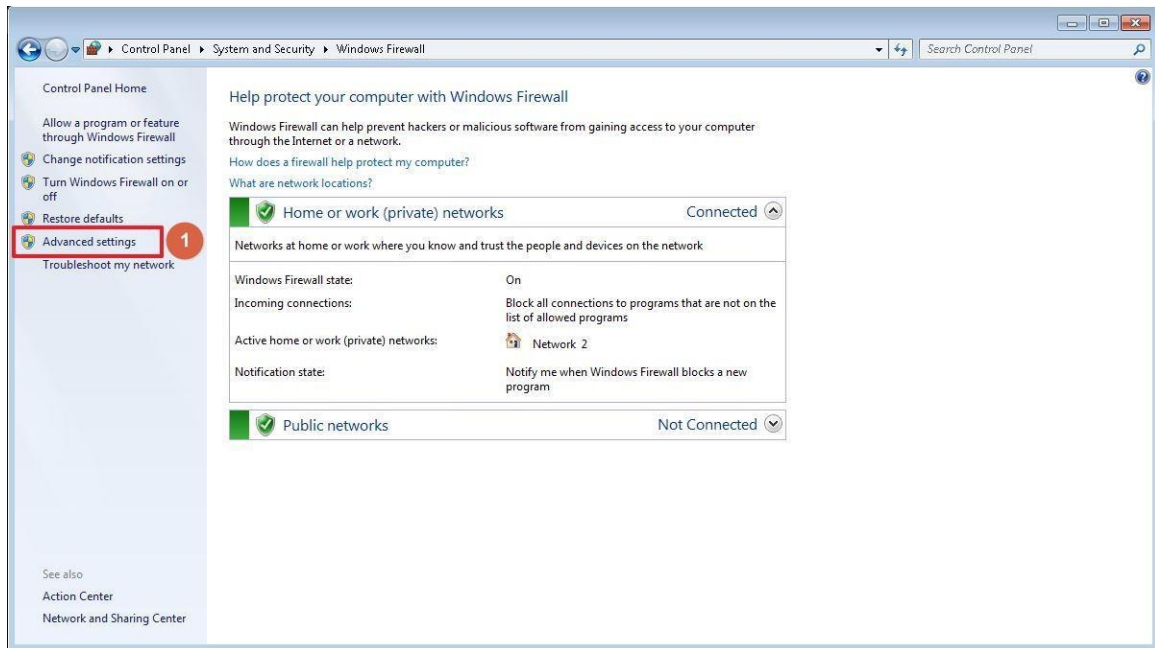


NOTE: IRM uses ICMP protocol to search for devices within a specified IP address range. If the target device does not allow ICMP requests, IRM will not be able to find the target device. To support IRM search,

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).



4.2.2 Stop Scanning

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

The screenshot shows the iRM LAN Scan interface. On the left sidebar, 'LAN Scan' is highlighted. The main area shows a table of devices being scanned. The 'Cancel Scan' button is highlighted with a red box. The table has the following data:

Search Condition:	Hostname	IP Address	Role	OS	Status	Progress
<input type="radio"/> IP Range	B11400323-P	10.10.40.18			Scanning...	
<input checked="" type="radio"/> Subnet	B10801307-N	10.10.40.24			Scanning...	
Subnet ID: 10.10.40.1 / 24	CLW-NAS	10.10.40.26			Scanning...	
<input type="button" value="Start Scan"/>	IRM410E	10.10.40.34			Scanning...	
<input type="button" value="Cancel Scan"/>	B11301366-P	10.10.40.39			Scanning...	
<input type="button" value="Reset All"/>	DELL-LATITUDE-7	10.10.40.59			Scanning...	
<input type="checkbox"/> Scan only IPMI devices	B11400027-N	10.10.40.62			Scanning...	
Scanning (2%)	IRM-TSI-410X	10.10.40.80			Scanning...	
Searching...	B10800116-P	10.10.40.84			Scanning...	
History (Last 5 records)	A1112038-P	10.10.40.86			Scanning...	
2025-12-26 17:46:03	ANDY-NAS	10.10.40.91			Scanning...	
2025-12-26 17:24:14	DESKTOP-DQE63SQ	10.10.40.97			Scanning...	

4.2.3 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 LAN Scan interface after a scan has been canceled. The 'Reset All' button is highlighted with a red box. The table has the following data:

Search Condition:	Hostname	IP Address	Role	OS	Status	Progress
<input type="radio"/> IP Range	B11400323-P	10.10.40.18			Canceled	
<input checked="" type="radio"/> Subnet	B10801307-N	10.10.40.24			Canceled	
Subnet ID: 10.10.40.1 / 24	CLW-NAS	10.10.40.26			Canceled	
<input type="button" value="Start Scan"/>	IRM410E	10.10.40.34			Canceled	
<input type="button" value="Cancel Scan"/>	B11301366-P	10.10.40.39			Canceled	
<input type="button" value="Reset All"/>	DELL-LATITUDE-7	10.10.40.59			Canceled	
<input type="checkbox"/> Scan only IPMI devices	B11400027-N	10.10.40.62			Canceled	
History (Last 5 records)	IRM-TSI-410X	10.10.40.80			Canceled	
2025-12-26 17:46:13	B10800116-P	10.10.40.84			Canceled	
2025-12-26 17:46:03	A1112038-P	10.10.40.86			Canceled	
2025-12-26 17:24:14	ANDY-NAS	10.10.40.91			Canceled	
	DESKTOP-DQE63SQ	10.10.40.97			Canceled	

4.2.4 Scan History

IRM maintains a scan history. Users can view the last 5 scans in the history pane of the left column.

The screenshot shows the IRM web interface for LAN Scan. The left sidebar contains a navigation menu with 'LAN Scan' highlighted. The main area displays a table of scanned devices with columns for Hostname, IP Address, Role, OS, Status, and Progress. A history pane on the left shows the last 5 scan records.

Hostname	IP Address	Role	OS	Status	Progress
10.10.40.230	10.10.40.230	Device	Linux	New Device	Completed
IRM-TSI-410X	10.10.40.231	NAS	QTS	New Device	Completed
PPC2-CW22-EHL	10.10.40.232	Device	Unknown	New Device	Completed
10.10.40.235	10.10.40.235	Device	Microsoft Windows 10 專業版	Already Added	Completed
10.10.40.239	10.10.40.239	Device	Ubuntu	Already Added	Completed
TS-1410X-DEMO	10.10.40.240	NAS	QTS	New Device	Completed
10.10.40.241	10.10.40.241	Device	Linux	New Device	Completed
IRM-I410XSL	10.10.40.242	NAS	QTS	New Device	Completed
10.10.40.244	10.10.40.244	Device	Linux	New Device	Completed
10.10.40.245	10.10.40.245	Device	Microsoft Windows 10 Pro	Already Added	Completed
10.10.40.250	10.10.40.250	Device	IPMI Management System	Already Added	Completed
10.10.40.251	10.10.40.251	Device	Microsoft Windows 11 Pro	Already Added	Completed
10.10.40.252	10.10.40.252	Device	Unknown	New Device	Completed

History (Last 5 records):

- 2025-12-29 16:53:34
- 2025-12-29 14:27:54
- 2025-12-29 14:27:00
- 2025-12-29 14:25:48

4.4 IPMI KVM

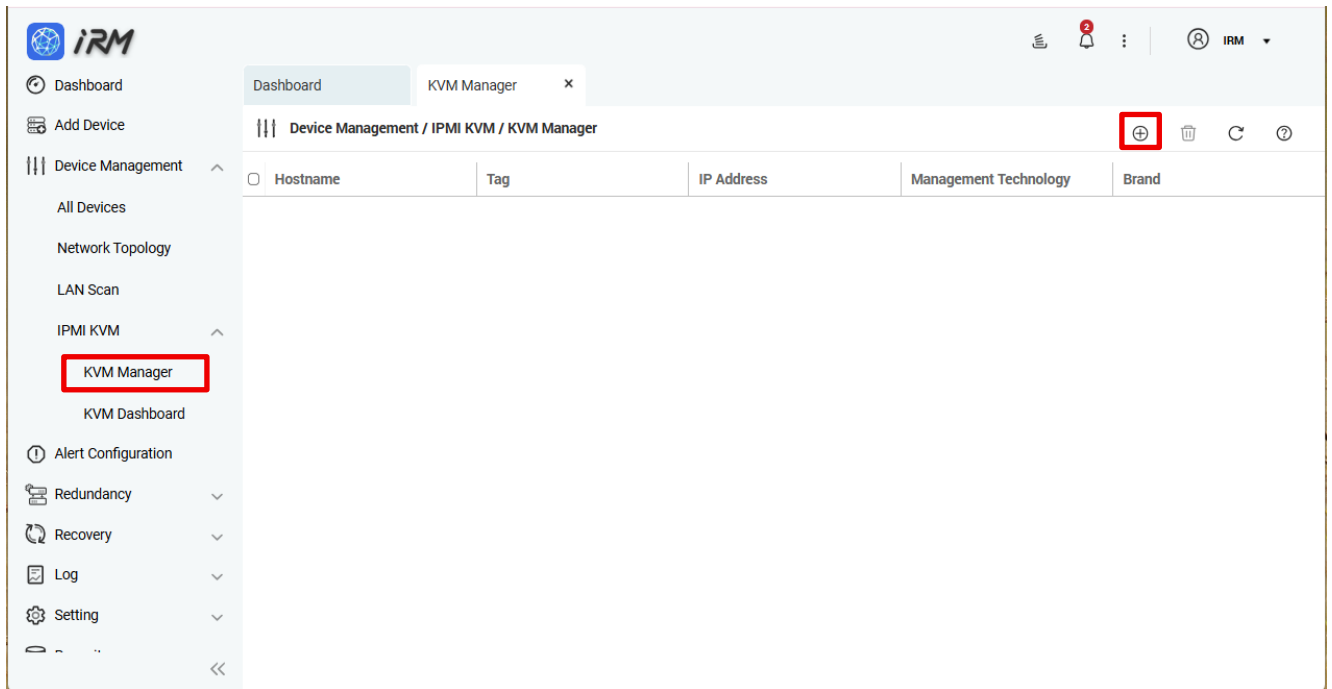
IPMI KVM allows administrators to centrally manage devices that support IPMI (iRIS) in IRM and view the remote host's screen through a web browser. Even if the operating system is unresponsive and RDP/VNC/SSH cannot be used, administrators can still perform basic viewing and maintenance operations via IPMI KVM, improving remote maintenance efficiency.

4.4.1 KVM Manager

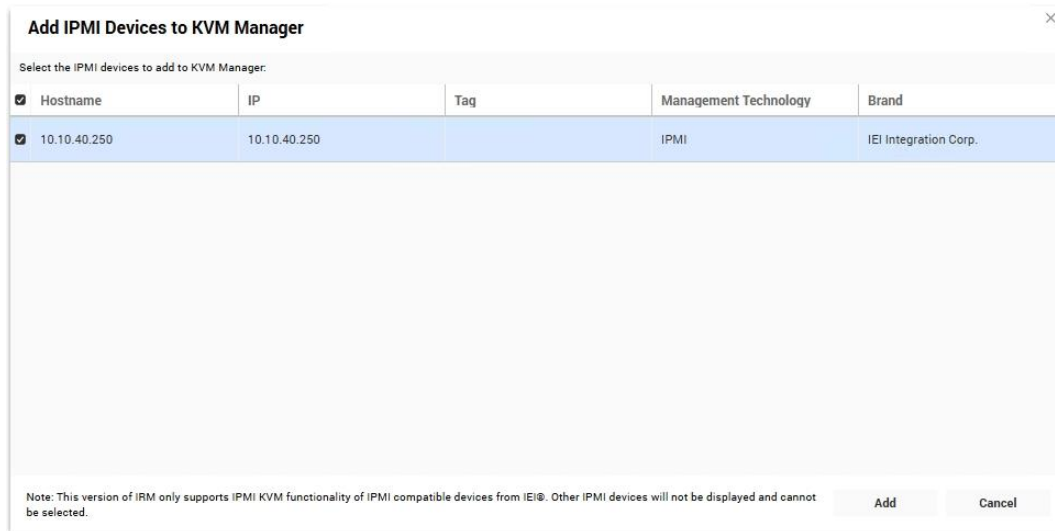
The KVM Manager is used to centrally manage the list of devices that can be accessed via IPMI KVM. On this page, administrators can add/remove IPMI (iRIS) devices and view basic device information (such as hostname, IP address, tag, management method, and brand), so they can later monitor devices as thumbnails in the KVM Dashboard and launch remote KVM connections.

4.4.1.1 Add an IPMI device to the KVM Manager

Step 1: Go to the KVM Manager page and click the "Add Device" button.



Step 2: The system displays the “Add IPMI Device to Manager” window. To add an IPMI device to the KVM Manager, select the IPMI device you want to add, confirm the selection, and then click Add.



4.4.1.2 Remove IPMI Device

Go to the KVM Manager page and click the "Remove Device" button.

The screenshot shows the iRM KVM Manager interface. On the left is a navigation menu with 'KVM Manager' highlighted. The main area displays a table of devices under the heading 'Device Management / IPMI KVM / KVM Manager'. A trash icon in the top right of the table area is highlighted with a red box.

Hostname	Tag	IP Address	Management Technology	Brand
10.10.40.250	IRIS Device	10.10.40.250	IPMI	IEI Integration Corp.

This screenshot shows the same iRM KVM Manager interface as above, but with a confirmation dialog box overlaid in the center. The dialog box is titled 'KVM Manager' and asks 'Are you sure you want to remove the selected device(s) from KVM manager?'. It has 'Yes' and 'No' buttons. The 'KVM Manager' menu item in the left sidebar is also highlighted with a red box.

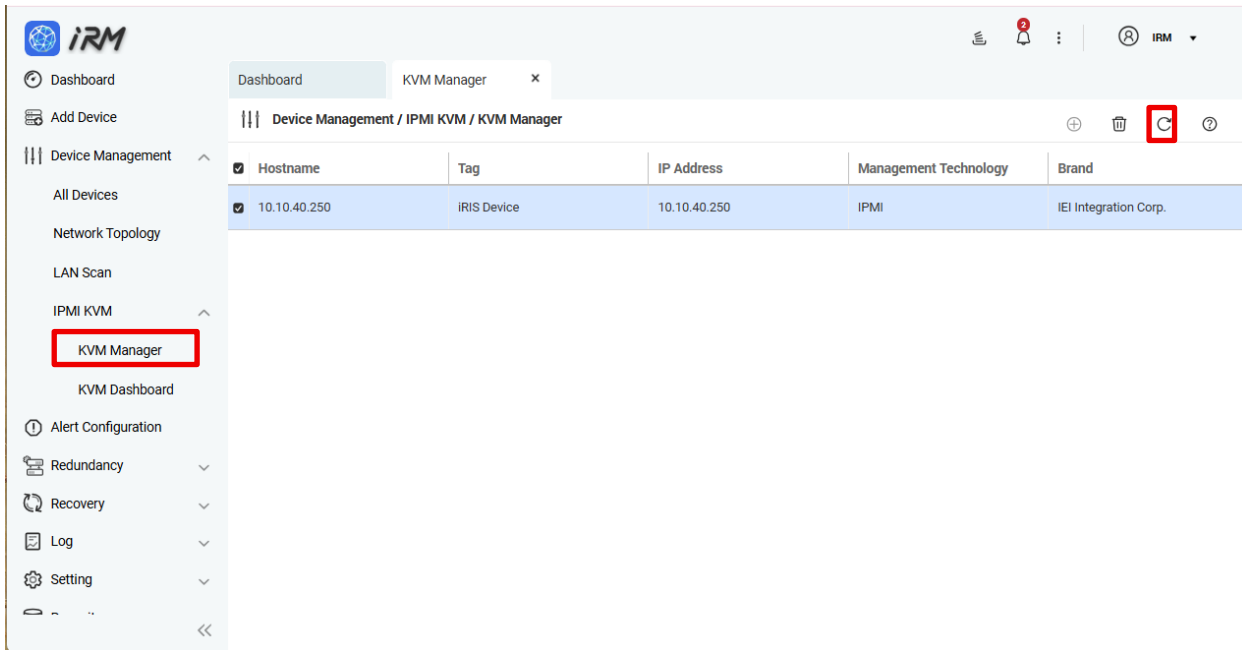
KVM Manager

Are you sure you want to remove the selected device(s) from KVM manager?

Yes No

4.4.1.3 更新 IPMI 裝置

Step 1: Go to the KVM Manager page and click the "Refresh" button.

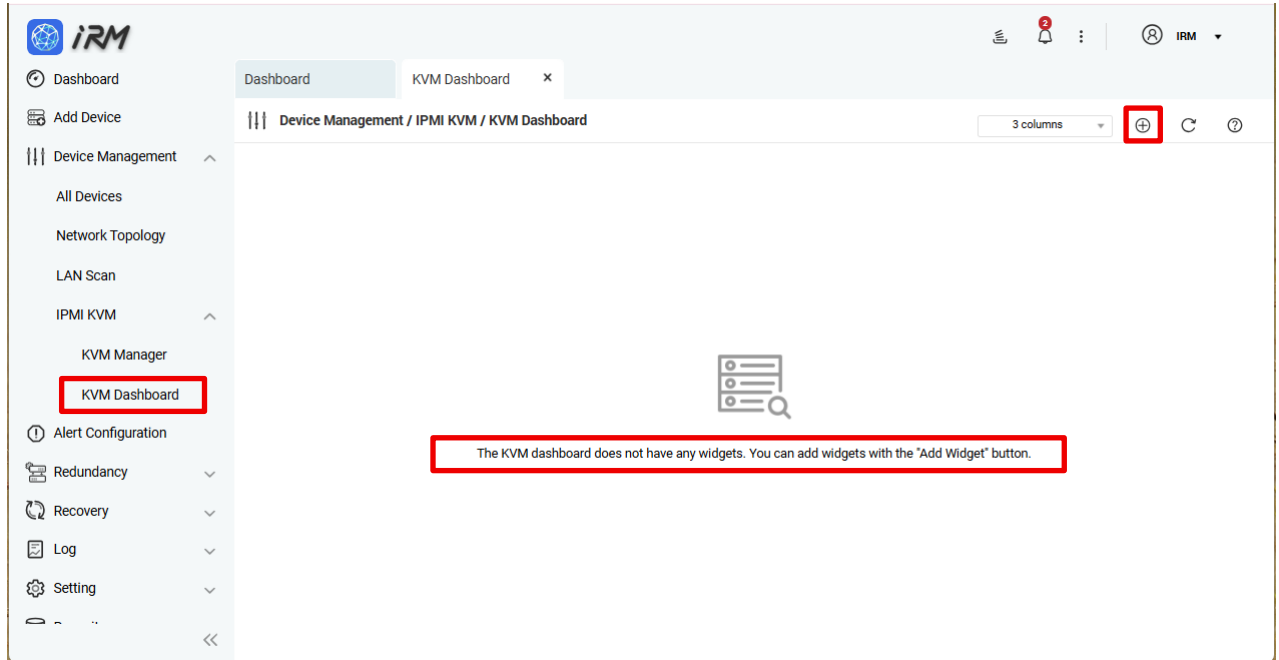


4.4.2 KVM Dashboard

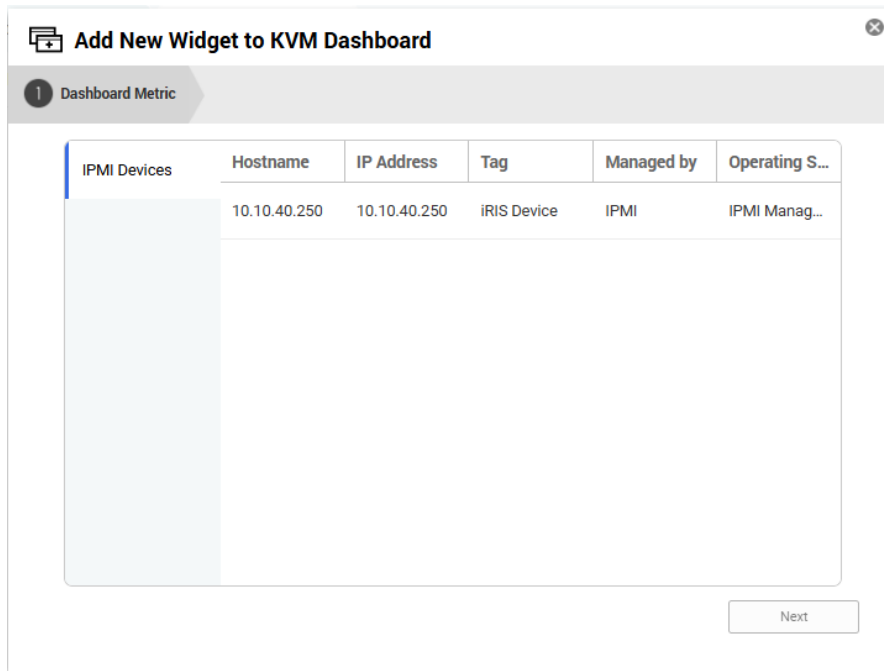
The KVM Dashboard provides a centralized preview of the remote screen images of managed IPMI (iRIS) devices. Users can quickly view the current screen of each device and launch a Remote KVM session from the preview to perform remote maintenance tasks (such as viewing the BIOS/boot screen, operating the OS, and troubleshooting).

4.4.2.1 Add widget to the KVM Dashboard

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

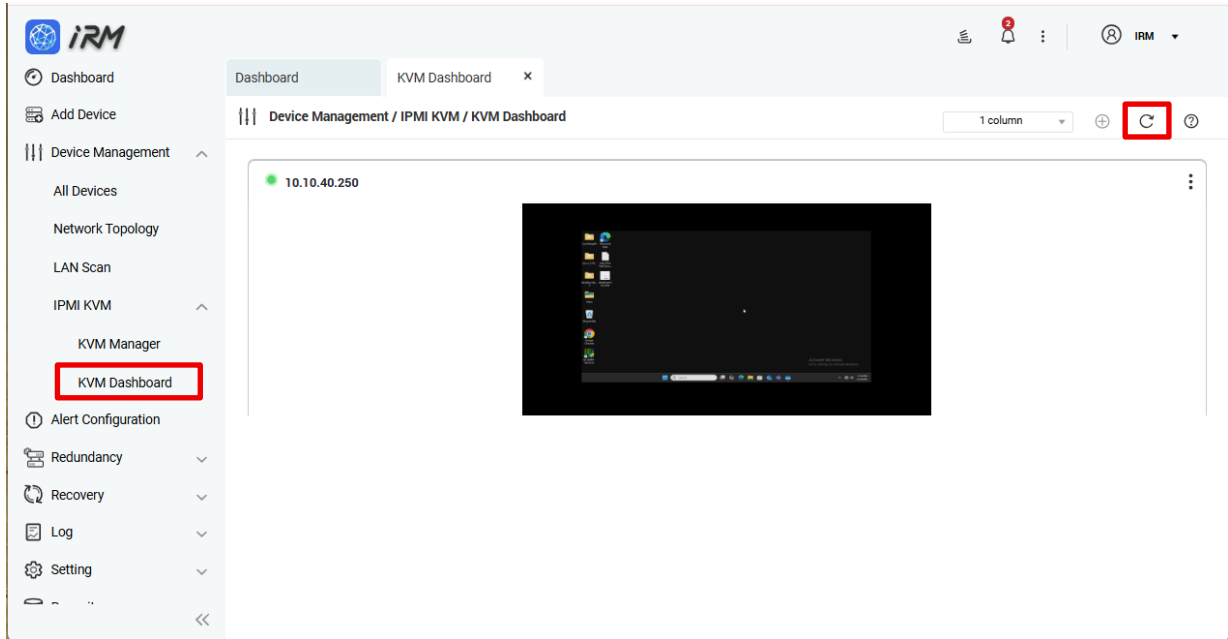


The “Add Widget to KVM Dashboard” window appears. Select the IPMI device you want to add, and then click Next.



4.2.2.2 Refresh KVM Dashboard

Step 1: Go to the KVM Dashboard page and click the "Refresh" button.



4.2.2.3 Select the Layout Mode

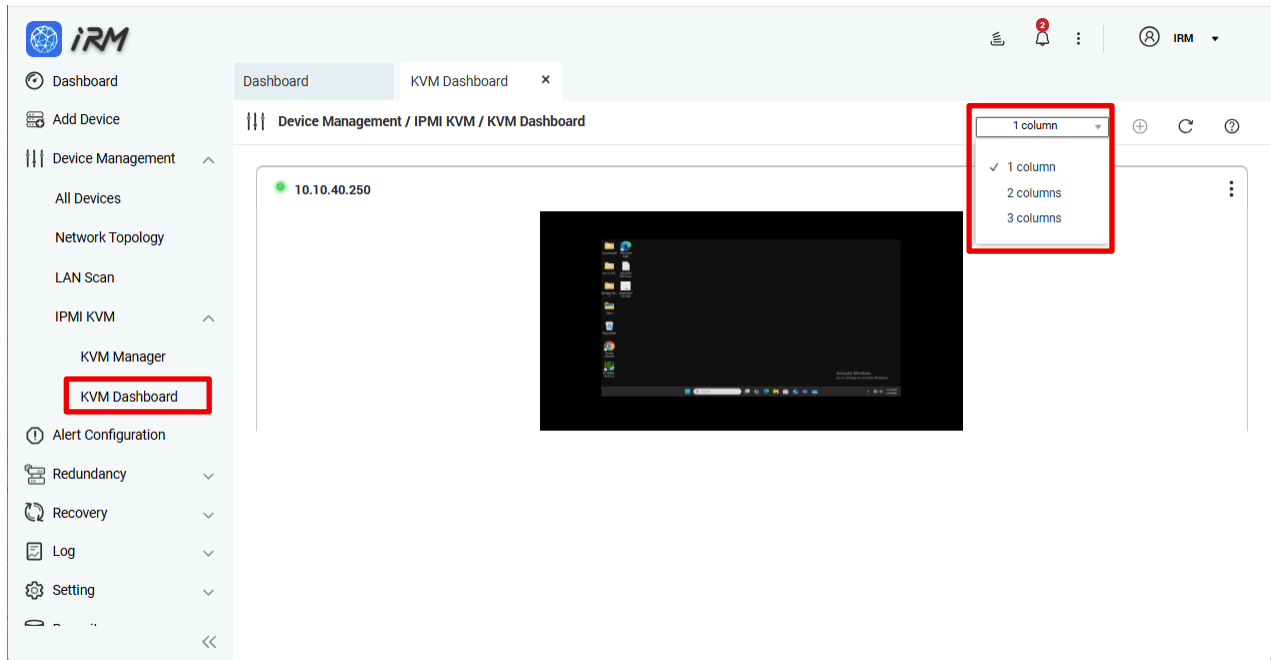
User can adjust the layout of the main KVM Dashboard according to their requirements. KVM Dashboard provides:

- 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 2: Go to the KVM Dashboard page and click the select layout menu.

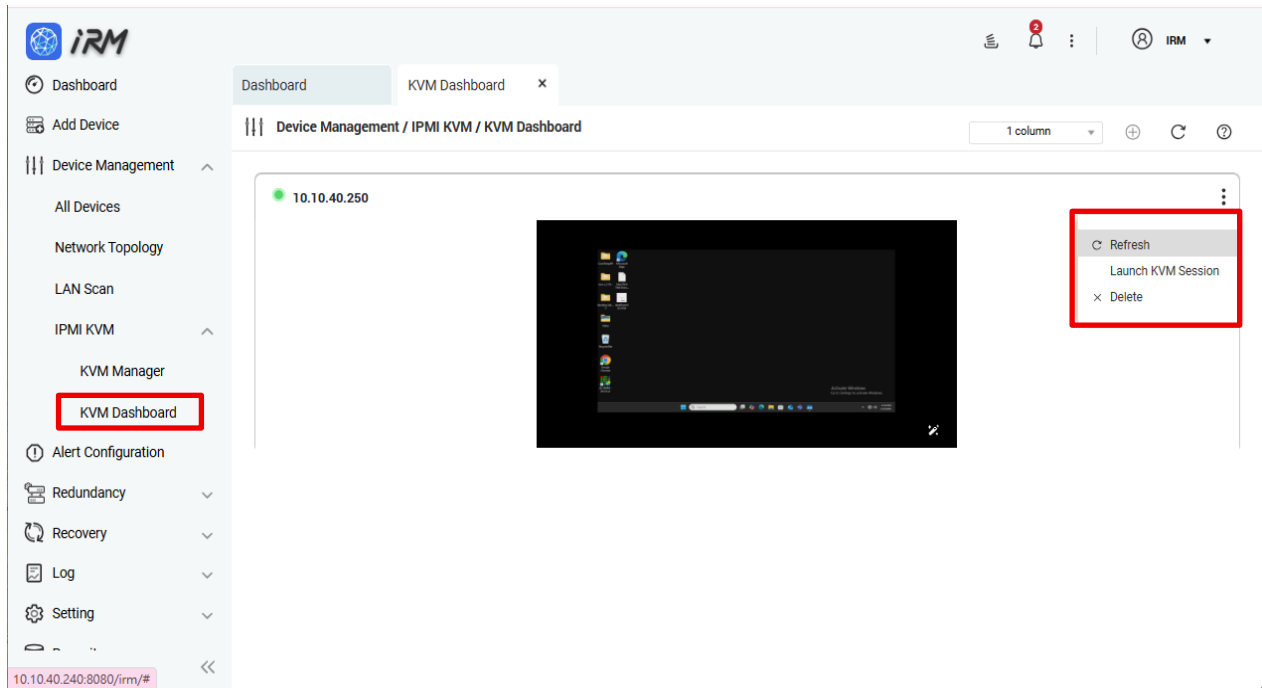
Step 3: Select "1 column", "2 columns" or "3 columns" from the dropdown list.



4.2.2.4 More Options

After adding a widget to the KVM Dashboard, you can perform the following actions for any KVM session: Refresh, Open Remote Desktop, or Delete.

1. Refresh: Immediately refresh the current screen/screenshot of this KVM widget.
2. Launch KVM Session: Open a remote KVM connection directly to enter the KVM console of the IPMI device.
3. Delete: Remove this widget from the KVM Dashboard.



Step 4: 開啟遠端桌面：

1. For any KVM session, click Open Remote Desktop. The system will automatically open a new browser tab and start the remote KVM connection.
2. Alternatively, double-click the thumbnail of the remote screen preview to launch the remote KVM connection.

The screenshot shows the iRM web interface. On the left is a navigation menu with items: Dashboard, Add Device, Device Management (expanded), All Devices, Network Topology, LAN Scan, IPMI KVM (expanded), KVM Manager, **KVM Dashboard** (highlighted with a red box), Alert Configuration, and Redundancy. The main content area shows a 'Dashboard' tab and a 'KVM Dashboard' tab. Below the tabs is a breadcrumb: 'Device Management / IPMI KVM / KVM Dashboard'. A device IP '10.10.40.250' is listed. A central window displays a remote desktop view of a Windows desktop with a red box overlaid containing the text: 'Please Double Click on the remote screenshot to launch Remote KVM Session.'

The screenshot shows a remote KVM session of a Windows desktop. The desktop background is dark. On the left, there are icons for Video, Recycle Bin, Microsoft Edge, Google Chrome, and several folders. A window titled 'Local (127.0.0.1)' is open, displaying 'Temperature Sensors' data. The data is as follows:

Sensor	Value(C)	High Limit	Low Limit	Alert
CPU Temp	44	80	20	<input type="checkbox"/>
Sys Temp	42	60	20	<input type="checkbox"/>

At the bottom of the window, it says 'iSMMP v1.33' and 'iEi'. In the bottom right corner of the desktop, there is an 'Activate Windows' watermark.

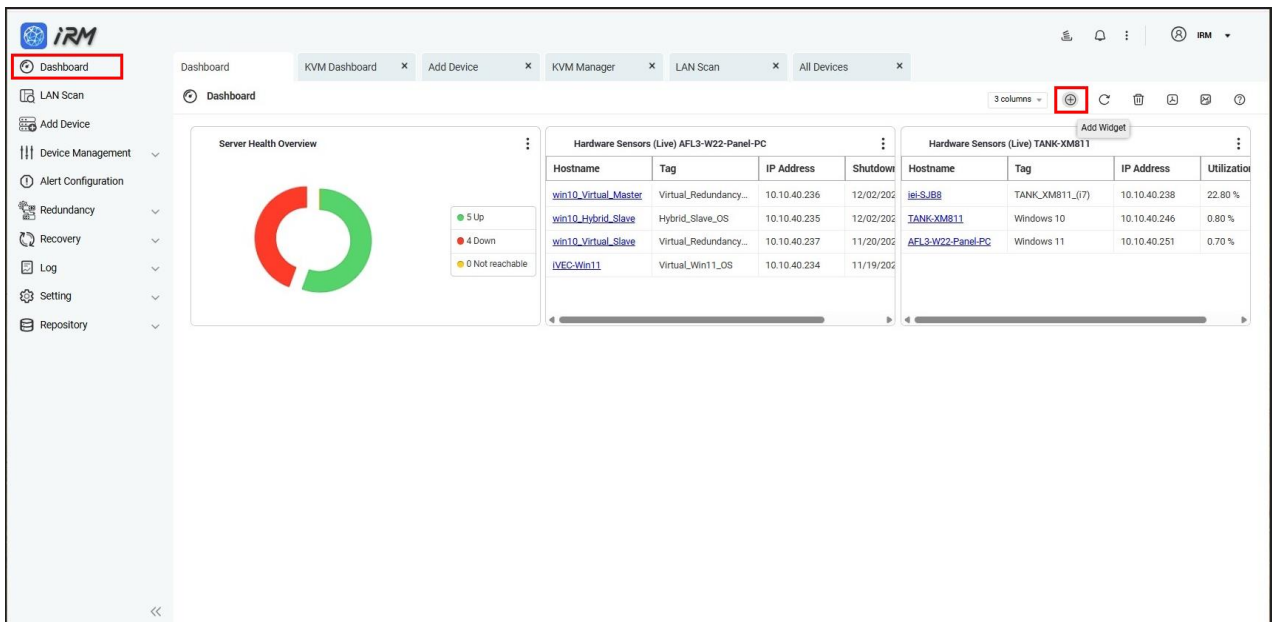
4.4.3 IPMI Add Widget

Users can add **widget** to the dashboard to continuously monitor the health of the IEI iRIS device. The following information can be monitored:

1. CPU TEMP0
2. SYS TEMP1
3. 3V3
4. 3V3SB
5. 12V
6. CPU CORE0
7. DDR
8. Power status

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

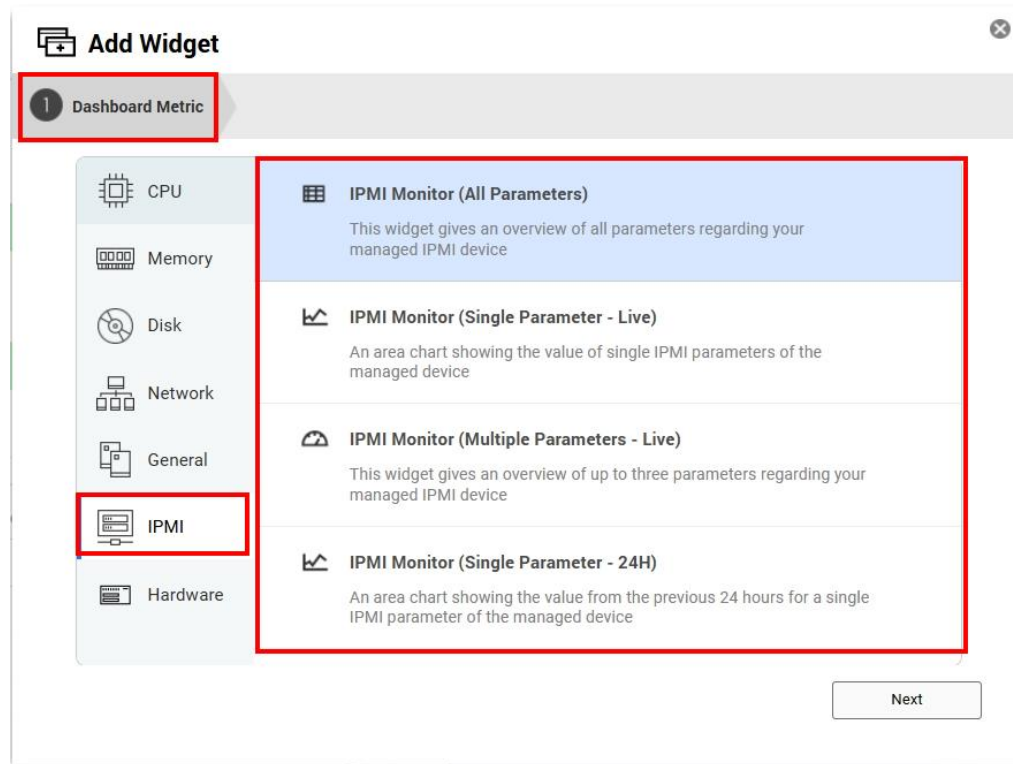
Step 1: Go to the Dashboard page and click the "Add Widget" button.



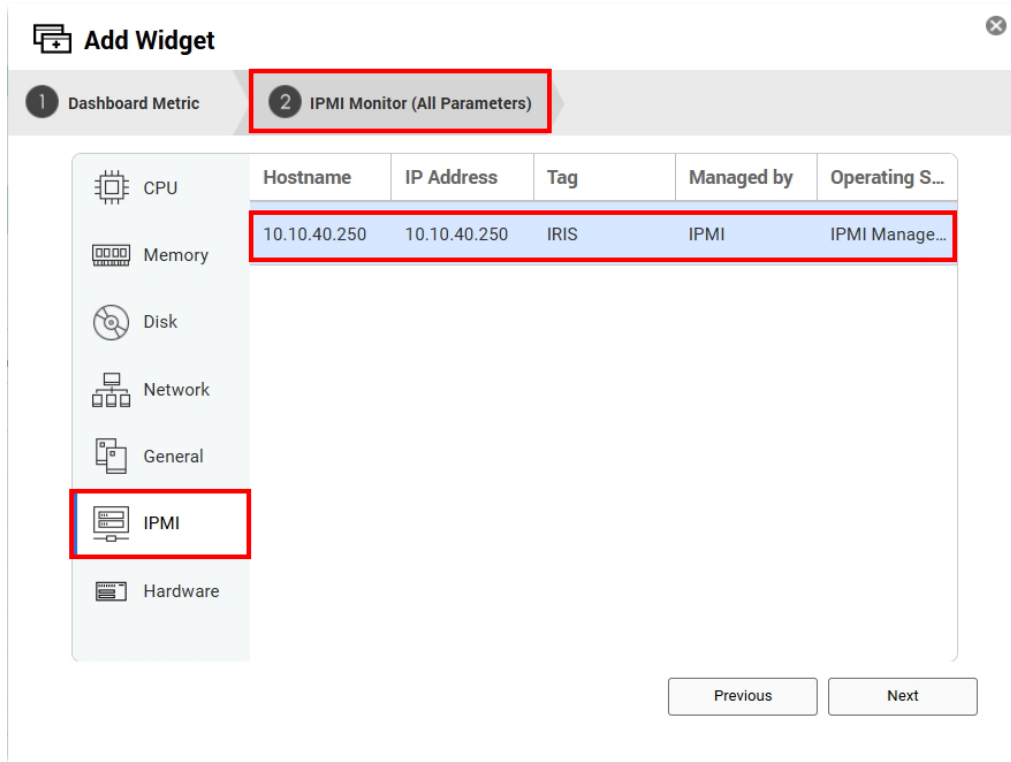
Step 2: Select the type of data you want to monitor:

Select the data type you want to monitor in the right column. There are four types: IPMI Monitor (All

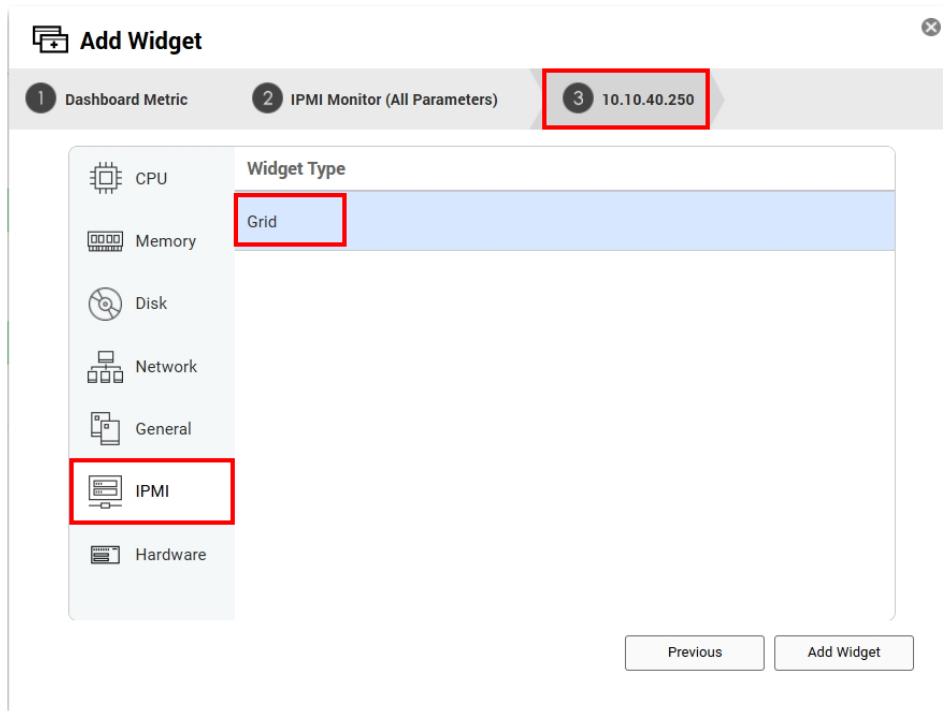
Parameters) Grid displays, IPMI Monitor (Single Parameter - Live) Area Chart display, IPMI Monitor (Multiple Parameters - Live) Gauge display and IPMI Monitor (Single Parameter - 24H) Area Chart display.
(2) Select the method of data presentation that matches your needs.



Step 3: After selecting the iRIS 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.

Dashboard

Dashboard 2 columns

IPMI Monitor (All Parameters) 10.10.40.250

Metric Name	Status	Value
CPU TEMP0	Normal	48 °C
SYS TEMP1	Normal	42 °C
3V3	Normal	3.276 Volts
3V3SB	Normal	3.276 Volts
5V	Normal	4.914 Volts
12V	Normal	11.970 Volts

IPMI Monitor (Single Parameter - Live) - CPU TEMP0

10.10.40.250

IPMI Monitor (Multiple Parameters - Live)

10.10.40.250

IPMI Monitor (Single Parameter - 24H) - CPU TEMP0

10.10.40.250

Chapter

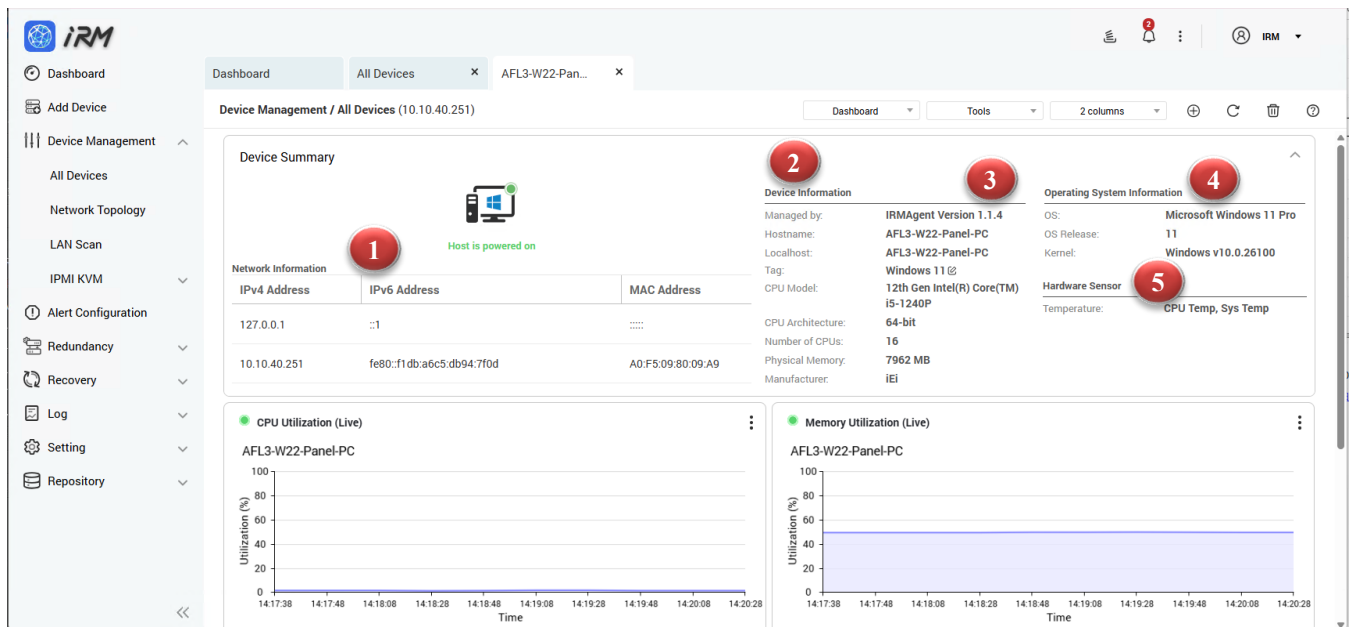
5

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
5. Hardware Sensor

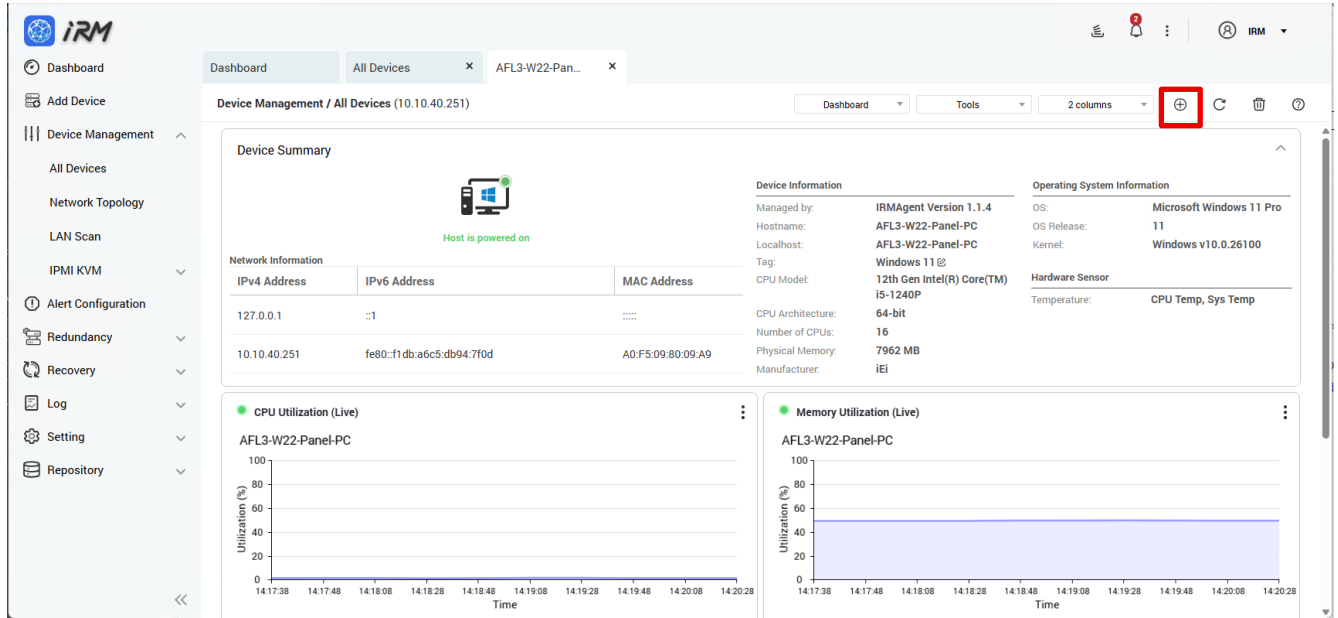


In Single Device Dashboard, users can add or remove widgets, select layout modes, and use the tools in the tool set to manage IRMAgent devices.

5.2 Add Widget

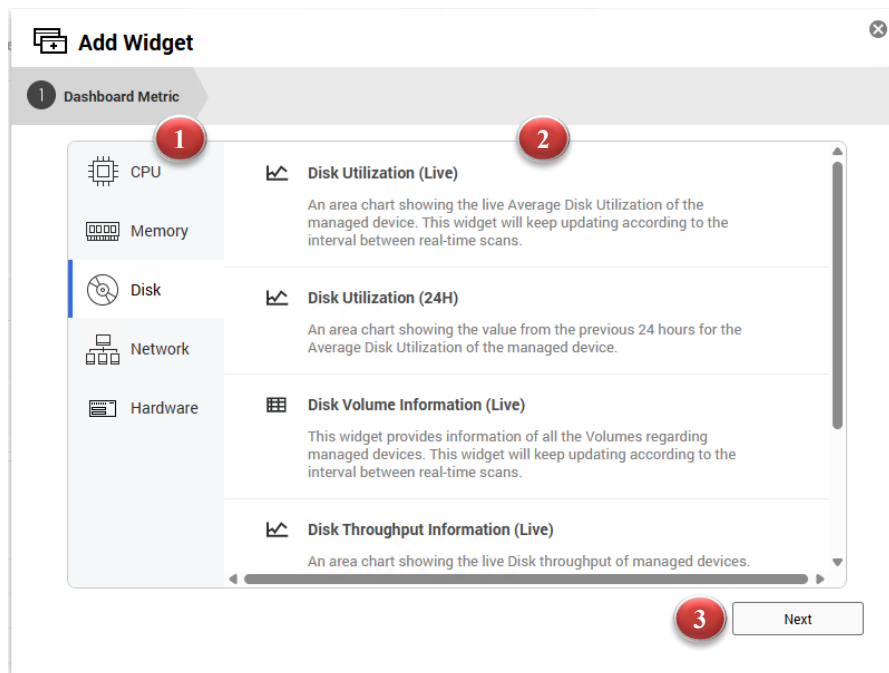
Users can add multiple widgets to customize Single Device Dashboard to monitor CPU usage, memory usage, disk usage, network usage and more, there are also multiple chart types at the user's disposition. Setup steps are described below:

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:

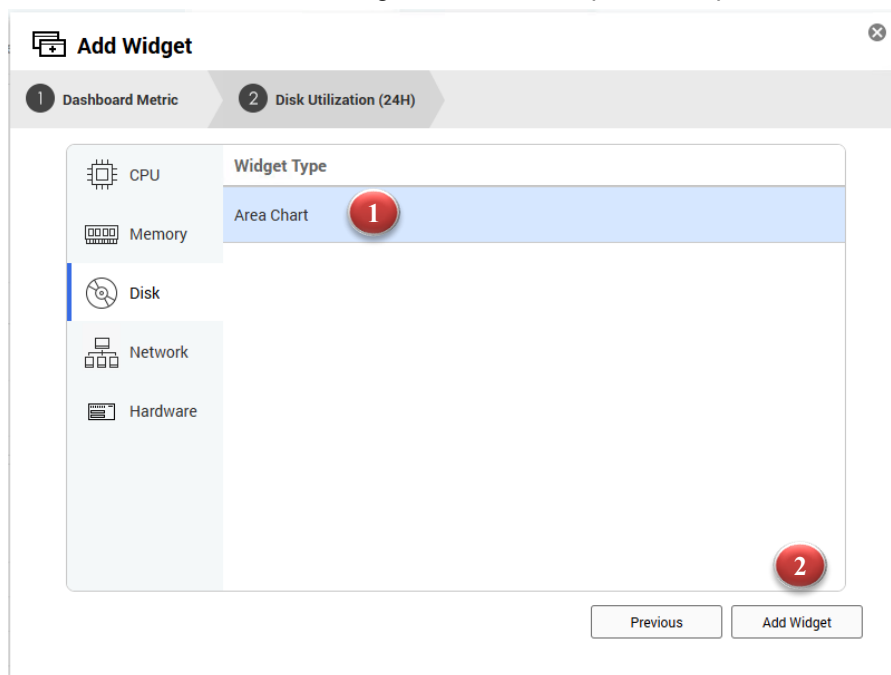
1. Select the type of data you want to monitor. There are four types: CPU usage, memory usage, disk usage, and network usage.
2. Select the data range (real-time data or last 24 hours of historical data).
3. Click "Next".



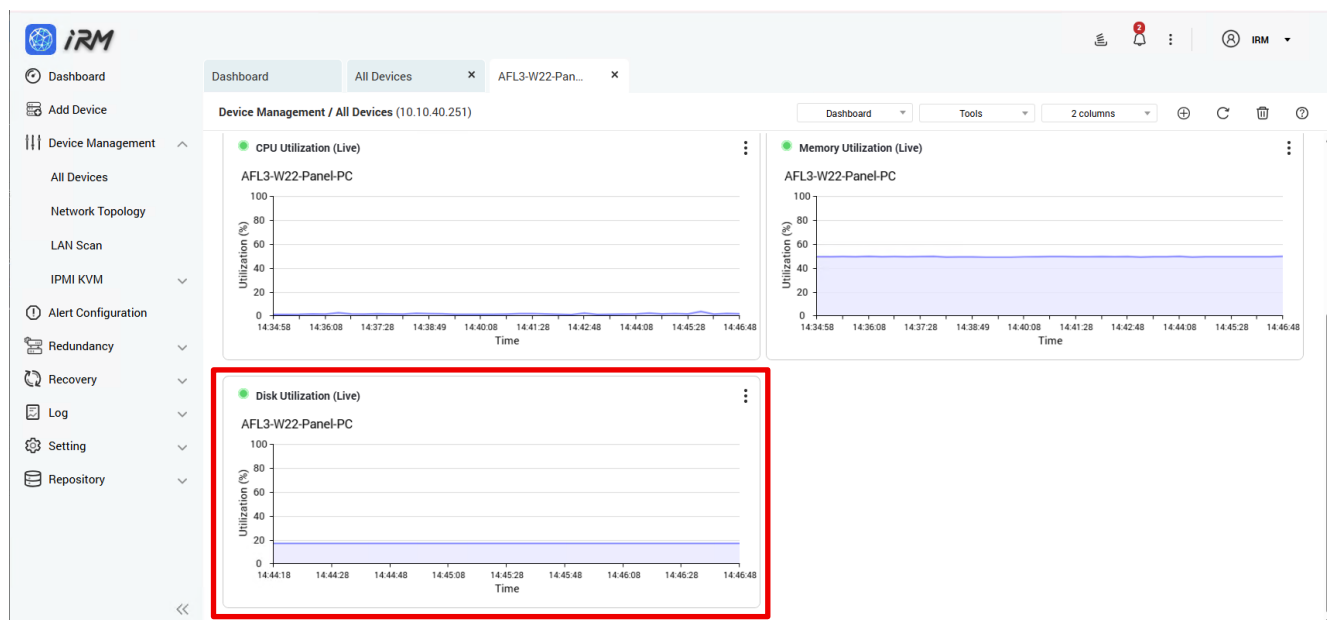
Step 3: Complete the chart type setting:

1. Select the type of chart.

2. Click the "Add Widget" button to complete the operation.

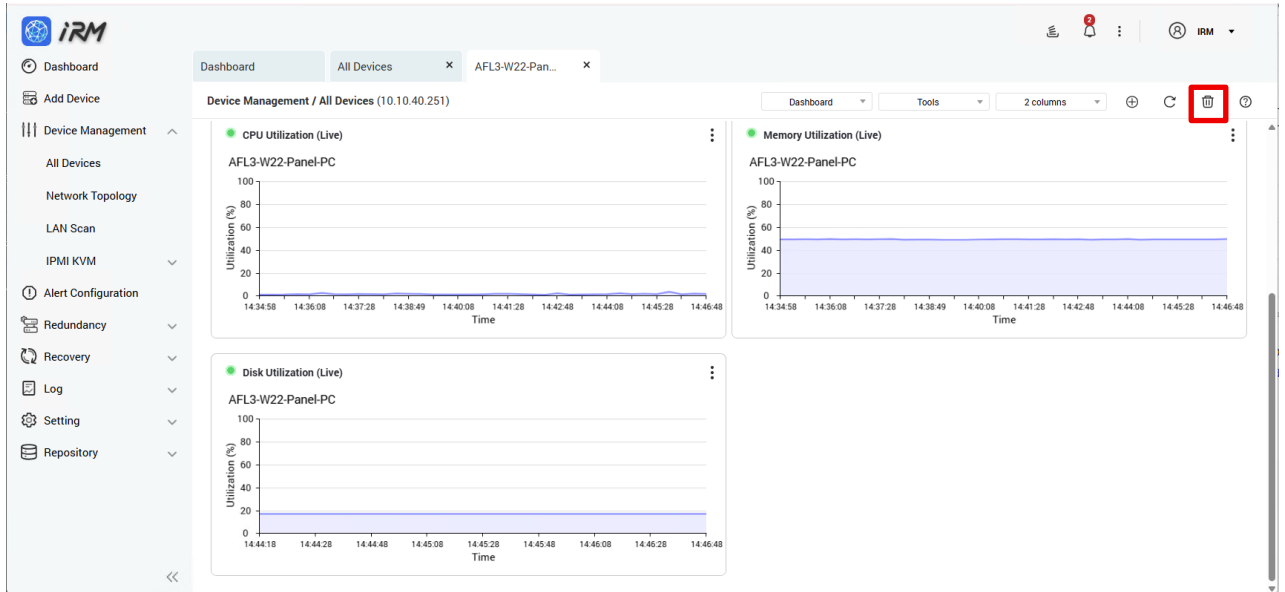


Step 4: When the setup is complete, the widget will be added to the last position in the Dashboard



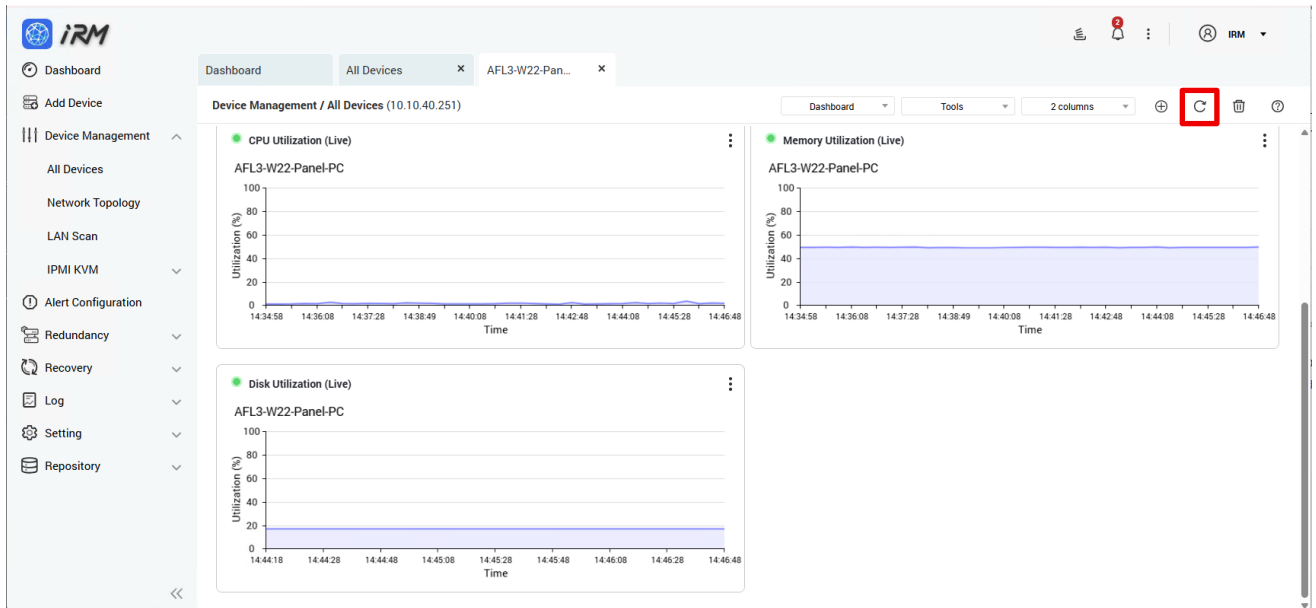
5.3 Delete All Widgets in the Single Device Dashboard

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.



5.5 Select the Layout Mode

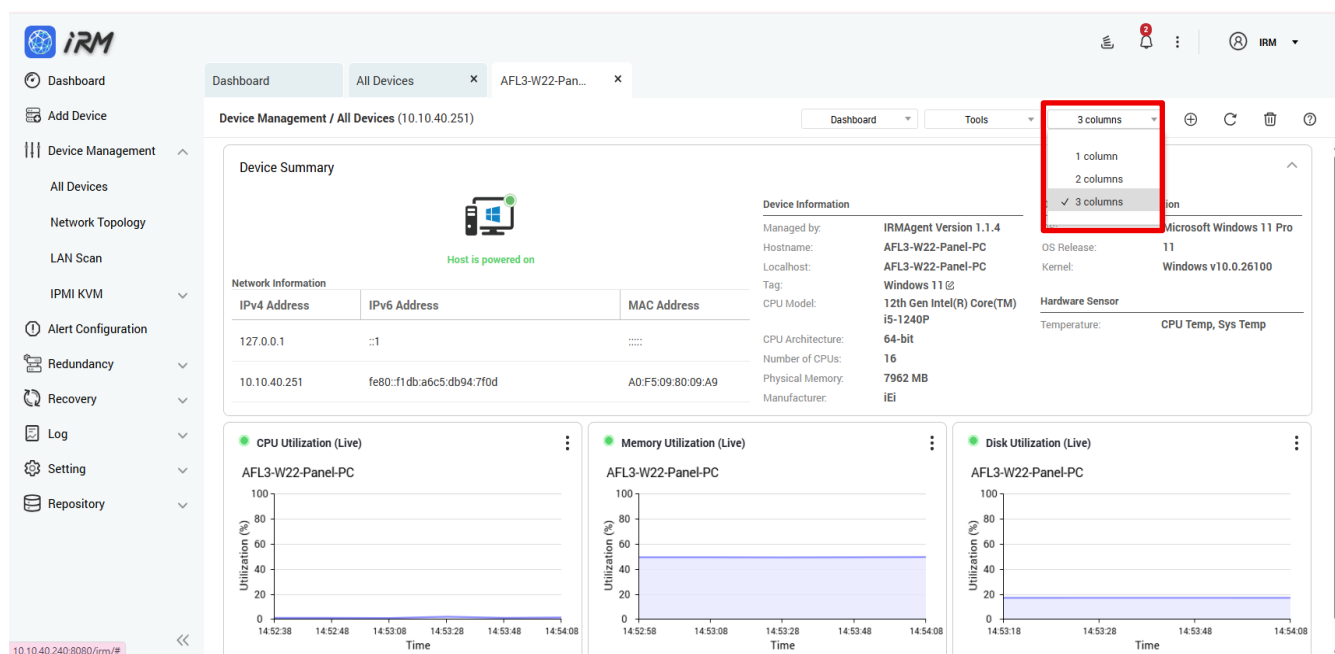
Users can customize the layout of Single Device Dashboard, and the widgets will re-arrange themselves accordingly.

- 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.



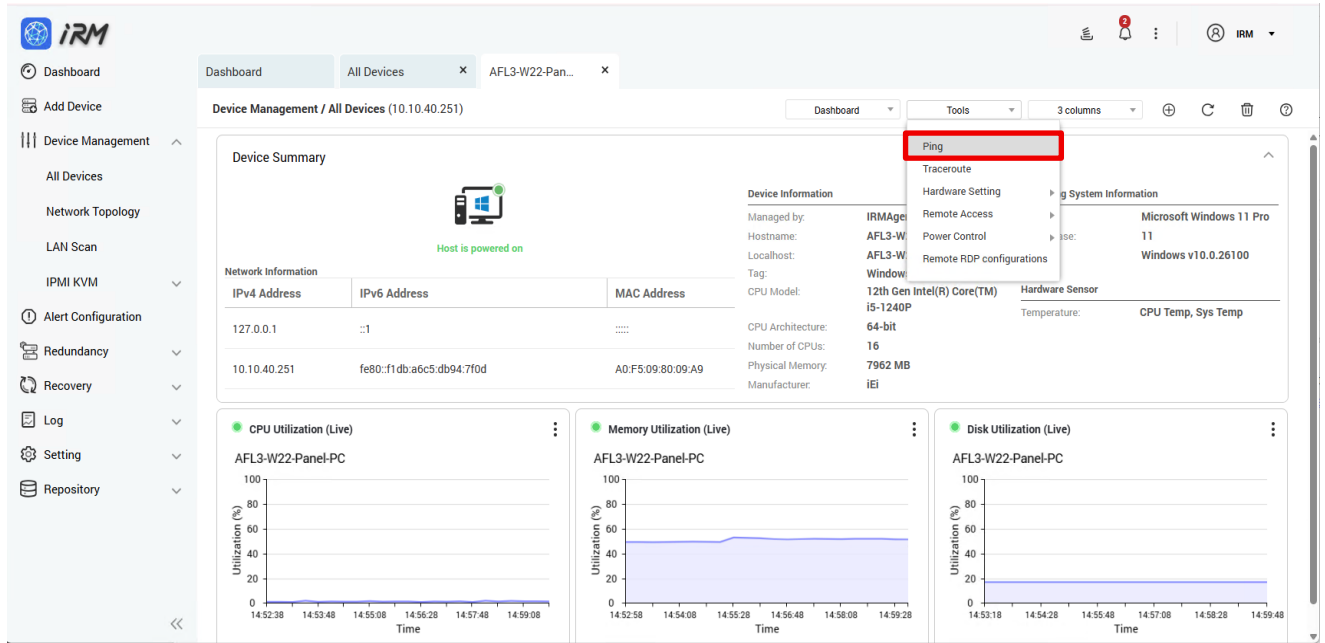
5.6 Tools - Ping

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

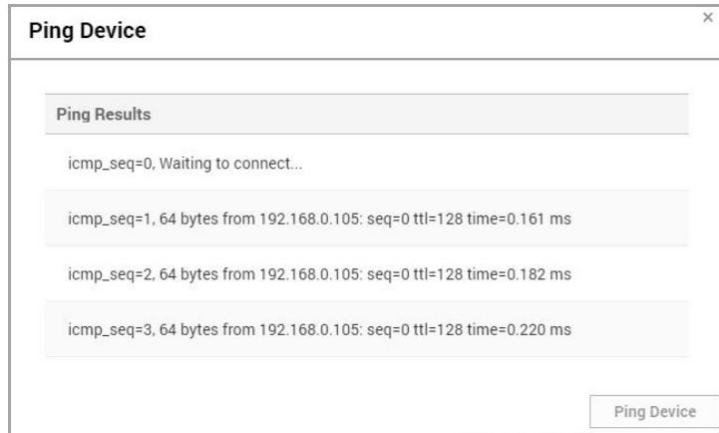
Setup steps are described below:

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.

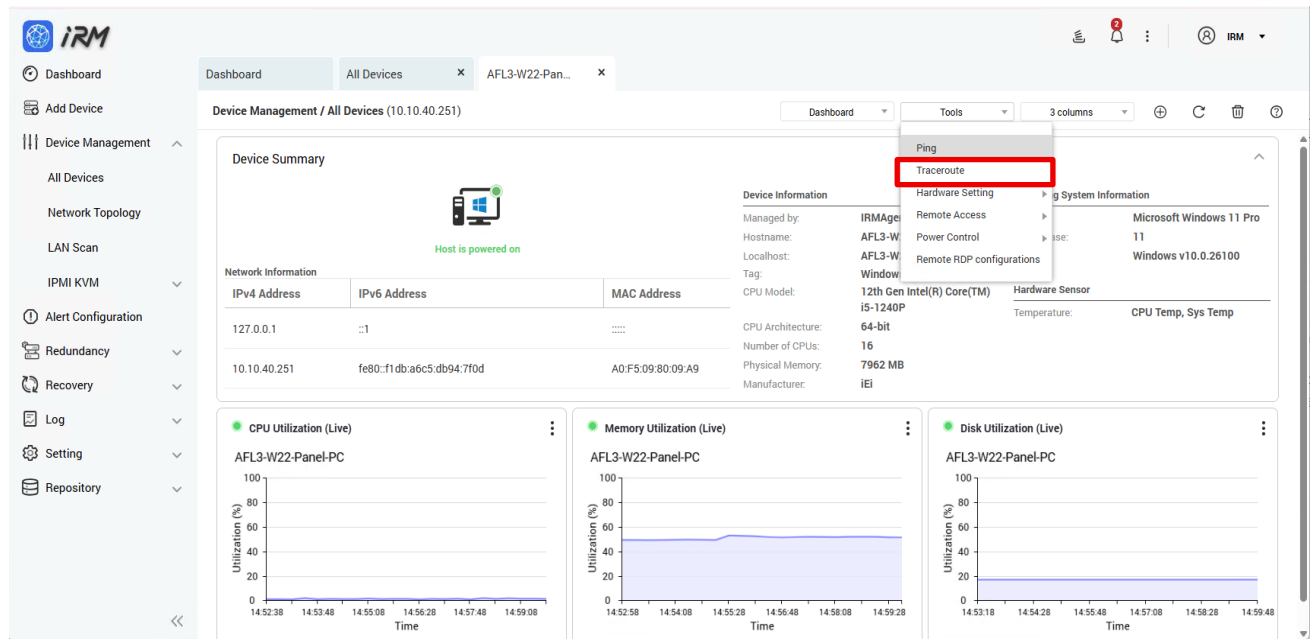
5.7 Tools – Traceroute

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

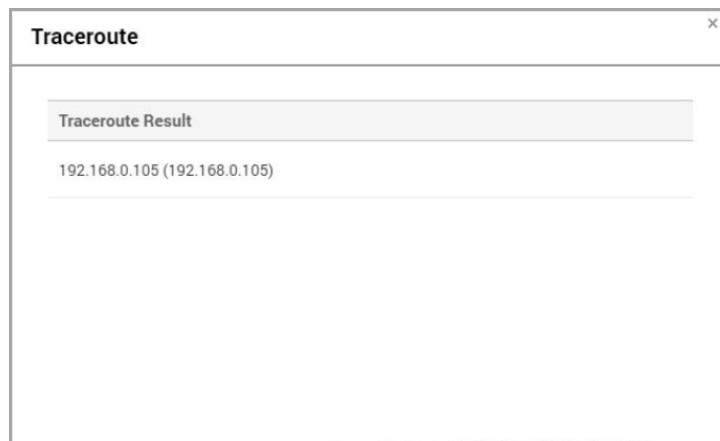
Setup steps are described below:

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

Step 2: Select "Traceroute".

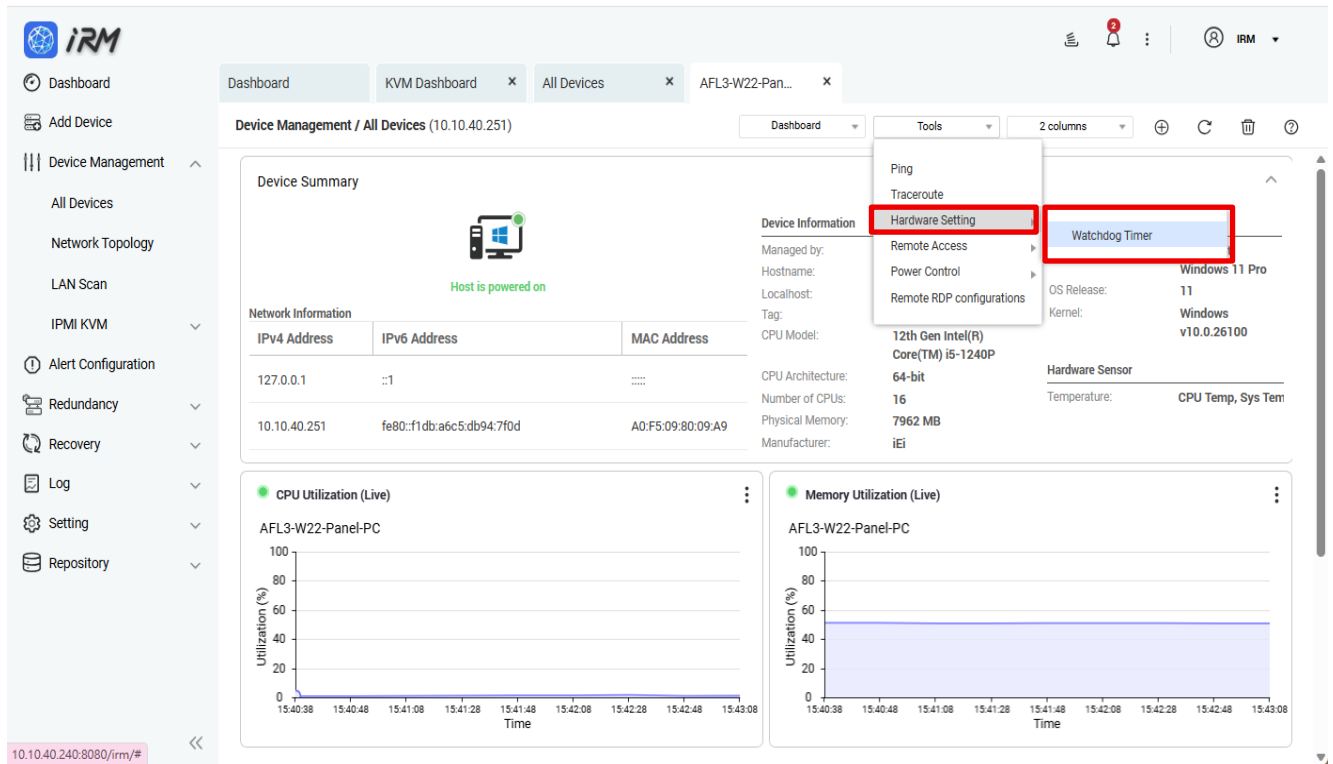


Step 3: A window pops up and displays the Traceroute command execution result.



5.8 Tools - Hardware Setting (Watchdog Timer)

This section is the same as **4.1.10.5 Hardware Setting (Watchdog Timer)**. Please refer to **Section 4.1.10.5** for the complete description, including support scope, WDT switch, timer interval, and Auto Send WDT Interruption / Reload Timer settings.



5.9 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)

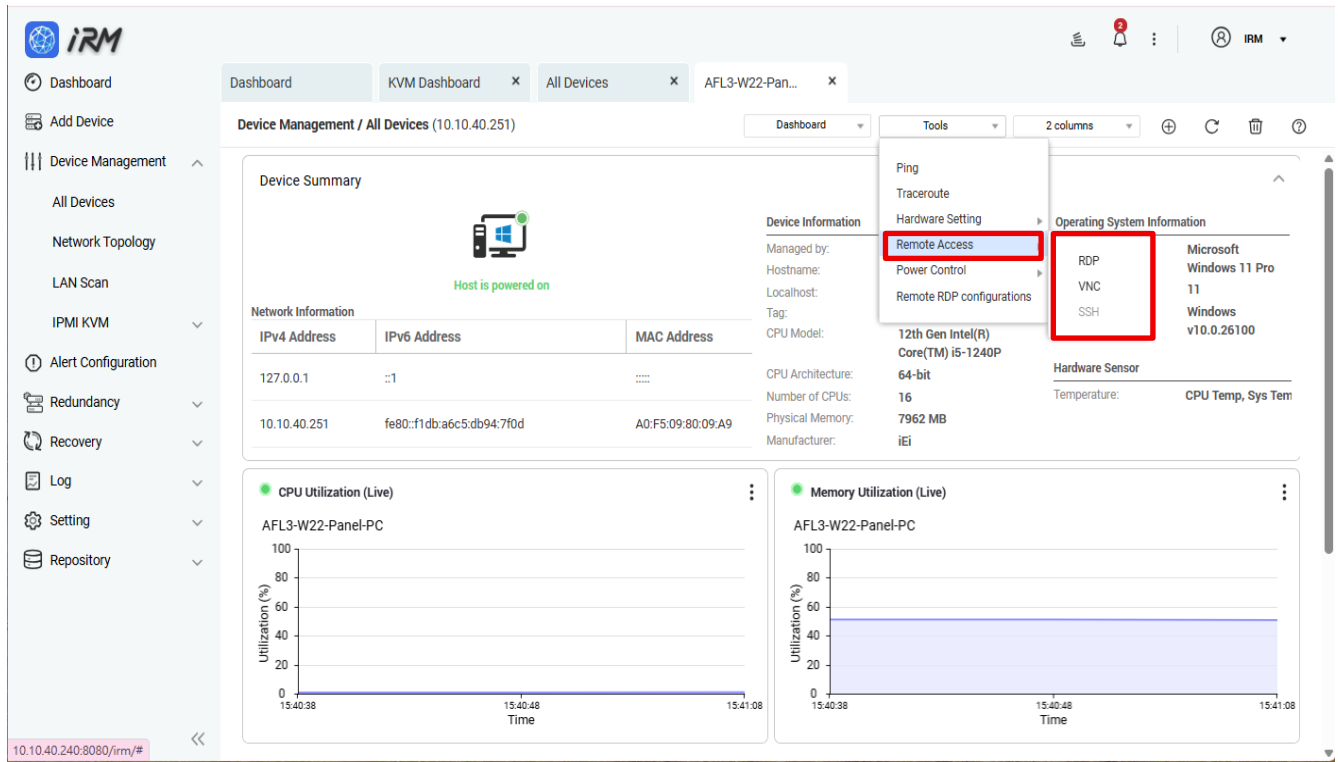
Note: The remote device must enable the option to allow users to connect to the computer Setup steps are described below:

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

Step 2: Select "Remote Desktop".

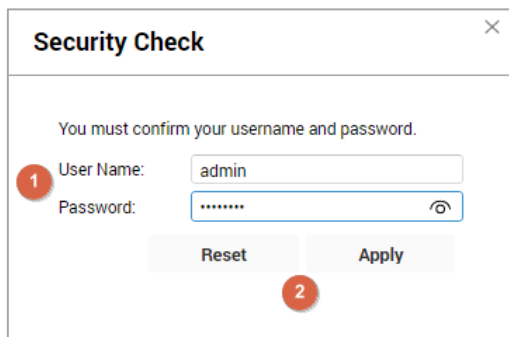
Step 3: Select the appropriate remote access method according to different device types.

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)



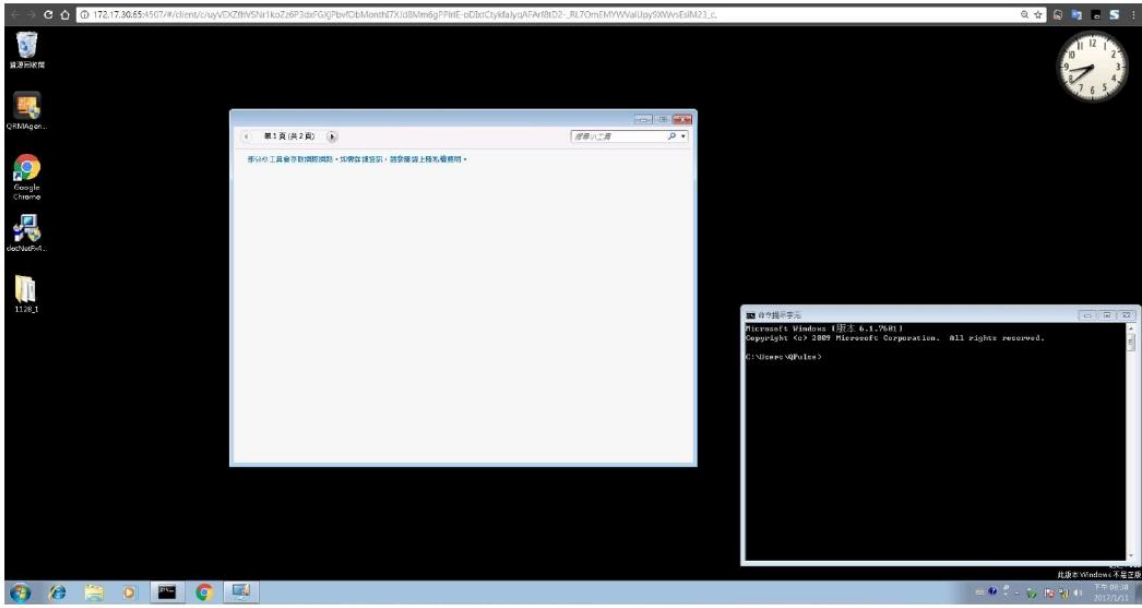
Step 4: A security check window will pop up, asking the user to enter the remote device account number and password.

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

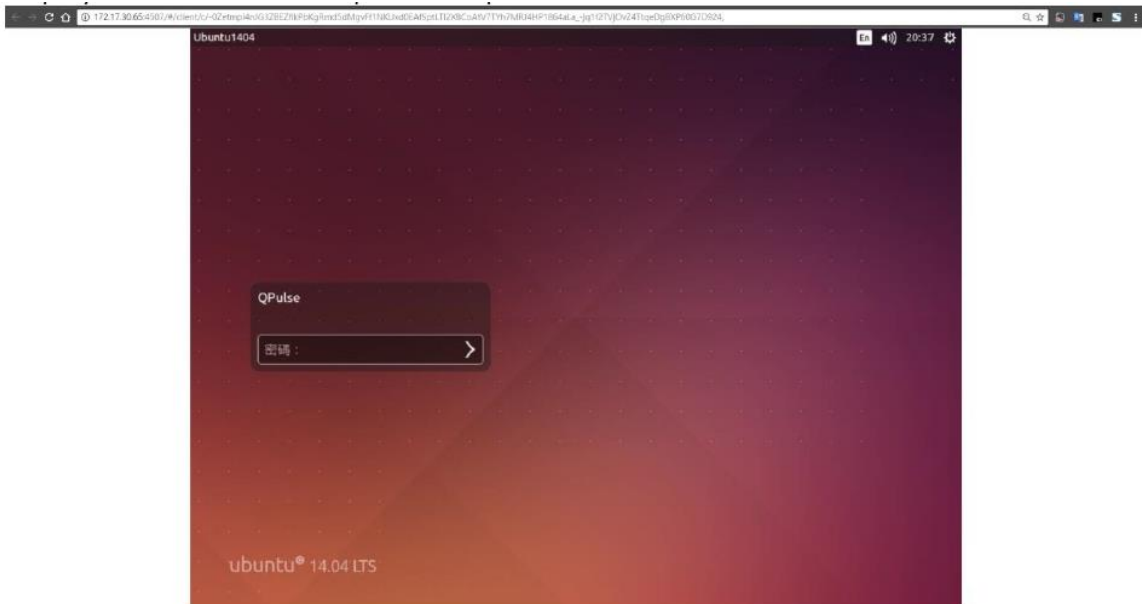


Step 6: The browser opens a new page to display the remote desktop. If the connection is successful, the remote desktop will be displayed. If the connection fails, an error message will be displayed and the user can try to reconnect.

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

```

Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

154 packages can be updated.
278 updates are security updates.

New release '16.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue May  2 17:33:53 2017 from 192.168.0.109
spulse@Ubuntu1404:~$
    
```

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

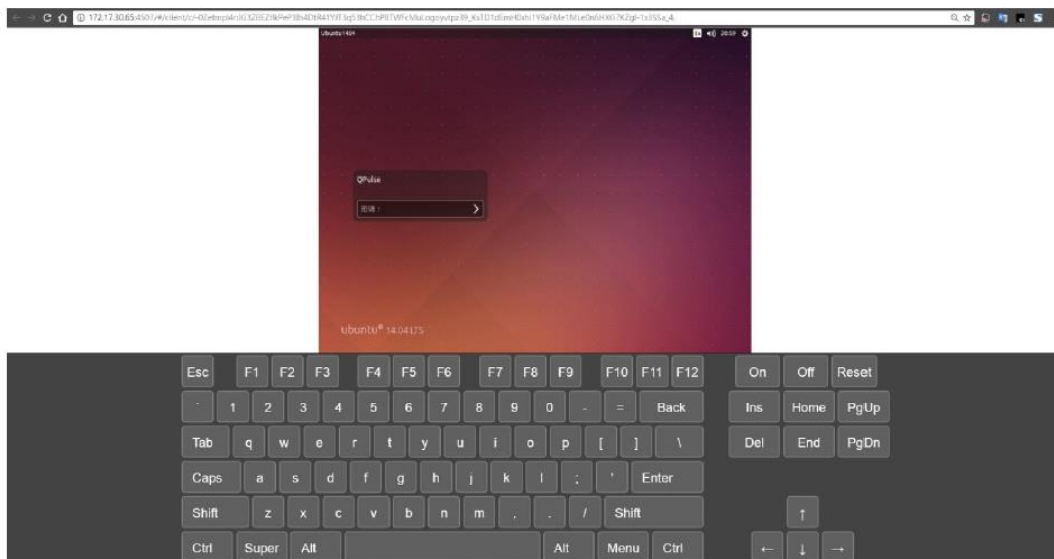
CONNECTION ERROR

The connection has been closed because the server is taking too long to respond. This can be caused by network errors, disconnections, and insufficient bandwidth. Check your network connection and try again.

Reconnecting in 10 seconds...

Reconnect

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



5.10 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 displays the IRMAgent web interface for device management. The main area shows the 'Device Management / All Devices (10.10.40.251)' dashboard. A 'Tools' dropdown menu is open, with 'Power Control' selected. Below it, 'Power Off' and 'Restart' are highlighted. The dashboard includes a 'Device Summary' section with a 'Host is powered on' status, a 'Network Information' table, and two live utilization graphs for CPU and Memory.

IPV4 Address	IPV6 Address	MAC Address
127.0.0.1	::1
10.10.40.251	fe80::f1db:a6c5:db94:7f0d	A0:F5:09:80:09:A9

Device Information	Operating System Information
Managed by:	OS: Microsoft
Hostname:	Windows 11 Pro
Localhost:	11
Tag:	Windows v10.0.26100
CPU Model: 12th Gen Intel(R) Core(TM) i5-1240P	Hardware Sensor
CPU Architecture: 64-bit	Temperature: CPU Temp, Sys Tem
Number of CPUs: 16	
Physical Memory: 7962 MB	
Manufacturer: iEi	

5.11 Tools - Remote RDP configurations

This configures Remote Desktop (RDP) connection settings on the target Windows device. You can choose whether to allow RDP connections and whether to require Network Level Authentication (NLA) for better security. Click Save to apply changes, or Close to exit without changes.

The screenshot shows the iRM web interface. On the left is a navigation menu with options like Dashboard, Add Device, Device Management, and Alert Configuration. The main area displays 'Device Management / All Devices (10.10.40.251)'. A 'Tools' dropdown menu is open, with 'Remote RDP configurations' highlighted in red. Below the menu, there are two live utilization graphs: 'CPU Utilization (Live)' and 'Memory Utilization (Live)', both showing 0% utilization for the device 'AFL3-W22-Panel-PC'.

Managed by:	
Hostname:	
Localhost:	
Tag:	
CPU Model:	12th Gen Intel(R) Core(TM) i5-1240P
CPU Architecture:	64-bit
Number of CPUs:	16
Physical Memory:	7962 MB
Manufacturer:	iEi

OS:	Microsoft Windows 11 Pro
OS Release:	11
Kernel:	Windows v10.0.26100

Temperature:	CPU Temp, Sys Tem
--------------	-------------------

IPv4 Address	IPv6 Address	MAC Address
127.0.0.1	::1
10.10.40.251	fe80::f1db:a6c5:db94:7f0d	A0:F5:09:80:09:A9

Remote RDP configurations

Remote RDP configurations:

- Do not allow connections to this computer
- Allow connections from computers running any version of Remote Desktop (less secure)
- Only allow connections from computers running Remote Desktop with Network Level Authentication (more secure)

Chapter

7

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.

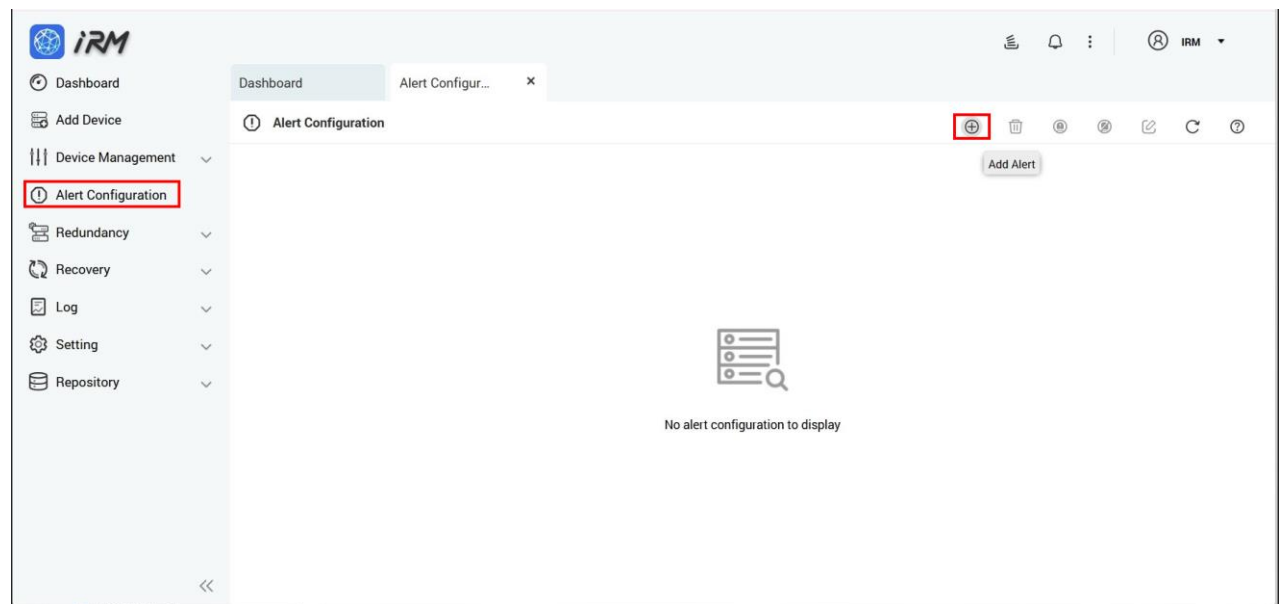
IRM Alert Types

- Agent Alert: Applies to Windows/Linux devices with the IRM Agent installed.
- Hardware Sensor: Applies to hardware sensor monitoring on Windows devices (depending on iSMM-supported items).
- IPMI Alert: Applies to IPMI sensors on iRIS devices (Temperature / Voltage / Power).

6.1 Add Agent Alert

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

Enter the Alert Configuration page and click the "Add Alert" button.



IRM Add Alert Steps:

Step 1: In the Add Alert window, complete the alert type setting:

1. Set Alert Name
2. Set Alert Type: **IRM Alert**
3. Metric: There are four types of IRM alerts: CPU utilization, memory utilization, disk utilization and power status.
4. Condition: Available alert conditions include:
 - CPU utilization: > / < 0–100 (%)
 - Memory utilization: > / < 0–100 (%)
 - Disk utilization: > / < 0–100 (%)
 - Power status: State transition conditions:
 - Power Off → Power On
 - Power On → Power Off

Add Alert

Alert Name: **1**

Alert Type: **2**

Metric: **3**

Condition: **4** **5**

Selected Devices

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

Page 0 of 0 | No devices to display

Step 2: Select the device you want to set the alert, you can select one or multiple devices, then click the OK button.

Selected Devices

Hostname, IP address, Device tag 🔍 ↻

<input type="checkbox"/>	Hostname	IP Address	Tag ↓	Managed by	Brand	Model	Operating System
<input type="checkbox"/>	iei-SJB8	10.10.40.239	iVEC	IRMAgent	IEi	13th Gen Intel(R) C...	Ubuntu
<input checked="" type="checkbox"/>	AFL3-W22-Panel-PC	10.10.40.251	Windows 11	IRMAgent	IEi	12th Gen Intel(R) C...	Microsoft Window...
<input type="checkbox"/>	TANK-811	10.10.40.246	Windows 10	IRMAgent	IEi	13th Gen Intel(R) C...	Microsoft Window...
<input type="checkbox"/>	DRPC-140	10.10.40.245	Windows 10	IRMAgent	IEi	Intel(R) Celeron(R) ...	Microsoft Window...
<input type="checkbox"/>	win10_Virtual_Slave	10.10.40.237	Virtual_Reduo...	IRMAgent	QEMU	Westmere E56xx/L...	Microsoft Window...
<input type="checkbox"/>	win10_Virtual_Mas...	10.10.40.236	Virtual_Reduo...	IRMAgent	QEMU	Westmere E56xx/L...	Microsoft Window...

Page 1 of 1 | 1 - 8 of 8 Only list the selected servers or devices.

OK Cancel

Step 3: 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:

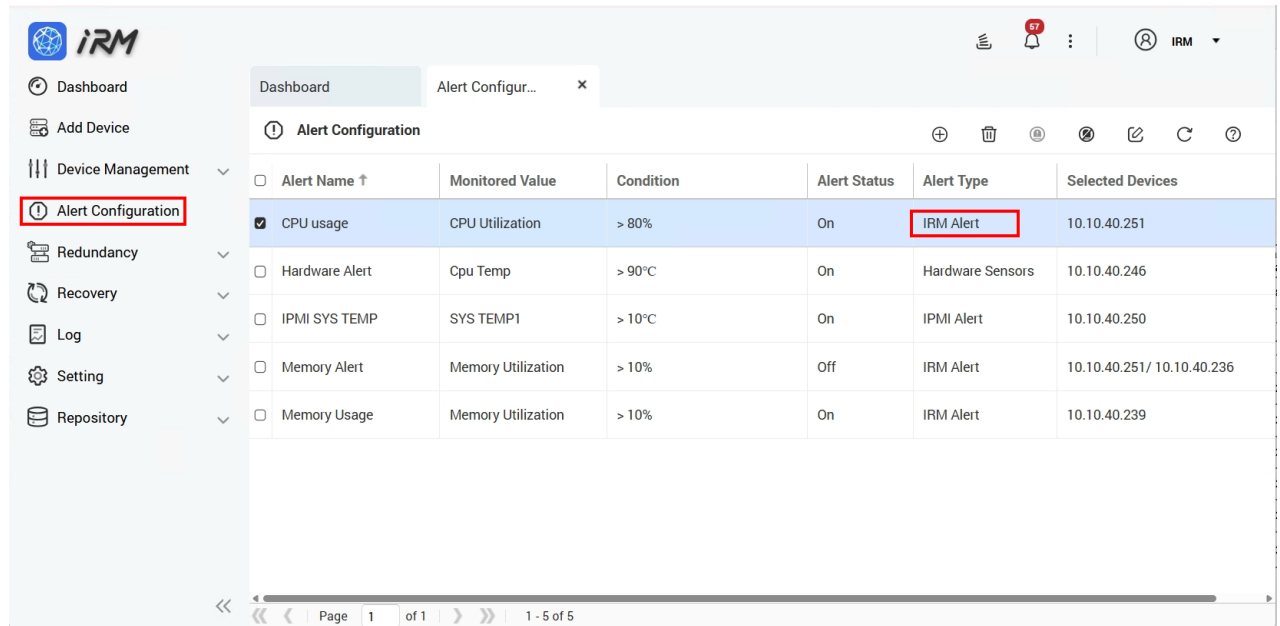
Selected Devices

<input checked="" type="checkbox"/>	Hostname	IP Address ↑	Tag	Managed by	Brand	Model	Operating S...
<input checked="" type="checkbox"/>	AFL3-W22-Panel-PC	10.10.40.251	Windows 11	IRMAgent	IEi	12th Gen Int...	Microsoft Wi...

Page 1 of 1 | 1 - 1 of 1

Save Cancel

Step 4: The IRM alert has been successfully added to Alert Configuration. You can find the alert name in the Alert Configuration list.



6.2 Add Hardware Sensors Alert

Step 1: In the Add Alert window, complete the alert type setting:

1. Set Alert Name
2. Set Alert Type: **Hardware Sensors**
3. Sensor Name: There are sensor follow 4.1.8 IEI System Monitoring Module.
4. Condition: Available Hardware Sensors conditions depend on the sensor unit: include:
 - Temperature (°C) : Configure > / < 0–120 (e.g., CPU Temp).
 - Fan Speed (RPM) : Configure > / < 0–22000 (e.g., CPU Fan).

Note : The available sensor names, condition fields, and ranges may vary depending on the sensors supported by the device. Supported sensor items differ across IEI IPC models; however, CPU Temp and SYS Temp are common to all supported models. These sensors are available only on IEI physical IPC hosts. Virtual machines (VMs) do not support hardware sensor display.

Add Alert ✕

Alert Name: 1

Alert Type: Hardware Sensors 2

Sensor Name: Cpu Temp 3

Condition (°C): 4

Selected Device: Cpu Temp 5

	Tag	Managed by	Brand	Model	Operat Select Device
<input checked="" type="checkbox"/>	Hostname				
<input checked="" type="checkbox"/>	TANK-811	Windows 10	IRMAGENT	IEi	13th Gen Int... Microsoft Wi...

⏪ ⏩ | Page of 1 | ⏪ ⏩ | 1 - 1 of 1

Step 2: Select the device you want to set the alert, you can select one or multiple devices, then click the OK button.

Selected Devices

Hostname, IP address, Device tag 🔍 ↻

	Hostname	IP Address ↓	Tag	Managed by	Brand	Model	Operating System
<input type="checkbox"/>	AFL3-W22-Panel-PC	10.10.40.251	Windows 11	IRMAgent	IEi	12th Gen Intel(R) Cor...	Microsoft Windows 11 Pro
<input checked="" type="checkbox"/>	TANK-811	10.10.40.246	Windows 10	IRMAgent	IEi	13th Gen Intel(R) Cor...	Microsoft Windows 10 Pro
<input type="checkbox"/>	DRPC-140	10.10.40.245	Windows 10	IRMAgent	IEi	Intel(R) Celeron(R) J6...	Microsoft Windows 10 Pro

Page 1 of 1 | 1 - 3 of 3 Only list the selected servers or devices.

OK Cancel

Step 3: 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:

Sensor Name:

Condition (°C):

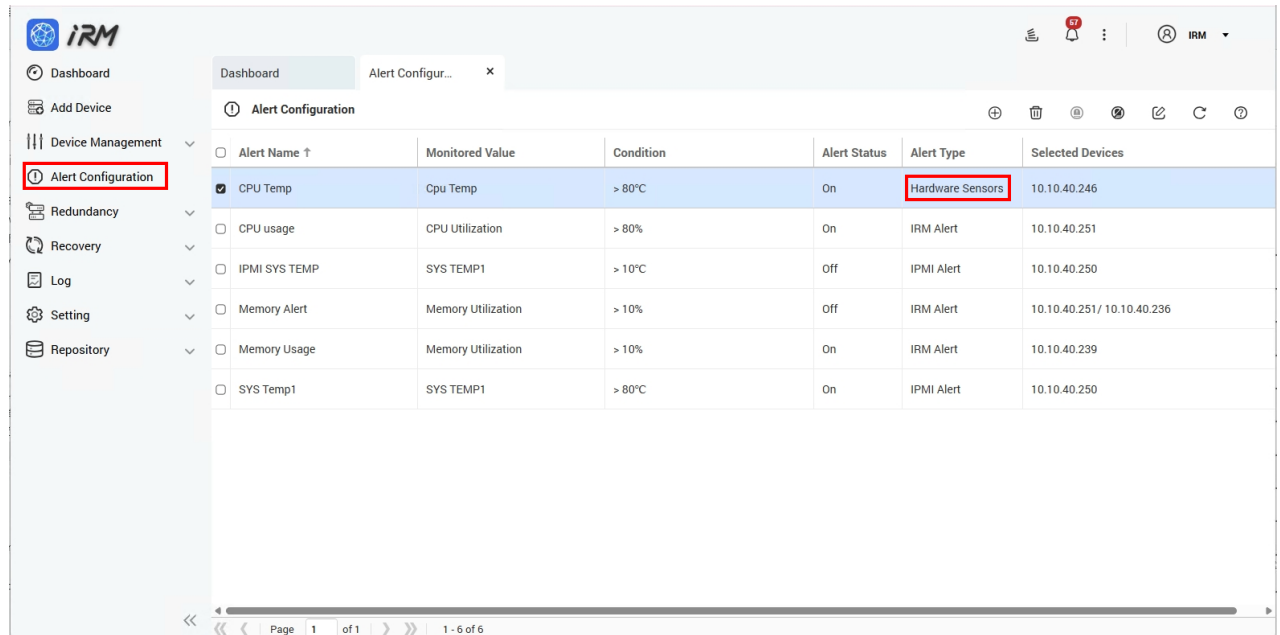
Selected Devices

<input checked="" type="checkbox"/>	Hostname	IP Address ↑	Tag	Managed by	Brand	Model	Operating S...
<input checked="" type="checkbox"/>	TANK-811	10.10.40.246	Windows 10	IRMAgent	IEi	13th Gen Int...	Microsoft Wi...

Page 1 of 1 | 1 - 1 of 1

Save Cancel

Step 4: The Hardware Sensor alert has been successfully added to Alert Configuration. You can find the alert name in the Alert Configuration list.



6.3 Add IPMI(iRIS2) Alert

Step 1: In the Add Alert window, complete the alert type setting:

1. Set Alert Name
2. Set Alert Type: **IPMI Alert**
3. Sensor Type: The following sensors are available for IEI iRIS devices. You can select Temperature, Voltage, or Power.
4. Metric Name: Available options are displayed dynamically based on the selected Sensor Type.
 - Temperature : e.g., TEMP1 \ CPU TEMP0
 - Voltage : e.g., DDR \ CPU CORE0 \ 5V \ 12V \ 3V3SB \ 3V3.
 - Temperature (°C) : Configure < / > 0–120 (e.g., CPU TEMP0).
 - Voltage (V) :
 - DDR: Configure < / > and a threshold value (range 0–12.6).
 - CPU CORE0: Configure < / > and a threshold value (range 0–12.6).
 - 5V: Configure < / > and a threshold value (range 4.75–5.25).
 - 12V: Configure < / > and a threshold value (range 11.4–12.6).
 - 3V3SB: Configure < / > and a threshold value (range 3.135.4–3.465).
 - 3V3: Configure < / > and a threshold value (range 3.135.4–3.465).
 - Power : State transition conditions:

Power Off → Power On

Power On → Power Off

Add Alert ✕

Alert Name: 1

Alert Type: 2

Sensor Type: 3

Metric Name: 4

Condition (°C): 5 6

Selected Devices ⊕ ⊖

<input checked="" type="checkbox"/>	Hostname	IP Address ↑	Tag	Managed by	Brand	Model	Operat Select Devic
<input checked="" type="checkbox"/>	10.10.40.250	10.10.40.250 ↗	iRIS Device	IPMI	IEI Integratio...	IRIS2-2600	IPMI Manag...

⏪ ⏩ | Page of 1 | 1 - 1 of 1

Note: Temperature Sensors

CPU TEMP0: Monitors the core temperature of the primary processor.

SYS TEMP1: Measures the ambient temperature of the system board (motherboard) or the internal temperature of the chassis.

5V: Monitors the +5V power rail, which typically supplies power to peripherals and onboard circuits.

12V: Monitors the +12V power rail, the primary power source for high-draw components like CPU voltage regulators, cooling fans, and storage drives.

3V3: Monitors the +3.3V power rail, which typically powers lower-power components.

3V3SB: Monitors the +3.3V Standby power.

CPU CORE0: Monitors the Vcore voltage supplied directly to the CPU cores.

DDR: Tracks the status or voltage of the System Memory (RAM).

Sensor Name	Unit	Lower Non-Recoverable	Low Critical	Lower Non Critical	Upper Non Critical	Upper Critical	Upper Non Recoverable
				(Lower warning)	(Upper warning)		
CPU_TEMP0	degrees c	0	5	15	70	80	100
CPU_TEMP1	degrees c	0	5	15	70	80	100
SYS_TEMP1	degrees c	0	5	15	70	80	100

SYS_TEMP2	degrees c	0	5	15	70	80	100
SYS_TEMP3	degrees c	0	5	15	70	80	100
CPU_FAN1	RPM	0	260	510	-	-	-
CPU_FAN2	RPM	0	260	510	-	-	-
SYS_FAN1	RPM	0	260	510	-	-	-
SYS_FAN2	RPM	0	260	510	-	-	-
SYS_FAN3	RPM	0	260	510	-	-	-
CPU_CORE0	Volts	0.45	0.51	0.68	2.195	2298	2.383
CPU_CORE1	Volts	0.45	0.51	0.68	2.195	2298	2.383
5V	Volts	4.495	4.624	4.76	5.304	5.44	5.5
12V	Volts	10.511	10.88	11.2	12.8	13.44	14.751
DDR	Volts	0.45	0.51	0.68	1.632	1.855	2.063
5VSB	Volts	4.495	4.624	4.76	5.304	5.44	5.5
3V3	Volts	2.703	2.822	2.988	3.569	3.818	3.983
3V3SB	Volts	2.703	2.822	2.988	3.569	3.818	3.983

Step 2: Select the device you want to set the alert, you can select one or multiple devices, then click the OK button.

Selected Devices ✕

🔍
🔄

	Hostname	IP Address	Tag	Managed by	Brand	Model	Operating System
<input checked="" type="checkbox"/>	● 10.10.40.250	10.10.40.250 🔗	iRIS Device	IPMI	IEI Integration Corp.	IRIS2-2600	IPMI Management ...

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

OK
Cancel

Step 3: 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:

Sensor Type:

Metric Name:

Condition (°C):

Selected Devices ⊕ 🗑

<input checked="" type="checkbox"/>	Hostname ↑	IP Address	Tag	Managed by	Brand	Model	Operating S...
<input checked="" type="checkbox"/>	10.10.40.250	10.10.40.250	iRIS Device	IPMI	IEI Integratio...	IRIS2-2600	IPMI Manag...

Page 1 of 1 | 1 - 1 of 1

Save
Cancel

Step 4: IPMI Alert 成功新增至 Alert Configuration 。您可以在 Alert Configuration 列表中查詢該 Alert Name 。

Dashboard
Alert Configur... ✕

- Dashboard
- Add Device
- Device Management
 - Alert Configuration
 - Redundancy
 - Recovery
 - Log
 - Setting
 - Repository

Alert Configuration

<input type="checkbox"/>	Alert Name ↓	Monitored Value	Condition	Alert Status	Alert Type	Selected Devices
<input type="checkbox"/>	SYS Temp1	SYS TEMP1	> 80°C	Off	IPMI Alert	10.10.40.250
<input type="checkbox"/>	Memory Usage	Memory Utilization	> 10%	On	IRM Alert	10.10.40.239
<input type="checkbox"/>	Memory Alert	Memory Utilization	> 10%	Off	IRM Alert	10.10.40.251 / 10.10.40.236
<input checked="" type="checkbox"/>	IPMI SYS TEMP	SYS TEMP1	> 80°C	On	IPMI Alert	10.10.40.250
<input type="checkbox"/>	CPU usage	CPU Utilization	> 80%	On	IRM Alert	10.10.40.251
<input type="checkbox"/>	CPU Temp	Cpu Temp	> 80°C	On	Hardware Sensors	10.10.40.246

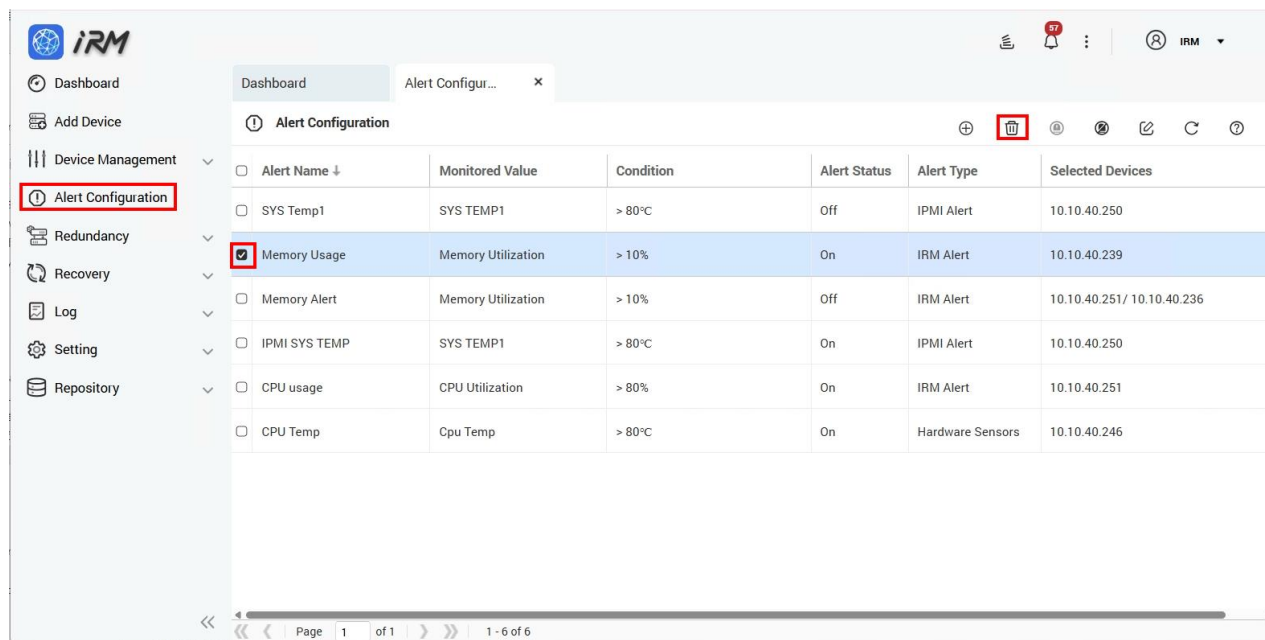
Page 1 of 1 | 1 - 6 of 6

6.4 Delete Alert

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

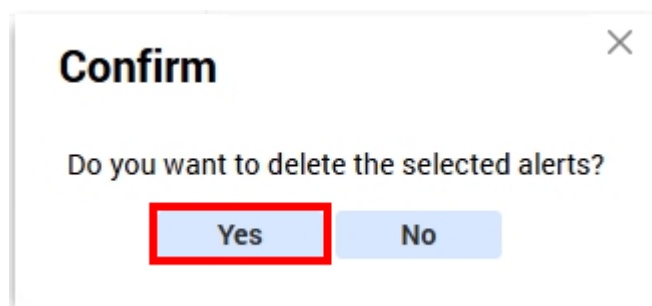
Step 1: Enter the Alert Configuration page and select the alert configuration you want to delete.

Step 2: Click the "Delete Alert" button.



Alert Name ↓	Monitored Value	Condition	Alert Status	Alert Type	Selected Devices
<input type="checkbox"/> SYS Temp1	SYS TEMP1	> 80°C	Off	IPMI Alert	10.10.40.250
<input checked="" type="checkbox"/> Memory Usage	Memory Utilization	> 10%	On	IRM Alert	10.10.40.239
<input type="checkbox"/> Memory Alert	Memory Utilization	> 10%	Off	IRM Alert	10.10.40.251/ 10.10.40.236
<input type="checkbox"/> IPMI SYS TEMP	SYS TEMP1	> 80°C	On	IPMI Alert	10.10.40.250
<input type="checkbox"/> CPU usage	CPU Utilization	> 80%	On	IRM Alert	10.10.40.251
<input type="checkbox"/> CPU Temp	Cpu Temp	> 80°C	On	Hardware Sensors	10.10.40.246

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



Confirm ✕

Do you want to delete the selected alerts?

6.5 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.

<input type="checkbox"/>	Alert Name ↓	Monitored Value	Condition	Alert Status	Alert Type	Selected Devices
<input type="checkbox"/>	SYS Temp1	SYS TEMP1	> 80°C	Off	IPMI Alert	10.10.40.250
<input type="checkbox"/>	Memory Usage	Memory Utilization	> 10%	On	IRM Alert	10.10.40.239
<input checked="" type="checkbox"/>	Memory Alert	Memory Utilization	> 10%	Off	IRM Alert	10.10.40.251 / 10.10.40.236
<input type="checkbox"/>	IPMI SYS TEMP	SYS TEMP1	> 80°C	On	IPMI Alert	10.10.40.250
<input type="checkbox"/>	CPU usage	CPU Utilization	> 80%	On	IRM Alert	10.10.40.251
<input type="checkbox"/>	CPU Temp	Cpu Temp	> 80°C	On	Hardware Sensors	10.10.40.246

6.6 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.

Dashboard | Alert Configur... x

Alert Configuration

<input type="checkbox"/>	Alert Name ↓	Monitored Value	Condition	Alert Status	Alert Type	Selected Devices
<input type="checkbox"/>	SYS Temp1	SYS TEMP1	> 80°C	Off	IPMI Alert	10.10.40.250
<input checked="" type="checkbox"/>	Memory Usage	Memory Utilization	> 10%	On	IRM Alert	10.10.40.239
<input type="checkbox"/>	Memory Alert	Memory Utilization	> 10%	Off	IRM Alert	10.10.40.251/ 10.10.40.236
<input type="checkbox"/>	IPMI SYS TEMP	SYS TEMP1	> 80°C	On	IPMI Alert	10.10.40.250
<input type="checkbox"/>	CPU usage	CPU Utilization	> 80%	On	IRM Alert	10.10.40.251
<input type="checkbox"/>	CPU Temp	Cpu Temp	> 80°C	On	Hardware Sensors	10.10.40.246

Page 1 of 1 | 1 - 6 of 6

6.7 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.

Dashboard | Alert Configur... x

Alert Configuration

<input type="checkbox"/>	Alert Name ↓	Monitored Value	Condition	Alert Status	Alert Type	Selected Devices
<input checked="" type="checkbox"/>	SYS Temp1	SYS TEMP1	> 80°C	Off	IPMI Alert	10.10.40.250
<input type="checkbox"/>	Memory Usage	Memory Utilization	> 10%	On	IRM Alert	10.10.40.239
<input type="checkbox"/>	Memory Alert	Memory Utilization	> 10%	Off	IRM Alert	10.10.40.251/ 10.10.40.236
<input type="checkbox"/>	IPMI SYS TEMP	SYS TEMP1	> 80°C	On	IPMI Alert	10.10.40.250
<input type="checkbox"/>	CPU usage	CPU Utilization	> 80%	On	IRM Alert	10.10.40.251
<input type="checkbox"/>	CPU Temp	Cpu Temp	> 80°C	On	Hardware Sensors	10.10.40.246

Page 1 of 1 | 1 - 6 of 6

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 ⊕ 🗑️

<input checked="" type="checkbox"/>	Hostname ↑	IP Address	Tag	Managed by	Brand	Model	Operating S...
<input checked="" type="checkbox"/>	AFL3-W22-Panel...	10.10.40.251	Windows 11	IRMAgent	IEi	12th Gen Inte...	Microsoft Wi...

« < | Page of 1 | > » | 1 - 1 of 1

Chapter

7

7 Redundancy

The Redundancy feature provides a OS Level Redundancy mechanism for primary/secondary devices. It helps reduce service interruption risk by switching or performing recovery actions according to predefined rules when the primary host encounters an issue. Users can create a Device Pair, configure a Policy, create a Redundancy Plan, and review execution results through the Redundancy Log. The Policy can be reused by different Plan.

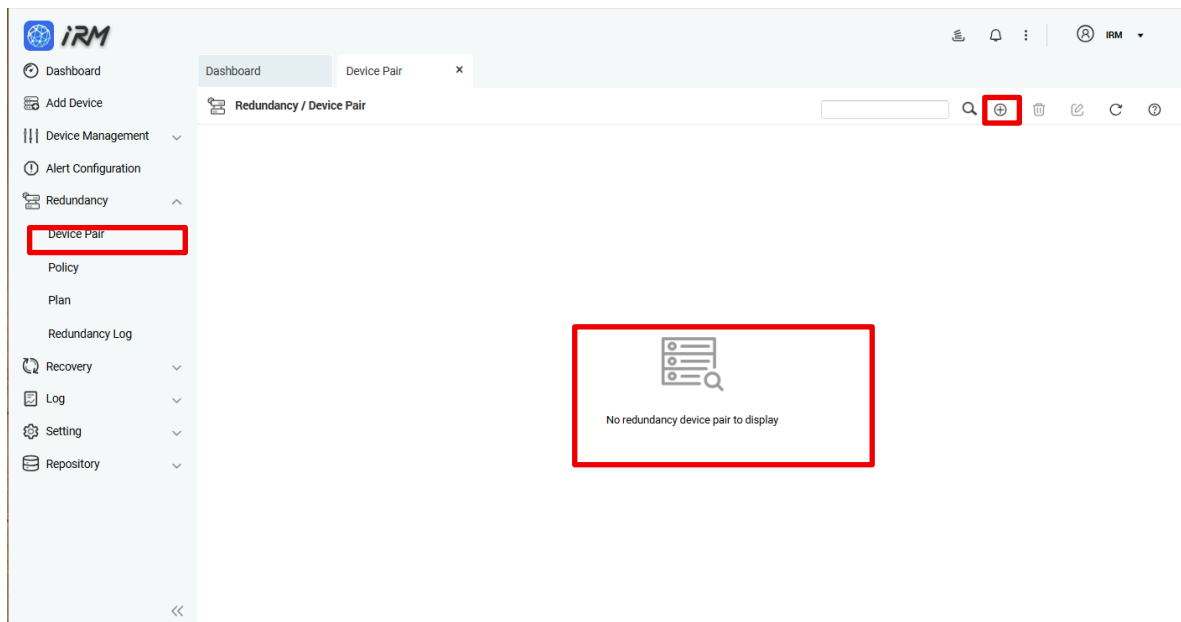
Steps to setup an redundancy monitoring agent:




7.1 Device Pair

A Device Pair is used to establish a redundancy pairing relationship between a Primary Host and a Secondary Host. After creating a device pair, it can be applied to a redundancy Policy and Plan for subsequent monitoring and failover/recovery operations.

Note: A device pair should typically consist of two devices with the same or compatible roles to ensure service continuity after failover.



Step 1: Go to Redundancy > Device Pair, and click  to create a new device pairing. The system first displays the Select Device Pairing step. Select the redundancy pairing type. IRM supports three redundancy modes:

1. Physical-to-Physical
2. Physical-to-Virtual
3. Virtual-to-Virtual

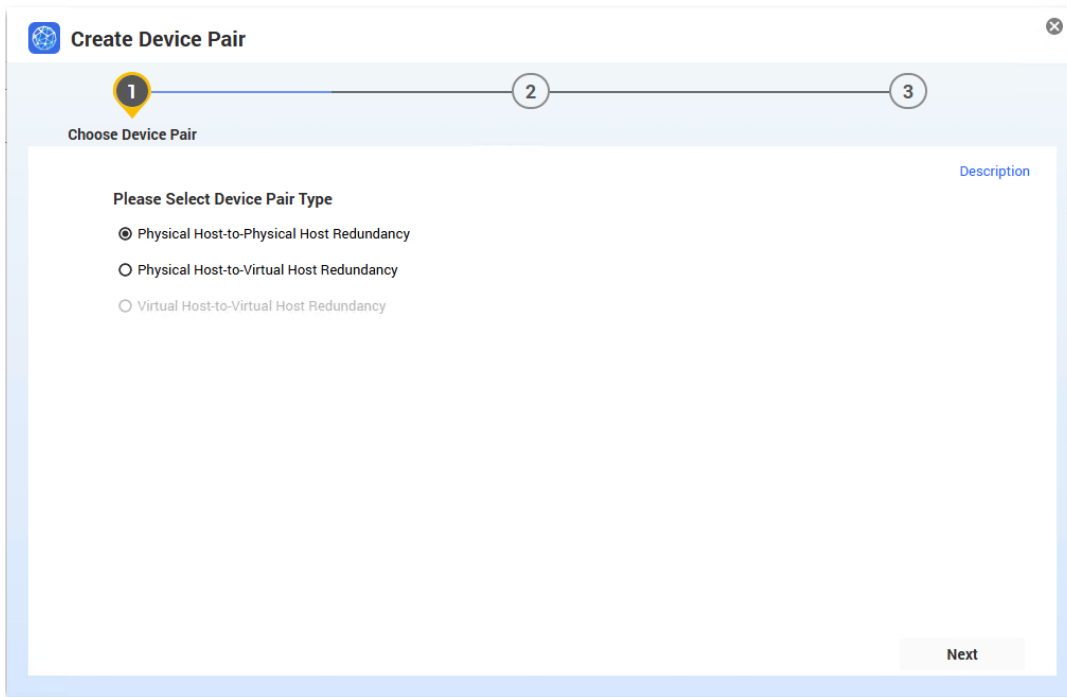
After making your selection, click Next to proceed to Step 2: Set Up Device Pairing.

Create device pairing instructions

Before you begin, make sure the following requirements are met and connectivity between the two hosts is available :

1. The IRM Agent version is the same on both hosts.
2. Both hosts are connected to the IRM server.
3. Both hosts are on the same LAN, and the network supports the UDP protocol.
4. Wake-on-LAN (WOL) is enabled on the standby (backup) host.
5. The standby host has completed all network settings and application auto-start is enabled.
6. The standby host can take over your services after it boots.

7. After the redundancy cluster is enabled, the standby host will enter standby mode and power off.



Step 2: Set Up Device Pairing

After completing Step 1: Select Device Pairing Type, click Next. The system opens the Set Up Device Pairing window.

In this step, configure the pairing information and select the Primary and Secondary hosts.

After selecting the device pairing type, click Next.

Step 3: Set the Pair Name and Description

Pair Name*: Enter the device pairing name.

Pair Description*: Enter the device pairing description.

Step 4: Pairing Host Selection

Only IRM Agent devices can be selected in this step.

- (1) Select Primary Host* → Click Select Host → the Select Device window appears. In the window, select the primary physical host to be paired, and click Confirm.
- (2) Select Secondary Host* → Click Select → the Select Device window appears. In the window, select the secondary physical host to be paired, and click Confirm.

After completing the selections, click Next to proceed to Step 3: Confirm Device Pairing.

Selected Devices

Hostname, IP address, Device tag 🔍 🔄

	Hostname	IP Address	Tag	Manage...	Brand	Model	Operati...
<input checked="" type="checkbox"/>	iei-SJB8	10.10.40.238	TANK_XM811_(i7)	IRMAgent	IEi	13th Gen Intel(R) Core(TM) i7-13700TE	Ubuntu
<input type="checkbox"/>	iei-SJB8	10.10.40.239	TANK_XM811_(i9)	IRMAgent	IEi	13th Gen Intel(R) Core(TM) i9-13900T	Ubuntu
<input type="checkbox"/>	win10_Virtual_...	10.10.40.237	Virtual_Redunda...	IRMAgent	QEMU	Westmere E56xx/L56xx/X56xx (Nehalem...	Micros...
<input type="checkbox"/>	win10_Hybrid_...	10.10.40.235	Hybrid_Slave_OS	IRMAgent	QEMU	Westmere E56xx/L56xx/X56xx (Nehalem...	Micros...
<input type="checkbox"/>	iVEC-Win11	10.10.40.234	Virtual_Win11_OS	IRMAgent	QEMU	Westmere E56xx/L56xx/X56xx (Nehalem...	Micros...

Page 1 of 1 | 1 - 5 of 5 Only list the selected servers or devices.

OK Cancel

Pairing Types Notes:

- Physical-to-Physical : Both the primary and secondary hosts are physical devices.
- Physical-to-Virtual :
 - The primary host is a physical device.
 - The secondary host is an iVEC VM.
- Virtual-to-Virtual: Both the primary and secondary hosts are iVEC VMs.

Step 5: Confirm Device Pairing

After completing Step 2: Set Up Device Pairing, click Next to proceed to Step 3: Confirm Device Pairing.

Verify that the pairing information is correct, including:

- Device Pair Type
- Pairing Device Name / Description
- Primary Host / Secondary Host

After confirming everything is correct, click Save to complete the device pairing. If you need to make changes, go back to the previous step and modify the settings.

Create Device Pair
✕

✓
 Choose Device Pair

✓
 Setup Device Pair

3
Confirm Redundancy Pairing Device

Device Information	Primary Host	Secondary Host
Hostname	iei-SJB8	win10_Hybrid_Slave
IP Address	10.10.40.238	10.10.40.235
MAC Address	00:94:93:14:78:ce	52:54:00:54:B1:C4
Tag	TANK_XM811	Hybrid_Slave_OS
Connect Status	● Online	● Offline

Pairing Information

Pairing Device Name : physical to physical

Pairing Device Description : physical to physical

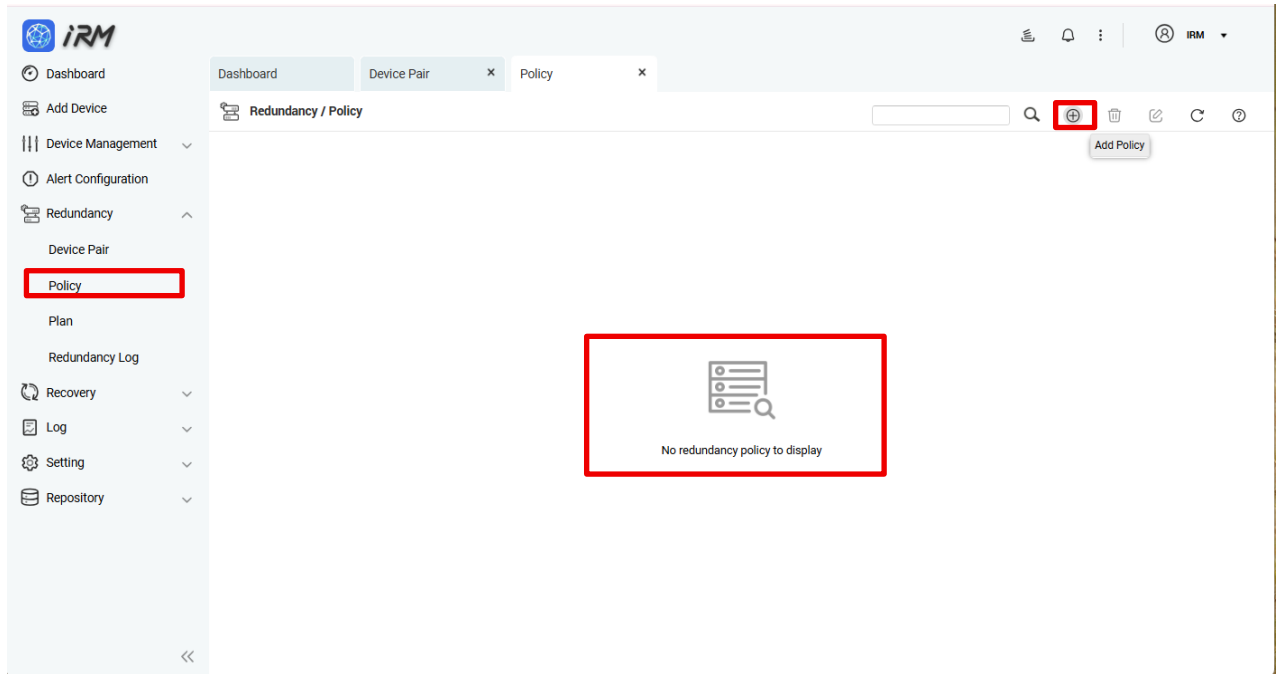
Device Pair Type

Physical Host-to-Physical Host Redundancy

Previous
Save

7.2 Policy

A Policy defines the monitoring criteria and decision rules used by a Redundancy Plan. Users can create a policy by specifying the protection type, sensor/monitoring item, trigger condition, how long the condition must persist to be considered valid (Stay Duration), and the retry timer.



Step 1: Add Policy

Go to Redundancy > Policy and click Add Policy (+). The system opens the Add Policy window. Configure the following fields in order.

1. Policy Name: Enter the policy name.
2. Description: Enter the policy description.
3. Protection Type: Select the protection type (host-level protection) for host level accessible detection. This system adds different levels of protection modes in the future.
4. Sensor Type: Select the sensor type (power status). This system adds different sensor type of protection modes in the future.
5. Condition: Select the condition (Power On → Power Off).
6. Duration: Enter 0–60 minutes and 10–59 seconds.
7. Retry Time: Enter 2–10 minutes for fail to enable the secondary node and iRM retry again in this duration.

After confirming the settings, click Save to add the policy. To exit without adding, click Cancel.

Add Policy ✕

Policy Name *

Description *

Protection Type *

Sensor Type *

Condition *

Stay Duration * minutes seconds

Retry Timer * minutes

Note: After a policy is created, it can be selected and applied when creating a **Plan**.

7.3 Plan

A **Plan** combines a **Device Pair** and a **Policy** into an executable redundancy configuration. After a plan is created, the system monitors the primary host based on the selected policy. When the condition is met, the plan performs redundancy handling, and the event/results can be reviewed in the **Redundancy Log**. Users can also manage the plan by enabling or disabling it.

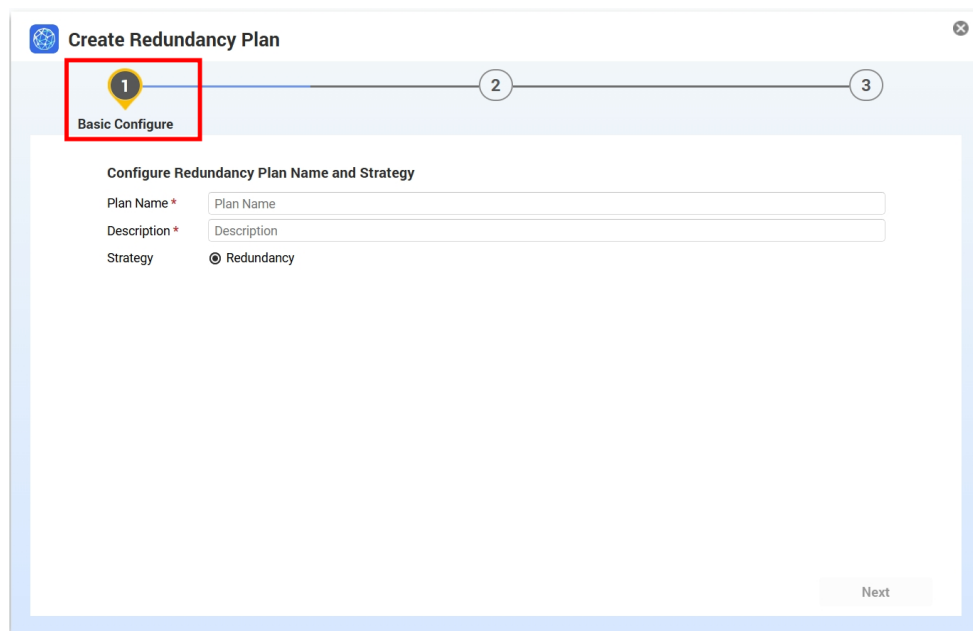
The screenshot shows the iRM web interface. On the left sidebar, the 'Plan' menu item is highlighted with a red box. The main content area shows a 'Redundancy / Plan' view with a search bar and a 'Create Redundancy Plan' button. A red box highlights a message that says 'No redundancy plans to display' with a magnifying glass icon over a list of items.

Step 1: Basic Settings

Go to Redundancy > Plan, and select Add to create a new backup plan. The system will open the plan creation wizard page. Please complete the basic information settings for the plan in Step 1: Basic Settings, including:

1. Plan Name*: Enter the backup plan name.
2. Description: Enter the plan description (optional).
3. Strategy: Select the strategy type. The default here is Redundancy.

Once finished, click Next to proceed to the next setting; to return to the previous page, click Previous.

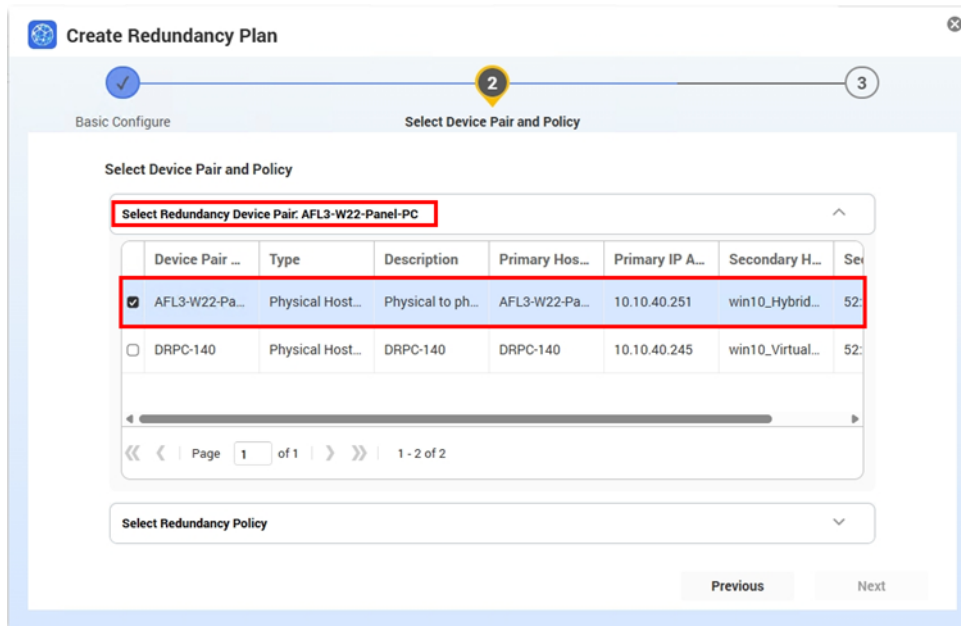


Step 2: Select Device Pair and Policy

After completing Step 1: Basic Configuration, click Next to proceed to Step 2: Select Device Pair and Policy. In this step, specify the Device Pair and Policy to be applied to this redundancy plan.

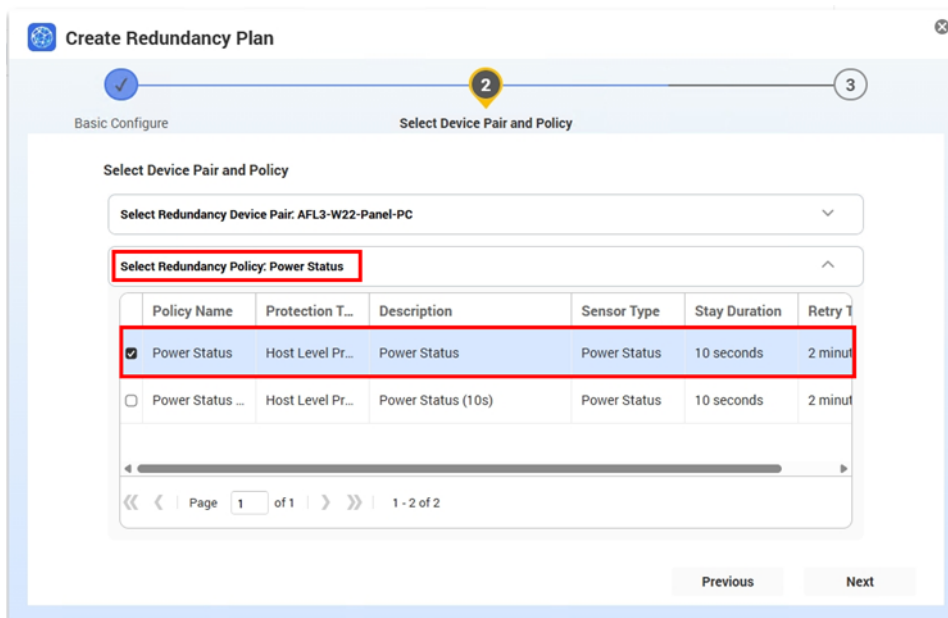
- Select Redundancy Device Pair

1. In the Select Redundancy Device Pair section, click the drop-down list to expand the pairing list.
2. Select the device pair to apply. The list displays pairing details for verification, such as Type, Description, Primary Hostname/IP, and Secondary Hostname.



- **Select Redundancy Policy**

1. In the Select Redundancy Policy section, click the drop-down list to expand the policy list.
2. Select the policy to apply. The list displays policy details for verification, such as Policy Name, Protection Type, Sensor Type, Stay Duration, and Retry Timer.



完成 Device Pair 與 Policy 選擇後，點選 Next 進入 Step 3；若需返回上一頁，點選 Previous。

Step 3: Summary

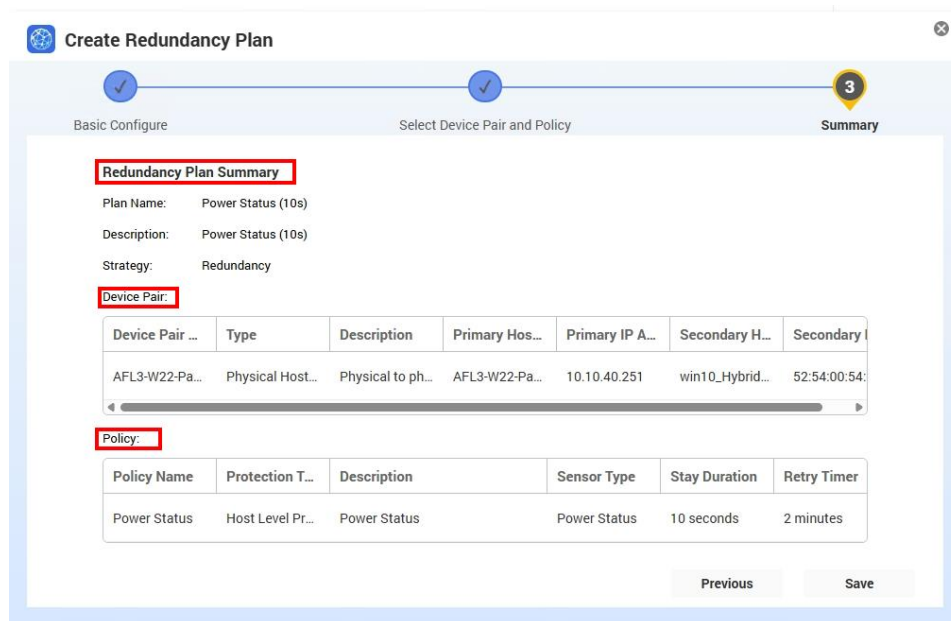
After selecting the Device Pair and Policy, click Next to proceed to Step 3. To return to the previous page, click Previous.

Step 3: Summary

After completing Step 2: Select Device Pair and Policy, click Next to open Step 3: Summary. Verify that the following information is correct:

- Redundancy Plan Summary: Plan Name / Description / Strategy
- Device Pair: The primary/secondary host pairing information applied to this plan
- Policy: The policy information applied to this plan (e.g., Policy Name, Sensor Type, Stay Duration, Retry Timer)

After confirming everything is correct, click Save to create the redundancy plan. If changes are needed, click Previous to go back and modify the settings.



Redundancy Plan Summary

Plan Name: Power Status (10s)
 Description: Power Status (10s)
 Strategy: Redundancy

Device Pair:

Device Pair ...	Type	Description	Primary Hos...	Primary IP A...	Secondary H...	Secondary
AFL3-W22-Pa...	Physical Host...	Physical to ph...	AFL3-W22-Pa...	10.10.40.251	win10_Hybrid...	52:54:00:54:

Policy:


Policy Name	Protection T...	Description	Sensor Type	Stay Duration	Retry Timer
Power Status	Host Level Pr...	Power Status	Power Status	10 seconds	2 minutes

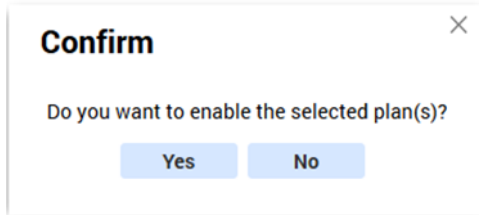
Previous Save


Step 4: Enable/Disable Redundancy Plan


On the Redundancy/Plan page, users can enable or disable existing redundancy plans to control whether the redundancy mechanism is active.


Steps

- 1). Click Redundancy -> Plan in the left menu to enter the Redundancy Plan list page.
- 2). Select the redundancy plan you want to manage from the list.
- 3). Enable: Click the Enable Redundancy Plan button  on the toolbar.



After the plan is enabled, its status will be displayed as  Enabled, and you can view it by selecting Enabled / Disabled at the top.

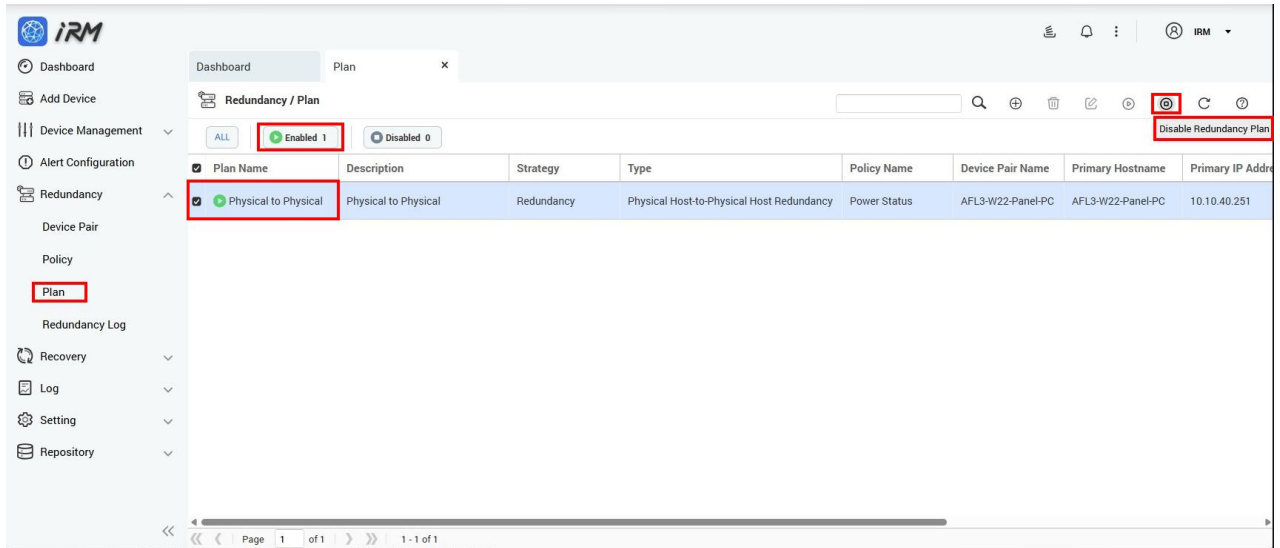
- 4). Disable: Click the Disable Redundancy Plan button  on the toolbar.

After the plan is disabled, its status will be displayed as  Disabled, and you can view it by selecting Enabled / Disabled at the top.

The screenshot shows the iRM interface with the following details:

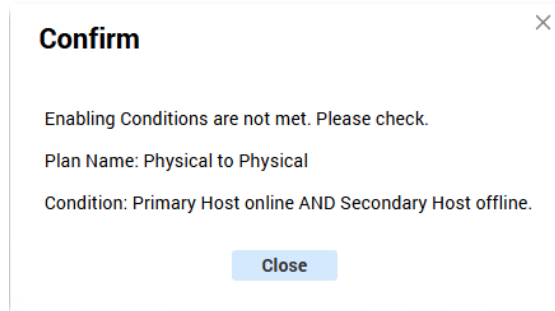
- Left Menu:** Dashboard, Add Device, Device Management, Alert Configuration, Redundancy (expanded), Device Pair, Policy, Plan (highlighted), Redundancy Log, Recovery, Log, Setting, Repository.
- Toolbar:** Search, Add, Delete, Edit, Enable (highlighted), Disable, Refresh, Refresh.
- Filters:** ALL, Enabled 0, Disabled 1 (highlighted).
- Table:**

Plan Name	Description	Strategy	Type	Policy Name	Device Pair Name	Primary Hostname
<input checked="" type="checkbox"/> Physical to Physical	Physical to Physical	Redundancy	Physical Host-to-Physical Host Redundancy	Power Status	AFL3-W22-Panel-PC	AFL3-W22-Panel-P
- Footer:** Page 1 of 1, 1 - 1 of 1



Note:

1. When you click Enable Redundancy Plan, if the activation conditions are not met, the system will display a prompt message explaining the reason.
2. It will only execute automatically once, and will only re-enter the running state after being restarted by the user manually.
3. **Enable conditions:** The primary host must be powered on, and the secondary host must be powered off. Please go to Device Management to confirm that the secondary host is powered off, and then return to enable the redundancy plan.

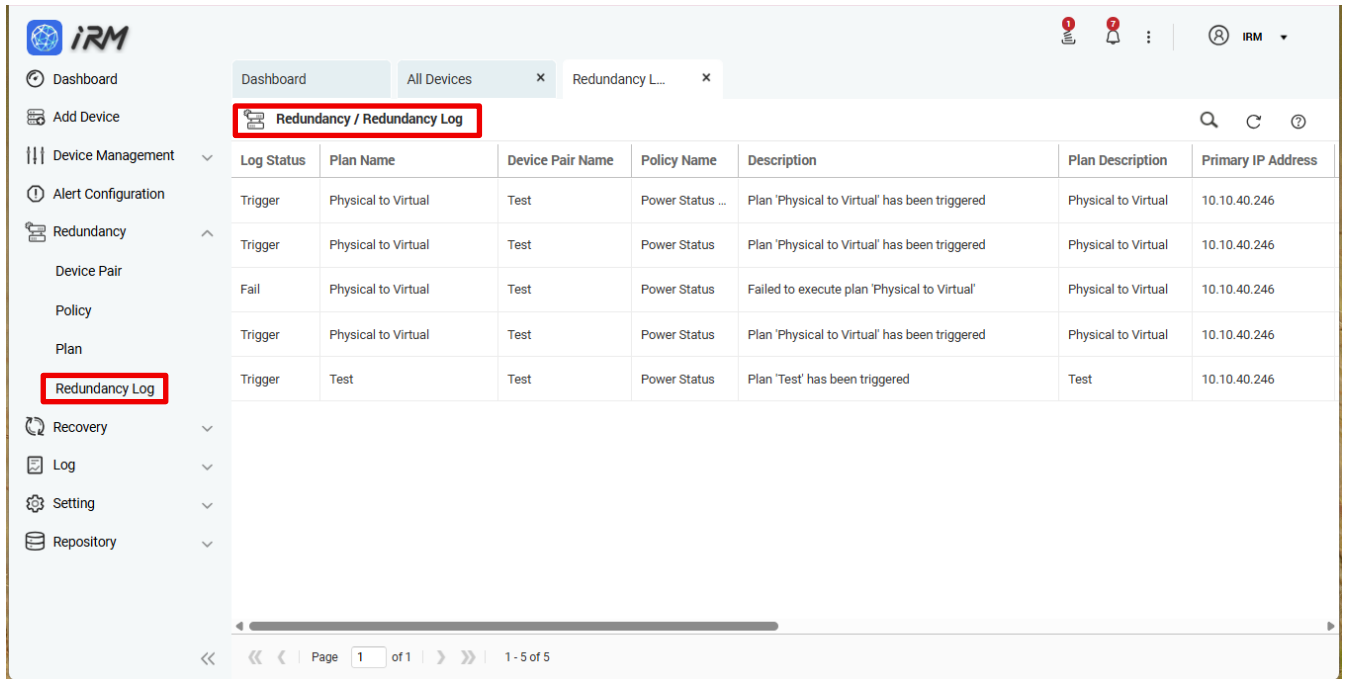


7.4 Redundancy Log

The Redundancy Log is used to view and track records of redundancy operations. After a Plan is enabled, the system monitors the primary host status based on the Policy. When a trigger event occurs or a redundancy action is executed, the related information is recorded in the Redundancy Log, allowing administrators to perform auditing, troubleshooting, and status tracking.

The Redundancy Log typically includes (as shown on the screen): the trigger time, plan name, device pair, primary/secondary host information, trigger condition, and the processing result/status.

How to access the Redundancy Log: On the Redundancy page, select Redundancy Log.



Log Status	Plan Name	Device Pair Name	Policy Name	Description	Plan Description	Primary IP Address
Trigger	Physical to Virtual	Test	Power Status ...	Plan 'Physical to Virtual' has been triggered	Physical to Virtual	10.10.40.246
Trigger	Physical to Virtual	Test	Power Status	Plan 'Physical to Virtual' has been triggered	Physical to Virtual	10.10.40.246
Fail	Physical to Virtual	Test	Power Status	Failed to execute plan 'Physical to Virtual'	Physical to Virtual	10.10.40.246
Trigger	Physical to Virtual	Test	Power Status	Plan 'Physical to Virtual' has been triggered	Physical to Virtual	10.10.40.246
Trigger	Test	Test	Power Status	Plan 'Test' has been triggered	Test	10.10.40.246

Chapter

8

8 Recovery

8.1 Remote Recovery

IRM provides remote recovery for IEI physical hosts via **OneKey Recovery 2 (OKR2)**. When a target host encounters an issue or requires rapid OS restoration, administrators can trigger the OS recovery process through the IRM interface to reduce downtime and improve system availability. One IEI physical host can backup Max 3 copies OS backup image in same storage with the OS. IRM can let end user remote trigger and selection one of 3 copies OS backup image to process OS restoration.

Before you begin, make sure the target host has **OKR2** properly installed and enabled, and that the **OKR2 Support icon** is displayed in the IRM device list.


Prerequisites

1. Supported Scope

IRM supports remote recovery only for **IEI physical hosts (IPCs)** running **Windows**. Remote recovery is not supported on non-IEI platforms or on devices running **Linux OS**.

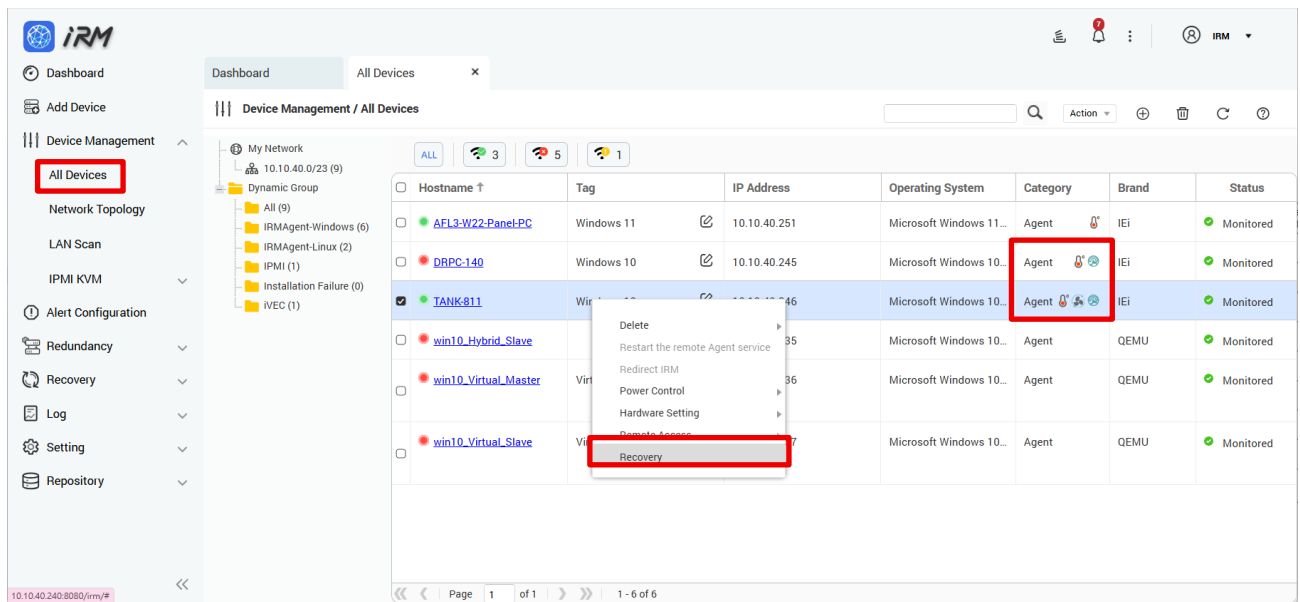
2. Confirm OKR2 Installation Status

Before using Remote Recovery, go to Device Management > All Devices > IRMAgent-Windows and confirm that the target host shows the OKR2 Support icon. If the icon is not displayed, IRM cannot perform remote recovery on the host.

**OKR2 Support ICO  ** : Indicates that OKR2 has been installed on the IEI host.

3. OKR2 Installation and Image Creation

For OKR2 installation steps and how to create a recovery image, refer to the 《OneKey Recovery2 User Manual》 .



Step 1: Open the Device List and Start Recovery

1. Go to **Device Management > All Devices**. In the left-side group list, switch to **IRMAgent-Windows** to quickly locate Windows hosts that support OKR2.
2. In the device list, confirm that the target host displays the **OKR2 Support** icon.
3. Right-click the target host row, then select **Recovery** from the context menu to start the remote recovery process.



Step 2: Before Start Recovery

1. The system displays the Before Start Recovery window and checks whether the target device has an available recovery image.
2. Under Selected Device, confirm that the device status shows Recoverable.
3. Click Next to proceed to the next step.

The screenshot shows a window titled "Remote Recovery" with a close button in the top right corner. Below the title bar is a grey header with a red-bordered box containing a red circle with the number "1" and the text "Select Recovery Image". The main content area has the heading "Please Select Recovery Image". Underneath, there is a "Host" section with a green status indicator, "Name: DRPC-140", and "Tag: Hybrid_Master_OS". To the right is a "Recovery Image" section with a red-bordered box containing a dropdown menu. The dropdown menu is currently open, showing three options: "Please Select Recovery Image", "User image 1 (2025-12-03 09:22:48)", and "Factory (2025-12-03 09:08:00)". At the bottom right of the window is a "Next" button.

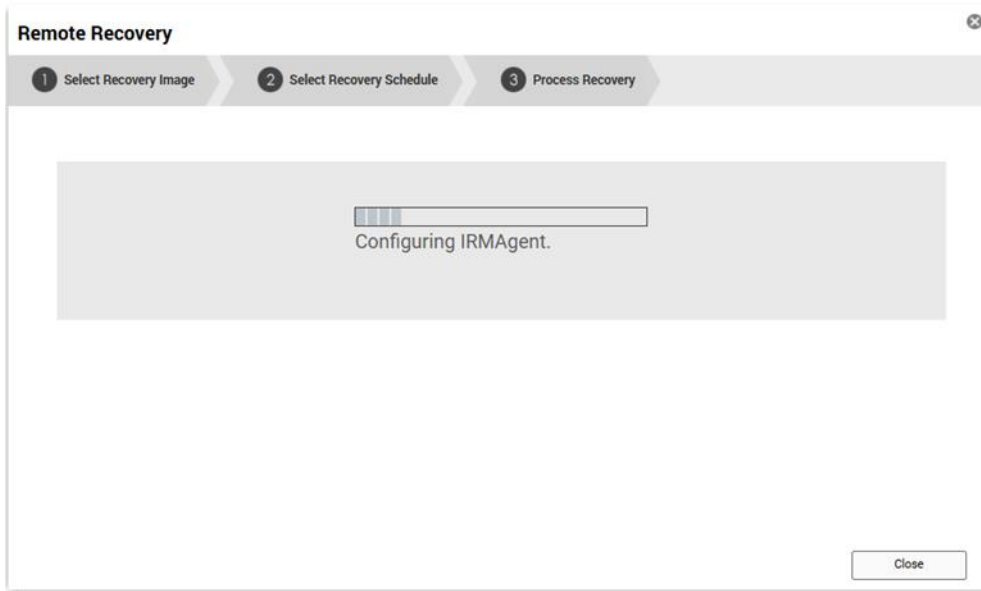
Step 3: Select Recovery Image

1. From the Recovery Image drop-down list, select the image to apply (for example, User image 1 or Factory).
2. Click Next to proceed to the next step.

The screenshot shows a window titled "Remote Recovery" with a close button in the top right corner. Below the title bar is a progress indicator with two steps: "1 Select Recovery Image" and "2 Select Recovery Schedule", where the second step is active. The main content area is titled "Please Select Recovery Schedule". On the left, under the heading "Host", there is a green dot next to the text "Name : TANK-811" and "Tag : Windows 10". On the right, under the heading "Recovery Schedule", the text "Current system time: 2026-01-05 13:56:41" is displayed. Below this, there are two radio button options: "Now" (which is selected) and "Scheduled". The "Scheduled" option is followed by a date and time picker showing "00 : 00". At the bottom right of the window, there are two buttons: "Previous" and "Next".

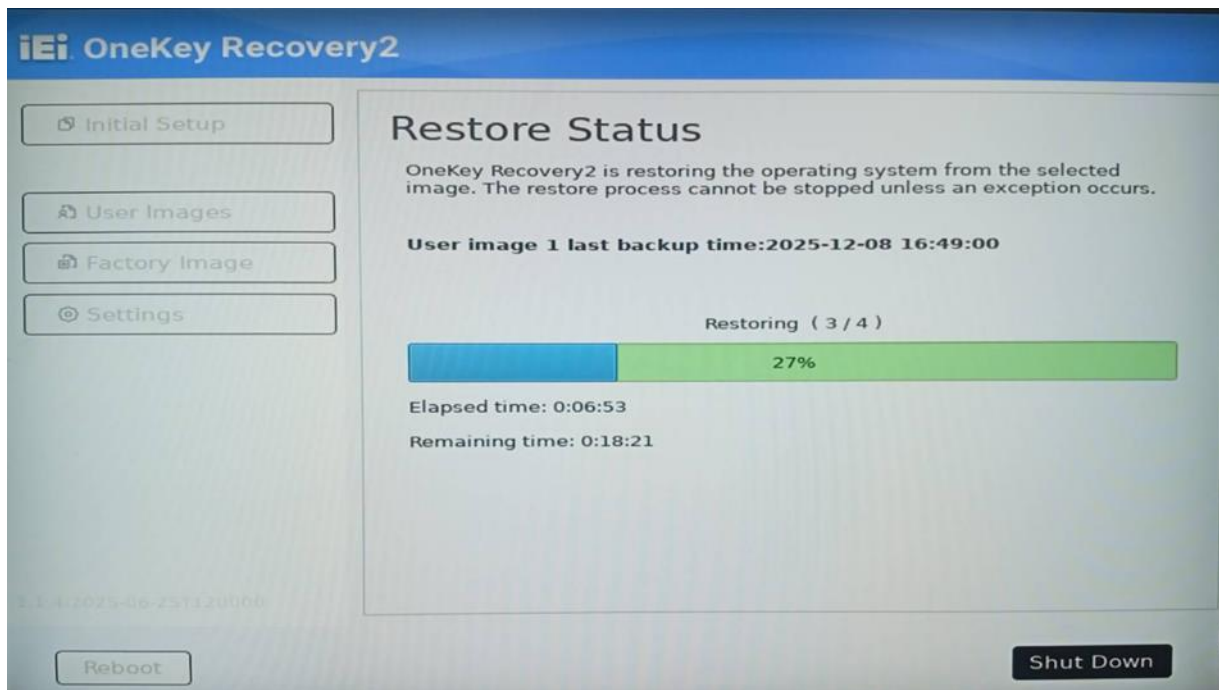
Step 4: Select a Recovery Schedule

1. Under **Recovery Schedule**, choose how to run the recovery:
 - **Now:** Run recovery immediately.
 - **Scheduled:** Run recovery at a specified date and time (the **Current system time** is shown on the right for reference).
2. After completing the settings, click Next to start the process.

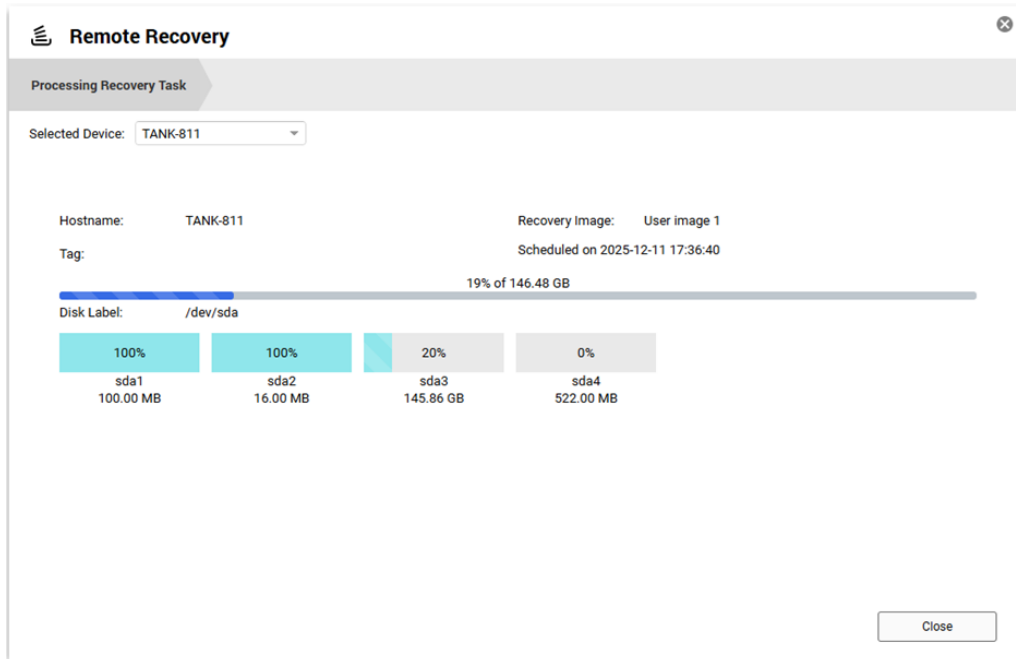


Step 5: Process Recovery

1. The system enters **Process Recovery** and displays status messages (for example, **Configuring IRMAgent**), indicating that IRM is configuring the IRM Agent and preparing to trigger the recovery task.
2. After the recovery is triggered, the target host will reboot automatically and start the **OneKey Recovery 2 (OKR2)** recovery process, restoring the selected image to the system disk.



Step 6: Processing Recovery Task



Remote Recovery

Processing Recovery Task

Selected Device: TANK-811

Hostname: TANK-811 Recovery Image: User image 1

Tag: Scheduled on 2025-12-11 17:36:40

19% of 146.48 GB

Disk Label: /dev/sda

Partition	Progress	Size
sda1	100%	100.00 MB
sda2	100%	16.00 MB
sda3	20%	145.86 GB
sda4	0%	522.00 MB

Close

During recovery, you can view detailed information on the **Processing Recovery Task** page:

- **Selected Device:** The device currently performing recovery
- **Hostname / Tag:** Device identification information
- **Recovery Image / Scheduled on:** The image used for this recovery and the scheduled time
- **Overall Progress:** Percentage and data volume (e.g., **19% of 146.48 GB**)
- **Disk Label:** Target disk (e.g., **/dev/sda**)
- **Partition Progress:** Recovery progress for each partition (**sda1 / sda2 / sda3 / sda4**)

At the same time, the target host will display the **OKR2 Restore Status** screen, where you can view the restoring progress, **Elapsed time**, **Remaining time**, and other details.

After the recovery is completed, click **Close** to close the window and return to IRM.

Note:

1. After you click Confirm and Set Recovery, the target device will reboot automatically and enter the OKR2 recovery process. If a schedule time is set, the device will automatically enter recovery mode at the specified time and start the recovery.

2. After the user logs in to the system, it is recommended to pause or disable Windows Update to avoid affecting the recovery process and reporting time.
3. If the client device does not report the OKR2 execution status/report for a period of time, IRM may consider the OKR2 recovery to have failed. Prolonged Windows updates may delay status reporting and cause IRM to misjudge the recovery result.

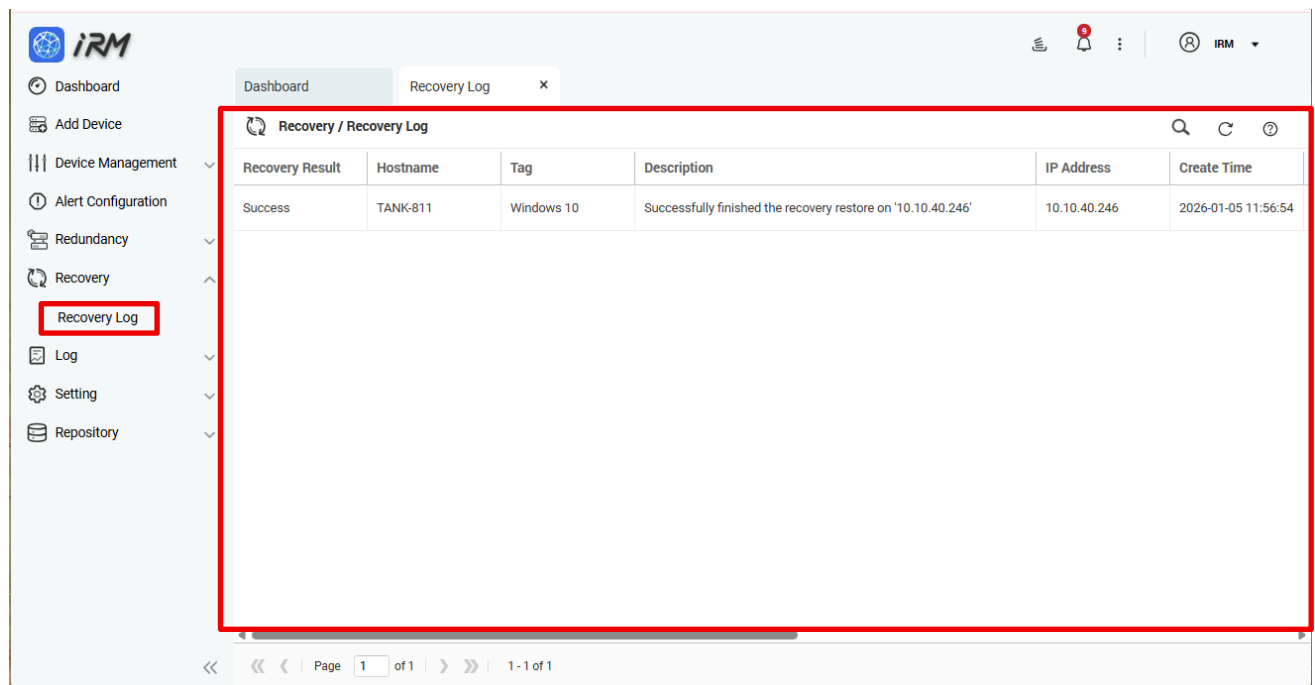
8.2 Recovery Log

The **Recovery Log** is used to record and query the execution history and results of **remote recovery (OKR2 Remote Recovery)**. After an administrator initiates a recovery task, IRM writes key task information to the log, making it easier to track recovery status, confirm whether it succeeded, and troubleshoot issues later.

The Recovery Log typically includes (as shown on the screen):

- Device information: Hostname, Tag, IP, etc.
- Recovery details: The applied Recovery Image (User image / Factory) and the schedule option (Now / Scheduled)
- Task status: Start/end time, execution result (Success / Failed), and error reason/messages (if any)

How to access the Recovery Log: On the Recovery page, select Recovery Log.



Recovery Result	Hostname	Tag	Description	IP Address	Create Time
Success	TANK-811	Windows 10	Successfully finished the recovery restore on '10.10.40.246'	10.10.40.246	2026-01-05 11:56:54

Chapter

9

9 Logs

Logs provides centralized access to system, device, and event records, helping administrators troubleshoot issues, track events, and perform audits. This feature includes the following log types:

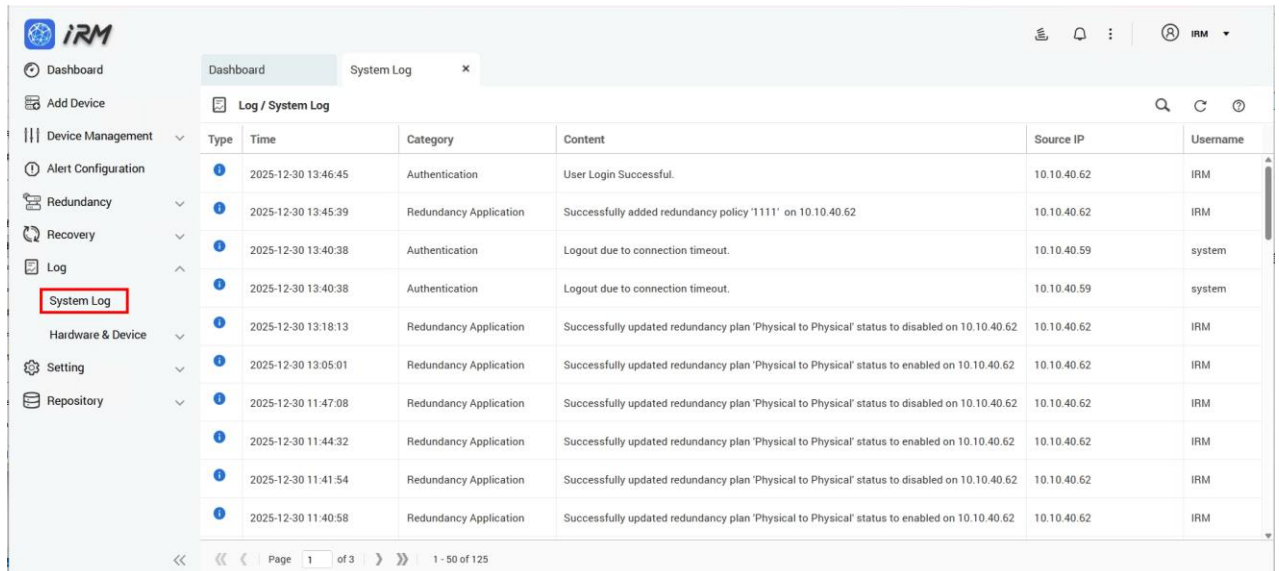
- **System Log:** Records system-level events and operating status.
- **Agent Alert Log:** Aggregates alert events reported to IRM by Agents on managed devices.
- **IPMI Alert Log:** Records alert events triggered by IPMI (IEI iRIS) monitoring items.
- **IPMI Event List:** Displays event logs reported by IPMI devices.
- **Historical Data Log:** Stores historical records of monitored values or system-collected data.

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).

9.1 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".

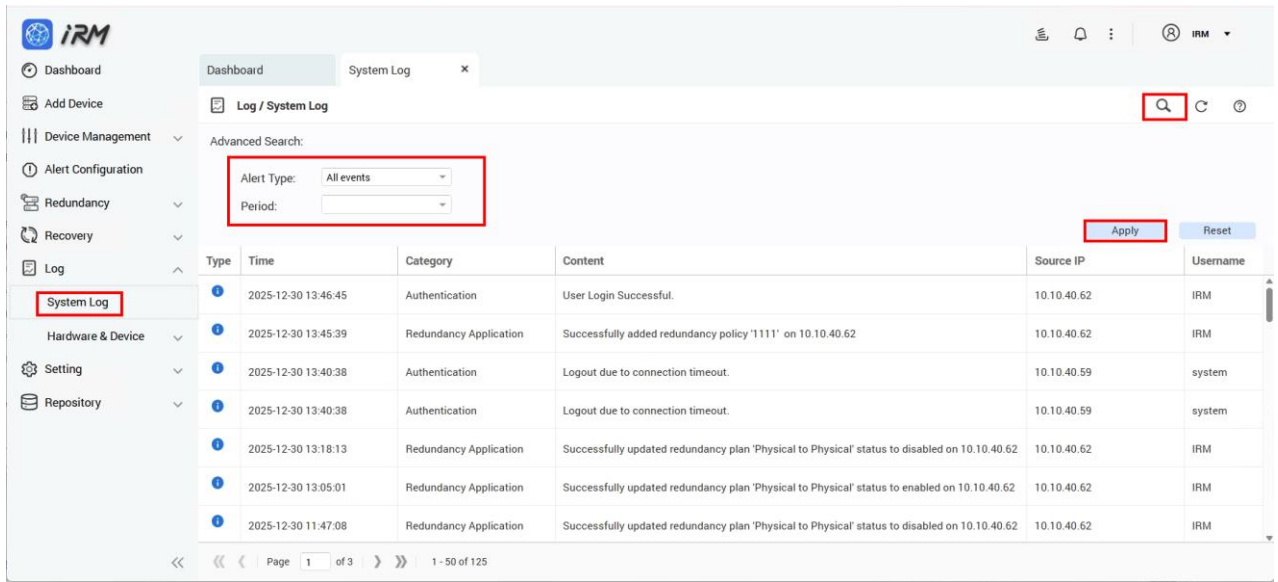


Type	Time	Category	Content	Source IP	Username
●	2025-12-30 13:46:45	Authentication	User Login Successful.	10.10.40.62	IRM
●	2025-12-30 13:45:39	Redundancy Application	Successfully added redundancy policy '1111' on 10.10.40.62	10.10.40.62	IRM
●	2025-12-30 13:40:38	Authentication	Logout due to connection timeout.	10.10.40.59	system
●	2025-12-30 13:40:38	Authentication	Logout due to connection timeout.	10.10.40.59	system
●	2025-12-30 13:18:13	Redundancy Application	Successfully updated redundancy plan 'Physical to Physical' status to disabled on 10.10.40.62	10.10.40.62	IRM
●	2025-12-30 13:05:01	Redundancy Application	Successfully updated redundancy plan 'Physical to Physical' status to enabled on 10.10.40.62	10.10.40.62	IRM
●	2025-12-30 11:47:08	Redundancy Application	Successfully updated redundancy plan 'Physical to Physical' status to disabled on 10.10.40.62	10.10.40.62	IRM
●	2025-12-30 11:44:32	Redundancy Application	Successfully updated redundancy plan 'Physical to Physical' status to enabled on 10.10.40.62	10.10.40.62	IRM
●	2025-12-30 11:41:54	Redundancy Application	Successfully updated redundancy plan 'Physical to Physical' status to disabled on 10.10.40.62	10.10.40.62	IRM
●	2025-12-30 11:40:58	Redundancy Application	Successfully updated redundancy plan 'Physical to Physical' status to enabled on 10.10.40.62	10.10.40.62	IRM

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.



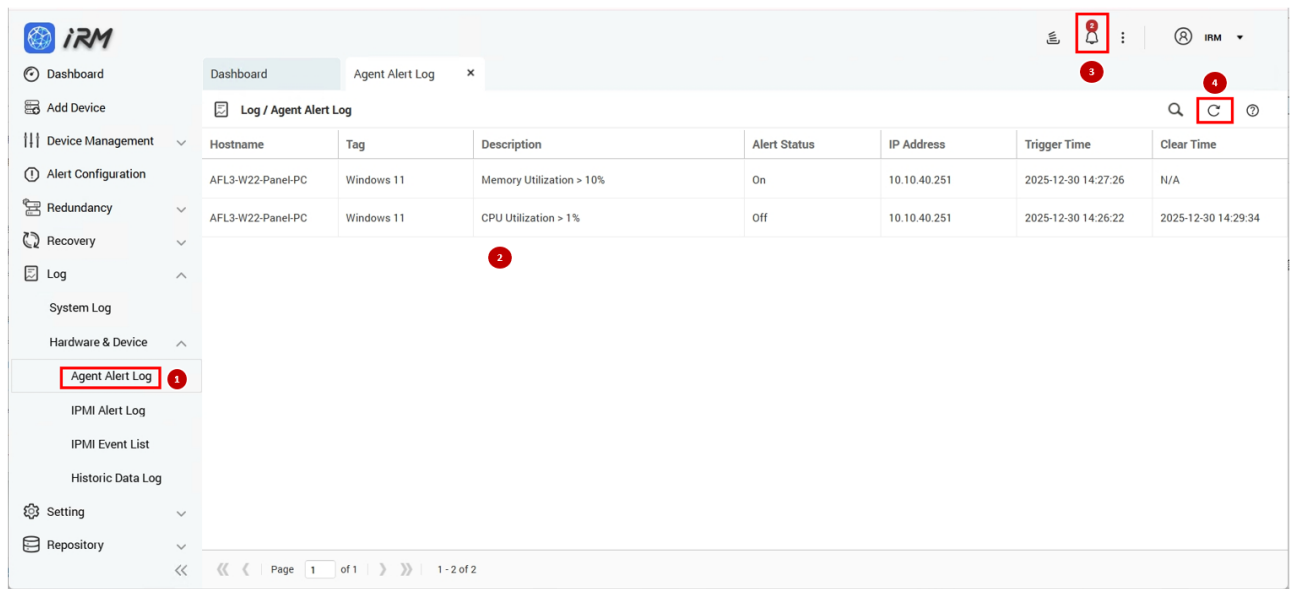
9.2 Hardware & Device

9.2.1 Agent Alerts Log

IRM Alerts Log page displays alerts for all Windows or Linux devices. Users need to select IRM Alerts from the **Alert Configuration** 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 **Agent Alerts Log** in the Logs page.
- Step 2:** View the agent alert info, including the Hostname, Tag, Description and Alert Status etc.
- Step 3:** View the current number of alerts.
- Step 4:** Click the "Refresh" button at any time to get the latest alert message.

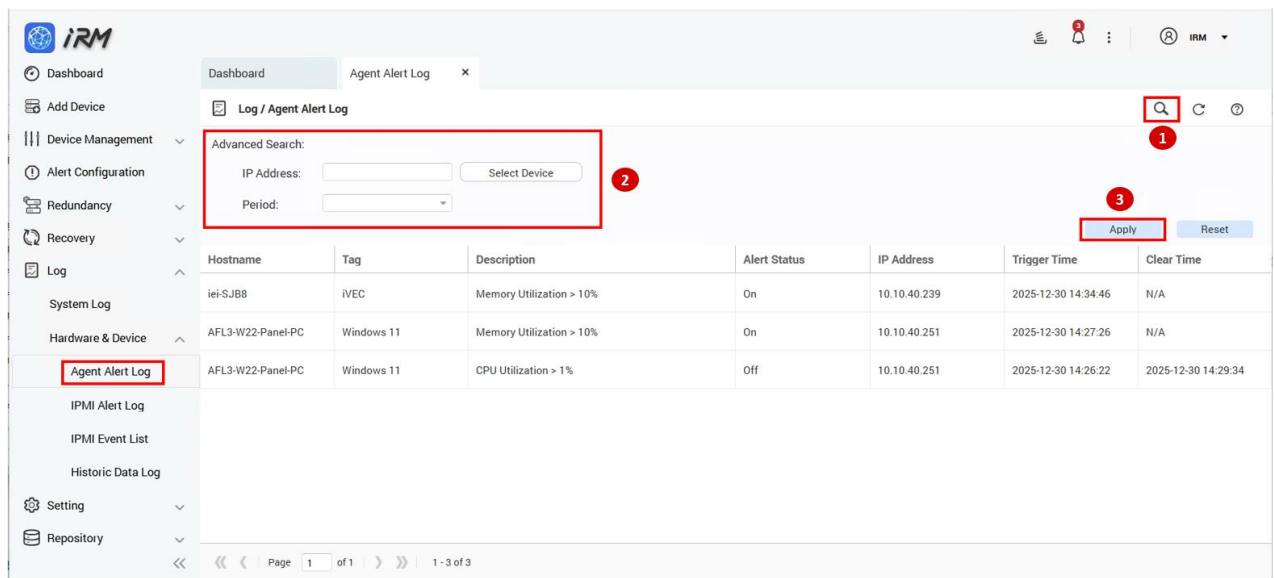


The Agent Alerts Log has advanced search features:

Step 1: Click the "Search Device" button on the Agent 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.



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 10.3 Application Settings.

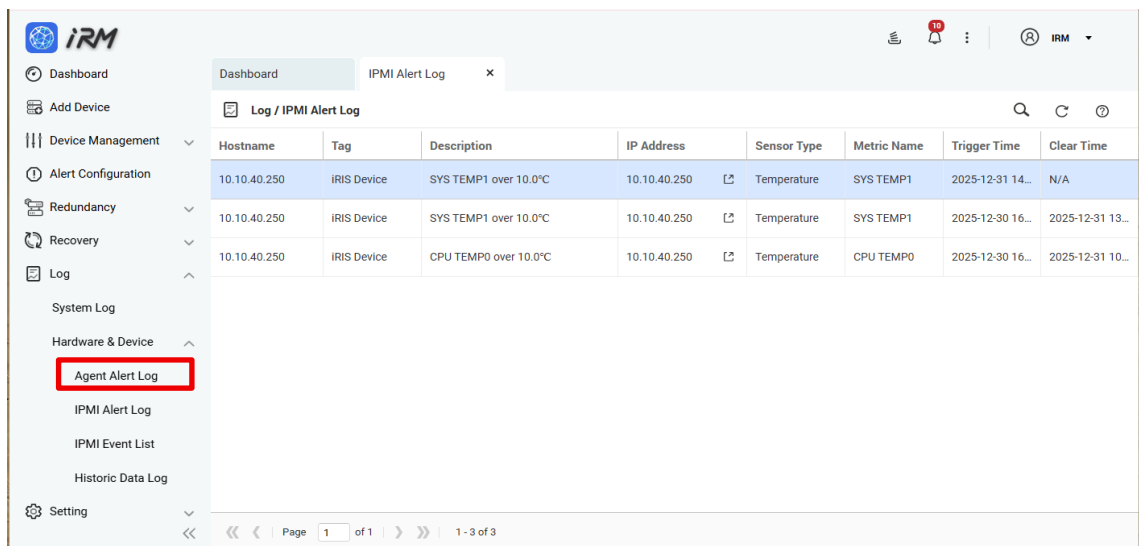
9.2.2 IPMI Alert Log

The **IPMI Alert Log** page displays IPMI sensor alert events (such as temperature, voltage, or power status) for all managed **iRIS** devices. You must first create and enable an **IPMI Alert** rule in **Alert Configuration**. After an event is triggered, you can view the alert details on this page.

Before records can appear in **IPMI Alert Log**, complete the following setup:

1. Add the iRIS device to IRM management : Go to **Add Device**, select **IEI iRIS Device**, add it by **IP address**, and configure the management account.
2. Go to **Alert Configuration**, click **Add (+)**, create an **IPMI Alert**, and apply it to the target iRIS device after configuring the following items:
 - Alert Name
 - Sensor Type : Temperature / Voltage / Power
 - Sensor Name : Displayed dynamically based on the selected Sensor Type
 - Temperature : 例如 SYS TEMP1 、 CPU TEMP0
 - Voltage : 例如 DDR 、 CPU CORE0 、 5V 、 12V 、 3V3SB 、 3V3
 - Condition :
 - Temperature : Condition (°C). Set the comparison operator and threshold (range: 0–120).
 - Condition (V). Set < / > and the threshold (range: 0–12.6).
 - Power : Condition (e.g., Power On → Power On / Power On → Power Off)
3. Records are generated only after an event is triggered:

An entry will appear in IPMI Alert Log only after the device status meets the alert condition and triggers an event.



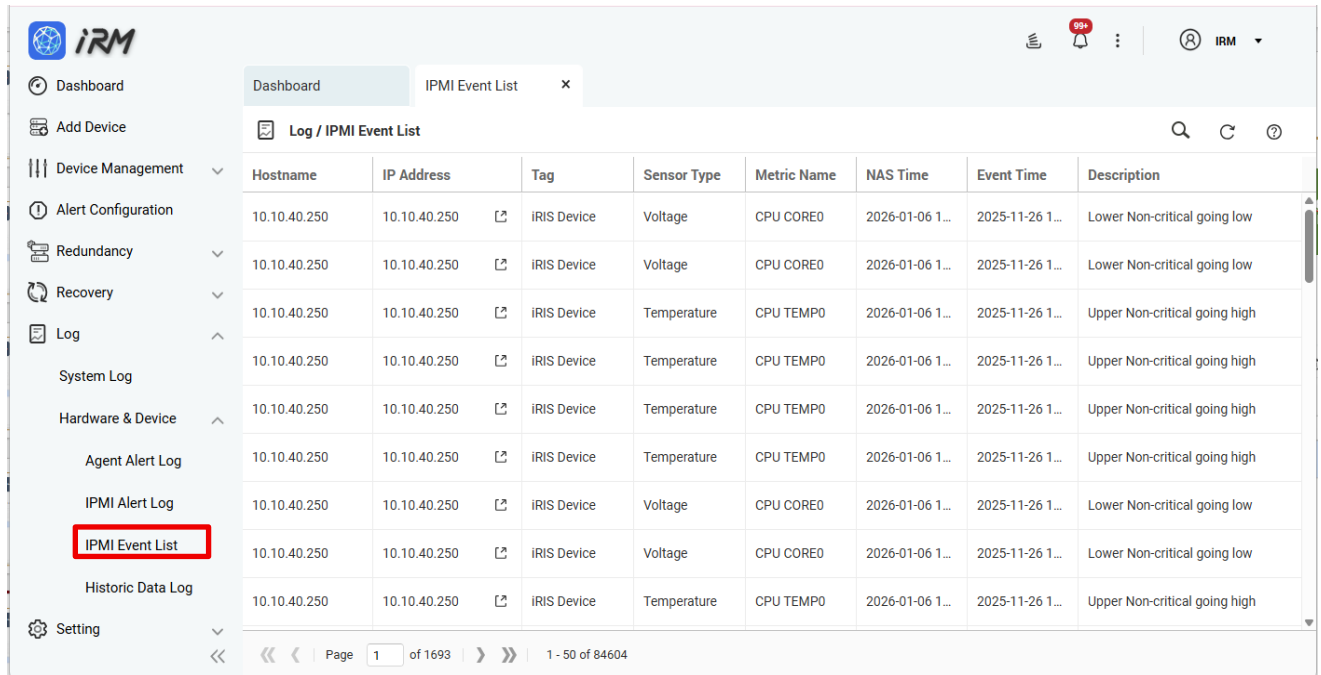
The screenshot shows the iRM web interface with the IPMI Alert Log page open. The left sidebar contains a navigation menu with 'Agent Alert Log' highlighted in a red box. The main content area displays a table of alert events.

Hostname	Tag	Description	IP Address	Sensor Type	Metric Name	Trigger Time	Clear Time
10.10.40.250	iRIS Device	SYS TEMP1 over 10.0°C	10.10.40.250	Temperature	SYS TEMP1	2025-12-31 14...	N/A
10.10.40.250	iRIS Device	SYS TEMP1 over 10.0°C	10.10.40.250	Temperature	SYS TEMP1	2025-12-30 16...	2025-12-31 13...
10.10.40.250	iRIS Device	CPU TEMP0 over 10.0°C	10.10.40.250	Temperature	CPU TEMP0	2025-12-30 16...	2025-12-31 10...

At the bottom of the page, there is a pagination control showing 'Page 1 of 1' and '1 - 3 of 3'.

9.2.3 IPMI Event List

The IPMI Event List provides a centralized view of event logs (Events) reported to IRM by IEI iRIS (IPMI) devices. On this page, administrators can quickly identify abnormal events and threshold status changes for monitored items such as temperature and voltage (for example, Upper Non-critical going high or Lower Non-critical going low) to support tracking and troubleshooting. ◦

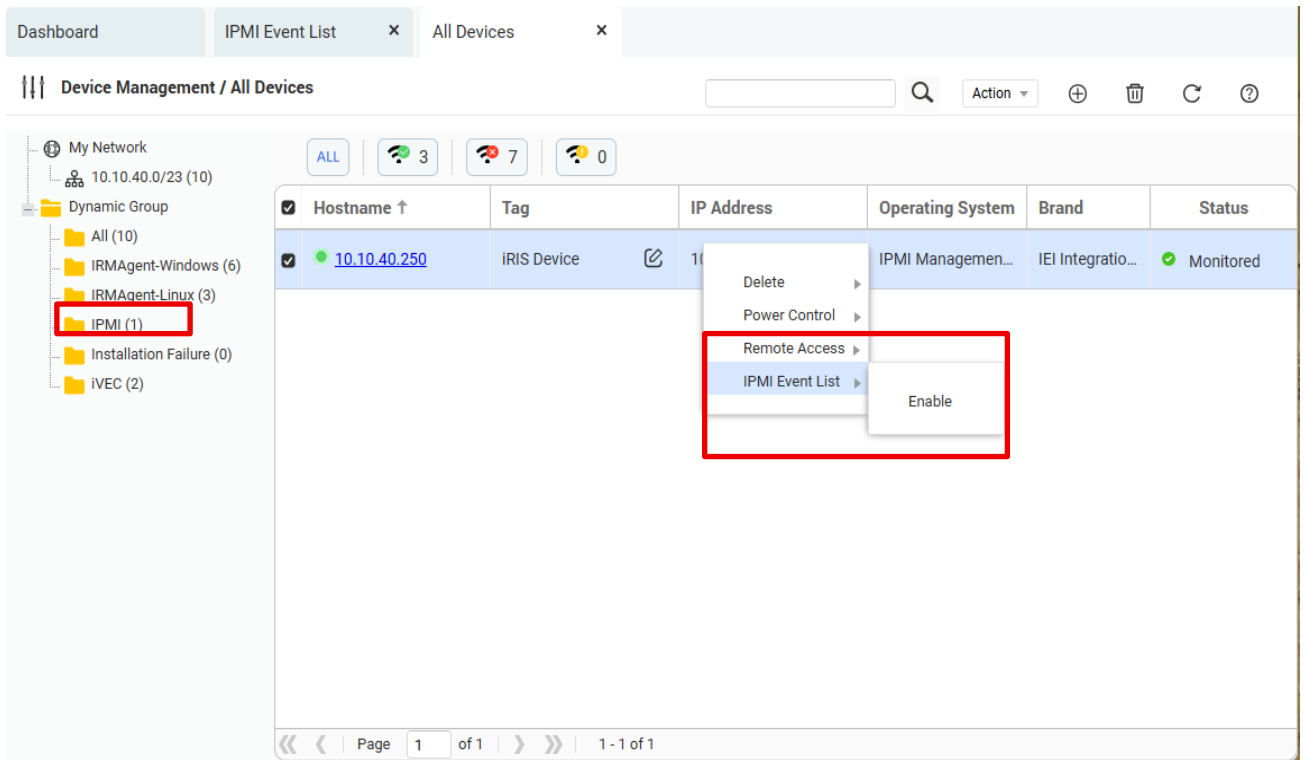


The screenshot shows the IRM web interface with the 'IPMI Event List' tab selected. The left sidebar contains navigation options like 'Dashboard', 'Add Device', 'Device Management', 'Alert Configuration', 'Redundancy', 'Recovery', 'Log', 'System Log', 'Hardware & Device', 'Agent Alert Log', 'IPMI Alert Log', 'IPMI Event List' (highlighted with a red box), and 'Historic Data Log'. The main content area displays a table of event logs with the following columns: Hostname, IP Address, Tag, Sensor Type, Metric Name, NAS Time, Event Time, and Description. The table contains 10 rows of data, all for the IP address 10.10.40.250. The descriptions include 'Lower Non-critical going low' and 'Upper Non-critical going high'. At the bottom, there is a pagination bar showing 'Page 1 of 1693' and '1 - 50 of 84604'.

Hostname	IP Address	Tag	Sensor Type	Metric Name	NAS Time	Event Time	Description
10.10.40.250	10.10.40.250	iRIS Device	Voltage	CPU CORE0	2026-01-06 1...	2025-11-26 1...	Lower Non-critical going low
10.10.40.250	10.10.40.250	iRIS Device	Voltage	CPU CORE0	2026-01-06 1...	2025-11-26 1...	Lower Non-critical going low
10.10.40.250	10.10.40.250	iRIS Device	Temperature	CPU TEMPO	2026-01-06 1...	2025-11-26 1...	Upper Non-critical going high
10.10.40.250	10.10.40.250	iRIS Device	Temperature	CPU TEMPO	2026-01-06 1...	2025-11-26 1...	Upper Non-critical going high
10.10.40.250	10.10.40.250	iRIS Device	Temperature	CPU TEMPO	2026-01-06 1...	2025-11-26 1...	Upper Non-critical going high
10.10.40.250	10.10.40.250	iRIS Device	Temperature	CPU TEMPO	2026-01-06 1...	2025-11-26 1...	Upper Non-critical going high
10.10.40.250	10.10.40.250	iRIS Device	Voltage	CPU CORE0	2026-01-06 1...	2025-11-26 1...	Lower Non-critical going low
10.10.40.250	10.10.40.250	iRIS Device	Voltage	CPU CORE0	2026-01-06 1...	2025-11-26 1...	Lower Non-critical going low
10.10.40.250	10.10.40.250	iRIS Device	Temperature	CPU TEMPO	2026-01-06 1...	2025-11-26 1...	Upper Non-critical going high

Notes

- The target device must be added to IRM and must be a manageable IPMI (iRIS) device.
- Before using the IPMI Event List, make sure IPMI Event reporting for the device is enabled. If it is Disabled, the event list will not be displayed or updated.
- If the event list is not displayed or not updating, go to Device Management > IPMI: Right-click the target IPMI device → IPMI Event List > Enable.
If event reporting is not required, you can select Disable to turn it off.



9.2.4 Historic Data Log

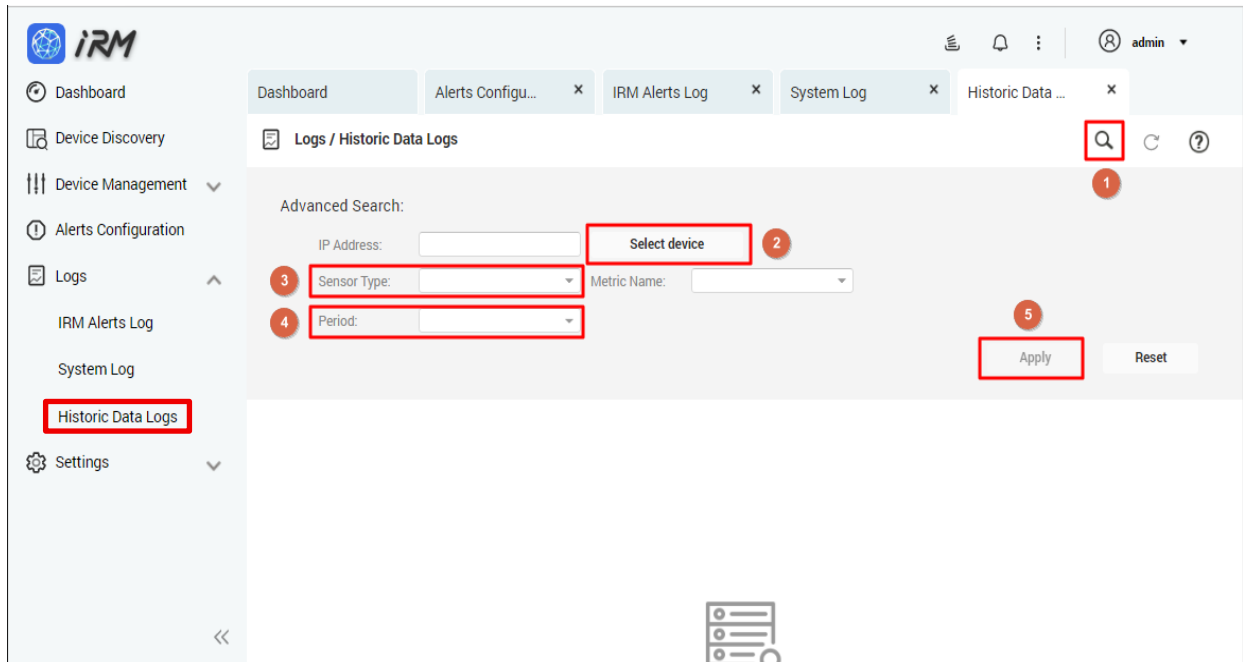
IRM provides historical data obtained by a specific sensor type of a specific device over a specific time frame. For example, a user can select a device, set the period as one day or one week, select the sensor type as CPU usage, then IRM will present the CPU Utilization as a line chart. This feature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

Notes

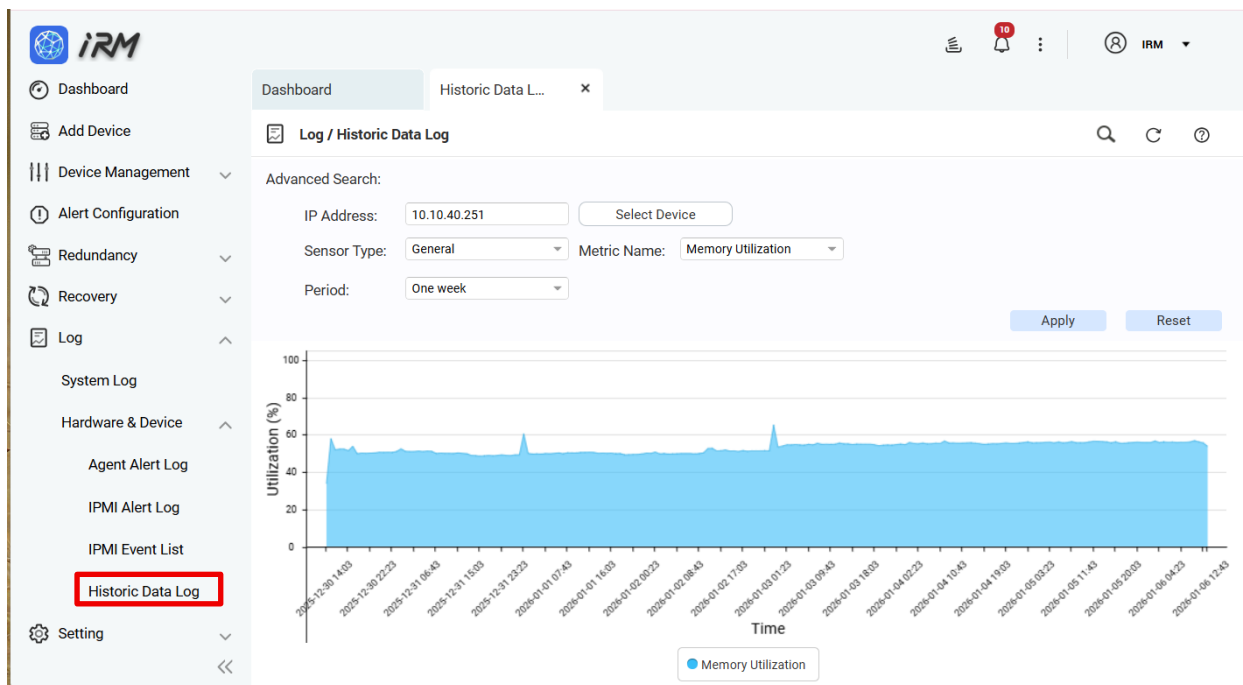
- The maximum query range is 3 months (the longest Period is Three months; Custom is also limited to a maximum of 3 months).

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 **9.3.1 Log Retention Period**.

Chapter

10

10 Settings

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

10.1 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:

Setting / Notification
?

Notification Settings

SMTP Settings

2

Select an Email Account:

3

SMTP Server:

4

SMTP Port:

5

Sender Email ID:

6

Username:

7

Password:

8

Secure Connection:

Alert Notification Settings

9

IRMAGENT alert check interval (minutes):

Note: IPMI event generation frequency will be based on BMC settings, IRM will just poll for new IPMI events and display them.

10

Enable Email notifications for IRMAGENT and IPMI Alerts

11

IRMAGENT and IPMI Alert check interval (minutes) for sending email notifications:

Notification Group

	Username	Role	Email
1	admin	Admin	

12

Notification Center

With Notification Center, you can quickly create custom notification rules to monitor the events on your devices and address potential issues more effectively. Ensure that you select "Set as dedicated rule" when creating notification rules in Notification Center. When this option is enabled, any changes made to rules will be automatically applied to and synced between IRM and Notification Center.

Status	Name	Delivery Method	Recipient	Action
<div style="text-align: center;"> <p>Configure Notification Rule</p> </div>				

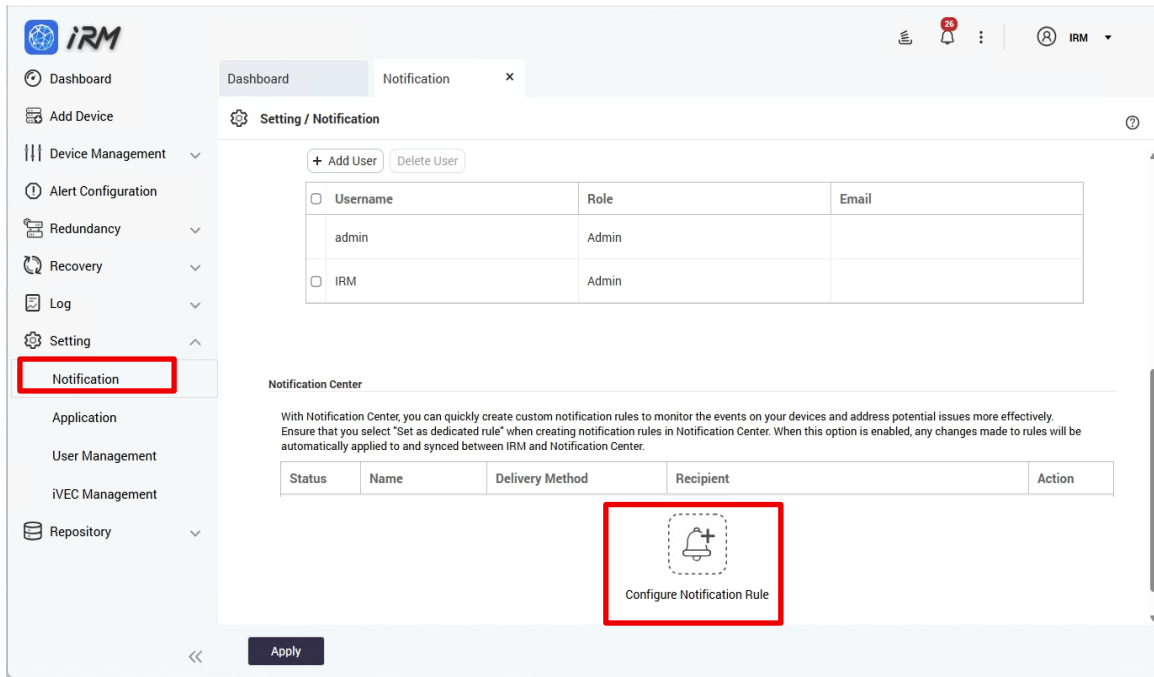
1. The list of accounts that need to be notified
2. SMTP type
3. SMTP server location
4. SMTP server port
5. Email Address
6. E-mail account
7. E-mail password
8. Secure connection mode
9. Sets how often IRM checks alert status at a fixed interval.
10. Whether to enable e-mail sent Agent alert
11. Time interval for sending repeat alerts
12. Notification Center

Notification Center

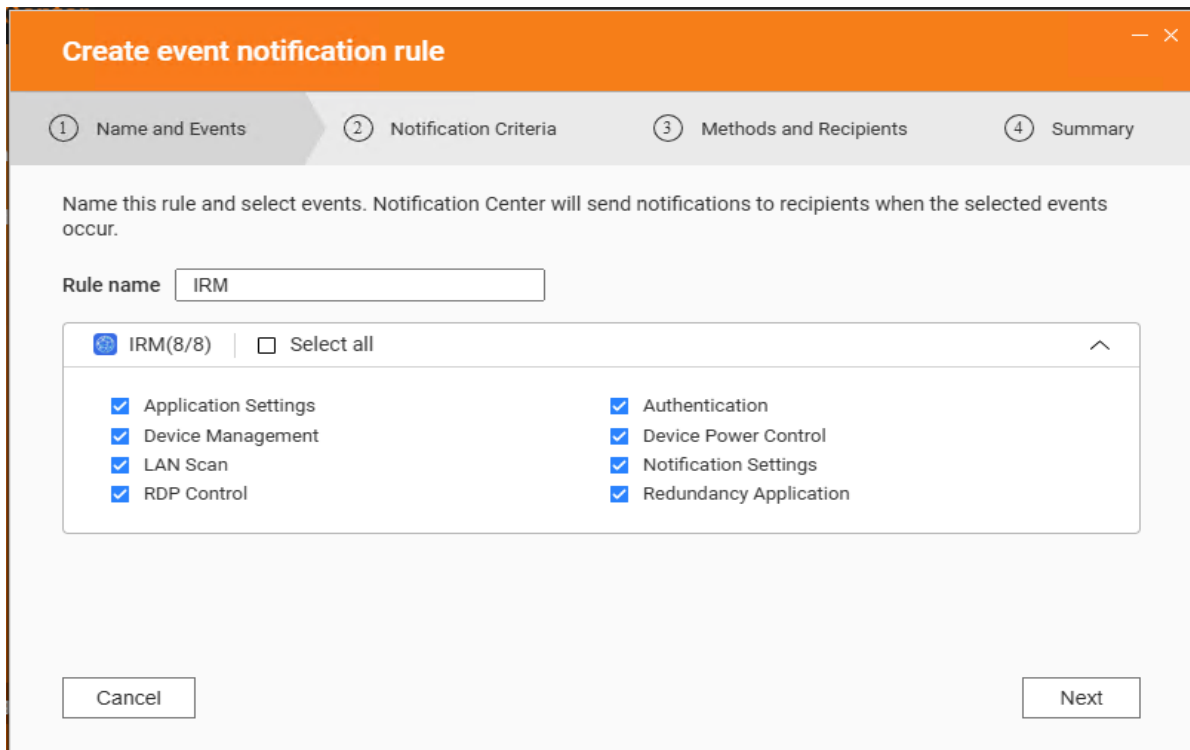
The **Notification Center** is used to manage IRM's notification mechanism. Administrators can create and maintain notification rules here. This feature integrates with **QTS** on the IRM Server to provide notification services. When the system detects an **Event Notification**, it can automatically send notifications to designated recipients based on the configured **severity level**, **keywords**, and **time range**, using the specified delivery method. Through the Notification Center, administrators can track system operation logs and monitoring/alert status in real time, improving event tracking and troubleshooting efficiency.

Supported type : Event Notification.

Notification methods: Supports Email, and can also enable SMS, Push Service, and Qmix notification channels depending on system settings.



After clicking** 「Configure Notification Rules」**, the system automatically opens your browser and redirects you to the Notification Center page to create event notification rules.



On the ① **Name and Events** page, enter a rule name (for example, **IRM**) and select the event categories you want to receive notifications for.

After finishing, click **Next** to proceed to ② **Notification Criteria**.

The screenshot shows a dialog box titled "Create event notification rule" with four steps: ① Name and Events, ② Notification Criteria (current), ③ Methods and Recipients, and ④ Summary. The current step is "Notification Criteria".

Instructions: Specify the severity levels, keywords, and time range of notifications that you want to receive.

Severity Level

Information Warning Error

Keyword Filter ⓘ

All messages ▾ --

Only send notifications for events that occur during a certain time period.

Time range: 00 ▾ : 00 ▾ ~ 23 ▾ : 59 ▾

Buttons: Cancel, Back, Next

On the ② **Notification Criteria** page, configure the notification trigger conditions, including the severity level, keywords, and time range:

1. **Severity Level:** Select the levels you want to receive notifications for (**Information / Warning / Error**).
2. **Keyword Filter:** Select **All messages**, or configure keyword conditions as needed.
3. **Time Range:** If you only want to receive notifications during specific periods, select **Time Range** and set the start and end time.

After finishing, click **Next** to proceed to ③ **Method and Recipients**.

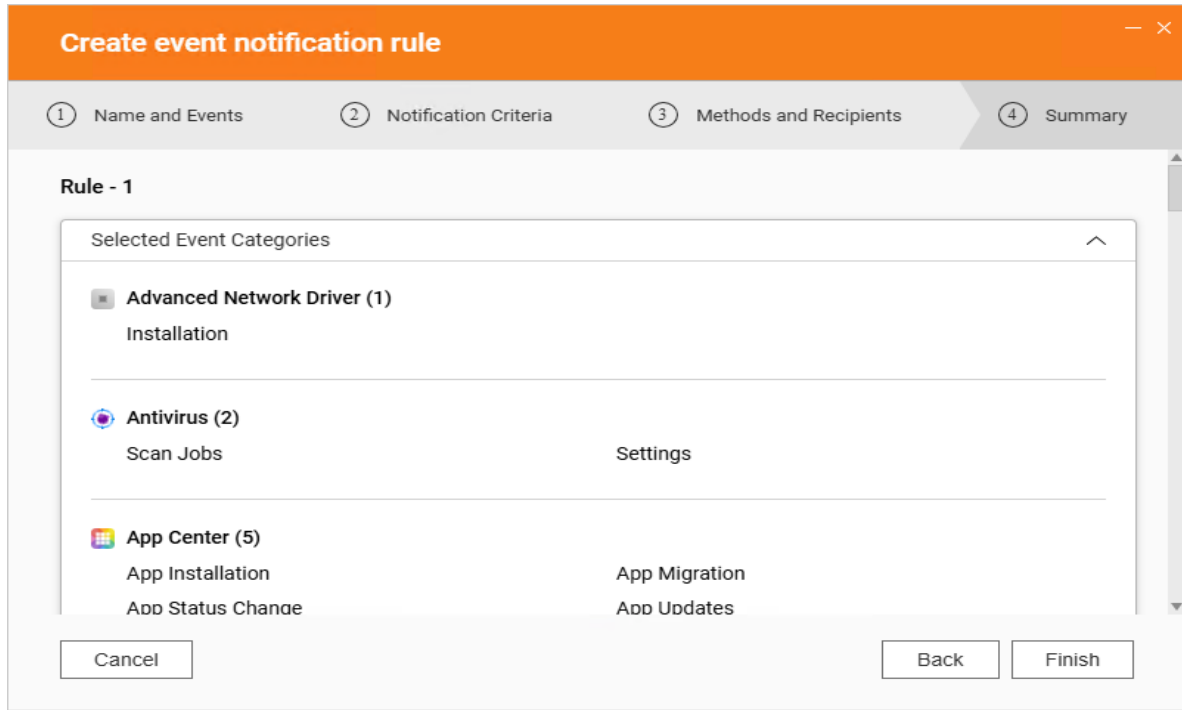
Step 6: ③ Method and Recipients

In this step, select the notification delivery method and configure the recipient information. The system supports multiple notification channels, including Email, SMS, Push Service, and Qmix. Depending on the selected method, you must complete the corresponding service settings (for example, Email requires selecting an SMTP sender account; SMS requires configuring an SMSC service; Push Service requires signing in to myQNAPcloud; and Qmix requires QNAP ID pairing).

You can also click 「+ Add Pair」 to add multiple delivery methods and recipient sets, allowing the same rule to send notifications to different recipient groups.

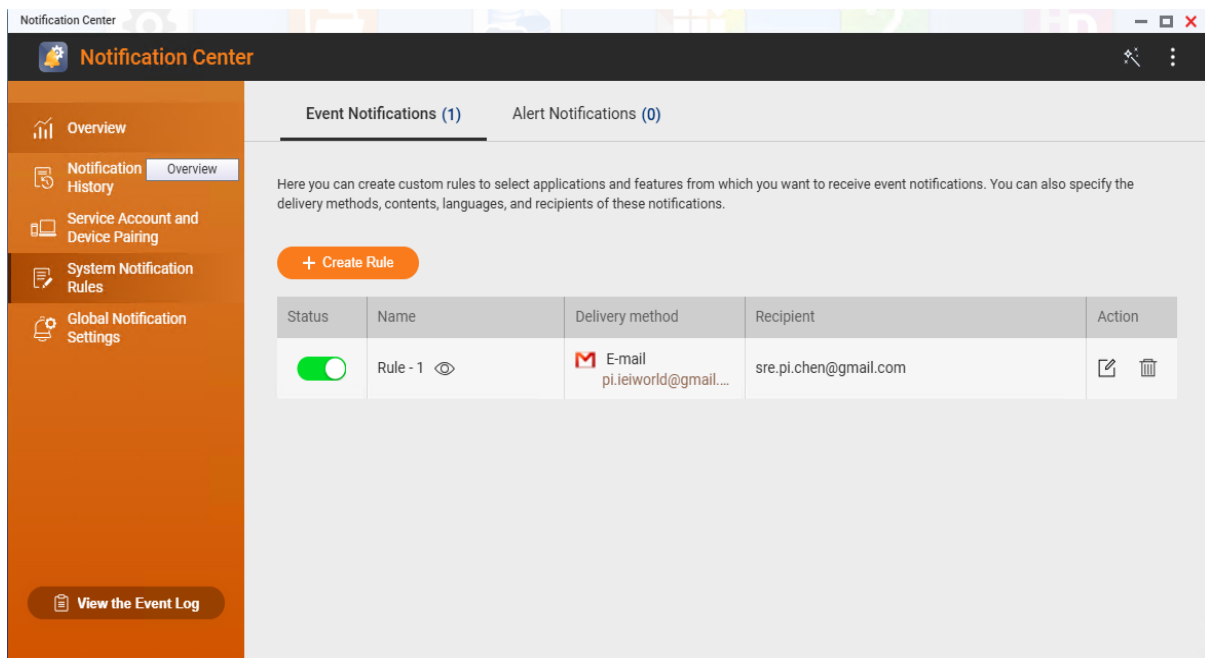
- **Email:** Gmail, Yahoo, QQ/QQ VIP, NetEase 126 / NetEase 163, Yahoo Kimo, Outlook.com
- **SMSC:** Clickatell, Nexmo, Twilio
- **Push Service:** myQNAPcloud: <https://www.myqnapcloud.com/>
- **Qmix:** <https://www.qnap.com/zh-tw/software/qmiix>

After completing the settings, click Next to proceed to ④ **Summary**.



Step 7: ④ **Summary** ◦

On the ④ **Summary** page, the system summarizes the settings of the event notification rule (including the rule name and the selected event categories/items). Verify that the information is correct. If changes are needed, click **Back** to revise the settings. After confirmation, click **Finish** to create the event notification rule.



Step 8: Confirm the System Notification Rule Is Created and Enabled

After creation, go back to IRM Settings > Notification > Notification Center. You should see the newly created rule (for example, IRM) in the rule list. Confirm that the Status switch on the left is Enabled (green), and verify that the Delivery method (for example, E-mail) and Recipient information are correct.

Setting / Notification

<input type="checkbox"/>	admin	Admin		
<input checked="" type="checkbox"/>	IRM	Admin		

Notification Center

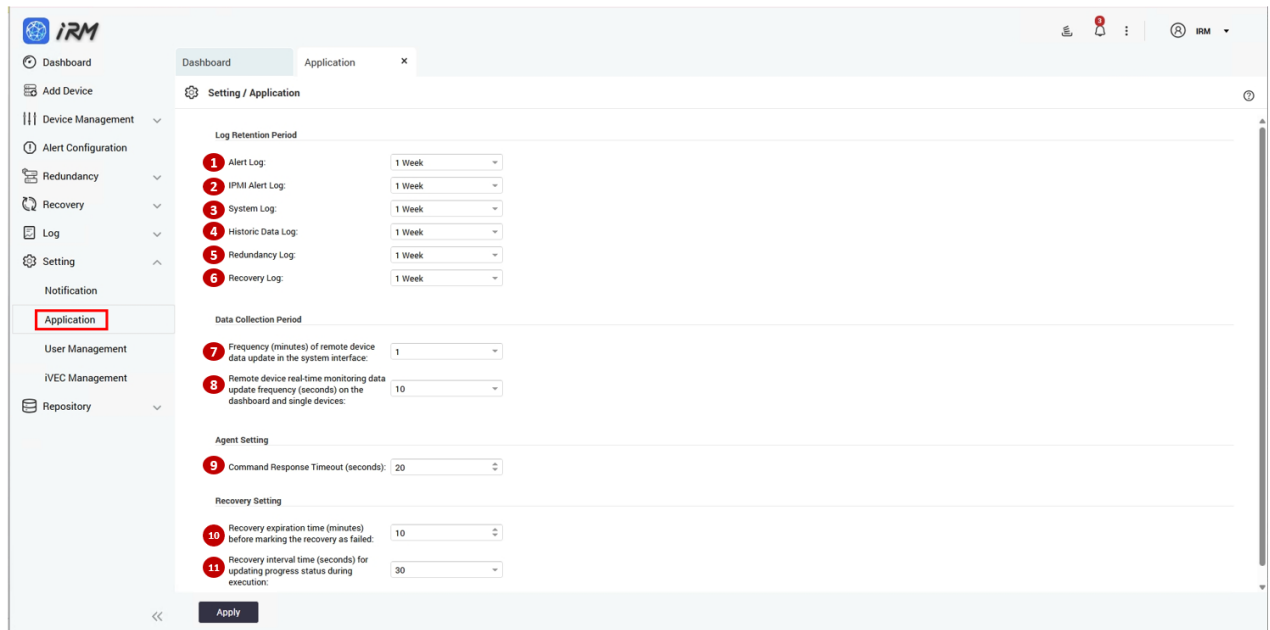
With Notification Center, you can quickly create custom notification rules to monitor the events on your devices and address potential issues more effectively. Ensure that you select "Set as dedicated rule" when creating notification rules in Notification Center. When this option is enabled, any changes made to rules will be automatically applied to and synced between IRM and Notification Center.

Status	Name	Delivery Method	Recipient	Action
<input checked="" type="checkbox"/>	IRM	Email pi.ieiworld@gmail.com	pm@gmail.com	

Apply

10.1 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.



10.1.1 Log Retention Period

You can configure how long each type of log is retained in the system (via a drop-down list). Available options are **1 Week**, **1 Month**, and **3 Months**.

1. Alert log retention period
2. IPMI alert log retention period
3. System log retention period
4. Historical data log retention period
5. Redundancy log retention period
6. Recovery log retention period

Note : : A longer retention period may consume more storage space.

10.1.2 Data Collection Period

Configure the update frequency for device data on the interface/dashboard.

7. Frequency (minutes) of remote device data update in the system interface
8. Remote device real-time monitoring data update frequency (seconds) on the dashboard and single devices

Note : A higher update frequency may increase system and network load.

10.1.3 Agent Setting

9. Command Response Timeout (seconds)

The maximum time IRM waits for an agent response after sending a command.

10.1.4 Recovery Setting

10. Recovery expiration time (minutes) before marking the recovery as failed
11. Recovery interval time (seconds) for updating progress status during execution

10.2 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.

10.2.1 Default User

The default ID is "IRM" and the password is "Irm" followed by the last six letters of the hardware's first MAC address (in uppercase and without special characters).

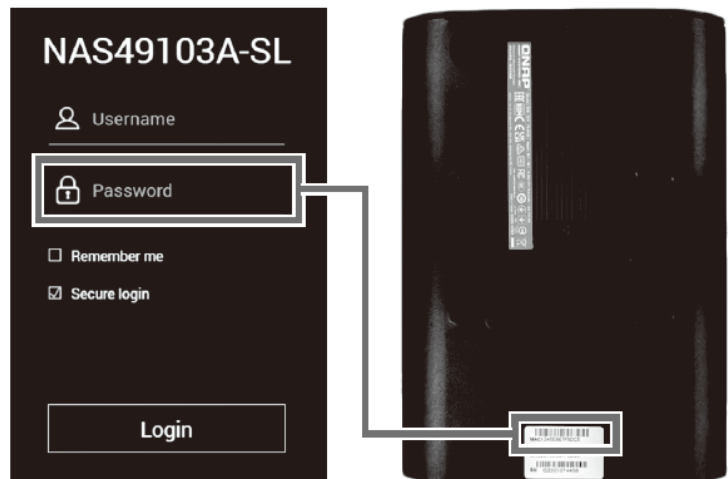
Note: The ID and password are case-sensitive.

Example:

MAC1 address: 00-08-9B-F6-15-75

Username: IRM

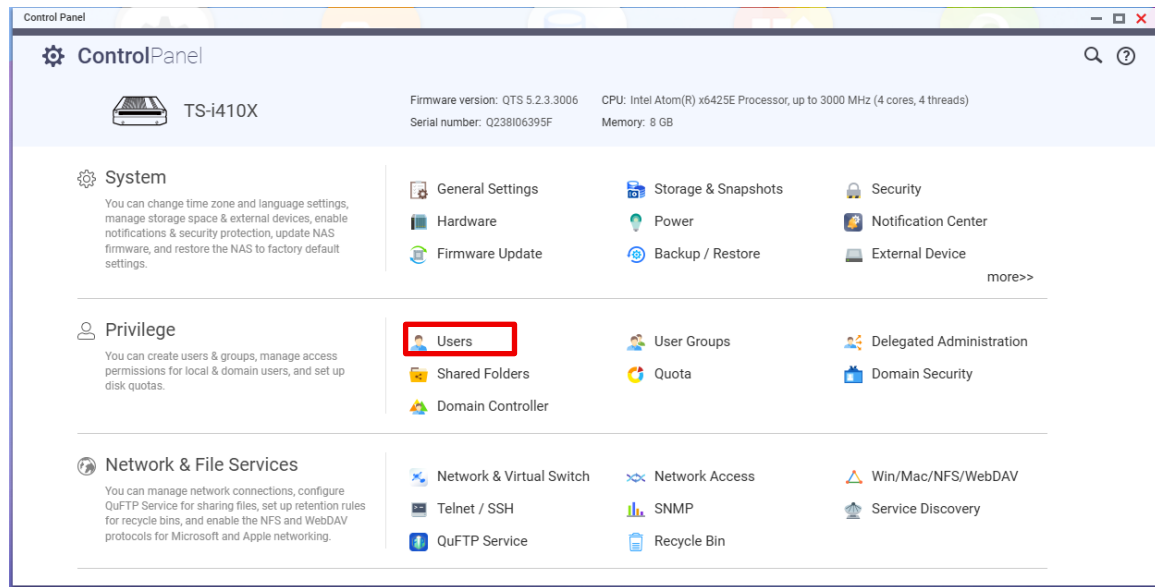
Password: IrmF61575



10.2.2 Create New User

To create a new user other than using the default user account, you need to create a local user in the QTS by following the steps below.

Step 1: Go to **Control Panel > Privilege > Users**.




Step 2: Click **Create > Create a User**.

The **Create a User** window appears.

Step 3: Specify the following information.

Field	Description
Profile photo	Optional: Upload a profile photo for the user.
User Description (optional)	Specify a user description that contains a maximum of 50 characters.
Username	Specify a username that contains 1 to 32 characters from any of the following groups: <ul style="list-style-type: none"> • Letters: A to Z, a to z • Numbers: 0 to 9 • Multi-byte characters: Chinese, Japanese, Korean, and Russian • The username cannot contain the following special characters: grave accent (`), asterisk (*), equal sign (=), plus sign (+), square brackets ([]), curly brackets ({}), slash (/), vertical bar (), semicolon (;), colon (:), apostrophe ('), quotation mark ("), comma (,), less than sign (<), greater than sign (>), backslash (/), question

	mark (?), percent sign (%), dollar sign (\$), and the space character.
Password	Specify a password that contains a maximum of 64 ASCII characters.
Verify Password	Enter the password again.
Mobile phone (optional)	Specify a phone number that will receive SMS notifications from QTS. Note: Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.
Email (optional)	Specify an email address that will receive notifications from QTS. Note: Other NAS users might be able to see this information. If you do not want to share this information, leave the field blank.
UID	A UID is automatically generated for the user. You can also click  to specify a custom UID.
User must change password at first logon	When selected, the user must change the password when logging in for the first time.
Send a notification mail to the newly created user (optional)	When selected, QTS sends a message that contains the following information to the specified email address: <ul style="list-style-type: none"> • Username and password • URLs for connecting to the NAS Tip: You can edit the notification message.

Step 4: Optional: Add the user to one or more user groups.

- a. Under **User Group**, click **Edit**.
- b. Select one or more user groups.

Step 5: Optional: Specify shared folder permissions for the user.

- a. Under **Shared Folder Permission**, click **Edit**.
- b. Select the shared folder permissions for the user.
- c. **Optional:** Select **Apply changes to subfolders**.

Step 6: Optional: Specify application privileges for the user.

- a. Under **Edit Application Privilege**, click **Edit**.
- b. Select application permissions for the user.

Tip:

QNAP recommends denying access to applications and network services that the user does not require. Users without privileges to specific applications will not see it on their main menu.

Step 7: Optional: Set a quota for the user.

Note:

This option is only available when quotas are enabled.

- a. Under **Quota**, click **Edit**.
- b. Set the quota.

- **No Limit:** Quota settings do not apply to the user.
- **Limit disk space to:** Specify a quota for the user.
- **Use group quotas:** Group quota settings apply to the user.

Note:

Individual quotas may override group quotas. For details, see [Quota conflicts](#).

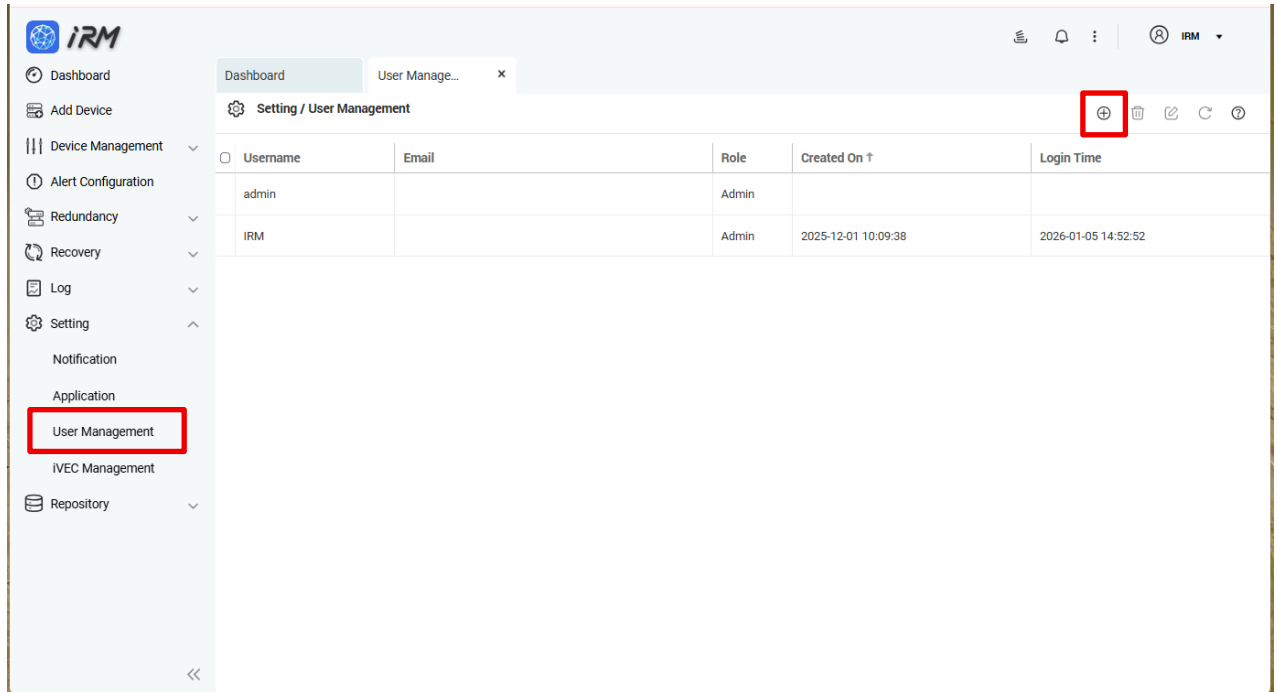
Step 8: Click **Create**.

NOTE:

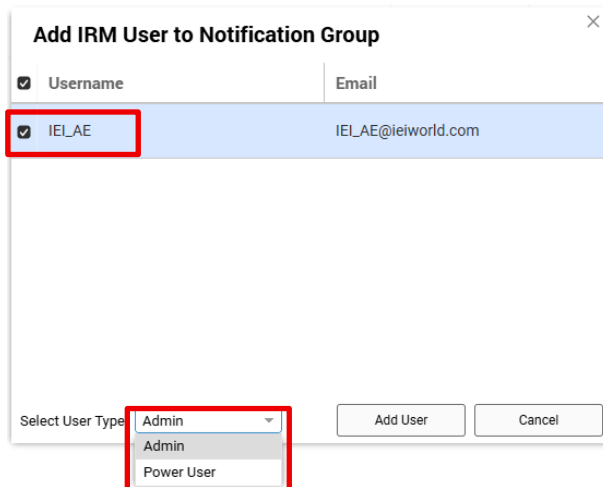
For more information on QTS related topics, please see the [QTS online user manual](#).

10.2.3 Add User

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



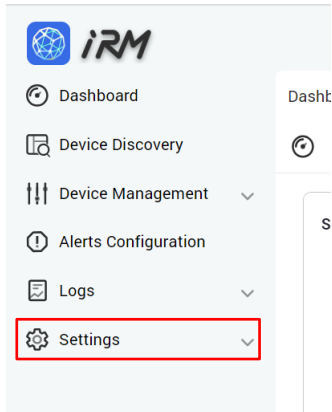
Step 2: After select the user and the permissions that you want to add, click "Add User" to finish.



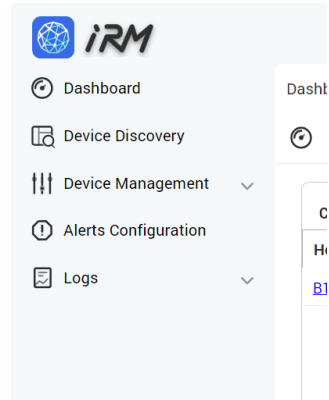
NOTE: 1. The difference in permissions between Admin and Power User is that only Admin can access

Settings. Power User has no authority to modify or change system settings.

Administrator's UI

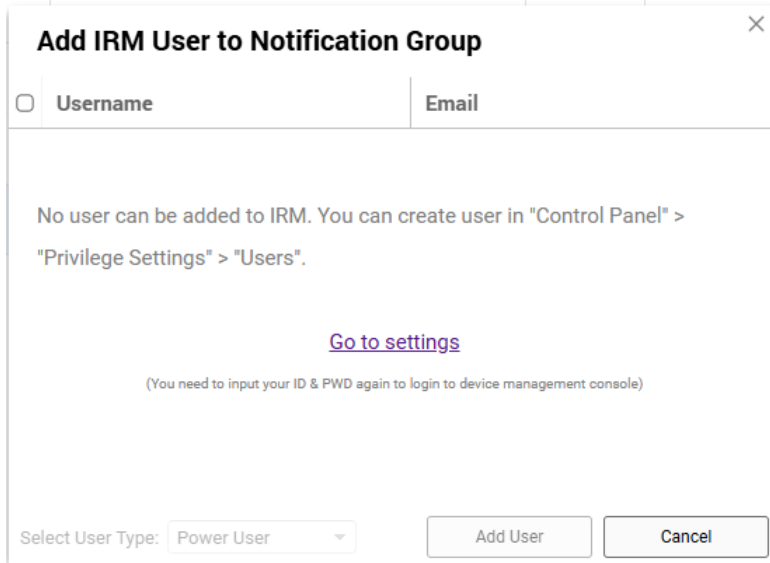


Power User's UI



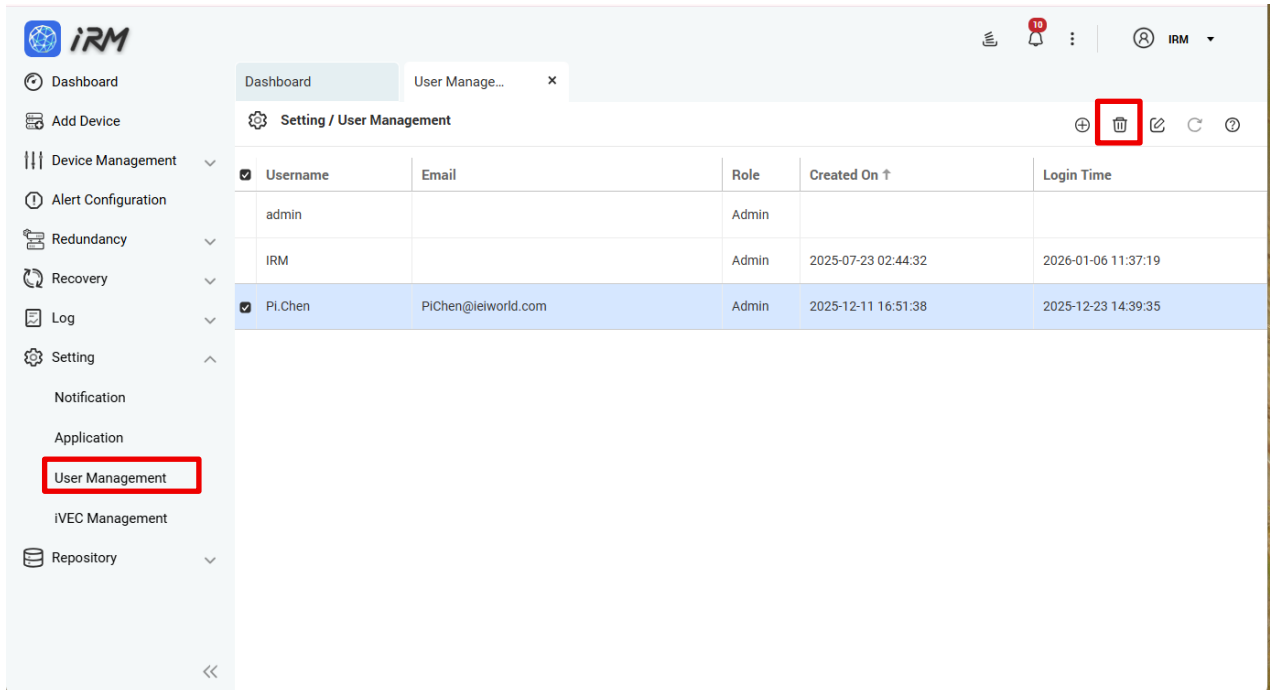
2. When the **Add IRM User to Notification Group** window appears and shows **“No user can be added to IRM...”**, it means that no IRM users have been created in the system that can be added to a notification group. Therefore, the list will be empty and you will not be able to select or add any users.

Please refer to **Section 10.1.2, “Create New User.”**



10.2.4 Deleting Users

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

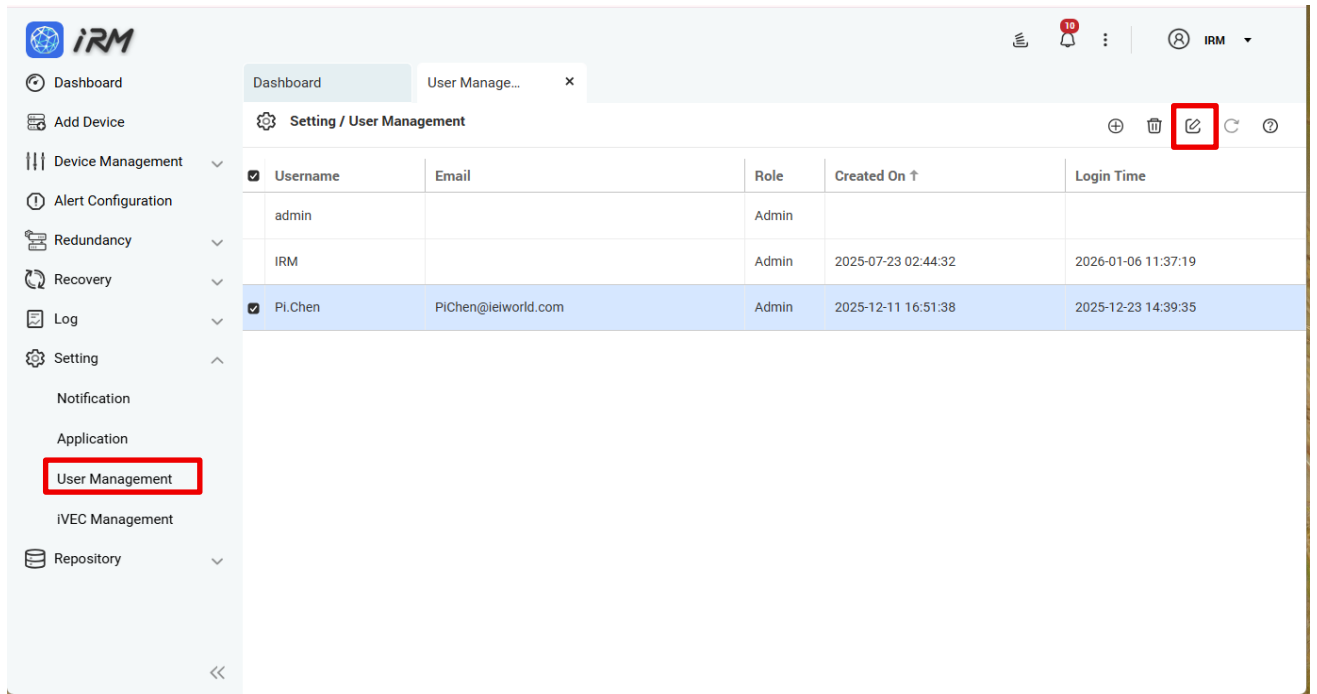


The screenshot shows the iRM web interface. On the left is a navigation menu with 'User Management' highlighted in a red box. The main content area is titled 'Setting / User Management' and contains a table of users. A red box highlights the delete icon (trash can) in the top right corner of the table.

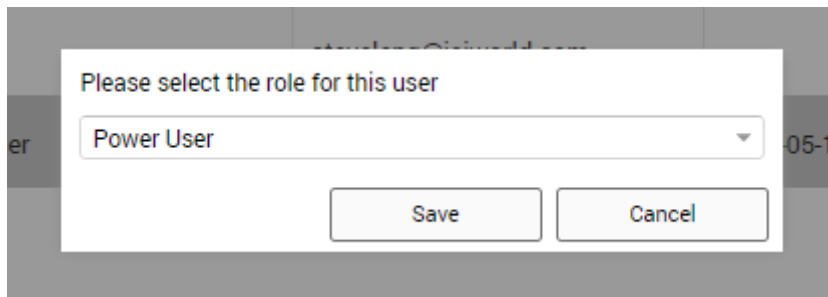
<input checked="" type="checkbox"/>	Username	Email	Role	Created On ↑	Login Time
	admin		Admin		
	IRM		Admin	2025-07-23 02:44:32	2026-01-06 11:37:19
<input checked="" type="checkbox"/>	Pl.Chen	PlChen@ielworld.com	Admin	2025-12-11 16:51:38	2025-12-23 14:39:35

10.2.5 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.



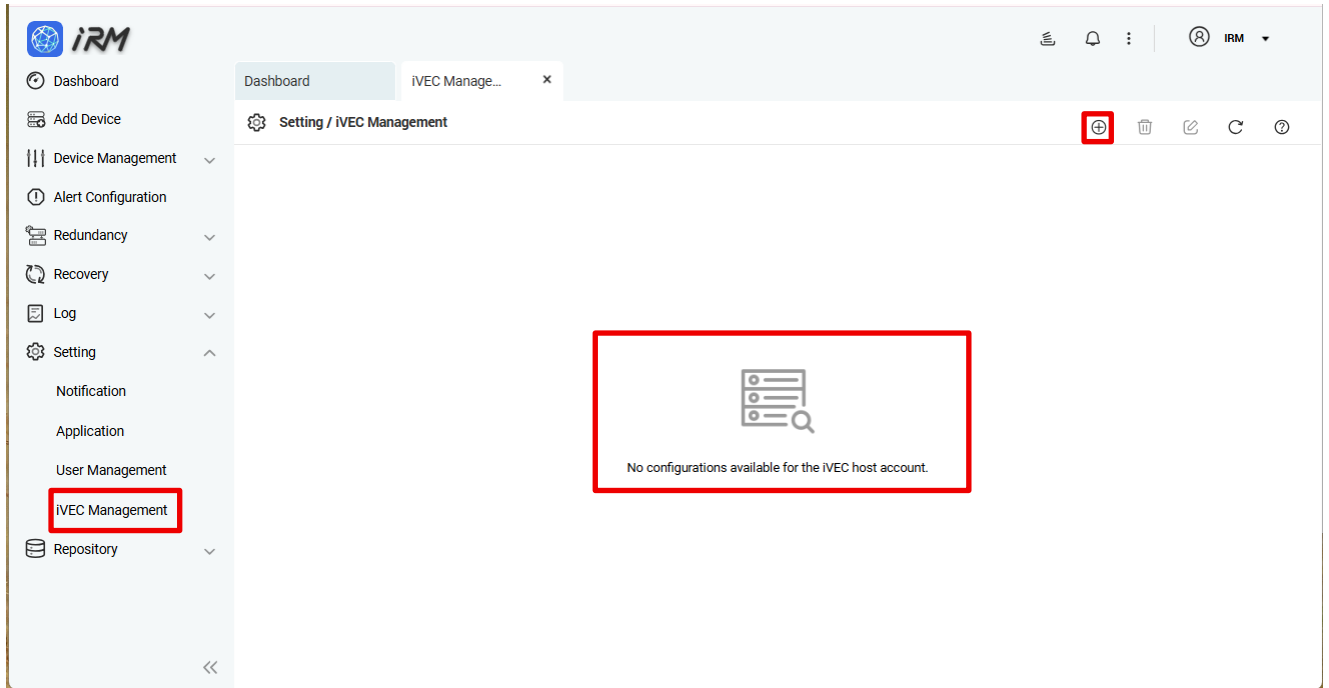
10.3 iVEC Management

iVEC Management provides a centralized entry in IRM for administrators to manage iVEC environments. After an iVEC device is added and managed by IRM, administrators can use VM via iVEC VM list and iVEC management console by your browser to view iVEC-related information, check iVEC host status, and perform necessary management operations for monitoring, maintenance, and troubleshooting.

- iVEC VM List : View the list of virtual machines on the iVEC host.
- iVEC management console (by your browser) : Open the iVEC management console in your web

browser.

If no iVEC host configuration has been created, the page displays: **No configurations available for the iVEC host account.**



Step 1: Create iVEC Host Account

1. Go to the iVEC Management page and click the "Create iVEC Host Account" button.

Create iVEC Host Account ✕

iVEC Host * Select Device

iVEC Hostname

Port * Use SSL Certificates

Account *

Password *

Confirm Password *

iVEC Host*: Click Select Device. The system displays the Selected Device window. Select the iVEC host you want to add for management from the list (the iVEC host must have the IRM Agent installed), and then click OK button.

Port*: The default port for the iVEC host is 8089, using an SSL certificate.

Account*: Enter the login account for the iVEC host.

Password*: Enter the login password for the iVEC host.

Confirm Password*: Re-enter the login password for the iVEC host.

Selected Devices

Hostname, IP address, Device tag

	Hostname	IP Address	Tag	Managed by	Brand	Model	Operating Syst...
<input type="checkbox"/>	iei-SJB8	10.10.40.244	Tank_XM811	IRMAgent	IEI	13th Gen Intel(R...	Ubuntu
<input type="checkbox"/>	iei-SJB8	10.10.40.104		IRMAgent	IEI	13th Gen Intel(R...	Ubuntu

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

OK Cancel

After the settings are saved successfully, the iVEC host configuration will appear in the list, and you can view the following information: iVEC Hostname, IP Address, Port, Protocol, and Account.

Note: After completing the iVEC host configuration, you can use features such as iVEC VM List and iVEC Management Console (by your browser).

iRM

Dashboard | iVEC Manage... x

Setting / iVEC Management

<input type="checkbox"/>	iVEC Hostname	IP Address	Port	Protocol	Account ↑
<input type="checkbox"/>	iei-SJB8	10.10.40.244	8089	HTTPS	iei

Page 1 of 1 | 1 - 1 of 1

Chapter

11

11 Repository

The Repository is used to centrally manage the installation packages and related resources required by IRM. From this page, administrators can download the IRM Agent installer for the corresponding operating system. After deploying the agent on the device, the device can then be added to IRM for monitoring and management. ◦

11.1 IRMAgent download

IRMAgent Download provides IRMAgent installer packages for different operating systems. Administrators can download the correct package based on the target device OS and architecture (32-bit/64-bit), then install it to enroll devices into IRM for monitoring and management.

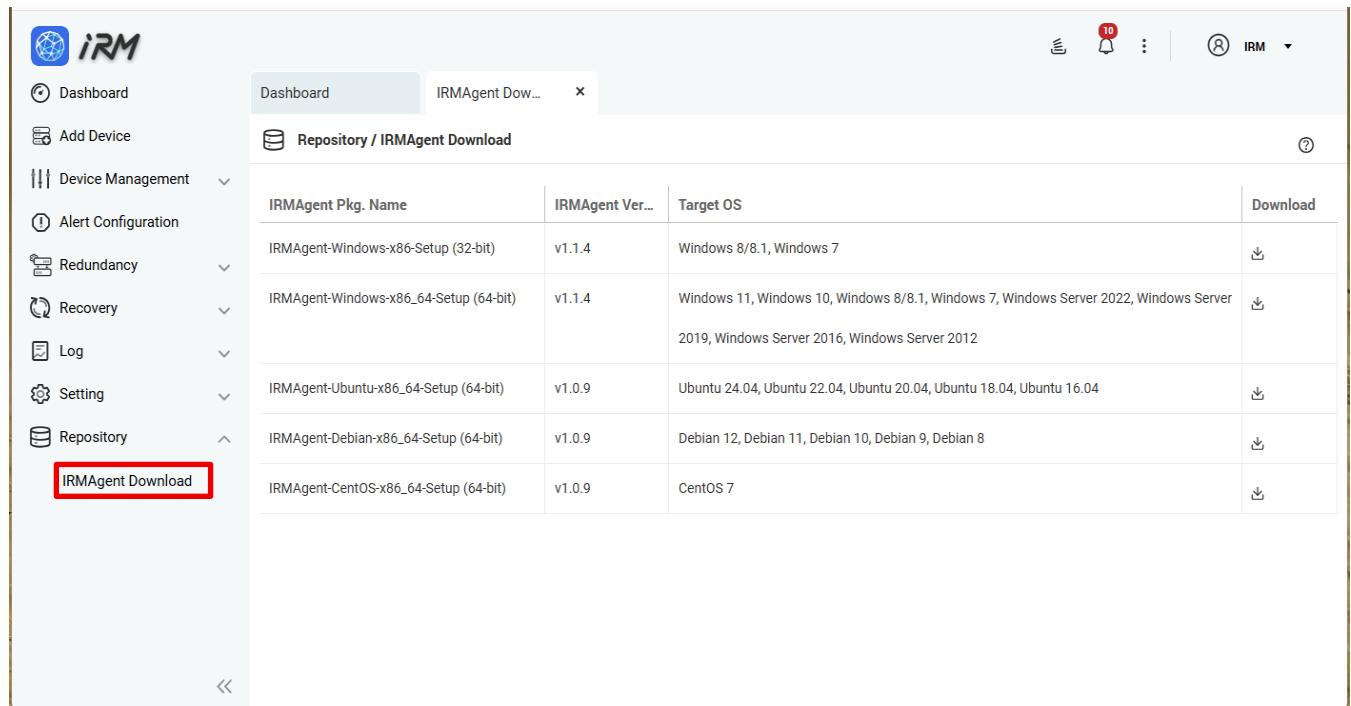
Basic Steps:

Step 1: Go to Repository > IRMAgent Download.

Step 2: Identify the correct package for the target device OS and architecture (32/64-bit).

Step 3: Click the Download icon to download the installer.

Step 4: Deploy and install the package on the target device to enable device enrollment.



IRM Agent Pkg. Name	IRM Agent Ver...	Target OS	Download
IRMAgent-Windows-x86-Setup (32-bit)	v1.1.4	Windows 8/8.1, Windows 7	⬇
IRMAgent-Windows-x86_64-Setup (64-bit)	v1.1.4	Windows 11, Windows 10, Windows 8/8.1, Windows 7, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012	⬇
IRMAgent-Ubuntu-x86_64-Setup (64-bit)	v1.0.9	Ubuntu 24.04, Ubuntu 22.04, Ubuntu 20.04, Ubuntu 18.04, Ubuntu 16.04	⬇
IRMAgent-Debian-x86_64-Setup (64-bit)	v1.0.9	Debian 12, Debian 11, Debian 10, Debian 9, Debian 8	⬇
IRMAgent-CentOS-x86_64-Setup (64-bit)	v1.0.9	CentOS 7	⬇

Chapter

12

12 Licenses

12.1 License Portals and Utility

IEI and QNAP (initially an IEI subsidiary) form a dynamic alliance to offer the iRM solution. QNAP's secure platforms is utilized for license management of IEI iRM. These QNAP's license platforms are as the followings:

Portal	Description
License Center	The License Center is an app in the iRM Mini Server, serving as a proxy of the License Manager for monitoring and managing iRM license.
License Manager https://license.qnap.com	The License Manager is a web site hosted by QNAP. It allows you to remotely activate and manage licenses under your QNAP ID.
QNAP Software Store https://software.qnap.com	The QNAP Software Store is a one-stop shop where you can purchase software licenses such as iRM.
QNAP Account / QNAP ID (QID) https://account.qnap.com	The QNAP Account is a portal that lets you manage your QNAP ID and access the Cloud SSO function for various QNAP Cloud Services and devices. QNAP ID (QID) is a unique identifier for end users that allows them to manage their cloud services and devices through QNAP Account. End users can create their own QID using their email address.

12.2 iRM Perpetual License

The iRM Perpetual License has 8 different SKUs, each supporting a specific number of client devices. You can also use the free version, which supports up to 10 client devices without requiring a license.

SKU ID	Description
SKU 1	iRM V1.* Perpetual License for 20 devices
SKU 2	iRM V1.* Perpetual License for 50 devices
SKU 3	iRM V1.* Perpetual License for 80 devices
SKU 4	iRM V1.* Perpetual License for 100 devices
SKU 5	iRM V1.* Perpetual License for 150 devices
SKU 6	iRM V1.* Perpetual License for 200 devices
SKU 7	iRM V1.* Perpetual License for 250 devices
SKU 8	iRM V1.* Perpetual License for 300 devices

Note: The license quantity will be added up, and the iRM will display the total count.

12.3 License Activation

To use the features of IRM, you need to buy a license from IEI sales or QNAP Software Store, and activate the license. The process of license activation includes the following key steps that should be taken:

1. Apply your QNAP ID
2. Sign in the IRM mini server with your QNAP ID, and set up the myQNAPcloud service
3. Active your license through License Center or License Manager by using product key bundled with your QID
4. Check your IRM license in IRM's About page

IRM only accepts licenses that are valid and active. IEI advises users to activate their licenses from the license center using a product key bundled with your QID. The product key provided by IEI is not bundle with the QID and requires the setup of the QID in the IRM Mini Server before activation.

Activation of an IRM license can be done using either a product key or a license key. The product key is obtained through IEI's sales channel, while the license key is from the QNAP Software Store. When end users purchase a license key from the QNAP Software Store, it will be bundled with their QID. However, the product key will not be bundled with any QID during the purchase stage. Both the product key and the license key will be finally bundled with the end user's QID when the user activates the license.

Difference between Product Key and License Key:

	Product Key	License Key
Buy from	IEI	QNAP Software Store (online)
Bundled with QID	No	Yes
Payment	Depend on IEI	Online via credit card
License Activation	Online	Online

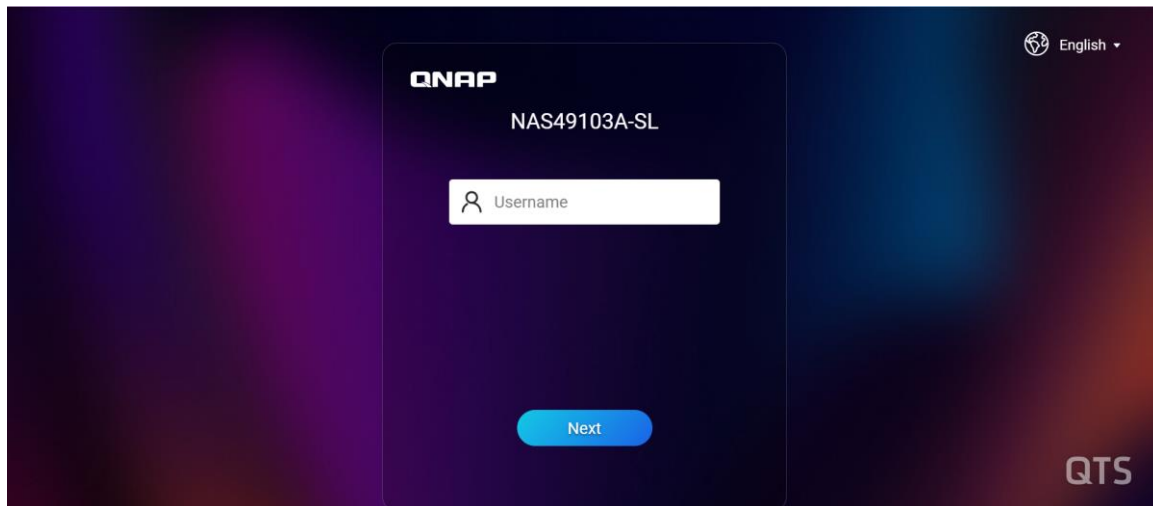
12.3.1 Activation Methods

Activation Method	Description
Using a product key	<p><Online activation></p> <p>Licenses purchased from IEI sales must be activated through the 25-character product key.</p> <p>For license activation instructions, see Section 12.3.3</p>
Using a license key	<p><Online activation></p> <p>You can generate the 25-character license key after purchasing licenses through the QNAP Software Store. For details, see Generating a License Key.</p> <p>For license activation instructions, see Section 12.3.4</p>
Using QNAP ID (QID)	<p><Online activation></p> <p>Licenses purchased through QNAP Software Store are stored in your QNAP ID account. They can be accessed through both License Center and the QNAP License Manager website.</p> <p>For license activation instructions, see Section 12.3.5</p>
Offline	<p><Offline activation></p> <p>Use this method when connecting the IRM mini server to the internet may not be feasible or advisable in certain industrial settings. Offline activation is more complicated and involves more steps. See Activating a License Offline for step-by-step instruction.</p>

12.3.2 Setting up myQNAPcloud for Your IRM Mini Server

Before activating IRM license, you should first sign in the IRM mini server with your QNAP ID and then set up the myQNAPcloud service. To do so, follow the steps below.

Step 1: Login IRM Mini Server Management Desktop. Ensure the mini server is connected to the internet.



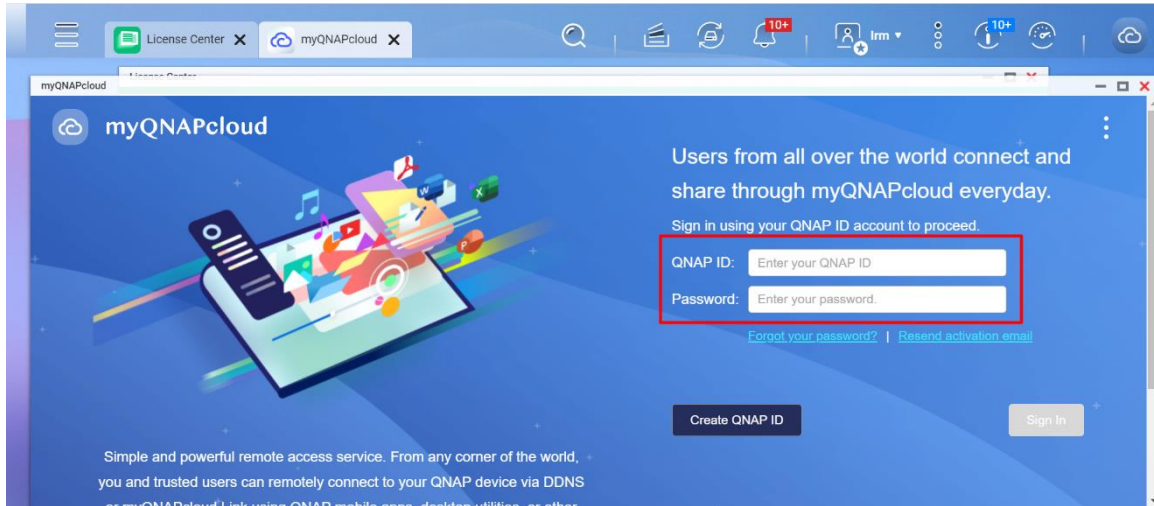
Step 2: Launch the myQNAPcloud Link.



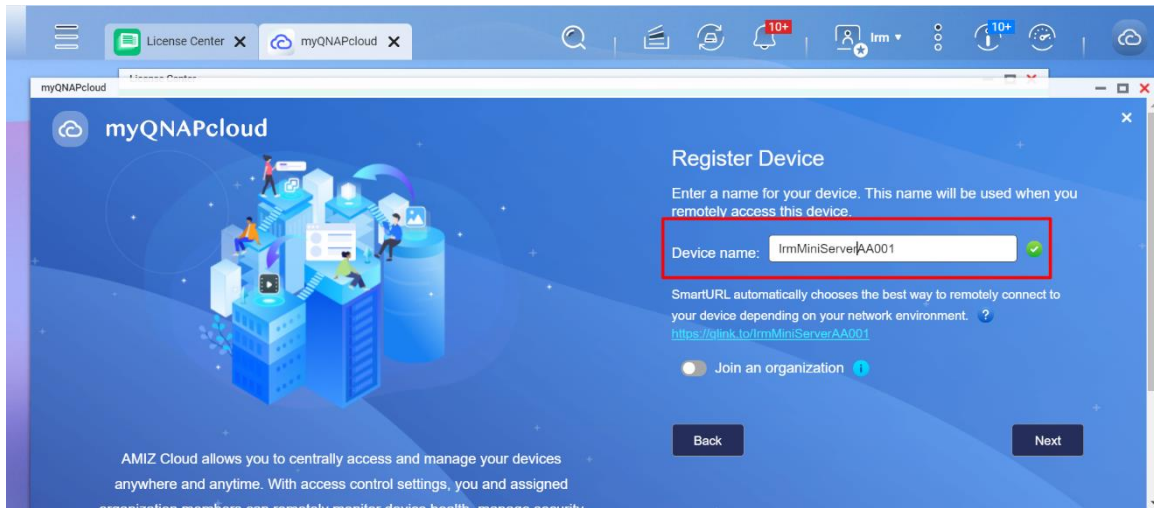
Step 3: Enter your QNAP ID and password, and click **Sign In**.

NOTE:

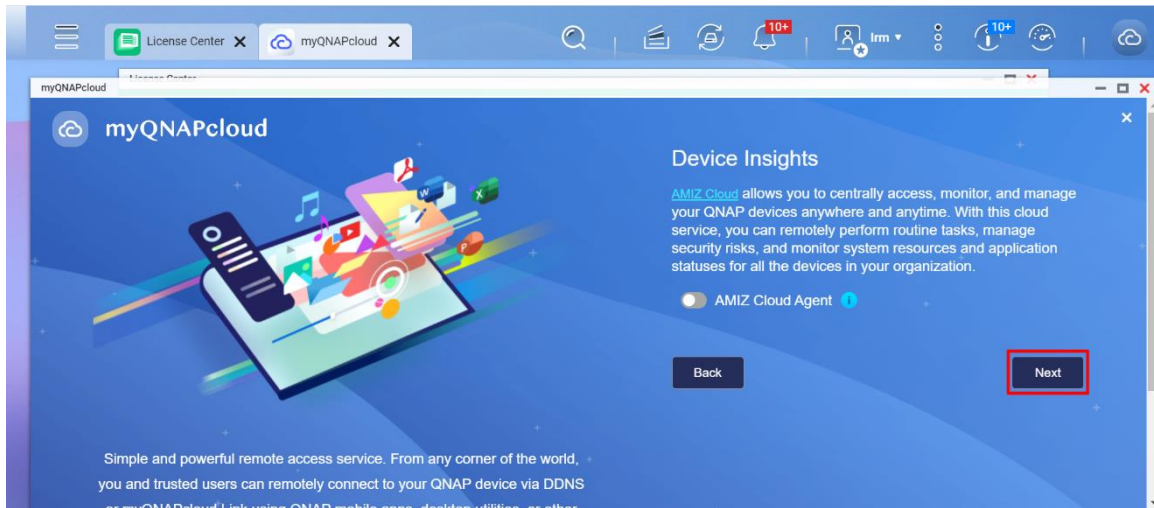
- End user can apply QID from <https://account.qnap.com/>
- To manage the license effectively, we recommend entering the QID of the license owner. A system integrator (SI) can use their own QID to buy and activate the license for their customer on the IRM mini server. This way, the SI can assist the end user with license management in the future.



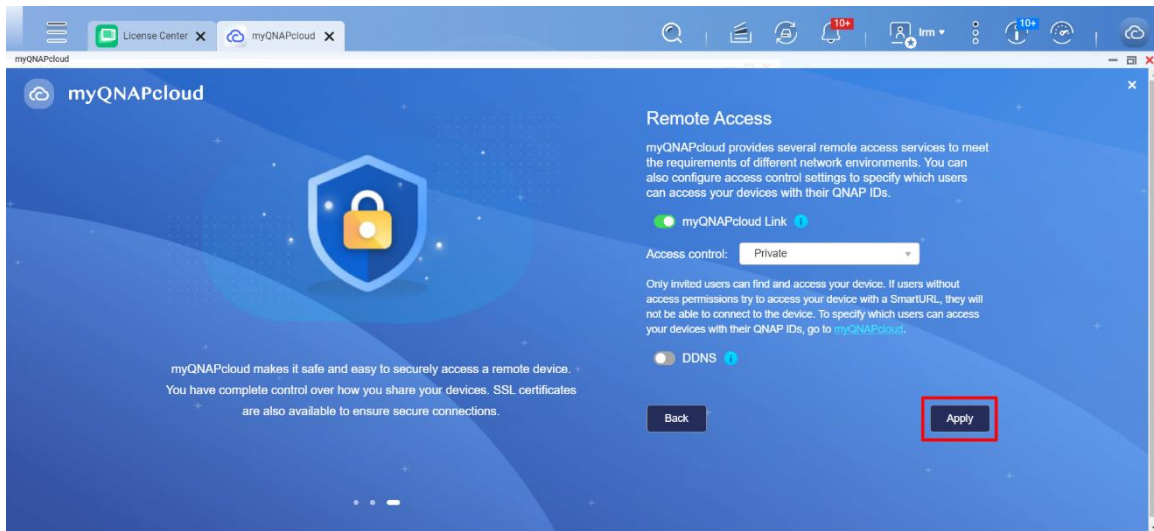
Step 4: Specify a device name. Click **Next**.



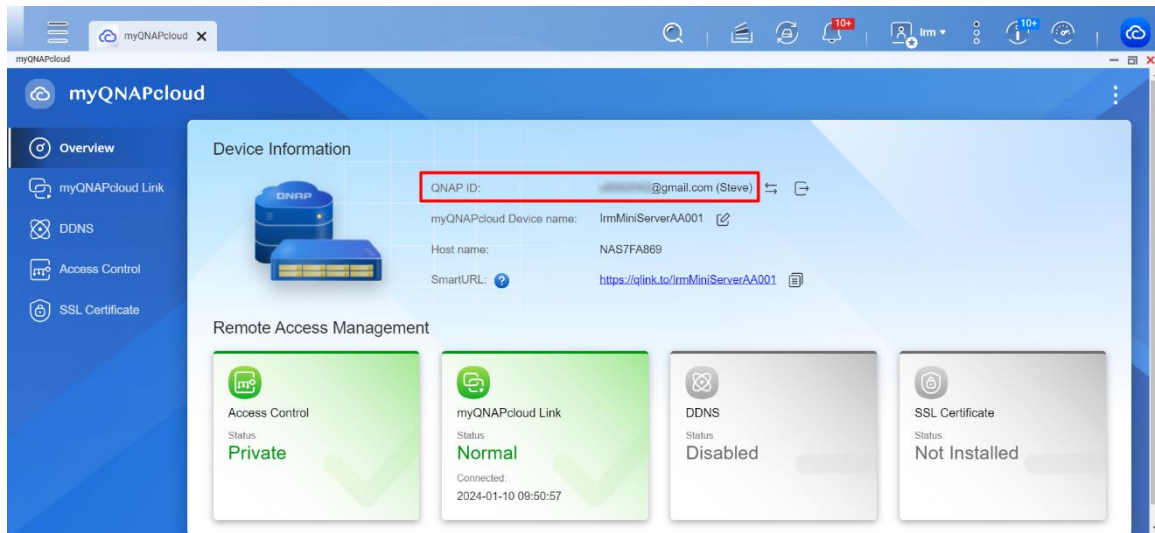
Step 5: Click **Next**.



Step 6: Click **Apply** to apply the settings.



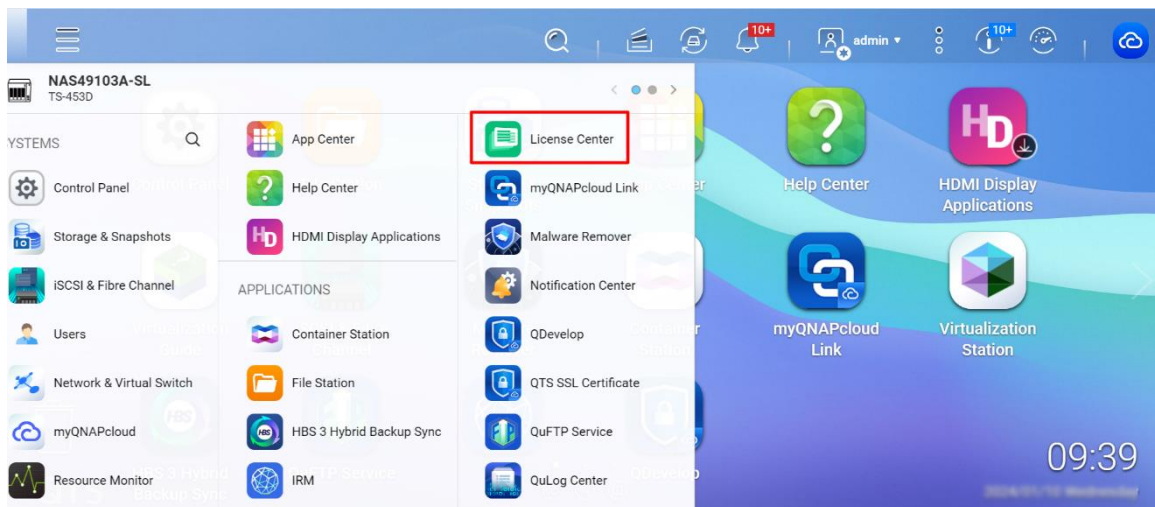
Step 7: The system configure the mini server according to your settings.



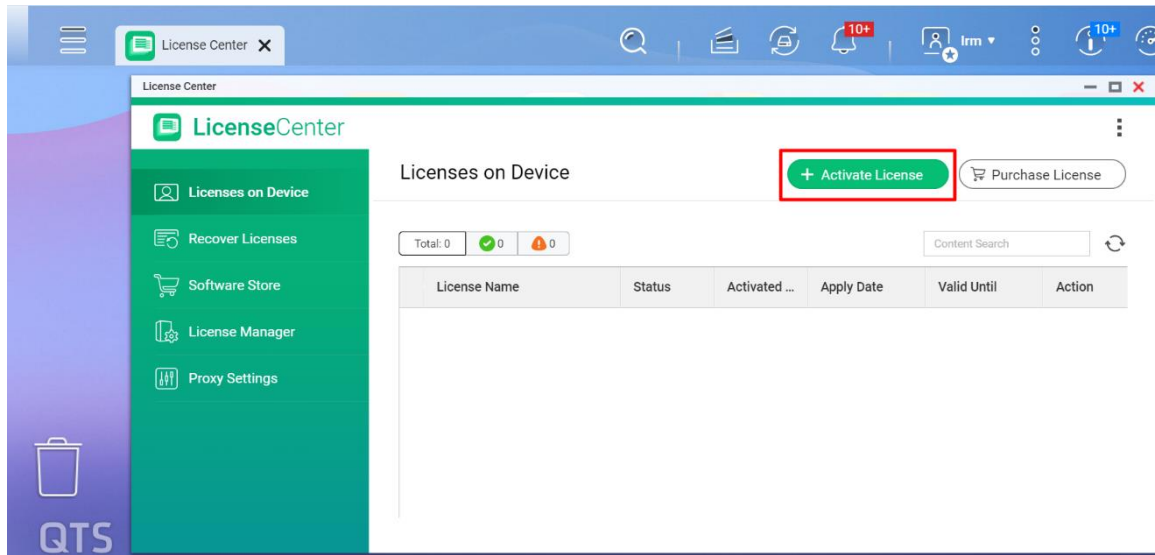
12.3.3 Activating a License Using a Product Key

Before activating your license, ensure that your device is connected to the internet and you have signed in with your QNAP ID. To activate a license using a product key, follow the steps below.

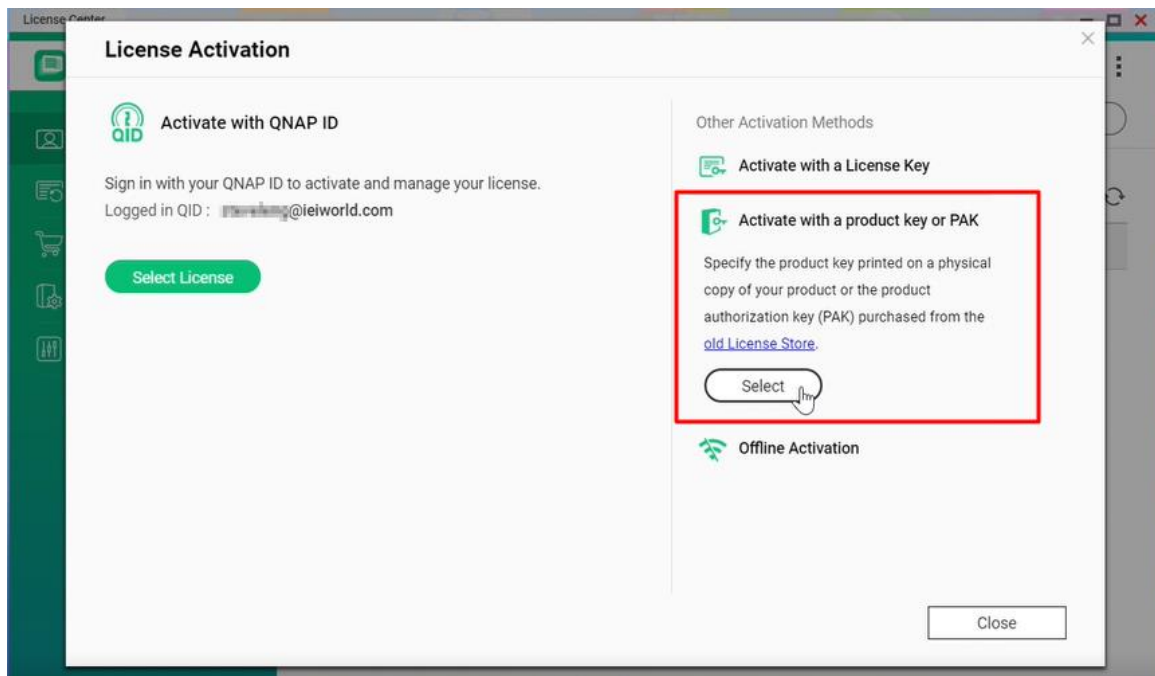
Step 1: Open **License Center**.



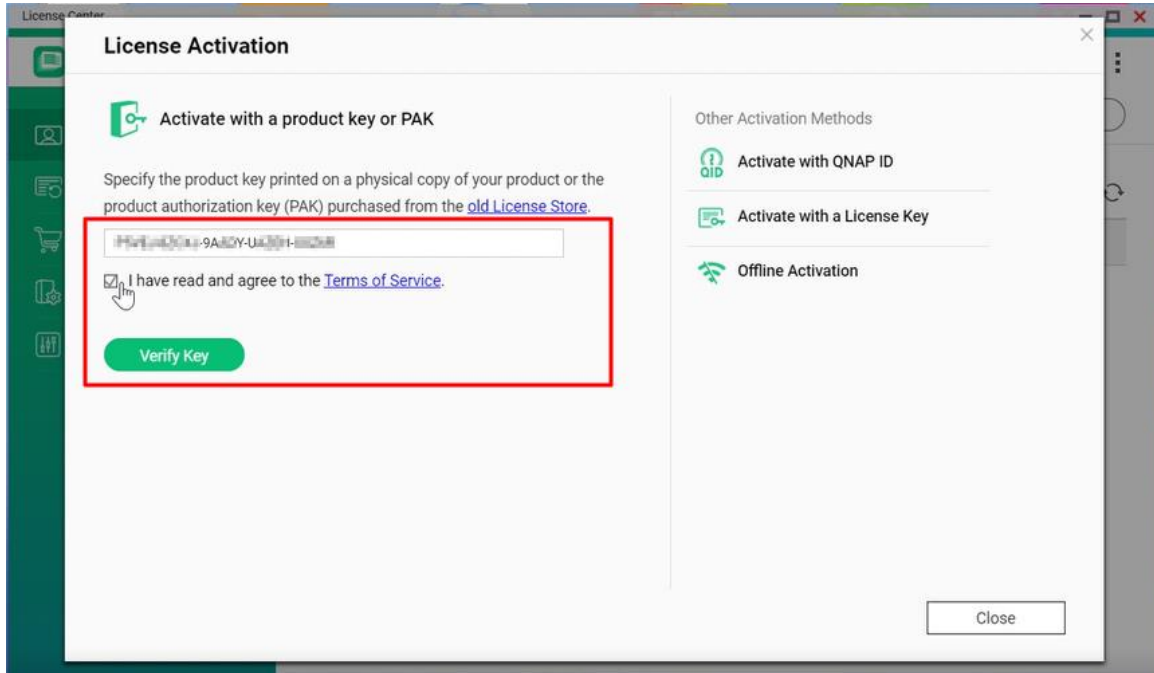
Step 2: Click **Activate License**.



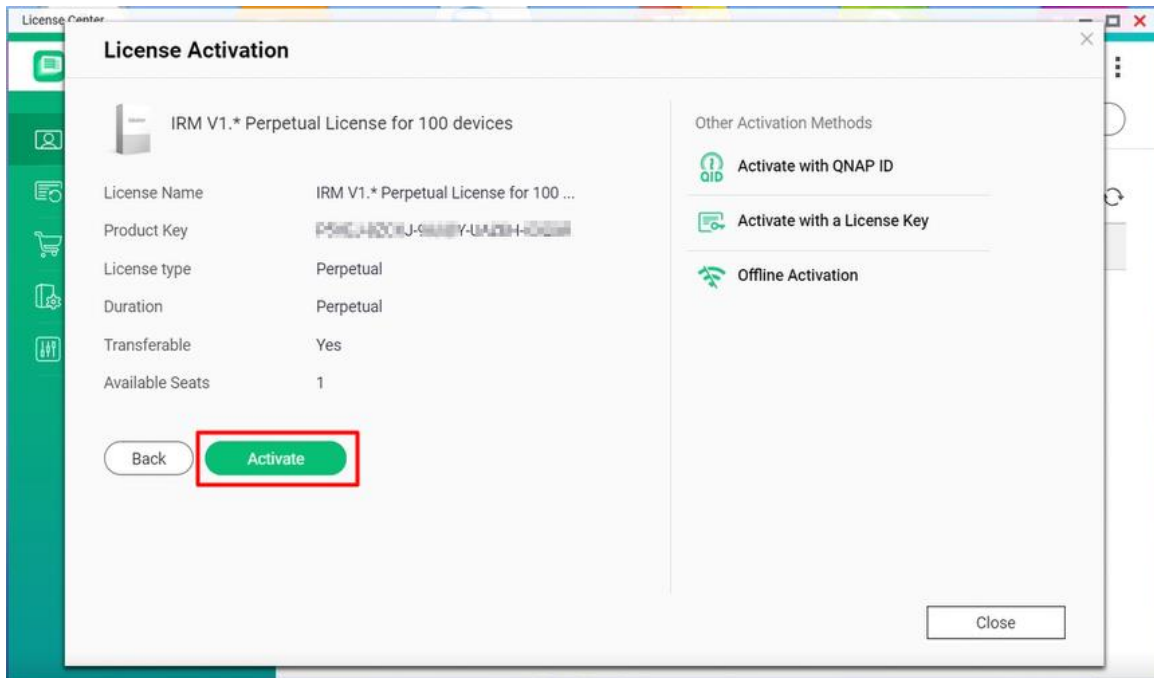
Step 3: The License Activation window appears. Select **Activate with a product key or PAK**.



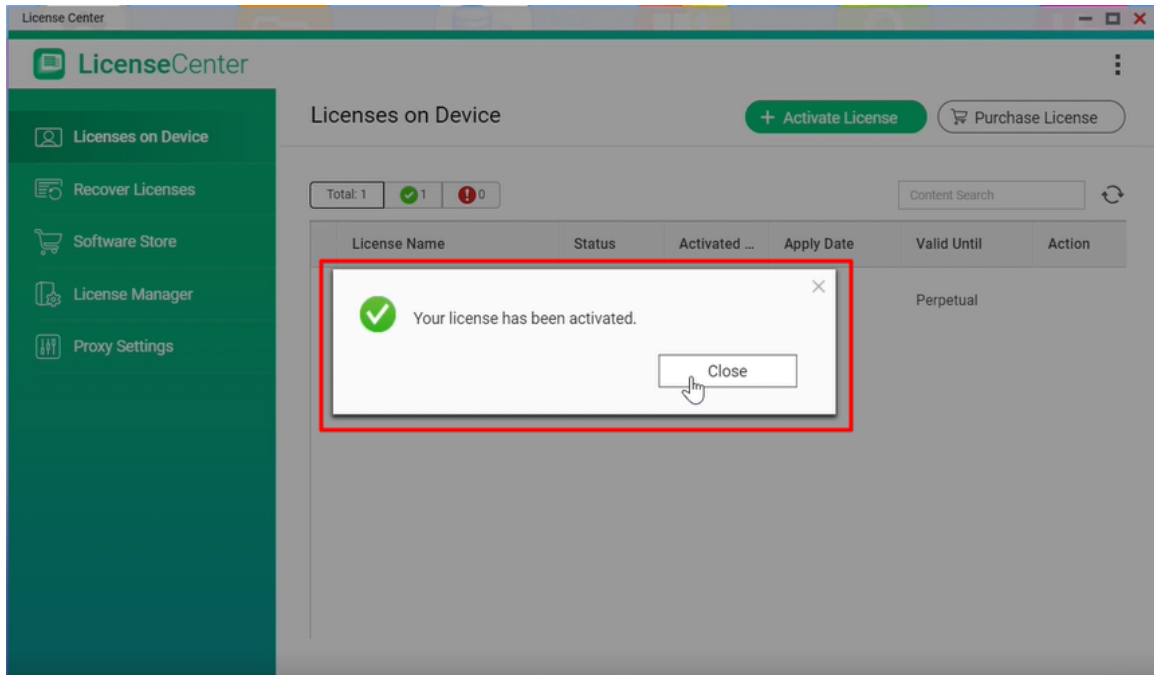
Step 4: Specify the key. Read and agree to the terms of service. Click **Verify Key**.



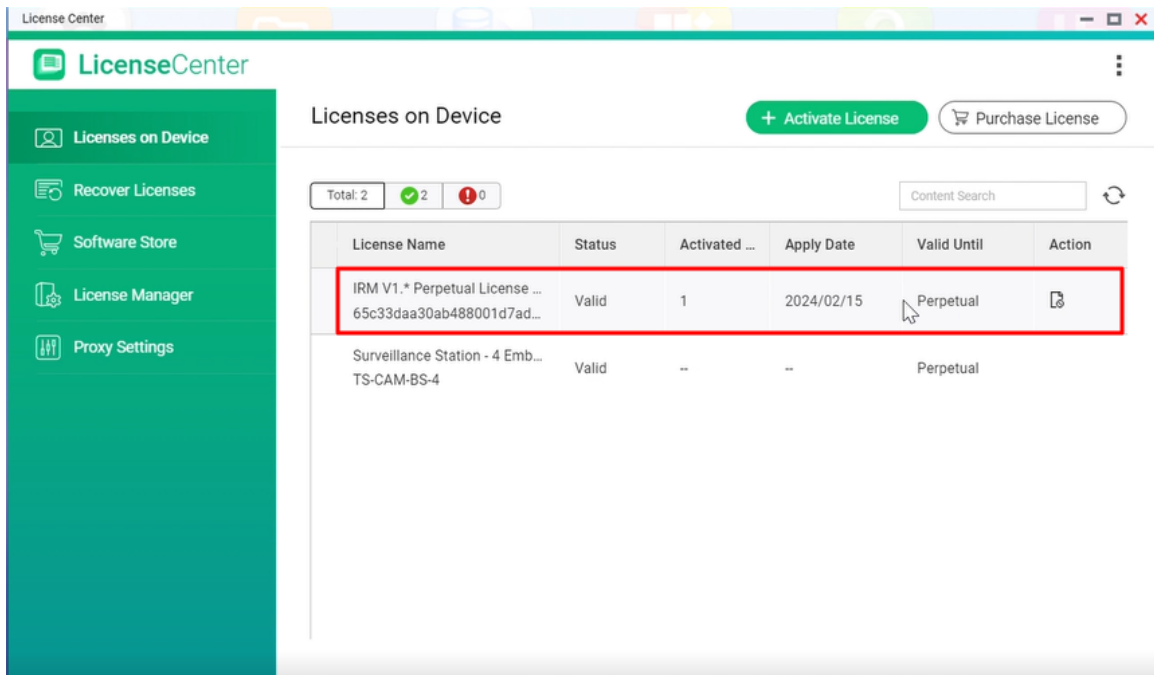
Step 5: Verify the license information, and click **Activate**.



Step 6: The license is activated. A confirmation message appears. Click **Close**.



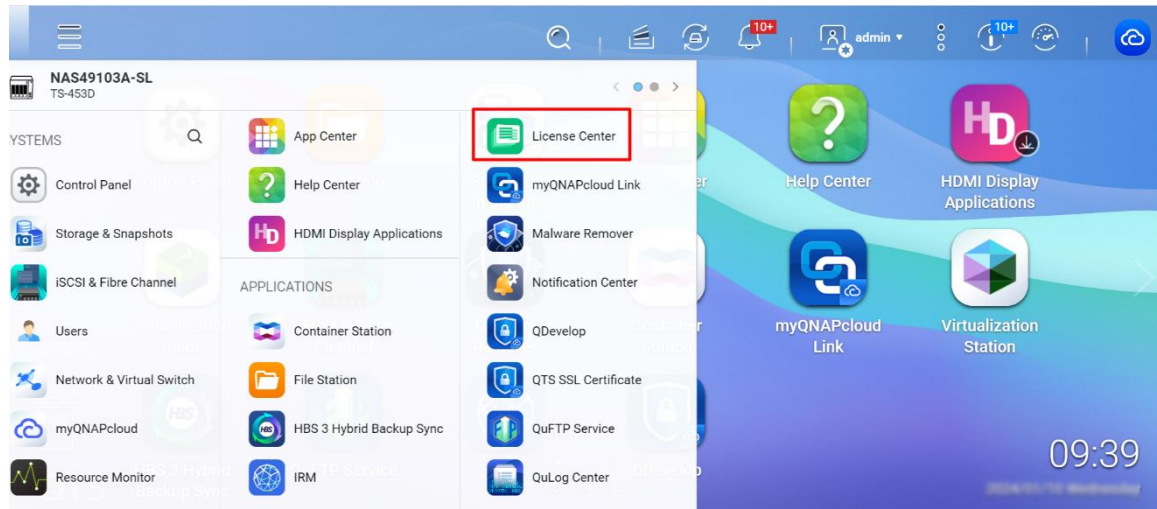
Step 7: The license appears on the list of active licenses.



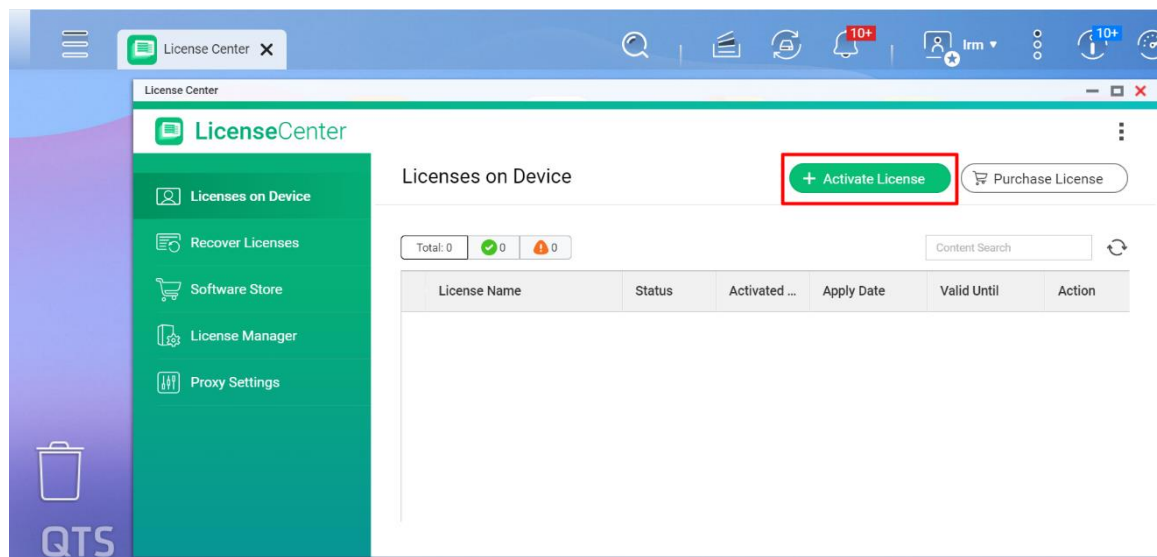
12.3.4 Activating a License Using a License Key

Before activating your license, ensure that your device is connected to the internet and you have signed in with your QNAP ID. To activate a license using a license key, follow the steps below.

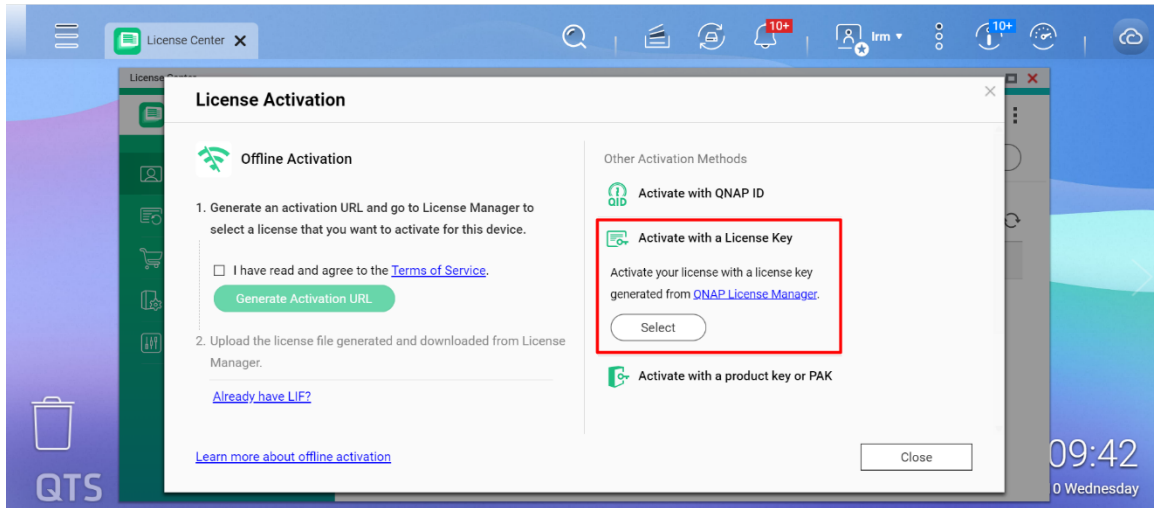
Step 1: Open License Center.



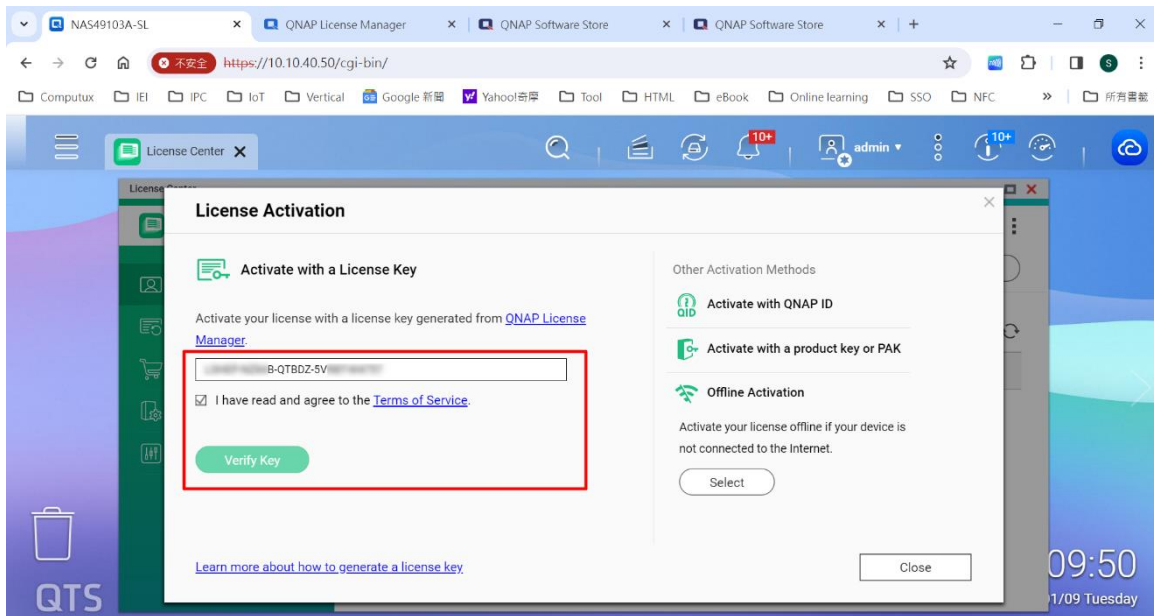
Step 2: Click **Activate License**.



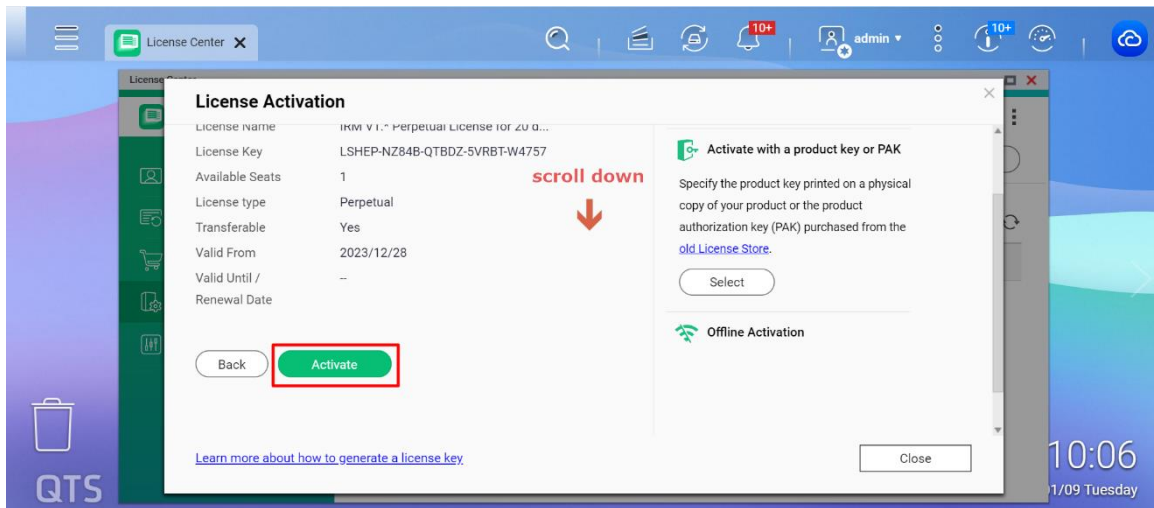
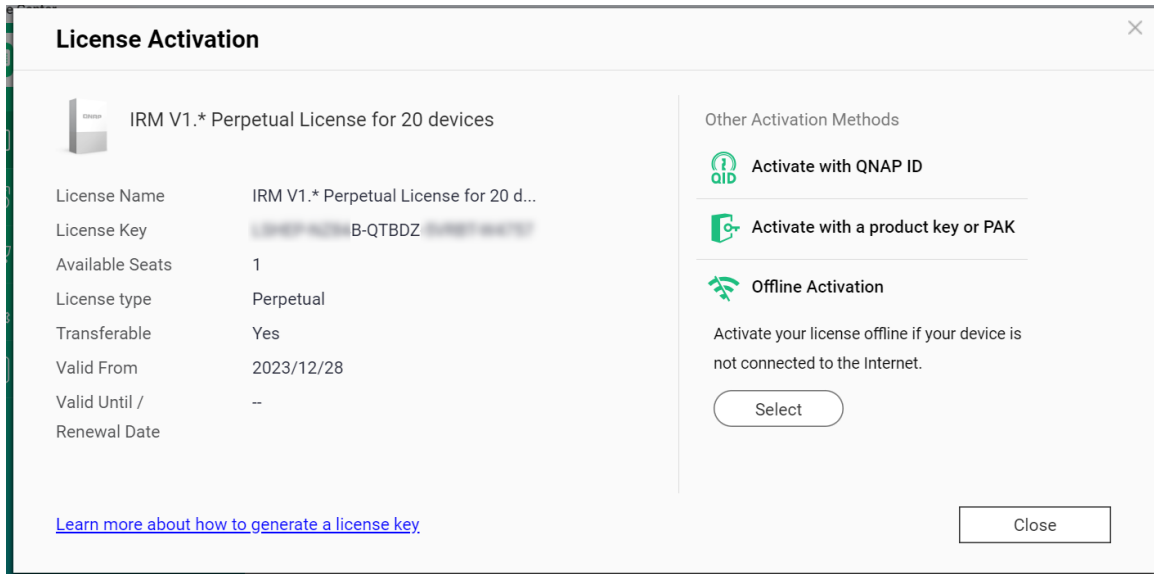
Step 3: The License Activation window appears. Select **Activate with a License Key**.



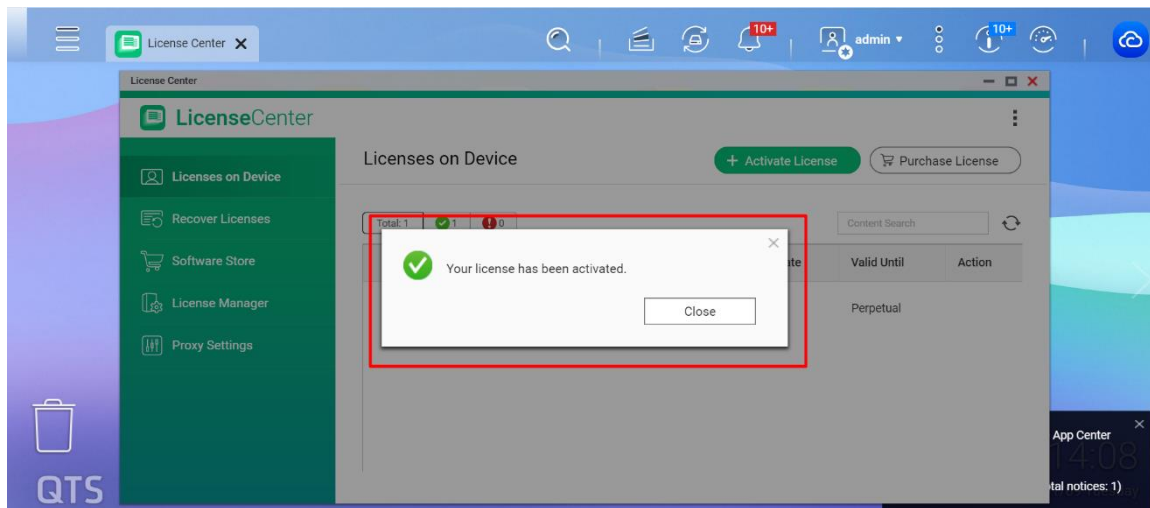
Step 4: Specify the key. Read and agree to the terms of service. Click **Verify Key**.



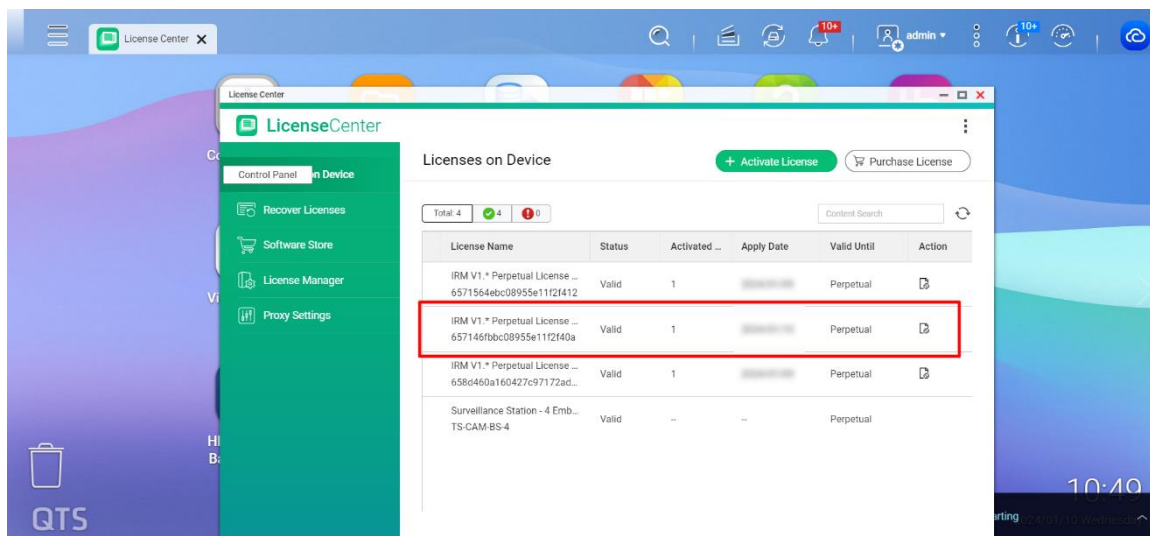
Step 5: Verify the license information. Scroll down to the bottom, and click **Activate**.



Step 6: The license is activated. A confirmation message appears. Click **Close**.



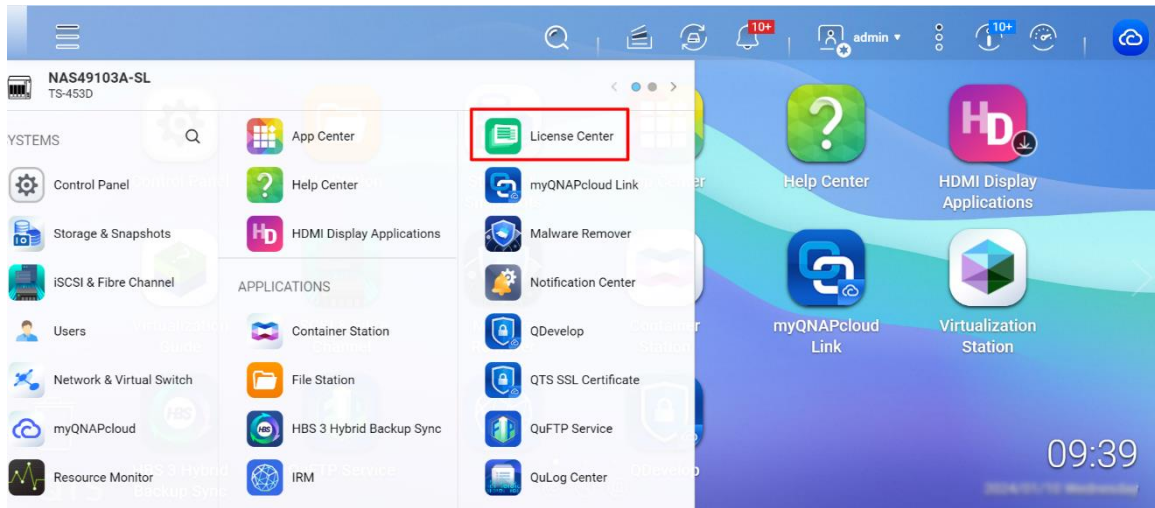
Step 7: The license appears on the list of active licenses.



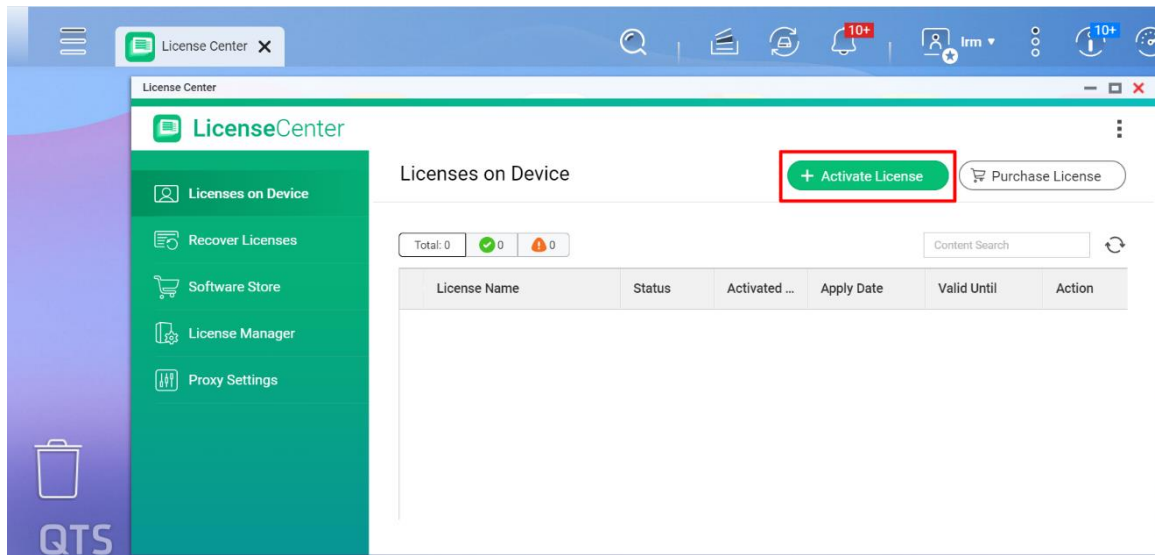
12.3.5 Activating a License Using QNAP ID

Before activating your license, ensure that your device is connected to the internet and you have signed in with your QNAP ID. To activate a license using QNAP ID, follow the steps below.

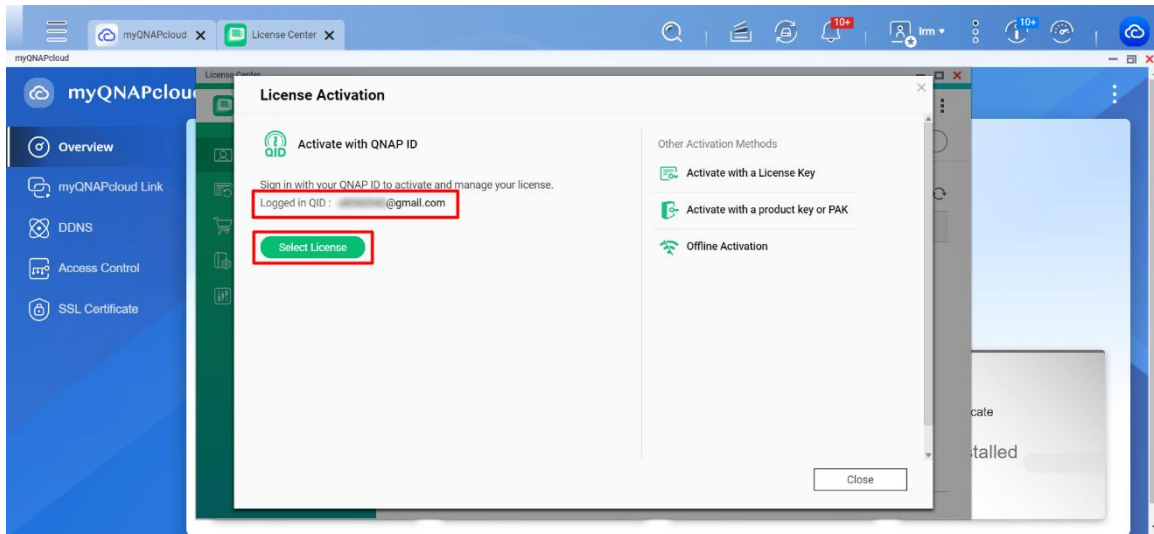
Step 1: Open License Center.



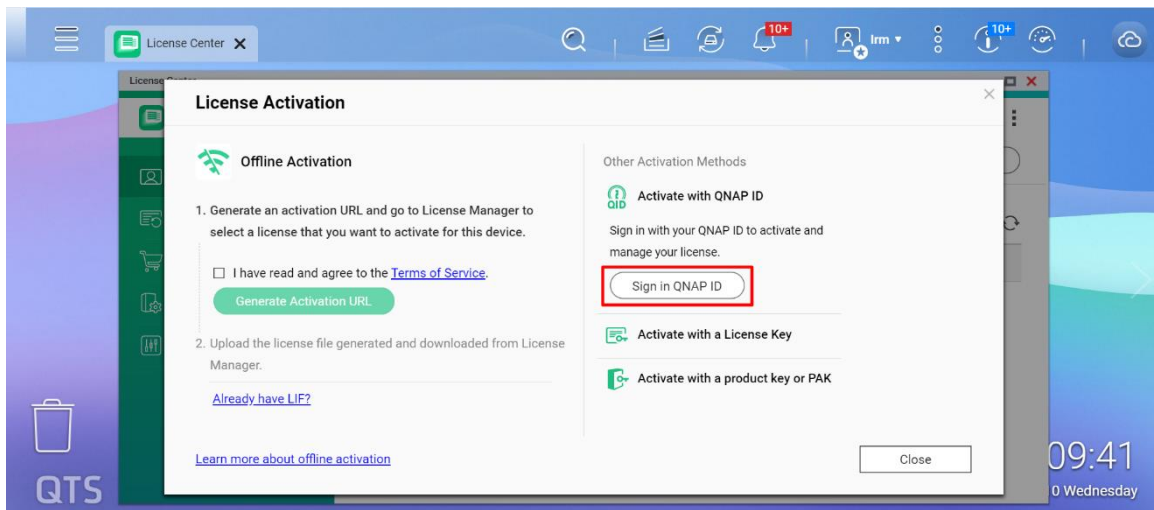
Step 2: Click Activate License.



Step 3: The License Activation window appears. In **Activate with QNAP ID**, make sure that the QID you are logged in with belongs to the license owner. Click **Select License**.



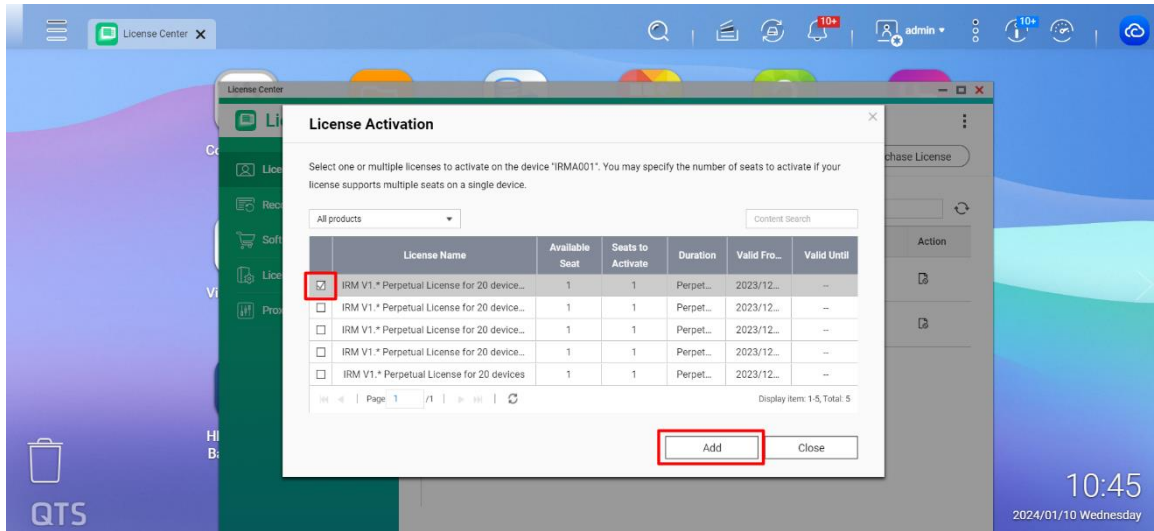
Note: You need to sign in with your QID if it is not already set to the IRM mini server. See below.



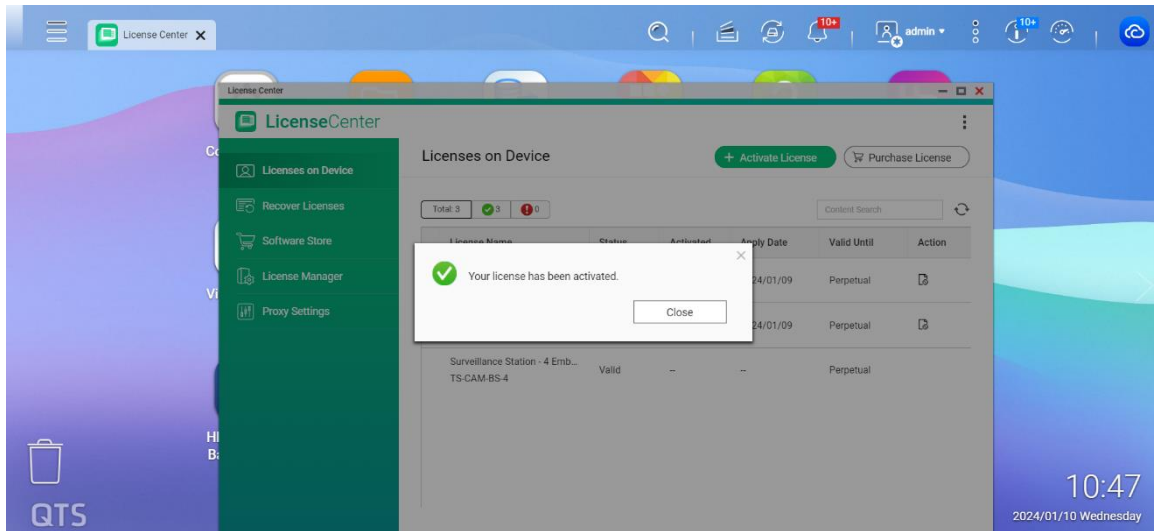
Step 4: Select a license from the list, and click **Add**.

Tip:

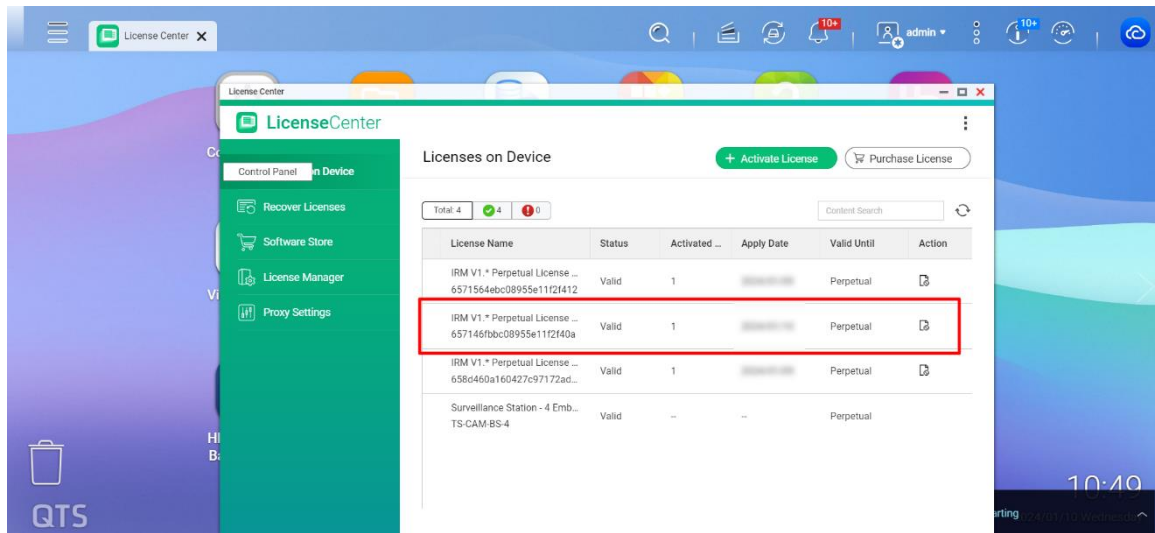
If you select a multi-seat license, you can specify the number of seats that you want to activate.



Step 5: License Center activates the license. A confirmation message appears. Click **Close**.



Step 6: The license appears on the list of active licenses.



12.3.6 License Activation Email

When an end user activates a license through the license manager or license center in the IRM Mini Server, the QID owner's mailbox will receive the following email.

Dear Sir/Madam,

Congratulations! You have successfully activated your IRM V1.* Perpetual License for 20 devices (5) license.

Product	IRM V1.* Perpetual License for 20 devices (5)
License ID	658d460a160427c97172ad0e
License Key	-----QTBDZ-5*-----
Valid until	Perpetual
Activated by	-----

12.3.7 How to Check Your Activated IRM License

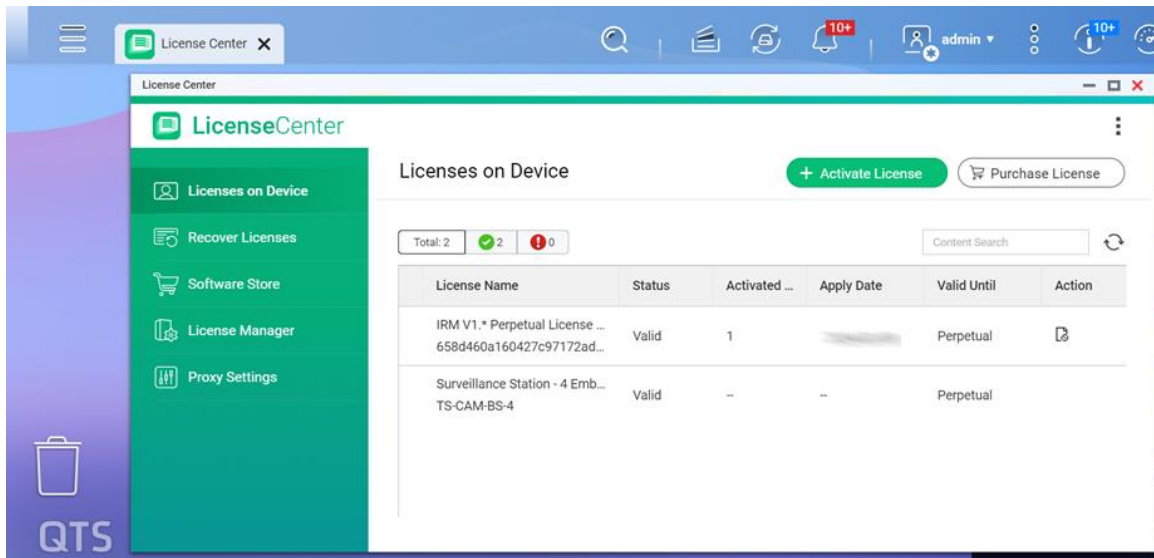
You can check your activated IRM license from **IRM** → **About**.

The screenshot shows the IRM web interface. In the top right corner, a dropdown menu is open, with the 'About' option highlighted in red. Below this, the 'About' dialog box is displayed, also with a red border. The dialog contains the following information:

- IRM logo and version: Version 1.4.18 (2025-12-22)
- Licensing Information - Not Installed (Redundancy Plan Limit: 3)
- A table with the following columns: Status, Name, Activated Date, Client Quantity, Detail. The table is currently empty, displaying 'No data could be shown.'
- IEI logo and website: www.ieiworld.com
- Copyright: ©2025 IEI Integration Corp. All Rights Reserved.

The background dashboard shows various monitoring widgets, including 'Server Health Overview', 'Shutdown Devices', and 'CPU Utilization'. A table of 'Shutdown Devices' is visible on the right side of the dashboard.

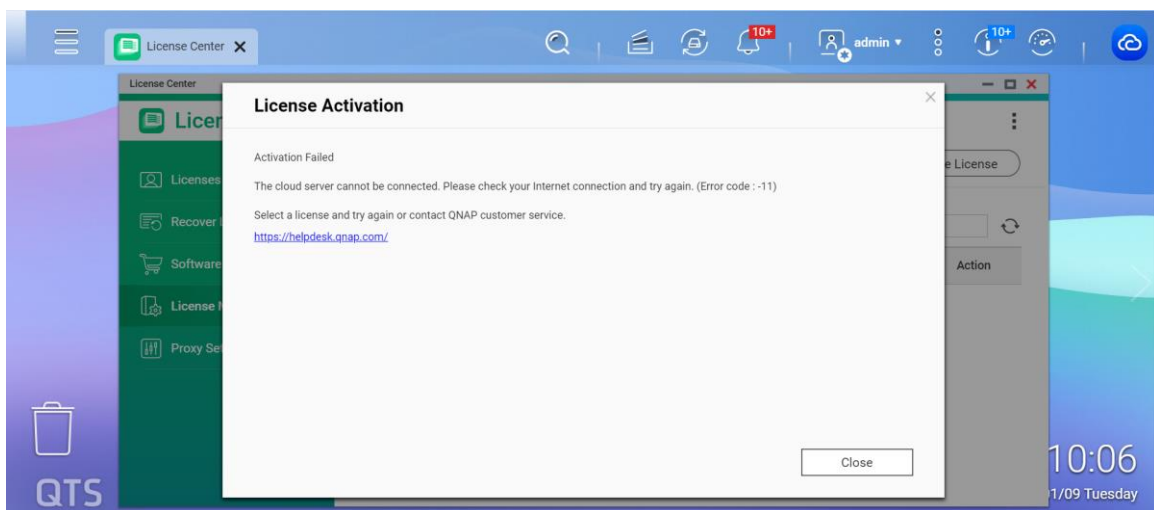
You can also check your activated IRM license in the License Center.



12.3.8 Activation Failed

If you fail to activate your license, please

1. contact with IEI if your license is bought from IEI
2. contact with QNAP helpdesk if your license is bought from QNAP Software Store



12.4 Checking and Buy License

Step 1: Go to IRM landing page to select your license and ordering from your IEI account sales.

- Step 2:** IEI account sales will send your License to let you to import to your License Center APP in IRM Server and your can check your license detail from License Manager (<https://license.qnap.com/>) website.
- Step 3:** Login License Manager (<https://license.qnap.com/>) website and Sign in with your QNAP ID.
- Step 4:** Locate the product on the list, and then click **SUBSCRIPTION**.
- Step 5:** The license details appear.
- Step 6:** You can activate your license right after the purchase or at a later time. For details, see **Section 12.3 License Activation**.

12.5 Deactivating a License for License Migration

12.5.1 Migrating an Activated License

If the license is already activated on an IRM mini server, the license should be deactivated online or offline before applying the license to a new IRM mini server.

If you can still access your old device

- Step 1:** Deactivate a license by following the instructions on License Deactivation
- Step 2:** Activate the license on the new IRM mini server by following the instructions on License Activation

If you cannot access your old device, or it is not functioning.

- Step 1:** Go to QNAP Customer Service and submit a support ticket for license deactivation. Our customer support team may ask you to provide further information before the process.
- Step 2:** Once the license is deactivated, activate the license on the new IRM mini server by following the instructions on License Activation

12.5.2 License Deactivation

You can deactivate IRM licenses using the following methods

Activation Method	Description
-------------------	-------------

Using QNAP ID (QID)	Licenses purchased through Software Store are stored in your QNAP ID account, and can be accessed through both License Center and the QNAP License Manager website. To deactivate this type of license, see Deactivating a License Using QNAP ID .
Offline	Use this method when the device is not connected to the internet. For details, see Deactivating a License Offline .