

v4.0



# **ASUS Control Center**

## **User Guide**

**Copyright © 2025 ASUSTeK COMPUTER INC. All Rights Reserved.**

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK COMPUTER INC. ("ASUS").

ASUS provides this manual "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties or conditions of merchantability or fitness for a particular purpose. In no event shall ASUS, its directors, officers, employees, or agents be liable for any indirect, special, incidental, or consequential damages (including damages for loss of profits, loss of business, loss of use or data, interruption of business and the like), even if ASUS has been advised of the possibility of such damages arising from any defect or error in this manual or product.

Specifications and information contained in this manual are furnished for informational use only, and are subject to change at any time without notice, and should not be construed as a commitment by ASUS. ASUS assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including the products and software described in it.

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.



# Contents

|                        |      |
|------------------------|------|
| About this guide ..... | viii |
|------------------------|------|

## Chapter 1: Getting Started

|            |                                                           |             |
|------------|-----------------------------------------------------------|-------------|
| <b>1.1</b> | <b>Introduction to ASUS Control Center .....</b>          | <b>1-2</b>  |
| 1.1.1      | How ASUS Control Center works.....                        | 1-2         |
| 1.1.2      | ASUS Control Center Licensing .....                       | 1-3         |
| <b>1.2</b> | <b>Installation .....</b>                                 | <b>1-5</b>  |
| 1.2.1      | Installing the hypervisor and importing the OVA file..... | 1-5         |
| 1.2.2      | Setting up the VM specification.....                      | 1-7         |
| <b>1.3</b> | <b>Initialize settings.....</b>                           | <b>1-8</b>  |
| 1.3.1      | Initialize startup settings .....                         | 1-8         |
| 1.3.2      | Logging into ASUS Control Center .....                    | 1-11        |
| <b>1.4</b> | <b>ASUS Control Center layout .....</b>                   | <b>1-12</b> |
| 1.4.1      | Banner.....                                               | 1-12        |

## Chapter 2: Monitor

|            |                                 |             |
|------------|---------------------------------|-------------|
| <b>2.1</b> | <b>System Overview.....</b>     | <b>2-2</b>  |
| 2.1.1      | Status Dashboard .....          | 2-3         |
| 2.1.2      | Devices list.....               | 2-8         |
| 2.1.3      | Search Options .....            | 2-14        |
| 2.1.4      | Search and Filter Devices ..... | 2-21        |
| <b>2.2</b> | <b>Device Information .....</b> | <b>2-26</b> |
| 2.2.1      | Hardware Sensor .....           | 2-28        |
| 2.2.2      | Utilization .....               | 2-34        |
| 2.2.3      | Inventory.....                  | 2-40        |
| 2.2.4      | Software .....                  | 2-42        |
| 2.2.5      | Event Log .....                 | 2-51        |
| 2.2.6      | BMC .....                       | 2-62        |
| 2.2.7      | BIOS.....                       | 2-64        |
| 2.2.8      | Security.....                   | 2-72        |
| 2.2.9      | Configuration .....             | 2-75        |
| 2.2.10     | GPU.....                        | 2-78        |
| <b>2.3</b> | <b>VM Overview .....</b>        | <b>2-87</b> |
| <b>2.4</b> | <b>Storage Overview.....</b>    | <b>2-89</b> |
| <b>2.5</b> | <b>OOB Overview.....</b>        | <b>2-91</b> |

# Contents

|            |                                  |              |
|------------|----------------------------------|--------------|
| <b>2.6</b> | <b>Host Information .....</b>    | <b>2-93</b>  |
| 2.6.1      | Hardware Sensor .....            | 2-94         |
| 2.6.2      | VM Information .....             | 2-99         |
| <b>2.7</b> | <b>Redfish Information .....</b> | <b>2-104</b> |
| 2.7.1      | Hardware Sensor .....            | 2-106        |
| 2.7.2      | Network.....                     | 2-107        |
| 2.7.3      | Event Log .....                  | 2-109        |

## Chapter 3: Deployment

|            |                                   |             |
|------------|-----------------------------------|-------------|
| <b>3.1</b> | <b>Agent Management .....</b>     | <b>3-2</b>  |
| 3.1.1      | Deploy Agents.....                | 3-3         |
| 3.1.2      | Scan and Deploy.....              | 3-14        |
| 3.1.3      | Remove agents.....                | 3-19        |
| 3.1.4      | Windows Agent .....               | 3-27        |
| 3.1.5      | Linux Agent .....                 | 3-31        |
| 3.1.6      | Agent Deploy Report .....         | 3-33        |
| <b>3.2</b> | <b>Agentless Management .....</b> | <b>3-34</b> |
| 3.2.1      | Add vSphere .....                 | 3-35        |
| 3.2.2      | Remove vSphere .....              | 3-40        |
| 3.2.3      | Add Redfish .....                 | 3-41        |
| 3.2.4      | Remove Redfish .....              | 3-46        |
| 3.2.5      | Redfish Profile.....              | 3-47        |
| 3.2.6      | Redfish Change Password .....     | 3-57        |
| 3.2.7      | Add Storage.....                  | 3-58        |
| 3.2.8      | Remove Storage.....               | 3-59        |

# Contents

## Chapter 4: Centralized

|            |                                     |             |
|------------|-------------------------------------|-------------|
| <b>4.1</b> | <b>Metadata Management.....</b>     | <b>4-2</b>  |
| <b>4.2</b> | <b>BIOS Flash Management.....</b>   | <b>4-12</b> |
| 4.2.1      | BIOS Cache.....                     | 4-13        |
| 4.2.2      | BIOS Flash Task.....                | 4-15        |
| 4.2.3      | BIOS Flash Task Report.....         | 4-20        |
| <b>4.3</b> | <b>Security Management.....</b>     | <b>4-21</b> |
| 4.3.1      | Device Access Control.....          | 4-22        |
| 4.3.2      | Software Blocklist.....             | 4-24        |
| 4.3.3      | Policy Management.....              | 4-26        |
| <b>4.4</b> | <b>Software Dispatch.....</b>       | <b>4-28</b> |
| 4.4.1      | Software Pool.....                  | 4-29        |
| 4.4.2      | Software Dispatch Task.....         | 4-33        |
| 4.4.3      | Software Dispatch Task Report.....  | 4-36        |
| <b>4.5</b> | <b>Task Scheduler.....</b>          | <b>4-37</b> |
| <b>4.6</b> | <b>Power Control.....</b>           | <b>4-48</b> |
| <b>4.7</b> | <b>Firmware Management.....</b>     | <b>4-50</b> |
| 4.7.1      | Edit Host.....                      | 4-51        |
| 4.7.2      | Firmware Information.....           | 4-52        |
| 4.7.3      | Firmware Update.....                | 4-53        |
| 4.7.4      | Redfish Firmware Cache.....         | 4-54        |
| 4.7.5      | Redfish Firmware Update.....        | 4-55        |
| 4.7.6      | Firmware Update Summary.....        | 4-56        |
| 4.7.7      | Redfish Firmware Update Report..... | 4-56        |

# Contents

## Chapter 5: Report

|            |                                    |             |
|------------|------------------------------------|-------------|
| <b>5.1</b> | <b>Software Report .....</b>       | <b>5-2</b>  |
| 5.1.1      | Software Inventory.....            | 5-2         |
| 5.1.2      | Hotfix Report (Windows only).....  | 5-9         |
| 5.1.3      | License Report.....                | 5-13        |
| 5.1.4      | Service Report .....               | 5-15        |
| 5.1.5      | Application Usage Analysis.....    | 5-22        |
| 5.1.6      | Application Change Log .....       | 5-23        |
| <b>5.2</b> | <b>Hardware Report.....</b>        | <b>5-26</b> |
| 5.2.1      | Hardware Inventory.....            | 5-27        |
| 5.2.2      | Hardware Inventory Change Log..... | 5-35        |
| <b>5.3</b> | <b>Task Report .....</b>           | <b>5-36</b> |
| 5.3.1      | Software Dispatch Report.....      | 5-37        |
| 5.3.2      | BIOS Flash Report.....             | 5-38        |
| 5.3.3      | Agent Update Report.....           | 5-39        |
| 5.3.4      | Agent Deploy Report .....          | 5-40        |

## Chapter 6: Notification

|            |                                 |             |
|------------|---------------------------------|-------------|
| <b>6.1</b> | <b>Conditional Trigger.....</b> | <b>6-2</b>  |
| 6.1.1      | Trust Software Asset.....       | 6-3         |
| 6.1.2      | Focus Software Asset.....       | 6-5         |
| 6.1.3      | Hardware Asset .....            | 6-7         |
| 6.1.4      | Hardware & Utilization.....     | 6-9         |
| <b>6.2</b> | <b>Subscription.....</b>        | <b>6-22</b> |
| 6.2.1      | Subscription Report .....       | 6-23        |

# Contents

## Chapter 7: Account Management

|       |                                |      |
|-------|--------------------------------|------|
| 7.1   | Role Privilege Management..... | 7-2  |
| 7.2   | Accounts Management .....      | 7-10 |
| 7.3   | System Audit Log .....         | 7-19 |
| 7.3.1 | System audit log events.....   | 7-19 |

## Chapter 8: Options

|       |                                |      |
|-------|--------------------------------|------|
| 8.1   | General Configuration.....     | 8-2  |
| 8.2   | Network Configuration .....    | 8-5  |
| 8.3   | Appearance Configuration.....  | 8-7  |
| 8.4   | Security Configuration .....   | 8-10 |
| 8.4.1 | Agent Uninstall Password ..... | 8-11 |
| 8.4.2 | BIOS Setting Password .....    | 8-13 |
| 8.5   | SMTP Settings.....             | 8-16 |
| 8.6   | Backup & Restore .....         | 8-20 |
| 8.7   | Maintenance .....              | 8-30 |
| 8.8   | DBExpose Configuration .....   | 8-32 |
| 8.9   | Update.....                    | 8-37 |
| 8.10  | Access Control List .....      | 8-42 |
| 8.11  | Customize Page.....            | 8-44 |
| 8.12  | Sensor Threshold.....          | 8-50 |
| 8.13  | Software List.....             | 8-51 |

## Chapter 9: License

|     |                          |     |
|-----|--------------------------|-----|
| 9.1 | License Information..... | 9-2 |
|-----|--------------------------|-----|

## Appendix

|                           |     |
|---------------------------|-----|
| System Requirements ..... | A-2 |
| Service and Support.....  | A-4 |

# About this guide

## Audience

This user guide is intended for system integrators, and experienced users with basic knowledge of configuring a server.

## Contents

This guide contains the following parts:

### **Chapter 1: Getting Started**

This chapter provides an overview of ASUS Control Center, as well as the installation and initialization of the ASUS Control Center.

### **Chapter 2: Monitor**

This chapter describes the various monitoring tools and options available.

### **Chapter 3: Deployment**

This chapter describes how to deploy ASUS Control Center agents and remove agents through Microsoft® Active Directory or manually. You may also add and manage agentless vSphere.

### **Chapter 4: Centralized**

This chapter describes centralized management of metadata, BIOS flash, security, software, tasks, and power control of ASUS Control Center managed devices.

### **Chapter 5: Report**

This chapter describes the various reports ASUS Control Center generates from tasks, software, and hardware related subscriptions.

### **Chapter 6: Notification**

This chapter describes notification rules and asset report options.

### **Chapter 7: Account Management**

This chapter describes how to add and edit accounts and roles for different users.

### **Chapter 8: Options**

This chapter describes system, network, appearance, security, SMTP, backup and restore, maintenance, DBExpose, update, access control, sensor threshold, and software list configuration options.

### **Chapter 9: License**

This chapter describes the license settings.

### **Appendix**

This appendix includes additional information on system requirements and contact information.

## Conventions

To make sure that you perform certain tasks properly, take note of the following symbols used throughout this manual.



**DANGER/WARNING:** Information to prevent injury to yourself when trying to complete a task.



**CAUTION:** Information to prevent damage to the components when trying to complete a task.



**IMPORTANT:** Instructions that you **MUST** follow to complete a task.



**NOTE:** Tips and additional information to help you complete a task.

## Typography

**Bold text**

Indicates a menu or an item to select.

*Italics*

Used to emphasize a word or a phrase.

<Key>

Keys enclosed in the less-than and greater-than sign means that you must press the enclosed key.

Example: <Enter> means that you must press the Enter or Return key.

<Key1>+<Key2>+<Key3>

If you must press two or more keys simultaneously, the key names are linked with a plus sign (+).

Example: <Ctrl>+<Alt>+<Del>

Command

Means that you must type the command exactly as shown, then supply the required item or value enclosed in brackets.

Example: At the command prompt, type the command line: **format A: /S**

## Reference

Visit the ASUS websites that provide updated information for all ASUS hardware and software products.





# Chapter 1

This chapter provides an overview of ASUS Control Center, and how to install it.

# Getting Started

## **1.1 Introduction to ASUS Control Center**

Welcome! The ASUS Control Center is a server management solution that gives a vital distinction to our servers, and is also compatible with our ASUS commercial products. In server management, system stability is a major factor, with efficiency, cost-effectiveness, and convenience following close behind. To comply with this, we have created a reliable and user-friendly monitoring tool. The ASUS Control Center is a web-based interface that allows system administrators to conveniently manage computers either locally or remotely using a web-browser. With its colorful, graphical, and informative interface, the ASUS Control Center makes server management a delightful experience!

### **1.1.1 How ASUS Control Center works**

The ASUS Control Center is composed of “agents” that generally act as data collectors, and a set of HTTPS web pages that serve as the user interface (UI). The data collected by the agent, which are essential for the continuous monitoring operations performed by ASUS Control Center, are displayed in the UI.

In the monitoring process, the agent basically keeps track of the hardware and software status of the system. The agent has “sensors” that monitor fan rotation speeds, working voltages, motherboard and CPU temperatures, and the backplane (if present).

In addition, the agent also monitors hard disk drives health status through the S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) feature, space utilization of a file system, CPU or system memory loading, and even the traffic status of a network device.

The agent records the history of the detected status of all monitored hardware items. The status record includes the time of alert events (fan, voltage, or temperature), and the type of alert event (critical, warning, or normal).

You can also configure ASUS Control Center to react to exceptional situations. For example, the administrator can be automatically notified by e-mail when a hard drive starts to malfunction or when a chassis intrusion is detected. In this way, ASUS Control Center acts as an active guardian of the system's key components.

## 1.1.2 ASUS Control Center Licensing

ASUS Control Center provides two license editions:

- **Classic edition** for assisting management on ASUS servers and workstations.
- **Enterprise edition** for a comprehensive management on ASUS servers and workstations, and all supported ASUS commercial products.

---

**NOTE:** For more information on the licensing options, please refer to <https://asuscontrolcenter.asus.com> and <https://www.asus.com/microsite/csm>.

---

| Features           |                       |                        | Classic                       | Enterprise |
|--------------------|-----------------------|------------------------|-------------------------------|------------|
| Banner             | Mission Center        |                        | ✓                             | ✓          |
|                    | System Overview       |                        | Partial functions unavailable | ✓          |
| Monitor (Overview) | VM Overview           |                        | -                             | ✓          |
|                    | Host Information      |                        | -                             | ✓          |
| Monitor (one node) | Device Information    |                        | ✓                             | ✓          |
|                    | Hardware Sensor       |                        | Partial functions unavailable | ✓          |
|                    | Utilization           |                        | Partial functions unavailable | ✓          |
|                    | GPU                   |                        | -                             | ✓          |
|                    | Inventory             |                        | Partial functions unavailable | ✓          |
|                    | Event Log             |                        | Partial functions unavailable | ✓          |
|                    | Software              |                        | Partial functions unavailable | ✓          |
|                    | BMC (BMC Required)    |                        | ✓                             | ✓          |
|                    | BIOS                  |                        | ✓                             | ✓          |
|                    | Security              |                        | Partial functions unavailable | ✓          |
|                    | Configuration         |                        | Partial functions unavailable | ✓          |
| Deployment         | Agent Management      | Deploy Agents          | ✓                             | ✓          |
|                    |                       | Remove Agents          | ✓                             | ✓          |
|                    |                       | Scan and Deploy        | ✓                             | ✓          |
|                    | Agentless Management  | Add vSphere            | -                             | ✓          |
|                    |                       | Remove vSphere         | -                             | ✓          |
|                    |                       | Add Redfish            | -                             | ✓          |
|                    |                       | Remove Redfish         | -                             | ✓          |
| Centralized        | Metadata Management   |                        | ✓                             | ✓          |
|                    | BIOS Flash Management | BIOS Cache             | ✓                             | ✓          |
|                    |                       | BIOS Flash Task        | -                             | ✓          |
|                    |                       | BIOS Flash Task Report | -                             | ✓          |
|                    | Security Management   | Device Access Control  | -                             | ✓          |
|                    |                       | Software Blocklist     | -                             | ✓          |

(continued on the next page)

| Features     |                           |                               | Classic                       | Enterprise |
|--------------|---------------------------|-------------------------------|-------------------------------|------------|
| Centralized  | Software Dispatch         | Software Pool                 | ✓                             | ✓          |
|              |                           | Software Dispatch Task        | -                             | ✓          |
|              |                           | Software Dispatch Task Report | -                             | ✓          |
|              | Task Scheduler            |                               | -                             | ✓          |
|              | Power Control             |                               | -                             | ✓          |
| Report       | Software Report           | Software Inventory            | -                             | ✓          |
|              |                           | Hotfix Report                 | -                             | ✓          |
|              |                           | License Report                | -                             | ✓          |
|              |                           | Application Usage Analysis    | -                             | ✓          |
|              |                           | Service Report                | -                             | ✓          |
|              | Hardware Inventory        |                               | -                             | ✓          |
|              | Task Report               | Software Dispatch             | -                             | ✓          |
|              |                           | BIOS Dispatch                 | -                             | ✓          |
|              |                           | Agent Update                  | ✓                             | ✓          |
|              |                           | Agent Deploy                  | ✓                             | ✓          |
| Notification | Hardware & Utilization    |                               | ✓                             | ✓          |
|              | Asset Changes             | Trust Software Asset          | -                             | ✓          |
|              |                           | Focus Software Asset          | -                             | ✓          |
|              |                           | Hardware Asset                | -                             | ✓          |
| Account      | Subscription Report       |                               | -                             | ✓          |
|              | Role Privilege Management |                               | -                             | ✓          |
|              | Accounts Management       |                               | -                             | ✓          |
| Options      | General Configuration     |                               | ✓                             | ✓          |
|              | Network Configuration     |                               | ✓                             | ✓          |
|              | Appearance Configuration  |                               | -                             | ✓          |
|              | Security Configuration    |                               | Partial functions unavailable | ✓          |
|              | SMTP Settings             |                               | ✓                             | ✓          |
|              | Backup & Restore          |                               | -                             | ✓          |
|              | Maintenance               |                               | ✓                             | ✓          |
|              | DBExpose Configuration    |                               | -                             | ✓          |
|              | Update                    |                               | ✓                             | ✓          |
|              | Access Control List       |                               | -                             | ✓          |
|              | Sensor Threshold          |                               | ✓                             | ✓          |
|              | Software List             |                               | -                             | ✓          |
| License      | License                   |                               | Partial functions unavailable | ✓          |

\* Please contact your local ASUS Sales representative and/or TPM for more information on the availability of other functions this feature supports.

## 1.2 Installation

ASUS Control Center is a virtual appliance running on a virtual machine (VM), with all required services and settings pre-installed. The system requirements can be found in the **Appendix** section of this manual.

To install the ASUS Control Center on the VM, please refer to the following sections.

### 1.2.1 Installing the hypervisor and importing the OVA file

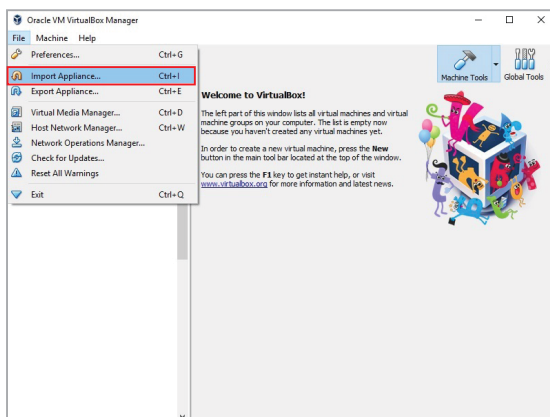
**NOTE:** Oracle Virtualbox will be used as an example for Hypervisor related items.

1. Download **Oracle VirtualBox** and the **ASUS Control Center Open Virtual Appliance (OVA)** file.

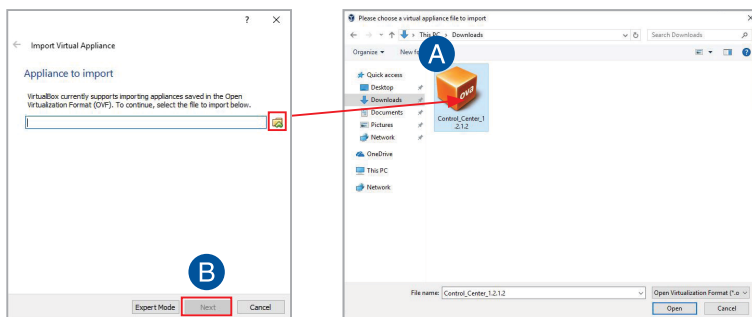
**NOTE:**

- Please refer to <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html> to download **Oracle VirtualBox**.
- Please contact your local ASUS sales representative for the **ASUS Control Center OVA** file.

2. Install and launch **Oracle VirtualBox**, then select **File > Import Appliance...** to launch the **Import Virtual Appliance** wizard.

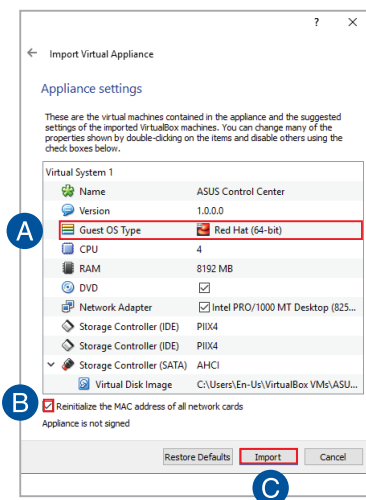


3. Select the OVA file to import (A) and click **Next** (B).



4. Ensure the **Guest OS Type** is set to **Red Hat (64-bit)** (A).
5. Check the **Reinitialize the MAC address of all network cards** checkbox (B), then click **Import** (C).

**NOTE:** The minimum requirements for the VM are 4 vCPUs, 8GB RAM, and a 100GB HDD.



6. Wait for the OVA file to be imported. This may take a few minutes.
7. Select the VM on the list, then click **Start** on the toolbar to start the VM.

**NOTE:**

If your **Oracle VirtualBox** installation was unsuccessful, please check the following:

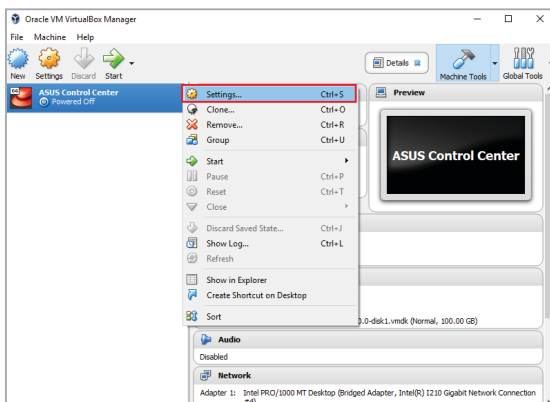
- Check if VT-x is enabled in the BIOS:  
**BIOS > Advanced > Intel Virtualization Technology > Enabled**
- Check if the correct network card was selected:  
Select the network connection you are currently using.

## 1.2.2 Setting up the VM specification

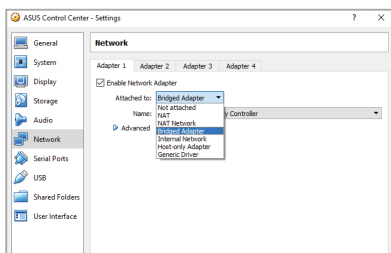
A message may appear when starting up the virtual machine (VM) for the first time, follow the steps below to set up the VM specification, such as network settings:

**NOTE:** Ensure your system meets the system requirements listed in the **Appendix** chapter.

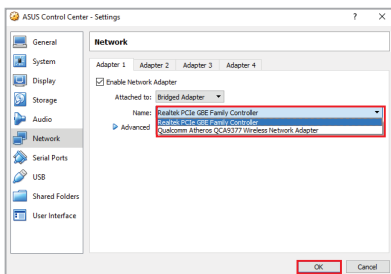
1. Right click on the VM and select **Settings**.



2. Select **Network** from the menu list on the left, then select **Bridged Adapter** in the **Attached to:** field.



3. Select the Network card you are currently using and has an Internet connection from the drop down menu in the **Name:** field, then click **OK**.



### 1.3 Initialize settings

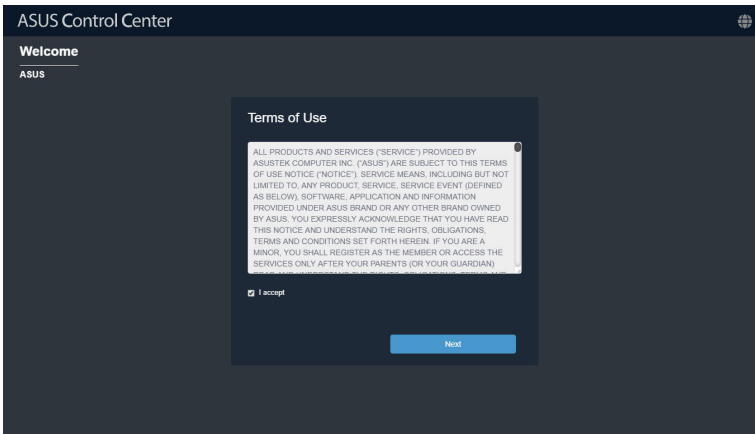
Once your ASUS Control Center is installed successfully, you will need to initialize the ASUS Control Center settings such as time zone, account and password, and network settings.

#### 1.3.1 Initialize startup settings

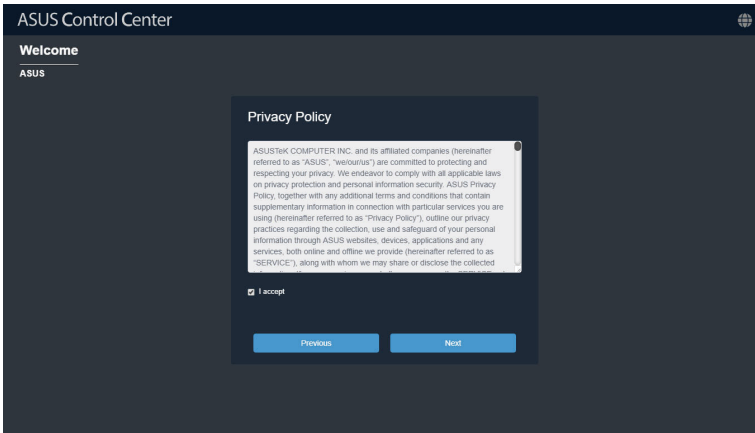
Once ASUS Control Center has launched, follow the steps below to initialize startup settings:

**NOTE:** The information entered in this section is for reference only.

1. Read through the end user license agreement, check **I accept**, then click **Next**.



2. Carefully read through the Privacy Policy, check **I accept**, then click **Next**.



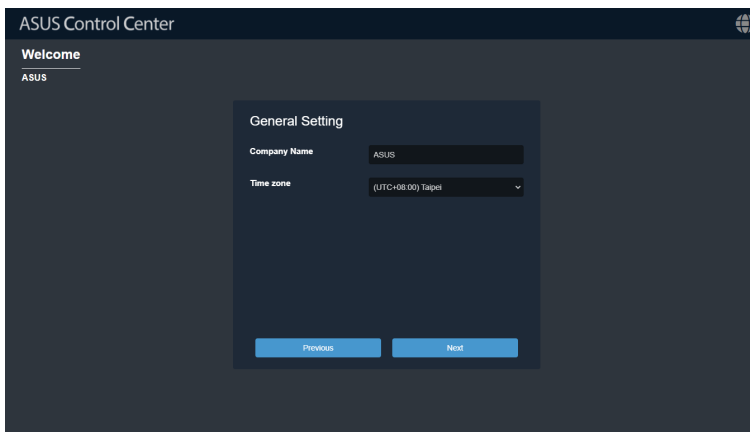


3. Enter the **Company Name**, then select the **Time Zone**. Click on **Next** once you are finished.

---

**NOTE:** When setting the **Time Zone**, ensure that the time zone selected matches the time zone displayed on the physical device which has a hypervisor installed.

---

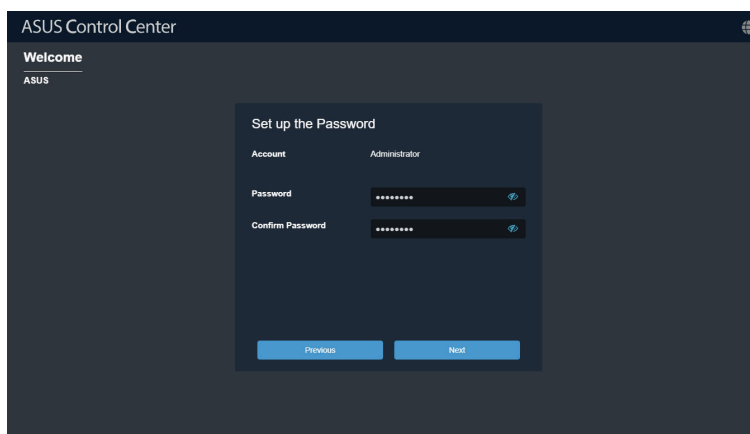


The screenshot shows the 'ASUS Control Center' interface. At the top, there's a 'Welcome' section with the 'ASUS' logo. The main content area is titled 'General Setting'. It contains two fields: 'Company Name' with the value 'ASUS' and 'Time zone' with a dropdown menu showing '(UTC+08:00) Taipei'. At the bottom, there are two buttons: 'Previous' and 'Next'.

4. Enter and initialize the password, then click **Next**.

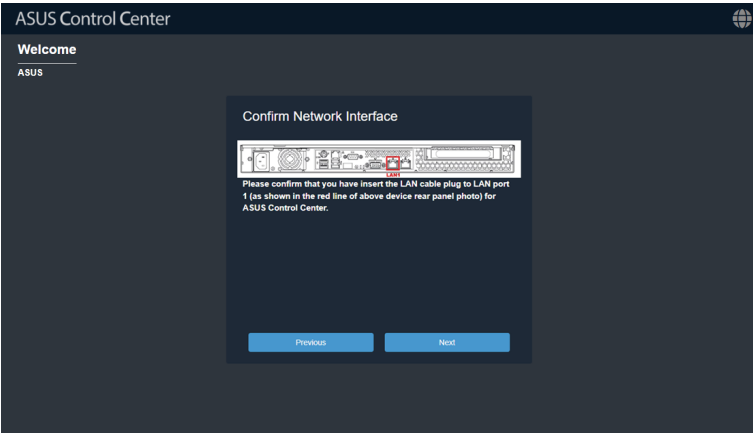
**NOTE:**

- The default ASUS Control Center administrator account is **Administrator**.
- Your password should contain at least 8 characters, and consist of at least one lower case letter, one upper case letter, one digit, and a special character.



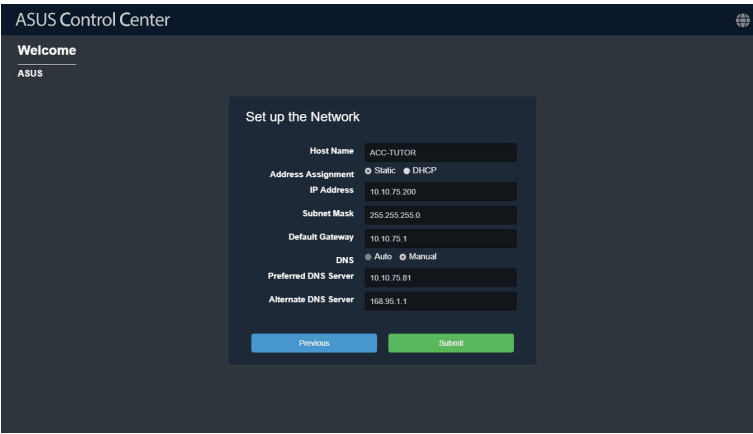
The screenshot shows the 'ASUS Control Center' interface. At the top, there's a 'Welcome' section with the 'ASUS' logo. The main content area is titled 'Set up the Password'. It contains three fields: 'Account' with the value 'Administrator', 'Password' with a masked input field (8 dots) and a toggle icon, and 'Confirm Password' with a masked input field (8 dots) and a toggle icon. At the bottom, there are two buttons: 'Previous' and 'Next'.

5. Confirm if the LAN cable is plugged into the correct LAN port, then click **Next**.

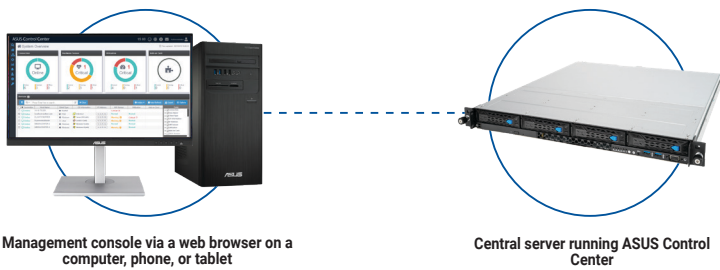


6. Set the network configurations and Host Name, then click **Submit** once you are finished with all the settings.

**NOTE:** If **Static** is selected, the IP Address and Subnet Mask should be filled in manually. If **DHCP** is selected, the IP Address and Subnet Mask will automatically be filled in.



### 1.3.2 Logging into ASUS Control Center



To log into ASUS Control Center:

1. Open a web browser and navigate to the main server URL:

| Type                           | URL format                        |
|--------------------------------|-----------------------------------|
| Connecting using a hostname    | https://<hostname>/ACC            |
|                                | Example: https://ACC-TUTOR/ACC    |
| Connecting using an IP address | https://<IP address>/ACC          |
|                                | Example: https://10.10.75.200/ACC |

**NOTE:**

- The ACC portion of the URL is case sensitive.
- Replace "ACC-TUTOR" or "10.10.75.200" with the correct hostname or IP address for your server environment.
- To connect via the HTTP protocol (less secure), replace "https://" with "http://" in the URL.
- File export and import functionality is disabled when using ACC through a virtual machine. For the optimal experience, connect using an Internet browser installed on the host system.

2. Enter your **Account** and **Password**, then click **Login** to log into ASUS Control Center.
3. If Multi-Factor Authentication (MFA) is enabled, enter the 6-digit passcode displayed in your authenticator app.

**NOTE:** Refer to the **Enabling Multi-Factor Authentication** section of the **Account Management** chapter for more information.

4. Activate or import a license key.

**NOTE:** Refer to the **Activating/Importing a License Key** section of the **License** chapter for more information.

## 1.4 ASUS Control Center layout

The main control panel of the ASUS Control Center user interface is displayed as below:



### 1.4.1 Banner

The banner features the logo of ASUS Control Center, as well as some quick functions such as the language option or the mission center.

#### Logo

You can customize the logo of your ASUS Control Center. For more details on customizing the logo for ASUS Control Center, please refer to the **Appearance Configuration** section.

## Feedback

Click  in the top right corner of the banner to bring up the ASUS Control Center Feedback window. You can provide feedback regarding your experience or on issues, and also upload screenshots using the feedback window.

## Multiple Languages

Click  in the top right corner of the banner, then select a language to change the language of ASUS Control Center. The languages currently supported are as follows: English, Traditional Chinese, Simplified Chinese, Japanese, Korean, German, Spanish, French, Russian, and Thai.

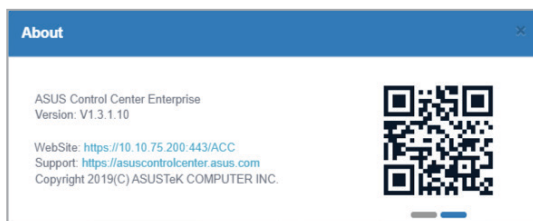
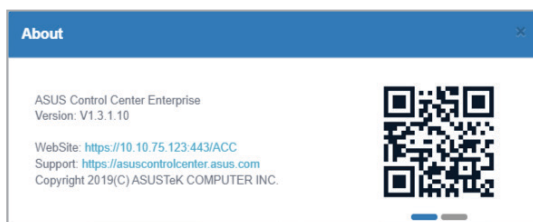
## About

Click  in the top right corner of the banner for information such as the version, and support site of ASUS Control Center. You can also scan the QR code for the mobile website version of ASUS Control Center. If you have multiple network cards, and have set the network configurations for all of them, you can slide and view the different networks and scan the QR codes to access the mobile website version of ASUS Control Center.

---

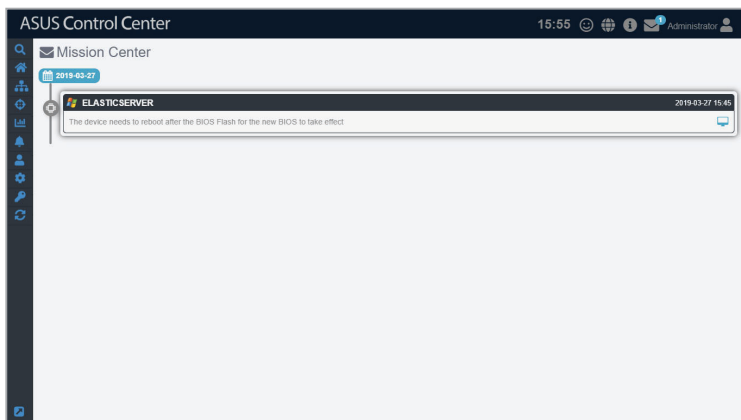
**NOTE:** For more information on setting the network configurations for all network cards, please refer to the **Network Configuration** section.

---



## Mission Center

Click  in the top right corner of the banner to access the **Mission Center**. The Mission Center automatically lists pending actions that still need to be configured on devices, such as devices which still need to be restarted after a BIOS Flash, or devices which need to be restarted in order for updates to take effect. Events or pending actions will be denoted by a blue notification circle on the **Mission Center** icon; the amount of events or pending actions will also be displayed.



## Account Information

Click  in the top right corner of the banner, you can click on **Logout** to logout of the currently logged in account, or click on **Settings** to be redirected to the **Accounts Management** screen.

---

**NOTE:** For more details on Accounts Management, please refer to the **Accounts Management** section.

---

# Chapter 2

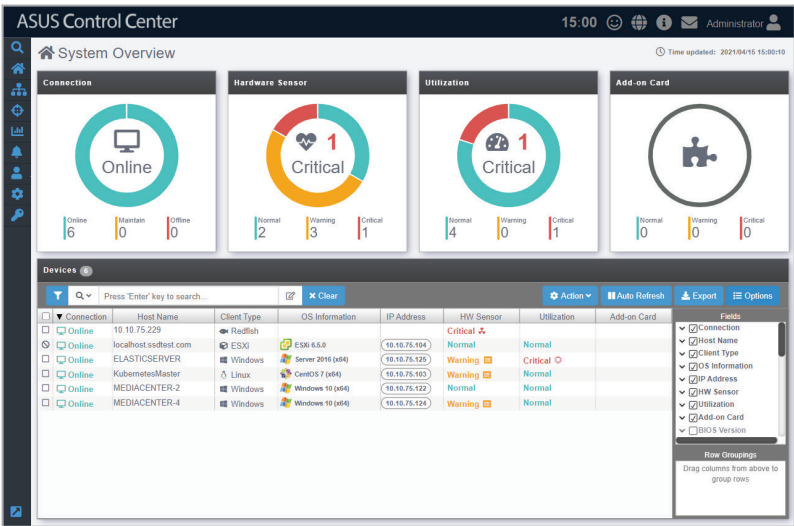
This chapter describes the various monitoring tools and options available.

# Monitor

## 2.1 System Overview

The **System Overview** screen gives you a quick overall status check for all managed devices and basic overview of device status at a glance. You may also select an individual managed device for details on its status, or perform actions such as remotely control it, power it off, or turn on its locator LED.

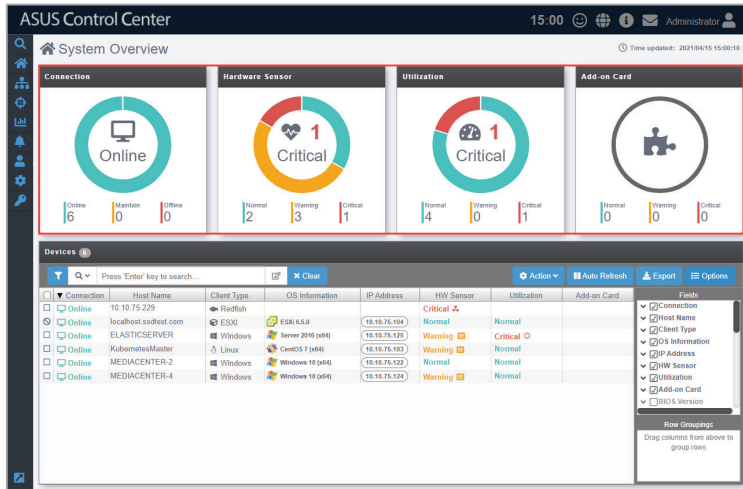
To access the **System Overview**, click  > **System Overview** from the left menu.





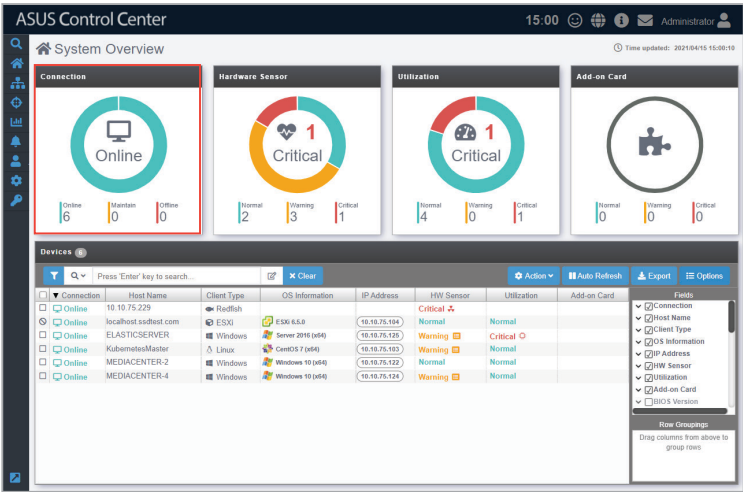
## 2.1.1 Status Dashboard

These items allow you to view a summary of the connection status, hardware status, and utilization status of all managed devices, as well as the event log of the managed devices. This will help you pinpoint problems such as connection errors, hardware sensor errors, or utilization errors at a quick glance.



Connection overview

The Connection overview circle displays the connection statuses of managed devices. The number of devices for each status is also displayed below the overview circle.



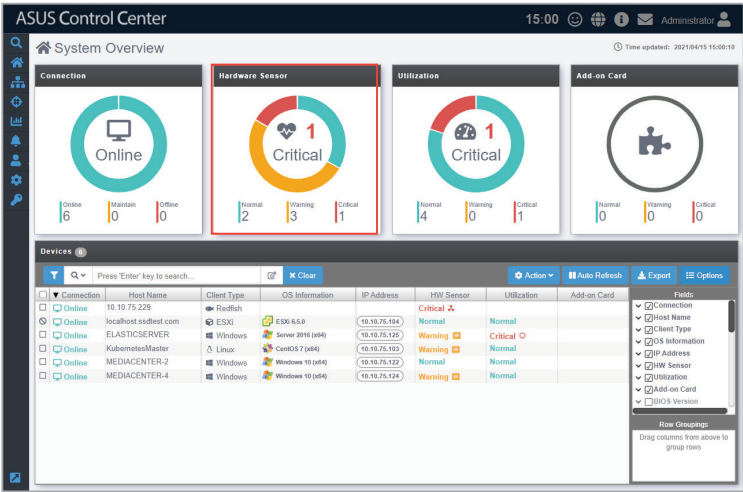
Please refer to the table below for the color status of the Connection overview circle

|                   | Green  | Orange    | Red     |
|-------------------|--------|-----------|---------|
| Connection Status | Online | Maintain* | Offline |

NOTE: This status indicates that the managed device's agent is updating.

Hardware Sensor overview

The Hardware Sensor overview circle displays an overview of the Voltage, Temperature, Fan, Backplane, Power Supply, Chassis, and S.M.A.R.T. statuses of managed devices. The number of devices for each status is also displayed below the overview circle.

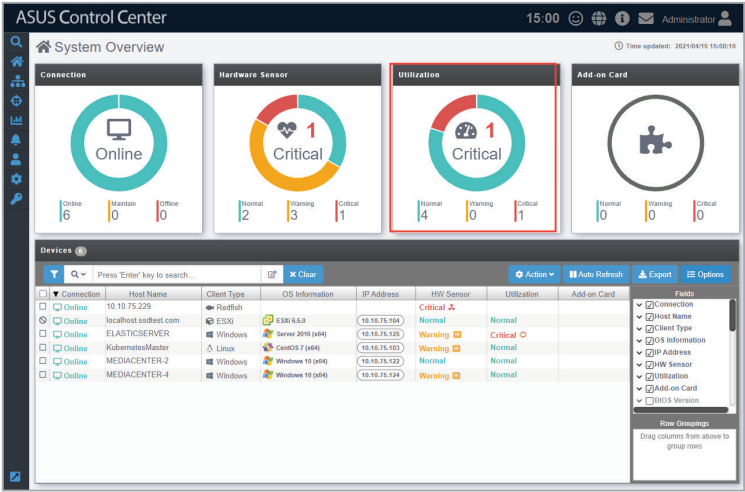


Please refer to the table below for the color status of the Hardware Sensor overview circle

|                        | Green  | Orange  | Red      |
|------------------------|--------|---------|----------|
| Hardware Sensor Status | Normal | Warning | Critical |

Utilization overview

The Utilization overview circle displays an overview of the CPU, DIMM, Partition, and Network statuses of managed devices. The number of devices for each status is also displayed below the overview circle.

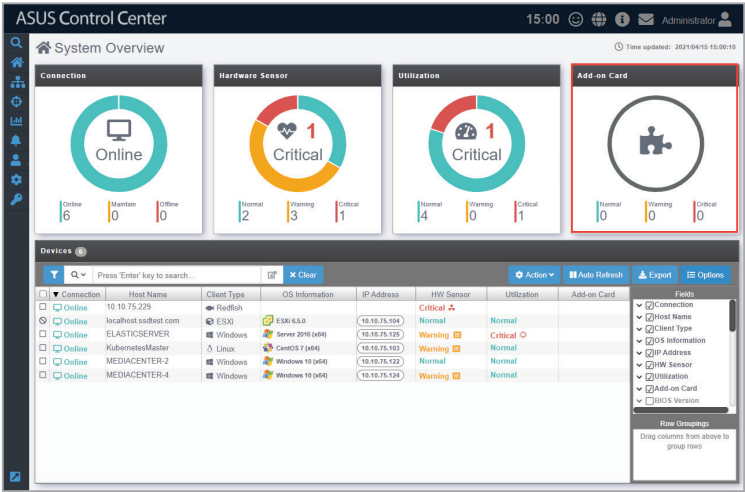


Please refer to the table below for the color status of the Utilization overview circle

|                    | Green  | Orange  | Red      |
|--------------------|--------|---------|----------|
| Utilization Status | Normal | Warning | Critical |

Add-on Card overview

The Add-on Card overview circle displays an overview of the Add-on card statuses of managed devices. The number of devices for each status is also displayed below the overview circle.



Please refer to the table below for the color status of the Add-on Card overview circle

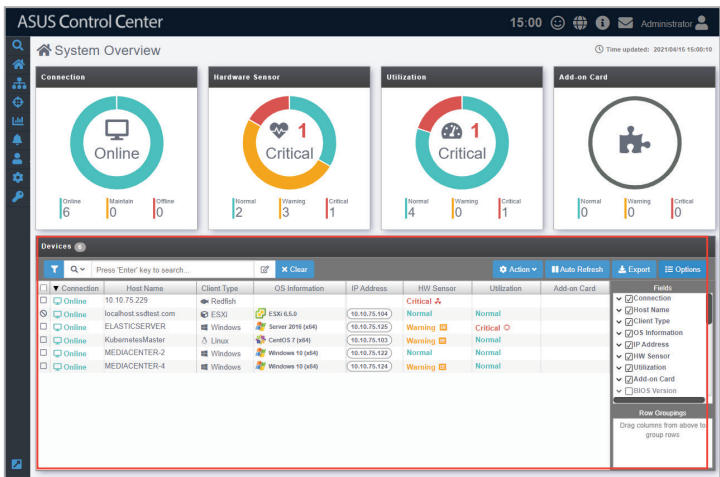
|                    | Green  | Orange  | Red      |
|--------------------|--------|---------|----------|
| Add-on Card Status | Normal | Warning | Critical |

# 2.1.2 Devices list

The **Devices** list displays all managed devices as well as the metadata on each managed device. You may also access the remote desktop for these managed devices; remotely power on, off, or reset these managed devices; or export the list of managed devices and their metadata to a .csv file. These functions provide you with a effortless method of accessing commonly used functions for managing these devices.

**NOTE:**

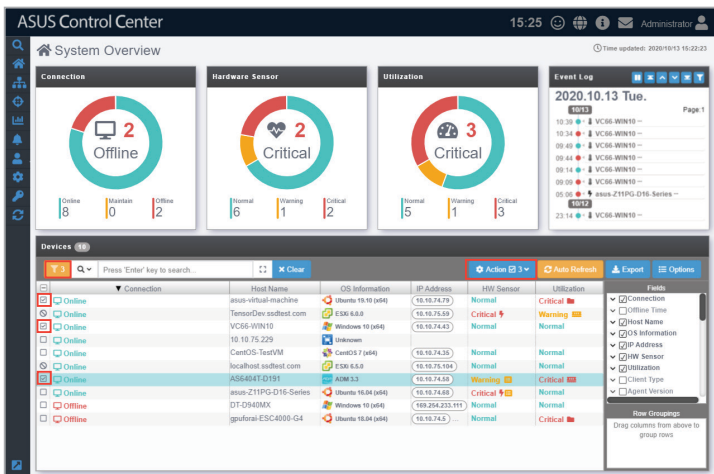
- To add more metadata columns to the **Devices** list, click on **Options**, then check the metadata item you wish to display.
- Click on the name of a column header to sort the filter results alphabetically.
- The **Devices** list will display the items that correspond to the search and filter results. For more information on using search and filter, please refer to the **Search and Filter devices** section.



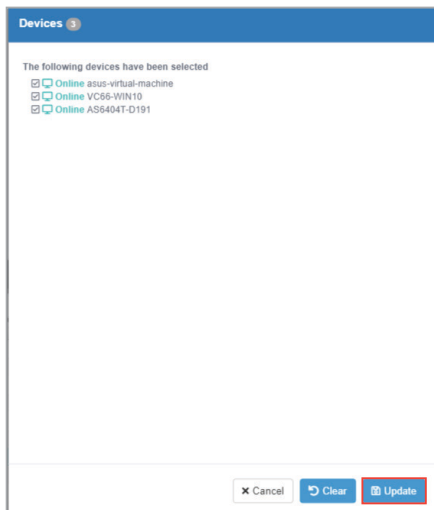
## Setting power control (Action)

You can control the power settings of selected devices from the **Devices** list allowing you quick access to power controls such as powering on and off, rebooting, and refreshing the device without having to navigate to **Power Control** located under **Centralized** or **Device Information**.

1. Select the devices you would like to apply the power control option to.
2. Click on the . You can check or uncheck items in the popup window that appears, confirm that the correct devices are selected, then click **Update**.

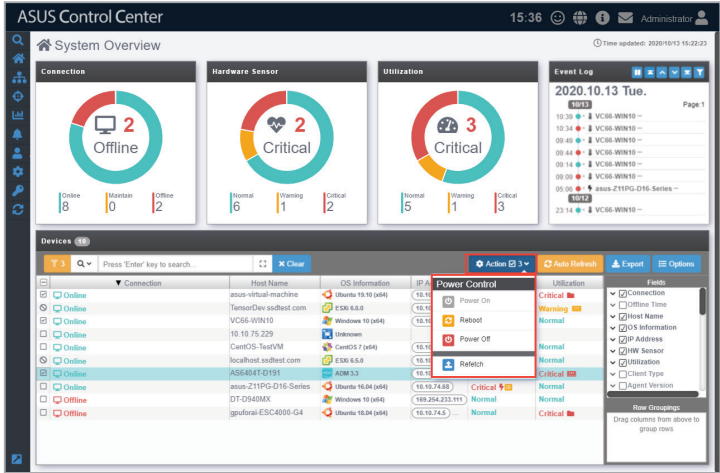


The screenshot shows the ASUS Control Center interface. The top navigation bar includes 'System Overview', 'Connection', 'Hardware Sensor', 'Utilization', and 'Event Log'. The 'Devices' section is active, displaying a table of devices with columns for Connection, Host Name, OS Information, IP Address, HW Sensor, and Utilization. The table lists several devices, including 'asus-virtual-machine', 'TensorDev.sdfest.com', 'VC66-WIN10', 'Cam05-TestVM', 'localhost.sdfest.com', 'AS6404T-D191', 'asus-Z11PG-D16-Series', 'DT-D640MX', and 'gprofzot-ESC4006-G4'. A popup window titled 'Devices' is open, showing a list of selected devices: 'Online asus-virtual-machine', 'Online VC66-WIN10', and 'Online AS6404T-D191'. The popup also includes a search bar, a 'Clear' button, and 'Cancel', 'Clear', and 'Update' buttons at the bottom.



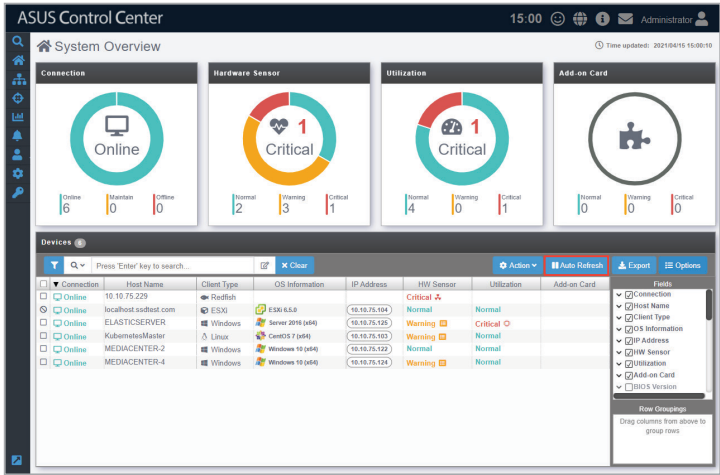
The screenshot shows the 'Devices' popup window. It has a blue header with the title 'Devices'. Below the header, it says 'The following devices have been selected'. There is a list of three devices, each with a checkbox and a status indicator: 'Online asus-virtual-machine', 'Online VC66-WIN10', and 'Online AS6404T-D191'. At the bottom of the popup, there are three buttons: 'Cancel', 'Clear', and 'Update'.

- Click on **Action**, then select the power control option you would like to apply to the selected devices.



### Auto Refreshing the devices list (Auto Refresh)

The **Auto Refresh** function will automatically refresh the items shown on the web page. Disabling Auto Refresh will only disable the web page refresh, but the ASUS Control Center will still receive updates from the agents of managed devices. Click on the **Auto Refresh** button to enable () or disable () it.

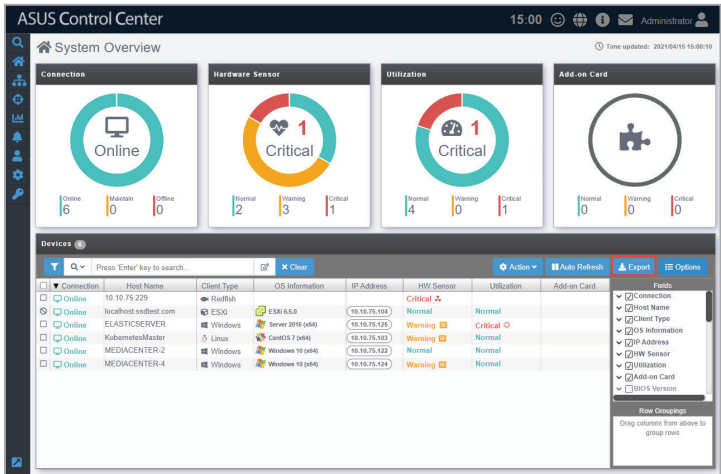




### Exporting devices list (Export)

You can export the managed devices and metadata in the **Devices** list to a CSV or PDF file.

1. Click **Export**, then select an **Export Type** and enter the **File Name** in the popup window.
2. (Optional) To include or exclude a metadata field in the export, click and drag it to the left column to include it or to the right column to exclude it.
3. Click **Export in the popup window** to export the device list based on the selected settings.



Export

Export Type

☒ CSV ☐ PDF

File Name

Fields

BIOS Version

BIOS Release Date

Agent Version

Model Name

WatchDog

Registry Editor

USB Storage Device

Current User

MAC

Connection

Host Name

Client Type

OS Information

IP Address

HW Sensor

Utilization

Add-on Card

☐ Reverse X-Y Axis

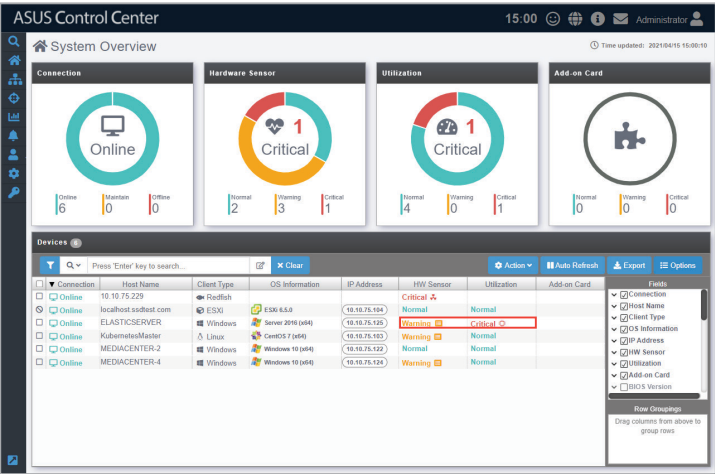
Cancel

Export

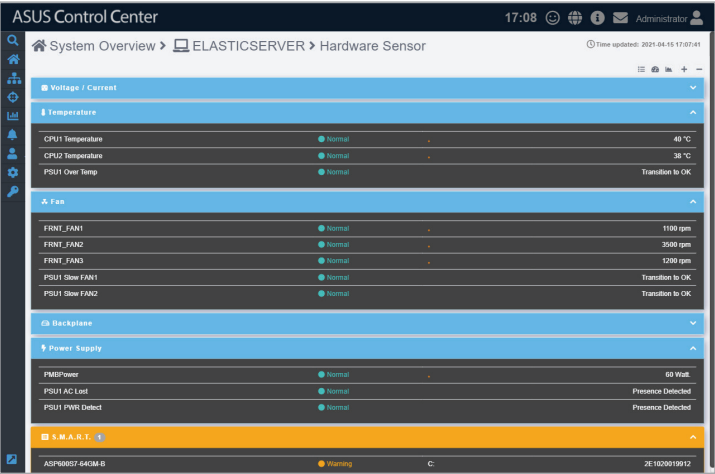
### Using the sensor shortcut

Clicking on a **Warning** or **Critical** status in the **HW Sensor**, **Utilization**, and **Add-on Card** column of a managed device will redirect you to the **Hardware Sensor** and **Utilization** page of a managed device, allowing you to quickly locate your problem.

**NOTE:** The sensor shortcut function will only redirect you to the **Hardware Sensor** or **Utilization** page of the managed device if the status is **Warning** or **Critical**.



Link to managed device's Hardware Sensor:



Link to managed device's Utilization:



### 2.1.3 Search Options

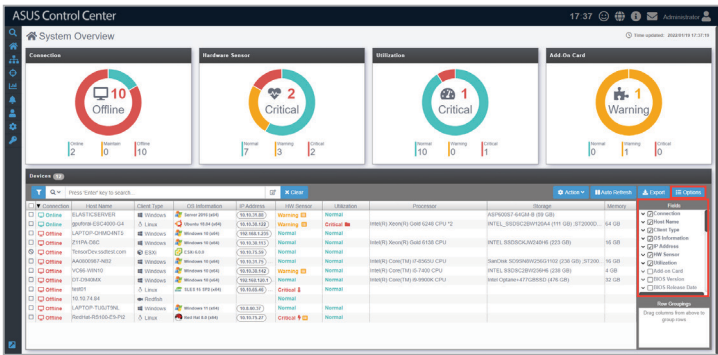
Clicking on **Options** will display the **Fields** and **Row Groupings** functions. The **Fields** function controls which metadata columns are displayed in the **Devices** list. You can check the metadata items you wish to hide or display in the **Fields** list.

**NOTE:** For more information, please refer to the **Metadata Management** section.

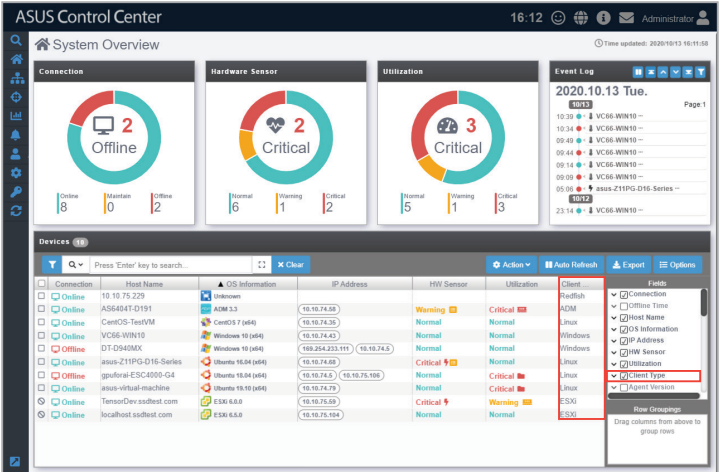
You can sort and group the managed devices in the **Devices** list according to a column criteria using the **Row Groupings** function.

#### Hiding or displaying metadata fields

- Click on **Options** to display the **Fields** window.



2. You can check the metadata field in the **Fields** window to hide or display the metadata field. In the screenshot below, the **Client Type** field is checked.



## Using the Row Groupings function

1. Drag the column items from the **Fields** list into the **Row Groupings** list to filter by those columns.

The screenshot shows the ASUS Control Center interface. At the top, there are three circular gauges for Connection (Offline), Hardware Sensor (Critical), and Utilization (Critical). Below these is a table of devices. The 'Fields' list on the right contains various columns: Connection, Offline Time, Host Name, OS Information, IP Address, HW Sensor, and Utilization. The 'Row Groupings' list is currently empty. A red box highlights the 'Fields' list, and a red 'X' is visible in the 'Row Groupings' list, indicating the action to remove or disband a row.

2. Click on the **X** to remove or disband a row.

The screenshot shows the ASUS Control Center interface. At the top, there are three circular gauges for Connection (Offline), Hardware Sensor (Critical), and Utilization (Critical). Below these is a table of devices. The 'Fields' list on the right contains various columns: Connection, Offline Time, Host Name, OS Information, IP Address, HW Sensor, and Utilization. The 'Row Groupings' list is currently empty. A red box highlights the 'Fields' list, and a red 'X' is visible in the 'Row Groupings' list, indicating the action to remove or disband a row.

Accessing remote desktop

The remote control function provides a flexible interface for device management through the desktop or command-line accessed in ASUS Control Center. You can quickly access the remote desktop of managed devices from the **Devices** list, without having to navigate to **Device Information**.

Device operating systems which support remote control:

|                               |              |            |          |         |      |
|-------------------------------|--------------|------------|----------|---------|------|
| Windows 7                     | Professional | Enterprise | Ultimate |         |      |
| Windows 8                     | Professional | Enterprise |          |         |      |
| Windows 10                    | Professional | Enterprise |          |         |      |
| Windows Server                | 2008         | 2008 R2    | 2012     | 2012 R2 | 2016 |
| Windows Multipoint Server     | 2011         | 2012       |          |         |      |
| Windows Small Business Server | 2008         | 2011       |          |         |      |

- 1. In the **System Overview** screen, select a managed device from the **Devices** list.
- 2. Click on the **IP address** of the selected device, you should be directed to the **Remote Desktop Login** screen.

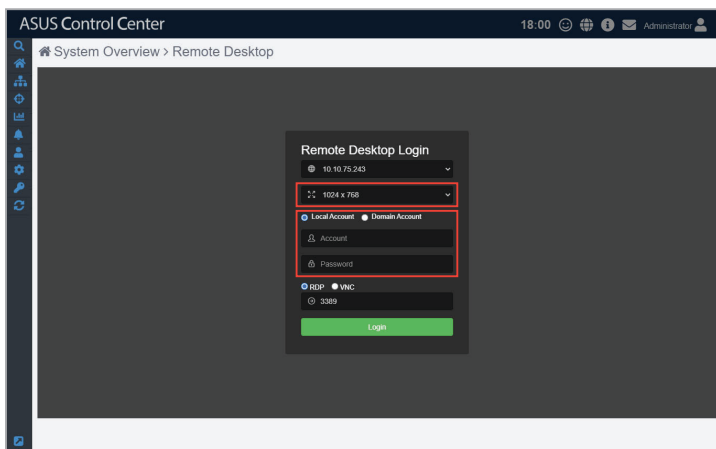


3. Select a resolution to display the managed device in the Remote Desktop window.
4. Select the login Account type, then enter the **Account**, **Password**, and **Domain** information.

---

**NOTE:**

- **Local Account:** The agent's administrator privileges only allow you to manage the device the agent is installed on.
  - **Domain Account:** The agent's administrator privileges allow you to manage all devices in the domain. The **Domain** field only appears if you selected **Domain Account**.
- 





5. Select the protocol to use when connecting, then click **Login**.

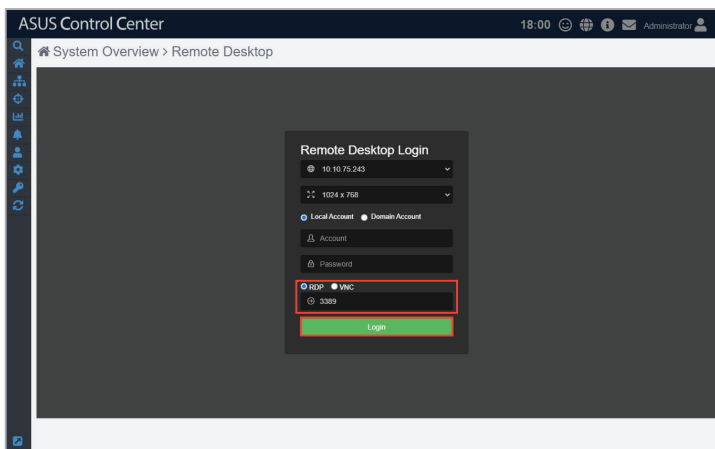
---

**NOTE:**

- Linux and Windows® systems use different protocols, ensure the managed device is reachable through the selected protocol:
    - **RDP**: Available on Windows only; allows only a single user to view and configure at the same time.
    - **VNC**: Available on both Windows and Linux; allows multiple users to view and configure at the same time.
    - **SSH**: Available on Linux only.
- 

**IMPORTANT:**

- Ensure the managed device you wish to remote control has a stable power supply and Internet connection.
  - The managed device may be remote controlled if it is logged out or locked, but cannot be remote controlled if the managed device is powered off or in sleep mode. If the managed device is in sleep mode, please wake the device using the **Power Control (Wake-on-LAN)** function.
  - (for RDP only) Please ensure that the following two items are checked on the remote device and enabled to allow remote connections to the remote device. Search for **Control Panel** in the Windows Search Box, then navigate to **System > Remote settings**.
  - (for RDP only) Please ensure that the **Microsoft Remote Desktop** application is enabled in the **Windows Defender Firewall Allowed Apps** list. Search for **Control Panel** in the Windows Search Box, then navigate to **Windows Defender Firewall > Allowed Apps**.
- 



6. Once the login has been successfully authenticated, you will be logged into the desktop or command line of the device system; this varies between systems.

---

**NOTE:** To switch mouse and keyboard control to the ASUS Control Center, press <Ctrl> + <Alt> on the keyboard. To switch mouse and keyboard control back to the remote device, click in the remote device window.

---

7. Click on the Menu Path at the top of the screen, or click on another menu item from the left menu to end the remote session.

## 2.1.4 Search and Filter Devices

There are various methods of searching and filtering managed devices on the System Overview screen, giving you the freedom of searching or filtering managed devices according to your needs.

**NOTE:** The screenshots in this section are for reference only and may differ according to the different ASUS Control Center functions, but the steps remain the same.

### Filter devices using the Overview Circle

**NOTE:** To clear the filter and view all managed devices, click on **Clear**.

- Click on a colored segment of an overview block to filter according to the selected overview and status:
  - Connection:** Click on a colored segment on the circle to display all items which correspond to the selected connection status.
  - Hardware Sensor:** Click on a colored segment on the circle to display all items which correspond to the selected hardware sensor status.
  - Utilization:** Click on a colored segment on the circle to display all items which correspond to the selected utilization status.
  - Add-on Card:** Click on a colored segment on the circle to display all items which correspond to the selected Add-on Card status.
- The filter criteria and filtered managed devices will be displayed in the **Devices** list. You may select a single managed device from the list to view more details.

ASUS Control Center 16:50 Administrator

System Overview

Time updated: 2020/10/12 16:00:05

**Connection** Offline 2

**Hardware Sensor** Normal

**Utilization** Critical 1

**Event Log** 2020.10.12 Mon.

Filter: Connection

| Connection | Host Name         | OS Information  | IP Address                  | HW Sensor | Utilization |
|------------|-------------------|-----------------|-----------------------------|-----------|-------------|
| Offline    | Dell-D940M5       | Windows 10 (64) | 100.204.22.107 (10.10.74.5) | Normal    | Normal      |
| Online     | general-ESC400-G4 | Windows 10 (64) | 10.10.74.5 (10.10.75.100)   | Normal    | Critical    |

Fields: Connection, Offline Time, Host Name, OS Information, IP Address, HW Sensor, Utilization, Client Type, Agent Version

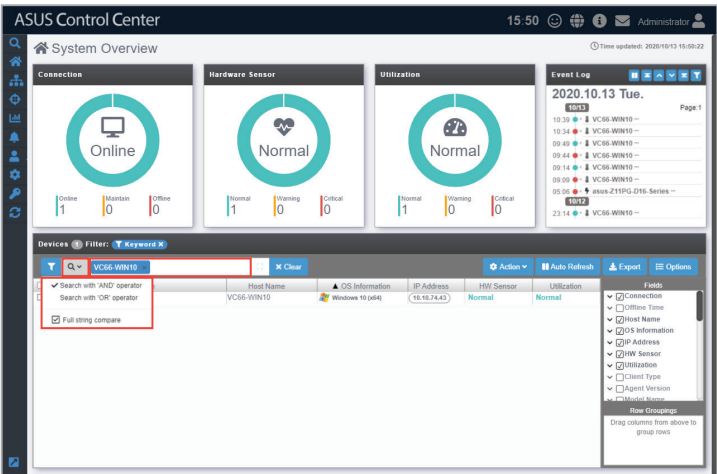
## Filter devices using the Search Bar

**NOTE:** To clear the filter and view all managed devices, click on **Clear**.

1. Enter keywords into the Search bar.
2. Click on , then select the operator you wish to use.

**NOTE:**

- Selecting the **Search with 'AND' operator** option will return search results of items which match all the keywords.
- Selecting the **Search with 'OR' operator** option will return search results of items which at least one of the keywords.
- Checking the **Full string compare** option will only return search results of items which have a string with an exact match to the keywords, and can be applied to any of the above search operators selected.

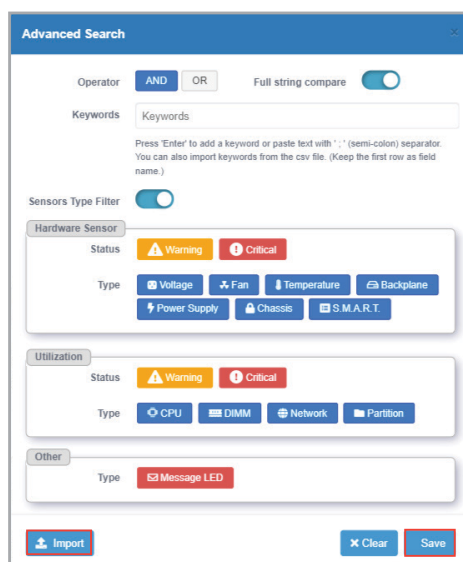


3. (optional) You may also click on  to expand the search bar to view, edit or add additional search criteria. You may also import a .csv file by clicking on **Import**. Click on **Save** once you are finished editing your search criteria.

---

**NOTE:**

- Selecting the '**AND**' option will return search results of items which match all the keywords.
  - Selecting the '**OR**' option will return search results of items which at least one of the keywords.
  - Enabling the **Full string compare** option will only return search results of items which have a string with an exact match to the keywords, and can be applied to any of the above search operators selected.
  - Enabling the **Sensors Type Filter** option will allow you to limit your search results to the **Hardware Sensor**, **Utilization** and **Other** criteria you have checked.
- 



The image shows a screenshot of the 'Advanced Search' dialog box. It has a blue header with the title 'Advanced Search' and a close button. Below the header, there are two sections for search criteria. The first section is for 'Operator' with buttons for 'AND' and 'OR', and a 'Full string compare' toggle switch. The second section is for 'Keywords' with a text input field. Below the keywords section, there is a 'Sensors Type Filter' toggle switch. Underneath, there are three expandable sections: 'Hardware Sensor', 'Utilization', and 'Other'. Each section has a 'Status' row with 'Warning' and 'Critical' buttons, and a 'Type' row with various sensor types. The 'Hardware Sensor' section includes Voltage, Fan, Temperature, Backplane, Power Supply, Chassis, and S.M.A.R.T. The 'Utilization' section includes CPU, DIMM, Network, and Partition. The 'Other' section includes Message LED. At the bottom of the dialog, there are three buttons: 'Import', 'Clear', and 'Save'.

Advanced Search

Operator: **AND** OR Full string compare: ☒

Keywords:

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.  
You can also import keywords from the csv file. (Keep the first row as field name.)

Sensors Type Filter: ☒

**Hardware Sensor**

Status: **Warning** **Critical**

Type: **Voltage** **Fan** **Temperature** **Backplane**  
**Power Supply** **Chassis** **S.M.A.R.T.**

**Utilization**

Status: **Warning** **Critical**

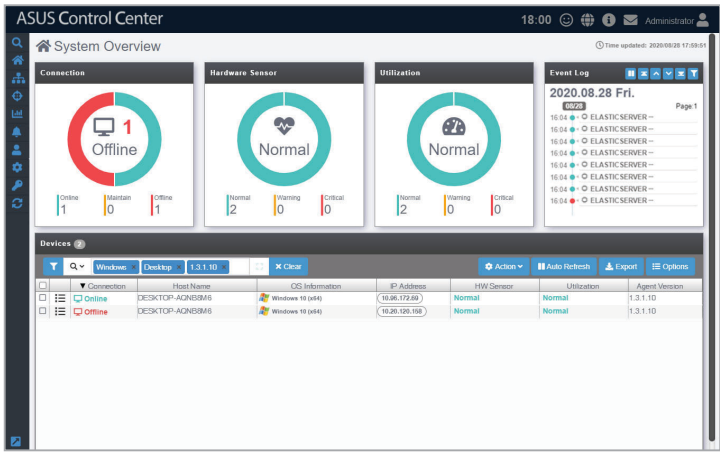
Type: **CPU** **DIMM** **Network** **Partition**

**Other**

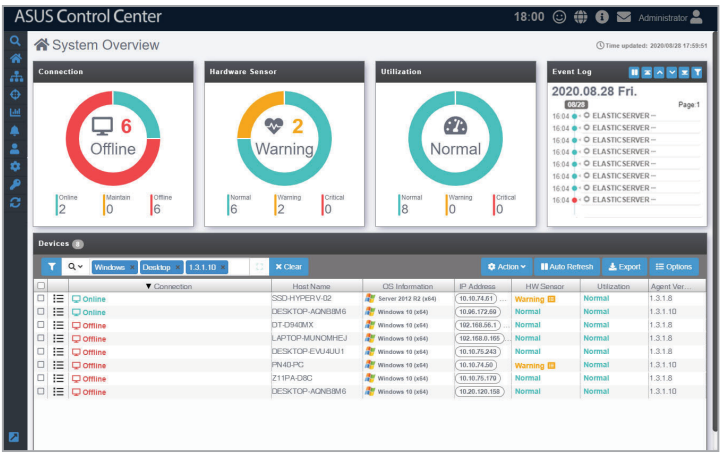
Type: **Message LED**

**Import** **Clear** **Save**

4. The search results will be displayed in the **Devices** list.
- Result of selecting the **Search with 'AND' operator** option.



- Result of selecting the **Search with 'OR' operator** option.



## Filter devices using Column Headers

**NOTE:** To clear the filter and view all managed devices, click on **Clear**.

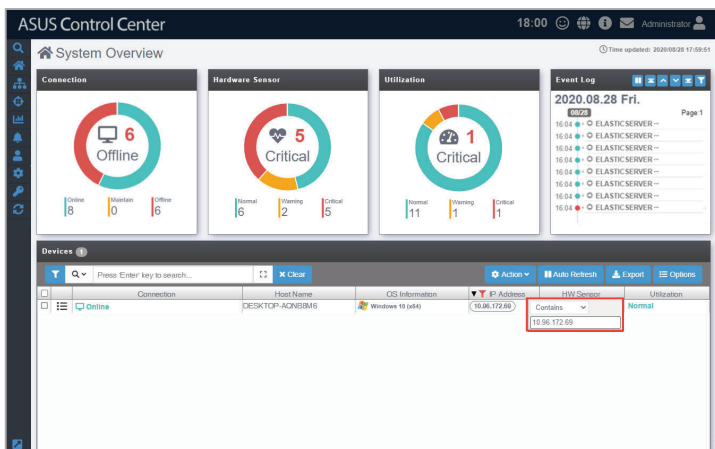
1. Hover over a column header in the **Devices** list then click on .

**NOTE:** Some column headers may not support the filter function.

2. Select a filter rule (**Contains**, **Equals**, **Starts with**, **Ends with**) and enter the keyword to search.

**NOTE:**

- To add more metadata columns to the **Devices** list, click on **Options**, then check the metadata item you wish to display.
- Click on the Name of a column header to sort the filter results alphabetically.



The screenshot displays the ASUS Control Center interface. At the top, there's a 'System Overview' section with three circular gauges: 'Connection' (6 Offline, 8 Online), 'Hardware Sensor' (5 Critical, 6 Normal, 2 Warning), and 'Utilization' (1 Critical, 11 Normal, 1 Warning). To the right is an 'Event Log' for 2020.08.28 Fri. Below this is the 'Devices' table, which is filtered by the IP address '10.96.172.69'. The table has columns for Connection, Host Name, OS Information, IP Address, and Utilization. The filtered device is 'DESKTOP-ACN3BMS' running Windows 10 (x64) with a 'Normal' utilization status. A red box highlights the filter dropdown menu showing 'Contains' and the value '10.96.172.69'.

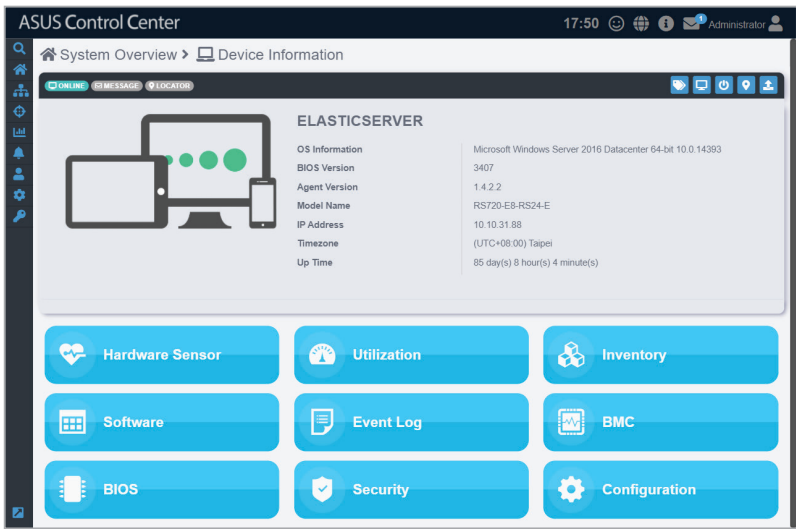
| Connection | Host Name       | OS Information   | IP Address   | Utilization |
|------------|-----------------|------------------|--------------|-------------|
| Online     | DESKTOP-ACN3BMS | Windows 10 (x64) | 10.96.172.69 | Normal      |

## 2.2 Device Information

**NOTE:** The screenshot may vary between agent and agentless devices, for more details on viewing agentless device details, refer to the **Host Information** section.

The **Device Information** screen gives you various functions to view the status and manage the selected device.

To access the **Device Information** of a managed device, click on the  icon located next to the managed device you wish to view in the **Devices list**.



The **Device Information** screen will display the **OS Information**, **BIOS Version**, **Agent Version**, **Model Name**, **IP Address**, **Timezone**, and **Up Time** of the device.

### Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.



## Device Statuses and Quick Buttons



### Connection status

This item displays the connection status of the selected managed device.



### Message status\*

This item will turn red if the selected device's BMC returns a hardware sensor warning/critical event.



### Locator status\*

This item will turn green if the locator LED is enabled through the ACC Web UI. The locator LED allows you quickly locate the physical location of the device in a server rack.



### Metadata Editor

This item allows you to edit the metadata of the managed device by double clicking in the **Value** field.



### Remote Desktop

This item allows you to remotely control a managed device. Refer to **Accessing remote desktop** under the **Devices list** section for more details.



### Power Control

This item allows you to power off or restart a managed device.



### Locator LED

This item allows you to turn on/off the Locator LED.



### Refetch

This item will refetch the device data.

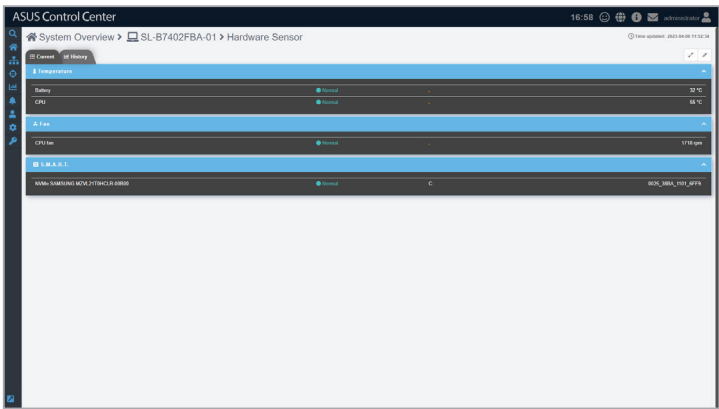
\* Only available on BMC enabled devices

## 2.2.1      Hardware Sensor

This item allows you to view the details and values for the Voltage, Temperature, Fan, Backplane, Power Supply, Chassis, and S.M.A.R.T items in real time.

**NOTE:**

- The Hardware Sensor values on Linux devices are returned only if the Linux device has BMC, otherwise only the S.M.A.R.T. details can be viewed.
- If the device is using Windows 11 or Server 2022 and the sensor readings keep failing, please navigate to **Start > Settings > Update & Security > Windows Security > Device Security**, then select **Core Isolation details** and set **Memory integrity** to **Off** on the device.



**Quick Buttons**

-  Click to switch to the Current tab.
-  Click to switch to the History tab.
-  Click to expand all blocks.
-  Click to minimize all blocks.
-  Click to expand this block.
-  Click to minimize this block.

Clicking on an item in the voltage, temperature, fans, Backplane, Power Supply, Chassis, and S.M.A.R.T groups will display the High and Low critical and warning values. Please refer to the table below for more details on the items shown in the example below of CPU Temperature Threshold, and the Normal status which is not shown in the threshold pop-up window.

| CPU1 Temperature Threshold |     |
|----------------------------|-----|
| High Critical              | 75  |
| High Warning               | 70  |
| Low Warning                | 0   |
| Low Critical               | -10 |

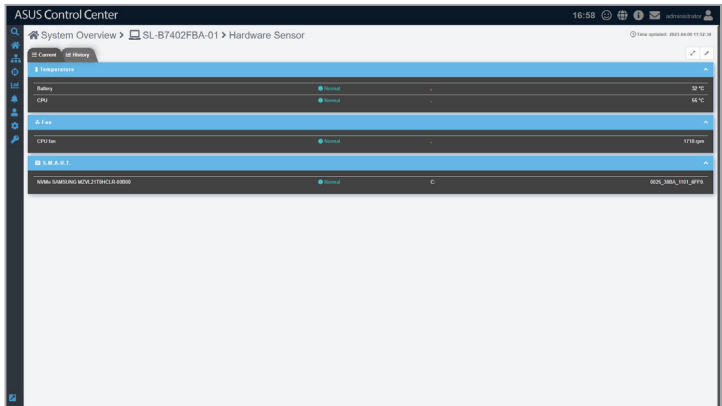
|               |                                                                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Critical | If the sensor value is equal to or exceeds this value the sensor status will be <b>Critical</b> . For the above example, if the sensor value is 75 or higher, the sensor status will be <b>Critical</b> .                                             |
| High Warning  | If the sensor value is equal to or exceeds this value, and below the <b>High Critical</b> value the sensor status will be <b>Warning</b> . For the above example, if the sensor value is between 70 ~ 74, the sensor status will be <b>Warning</b> .  |
| Normal        | The sensor will <b>Normal</b> if the sensor value is between the <b>Low Warning</b> and <b>High Warning</b> values. For this example, if the sensor value is between 1 ~ 69, the sensor status will be <b>Normal</b> .                                |
| Low Warning   | If the sensor value is equal to or lower than this value, and above the <b>Low Critical</b> value the sensor status will be <b>Warning</b> . For the above example, if the sensor value is between -9 ~ 0, the sensor status will be <b>Warning</b> . |
| Low Critical  | If the sensor value is equal to or lower than this value the sensor status will be <b>Critical</b> . For the above example, if the sensor value is -10 or lower, the sensor status will be <b>Critical</b> .                                          |

## Toggling between tabs

You can switch between different **Hardware Sensor** tabs by clicking the tabs in the top bar.

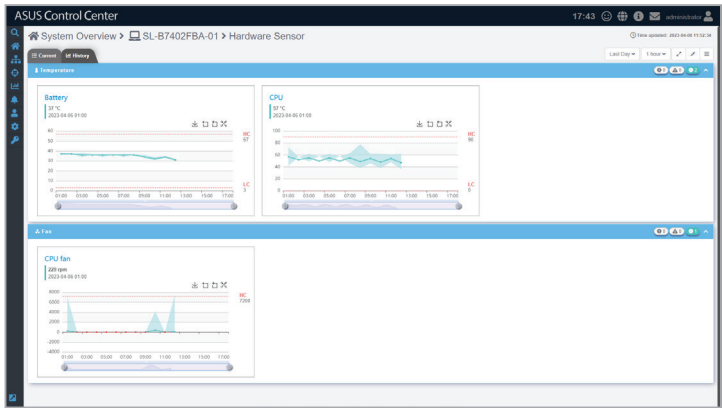
- 

Current tab (default)



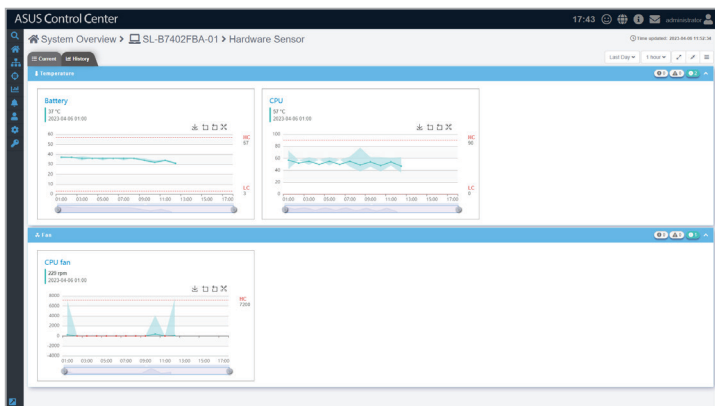
- 

History tab



## Customizing the Hardware Sensor history tab

You can customize the history tab which displays historical data for the Voltage / Current, Temperature, Fan, Backplane, and Power Supply sensor events according to different periods of time.



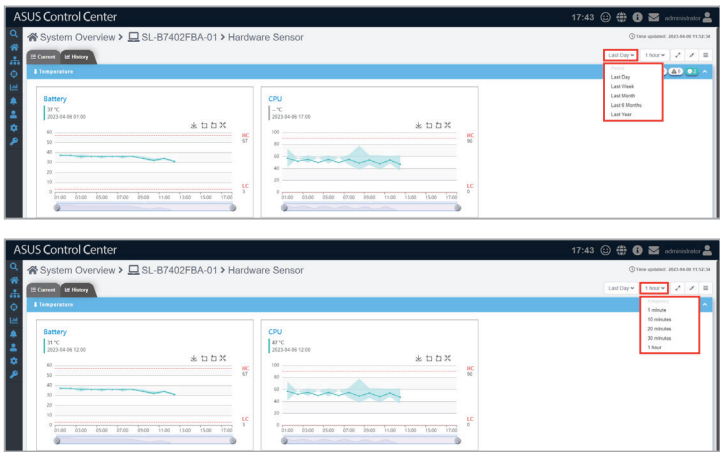
### Quick Buttons

-  Click to expand all blocks.
-  Click to minimize all blocks.
-  Click to expand this block.
-  Click to minimize this block.

### Chart Quick Buttons

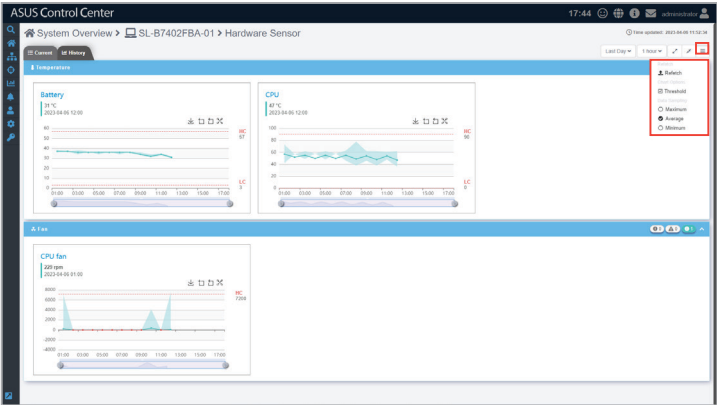
-  Click to download an image of the chart as a .png file.
-  Click to zoom in on the timeline of the chart.
-  Click to zoom out on the timeline of the chart.
-  Click to restore the chart to its default view.

You can customize the charts by selecting the period of time you wish to view for the charts, then selecting the frequency for which the sensors should return data. This will be applied to the charts for all the sensors shown on this page.



| Period of time | Frequency                                                              |
|----------------|------------------------------------------------------------------------|
| Last day       | 1 minute, 10 minutes, 20 minutes, 30 minutes, 1 hour                   |
| Last week      | 10 minutes, 20 minutes, 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours |
| Last month     | 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours, 1 day                  |
| Last 6 months  | 3 hours, 6 hours, 12 hours, 1 day, 7 days, 14 days                     |
| Last year      | 6 hours, 12 hours, 1 day, 7 days, 14 days, 30 days                     |

Additionally, by clicking on the  icon, you can customize the data you wish to view on the chart.



|               |                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Refetch       | Allows you to trigger a refetch of device data.                                                                                            |
| Chart Options | Allows you to select whether the <b>Threshold</b> should be displayed on the chart.                                                        |
| Data Sampling | Allows you to select whether the <b>Maximum</b> values, <b>Average</b> values, or <b>Minimum</b> values should be displayed on the charts. |

### 2.2.2 Utilization

This item allows you to view real time data and set the utilization threshold value for the CPU, DIMM, Partition, and Network.

**NOTE:** The Disk Partition block naming may differ between Windows® and Linux systems. The Disk Partition block is titled **Partition** for Windows® systems, and **File System** for Linux systems.



## Quick Buttons



Click to switch to the Current tab.



Click to switch to the History tab.



Click to expand all blocks.



Click to minimize all blocks.



Click to expand this block.



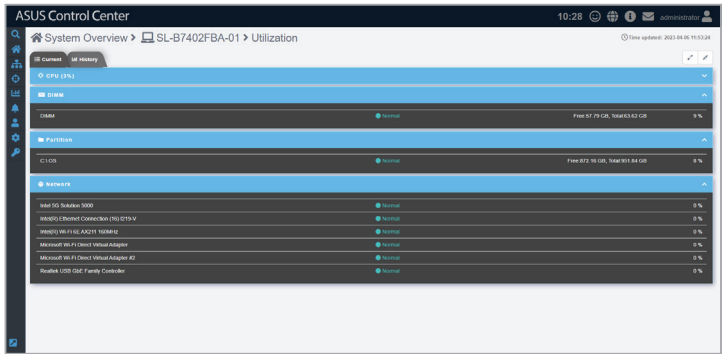
Click to minimize this block.



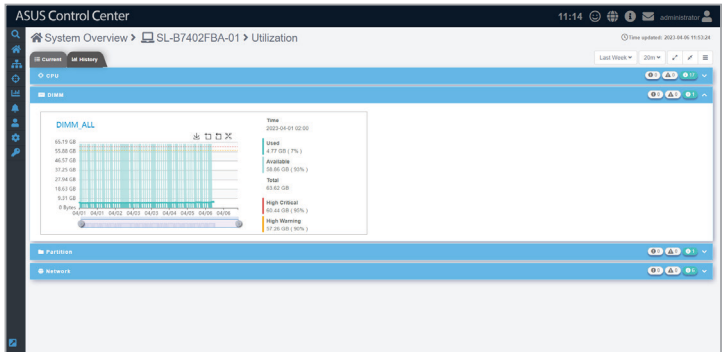
## Toggling between tabs

You can switch between different **Utilization** tabs by clicking the tabs in the top bar.

- Current tab (default)



- History tab



## Editing the threshold values

You can edit the critical and warning threshold values for **Utilization** items.

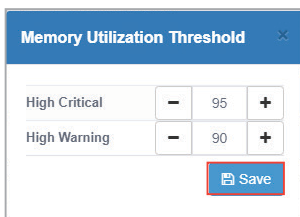
1. Click on a item to adjust the threshold values:
  - High Critical: When the value exceeds this threshold value, the sensor will display **Critical**.
  - High Warning: When the value exceeds this threshold value, the sensor will display **Warning**.

---

**NOTE:** The threshold options for each item may vary.

---

2. Click on **Save** once you have finished adjusting the threshold values of the item.



The image shows a dialog box titled "Memory Utilization Threshold" with a close button (X) in the top right corner. Inside the dialog, there is a table with two rows: "High Critical" and "High Warning". Each row has a minus sign button, a text input field containing the value (95 for High Critical and 90 for High Warning), and a plus sign button. At the bottom right of the dialog, there is a blue button with a floppy disk icon and the text "Save".

| Threshold Type | Adjustment | Value | Adjustment |
|----------------|------------|-------|------------|
| High Critical  | -          | 95    | +          |
| High Warning   | -          | 90    | +          |

Save

## Customizing the Utilization history tab

You can customize the history tab which displays historical data for the CPU, DIMM, Partition, and Network sensor events according to different periods of time.



## Quick Buttons



Click to expand all blocks.



Click to minimize all blocks.



Click to expand this block.



Click to minimize this block.

## Chart Quick Buttons



Click to download an image of the chart as a .png file.



Click to zoom in on the timeline of the chart.



Click to zoom out on the timeline of the chart.



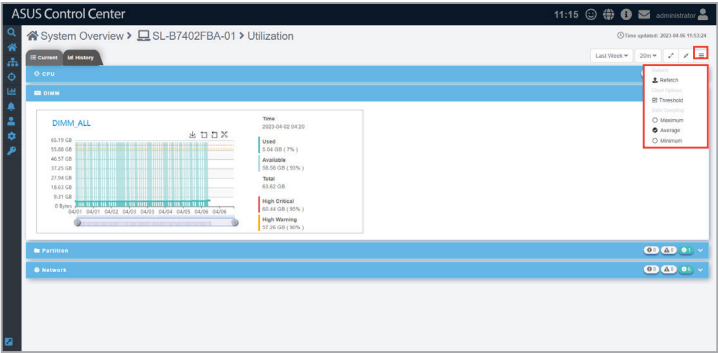
Click to restore the chart to its default view.

You can customize the charts by selecting the period of time you wish to view for the charts, then selecting the frequency for which the sensors should return data. This will be applied to the charts for all the sensors shown on this page.



| Period of time | Frequency                                                              |
|----------------|------------------------------------------------------------------------|
| Last day       | 1 minute, 10 minutes, 20 minutes, 30 minutes, 1 hour                   |
| Last week      | 10 minutes, 20 minutes, 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours |
| Last month     | 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours, 1 day                  |
| Last 6 months  | 3 hours, 6 hours, 12 hours, 1 day, 7 days, 14 days                     |
| Last year      | 6 hours, 12 hours, 1 day, 7 days, 14 days, 30 days                     |

Additionally, by clicking on the  icon, you can customize the data you wish to view on the chart.



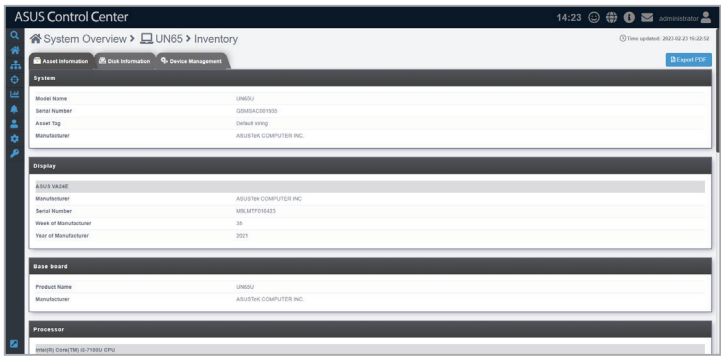
|               |                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Refetch       | Allows you to trigger a refetch of device data.                                                                                            |
| Chart Options | Allows you to select whether the <b>Threshold</b> should be displayed on the chart.                                                        |
| Data Sampling | Allows you to select whether the <b>Maximum</b> values, <b>Average</b> values, or <b>Minimum</b> values should be displayed on the charts. |

### 2.2.3 Inventory

This item displays more details about your managed device and disk.

#### Asset Information

View details for the **System**, **Display**, **Base Board**, **Memory**, **BIOS**, **Processor**, **Network Adapter**, **Storage**, and **RAID** of the managed device.

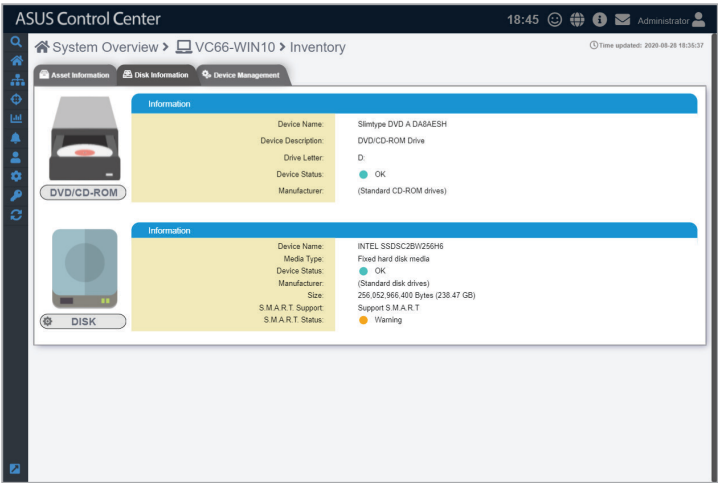


You can click on **Export PDF** to export the Asset Information to a PDF file.

| Asset Information - UN65        |                                |
|---------------------------------|--------------------------------|
| System                          |                                |
| Model Name                      | UN65U                          |
| Serial Number                   | GBMSAC001935                   |
| Asset Tag                       | Default string                 |
| Manufacturer                    | ASUSTek COMPUTER INC.          |
| Display                         |                                |
| ASUS VA24E                      |                                |
| Manufacturer                    | ASUSTek COMPUTER INC           |
| Serial Number                   | M9LMTF016423                   |
| Week of Manufacturer            | 35                             |
| Year of Manufacturer            | 2021                           |
| Base board                      |                                |
| Product Name                    | UN65U                          |
| Manufacturer                    | ASUSTek COMPUTER INC.          |
| Processor                       |                                |
| Intel(R) Core(TM) i3-7100U CPU  |                                |
| Name                            | Intel(R) Core(TM) i3-7100U CPU |
| Clock                           | 2.40GHz                        |
| Memory                          |                                |
| Total Memory Size               | 4.00 GB                        |
| Device LocatorChannelA-DIMM1    |                                |
| Manufacturer                    | SK Hynix                       |
| Part Number                     |                                |
| Serial Number                   | 27F7B91E                       |
| Capacity                        | 4.00 GB                        |
| Bank Label                      | BANK 0                         |
| ASUS Control Center Page 1 of 2 |                                |

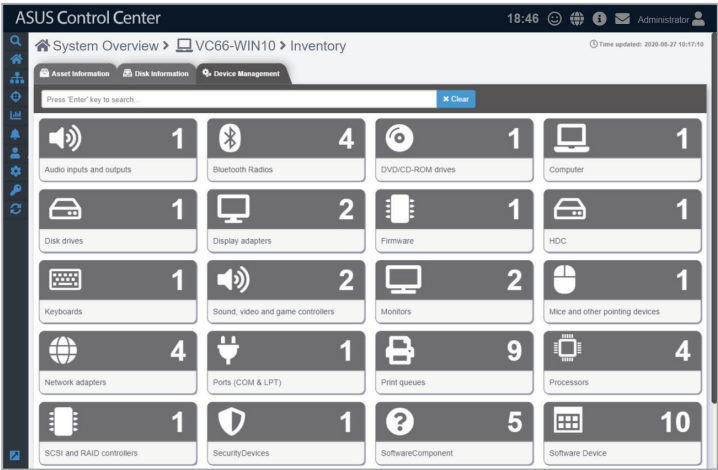
Disk Information

View details on disks installed on the managed device, such as ODD drives, hard disk drives, and USB drives.



Device Management

View the Device Management properties of the managed device.







This tab shows all the applications installed on the managed device. On Windows® devices, this is equivalent to the Programs and Feature list in most cases.

[illegible]

**ASUS Control Center**

**System Overview** > **KubernetesMaster** > Software

Time updated: 2020/10/12 18:00:39

Application Processes Software Market

Press Enter key to search.

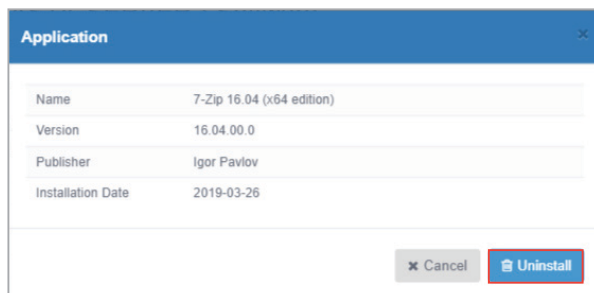
| Name                          | Version  | Publisher | Installation Date |
|-------------------------------|----------|-----------|-------------------|
| libvebp                       | 0.3.0    | CenOS     | 2018-01-02        |
| uniprj                        | 0.13     | CenOS     | 2017-07-31        |
| gpg-pubkey                    | 3626c4e5 | (none)    | 2017-07-31        |
| webkitgtk-plugin-process-gtk2 | 2.14.7   | CenOS     | 2018-01-02        |
| atomic registries             | 1.20.1   | CenOS     | 2018-01-02        |
| alsa-lib                      | 1.1.3    | CenOS     | 2018-01-02        |
| passwd                        | 0.79     | CenOS     | 2017-07-31        |
| genio6                        | 1.0.1    | CenOS     | 2018-01-02        |
| PackageKit-gstreamer-plugin   | 1.1.5    | CenOS     | 2018-01-02        |
| libtool-ltdl                  | 2.4.2    | CenOS     | 2018-01-02        |
| iscnssm                       | 1.0.10   | CenOS     | 2017-07-31        |
| libreport-gtk                 | 2.1.11   | CenOS     | 2018-01-02        |
| python-decorator              | 3.4.0    | CenOS     | 2017-07-31        |
| wcutils                       | 20139529 | CenOS     | 2018-01-02        |
| pom2                          | 10.23    | CenOS     | 2018-01-02        |
| xorg-x11-fonts-Type1          | 7.5      | CenOS     | 2017-07-31        |
| automake                      | 1.13.4   | CenOS     | 2017-08-01        |
| webkitgtk3                    | 2.4.11   | CenOS     | 2018-01-02        |
| hw205-firmware                | 22.07.0  | CenOS     | 2018-01-02        |
| cryptsetup-luks               | 1.7.4    | CenOS     | 2018-01-02        |
| lxcp-tools                    | 1.0.17   | CenOS     | 2017-07-31        |
| libvirt-server-dnval          | 0.9.9    | CenOS     | 2017-08-01        |
| gnome-shell-extension-common  | 3.22.2   | CenOS     | 2018-01-02        |
| system-config-printer-udev    | 1.4.1    | CenOS     | 2017-07-31        |
| cracklib                      | 2.9.0    | CenOS     | 2018-01-02        |
| iBSM                          | 1.2.2    | CenOS     | 2017-07-31        |

You may also click on an application then select **Uninstall** to uninstall the application.

---

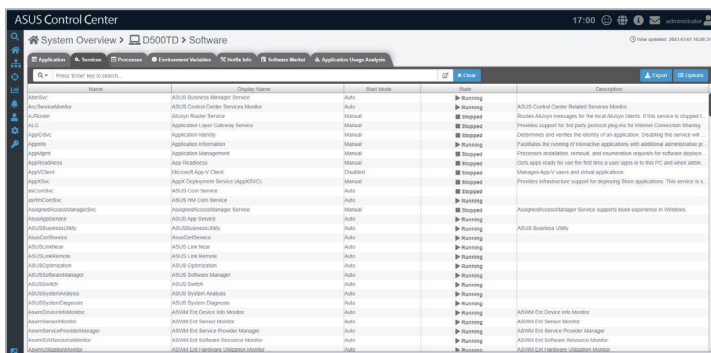
**NOTE:**

- Uninstalling applications using the **Application** tab is disabled on Linux systems.
  - The **Uninstall** button will be grayed out if the uninstall option is unavailable for the selected application.
- 

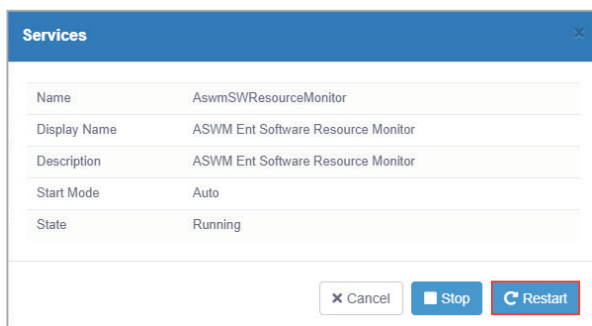


### Services (Windows only)

This tab shows all the services available on the managed device. On Windows® devices, this is equivalent to the Task Manager's services list in most cases.



You may click on a service then choose to start the service by clicking on **Start**, stop a running process by clicking on **Stop**, or restart the service by clicking on **Restart**.



## Processes

This tab shows all the processes on the managed device. On Windows® devices, this is equivalent to the Task Manager's processes list in most cases.

**For Windows® system:**

[illegible]

**For Linux system:**

ASUS Control Center

18:00

🌙

🌐

📧

👤 Administrator

🕒 Time updated: 2020/10/12 18:00:39

🏠 System Overview

➤ KubernetesMaster > Software

📄 Application

📄 Processes

📄 Software Market

Press 'Enter' key to search...

🔍 Clear

📄 Export

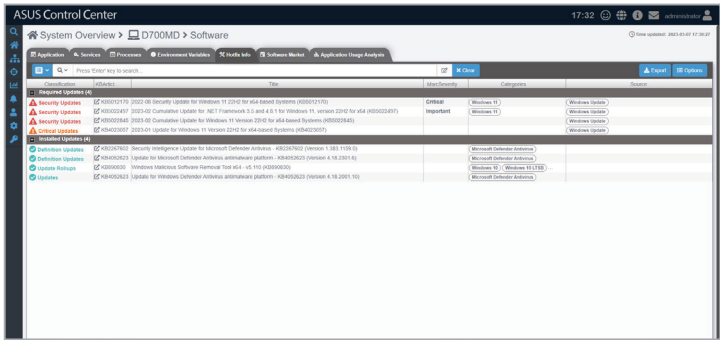
☰ Options

| PID | Name                     | Executable Path |
|-----|--------------------------|-----------------|
| 1   | /usr/lib/systemd/systemd |                 |
| 2   | [kthreadd]               |                 |
| 3   | [ksoftirqd]              |                 |
| 4   | [kworker/0-0H]           |                 |
| 8   | [migration/0]            |                 |
| 9   | [rcu_bh]                 |                 |
| 10  | [rcu_sched]              |                 |
| 11  | [watchdog/0]             |                 |
| 12  | [watchdog/1]             |                 |
| 13  | [migration/1]            |                 |
| 14  | [ksoftirqd/1]            |                 |
| 16  | [kworker/1-0H]           |                 |
| 17  | [watchdog/2]             |                 |
| 18  | [migration/2]            |                 |
| 19  | [ksoftirqd/2]            |                 |
| 21  | [kworker/2-0H]           |                 |
| 22  | [watchdog/3]             |                 |
| 23  | [migration/3]            |                 |
| 24  | [ksoftirqd/3]            |                 |
| 26  | [kworker/3-0H]           |                 |
| 27  | [watchdog/4]             |                 |
| 28  | [migration/4]            |                 |
| 29  | [ksoftirqd/4]            |                 |
| 31  | [kworker/4-0H]           |                 |
| 32  | [watchdog/5]             |                 |
| 33  | [migration/5]            |                 |

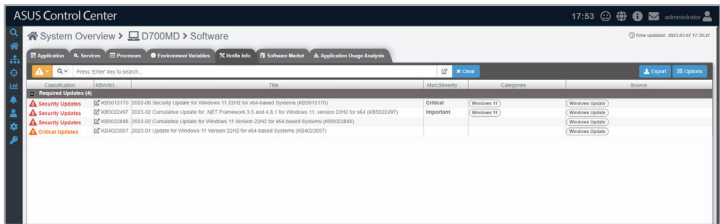
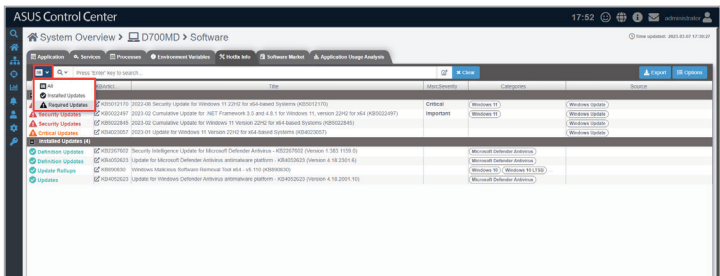


## Hotfix Info (Windows only)

This tab shows installed and still pending hotfix updates of a managed device, and also allows you to sort the hotfix by **MsrcSecurity**, **Categories**, or **Source**.



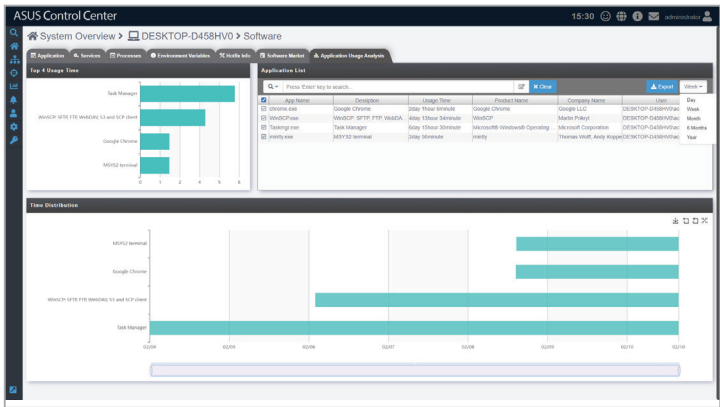
You can also filter the Hotfix by clicking on , then selecting **All**, **Installed Updates**, and **Required Updates** as your filter option, then view more information about the hotfix by clicking on an item in the hotfix list.



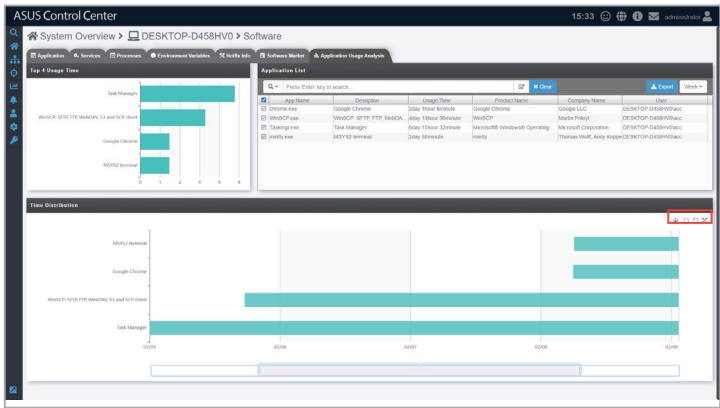


## Application Usage Analysis

This tab shows usage information for the top ten most used applications on the managed device. You can filter the Application List by date to only show usage information for the past day, week, month, half year, or year. Select an application in the Application List to view usage information for that specific application.



Click  to save a screenshot of the time distribution graph. Click  and drag select a portion of the graph to zoom in. To zoom out, click  to return to the previous zoom level or  to return to the default zoom level.





## 2.2.5 Event Log

This item displays the event logs for the **ASUS Control Center**, **Application**, **System**, **Security**, and **Power**. You may view each event log by clicking on the tabs and switch between **Logs** view or **Log Analysis** view within each tab. Click on an event to view more details about the event.

### NOTE:

- To export the Event Log click the **Export** button, enter a filename, then click **OK**.
- Linux systems only support the **ASUS Control Center** tab.

### For Windows® system:

ASUS Control Center 11:20 Administrator

System Overview > VC66-WIN10 > Event Log

The latest 5000 records

Normal 178 Warning 15 Critical 114

Logs (178)

Press 'Enter' key to search. [Clear] [Export] [Log Analysis]

| Level Type | Date & Time         | Message                                                                    |
|------------|---------------------|----------------------------------------------------------------------------|
| Normal     | 2020-08-08 14:25:50 | CPU Core ID: 1 Utilization: 49 % Status: Warning -> Normal                 |
| Warning    | 2020-08-08 14:22:50 | CPU Core ID: 1 Utilization: 90 % Status: Normal -> Warning                 |
| Critical   | 2020-08-08 13:37:40 | Sensor: MotherBoard Value: 43 -> 63 Status Changed: Normal -> HighCritical |
| Normal     | 2020-08-08 10:01:57 | Sensor: MotherBoard Value: 63 -> 43 Status Changed: HighCritical -> Normal |
| Normal     | 2020-08-08 07:59:15 | Sensor: MotherBoard Value: 62 -> 43 Status Changed: HighCritical -> Normal |
| Normal     | 2020-08-08 07:47:09 | Sensor: MotherBoard Value: 62 -> 43 Status Changed: HighCritical -> Normal |
| Critical   | 2020-08-08 07:36:03 | Sensor: MotherBoard Value: 43 -> 64 Status Changed: Normal -> HighCritical |
| Normal     | 2020-08-08 04:10:31 | Sensor: MotherBoard Value: 63 -> 43 Status Changed: HighCritical -> Normal |
| Critical   | 2020-08-08 03:36:08 | Sensor: MotherBoard Value: 43 -> 62 Status Changed: Normal -> HighCritical |
| Normal     | 2020-08-08 00:43:21 | Sensor: MotherBoard Value: 60 -> 43 Status Changed: HighCritical -> Normal |
| Normal     | 2020-08-07 17:46:47 | Sensor: MotherBoard Value: 60 -> 43 Status Changed: HighCritical -> Normal |
| Normal     | 2020-08-07 16:44:11 | Sensor: MotherBoard Value: 63 -> 43 Status Changed: HighCritical -> Normal |
| Critical   | 2020-08-07 16:43:11 | Sensor: MotherBoard Value: 43 -> 63 Status Changed: Normal -> HighCritical |
| Normal     | 2020-08-07 16:38:10 | Sensor: MotherBoard Value: 63 -> 43 Status Changed: HighCritical -> Normal |
| Critical   | 2020-08-07 16:37:10 | Sensor: MotherBoard Value: 43 -> 63 Status Changed: Normal -> HighCritical |
| Normal     | 2020-08-07 09:57:56 | Sensor: MotherBoard Value: 62 -> 44 Status Changed: HighCritical -> Normal |
| Normal     | 2020-08-07 09:24:33 | Sensor: MotherBoard Value: 63 -> 44 Status Changed: HighCritical -> Normal |
| Critical   | 2020-08-07 07:36:07 | Sensor: MotherBoard Value: 54 -> 62 Status Changed: Normal -> HighCritical |

### For Linux system:

ASUS Control Center 18:00 Administrator

System Overview > KubernetesMaster > Event Log

The latest 5000 records

Normal 25 Warning 36 Critical 17

Logs (17)

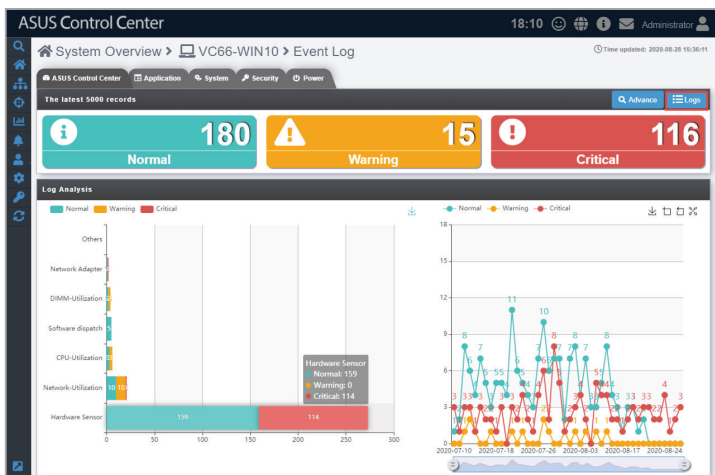
Press 'Enter' key to search. [Clear] [Export] [Log Analysis]

| Level Type | Date & Time         | Message                                                      |
|------------|---------------------|--------------------------------------------------------------|
| Normal     | 2019-10-24 04:46:26 | CPU Core ID: 0 Utilization: 83 % Status: Warning -> Normal   |
| Warning    | 2019-10-24 04:45:55 | CPU Core ID: 0 Utilization: 90 % Status: Normal -> Warning   |
| Normal     | 2019-10-24 04:39:08 | CPU Core ID: 0 Utilization: 90 % Status: Warning -> Normal   |
| Warning    | 2019-10-24 04:38:36 | CPU Core ID: 0 Utilization: 91 % Status: Normal -> Warning   |
| Normal     | 2019-10-24 04:35:28 | CPU Core ID: 0 Utilization: 88 % Status: Warning -> Normal   |
| Normal     | 2019-10-24 04:34:57 | CPU Core ID: 1 Utilization: 89 % Status: Warning -> Normal   |
| Warning    | 2019-10-24 04:34:26 | CPU Core ID: 1 Utilization: 91 % Status: Normal -> Warning   |
| Warning    | 2019-10-24 04:33:54 | CPU Core ID: 0 Utilization: 91 % Status: Normal -> Warning   |
| Normal     | 2019-10-24 04:32:52 | CPU Core ID: 0 Utilization: 88 % Status: Warning -> Normal   |
| Normal     | 2019-10-24 04:32:52 | CPU Core ID: 0 Utilization: 90 % Status: Warning -> Normal   |
| Warning    | 2019-10-24 04:32:20 | CPU Core ID: 0 Utilization: 94 % Status: Critical -> Warning |
| Critical   | 2019-10-24 04:31:49 | CPU Core ID: 0 Utilization: 95 % Status: Warning -> Critical |
| Warning    | 2019-10-24 04:31:17 | CPU Core ID: 1 Utilization: 90 % Status: Normal -> Warning   |
| Warning    | 2019-10-24 04:31:17 | CPU Core ID: 0 Utilization: 91 % Status: Normal -> Warning   |

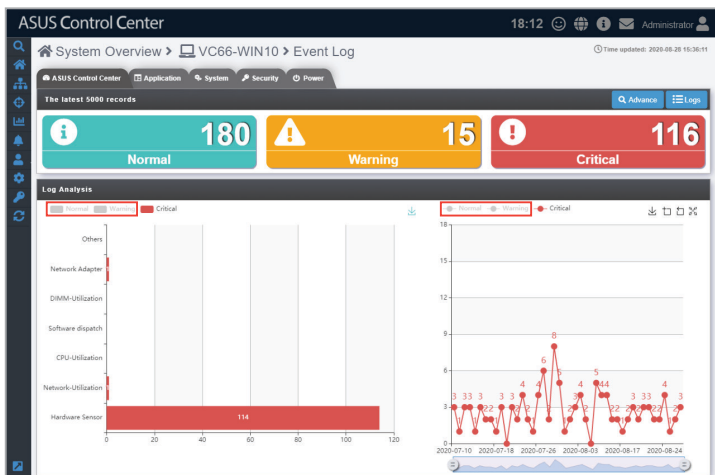
## Switching to Log Analysis view

Click on **Log Analysis** to view the event log as a bar chart and timeline chart, allowing you to view the amount of **Normal**, **Warning**, and **Critical** events.

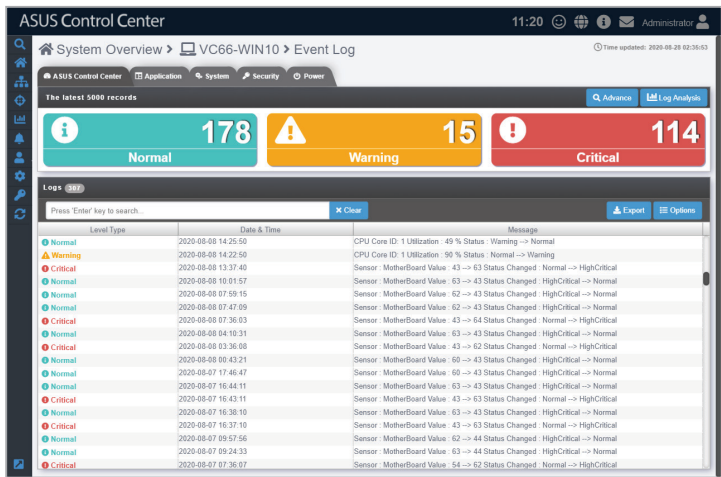
**NOTE:** Click on **Logs** to switch back to the list view of the event log.



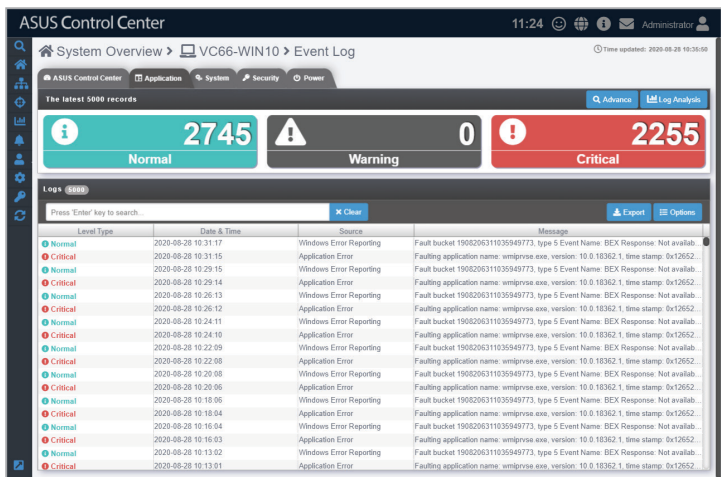
You can click on a item on either chart key to hide that item on both charts.



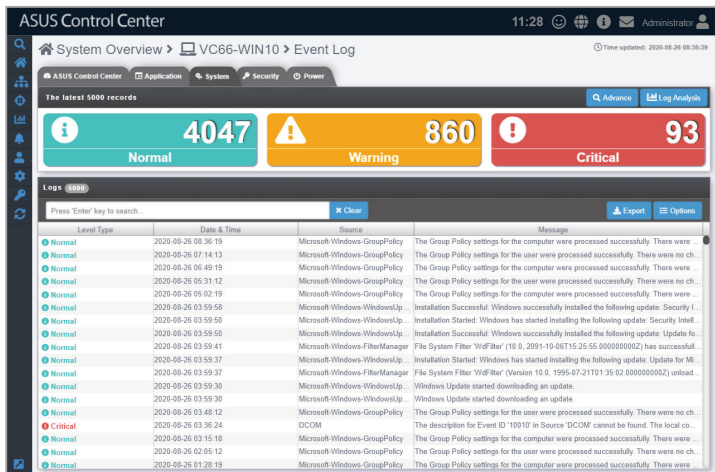
## ASUS Control Center tab



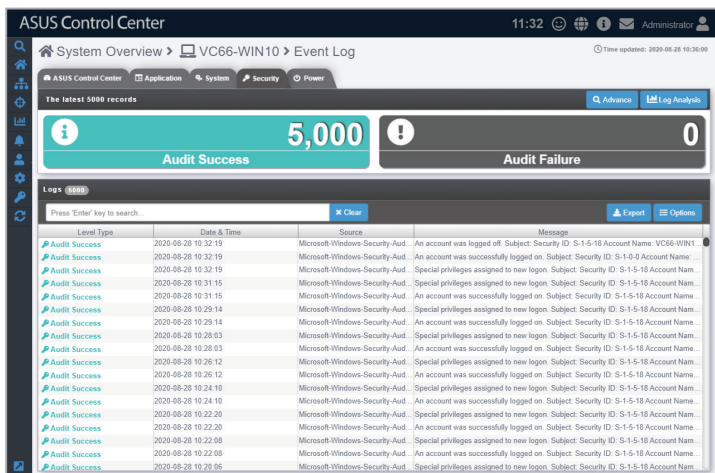
## Application tab (Windows only)



### System tab (Windows only)

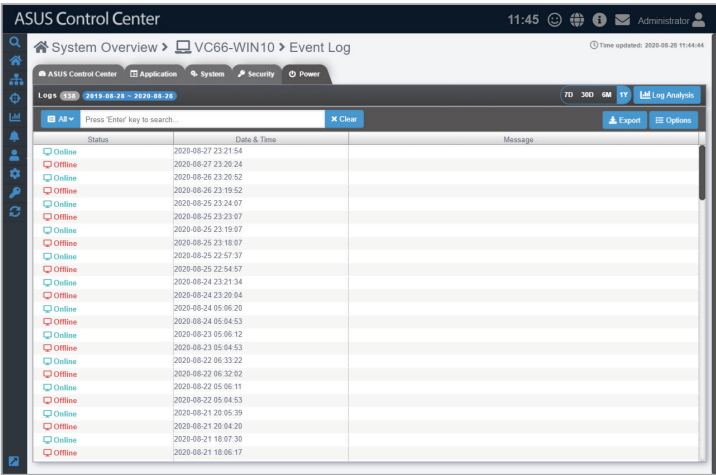


### **Security tab (Windows only)**

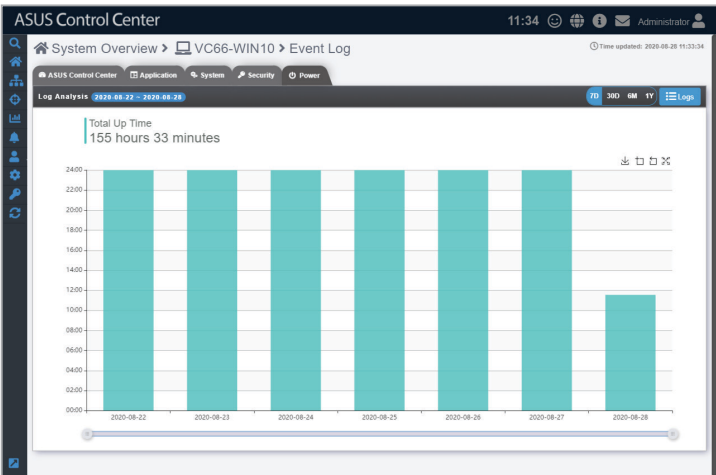


**Power tab (Windows only)**

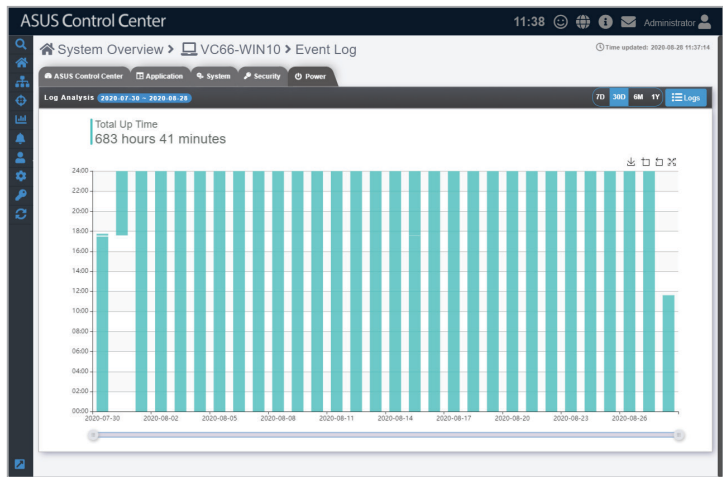
This tab will display the power on, power off, and restart event logs for the managed device. You can select to view the power event log events of different periods of time.



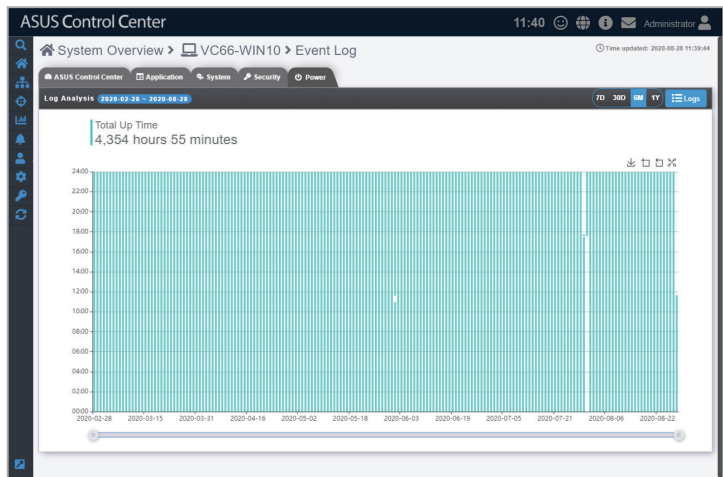
**7 Days (Log Analysis):**



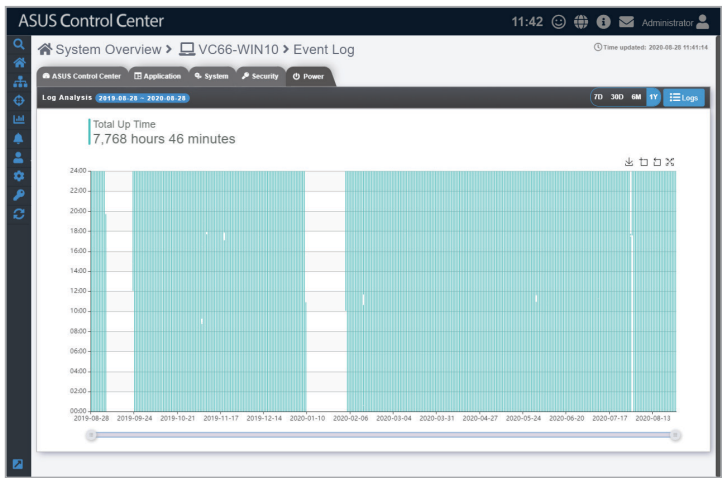
30 Days (Log Analysis):



6 Months (Log Analysis):

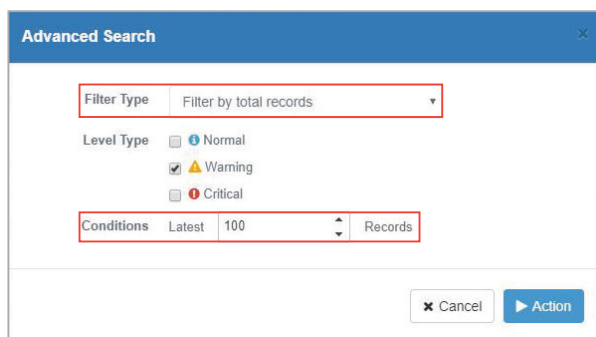


1 Year (Log Analysis):



## Filtering the event log using advanced search

1. Click on **Advance**.
2. Select the **Filter Type**.
  - **Filter by total records:** Filters according to the number of records.
  - **Filter by Timestamp:** Filters according to the set time period.
3. Select the **Level Type(s)** you wish to filter
4. The **Conditions** may vary depending on the **Filter Type** selected.
  - **Filter by total records:** Set the amount of records to show. This amounts increments by 100 and ranges from 100 to 5000 records.



The screenshot shows the 'Advanced Search' dialog box with a blue header and a close button. The 'Filter Type' dropdown is set to 'Filter by total records'. Under 'Level Type', 'Warning' is selected with a checkbox. The 'Conditions' section shows 'Latest' as the sort order and '100' as the number of records, with a 'Records' label to the right. At the bottom right are 'Cancel' and 'Action' buttons.

| Advanced Search                                                             |                                                                                                                     |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Filter Type                                                                 | Filter by total records                                                                                             |
| Level Type                                                                  | <input type="checkbox"/> Normal<br><input checked="" type="checkbox"/> Warning<br><input type="checkbox"/> Critical |
| Conditions                                                                  | Latest 100 Records                                                                                                  |
| <input type="button" value="Cancel"/> <input type="button" value="Action"/> |                                                                                                                     |



- **Filter by Timestamp:** Select a time period to show records, or set a custom time frame to show records within the set time frame.

The screenshot shows the 'Advanced Search' dialog box. The 'Filter Type' dropdown is set to 'Filter by Timestamp'. The 'Level Type' section has three options: 'Normal' (unchecked), 'Warning' (unchecked), and 'Critical' (checked). The 'Conditions' dropdown is set to 'Custom Time Period'. A dropdown menu is open below 'Custom Time Period', showing options: 'Custom Time Period' (highlighted), 'Latest 1 Hour', 'Latest 12 Hours', 'Latest 1 Day', 'Latest 1 Week', 'Latest 2 Weeks', and 'Latest 1 Month'. The 'Start Date & Time' and 'End Date & Time' fields are empty. There are 'Cancel' and 'Action' buttons at the bottom right.

When you select **Custom Time Period**, you can select a **Start Date & Time**, and **End Date & Time**.

The screenshot shows the 'Advanced Search' dialog box with the 'Filter Type' set to 'Filter by Timestamp' and 'Conditions' set to 'Custom Time Period'. The 'Start Date & Time' field is populated with '2019/01/24 18:10'. The 'End Date & Time' field is empty. A date and time picker is open, showing a calendar for January 2019. The date '24' is selected. To the right of the calendar, a time selection list shows times from 18:00 to 20:30 in 30-minute increments, with '18:00' currently selected. There are 'Cancel' and 'Action' buttons at the bottom right.

5. Click **Action** to start filtering the Event Log.

**NOTE:** This function will replace the Event Log list with the new results, and searching / filtering using the Search toolbar will only perform a search / filter on the new Event Log list.

Filter example of **Warning Level Type of Filter by total records:**

The screenshot shows the ASUS Control Center interface with the 'Event Log' tab selected. The top status bar displays 50 Normal, 30 Warning, and 47 Critical records. The 'Log' section shows a search bar and a table of events. The table is filtered to show only Warning level events.

| Level Type | Date & Time         | Message                                                     |
|------------|---------------------|-------------------------------------------------------------|
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 27 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 26 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 25 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 24 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 23 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 22 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 21 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 20 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 19 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 18 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 17 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 16 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 15 Utilization: 94 % Status: Normal -> Warning |
| Warning    | 2019-05-11 11:26:41 | CPU Core ID: 14 Utilization: 94 % Status: Normal -> Warning |

Filter example of **Critical Level Type Filter by Timestamp:**

The screenshot shows the ASUS Control Center interface with the 'Event Log' tab selected. The top status bar displays 50 Normal, 30 Warning, and 47 Critical records. The 'Log' section shows a search bar and a table of events. The table is filtered to show only Critical level events.

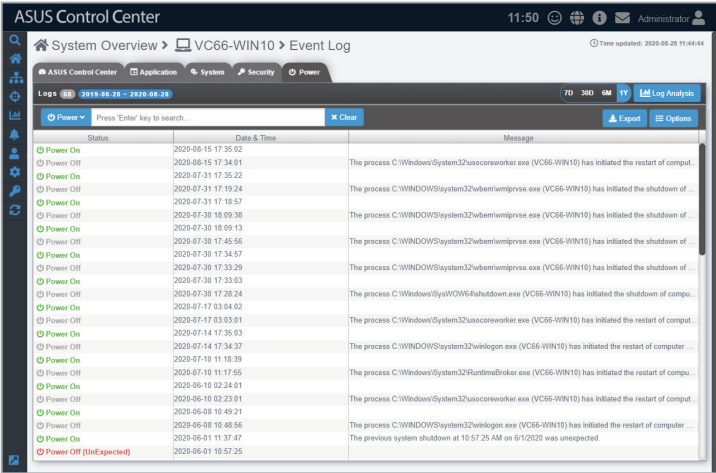
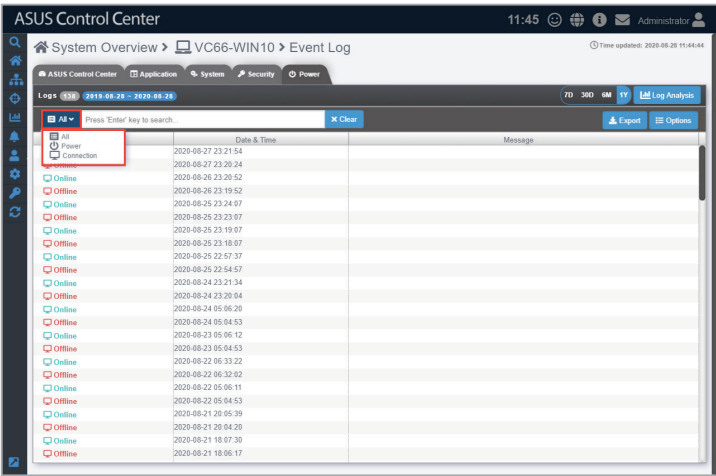
| Level Type | Date & Time         | Message                                                        |
|------------|---------------------|----------------------------------------------------------------|
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 0 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 1 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 2 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 3 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 4 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 5 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 6 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 7 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 8 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 9 Utilization: 100 % Status: Warning -> Critical  |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 10 Utilization: 100 % Status: Warning -> Critical |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 11 Utilization: 100 % Status: Warning -> Critical |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 12 Utilization: 100 % Status: Warning -> Critical |
| Critical   | 2019-05-11 11:27:41 | CPU Core ID: 13 Utilization: 100 % Status: Warning -> Critical |

## Filtering the Power event log

Click on , then select the criteria to filter.

**NOTE:**

- Selecting **All** will display all power event log items.
- Selecting **Power** will only display power related events.
- Selecting **Connection** will only display online/offline events.

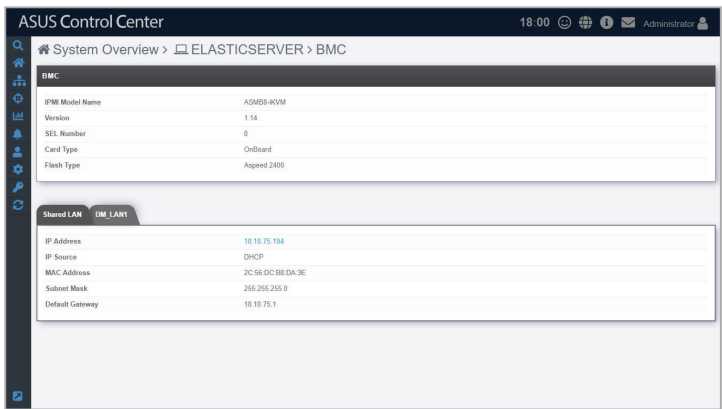


## 2.2.6 BMC

This item displays the information on the BMC of the managed device, you may also set the BMC using ASMB through the **Shared LAN** and **DM\_LAN** tabs.

**NOTE:**

- The managed device has to support BMC to use the functions described in this section. The BMC option will be grayed out if BMC is unavailable on the managed device.
- The information entered in this section is for reference only.



### Shared LAN

**NOTE:** BMC is required to use this item.

This item is the communication port for BMC and OS, clicking on the BMC IP in the **IP Address** field will redirect you to the ASMB page, allowing you to view the hardware sensor values of the device.

### DM\_LAN

**NOTE:** BMC is required to use this item.

This item is the communication port specifically for BMC, clicking on the BMC IP in the **IP Address** field will redirect you to the ASMB page, allowing you to view the hardware sensor values of the device.

## Edit BMC using ASMB

To edit BMC settings using ASMB on the device:

1. Select **DM\_LAN1** or **Shared LAN**, then click on any of the IP Addresses.

| DM_LAN1                               | Shared LAN |
|---------------------------------------|------------|
| Host Name                             |            |
| AM000EB112233                         |            |
| IPv4 Default Gateway                  |            |
| fe80::21b:178:675:5913                |            |
| MAC Address                           |            |
| 00:E9:EB:11:22:33                     |            |
| Speed                                 |            |
| 1000 Mbps                             |            |
| IPv4                                  |            |
| IP Address                            |            |
| 10.10.75.229                          |            |
| IP Source                             |            |
| Static                                |            |
| Subnet Mask                           |            |
| 255.255.0.0                           |            |
| Default Gateway                       |            |
| 0.0.0.0                               |            |
| IPv6 (SLAAC)                          |            |
| IP Address                            |            |
| 2001:b030:2311:202:2ef:ebff:fe11:2233 |            |
| IP Source                             |            |
| SLAAC                                 |            |
| Subnet Mask                           |            |
|                                       |            |
| Default Gateway                       |            |
|                                       |            |
| IPv6 (LinkLocal)                      |            |
| IP Address                            |            |
| fe80::2ef:ebff:fe11:2233              |            |
| IP Source                             |            |
| LinkLocal                             |            |
| Subnet Mask                           |            |
|                                       |            |
| Default Gateway                       |            |
|                                       |            |

2. Log into ASMB.

ASMB9-IRVM

Username

Password

en - English

☐ Remember Username

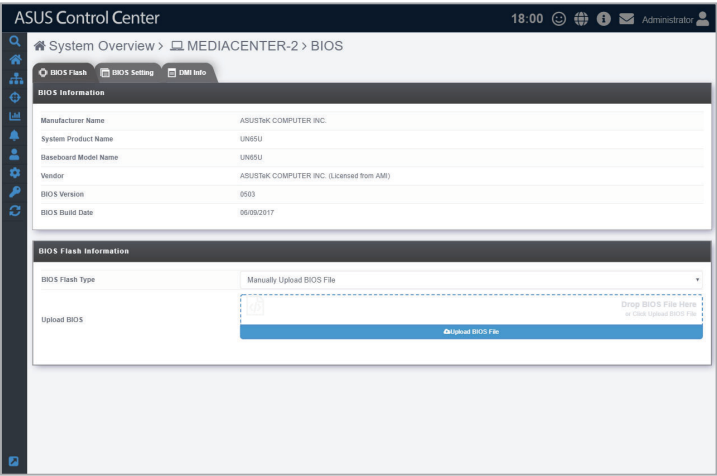
Log in

[Forgot my password](#)

# 2.2.7 BIOS

This item allows you to update the BIOS of a managed device by uploading a BIOS cap file or selecting a BIOS cap file from the BIOS Cache, view and adjust BIOS settings, and view the Desktop Management Interface Information.

**NOTE:** The functions available in this item may vary according to managed device.

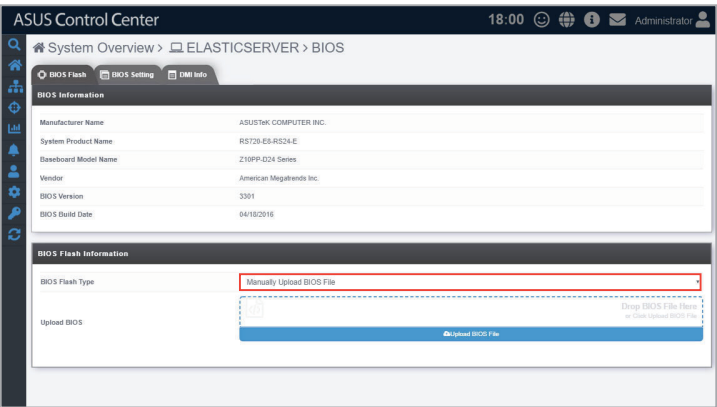


## BIOS Flash

The **BIOS Flash** tab allows you to flash the BIOS of the device by manually uploading a BIOS cap file or selecting a BIOS cap file from the BIOS Cache.

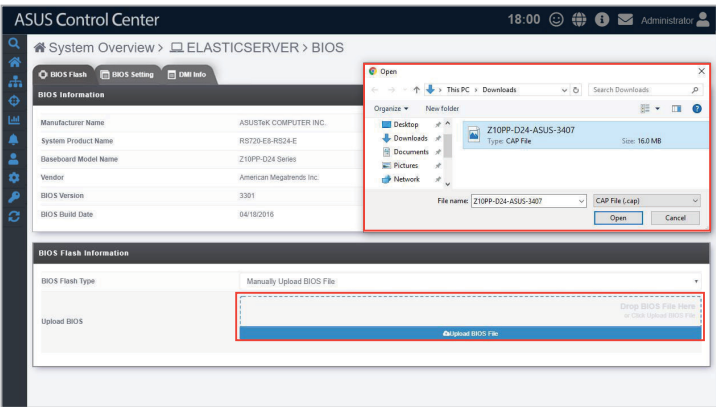
**IMPORTANT:** Flashing the BIOS using ASUS Control Center is only supported on managed devices that are ASUS products.

1. You can upload or select your BIOS cap file using the following methods:
  - **Manually uploading BIOS cap file**
    - a. Select **Manually Upload BIOS File** in the **BIOS Flash Type** field.



- b. Click on **Upload BIOS File** to select a BIOS cap file, or drag the BIOS cap file into the dotted square.

**NOTE:** The uploaded BIOS cap file will automatically be added to the **BIOS Cache**.



- **Selecting BIOS cap file from the BIOS Cache**

a. Select **Flash From BIOS Cache** in the **BIOS Flash Type** field.

ASUS Control Center 18:00 Administrator

System Overview > ELASTICSERVER > BIOS

BIOS Flash BIOS Setting CMM Info

**BIOS Information**

|                      |                          |
|----------------------|--------------------------|
| Manufacturer Name    | ASUSTEK COMPUTER INC.    |
| System Product Name  | RS720-ES-RS24-E          |
| Baseboard Model Name | Z10PP-D24 Series         |
| Vendor               | American Megatrends Inc. |
| BIOS Version         | 3301                     |
| BIOS Build Date      | 04/18/2016               |

**BIOS Flash Information**

|                      |                                                          |
|----------------------|----------------------------------------------------------|
| BIOS Flash Type      | Flash From BIOS Cache                                    |
| BIOS Cache List      | Z10PP-D24_3407                                           |
| Automatic Reboot     | <input type="checkbox"/> Reboot after BIOS Flash         |
| Locator LED          | <input type="checkbox"/> Turn on (BMC only)              |
| Baseboard Model Name | Z10PP-D24                                                |
| BIOS Version         | 3407                                                     |
| BIOS Build Date      | 01/11/2017                                               |
| BIOS Update Message  | Please click the 'Flash' button to start the BIOS Flash. |

Flash Cancel

b. Select a BIOS cap file to use from the **BIOS Cache List** drop down menu.

ASUS Control Center 18:00 Administrator

System Overview > ELASTICSERVER > BIOS

BIOS Flash BIOS Setting CMM Info

**BIOS Information**

|                      |                          |
|----------------------|--------------------------|
| Manufacturer Name    | ASUSTEK COMPUTER INC.    |
| System Product Name  | RS720-ES-RS24-E          |
| Baseboard Model Name | Z10PP-D24 Series         |
| Vendor               | American Megatrends Inc. |
| BIOS Version         | 3301                     |
| BIOS Build Date      | 04/18/2016               |

**BIOS Flash Information**

|                      |                                                          |
|----------------------|----------------------------------------------------------|
| BIOS Flash Type      | Flash From BIOS Cache                                    |
| BIOS Cache List      | Z10PP-D24_3407                                           |
| Automatic Reboot     | <input type="checkbox"/> Reboot after BIOS Flash         |
| Locator LED          | <input type="checkbox"/> Turn on (BMC only)              |
| Baseboard Model Name | Z10PP-D24                                                |
| BIOS Version         | 3407                                                     |
| BIOS Build Date      | 01/11/2017                                               |
| BIOS Update Message  | Please click the 'Flash' button to start the BIOS Flash. |

Flash Cancel



2. (optional) You may check the **Reboot after BIOS Flash** checkbox in the **Automatic Reboot** field to automatically reboot the device after BIOS has been flashed.

ASUS Control Center 18:00 Administrator

System Overview > ELASTICSERVER > BIOS

BIOS Flash BIOS Setting FMI Info

**BIOS Information**

|                      |                          |
|----------------------|--------------------------|
| Manufacturer Name    | ASUSTeK COMPUTER INC.    |
| System Product Name  | RS720-E8-RS24-E          |
| Baseboard Model Name | Z10PP-D24 Series         |
| Vendor               | American Megatrends Inc. |
| BIOS Version         | 3301                     |
| BIOS Build Date      | 04/18/2016               |

**BIOS Flash Information**

BIOS Flash Type: Manually Upload BIOS File

Upload BIOS: Z10PP-D24.ASUS-3407.CAP (19.00 MB) [Upload BIOS File](#)

**Automatic Reboot** ☒ Reboot after BIOS Flash

Locator LED ☐ Turn on (BMC only)

Baseboard Model Name: Z10PP-D24

BIOS Version: 3407

BIOS Build Date: 01/11/2017

BIOS Update Message: Please click the 'Flash' button to start the BIOS Flash.

[Flash](#) [Cancel](#)

3. (optional) You may check the **Turn On (BMC only)** checkbox in the Locator LED field to turn on the Locator LED once BIOS Flash is completed.

**NOTE:** BMC is required for this option to work properly.

ASUS Control Center 18:00 Administrator

System Overview > ELASTICSERVER > BIOS

BIOS Flash BIOS Setting FMI Info

**BIOS Information**

|                      |                          |
|----------------------|--------------------------|
| Manufacturer Name    | ASUSTeK COMPUTER INC.    |
| System Product Name  | RS720-E8-RS24-E          |
| Baseboard Model Name | Z10PP-D24 Series         |
| Vendor               | American Megatrends Inc. |
| BIOS Version         | 3301                     |
| BIOS Build Date      | 04/18/2016               |

**BIOS Flash Information**

BIOS Flash Type: Manually Upload BIOS File

Upload BIOS: Z10PP-D24.ASUS-3407.CAP (19.00 MB) [Upload BIOS File](#)

**Automatic Reboot** ☒ Reboot after BIOS Flash

**Locator LED** ☐ Turn on (BMC only)

Baseboard Model Name: Z10PP-D24

BIOS Version: 3407

BIOS Build Date: 01/11/2017

BIOS Update Message: Please click the 'Flash' button to start the BIOS Flash.

[Flash](#) [Cancel](#)

4. Click **Flash** to begin the BIOS flash, then wait for the BIOS flash to be completed.

ASUS Control Center 18:00 Administrator

System Overview > ELASTICSERVER > BIOS

BIOS Flash BIOS Setting OMI Info

**BIOS Information**

|                      |                        |
|----------------------|------------------------|
| Manufacturer Name    | ASUSTeK COMPUTER INC.  |
| System Product Name  | R572S-ES-RS24-E        |
| Baseboard Model Name | Z10PP-D24 Series       |
| Vendor               | American Megatech Inc. |
| BIOS Version         | 3301                   |
| BIOS Build Date      | 04/18/2016             |

**BIOS Flash Information**

BIOS Flash Type: Manually Upload BIOS File

Upload BIOS:  Z10PP-D24-ASUS-3407.CAP (19.05 MB)

Automatic Reboot: ☐ Reboot after BIOS Flash

Locator LED: ☐ Turn on (BMC only)

Baseboard Model Name: Z10PP-D24

BIOS Version: 3407

BIOS Build Date: 01/11/2017

BIOS Update Message: Please click the 'Flash' button to start the BIOS Flash.

ASUS Control Center 18:00 Administrator

System Overview > ELASTICSERVER > BIOS

BIOS Flash BIOS Setting OMI Info

**BIOS Information**

|                      |                        |
|----------------------|------------------------|
| Manufacturer Name    | ASUSTeK COMPUTER INC.  |
| System Product Name  | R572S-ES-RS24-E        |
| Baseboard Model Name | Z10PP-D24 Series       |
| Vendor               | American Megatech Inc. |
| BIOS Version         | 3301                   |
| BIOS Build Date      | 04/18/2016             |

**BIOS Flash Information**

BIOS Flash Type: Manually Upload BIOS File

Automatic Reboot: ☐ Reboot after BIOS Flash

Locator LED: ☐ Turn on (BMC only)

Baseboard Model Name: Z10PP-D24

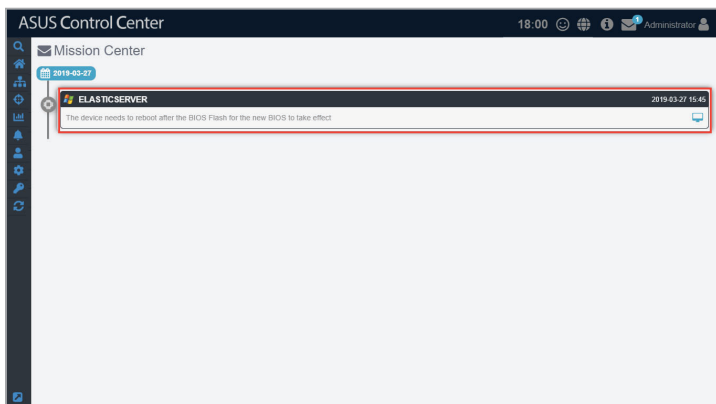
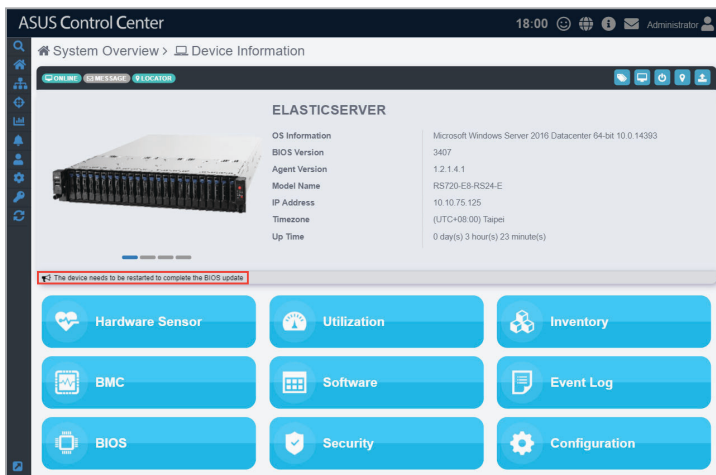
BIOS Version: 3407

BIOS Build Date: 01/11/2017

BIOS Update Progress:  100%

BIOS Update Message: BIOS Updated.

- Once the BIOS flash has been completed, a pop-up window will appear, prompting you to reboot the system, click **OK**. You can also view this message in the **Device Information** screen and **Mission Center**.



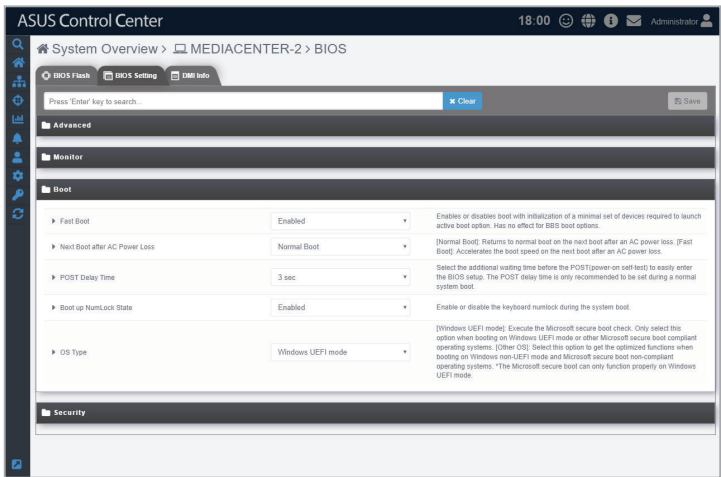
- Reboot the device to complete the BIOS flash.

## BIOS Setting

**IMPORTANT:** The **BIOS Setting** tab is only available on specific ASUS products such as an ASUS commercial notebook PC. For more information on ASUS products that support ASUS Control Center, please refer to <https://asuscontrolcenter.asus.com>.

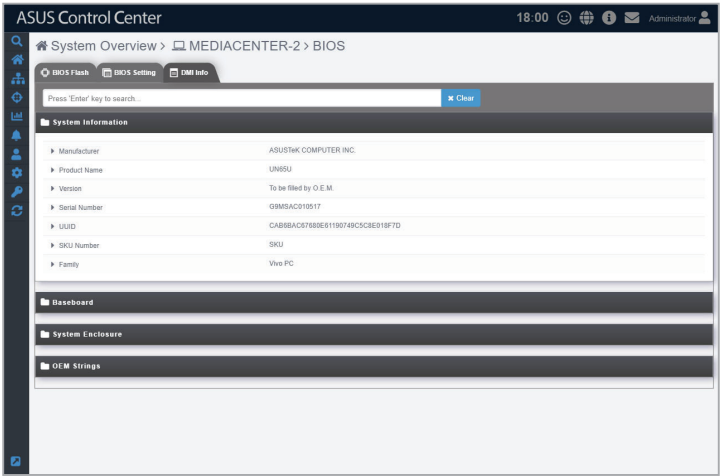
The **BIOS Setting** tab allows you to view and adjust the BIOS **Advanced**, **Monitor**, **Boot**, and **Security** settings of the device, providing you with a quick way of adjusting BIOS settings without having to enter the BIOS menu of the device.

**NOTE:** The BIOS settings may differ between devices. Please refer to the device's motherboard user manual for more information about the BIOS settings.



DMI Info

Under the SMBIOS standard, the **DMI Info** tab allows you to view details on certain items such as manufacturer name and hardware component information of the device without a hardware controller.

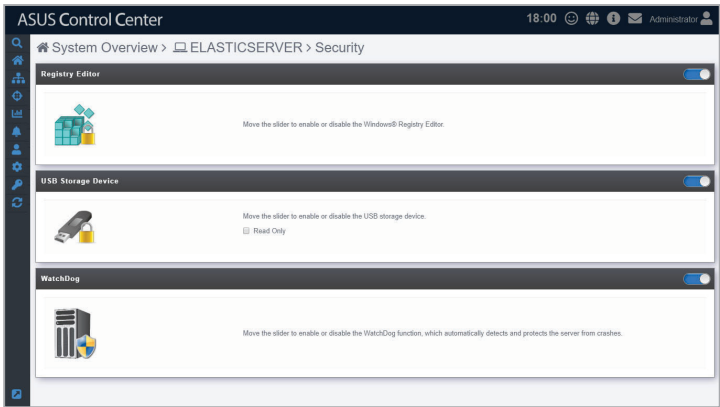


## 2.2.8 Security

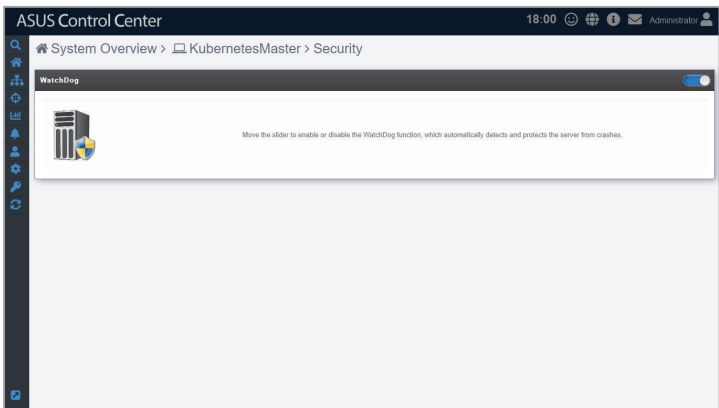
This item allows you to set permissions on the device for the **Registry Editor**, **USB Storage Device**, and **Watchdog**. For centralized permission settings on multiple devices, refer to the **Security Management** section.

**NOTE:** Linux systems only support **Watchdog**.

For Windows® system:

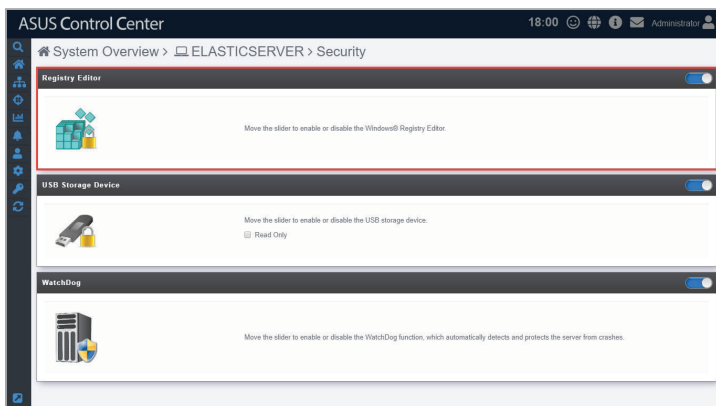


For Linux system:



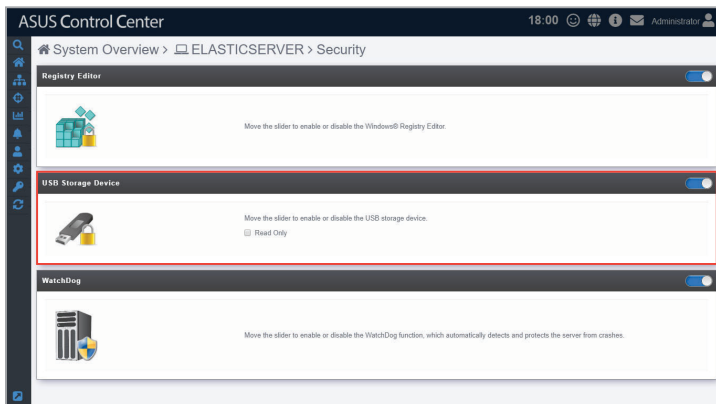
## Registry Editor (Windows only)

The **Registry Editor** allows you to enable or disable access to Regedit Tool in Windows® by the managed device's user. Click the slider to enable or disable the **Registry Editor**.



## USB Storage Device (Windows only)

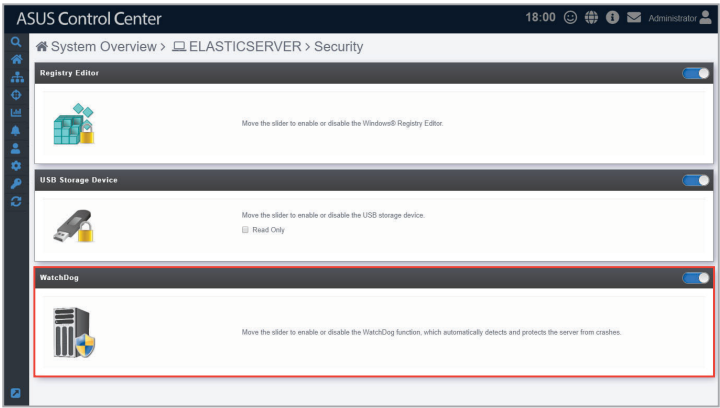
**USB Storage Device** allows you to enable or disable access of a USB storage device connected to a USB port on the managed device. You can also set USB storage devices to read-only permissions by checking the **Read Only** checkbox. Click the slider to enable or disable **USB Storage Device**.



## Watchdog

**Watchdog** allows you to enable or disable the Watchdog timer. When the watchdog timer in unresponsive due to hardware fault or program error, it will reboot the device. Click the slider to enable or disable **Watchdog**.

**NOTE:** Auto Restart needs to be disabled on Windows® Server 2016 or later versions for **Watchdog** to successfully reboot the device when required. To disable **Auto Restart**, search for **Control Center** in the Windows Search Box, then navigate to **System > Advanced System Settings > Startup and Recovery**.



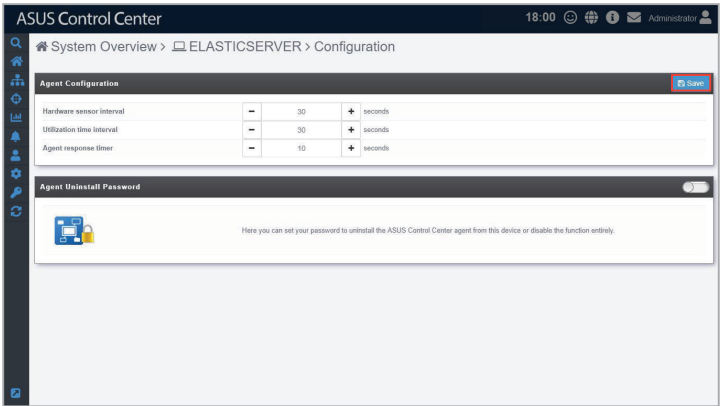


## 2.2.9 Configuration

This item allows you to configure the interval at which hardware and utilization sensors are checked, and set the interval which the agent will respond to the server's requests. You can also set a password which has to be entered when removing the agent from the managed device.

### Agent Configuration

Configure the interval at which hardware and utilization sensors are checked, and the interval at which the agent will request updates on tasks from the ASUS Control Center server. You can configure these options by clicking on  /  to increase or decrease the time, then click **Save** to save the changes made.



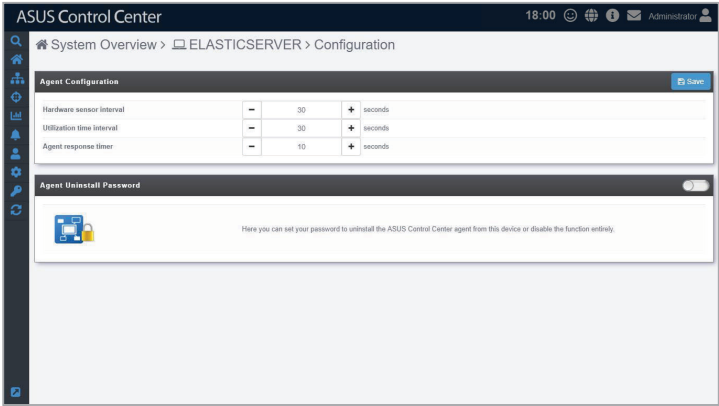
|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware sensor interval  | <p>Interval in seconds at which the hardware sensor information is sent to the ASUS Control Center server.</p> <ul style="list-style-type: none"><li>* The default is set to 30 seconds, which means that every 30 seconds the agent will report items such as fan disconnected back to the ACC server, and the ACC server will update this fan status within 30 seconds of receiving this report from the agent.</li></ul>                                                          |
| Utilization time interval | <p>Interval in seconds at which the utilization information is sent to the ASUS Control Center server.</p> <ul style="list-style-type: none"><li>* The default is set to 30 seconds, which means that every 30 seconds the agent will report items such as CPU stress test back to the ACC server, and the ACC server will update this CPU status within 30 seconds of receiving this report from the agent.</li></ul>                                                               |
| Agent response timer      | <p>Interval in seconds at which the agent will query the ASUS Control Center server for task updates.</p> <ul style="list-style-type: none"><li>* The default is set to 10 seconds, which means that every 10 seconds the agent will query the ACC server for new tasks. For example, when you set the Registry to disabled on the ACC server, the device will query the ACC server and receive this task, then perform this task within 10 seconds of receiving the task.</li></ul> |



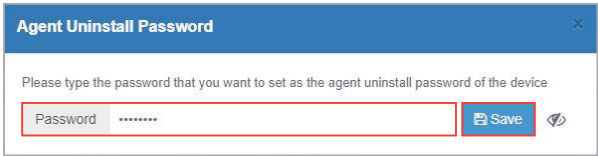
## Agent Uninstall Password

Set a password for agent uninstallation. The user will be prompted to enter the password when they want to uninstall the agent.

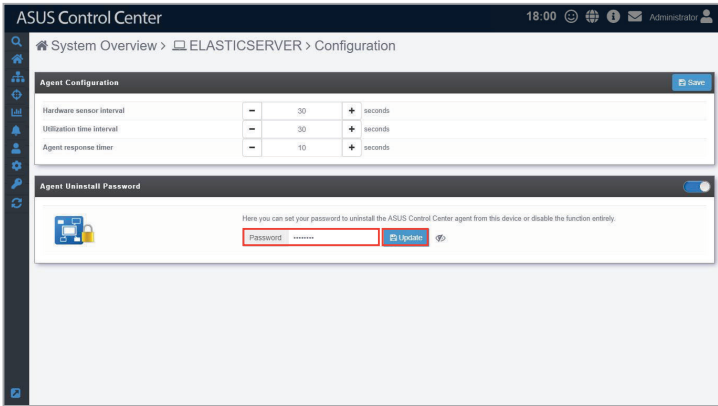
1. If **Agent Uninstall Password** is not enabled, click on the slider to enable it.



2. A pop-up window should appear, enter the password you wish to use, then click **Save**.

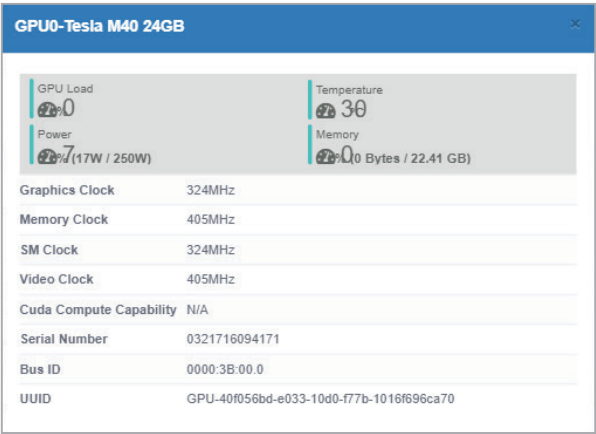
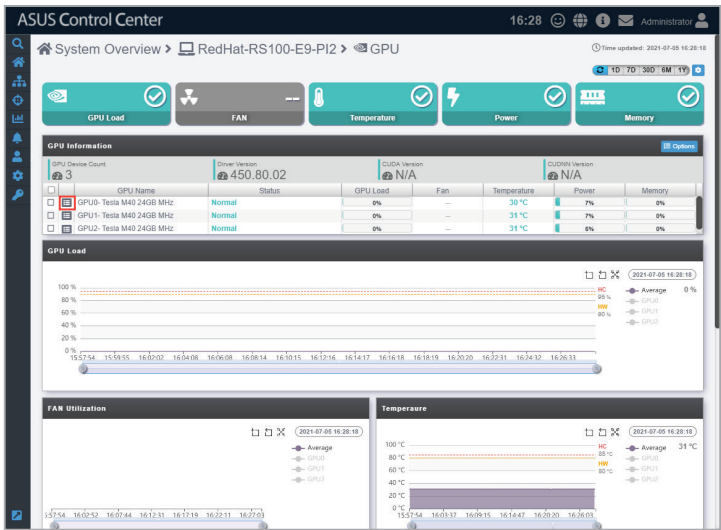


3. (optional) You can edit the password by entering a new password into the **Password** field, then clicking on **Update**.



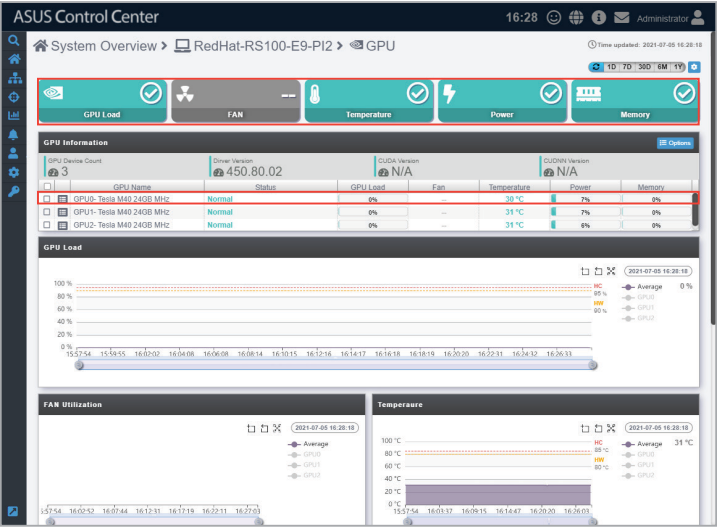
## 2.2.10 GPU

This item allows you to view the GPU Load, Fan, Temperature, Power, and Memory details on GPU cards installed on the device, and also view the timeline chart of these items. For more details on a GPU device click on  next to the GPU device.



### Filtering the GPU devices

By clicking on a status block you can filter the GPU devices shown in the GPU information block according to the status selected

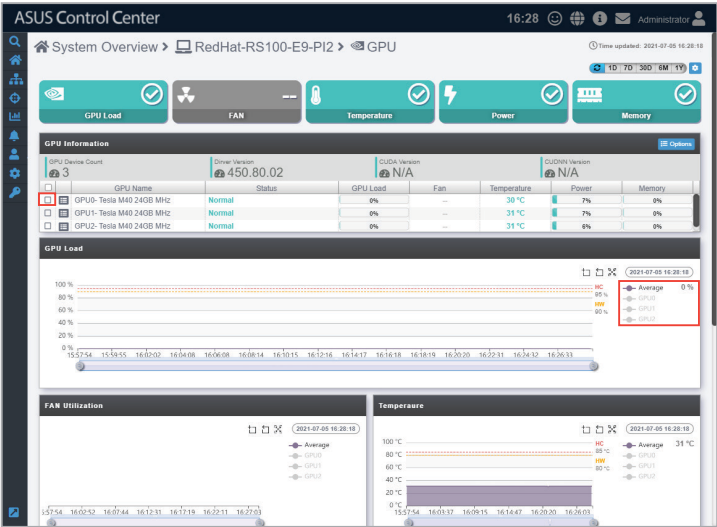


### Toggling the Chart View for GPU devices

You can view the timeline charts for GPU Load, Fan Utilization, Temperature, Power Utilization, Power Usage, Memory Utilization, and Memory Usage by scrolling down on the GPU page.

By default the timeline charts display the Average values, but you may select to view only selected GPU devices by checking the device in the GPU Information block, or by clicking on the GPU device(s) in the timeline chart legend.

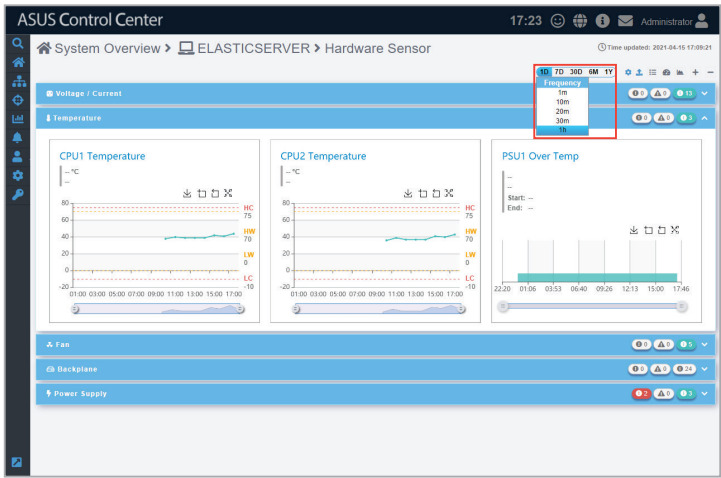
**NOTE:** Any changes made, such as selecting a device to view on a timeline chart will be applied to all other timeline charts, for example selecting GPU0 in the timeline chart legend of GPU Load timeline chart will cause all other timeline charts on this page to display information on GPU0 only.



### Chart Quick Buttons

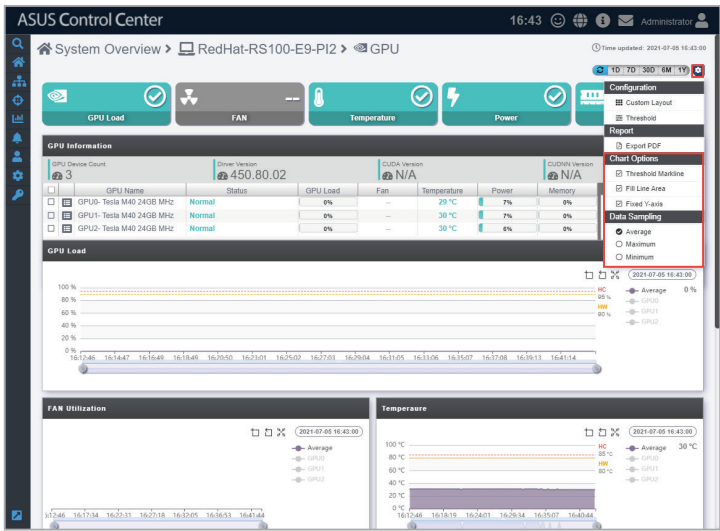
-  Click to zoom in on the timeline of the chart.
-  Click to zoom out on the timeline of the chart.
-  Click to restore the chart to its default view.

You can customize the timeline chart by selecting the period of time you wish to view for the timeline charts, then selecting the frequency for which the sensor should return data. This will be applied to the timeline charts for all the sensors shown on this page.



| Period of time | Frequency                      |
|----------------|--------------------------------|
| 1D             | 1m, 10m, 20m, 30m, 1h          |
| 7D             | 10m, 20m, 30m, 1h, 3h, 6h, 12h |
| 30D            | 30m, 1h, 3h, 6h, 12h, 1d       |
| 6M             | 3h, 6h, 12h, 1d, 7d, 14d       |
| 1Y             | 6h, 12h, 1d, 7d, 14d, 30d      |

Additionally, by clicking on the  icon, you can customize the data you wish to view on the timeline.



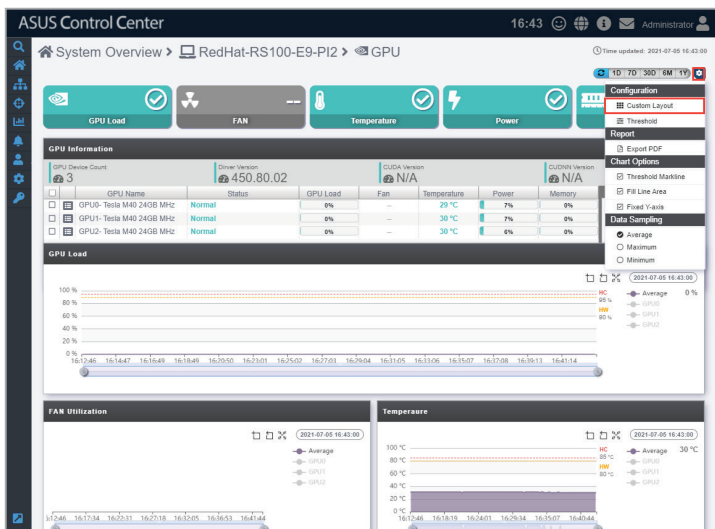
|                      |                                                                                                                                                                                             |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Chart Options</b> | Allows you to check the items you wish to display on the timeline charts such as <b>Threshold Markline</b> and <b>Fill Line Area</b> , or set a <b>Fixed Y-axis</b> for the timeline chart. |
| <b>Data Sampling</b> | Allows you to select whether the <b>Maximum</b> values, <b>Minimum</b> values, or <b>Average</b> values should be displayed on the timeline chart.                                          |



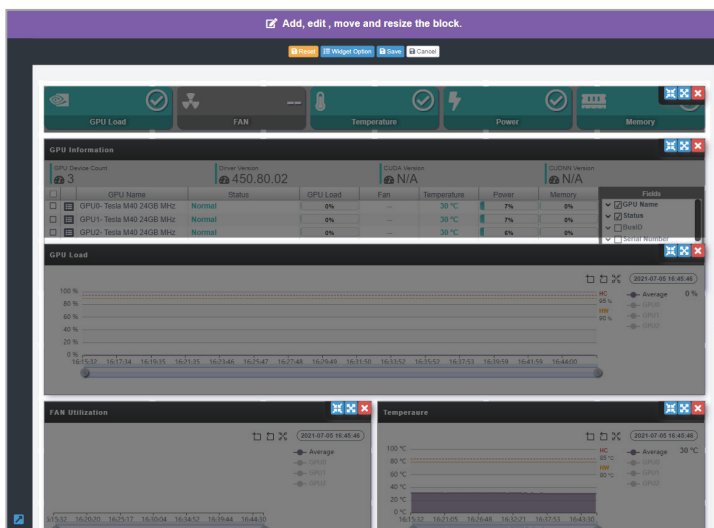
## Configuring the GPU layout

You can freely rearrange and resize the different blocks on the GPU page to change the layout of this page to your preference.

1. Click on the  icon, then select **Custom Layout**.



2. You can now rearrange or resize each of the blocks on this page. Please refer to the following for instructions on resizing or rearranging the blocks.

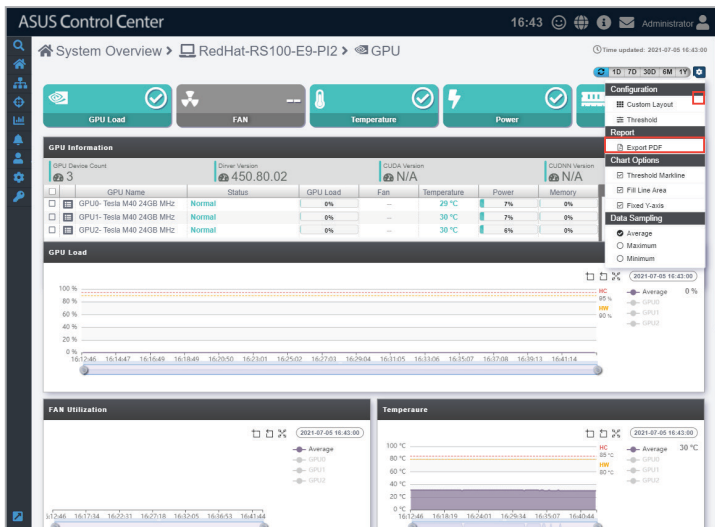


- **To resize the block:**  
Hover the mouse over the edges of the block you wish to resize until the resize arrows appear, then click and drag to resize the block.
  - **To expand the block to its maximum size:**  
Click on  to expand the block to its maximum size.
  - **To minimize the block to its minimum size:**  
Click on  to minimize the block to its minimum size.
  - **To rearrange the blocks:**  
Click and hold inside the block you would like to rearrange, then drag the block to rearrange it.
  - **To remove a block:**  
Click on  to remove the block, or click on  **Widget Option** and uncheck the block you wish to remove.
  - **To add a block:**  
Click on  **Widget Option** and check the block you wish to add.
  - **To reset to default layout:**  
Click on  **Reset** to reset the GPU page to its default layout.
3. Once you are finished rearranging and resizing the blocks, click on **Save** to save the changes made to this page.

## Editing the threshold valuesx

You can edit the critical and warning threshold values for **GPU** items.

1. Click on the  icon, then select **Threshold**.

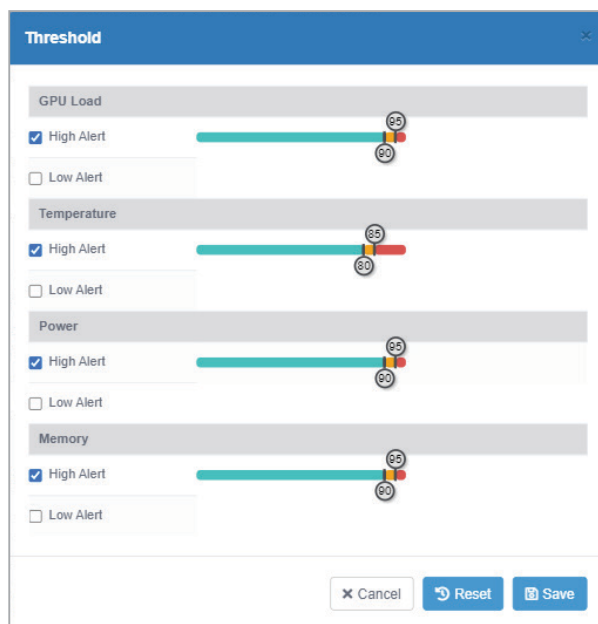


2. Adjust the thresholds for the sensors by sliding the **Normal** (green), **Warning** (yellow) and **Critical** (red) sliders for the **High Alert** and **Low Alert**. You can also disable or enable **High Alert** and/or **Low Alert** by checking/unchecking **High Alert** and/or **Low Alert**.

---

**NOTE:** Click on **Reset** to reset the threshold settings to default settings.

---



The image shows a 'Threshold' settings dialog box with a blue header and a close button. It contains four sections: GPU Load, Temperature, Power, and Memory. Each section has a horizontal slider with three colored segments: green (Normal), yellow (Warning), and red (Critical). The sliders are currently set to 25% for the green segment and 90% for the red segment. Each section also has two checkboxes: 'High Alert' (checked) and 'Low Alert' (unchecked). At the bottom, there are three buttons: 'Cancel', 'Reset', and 'Save'.

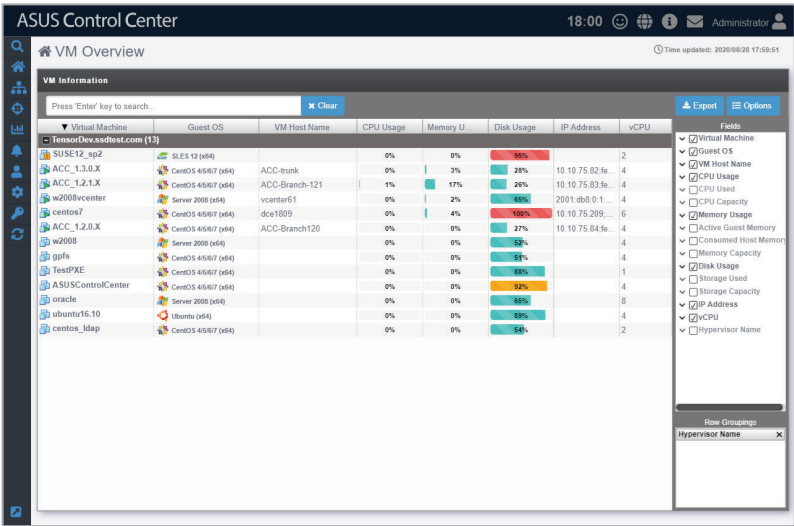
| Sensor      | High Alert                          | Low Alert                | Normal (Green) | Warning (Yellow) | Critical (Red) |
|-------------|-------------------------------------|--------------------------|----------------|------------------|----------------|
| GPU Load    | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 25%            |                  | 90%            |
| Temperature | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 25%            |                  | 90%            |
| Power       | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 25%            |                  | 90%            |
| Memory      | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 25%            |                  | 90%            |

3. Once you have finished adjusting the thresholds, click on **Save** to save the changes made.

## 2.3 VM Overview

The VM overview screen allows you to view all VMware vSphere Hypervisors as well as view the virtual machines of each vSphere device. The VM Information list displays details on all the virtual machines on the hypervisor, including CPU usage, Disk usage, Guest OS, and IP address.

To access the **VM Overview**, click  > **VM Overview** from the left menu.



**NOTE:**

- Click on the name of a column header to sort the filter results alphabetically.
- If **VMware Tool** is not installed, some items may not be displayed, such as IP address. To view all information about VMware vSphere installed, ensure to install **VMware Tool**.

### Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

## Exporting VMware vSphere Hypervisors list

You can export the list of VMware vSphere Hypervisors, virtual machines and metadata in the **VM Information** block to a .csv file by clicking on **Export**.

**NOTE:** Only metadata columns that are shown in the **VM Information** block will be exported to the .csv file. To add more metadata columns to the **VM Information** block, click on **Options**, then check the metadata item you wish to display.

ASUS Control Center18:00Administrator

VM Overview

Time updated: 2020/06/28 17:59:51

VM Information

Press 'Enter' key to search. Clear

ExportOptions

| Virtual Machine              | Guest OS            | VM Host Name   | CPU Usage | Memory U... | Disk Usage | IP Address        | vCPU |
|------------------------------|---------------------|----------------|-----------|-------------|------------|-------------------|------|
| [tenorDev.asustest.com (13)] |                     |                |           |             |            |                   |      |
| ASUS_E12_xp2                 | SLX'S 12 (x64)      |                | 0%        | 0%          | 90%        |                   | 2    |
| ACC_12.1.X                   | CentOS 4.56/7 (x64) | ACC-Funk       | 0%        | 3%          | 20%        | 10.10.75.82 fe... | 4    |
| ACC_12.1.X                   | CentOS 4.56/7 (x64) | ACC-Branch-121 | 1%        | 17%         | 20%        | 10.10.75.83 fe... | 4    |
| w2009vcenter                 | Server 2008 (x64)   | vcenter61      | 0%        | 2%          | 90%        | 2001.db.0.1...    | 4    |
| centos7                      | CentOS 4.56/7 (x64) | dca1009        | 0%        | 4%          | 100%       | 10.10.75.209      | 6    |
| ACC_12.0.X                   | CentOS 4.56/7 (x64) | ACC-Branch120  | 0%        | 0%          | 27%        | 10.10.75.84 fe... | 4    |
| w7008                        | Server 2008 (x64)   |                | 0%        | 0%          | 52%        |                   | 4    |
| gpf6                         | CentOS 4.56/7 (x64) |                | 0%        | 0%          | 31%        |                   | 4    |
| TestPXE                      | CentOS 4.56/7 (x64) |                | 0%        | 0%          | 99%        |                   | 1    |
| ASUSControlCenter            | Server 2008 (x64)   |                | 0%        | 0%          | 94%        |                   | 4    |
| oracle                       | Server 2008 (x64)   |                | 0%        | 0%          | 90%        |                   | 8    |
| ubuntu16.10                  | Ubuntu (x64)        |                | 0%        | 0%          | 90%        |                   | 4    |
| centos_1dnp                  | CentOS 4.56/7 (x64) |                | 0%        | 0%          | 94%        |                   | 2    |

Fields

☒ Virtual Machine

☒ Guest OS

☒ VM Host Name

☒ CPU Usage

☐ CPU Used

☐ CPU Capacity

☒ Memory Usage

☐ Active Guest Memory

☐ Consumed Host Memory

☐ Memory Capacity

☒ Disk Usage

☐ Storage Used

☐ Storage Capacity

☒ IP Address

☒ vCPU

☐ Hypervisor Name

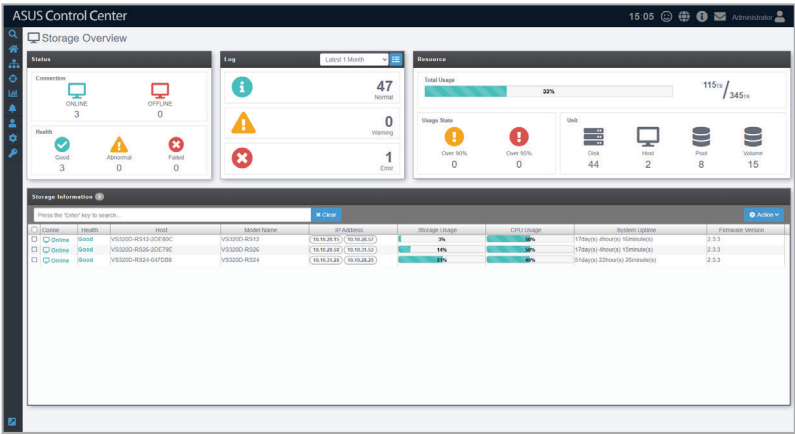
Row Groupings

Hypervisor Name X

## 2.4 Storage Overview

The storage overview screen allows you to view information from all managed storage devices.

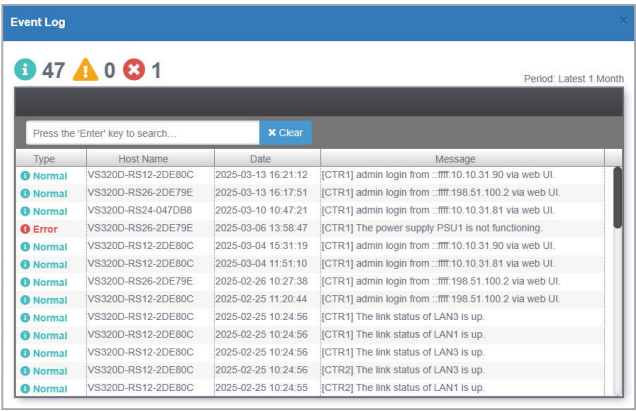
To access **Storage Overview**, click  > **Storage Overview** from the left menu.



**NOTE:** Refer to the **Add/Remove Storage** section of the **Deployment** chapter for more information on adding or removing managed storage devices.

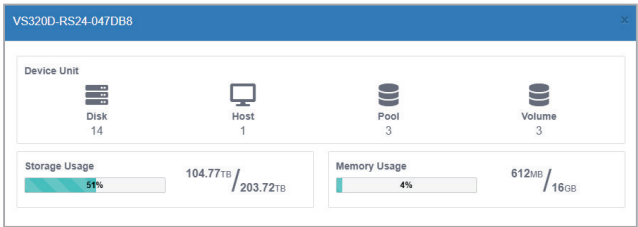
### Viewing the storage device event log

To view the storage device event log, select a date range from the drop-down menu in the **Log** block, then click the  icon.



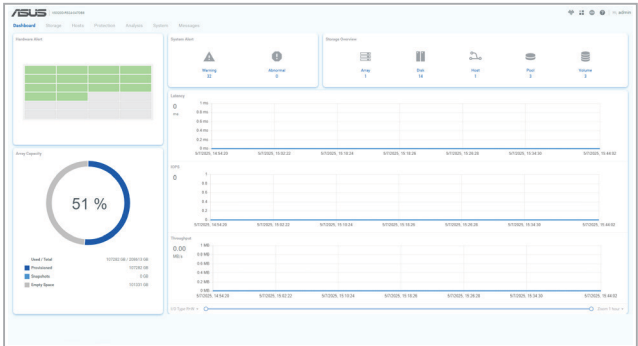
**Viewing detailed storage information**

Click a managed storage device in the **Storage Information** block to view detailed information.



**Opening the ASUS Storage dashboard**

Click the IP address of a managed storage device in the **Storage Information** block to open the ASUS Storage dashboard.



**Shutting down or restarting a managed storage device**

Click **Action** in the **Storage Information** block, then select the desired action from the **Power Control** menu.

**Using the search bar and search options**

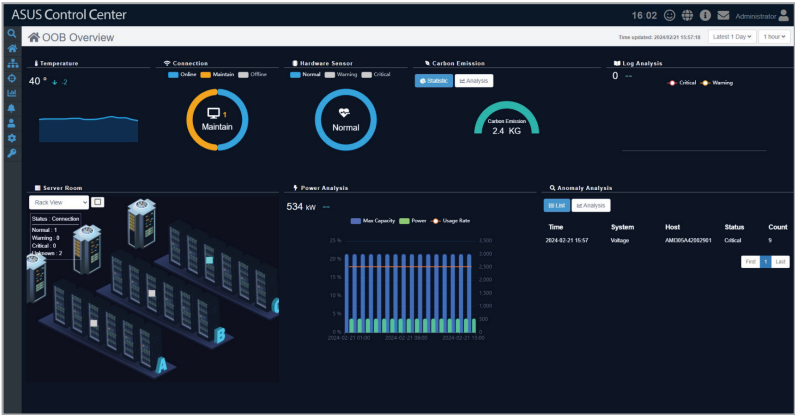
Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.



## 2.5 OOB Overview

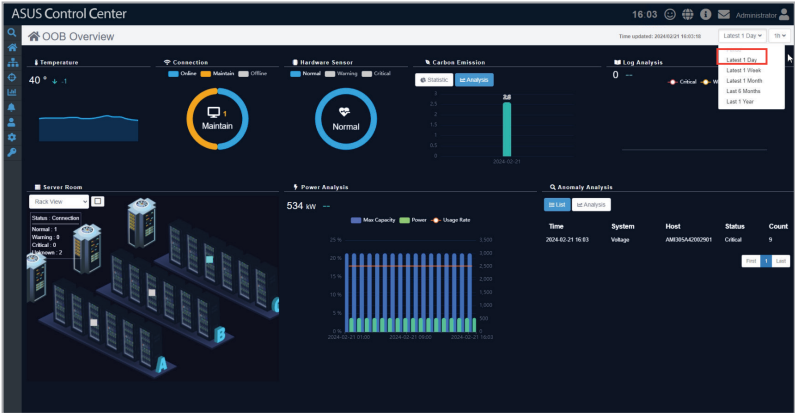
The OOB overview screen allows you to view information collected from sensors on all managed Redfish devices.

To access the **OOB Overview**, click  > **OOB Overview** from the left menu.



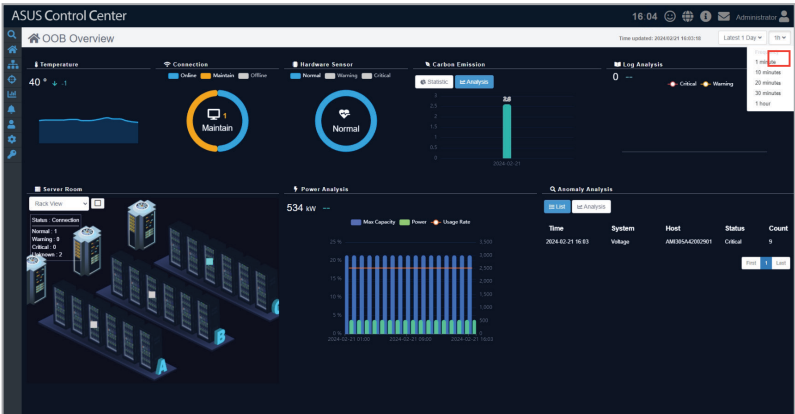
### Filtering the displayed information by time period

Select a time period from the **Period** drop down menu to only show records within the specified time period.



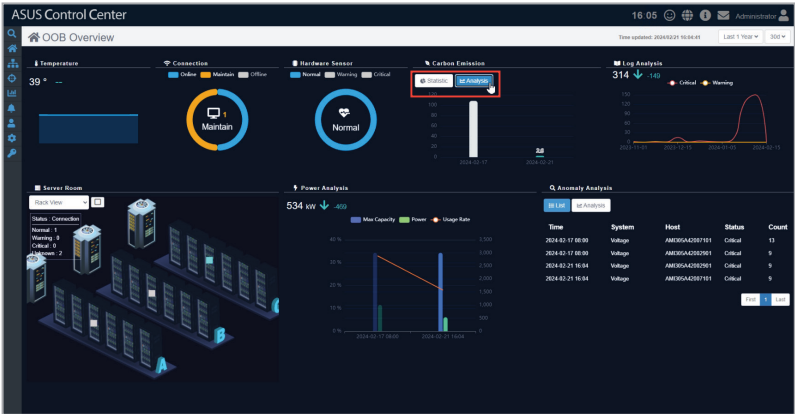
**Adjusting the frequency of displayed information**

Select a frequency from the **Frequency** drop down menu to group the displayed information by the selected frequency.



**Switching between views for displayed information**

In supported information blocks, select **Statistic**, **List**, or **Analysis** to switch between different views.



## 2.6 Host Information

**NOTE:** The screenshot may vary between agent and agentless devices, for more details on viewing details on devices with agents, refer to the **Device Information** section.

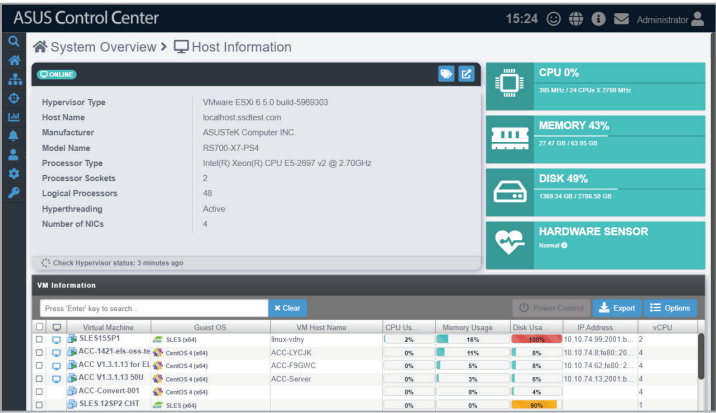
The **Host Information** screen gives you various functions to view the status and manage the selected hypervisor.

To access the **Host Information** of a hypervisor, you can use the following methods:

- From **System Overview**:
  - Click  > **System Overview** in the left menu.
  - Click on the hypervisor you wish to see more details about in the **Devices** list.

**NOTE:** VMware vSphere will display a  icon in the OS Information column.

- From **VM Overview**:
  - Click  > **VM Overview** in the left menu.
  - Click on a VM of a hypervisor you wish to see more details about in the **VM Information** list.



The screenshot shows the ASUS System Control Center interface. The top bar displays the title "ASUS System Control Center", the time "15:24", and the user "Administrator". The main navigation pane on the left includes icons for System Overview, Host Information, VM Overview, and VM Information. The "Host Information" tab is selected, showing details for a VMware ESX 6.5.0 build-5969303. The details include Host Name (localhost.ssdtest.com), Manufacturer (ASUSTeK Computer INC.), Model Name (RS700-X7-PS4), Processor Type (Intel(R) Xeon(R) CPU E5-2697 v2 @ 2.70GHz), Processor Sockets (2), Logical Processors (48), Hyperthreading (Active), and Number of NICs (4). On the right, there are four status cards: CPU 0% (35G MHz / 24 CPUs X 2700 MHz), MEMORY 43% (27.47 GB / 63.95 GB), DISK 49% (1585.54 GB / 2786.56 GB), and HARDWARE SENSOR (Normal). Below these, the "VM Information" section shows a table of virtual machines.

| Virtual Machine                                                                                          | Guest OS       | VM Host Name | CPU Use | Memory Usage | Disk Use | IP Address            | vCPU |
|----------------------------------------------------------------------------------------------------------|----------------|--------------|---------|--------------|----------|-----------------------|------|
|  SLES15SP1            | SLES (x64)     | linux-vbny   | 2%      | 16%          | 100%     | 10.10.74.99/2001.b... | 2    |
|  ACC-1421-489-098-8e  | CentOS 4 (x64) | ACC-LYCJK    | 0%      | 11%          | 8%       | 10.10.74.8/80-20...   | 4    |
|  ACC-V1.3.1.13 for EL | CentOS 4 (x64) | ACC-F9GWC    | 0%      | 5%           | 8%       | 10.10.74.62/600-2...  | 4    |
|  ACC-V1.3.1.13.500    | CentOS 4 (x64) | ACC-Server   | 0%      | 3%           | 8%       | 10.10.74.13/2001.b... | 4    |
|  ACC-Convert-001      | CentOS 4 (x64) |              | 0%      | 0%           | 4%       |                       | 4    |
|  SLES 12SP2 CHT       | SLES (x64)     |              | 0%      | 0%           | 80%      |                       | 1    |

Device Statuses and Quick Buttons

- **Connection status** This item displays the connection status of the selected managed device.
- **Metadata Editor** This item allows you to edit the metadata of the hypervisor by double clicking in the **Value** field.
- **VMware ESXi** This item allows you to link to the vSphere Web Client management interface.

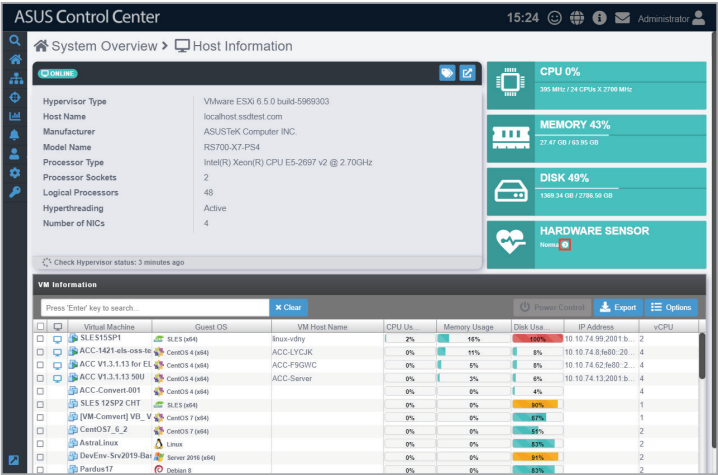
**NOTE:** VMware ESxi link is only available if a Web Client management interface link is detected.

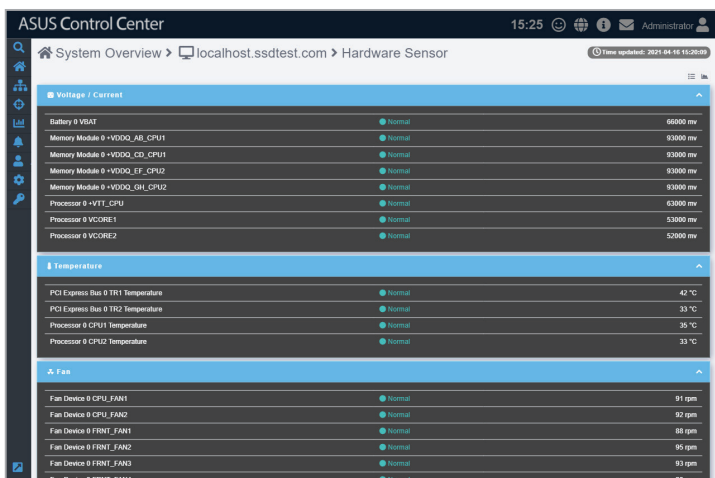
Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

2.6.1 Hardware Sensor

This item allows you to view the details and values for the Voltage / Current, Temperature, Fan, Power Supply, CPU, and Other items. You can view the Hardware Sensor information for the selected device by clicking on the  arrow in the Hardware Sensor block.





## Quick Buttons



Click to switch the layout to list view.



Click to view timeline chart of hardware sensor statuses.



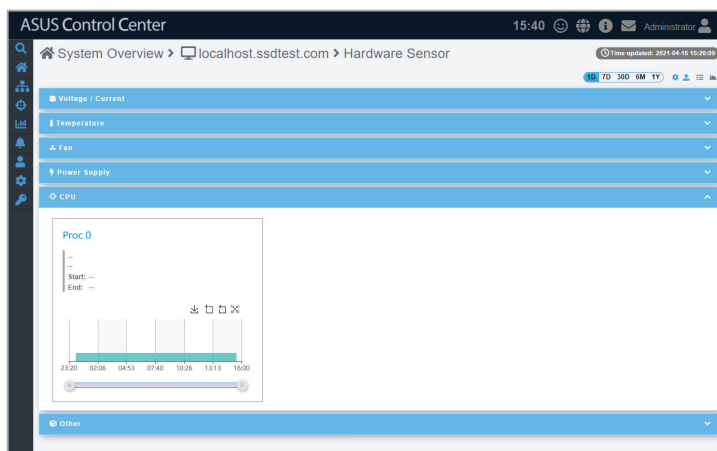
Click to expand this block.



Click to minimize this block.

## **Toggling the chart view for Hardware sensors**

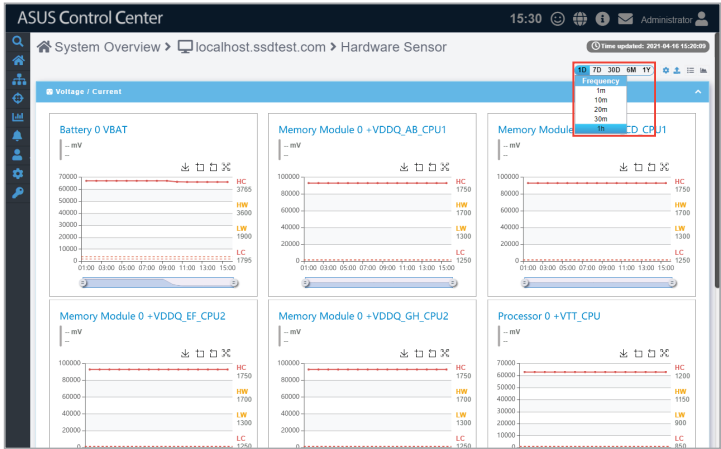
You can toggle the chart view which displays historical data for the Voltage / Current, Temperature, Fan, Power Supply, CPU, and Other sensor events according to different periods of time.



### **Quick Buttons for timeline chart**

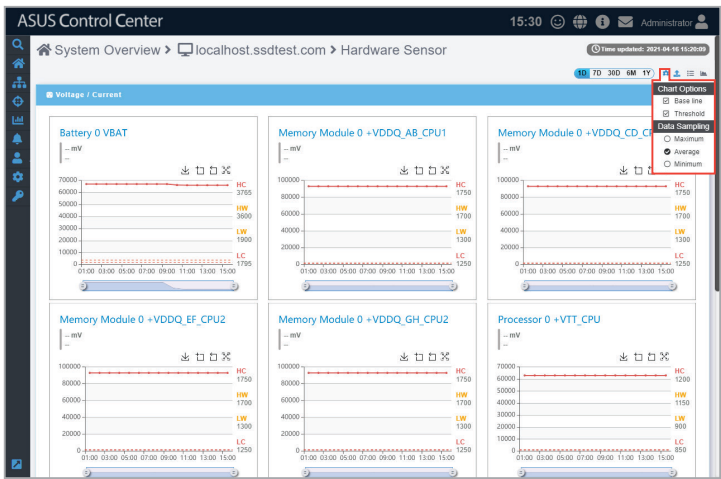
-  Click to refetch the device data.
-  Click to select which data to display on the timeline chart.
-  Click to expand this block.
-  Click to minimize this block.

You can customize the timeline chart by selecting the period of time you wish to view for the timeline charts, then selecting the frequency for which the sensor should return data. This will be applied to the timeline charts for all the sensors shown on this page.



| Period of time | Frequency                      |
|----------------|--------------------------------|
| 1D             | 1m, 10m, 20m, 30m, 1h          |
| 7D             | 10m, 20m, 30m, 1h, 3h, 6h, 12h |
| 30D            | 30m, 1h, 3h, 6h, 12h, 1d       |
| 6M             | 3h, 6h, 12h, 1d, 7d, 14d       |
| 1Y             | 6h, 12h, 1d, 7d, 14d, 30d      |

Additionally, by clicking on the  icon, you can customize the data you wish to view on the timeline

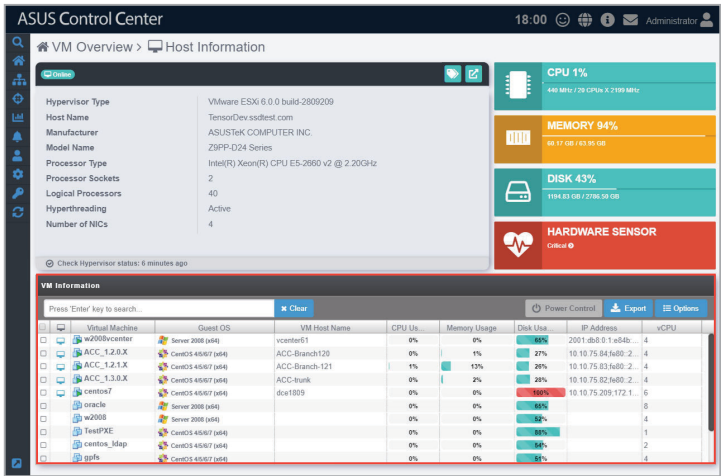


|                      |                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Chart Options</b> | Allows you to check the items you wish to display on the timeline charts such as the <b>Base line</b> and <b>Threshold</b> .                       |
| <b>Data Sampling</b> | Allows you to select whether the <b>Maximum</b> values, <b>Minimum</b> values, or <b>Average</b> values should be displayed on the timeline chart. |



## 2.6.2 VM Information

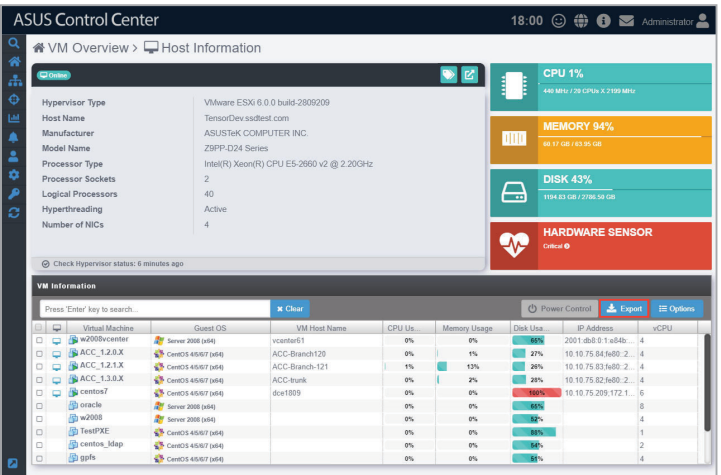
The virtual machines installed on the ESXi device are displayed in the VM Information block.



### Exporting VM Information

You can export the virtual machines and metadata of the selected hypervisor to a .csv file by clicking on **Export**.

**NOTE:** Only metadata columns that are shown in the **VM Information** block will be exported to the .csv file. To add more metadata columns to the **VM Information** block, click on **Options**, then check the metadata item you wish to display.

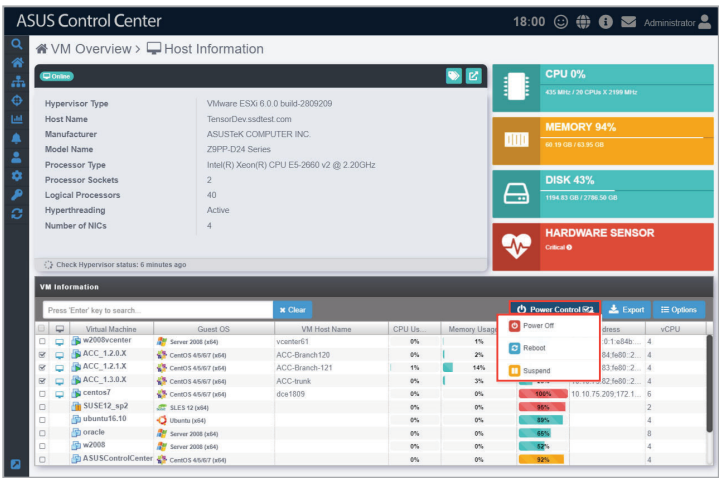


## Setting Power Control

You can control the power settings of selected VM(s) from the **VM Information** block allowing you quick access to power controls such as powering on and off, and rebooting selected VM(s).

**NOTE:** The Power Control options may vary between VMs and is controlled by the **VMware Tools** application managing the VM.

1. Select the VMs you would like to apply the power control option to.
2. Click on **Action**, then select the power control option you would like to apply to the selected VMs.



## Accessing remote desktop

The remote control function provides a flexible interface for device management through the desktop or command-line accessed in ASUS Control Center. You can quickly access the remote desktop of VMs from the **VM Information** block.

---

**IMPORTANT:** VMware Tools is required on the VM device you wish to use remote desktop on.

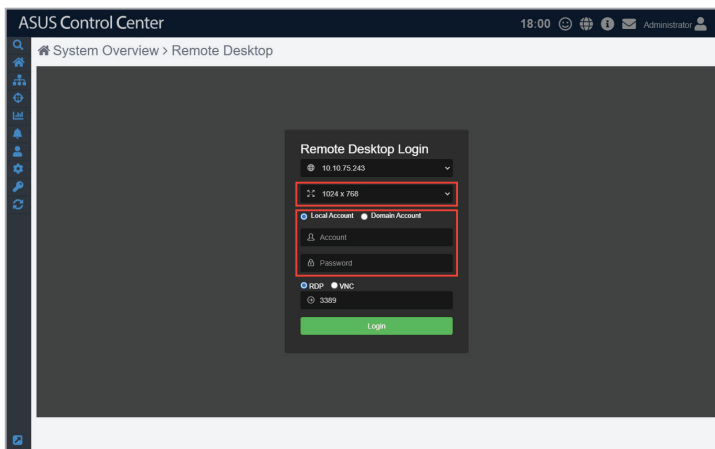
---

1. Select a VM from the **VM Information** block.
2. Click on the  icon located next to the VM you wish to view in the **VM Information** block, you should be directed to the **Remote Desktop Login** screen.
3. Select a resolution to display the managed device in the Remote Desktop window.
4. Select the login Account type, then enter the **Account**, **Password**, and **Domain** information.

---

### NOTE:

- **Local Account:** The agent's administrator privileges only allow you to manage the device the agent is installed on.
  - **Domain Account:** The agent's administrator privileges allow you to manage all devices in the domain. The **Domain** field only appears if you selected **Domain Account**.
- 



5. Select the protocol to use when connecting, then click **Login**.

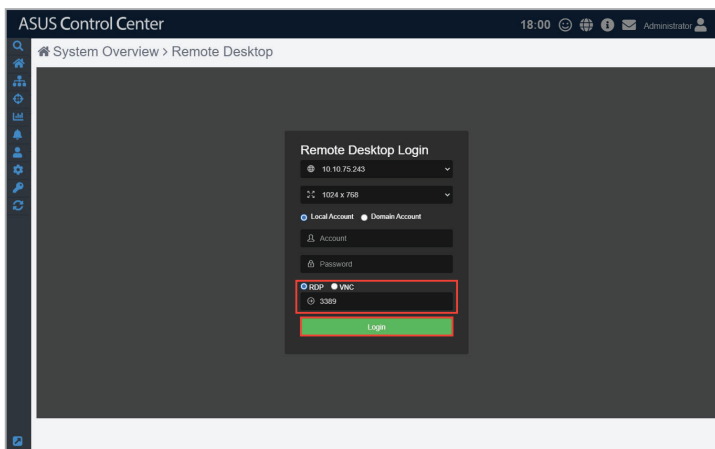
---

**NOTE:**

- Linux and Windows® systems use different protocols, ensure the managed device is reachable through the selected protocol:
    - **RDP**: Available on Windows only; allows only a single user to view and configure at the same time.
    - **VNC**: Available on both Windows and Linux; allows multiple users to view and configure at the same time.
    - **SSH**: Available on Linux only.
- 

**IMPORTANT:**

- Ensure the managed device you wish to remote control has a stable power supply and Internet connection.
  - The managed device may be remote controlled if it is logged out or locked, but cannot be remote controlled if the managed device is powered off or in sleep mode. If the managed device is in sleep mode, please wake the device using the **Power Control (Wake-on-LAN)** function.
  - (for RDP only) Please ensure that the following two items are checked on the remote device and enabled to allow remote connections to the remote device. Search for **Control Panel** in the Windows Search Box, then navigate to **System > Remote settings**.
  - (for RDP only) Please ensure that the **Microsoft Remote Desktop** application is enabled in the **Windows Defender Firewall Allowed Apps** list. Search for **Control Panel** in the Windows Search Box, then navigate to **Windows Defender Firewall > Allowed Apps**.
- 



6. Once the login has been successfully authenticated, you will be logged into the desktop or command line of the device system; this varies between systems.

---

**NOTE:** To switch mouse and keyboard control to the ASUS Control Center, press <Ctrl> + <Alt> on the keyboard. To switch mouse and keyboard control back to the remote device, click in the remote device window.

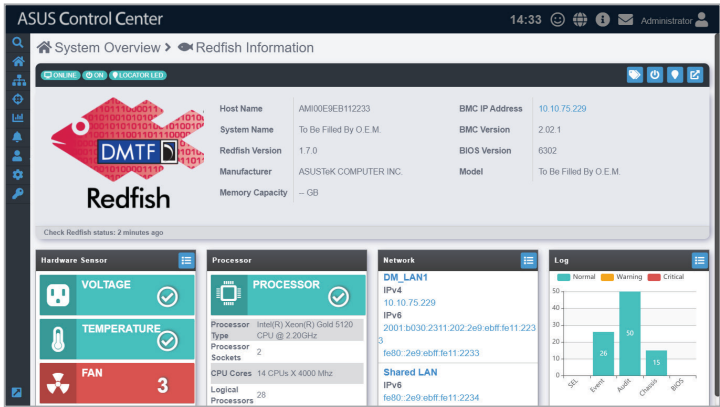
---

7. Click on the Menu Path at the top of the screen, or click on another menu item from the left menu to end the remote session.

## 2.7 Redfish Information

The **Redfish Information** screen gives you various functions to view detailed information and manage the selected Redfish device.

To access the **Redfish Information** of a managed device, click on the Redfish device you wish to view in the **Devices list**.



The **Redfish Information** screen will display the **Host Name**, **System Name**, **Redfish Version**, **Manufacturer**, **Memory Capacity**, **BMC IP Address**, **BMC Version**, **BIOS Version** and **Model** of the device. In the blocks located at the bottom of the screen, the **Processor** block also displays information on the processor of the Redfish device.

### Using the search bar and search options

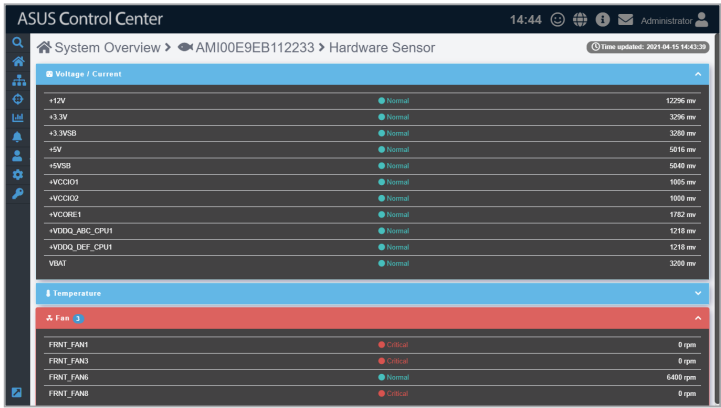
Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

Redfish device Statuses and Quick Buttons

|                                                                                   |                          |                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Connection status</b> | This item displays the connection status of the selected Redfish device.                                                                                                        |
|  | <b>Power Status</b>      | This item displays the power status of the selected Redfish device.                                                                                                             |
|  | <b>Locator status</b>    | This item will turn green if the locator LED is enabled through the ACC Web UI. The locator LED allows you quickly locate the physical location of the device in a server rack. |
|  | <b>Metadata Editor</b>   | This item allows you to edit the metadata of the Redfish device by double clicking in the <b>Value</b> field.                                                                   |
|  | <b>Power Control</b>     | This item allows you to power off or restart a Redfish device.                                                                                                                  |
|  | <b>Locator LED</b>       | This item allows you to turn on/off the Locator LED.                                                                                                                            |
|  | <b>BMC</b>               | This item will link to the BMC website.                                                                                                                                         |
|  | <b>Detail</b>            | This item will redirect you to the selected block's ( <b>Hardware Sensor, Network, Log</b> ) details screen.                                                                    |

## 2.7.1 Hardware Sensor

This item allows you to view the details and values for the Voltage/Current, Temperature, and Fan items.



### Quick Buttons

-  Click to expand this block.
-  Click to minimize this block.



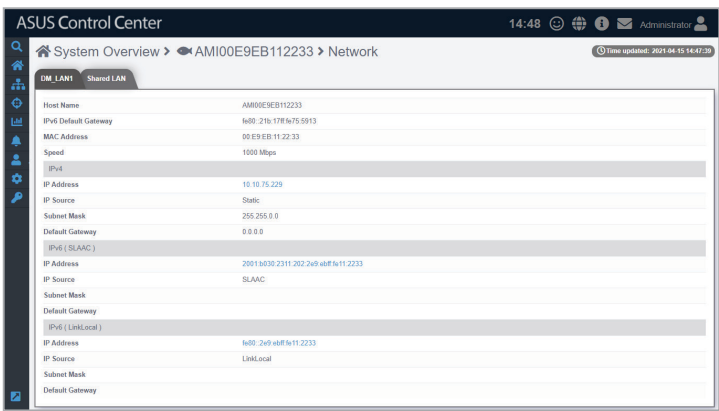
# 2.7.2 Network

This item displays the BMC network information of the Redfish device, you may also set the BMC using ASMB through the **DM\_LAN1** and **Shared LAN** tabs.

**NOTE:** The information entered in this section is for reference only.

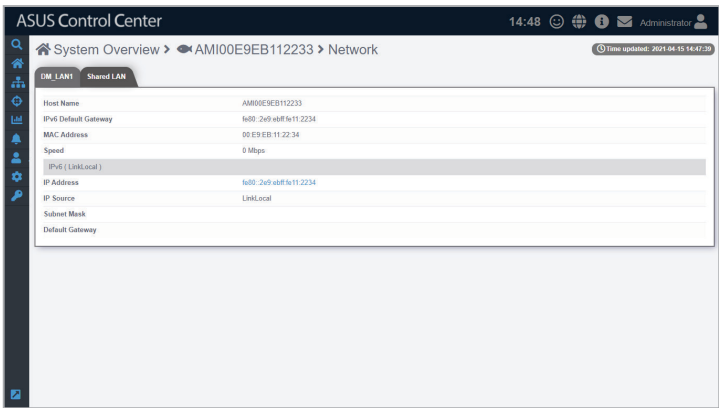
## DM\_LAN

This item is the communication port specifically for BMC, clicking on the BMC IP in the **IP Address** field for **IPv4**, **IPv6 (SLAAC)**, or **IPv6 (LinkLocal)** will redirect you to the ASMB page, allowing you to view the hardware sensor values of the device.



## Shared LAN

This item is the communication port for BMC and OS, clicking on the BMC IP in the **IP Address** field of **IPv6 (LinkLocal)** will redirect you to the ASMB page, allowing you to view the hardware sensor values of the device.



## Edit BMC using ASMB

To edit BMC settings using ASMB on the device:

1. Select **DM\_LAN1** or **Shared LAN**, then click on any of the IP Addresses.

| DM_LAN1                                | Shared LAN |
|----------------------------------------|------------|
| Host Name                              |            |
| AM000EB112233                          |            |
| IPv4 Default Gateway                   |            |
| fe80::21b:178:675:5913                 |            |
| MAC Address                            |            |
| 00:E9:EB:11:22:33                      |            |
| Speed                                  |            |
| 1000 Mbps                              |            |
| IPv4                                   |            |
| IP Address                             |            |
| 10.10.75.229                           |            |
| IP Source                              |            |
| Static                                 |            |
| Subnet Mask                            |            |
| 255.255.0.0                            |            |
| Default Gateway                        |            |
| 0.0.0.0                                |            |
| IPv6 (SLAAC)                           |            |
| IP Address                             |            |
| 2001:b030:2311:202::2ef:feff:fe11:2233 |            |
| IP Source                              |            |
| SLAAC                                  |            |
| Subnet Mask                            |            |
|                                        |            |
| Default Gateway                        |            |
|                                        |            |
| IPv6 (LinkLocal)                       |            |
| IP Address                             |            |
| fe80::2ef:feff:fe11:2233               |            |
| IP Source                              |            |
| LinkLocal                              |            |
| Subnet Mask                            |            |
|                                        |            |
| Default Gateway                        |            |
|                                        |            |

2. Log into ASMB.

ASMB9-IRVM

Username

Password

en - English

☐ Remember Username

Log in

[Forgot my password](#)

## 2.7.3 Event Log

This item displays the logs for the Redfish device's **SEL**, **Event**, **Audit**, **Chassis**, and **BIOS**. You may view each event log by clicking on the tabs. Click on an event to view more details about the event.

**NOTE:** To export the Event Log click the **Export** button, enter a filename, then click **OK**.

### SEL tab

ASUS Control Center

14:55

Administrator

System Overview > AMI00E9EB112233 > Log

Time updated: 2021-04-15 14:54:29

SEL

Event

Audit

Chassis

BIOS

Normal

0

Warning

0

Critical

0

Logs

Press 'Enter' key to search.

Clear

Export

Options

| Level Type | Event Time Stamp | Name | Entry Code | Sensor Number | Sensor Type | Message |
|------------|------------------|------|------------|---------------|-------------|---------|
|------------|------------------|------|------------|---------------|-------------|---------|

### Event tab

ASUS Control Center

14:55

Administrator

System Overview > AMI00E9EB112233 > Log

Time updated: 2021-04-15 14:54:29

SEL

Event

Audit

Chassis

BIOS

Normal

26

Warning

0

Critical

0

Logs

Press 'Enter' key to search.

Clear

Export

Options

| Level Type | Event Time Stamp    | Name         | Entry Code    | Sensor Number | Sensor Type | Message                                                          |
|------------|---------------------|--------------|---------------|---------------|-------------|------------------------------------------------------------------|
| Normal     | 2022-02-14 08:12:25 | Log entry 1  | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-02-14 08:12:43 | Log entry 2  | Informational |               |             | The value of attribute BoolComplete at redfish/v1/Security 1.0 R |
| Normal     | 2022-02-16 08:28:35 | Log entry 3  | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-02-28 08:49:41 | Log entry 4  | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-02-28 08:49:57 | Log entry 5  | Informational |               |             | The value of attribute BoolComplete at redfish/v1/Security 1.0 R |
| Normal     | 2022-02-28 09:01:09 | Log entry 6  | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-02-28 09:01:25 | Log entry 7  | Informational |               |             | The value of attribute BoolComplete at redfish/v1/Security 1.0 R |
| Normal     | 2022-02-28 09:02:56 | Log entry 8  | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-02-28 09:10:53 | Log entry 9  | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-02-28 09:14:54 | Log entry 10 | Informational |               |             | The value of attribute BoolComplete at redfish/v1/Security 1.0 R |
| Normal     | 2022-02-28 09:16:20 | Log entry 11 | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-03-01 10:22:22 | Log entry 12 | Informational |               |             | The value of attribute Attributes at redfish/v1/Security 1.0 R   |
| Normal     | 2022-03-01 10:22:40 | Log entry 13 | Informational |               |             | The value of attribute BoolComplete at redfish/v1/Security 1.0 R |

Audit tab

ASUS Control Center14:55Administrator

System Overview > AMI00E9EB112233 > Log

SEL | Event | Audit | Chassis | BIOS

Normal50

Warning0

Critical0

Logs (50)

Press 'Enter' key to search. X ClearExportOptions

| Level Type | Event Time Stamp    | Name                | Entry Code | Sensor Number | Sensor Type | Message                                                       |
|------------|---------------------|---------------------|------------|---------------|-------------|---------------------------------------------------------------|
| Normal     | 2021-03-31 17:16:16 | Audit Log Entry 141 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:16 | Audit Log Entry 142 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:30 | Audit Log Entry 143 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:31 | Audit Log Entry 144 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:32 | Audit Log Entry 145 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:33 | Audit Log Entry 146 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:34 | Audit Log Entry 147 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:41 | Audit Log Entry 148 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-03-31 17:16:41 | Audit Log Entry 149 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 R |
| Normal     | 2000-01-01 08:01:36 | Audit Log Entry 150 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2000-01-01 08:01:40 | Audit Log Entry 151 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-04-01 18:18:36 | Audit Log Entry 152 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |
| Normal     | 2021-04-01 18:18:41 | Audit Log Entry 153 |            |               |             | User in-band user, IP: 169.254.0.18, Protocol: Security 1.0 A |

Chassis tab

ASUS Control Center14:55Administrator

System Overview > AMI00E9EB112233 > Log

SEL | Event | Audit | Chassis | BIOS

Normal15

Warning0

Critical0

Logs (15)

Press 'Enter' key to search. X ClearExportOptions

| Level Type | Event Time Stamp    | Name    | Entry Code                      | Sensor Number | Sensor Type  | Message  |
|------------|---------------------|---------|---------------------------------|---------------|--------------|----------|
| Normal     | 2012-01-06 21:11:43 | Logs 1  | Lower Critical - going low      | 169           | Fan          | 0x20006  |
| Normal     | 2012-01-06 21:11:43 | Logs 2  | Lower Non-critical - going low  | 169           | Fan          | 0x20006  |
| Normal     | 2012-01-06 21:11:56 | Logs 3  | Assert                          | 148           | Power Supply | 0x03FFFF |
| Normal     | 2021-04-07 10:15:20 | Logs 4  | Assert                          | 151           | Power Supply | 0x01FFFF |
| Normal     | 2021-04-07 10:15:26 | Logs 5  | Deassert                        | 148           | Power Supply | 0x03FFFF |
| Normal     | 2021-04-07 10:15:26 | Logs 6  | Lower Critical - going low      | 225           | Power Supply | 0x20000  |
| Normal     | 2021-04-07 10:15:26 | Logs 7  | Lower Non-critical - going low  | 225           | Power Supply | 0x20000  |
| Normal     | 2021-04-07 10:15:26 | Logs 8  | Upper Non-critical - going high | 225           | Power Supply | 0x577D7D |
| Normal     | 2021-04-07 10:15:26 | Logs 9  | Upper Critical - going high     | 225           | Power Supply | 0x96A8A  |
| Normal     | 2021-04-07 10:15:29 | Logs 10 | Assert                          | 151           | Power Supply | 0x03FFFF |
| Normal     | 2021-04-07 10:15:31 | Logs 11 | Assert                          | 148           | Power Supply | 0x03FFFF |
| Normal     | 2021-04-07 10:15:36 | Logs 12 | Upper Critical - going high     | 225           | Power Supply | 0x96A8A  |
| Normal     | 2021-04-07 10:15:36 | Logs 13 | Upper Non-critical - going high | 225           | Power Supply | 0x577D7D |

BIOS tab

ASUS Control Center

14:55

Administrator

System Overview > AMI00E9EB112233 > Log

Time updated: 2021-04-15 14:50:09

SEL

Event

Audit

Chassis

BIOS

Normal

0

Warning

0

Critical

0

Logs

Press 'Enter' key to search... 

Clear

Export

Options

| Level Type | Event Time Stamp | Name | Entry Code | Sensor Number | Sensor Type | Message |
|------------|------------------|------|------------|---------------|-------------|---------|
|------------|------------------|------|------------|---------------|-------------|---------|



# Chapter 3

This chapter describes how to deploy ASUS Control Center agents and remove agents through Microsoft® Active Directory or manually. You may also add and manage agentless vSphere.

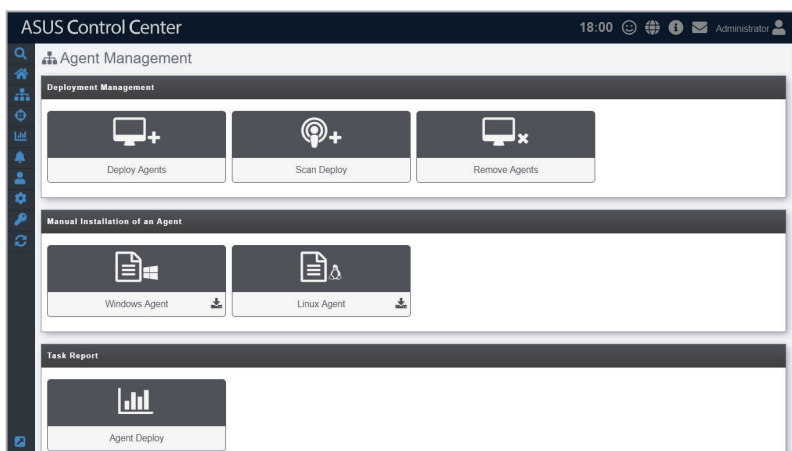
# Deployment

## 3.1 Agent Management

The **Agent Management** screen allows you to manage agent deployment, removal or view the Agent Deploy Report. You can automatically or manually deploy and install new ASUS Control Center agents on devices and add them to the ASUS Control Center server for convenient management, monitor and control.

Refer to the **Appendix** for more details on the ASUS Control Center agent system requirements.

To access **Agent Management**, click  > **Agent Management** in the left menu.



### Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.



## 3.1.1 Deploy Agents

The **Deploy Agents** function allows you to add devices you wish to deploy agents to. You can enter a single device, or multiple devices to be scanned, and then deploy agents to the scanned devices.

The screenshot displays the ASUS Control Center interface, specifically the Agent Management > Deploy Agents section. The top navigation bar shows the time as 18:00 and the user as Administrator. The main content area is divided into two sections: Deployment Management and Scan Result Information.

**Deployment Management**

| OS Type | Host Type | IP Address/Host Name | Account | Account       | Password | Main Server  | Port |
|---------|-----------|----------------------|---------|---------------|----------|--------------|------|
| Windows | IP        | 10.10.75.125         | local   | Administrator | ****     | 10.10.75.123 | 8080 |
| Linux   | IP        | 10.10.75.103         | local   | root          | ****     | 10.10.75.123 | 8080 |

Buttons: Import, Export, Add

Search: Scan

**Scan Result Information** (License count: 51)

| OS Type     | IP Address/Host Name | Scan Results | Message                                                                               |
|-------------|----------------------|--------------|---------------------------------------------------------------------------------------|
| Support (2) |                      |              |                                                                                       |
| Windows     | 10.10.75.125         | Support      | OK                                                                                    |
| Linux       | 10.10.75.103         | Support      | Scan Successful, Please check your "BMC" is installed, it cannot monitor hardware ... |

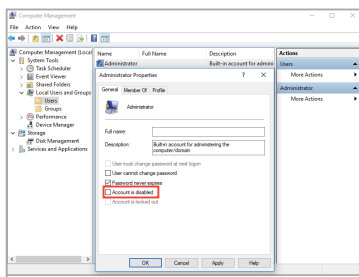
Buttons: Deploy All

## Agent deployment conditions and settings

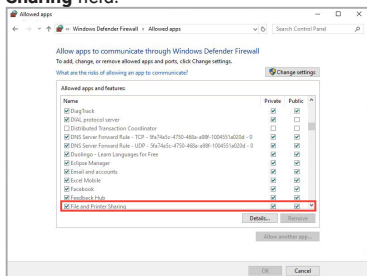
You may encounter problems when deploying agents to managed devices, if you do, you can first do a check and see if any of the following settings will resolve the problem.

**NOTE:** The examples used in this section are all based on Windows® 10.

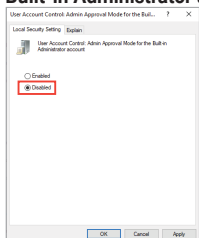
- Ensure the device has sufficient power and a steady connection to prevent packet loss when deploying the agent.
- For Windows clients
  - Windows® Home or lower versions of Windows® are not supported by ASUS Control Center.
  - The Administrator account of the client is enabled and has a password set. (Windows disables the Administrator account by default, to enable the account search for **Computer Management** in the Windows Search Box, then navigating to **System Tools > Local Users and Groups > Users > Administrator**, right click and select **Properties**, then uncheck the **Account is disabled** field, and click **OK**)



- **Private** and **Public** should be checked in the **File and Printer Sharing** option by searching for **Control Panel** in the Windows Search Box, then navigating to **System and Security > Windows Firewall > Allow an app or feature through Windows Firewall**, then checking both **Private** and **Public** checkboxes in the **File and Printer Sharing** field.



- **User Account Control: Admin Approval Mode for the Built-in Administrator account** should be disabled. To disable this option, search for **Local Security Policy** in the Windows Search Box, then navigate to **Local Policies > Security Options**, then double click on **User Account Control: Admin Approval Mode for the Built-in Administrator account** and set it to **Disabled**, then click **OK**.



- For Debian and Ubuntu clients

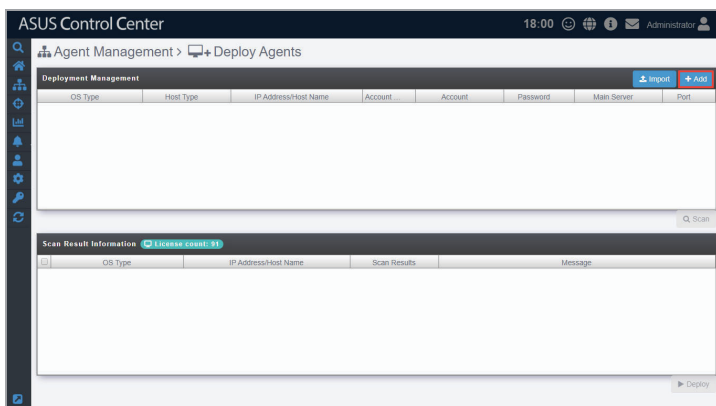
- **Enable SSH:**
  - Ensure the root account can be logged in through SSH.
  - Install SSH by executing the following:  
`sudo apt-get install ssh`
  - Confirm SSH server by executing the following:  
`systemctl start sshd`  
`systemctl status sshd`

- For RHEL, CentOS, and Scientific Linux clients

- **Enable SSH** (enabled by default for RHEL and CentOS):
  - Ensure the root account can be logged in through SSH.
  - Install SSH by executing the following:  
`sudo apt-get install ssh`
  - Confirm SSH server by executing the following:  
`systemctl start sshd`  
`systemctl status sshd`
- **Disable SELinux:**
  - Open `/etc/sysconfig/selinux`.
  - Set **SELINUX=enforcing** to **SELINUX=disabled**.
  - Reboot the system.

## Adding managed devices

1. Click on **Add**.



2. The IP and port of the main server should already be filled in, if not please enter the IP address and Port of the main ACC server.

The screenshot shows the 'Add Target Host' dialog box. It has a green header with the title 'Add Target Host' and a close button. The form contains the following fields:

- Main Server**: 10.10.75.123
- Port**: 8080
- OS Type**: Windows (selected), Linux, ADM
- Host Type**: IP Address (selected), Host Name
- IP Address**: 10.10.75.125
- Account Type**: Local Account (selected), Domain Account
- Account**: Administrator
- Password**: [Redacted]

At the bottom right, there are 'Cancel' and 'Save' buttons.

3. Select the **OS Type** of the device you wish to add from the **OS Type** options, then select the **Host Type**.

**NOTE:**

- **IP Address:** Enter the IP address of the device.
- **Host Name:** Enter the name of the device.

**Selecting Windows® system:**

The screenshot shows the 'Add Target Host' dialog box with a green header. The 'Main Server' field contains '10.10.75.123' and the 'Port' field contains '8080'. The 'OS Type' section has three buttons: 'Windows' (highlighted with a red box), 'Linux', and 'ADM'. The 'Host Type' section has two radio buttons: 'IP Address' (selected) and 'Host Name'. Below this, the IP address '10.10.75.125' is entered. The 'Account Type' section has two radio buttons: 'Local Account' (selected) and 'Domain Account'. The 'Account' field contains 'Administrator' and the 'Password' field contains '\*\*\*\*\*'. At the bottom right are 'Cancel' and 'Save' buttons.

**Selecting Linux system:**

The screenshot shows the 'Add Target Host' dialog box with a green header. The 'Main Server' field contains '10.10.75.123' and the 'Port' field contains '8080'. The 'OS Type' section has three buttons: 'Windows', 'Linux' (highlighted with a red box), and 'ADM'. The 'Host Type' section has two radio buttons: 'IP Address' (selected) and 'Host Name'. Below this, the IP address '10.10.75.103' is entered. The 'Account' field contains 'root' and the 'Password' field contains '\*\*\*\*\*'. At the bottom right are 'Cancel' and 'Save' buttons.

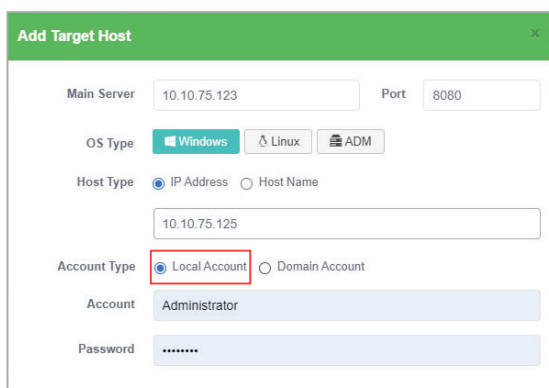
#### 4. Select the **Account Type**.

##### NOTE:

- **Local Account:** The agent's administrator (Windows) / root (Linux) privileges only allow you to manage the device the agent is installed on.
- **Domain Account (Windows only):** The agent's administrator privileges allows you to manage all devices in the domain.

**IMPORTANT:** When selecting **Local Account** as the **Account type**, and **Windows** as the **OS Type** for a device, ensure to configure your managed device settings as shown in **Agent deployment conditions and settings**.

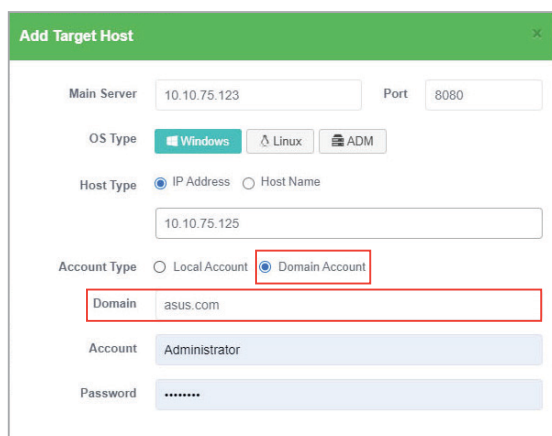
##### Selecting Local Account:



The screenshot shows the 'Add Target Host' dialog box with the following configuration:

- Main Server:** 10.10.75.123
- Port:** 8080
- OS Type:** Windows (selected), Linux, ADM
- Host Type:** IP Address (selected), Host Name
- Host Name:** 10.10.75.125
- Account Type:** Local Account (selected and highlighted with a red box), Domain Account
- Account:** Administrator
- Password:** (masked with dots)

##### Selecting Domain Account:



The screenshot shows the 'Add Target Host' dialog box with the following configuration:

- Main Server:** 10.10.75.123
- Port:** 8080
- OS Type:** Windows, Linux, ADM
- Host Type:** IP Address (selected), Host Name
- Host Name:** 10.10.75.125
- Account Type:** Local Account, Domain Account (selected and highlighted with a red box)
- Domain:** asus.com (highlighted with a red box)
- Account:** Administrator
- Password:** (masked with dots)

5. Enter the **Account** and **Password** for the administrator account or root account of the device, then click on **Save**.

**Add Target Host**

Main Server: 10.10.75.123 Port: 8080

OS Type: Windows Linux ADM

Host Type: ☒ IP Address ☐ Host Name

10.10.75.125

Account Type: ☒ Local Account ☐ Domain Account

Account: Administrator

Password: \*\*\*\*\*

Cancel Save

6. Repeat steps 1 to 5 to add additional devices to be scanned, or refer to the **To add multiple devices** section to import a list of devices.
7. Once you have added all the devices to scan for, click on **Scan**.

ASUS Control Center 18:00

Agent Management > Deploy Agents

Deployment Management

| OS Type | Host Type | IP Address/Host Name | Account | Account       | Password | Main Server  | Port |
|---------|-----------|----------------------|---------|---------------|----------|--------------|------|
| Windows | IP        | 10.10.75.123         | local   | Administrator | *****    | 10.10.75.123 | 8080 |
| Linux   | IP        | 10.10.75.100         | local   | root          | *****    | 10.10.75.123 | 8080 |

Import Export Add

Scan

Scan Result Information (Success count: 0)

| OS Type | IP Address/Host Name | Scan Results | Message |
|---------|----------------------|--------------|---------|
|---------|----------------------|--------------|---------|

Deploy

8. The scanned results will be displayed in the **Scan Result Information** block. Select the devices you wish to deploy agent then click **Deploy**.

**NOTE:** Unavailable devices will be listed as **Not Support**. You may click on the device to view details on why it is unavailable.

ASUS Control Center

18:00

Administrator

Agent Management > Deploy Agents

Deployment Management

| OS Type | Host Type | IP Address/Host Name | Account | Account       | Password | Main Server  | Port |
|---------|-----------|----------------------|---------|---------------|----------|--------------|------|
| Windows | IP        | 10.10.75.125         | local   | Administrator | ****     | 10.10.75.123 | 8080 |
| Linux   | IP        | 10.10.75.103         | local   | root          | ****     | 10.10.75.123 | 8080 |

Scan Result Information

Success count: 1/1

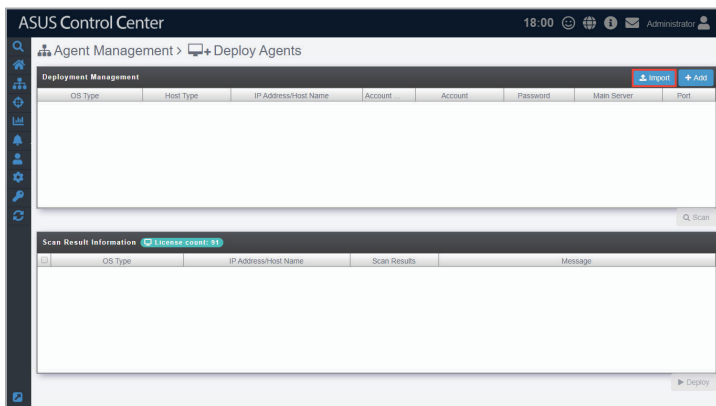
| OS Type     | IP Address/Host Name | Scan Results | Message                                                                            |
|-------------|----------------------|--------------|------------------------------------------------------------------------------------|
| Support (2) |                      |              |                                                                                    |
| Windows     | 10.10.75.125         | Support      | OK                                                                                 |
| Linux       | 10.10.75.103         | Support      | Scan Successful, Please check your "lvmc" is installed, it cannot monitor hardware |

Deploy AG

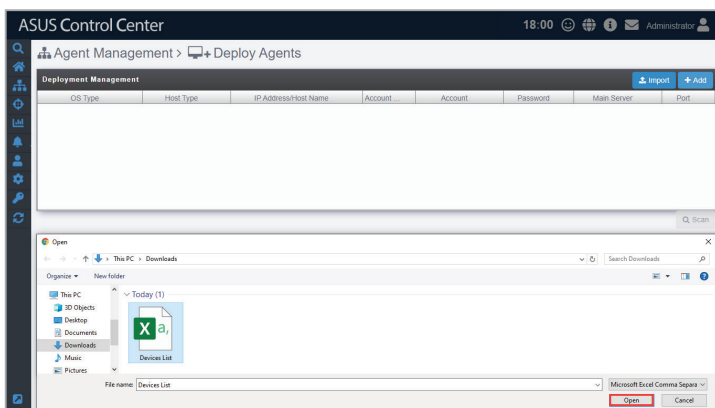


## Adding devices from CSV file

1. Click on **Import**.

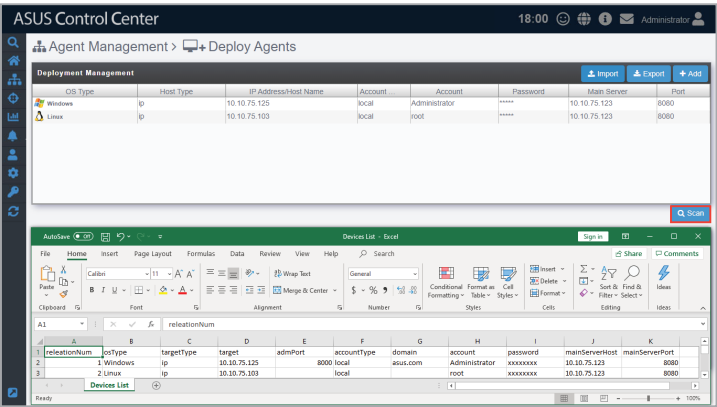


2. Select the CSV file to import and click **Open**.



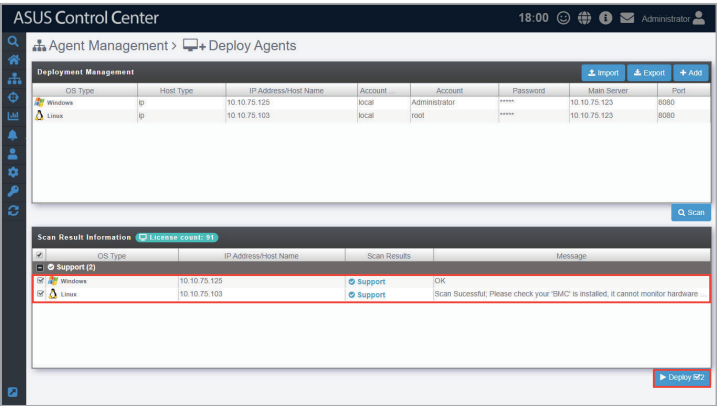
3. Once the CSV file is successfully imported, click on **Scan**.

**NOTE:** You may edit items added by clicking on it before scanning.



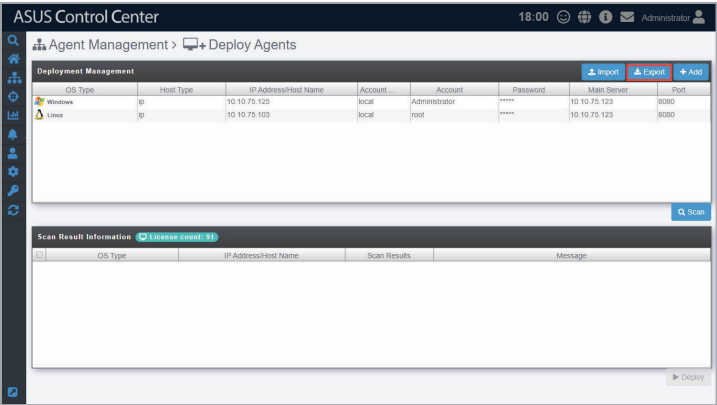
4. The scanned results will be displayed in the **Scan Result Information** block. Select the devices you wish to deploy agent then click **Deploy**.

**NOTE:** Unavailable devices will be listed as **Not Support**. You may click on the device to view details on why it is unavailable.



## Exporting Deployment Management list

You can export the list of devices added to the **Deployment Management** list to a CSV file by clicking on **Export**. You can edit the exported CSV file using a text editor.



## 3.1.2 Scan and Deploy

The **Scan and Deploy** function allows you to scan an IP range and display the managed devices which meet your set requirements for agent deployment, these requirements may vary from operating system to and connection status.

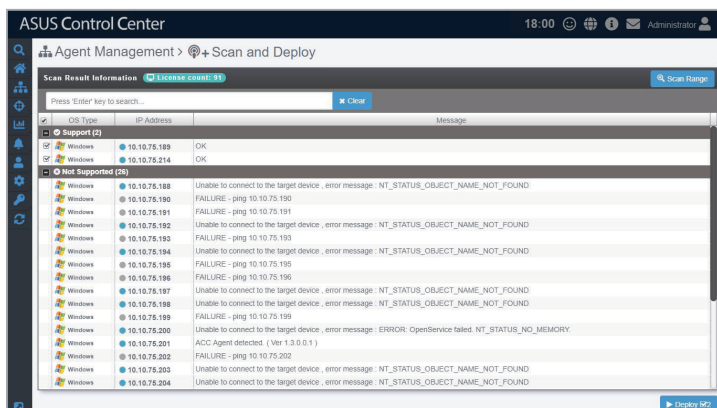
The scanned results also show which devices you can deploy new agents to and the devices you cannot deploy too as well as the reason these devices cannot be deployed to.

This makes it easy for you to quickly filter out all managed devices you wish to deploy agents to and then deploy agents to selected devices, saving you the time taken to manually deploy agents to each managed device individually.

---

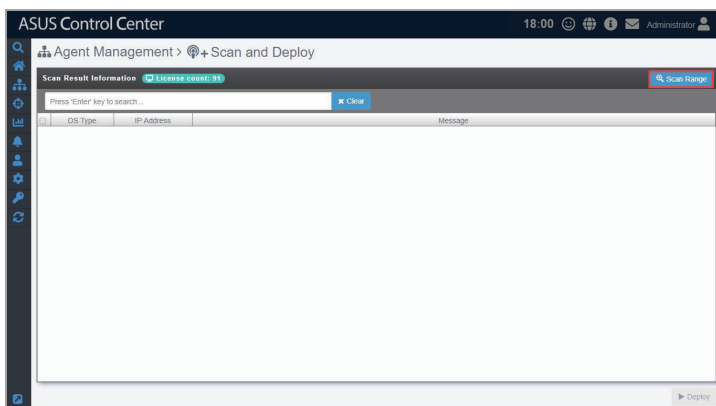
**IMPORTANT:** Before using the **Scan and Deploy** function, ensure that the agent deployment conditions and settings are met, for more information please refer to **Agent deployment conditions and settings** in the **Deploy Agents** section.

---



## Scanning for managed devices and deploying agents

1. Click on **Scan Range** to bring up the scan range pop-up window.



2. Enter the Main Server address, port number, the IP range you wish to scan, and the managed device OS type you would like to scan.

The screenshot shows the 'Scan Range' pop-up window. It has a blue header with the title 'Scan Range' and a close button. The form contains the following fields: 'Main Server' (10.10.75.200), 'Port' (8080), 'Starting IP' (10.10.75.188), 'Ending IP' (10.10.75.215), 'OS Type' (Windows, Linux, ADM), 'Account Type' (Local Account, Domain Account), 'Account' (Administrator), 'Password' (masked with dots), and 'Timeout Interval' (10 seconds). A red box highlights the 'Main Server', 'Port', 'Starting IP', 'Ending IP', and 'OS Type' fields. At the bottom right, there are 'Cancel' and 'Scan' buttons.

3. Select the **Local Account** or **Domain Account** in the **Account Type** field, and enter an account and password that the ASUS Control Center will use to log onto the devices scanned.

---

**IMPORTANT:** The account and password entered should be for an account that has administrator or root privileges on managed devices. For more information on activating the administrator account on managed devices, please refer to **Agent deployment conditions and settings** under the **Deploy Agents** section.

---

The screenshot shows the 'Scan Range' configuration window. The 'Account Type' section is highlighted with a red box, showing 'Local Account' selected with a radio button. Below it, the 'Account' field is set to 'Administrator' and the 'Password' field is masked with dots. Other fields include 'Main Server' (10.10.75.200), 'Port' (8080), 'Starting IP' (10.10.75.188), 'Ending IP' (10.10.75.215), 'OS Type' (Windows, Linux, ADM), and 'Timeout Interval' (10 seconds).

Selecting **Domain Account** will also allow you to enter the domain name and import the domain information when agents are deployed to the selected scanned devices. This provides you with more control over your managed devices.

The screenshot shows the 'Scan Range' configuration window with 'Domain Account' selected. A red box highlights the 'Domain' field, which contains 'ssdtest.com'. The 'Account' field is 'Administrator' and the 'Password' field is masked. Other fields are identical to the previous screenshot: 'Main Server' (10.10.75.200), 'Port' (8080), 'Starting IP' (10.10.75.188), 'Ending IP' (10.10.75.215), 'OS Type' (Windows, Linux, ADM), and 'Timeout Interval' (10 seconds).

- Set the **Timeout Interval**, this will determine the duration of time the scanned devices should be scanned before returning the scan results. Then click on **Scan**.

**Scan Range**

Main Server: 10.10.75.200 Port: 8080

Starting IP: 10.10.75.188

Ending IP: 10.10.75.215

OS Type: ☒ Windows ☐ Linux ☐ ADM

Account Type: ☐ Local Account ☒ Domain Account

Domain: ssctest.com

Account: Administrator

Password: .....

Timeout Interval: - 10 + seconds

- The scan results will display which devices you can deploy agents to and also the devices which cannot be deployed as well as the reasons they cannot be deployed to, for more information on agent deployment conditions, please refer to the **Deploy Agents** section.

**ASUS Control Center** 18:00 Administrator

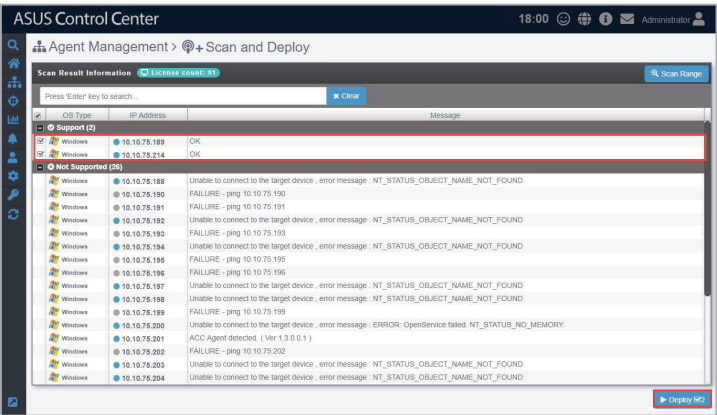
**Agent Management > Scan and Deploy**

**Scan Result Information** Success: 2/28 Scan Range

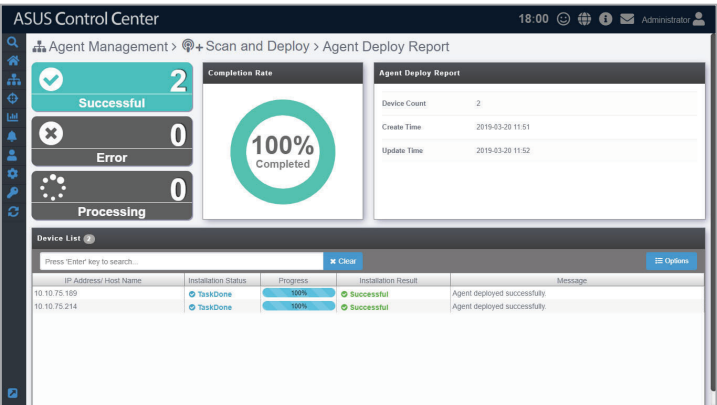
Press 'Enter' key to search...

| OS Type | IP Address   | Message                                                                                                 |
|---------|--------------|---------------------------------------------------------------------------------------------------------|
| Windows | 10.10.75.188 | OK                                                                                                      |
| Windows | 10.10.75.214 | OK                                                                                                      |
| Windows | 10.10.75.188 | Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND                |
| Windows | 10.10.75.190 | FAILURE - ping 10.10.75.190                                                                             |
| Windows | 10.10.75.191 | FAILURE - ping 10.10.75.191                                                                             |
| Windows | 10.10.75.192 | Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND                |
| Windows | 10.10.75.193 | FAILURE - ping 10.10.75.193                                                                             |
| Windows | 10.10.75.194 | Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND                |
| Windows | 10.10.75.195 | FAILURE - ping 10.10.75.195                                                                             |
| Windows | 10.10.75.196 | FAILURE - ping 10.10.75.196                                                                             |
| Windows | 10.10.75.197 | Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND                |
| Windows | 10.10.75.198 | Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND                |
| Windows | 10.10.75.199 | FAILURE - ping 10.10.75.199                                                                             |
| Windows | 10.10.75.200 | Unable to connect to the target device , error message : ERROR: OpenService failed. NT_STATUS_NO_MEMORY |
| Windows | 10.10.75.201 | ACC Agent detected. ( Ver 1.3.0.0.1 )                                                                   |
| Windows | 10.10.75.202 | FAILURE - ping 10.10.75.202                                                                             |
| Windows | 10.10.75.203 | Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND                |
| Windows | 10.10.75.204 | Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND                |

6. Check the scanned devices in the **Support** window you wish to deploy agents to and click on **Deploy**.



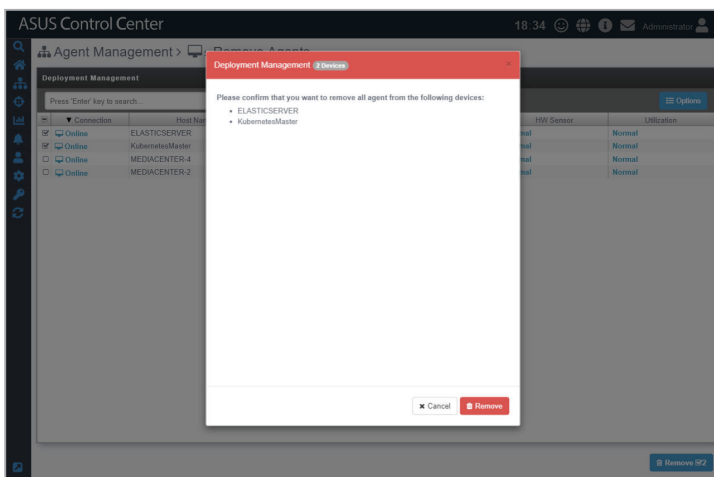
7. Once the agents deployment has finished, a **Agent Deploy Report** will appear, detailing the deploy status of each selected device. This will help you check if all agents have been successfully deployed.





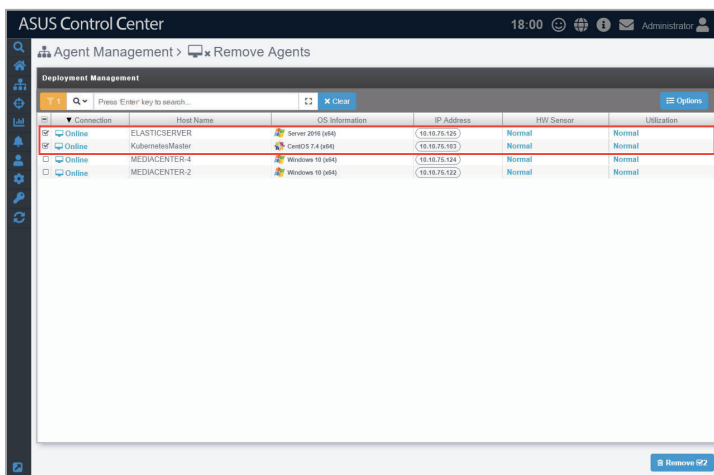
### 3.1.3 Remove agents

The **Remove Agents** function will allow you to remove agents installed on managed devices using ASUS Control Center, or allow you to remove the managed devices from ASUS Control Center after you remove the clients manually from the managed devices.



#### Remove agents using ASUS Control Center

1. Check the devices you wish to remove agents from on the list.

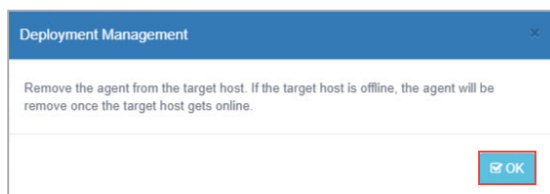
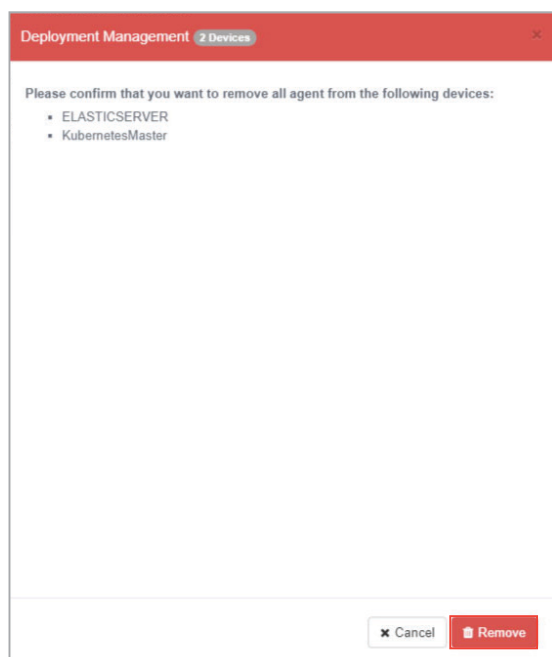


2. A pop-up window should appear, displaying the devices you wish to remove agents from. After confirming the correct managed devices are selected, click on **Remove**, then click on **OK**.

---

**NOTE:** If the target host(s) are offline, the agents on these host(s) will be removed once the host(s) are online.

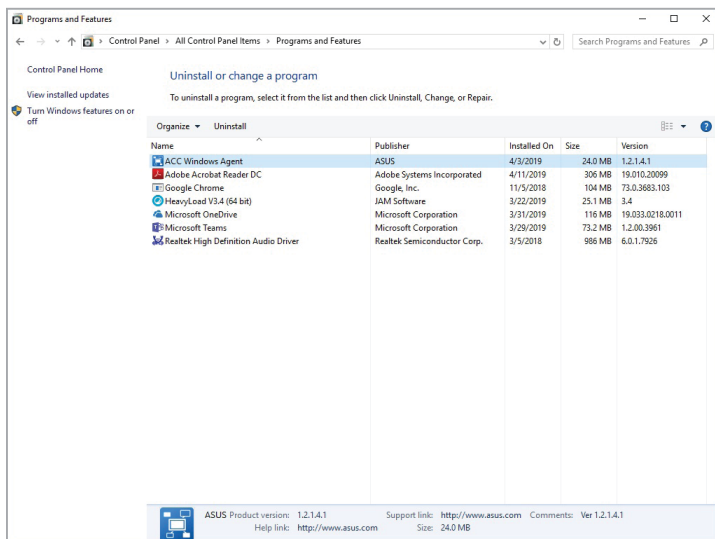
---



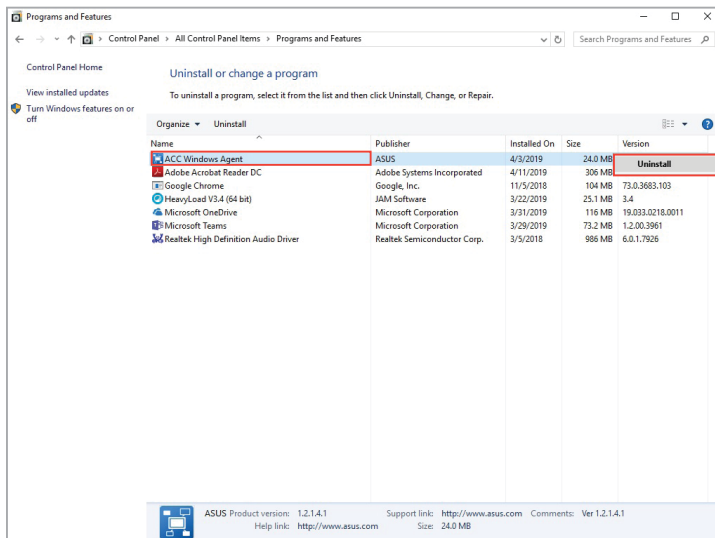
## Remove Windows Agent from local device

You may choose to remove Agents from Windows systems manually.

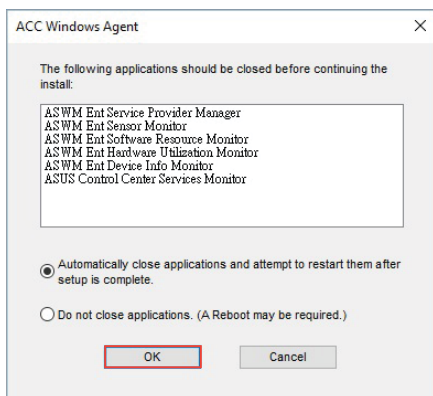
1. To remove the Windows Agent manually on a managed device, click on **Control Panel > Programs and Features**.



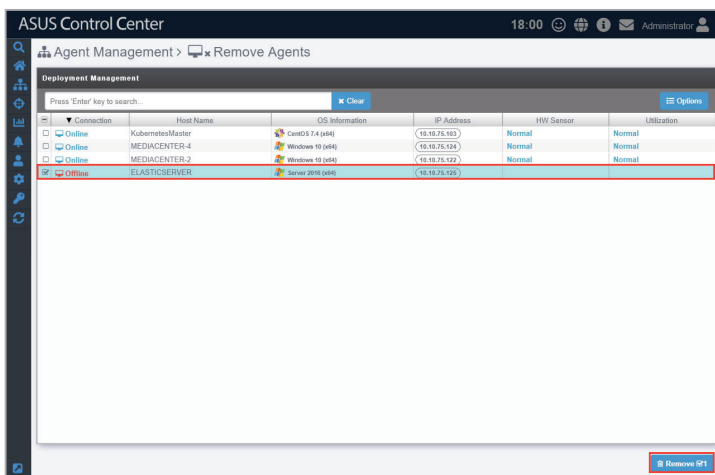
2. Select and uninstall **ACC Windows Agent** from the list of programs.



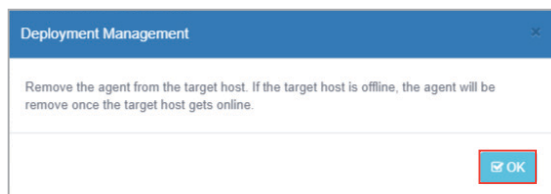
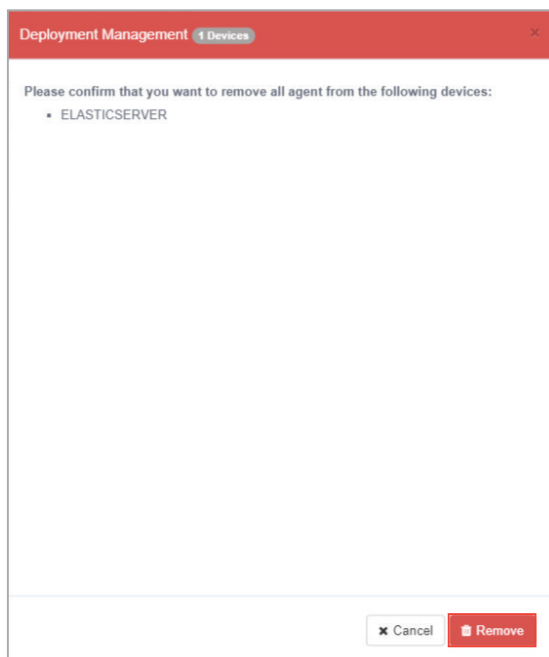
3. Ensure the applications shown in the pop-up window are closed, or you can check the **Automatically close applications and attempt to restart them after setup is complete** checkbox, then click **OK** to continue with the uninstallation process.



4. Once **ACC Windows Agent** is uninstalled on the managed device, please navigate to the **Remove Agents** menu of your ASUS Control Center (**Deployment > Agent Management > Remove Agents**).
5. Select the managed device which you manually removed the agent from, the connection status for that managed device should be **Offline**, then click on **Remove** to remove the managed device from ASUS Control Center.



6. A pop-up window should appear, displaying the managed devices you wish to remove agents from. After confirming the correct devices are selected, click on **Remove**, then click on **OK**.

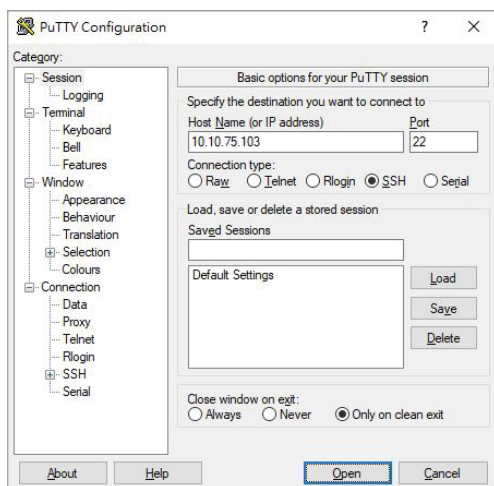


## Remove Linux Agent from local device

You may choose to remove Linux Agents from Linux systems manually.

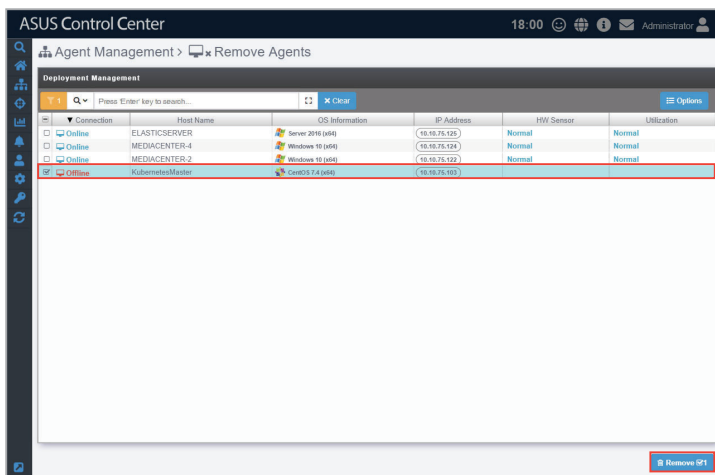
1. (optional) If you are using a Windows OS, you may use a third-party SSH or telnet client such as PuTTY to connect to the managed Linux device.

For this example we will be using PuTTY to log on to the managed Linux device and remove the Linux Agent.

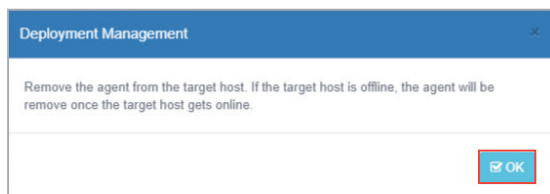
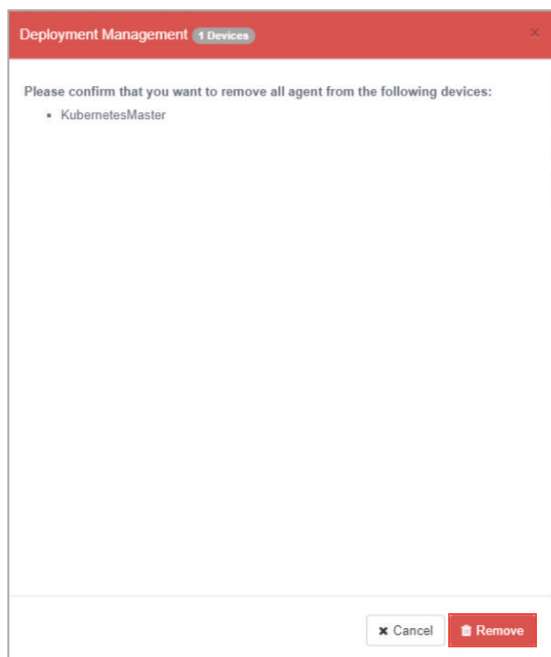


2. Enter the root account and password of the client Linux device.
3. Once you've logged in, execute `bash /root/uninstall.sh` to remove the Linux Agent from the managed device.
4. Once the Linux Agent is removed on the managed device, please navigate to the **Remove Agents** menu of your ASUS Control Center (**Deployment > Agent Management > Remove Agents**).

5. Select the managed device which you manually removed the agent from, the connection status for that managed device should be **Offline**, then click on **Remove** to remove the managed device from ASUS Control Center.



6. A pop-up window should appear, displaying the devices you wish to remove agents from. After confirming the correct devices are selected, click on **Remove**, then click on **OK**.





### 3.1.4 Windows Agent

You may install agents manually on the device by downloading the Windows Agent installation files from the ASUS Control Center web console.

---

**IMPORTANT:** CSM products only supports Windows Agents.

---

---

**NOTE:** The information entered in this section is for reference only.

---

#### Install Windows agents manually

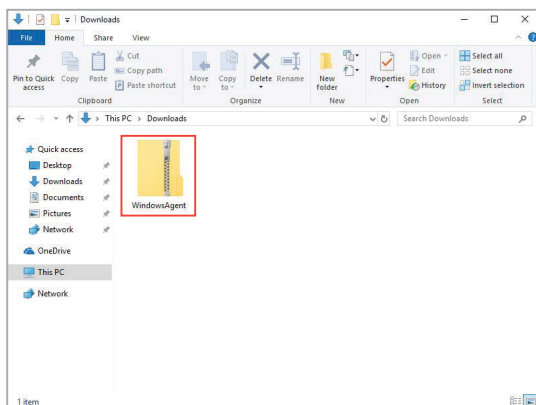
---

**IMPORTANT:**

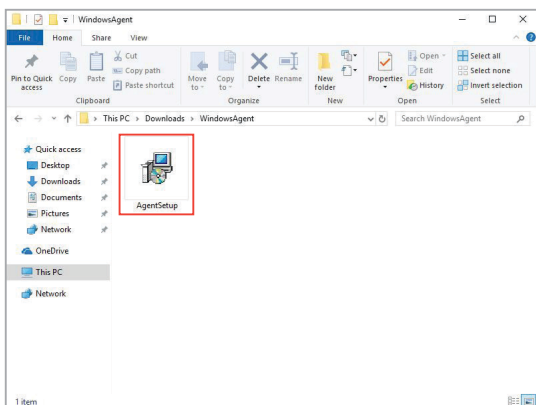
- When installing the Windows agent manually on devices with Windows 11 or Server 2022, two of the drivers - *AsUpIO.sys* (BIOS readings and flashing), and *ASUS Management Bus Driver* (Hardware Sensor reading) may be isolated by the Windows Core Isolation feature.
  - To successfully install a Windows Agent if you run into this situation you will need to set the **Memory integrity** option under **Core Isolation** to **Off**, to do so please navigate to **Start > Settings > Update & Security > Windows Security > Device Security** and then under **Core isolation**, select **Core isolation details** and set **Memory integrity** to **Off**.
- 

1. Log in remotely to the device you wish to install the Windows Agent on.
2. Download the Windows Agent installation files using the following methods.
  - Download installation files on ASUS Control Center
    - a. Click on **Windows Agent** to start downloading the installation files.
    - b. Copy the downloaded ZIP file to the remote desktop of the device.
  - Download installation files on managed device
    - a. Use the browser on the managed device to log into ASUS Control Center.
    - b. Click on **Windows Agent** to start downloading the installation files.

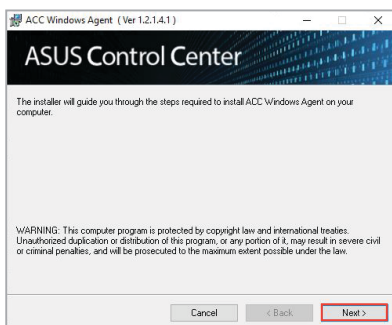
3. Unzip the ZIP file containing the installation files.



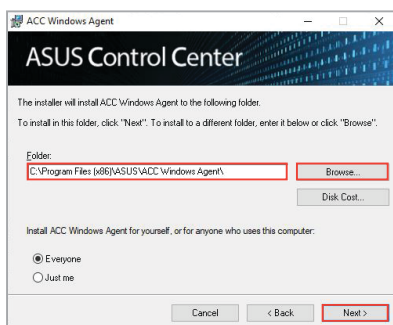
4. Click on the **AgentSetup.msi** file to launch the installation.



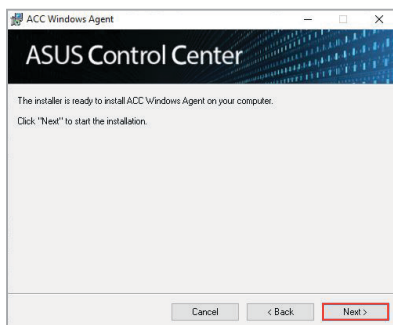
5. Click on **Next** to begin the installation.



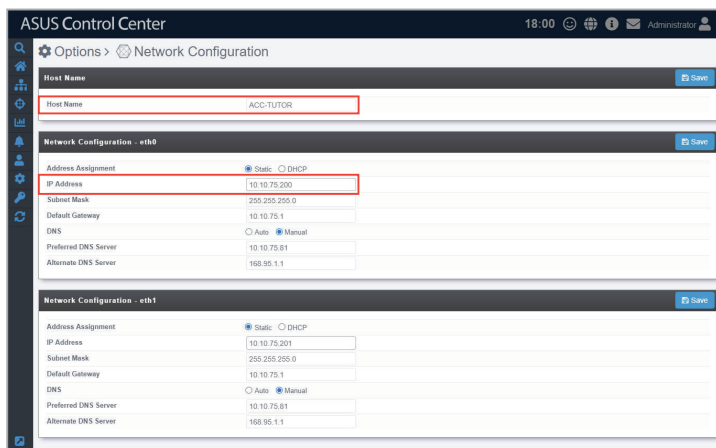
6. Browse and select a folder to install the agent, then click **Next**.



7. Click on **Next** again to continue the installation.



8. On ASUS Control Center, click  in the left menu, then click on **Network Configuration** to view the **Host Name** and **IP Address**.

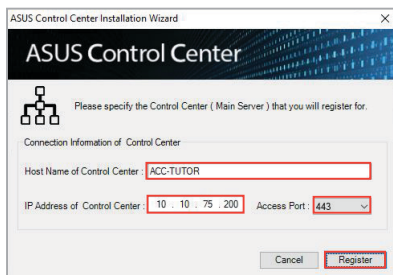


9. Enter the **Host Name** and **IP Address** from the previous step into the Windows® Agent Installer, select **443** as the **Access Port**, then click **Register**.

---

**NOTE:** The host name field supports Fully Qualified Domain Names (FQDN). The ASUS Control Center IP can be pinged via the host name during deployment.

---

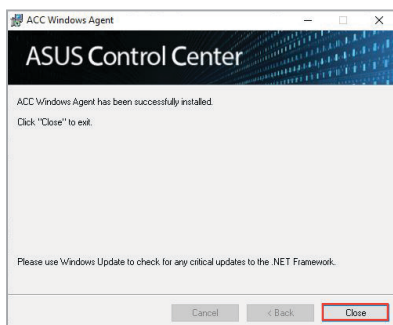


10. Wait for the installation to finish, then click **Close** to complete the installation. The device(s) should appear in the **Devices List** on the **System Overview** screen.

---

**NOTE:** The device's hardware performance and network speed will affect the time taken to deploy the agent.

---



### 3.1.5 Linux Agent

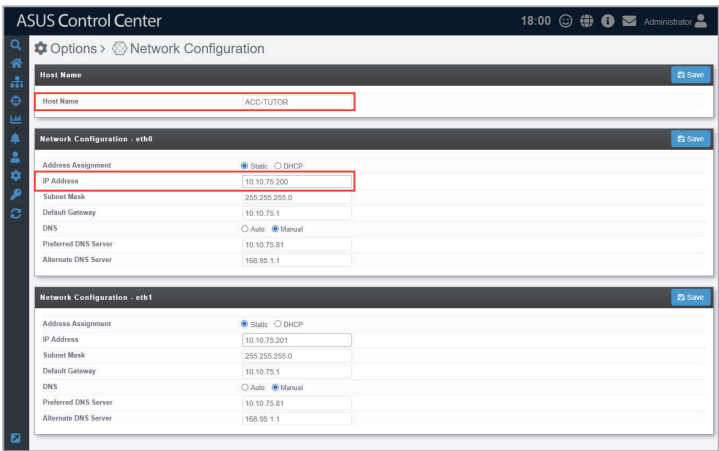
You may install agents manually on the device by downloading the Linux Agent installation files from the ASUS Control Center web console. The following 64-bits Linux distributions are supported: RHEL, CentOS, Scientific Linux, SLES, Ubuntu, Debian, and Pardus.

#### Install Linux agents manually

- Before installing the Linux agents manually, ensure that ssh is enabled, and the following software requirements are met:

|                                                               |               |                |          |
|---------------------------------------------------------------|---------------|----------------|----------|
| sysstat                                                       | smartmontools | ethtool        | curl     |
| ipmitool                                                      | OpenIPMI-libs | OpenIPMI-tools | pciutils |
| net-tools                                                     | ssh           |                |          |
| for RHEL 8~, CentOS 8~ : libnsl package installation required |               |                |          |
| for SLES 15~ : insserv-compat installation required           |               |                |          |

- Click on **Linux Agent** to download Linux Agent installation files.
- On ASUS Control Center, click  in the left menu, then click on **Network Configuration** to view the **Host Name** and **IP Address**.



- On your client device, create the folder `/tmp/ASWMAgentInstallFile`.
- Decompress the LinuxAgent.zip file, you should see a .tar file named **ASWMLinuxAgent-64bits.tar.gz**. Move the .tar file to `/tmp/ASWMAgentInstallFile` then decompress it.

6. Depending on your Linux distribution, execute the following to start the installation process:

- For RHEL, CentOS, Scientific Linux

Execute `/tmp/ASWMAgentInstallFile/Silentinstall_RHEL.sh XXXX.XXX.XXX.XXX`

- For SLES

Execute `/tmp/ASWMAgentInstallFile/Silentinstall_SLES.sh XXXX.XXX.XXX.XXX`

- For Ubuntu, Debian, Pardus

Execute `/tmp/ASWMAgentInstallFile/SilentInstall_Ubuntu.sh XXX.XXX.XXX.XXX`

---

**NOTE:** Please replace XXX.XXX.XXX.XXX with the actual IP of the ACC main server, for this example, it would be 10.10.75.200.

---

### 3.1.6 Agent Deploy Report

The Agent Deploy Report will display information of each time you deploy agent(s) onto managed devices. Each item showed on the **Agent Deploy Report** represents a single batch of deployment; clicking on each item will allow you to view information on the devices you deployed agents to in that batch.

ASUS Control Center

18:00

Administrator

Agent Management > Agent Deploy

Agent Deploy Report

Press the "Enter" key to search.

| Created Time     | Updated Time     | Client Count | Completion Rate | Success | Error | Process |
|------------------|------------------|--------------|-----------------|---------|-------|---------|
| 2019-04-15 (2)   |                  |              |                 |         |       |         |
| 2019-04-15 14:27 | 2019-04-25 16:52 | 1            | 100%            | 1       | 0     | 0       |
| 2019-04-15 11:48 | 2019-04-25 16:52 | 1            | 100%            | 1       | 0     | 0       |
| 2019-04-15 10:52 | 2019-04-25 16:52 | 1            | 100%            | 1       | 0     | 0       |
| 2019-04-03 (1)   |                  |              |                 |         |       |         |
| 2019-04-03 15:28 | 2019-04-25 17:27 | 2            | 100%            | 2       | 0     | 0       |
| 2019-03-20 11:51 | 2019-04-25 17:27 | 2            | 100%            | 2       | 0     | 0       |

ASUS Control Center

18:00

Administrator

Agent Management > Agent Deploy > Agent Deploy Report

Successful 2

Error 0

Processing 0

Completion Rate

100% Completed

Agent Deploy Report

Device Count 2

Create Time 2019-04-03 15:28

Update Time 2019-04-25 17:10

Device List

Press "Enter" key to search.

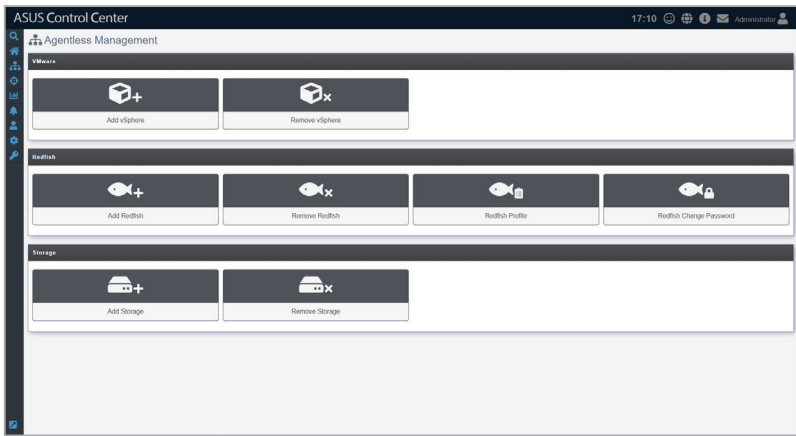
| IP Address/ Host Name | Installation Status | Progress | Installation Result | Message                                                                       |
|-----------------------|---------------------|----------|---------------------|-------------------------------------------------------------------------------|
| 10.10.75.103          | TaskDone            | 100%     | Successful          | Deployment Successful. Please check your "SMC" is installed. It cannot mon... |
| 10.10.75.125          | TaskDone            | 100%     | Successful          | Agent deployed successfully.                                                  |

Options

## 3.2 Agentless Management

The **Agentless Management** screen allows you to add vSphere or Redfish for monitoring and other management options. When adding the vSphere, the device added is the hypervisor. All VM on the hypervisor will be displayed once the vSphere has been added.

To access **Agentless Management**, click  > **Agentless Management** in the left menu.



### Using the search bar and search options

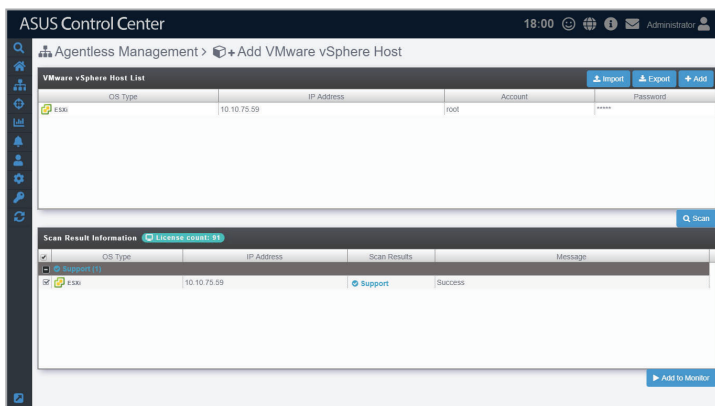
Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.



## 3.2.1 Add vSphere

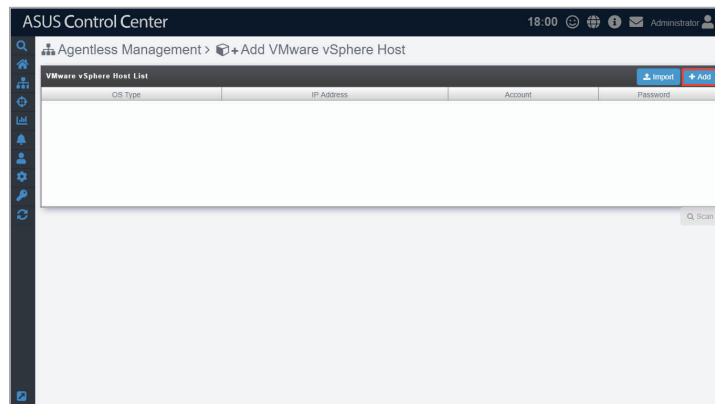
The **Add vSphere** function allows you to add vSphere you wish to manage. You can enter a single vSphere, or multiple vSpheres to be scanned, and then add the scanned vSpheres you wish to manage to ASUS Control Center.

**NOTE:** Ensure to register the License keys before adding the vSphere you wish to manage to ASUS Control Center. For more information on registering license keys, please refer to the **License** chapter.



### Adding managed vSphere

1. Click on **Add**.



2. Enter the **IP Address**, **Account**, and **Password** of the vSphere, then click **Save**.

**Add Target Host**

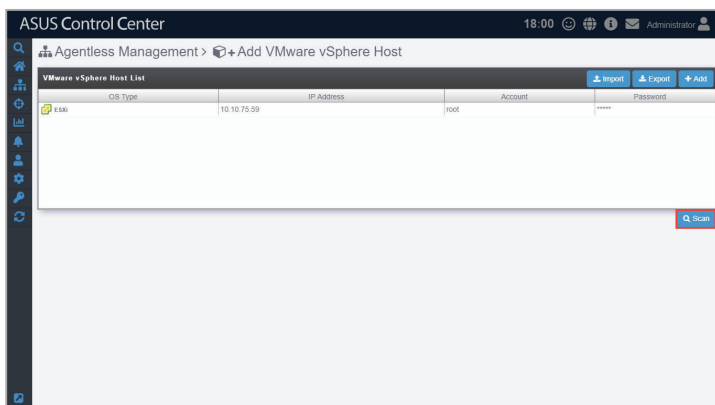
IP Address: 10.10.75.59

Account: root

Password: \*\*\*\*\*

Cancel Save

3. Repeat steps 1 and 2 to add additional vSpheres to be scanned, or refer to the **Add vSphere from CSV file** section to import a list of vSpheres.
4. Once you have added all the vSpheres you wish to scan, click on **Scan**.

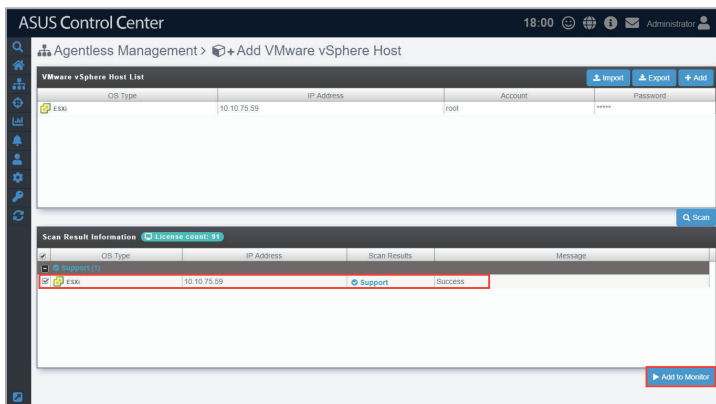


- The scanned results will be displayed in the **Scan Result Information** block. Select the vSpheres you wish to manage then click **Add to Monitor**. The vSpheres added should appear in the **Devices List** on the **System Overview** screen.

---

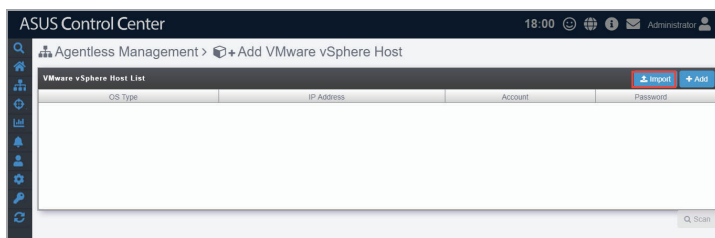
**NOTE:**

- Unavailable vSpheres will be listed as **Not Support**. You may click on the vSpheres to view details on why it is unavailable.
  - vSpheres added may take a few minutes before they are displayed in the overview.
- 



## Add vSphere from CSV file

1. Click on **Import**.



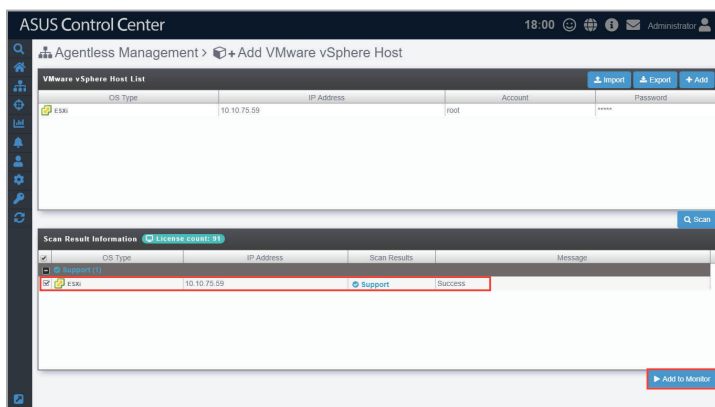
2. Select the CSV file to import and click **Open**.
3. Once the CSV file is successfully imported, click on **Scan**.

**NOTE:** You may edit items added by clicking on it before scanning.

4. The scanned results will be displayed in the **Scan Result Information** block. Select the vSpheres you wish to manage then click **Add to Monitor**. The vSpheres added should appear in the **Devices List** on the **System Overview** screen.

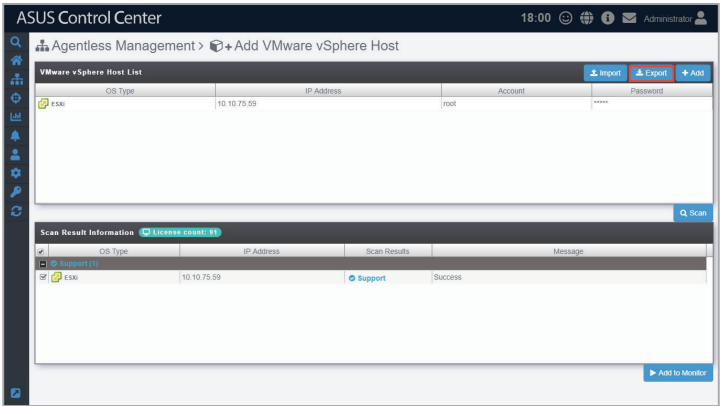
**NOTE:**

- Unavailable vSpheres will be listed as **Not Support**. You may click on the vSpheres to view details on why it is unavailable.
- vSpheres added may take a few minutes before they are displayed in the overview.



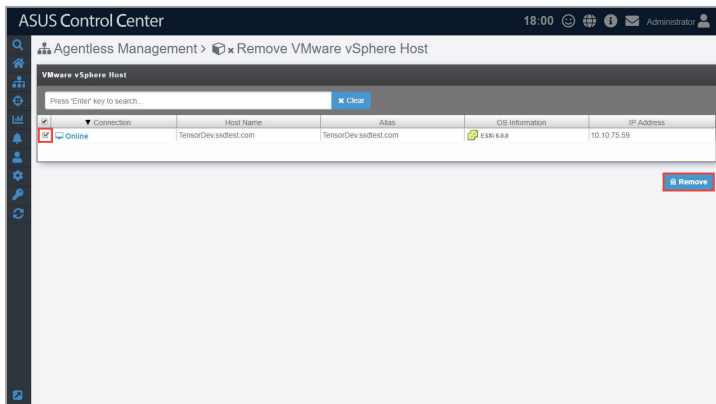
## Exporting VMware vSphere Host List

You can export the list of vSpheres added to the **VMware vSphere Host List** to a CSV file by clicking on **Export**. You can edit the exported CSV file using a text editor.



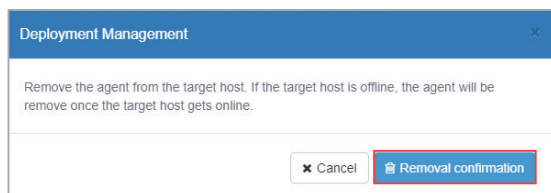
## 3.2.2 Remove vSphere

1. Check the vSphere(s) you wish to remove, then click **Remove**.



2. A confirmation window should pop-up, click **Removal confirmation** to remove the agents from the selected vSpheres.

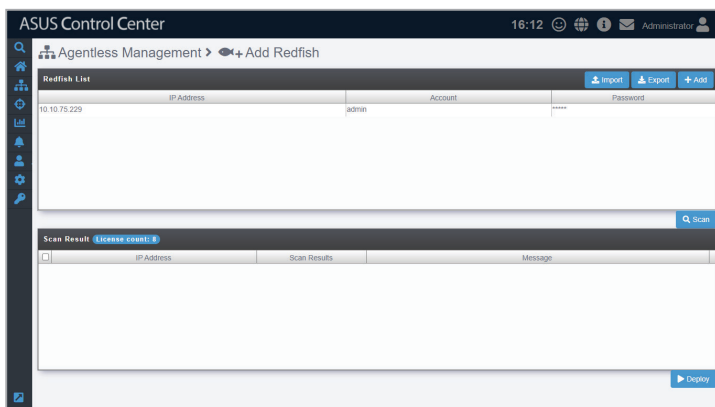
**NOTE:** If the target host(s) are offline, the agents on these host(s) will be removed once the host(s) are online.



### 3.2.3 Add Redfish

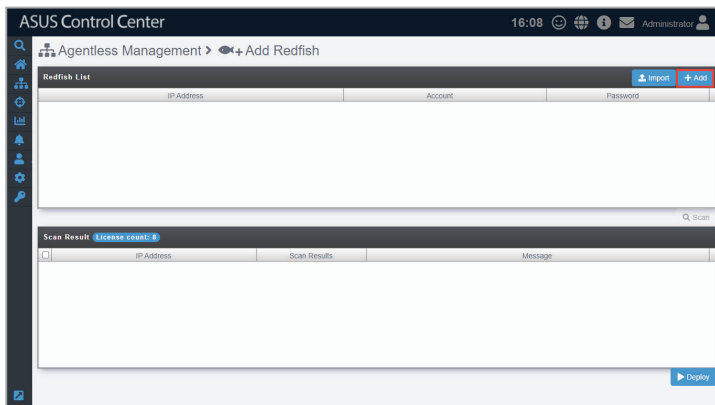
The **Add Redfish** function allows you to add Redfish devices you wish to manage. You can enter a single Redfish device, or multiple Redfish devices to be scanned, and then add the scanned Redfish devices you wish to manage to ASUS Control Center.

**NOTE:** Ensure to register the License keys before adding the Redfish device you wish to manage to ASUS Control Center. For more information on registering license keys, please refer to the **License** chapter.

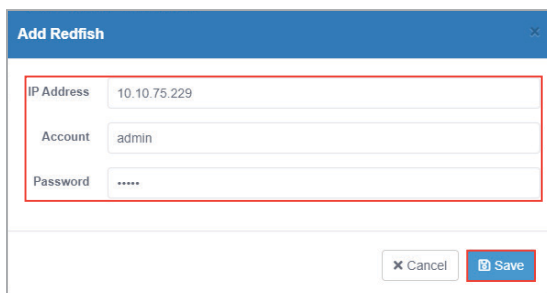


#### Adding managed Redfish device

1. Click on **Add**.

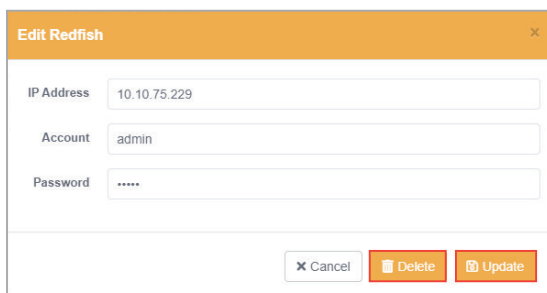


2. Enter the **IP Address**, **Account**, and **Password** of the Redfish device, then click **Save**.



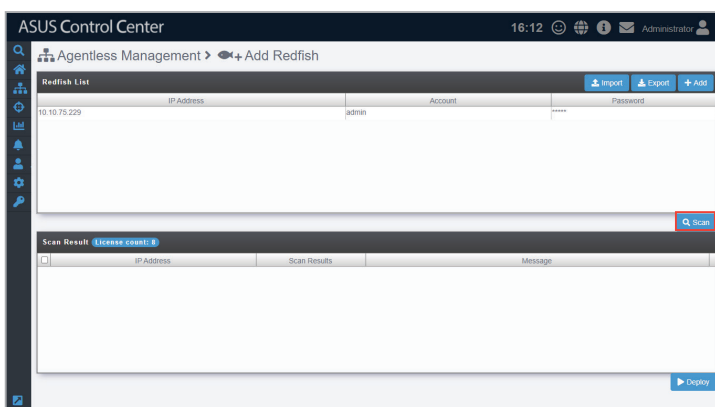
The 'Add Redfish' dialog box has a blue header with a close button. It contains three input fields: 'IP Address' with the value '10.10.75.229', 'Account' with the value 'admin', and 'Password' with masked characters '\*\*\*\*\*'. A red rectangle highlights these three fields. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

3. Repeat steps 1 and 2 to add additional Redfish devices to be scanned, or refer to the **Add Redfish devices from CSV file** section to import a list of Redfish devices.
4. (optional) You may edit or delete Redfish devices added before scanning by clicking on the Redfish device in the **Redfish List**.



The 'Edit Redfish' dialog box has an orange header with a close button. It contains three input fields: 'IP Address' with the value '10.10.75.229', 'Account' with the value 'admin', and 'Password' with masked characters '\*\*\*\*\*'. At the bottom right, there are three buttons: 'Cancel', 'Delete', and 'Update'.

5. Once you have added all the Redfish devices you wish to scan, click on **Scan**.

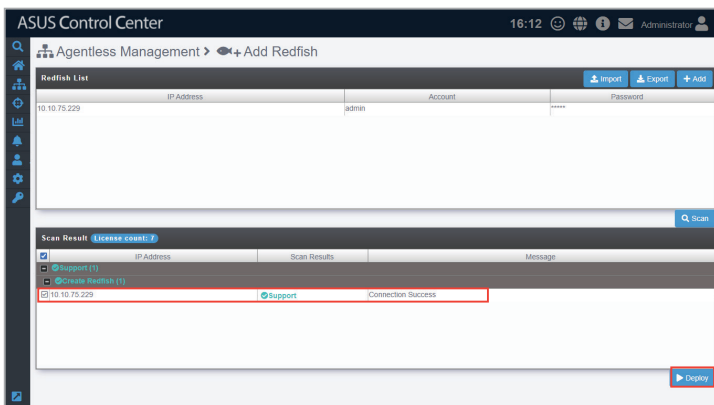


The screenshot shows the 'ASUS Control Center' interface. The top bar includes the title 'ASUS Control Center', the time '16:12', and a user profile 'Administrator'. The main area is titled 'Agentless Management > Add Redfish'. Below this is a 'Redfish List' table with columns for IP Address, Account, and Password. A single row is visible with the IP '10.10.75.229', Account 'admin', and Password '\*\*\*\*\*'. To the right of the table are buttons for 'Import', 'Export', and '+ Add'. Below the table is a 'Scan Result' section with a 'Scan' button. The 'Scan Result' section has a sub-header 'License count: 0' and a table with columns for IP Address, Scan Results, and Message. At the bottom right of the interface is a 'Display' button.

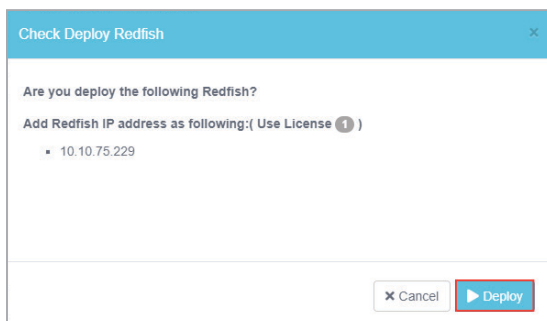


- The scanned results will be displayed in the **Scan Result** block. Select the Redfish devices you wish to manage then click **Deploy**.

**NOTE:** Unavailable Redfish devices will be listed as **Not Support**. You may click on the Redfish device to view details on why it is unavailable.

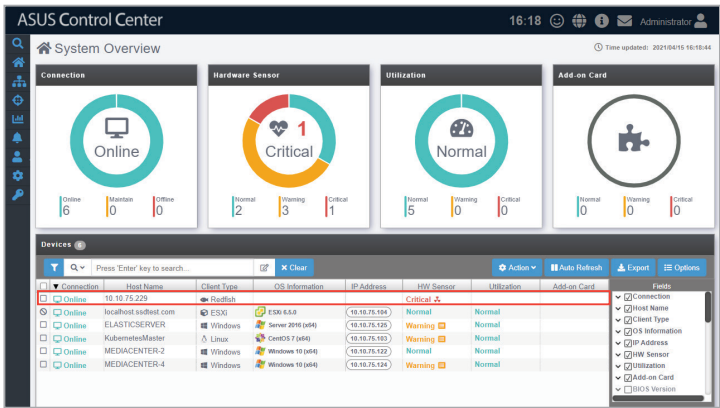


- A pop-up window should appear, displaying the devices you wish to deploy agents to. After confirming the correct devices are selected, click on **Deploy**, then click **OK**.



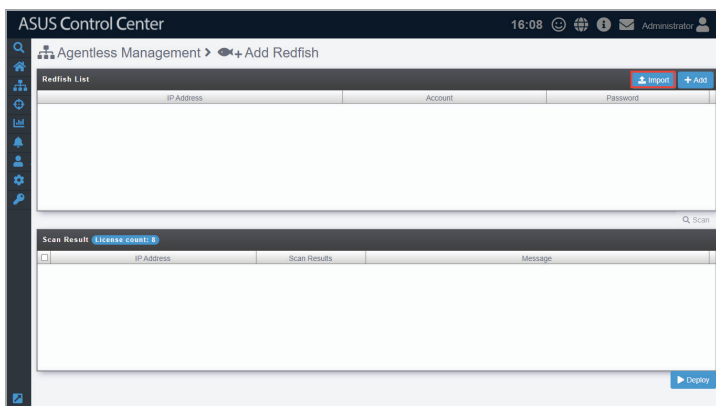
8. The Redfish devices added should appear in the **Devices List** on the **System Overview** screen.

**NOTE:** Redfish devices added may take a few minutes before they are displayed in the overview.



## Adding Redfish devices from a CSV file

1. Click on **Import**.



2. Select the CSV file to import and click **Open**.
3. Once the CSV file is successfully imported, click on **Scan**.

---

**NOTE:** You may edit items added by clicking on it before scanning.

---

4. The scanned results will be displayed in the **Scan Result** block. Select the Redfish devices you wish to manage then click **Deploy**.
5. A pop-up window should appear, displaying the devices you wish to deploy agents to. After confirming the correct devices are selected, click on **Deploy**, then click **OK**.
6. The Redfish devices added should appear in the **Devices List** on the **System Overview** screen.

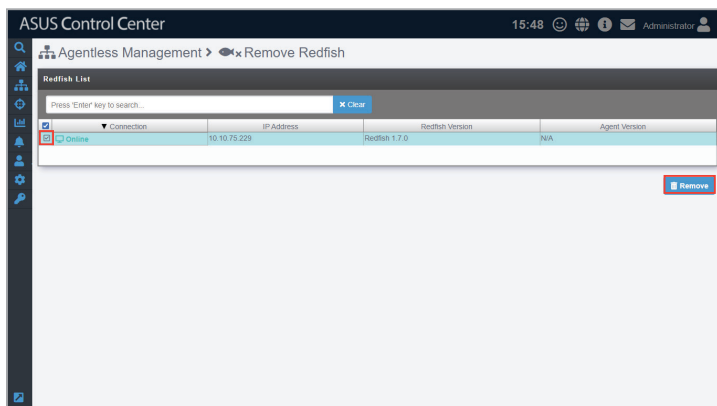
---

**NOTE:** Redfish devices added may take a few minutes before they are displayed in the overview.

---

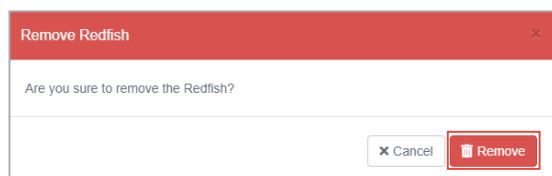
## 3.2.4 Remove Redfish

1. Check the Redfish device(s) you wish to remove, then click **Remove**.



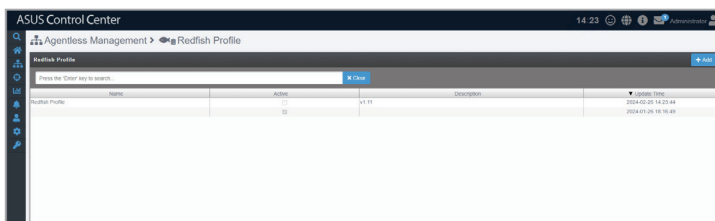
2. A confirmation window should pop-up, click **Remove** to remove the agents from the selected Redfish devices.

**NOTE:** If the target host(s) are offline, the agents on these host(s) will be removed once the host(s) are online.



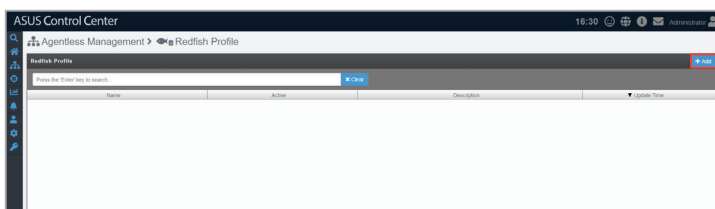
## 3.2.5 Redfish Profile

The **Redfish Profile** function allows you to add, edit, or delete Redfish profiles.

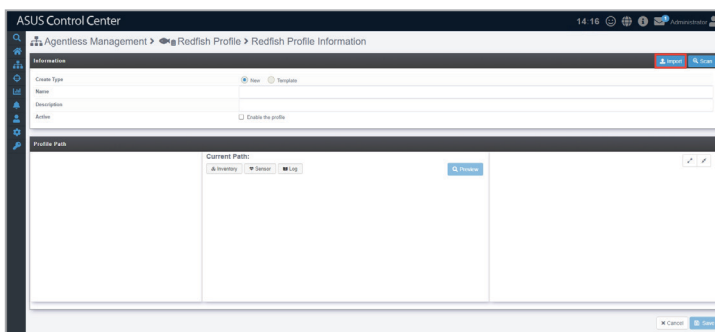


### Adding a Redfish profile by importing a profile file

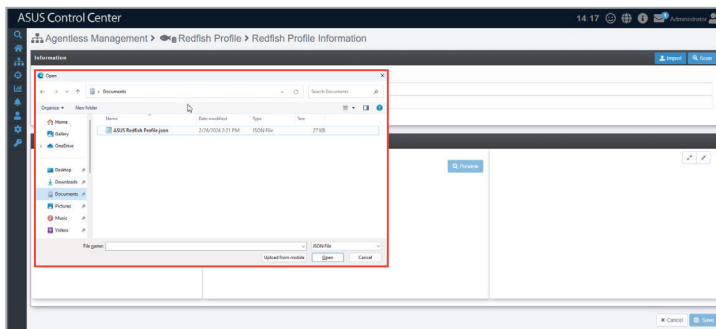
1. Click **Add**.



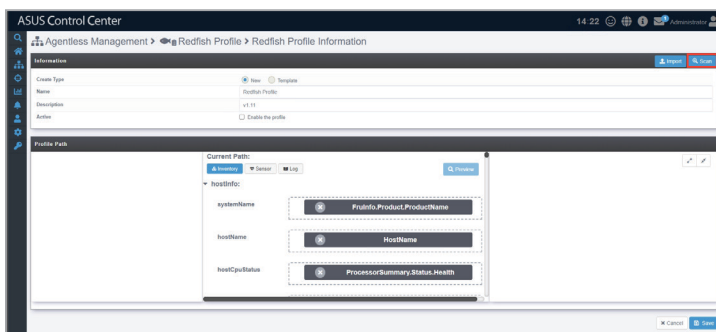
2. Click **Import**.



3. Select a Redfish profile JSON file, then click **Open**.

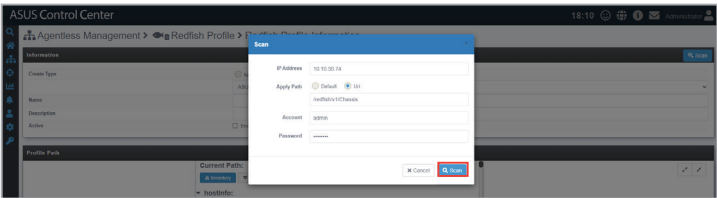


4. Fill in the **Name** and **Description** fields (optional) and tick **Enable this profile**, then click **Scan**.

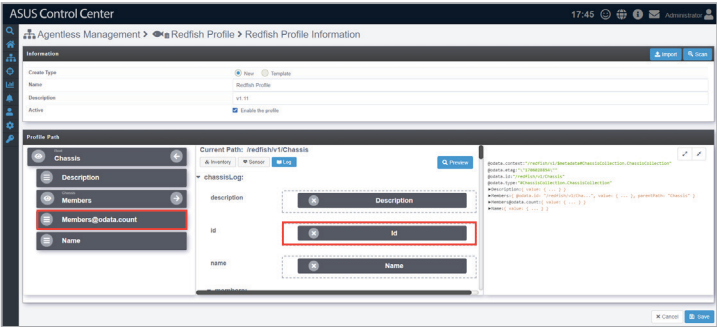


5. Fill in the **IP Address**, **Apply Path**, **Account**, and **Password** fields, then click **Scan**.

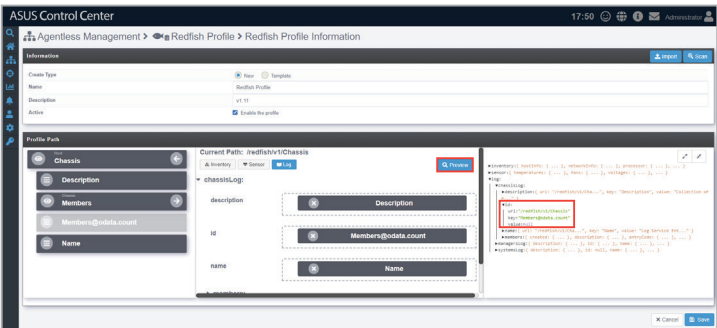
**NOTE:** If the **Apply Path** field is set to Default, the root directory will be scanned. If set to URI, the specified relative path will be scanned.



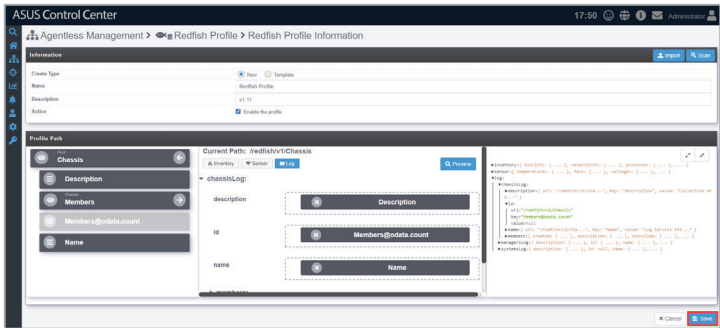
6. To make changes to the Redfish profile, follow the below instructions:
- A. Drag and drop a property from the left pane to the value field in the middle pane.



- B. Click **Preview** to show the updated JSON output in the right pane.



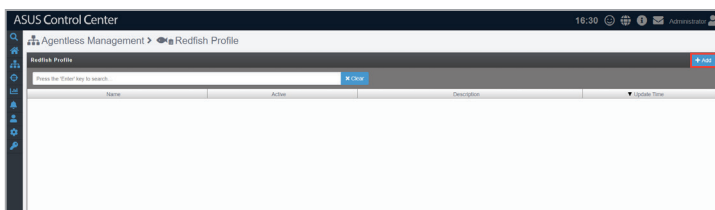
7. Click **Save**.



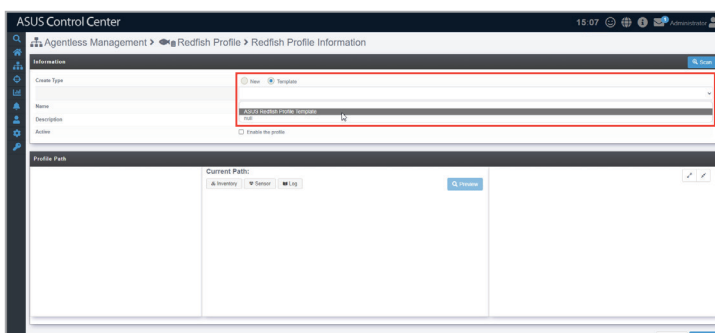


## Adding a Redfish profile from a template

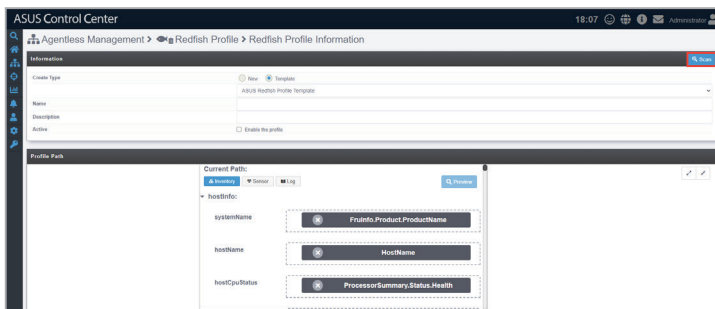
1. Click **Add**.



2. Select **Template** in the **Create Type** field, then select a template from the drop down menu.

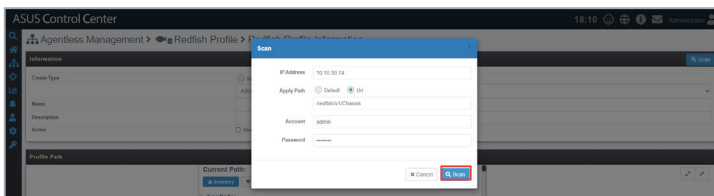


3. Fill in the **Name** and **Description** fields (optional) and tick **Enable this profile**, then click **Scan**.

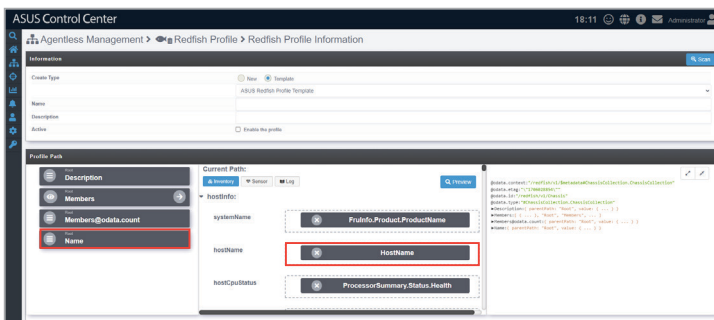


4. Fill in the **IP Address**, **Apply Path**, **Account**, and **Password** fields, then click **Scan**.

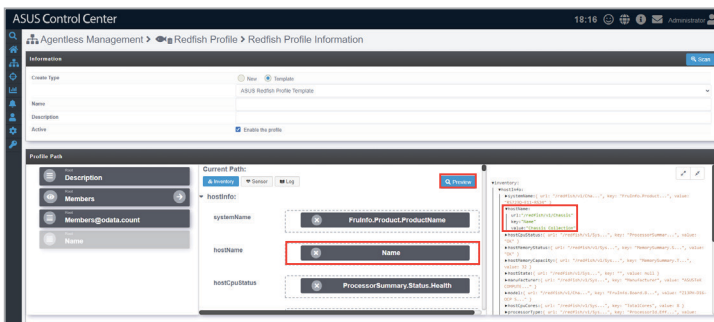
**NOTE:** If the **Apply Path** field is set to Default, the root directory will be scanned. If set to URI, the specified relative path will be scanned.



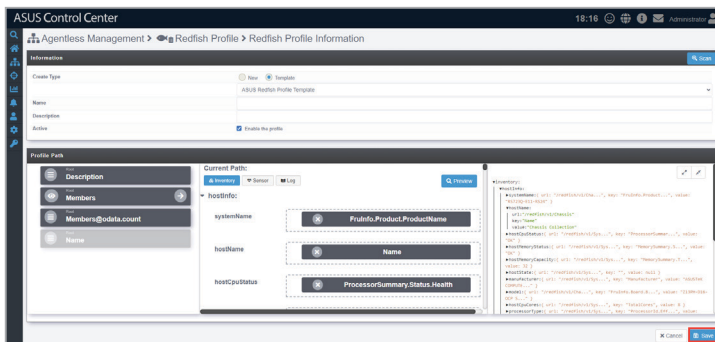
5. To make changes to the Redfish profile, follow the below instructions:
  - A. Drag and drop a property from the left pane to the value field in the middle pane.



- B. Click **Preview** to show the updated JSON output in the right pane.

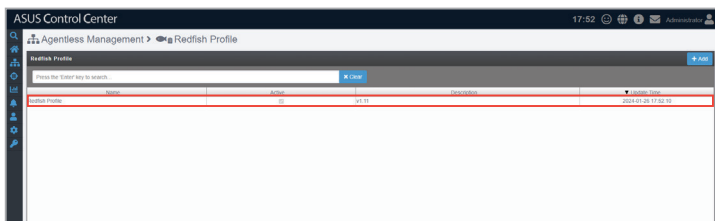


6. Click **Save**.

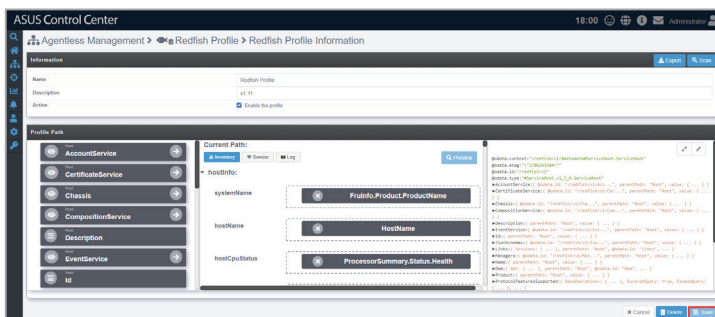


## Editing an existing Redfish profile

1. Select an existing Redfish profile.

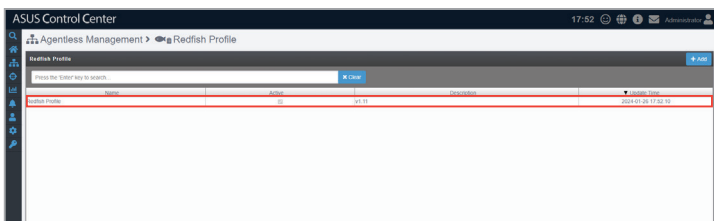


2. Make the desired changes to the Redfish profile, then click **Save**.

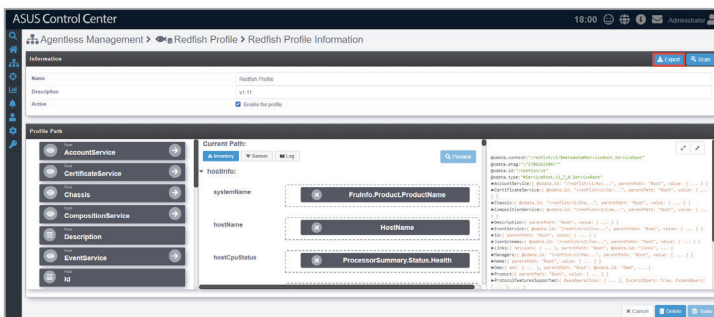


## Exporting an existing Redfish profile

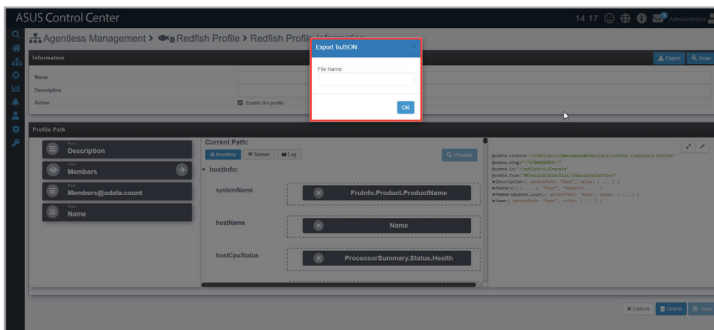
1. Select an existing Redfish profile.



2. Click **Export**.

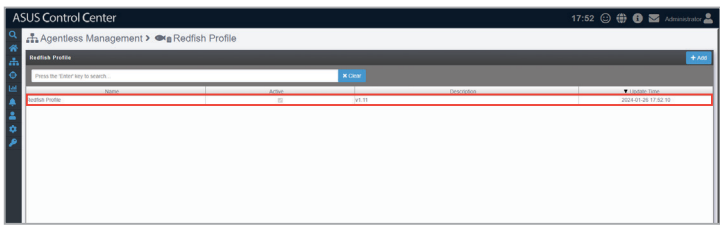


3. Enter a file name for the exported Redfish profile JSON file, then click **OK**.

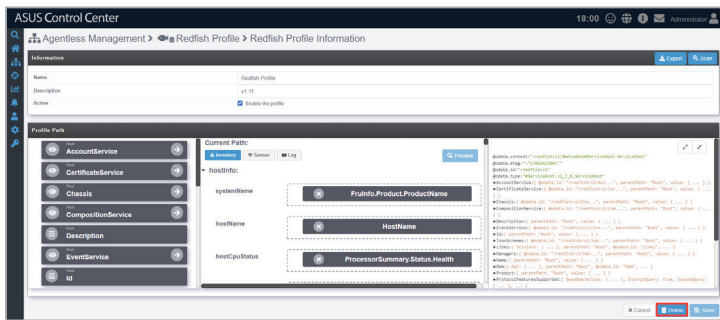


## Deleting an existing Redfish profile

1. Select an existing Redfish profile.



2. Click **Delete**.



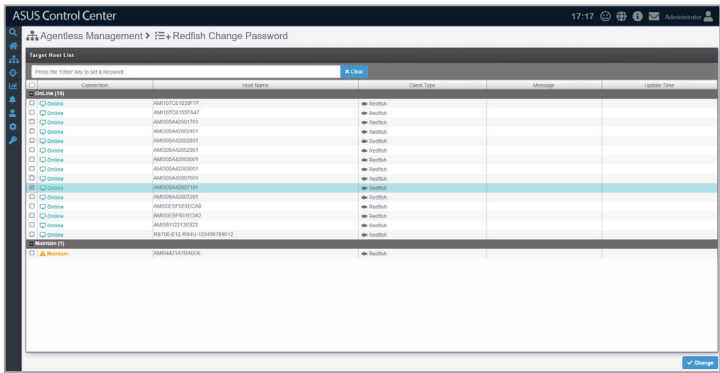
### 3.2.6 Redfish Change Password

The **Redfish Change Password** function allows you to modify the Redfish password for devices.

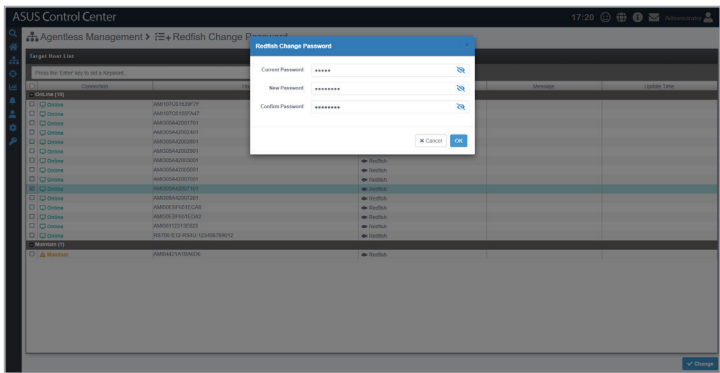
**NOTE:** If Preserve Configuration was not enabled during a Redfish firmware update, the Redfish password will be reset to the default password.

#### Changing a Redfish password

1. Select a Redfish device, then click **Change**.



2. Enter the current password and new password, then click **OK**.

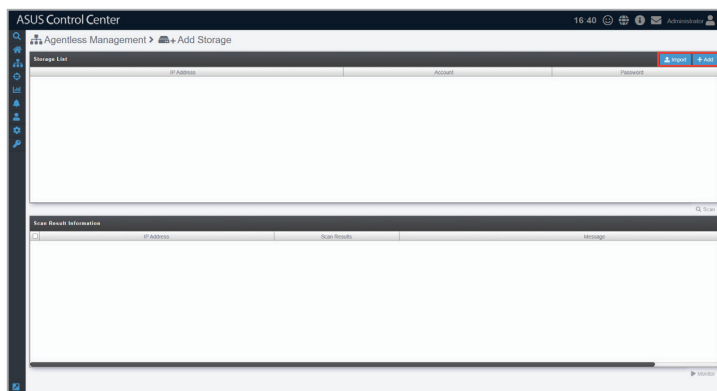


## 3.2.7 Add Storage

The **Add Storage** function allows you to add a managed storage device.

### Adding managed storage devices

1. Click **Import** to add a device using a CSV file, or click **Add** to manually enter the device details.



2. Click **Scan** and wait for the scan results to be displayed in the **Scan Result** block.
3. Select one or more managed storage devices in the **Scan Result Information** block, then click **Monitor**.
4. The selected managed storage devices added should appear in the **Devices List** on the **System Overview** screen.

---

**NOTE:** Newly added devices may take a few minutes to appear in the overview.

---

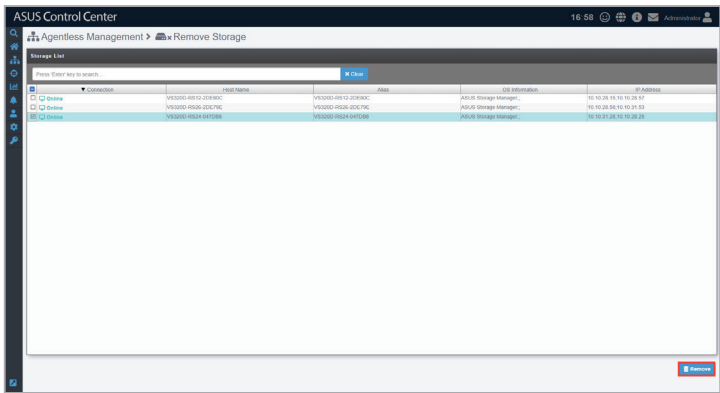


### 3.2.8 Remove Storage

The **Remove Storage** function allows you to remove a managed storage device.

#### Removing managed storage devices

Select one or more managed storage devices, then click **Remove**.





# Chapter 4

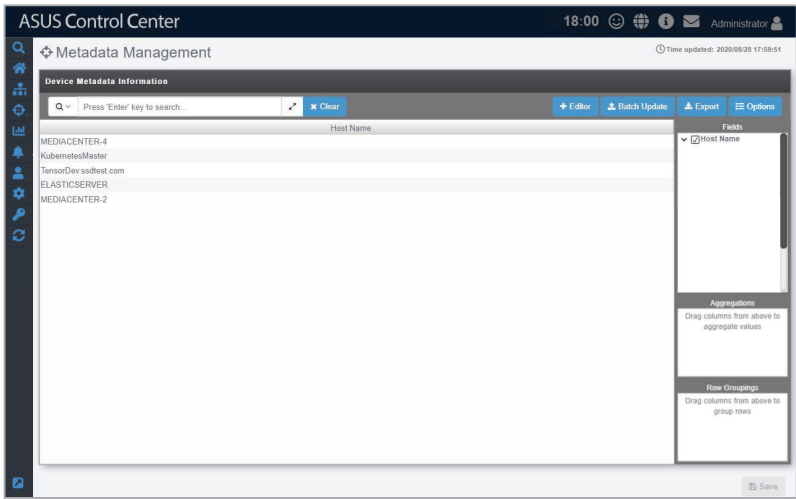
This chapter describes centralized management of metadata, BIOS flash, security, software, tasks, and power control of ASUS Control Center managed devices.

# Centralized

# 4.1 Metadata Management

The **Metadata Management** screen allows you to add metadata fields, and also enter the information for the newly added metadata fields for a single device or multiple devices. This allows you to manage your devices more efficiently by adding the information you need to each managed device, such as the department the managed device belongs to, or the extension line of the owner of the managed device.

To access **Metadata Management**, click  > **Metadata Management** in the left menu.



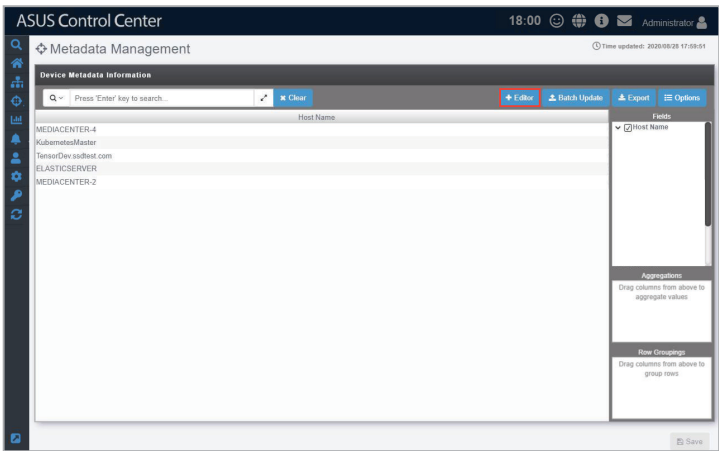
## Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

**Adding metadata fields**

You may add new metadata fields for managed devices using this function.

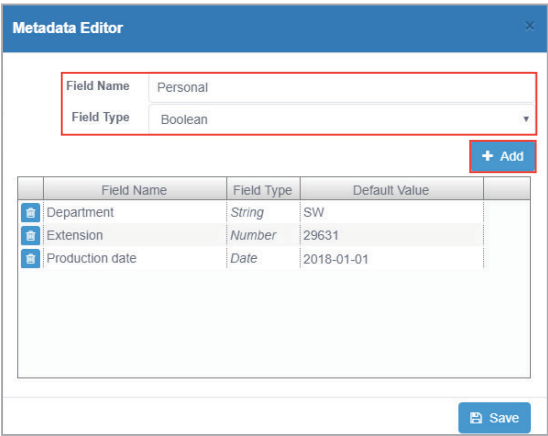
- 1. Click on **Editor** to open the Metadata Editor.



- 2. Enter the Field Name of the new metadata column and select the Field Type from the drop down menu (**String**, **Number**, **Date**, **Boolean**), then click **Add**.

**NOTE:**

- **String:** The data in this field contains string variables.
- **Number:** The data in this field contains numerical values.
- **Date:** The data in this field are in date form.
- **Boolean:** The data in this field are either true or false.



- (optional) You may set or edit the default value of the new field by double-clicking in the **Default Value** cell and then entering the new default value.

---

**NOTE:** The default values will be restricted to the Field Type chosen.

---

The screenshot shows the 'Metadata Editor' window. At the top, there are input fields for 'Field Name' and 'Field Type' (a dropdown menu currently showing '--Please Select--'). To the right of these fields is a blue '+ Add' button. Below the input fields is a table with the following data:

|  | Field Name      | Field Type | Default Value            |
|--|-----------------|------------|--------------------------|
|  | Department      | String     | SW                       |
|  | Extension       | Number     | 29631                    |
|  | Production date | Date       | 2018-01-01               |
|  | Personal        | Boolean    | <input type="checkbox"/> |

At the bottom right of the window is a blue 'Save' button. A red rectangle highlights the 'Default Value' column in the table.

- Repeat steps 2 to 4 to add additional metadata fields.
- Click on **Save** when you have finished adding or editing the metadata fields.

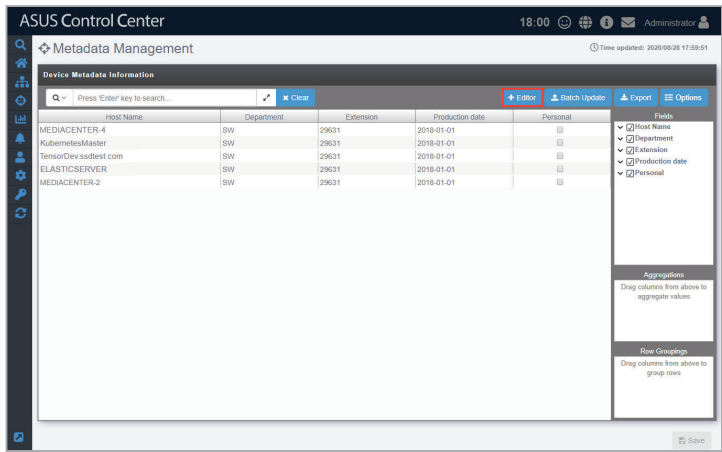
This screenshot shows the 'Metadata Editor' window with an 'Update' dialog box open over the 'Field Name' input field. The dialog box contains the text 'Done.' and a close button (X). The table below the dialog box is identical to the one in the previous screenshot:

|  | Field Name      | Field Type | Default Value            |
|--|-----------------|------------|--------------------------|
|  | Department      | String     | SW                       |
|  | Extension       | Number     | 29631                    |
|  | Production date | Date       | 2018-01-01               |
|  | Personal        | Boolean    | <input type="checkbox"/> |

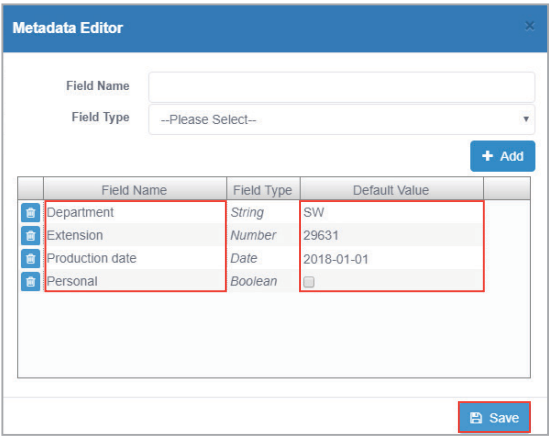
The 'Save' button at the bottom right is now highlighted with a red rectangle.

Editing metadata fields

- 1. Click on **Editor** to open the Metadata Editor.

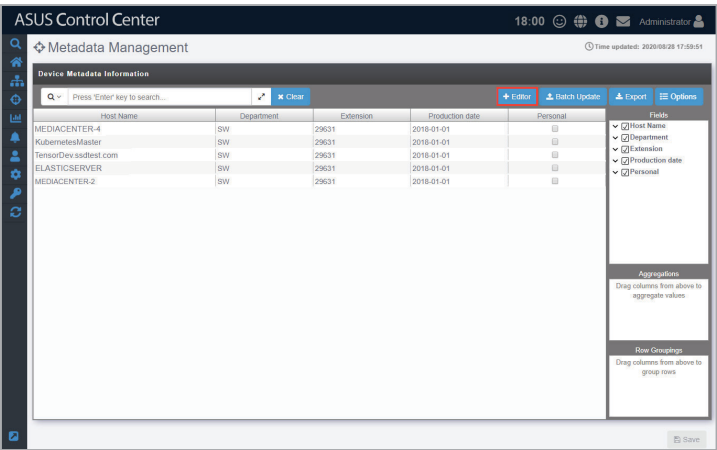


- 2. You can edit the **Field Name** and **Default Value** of existing metadata fields. When you are finished editing, click on **Save** to save the changes made.

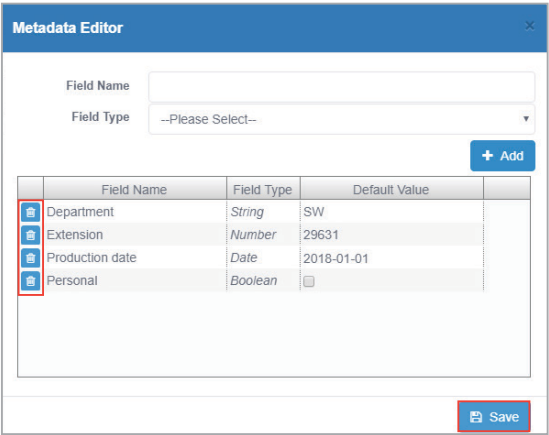


## Deleting metadata fields

1. Click on **Editor** to open the Metadata Editor.



2. Click on  next to the metadata field you wish to delete. Once you are finished, click on **Save** to save the changes made.





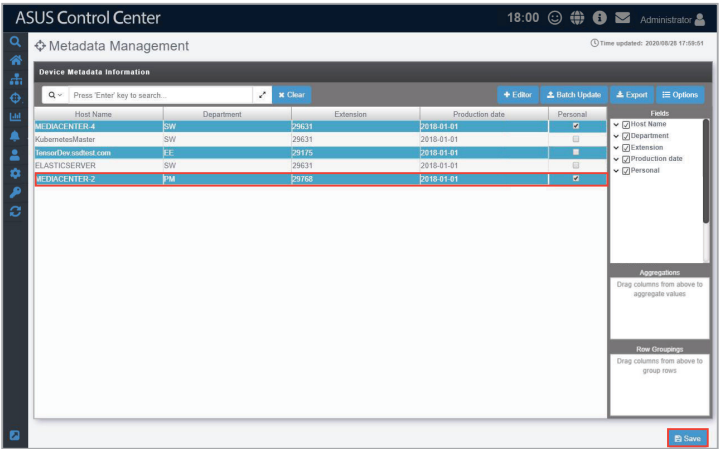
**Editing the metadata value of a single device**

- 1. Double-click on a field you wish to edit and enter the new value.

**NOTE:**

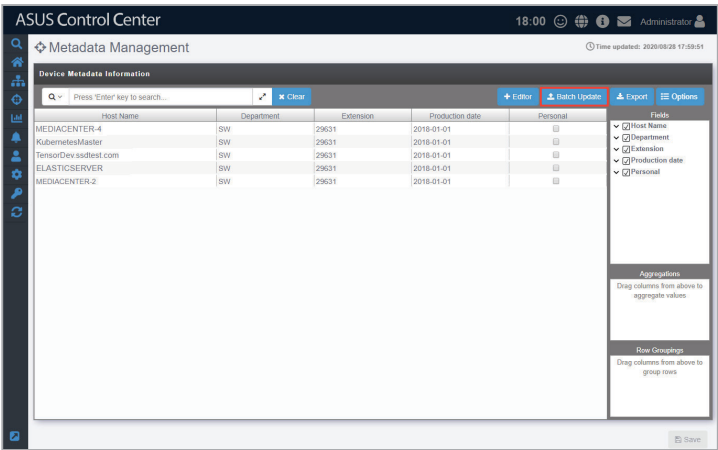
- Items in the **Host Name** field cannot be edited.
- Edited fields will have blue text.

- 2. Click on **Save** once you have finished making changes to the metadata.

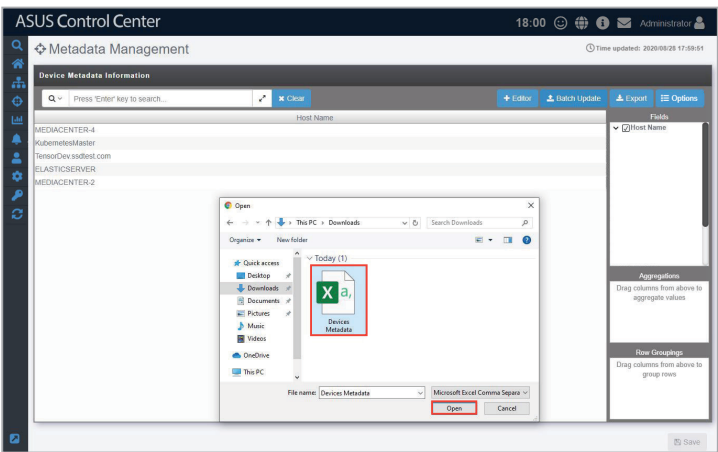


# Editing the metadata value of multiple devices

1. Click on **Batch Update**.



2. Select a CSV file to import, then click **Open**.



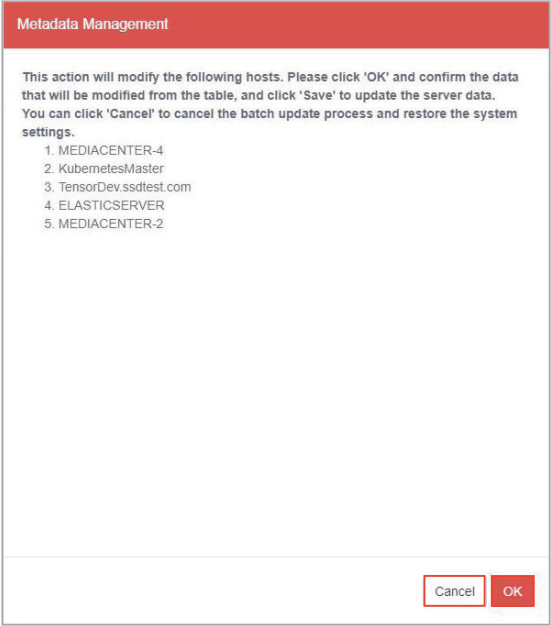
3. Select the metadata field columns to update to the server, then click **Batch Update**.

The screenshot shows a dialog box titled "Metadata Management" with a blue header. The main text says "Please select the fields you want to import from the csv file to the server." Below this, there is a list of four items: "Department", "Extension", "Production date", and "Personal". Each item has a checked checkbox to its left. A red rectangular box highlights the entire list of items. At the bottom right of the dialog, there are two buttons: "Cancel" and "Batch Update". The "Batch Update" button is highlighted with a red border.

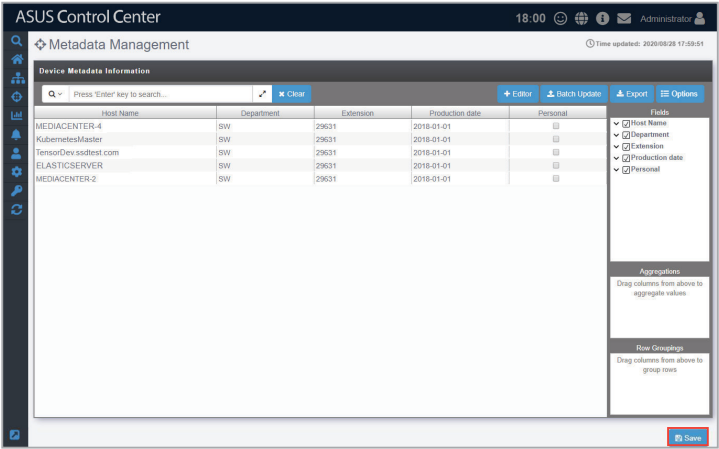
4. A confirmation window should pop-up, click **OK**.

The screenshot shows a confirmation window titled "Metadata Management" with a red header. The main text says "Please select the fields you want to import from the csv file to the server." Below this, the text "Department, Extension, Production date, Personal" is displayed. At the bottom right of the dialog, there are two buttons: "Cancel" and "OK". The "OK" button is highlighted with a red border.

5. Next, another pop-up window will appear notifying you of which devices will be affected by the updated data. Click **OK** to confirm these changes, or click **Cancel** to cancel the batch update.



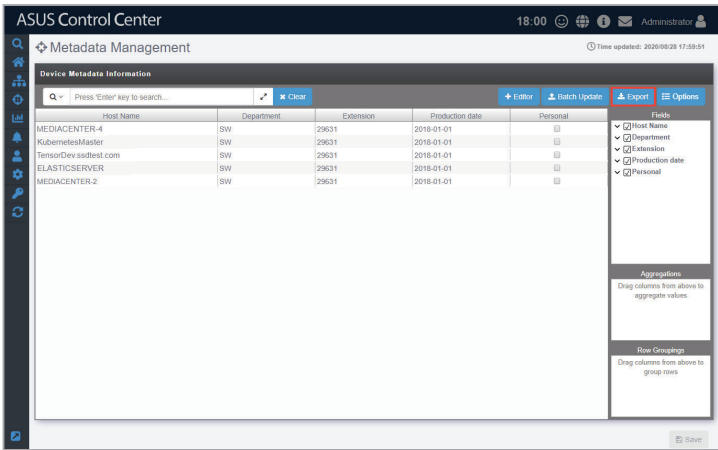
6. If you clicked **OK** in the previous step, click on **Save** to save the changes made.



**Exporting the metadata value**

Exporting the metadata to a CSV file allows you to edit multiple metadata fields together, then update them by importing it back into ASUS Control Center. To import the changes made to the metadata in the CSV file, refer to **Editing the metadata of multiple devices** under the **Metadata Management** section.

- 1. Click on **Export**.



- 2. Enter a filename for the CSV file, then click **OK**.

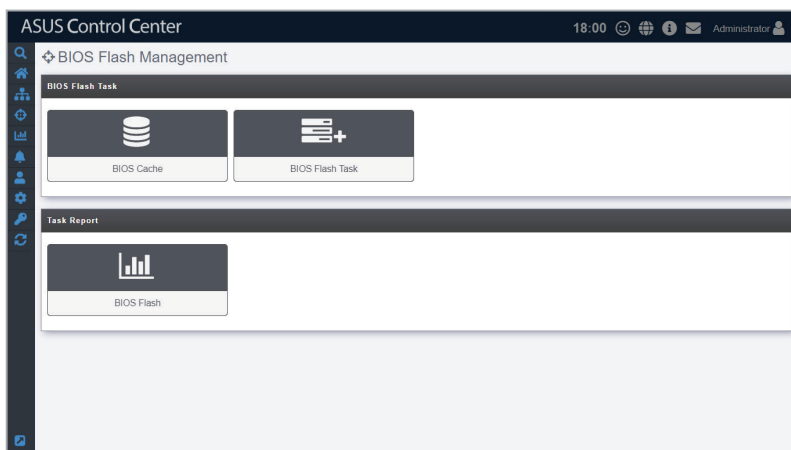
**NOTE:**

- Use a text editor when editing the exported CSV file.
- Do not edit the **aswm\_HostName** and **ClientGUID** fields.
- Only the existing data in the CSV file may be edited, adding new rows and columns to the CSV file may cause failure when importing to the ASUS Control Center.

## 4.2 BIOS Flash Management

**BIOS Flash Management** allows you to upload and flash the BIOS of all devices, uploaded BIOS is also stored in the BIOS cache for centralized management.

To access **BIOS Flash Management**, click  > **BIOS Flash Management** in the left menu.

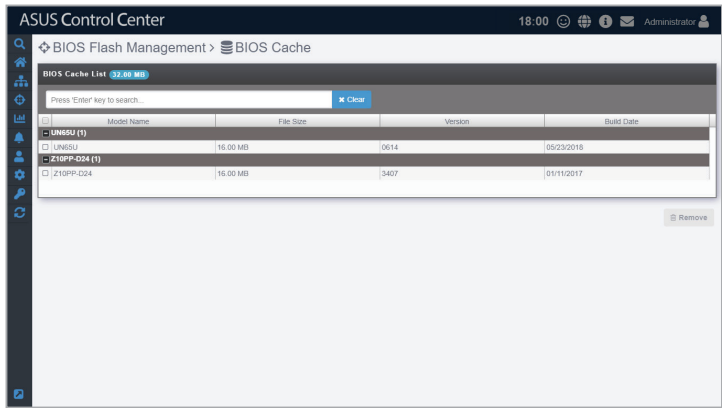


### Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

### 4.2.1 BIOS Cache

The **BIOS Cache** stores all the BIOS cap files uploaded when flashing the BIOS of a single device or using the BIOS Flash Task function, and allows you to view or delete the BIOS cap files in the BIOS Cache List. The BIOS Cache List also lists the BIOS cap file in groups based on the model, and displays information such as the file size, version, and build date.



#### Adding a BIOS cap file to the BIOS Cache

The BIOS cap file is automatically added to the BIOS Cache when you manually upload a BIOS cap file when flashing the BIOS from **Device Information**, or when you manually upload a BIOS cap file when using the **BIOS Flash Task** function.

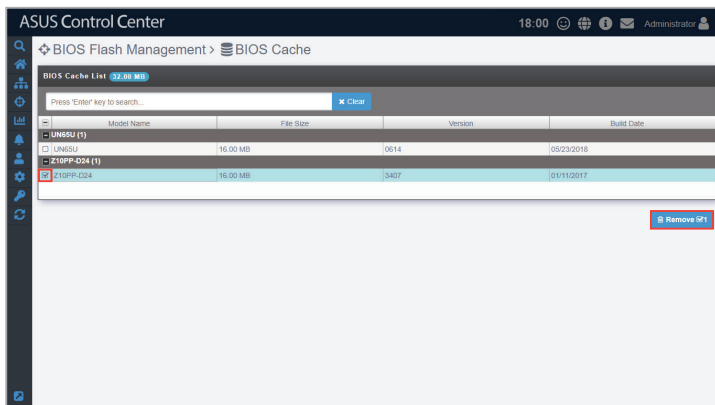
**NOTE:**

- For more details on manually uploading a BIOS cap file when flashing the BIOS from **Device Information**, please refer to **BIOS Flash** under the **BIOS** section.
- For more details on manually uploading a BIOS cap file when using the **BIOS Flash Task** function, please refer to **Manually uploading the BIOS cap file** under the **BIOS Flash Task** section.

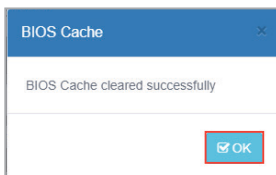
## Removing BIOS cap files from BIOS Cache

You can remove BIOS cap files from the BIOS Cache List when you need to, such as when the BIOS version is outdated.

1. Check the item(s) you wish to delete then click **Remove**.



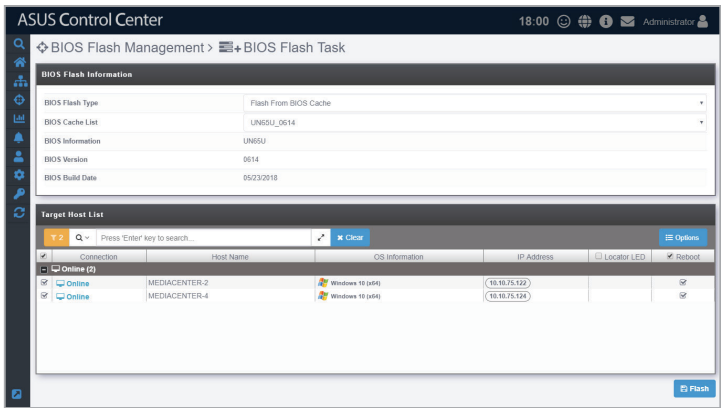
2. When the BIOS cap file(s) have been successfully removed, click **OK**.





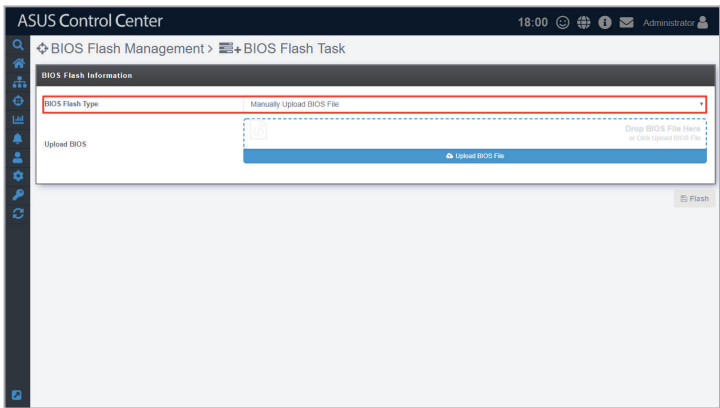
## 4.2.2 BIOS Flash Task

The **BIOS Flash Task** function allows you to update the BIOS of multiple managed devices by uploading the BIOS cap file or selecting the BIOS cap file from a BIOS cache list.

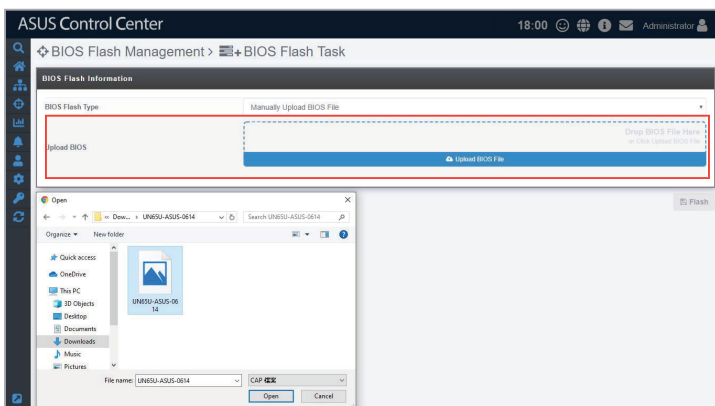


### Manually uploading the BIOS cap file

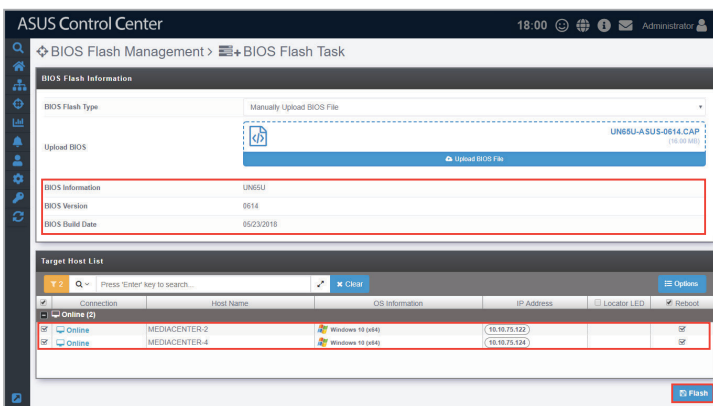
1. Select **Manually Upload BIOS File** from the drop down menu in the **BIOS Flash Type** field.



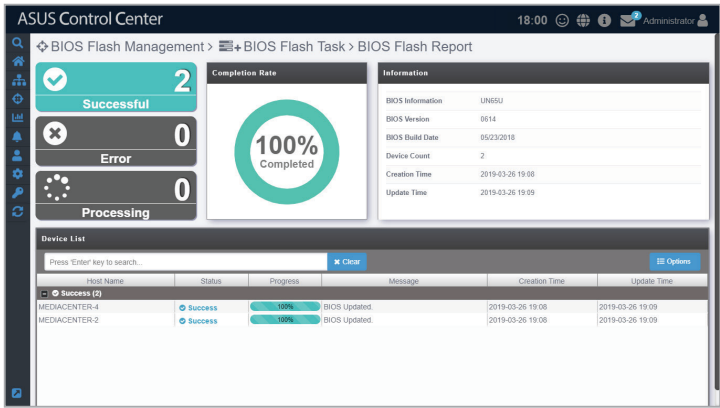
2. Drag and drop the BIOS cap file in the dotted square, or click on **Upload BIOS File** to select a BIOS cap file to upload.



3. After selecting the BIOS cap file, the BIOS information, BIOS version, BIOS build date, as well as applicable managed devices should appear. Click on **Flash** to begin the BIOS Flash process.

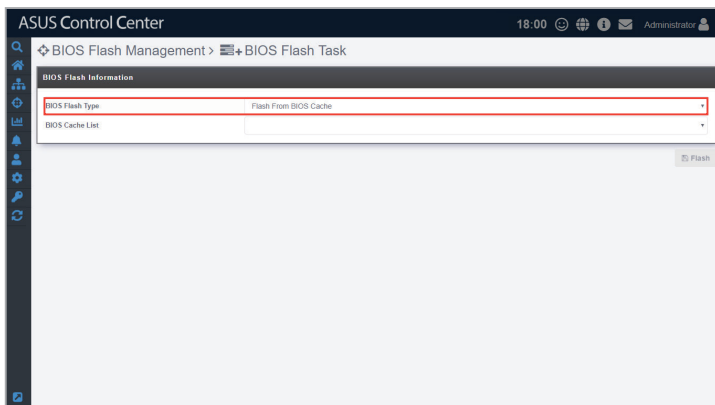


4. Once the flash process is finished, a BIOS Flash Report should appear allowing you to check the BIOS Flash status and progress of all selected devices.

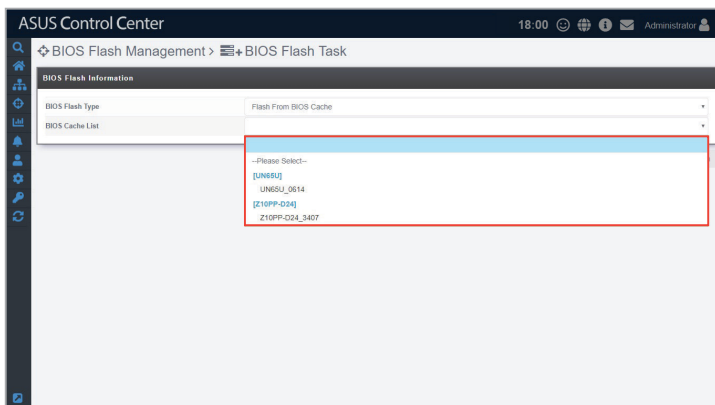


## Selecting the BIOS cap file from the BIOS cache

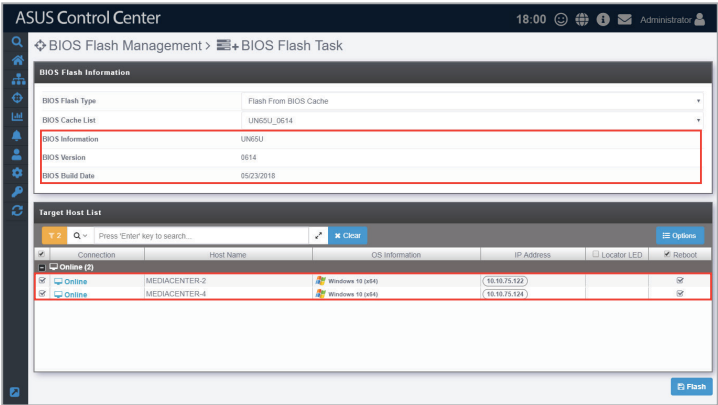
1. Select **Flash From BIOS Cache** from the drop down menu in the **BIOS Flash Type** field.



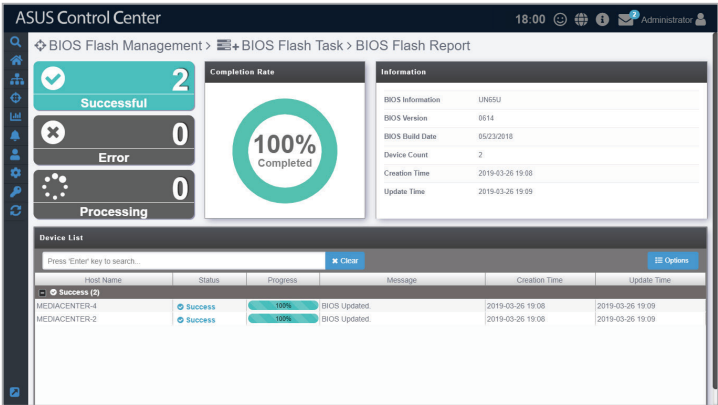
2. Select a **BIOS Cache List**.



3. After selecting the BIOS cap file, the BIOS information, BIOS version, BIOS build date, as well as applicable managed devices should appear. Click on **Flash** to begin the BIOS Flash process.



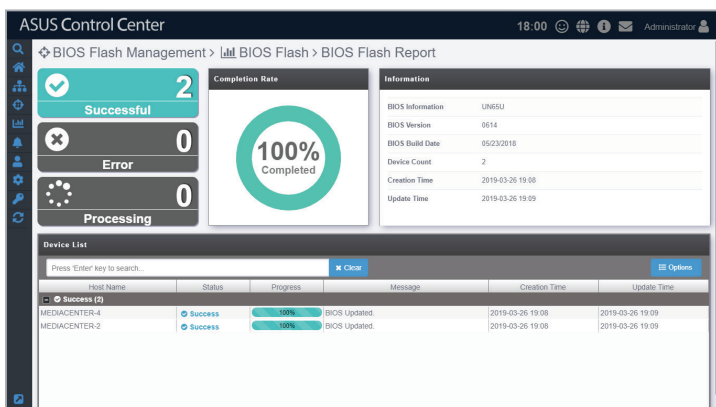
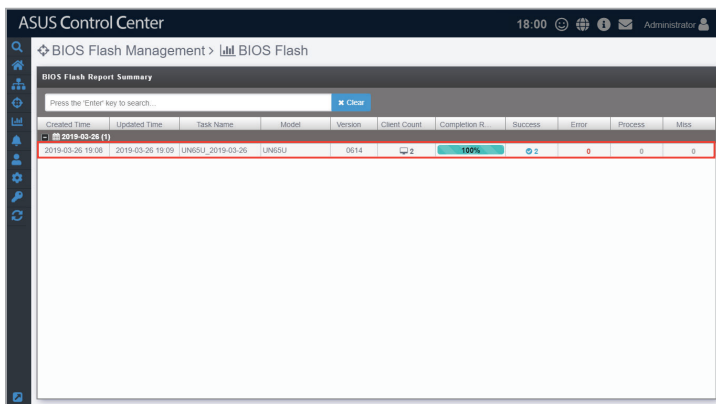
4. Once the flash process is finished, a BIOS Flash Report should appear allowing you to check the BIOS Flash status and progress of all selected devices.



**NOTE:** If the device is using Windows 11 or Server 2022 and the BIOS flash is failing, please navigate to **Start > Settings > Update & Security > Windows Security > Device Security**, then select **Core Isolation details** and set **Memory integrity** to **Off** on the device.

## 4.2.3 BIOS Flash Task Report

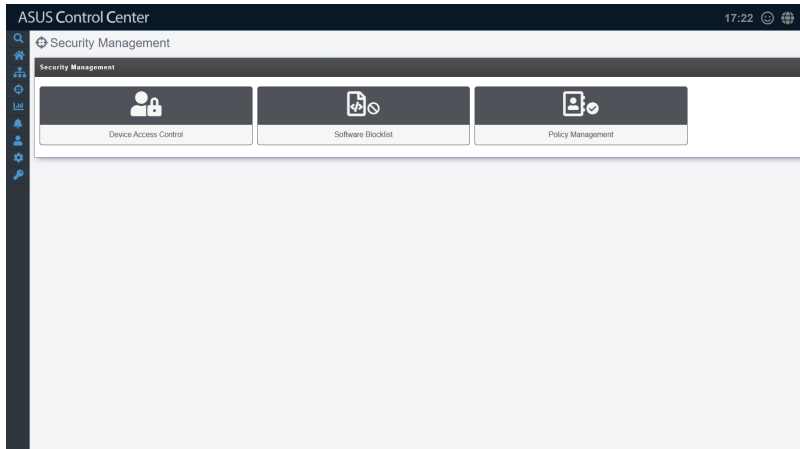
The **BIOS Flash Task Report** function will display a history of BIOS flashes performed using ASUS Control Center. Selecting a BIOS flash task listed in the BIOS Flash Report Summary will allow you to view information on the BIOS, which devices were flashed, and also the status of the BIOS flash to managed devices. This provides you with a quick overview of your BIOS flash tasks and also help you pinpoint devices which experienced errors when updating BIOS.



## 4.3 Security Management

**Security Management** allows you to modify the security settings for items such as Windows Registry Editor, USB access, or Watchdog for a single managed device or all managed devices. The centralized security management makes it so that you do not have to configure the security settings for each individual managed device through Device Information.

To access **Security Management**, click  > **Security Management** in the left menu.



---

**NOTE:** Registry Editor and USB configurations are only available for Windows system managed devices.

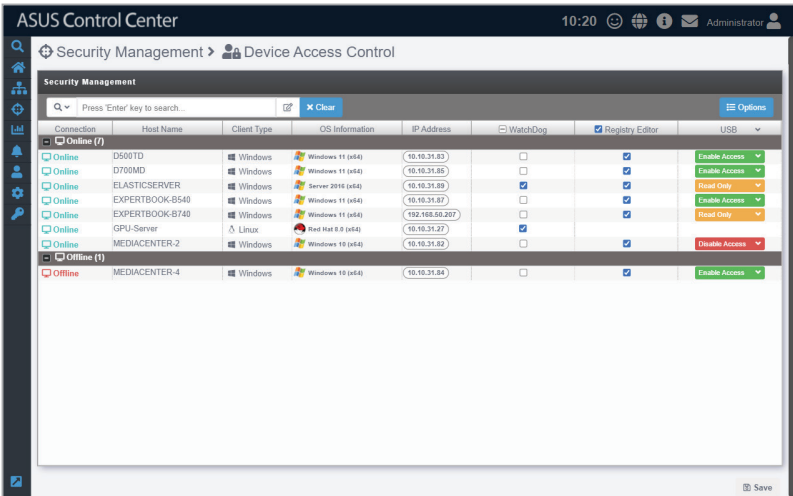
---

### Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

### 4.3.1 Device Access Control

**Device Access Control** allows you to modify the security settings for items such as Windows Registry Editor, USB access, or Watchdog for a single managed device or all managed devices. The centralized security management makes it so that you do not have to configure the security settings for each individual managed device through Device Information.





Setting the device access control for managed devices

- 1. You can set the security function for all managed devices by checking or unchecking the column headers for **Watchdog** or **Registry Editor**, or selecting a mode for **USB** from the drop down menu in the column header.

You can also set the security function for a single managed device by checking or unchecking the **Watchdog** or **Registry Editor** checkbox, or selecting a mode for **USB** from the drop down menu of the managed device.

You may refer to the brief descriptions for the different security functions below:

- Watchdog

Watchdog allows you to enable or disable the Watchdog timer. When the watchdog timer in unresponsive due to hardware fault or program error, it will reboot the device.

**NOTE:** Auto Restart needs to be disabled on Windows® Server 2016 or later versions for Watchdog to successfully reboot the device when required. To disable **Auto Restart**, search for **Control Center** in the Windows Search Box, then navigate to **System > Advanced System Settings > Startup and Recovery**.

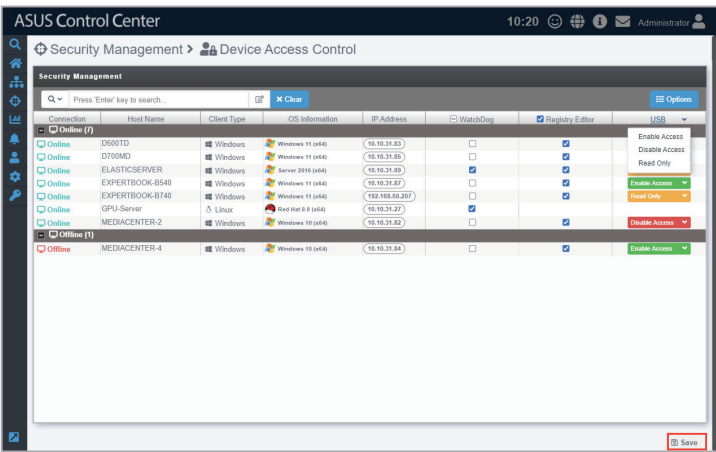
- Registry Editor (Windows only)**

The **Registry Editor** allows you to enable or disable access to Regedit Tool in Windows® by the managed device's user.

- USB (Windows only)**

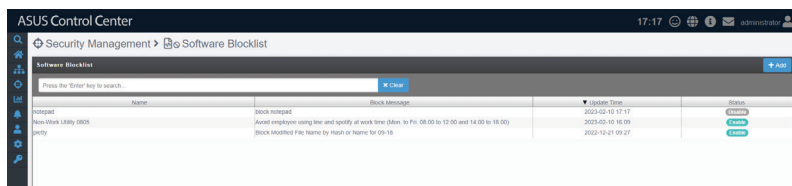
**USB** allows you to **Enable Access** or **Disable Access** of USB ports on the managed device, or set it to **Read Only**, which allows the users to view files on the USB storage device only.

- 2. Click on **Save** once you have finished making changes to save the changes made.



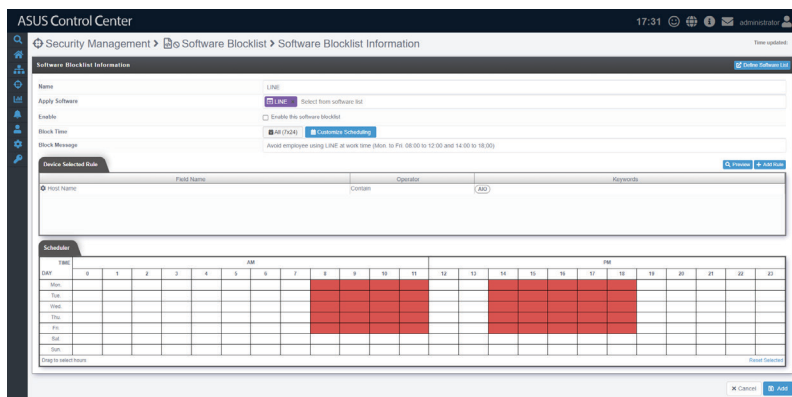
## 4.3.2 Software Blocklist

**Software Blocklist** allows you to create or manage rules to prevent selected software applications from running on the managed device during specified time periods.



### Adding a new software blocklist rule

1. Click **Add** to create a new software blocklist rule.



2. Enter a **Name** for the software blocklist rule, then use **Apply Software** to select an application from the software list.

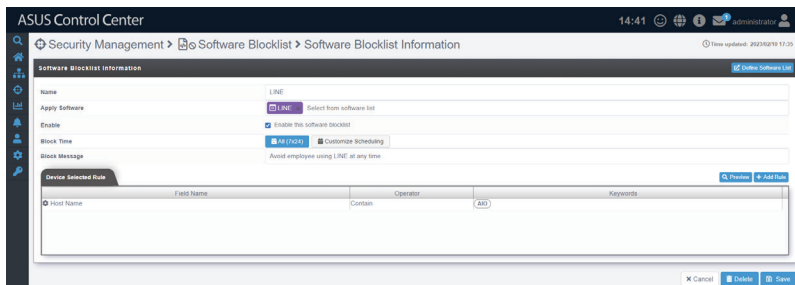
**NOTE:** For more information on software lists, please refer to the **Software List** section of the **Options** chapter.

3. Tick **Enable** to enable the software blocklist rule.
4. Select **All (7x24)** in the **Block Time** field to enable the software block list rule at all times, or select **Customize Scheduling** to specify a custom schedule using the **Scheduler**.
5. Fill in the **Block Message** field with a brief description that will be displayed on the managed device.

- Click **+ Add Rule** to specify which managed devices the software blocklist rule should apply to. To view a list of managed devices that will be affected by the software blocklist rule, click **Preview**.
- Click **Add** to save the software blocklist rule.

### **Editing a software blocklist rule**

- Double click an existing rule from the Software Blocklist rule list to open the rule editor.



- After making the desired changes, click **Save** to save the software blocklist rule.

### **Deleting a software blocklist rule**

- Click an existing rule from the Software Blocklist rule list to open the rule editor.
- Click **Delete** to delete the software blocklist rule.

### 4.3.3 Policy Management

This page allows you to add policies to automatically apply rules based on device metadata, such as disabling USB access based on the device's location.

Rules are applied in the following priority based on the source of the policy:

1. General Configuration > Policy Configuration (default policy)
2. Security Management > Policy Management (applied based on metadata)
3. Security Management > Device Access Control (applied to multiple devices)
4. Device Information > Security (applied to a specific device)

ASUS Control Center

Security Management > Policy Management

15:00 [Icons] Administrator

Policy List

Press the Enter key to search. [Clear]

[Select] [Import] [Export] [Add]

| SELECT                              | POLICY NAME                              | DEPENDENCY NAME | DEPENDENCY VALUE | RULE NAME | RULE VALUE | ACTION | LAST LASTMODIFIED   |
|-------------------------------------|------------------------------------------|-----------------|------------------|-----------|------------|--------|---------------------|
| <input checked="" type="checkbox"/> | Disallow USB default read only in Taipei | Location        | Taipei           | USB       | Disallow   | Deny   | 2023-09-12 14:58:29 |

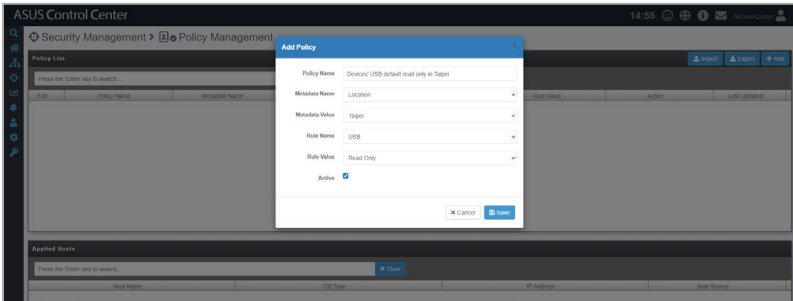
Applied Hosts

Press the Enter key to search. [Clear]

| HOST NAME   | OS TYPE                                                  | IP ADDRESS                          | RULE SOURCE |
|-------------|----------------------------------------------------------|-------------------------------------|-------------|
| F100L-2023  | Microsoft Windows Server 2022 Datacenter (ARM) 19H2.20H2 | 10.10.28.28                         | Policy List |
| NUC10CHN-01 | Microsoft Windows 11 Pro(64-bit) 22H2                    | 10.10.28.28                         | Policy List |
| BEN-DEV     | Microsoft Windows 10 專業版 64 位元 19H2                      | 10.10.31.150/192.168.0.1/172.16.0.1 | Policy List |

## Adding a policy

1. Click **Add**, then fill in the policy, metadata, and rule fields.
2. Tick the **Active** checkbox to enable the rule, then click **Save**.



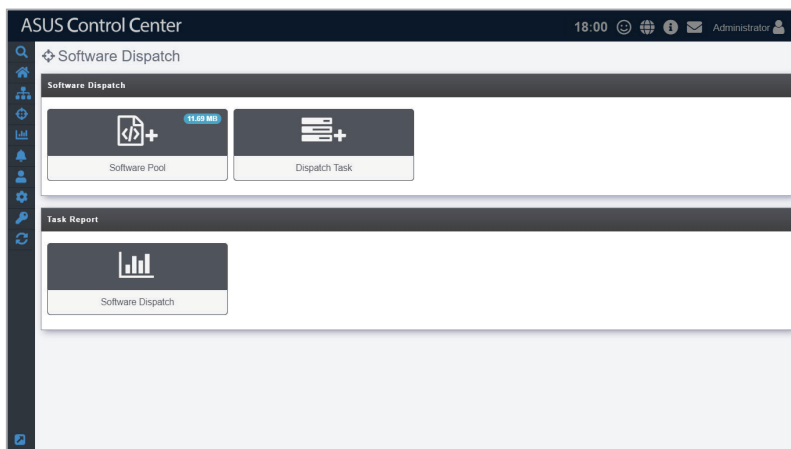
## Editing or removing a policy

1. Click the edit icon next to the policy in the **Policy List** block.
2. Make changes as required and click **Update** or **Delete**, then confirm the action if prompted.

## 4.4 Software Dispatch

**Software Dispatch** is a centralized software management function that allows you to add or remove software packages to a Software Pool, allowing for easy software dispatching to managed devices using the Software Dispatch Task function.

To access **Software Dispatch**, click  > **Software Dispatch** in the left menu.

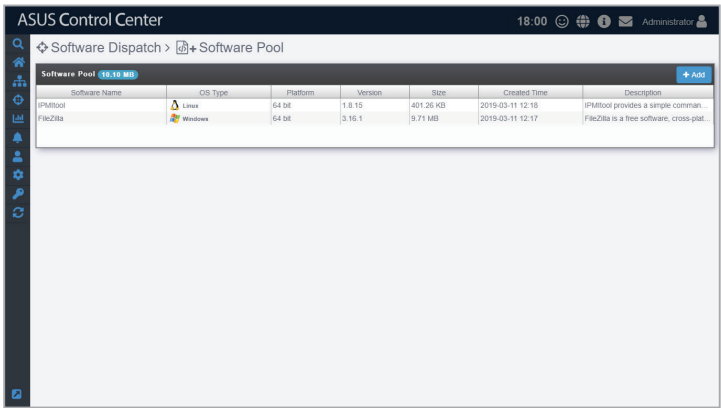


### Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

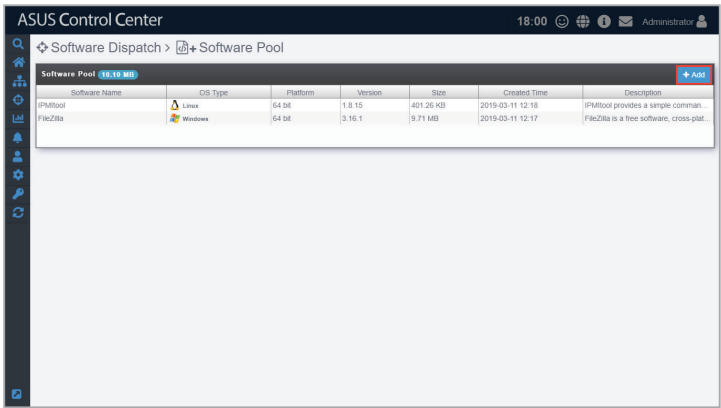
### 4.4.1 Software Pool

The Software Pool allows you to view all uploaded software packages. You may also add additional software packages or remove existing software packages from the Software Pool. The uploaded software packages will allow you to easily select and dispatch software to selected managed devices.



#### Adding software packages to the Software Pool

1. Click on Add.



2. Enter the name, OS type, version, platform and description of the software package, then click **Next**.

**Add Software Package**

Name: 7-Zip

OS Type: ☒ Windows ☐ Linux ☐ ADM

Version: 16.04.00.0

Platform: ☐ 32\_64Bit ☐ 32Bit ☒ 64Bit

Description: 7-Zip is a free and open-source file archiver, a utility used to place groups of files within compressed containers known as "archives".

Cancel Next

3. Add the script file by clicking on **Upload Script File** to select and upload a script file, or drag the script file into the **Script File** dotted square.

**NOTE:** For more information and examples of script files, please refer to <https://github.com/AsusControlCenter/Software-Dispatch-Guide>.

**Add Software Package**

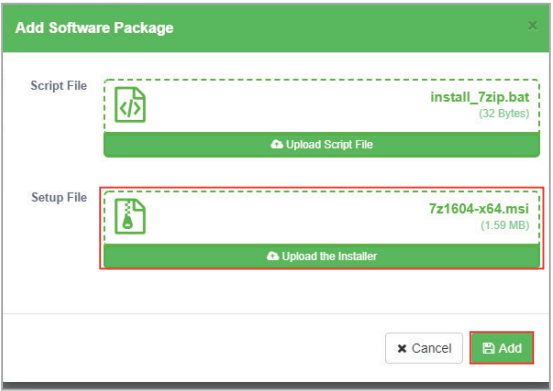
Script File: install\_7zip.bat (32 Bytes)  
Upload Script File

Setup File: 7z1604-x64.msi (1.59 MB)  
Upload the Installer

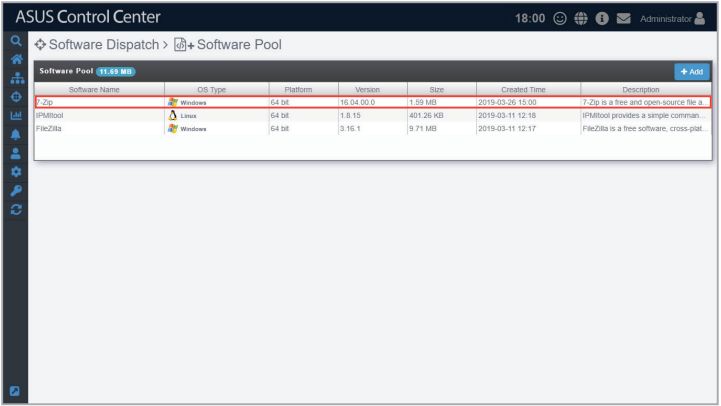
Cancel Add



4. Add the setup file by clicking on **Upload the Installer** to select and upload a setup file, or drag the setup file into the **Setup File** dotted square, then click on **Add**.

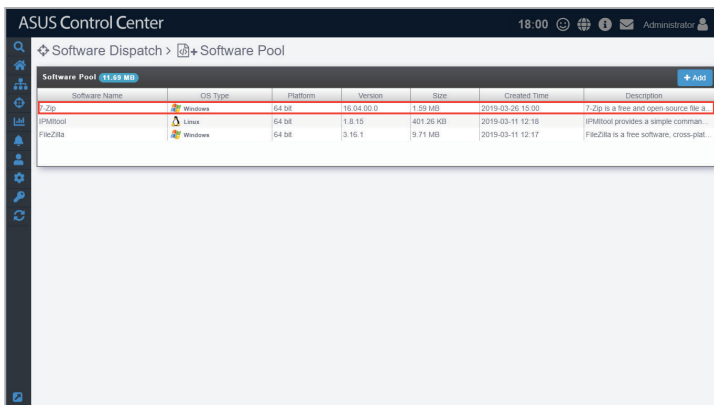


5. The newly added software package will appear in the Software Pool list.

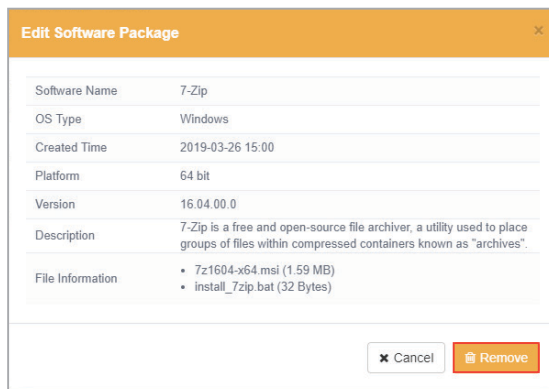


## Removing software packages from the Software Pool

1. Click on the software package you wish to remove in the Software Pool list.



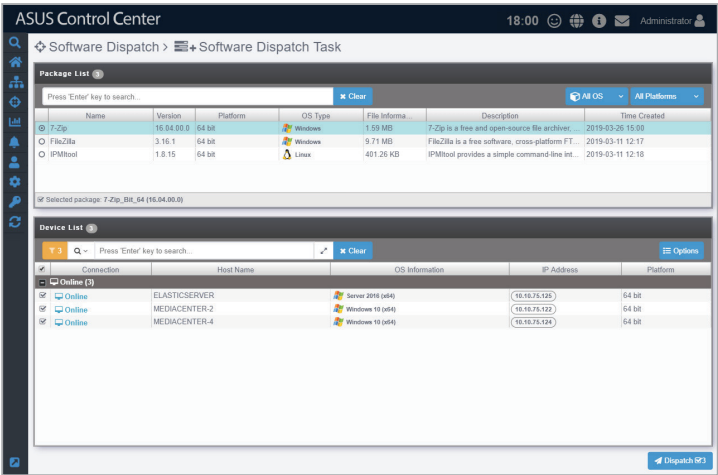
2. Click on **Remove** to remove the software package.



### 4.4.2 Software Dispatch Task

You can use Software Dispatch Task to dispatch software packages in the Software Pool to multiple managed devices to be installed in the background quickly and efficiently.

**NOTE:** To add or view software packages in the Software Pool, please refer to the **Software Pool** section.



## Dispatching software packages to devices

1. Select the software package you wish to dispatch from the Package List.

**NOTE:** You may filter the software packages by OS or platform by selecting the filter criteria from the drop down menus located to the right of the Search bar.

ASUS Control Center 18:00 Administrator

Software Dispatch > Software Dispatch Task

Package List

Press 'Enter' key to search. [Clear] [All OS] [All Platform]

| Name      | Version   | Platform | OS Type | File Info | Description                                        | Time Created     |
|-----------|-----------|----------|---------|-----------|----------------------------------------------------|------------------|
| 7-Zip     | 16.04.0.0 | 64 bit   | Windows | 1.59 MB   | 7-Zip is a free and open-source file archiver.     | 2019-03-26 15:50 |
| FileZilla | 3.16.1    | 64 bit   | Windows | 9.71 MB   | FileZilla is a free software, cross-platform FT... | 2019-03-11 12:17 |
| IPMTool   | 1.8.15    | 64 bit   | Linux   | 401.26 KB | IPMTool provides a simple command-line int...      | 2019-03-11 12:18 |

Selected package: 7-Zip\_16.04.0.0

Device List

Press 'Enter' key to search. [Clear] [Options]

| Connection | Host Name     | OS Information    | IP Address   | Platform |
|------------|---------------|-------------------|--------------|----------|
| Online     | ELASTICSERVER | Server 2016 (x64) | 10.10.75.123 | 64 bit   |
| Online     | MEDIACENTER-2 | Windows 10 (x64)  | 10.10.75.122 | 64 bit   |
| Online     | MEDIACENTER-4 | Windows 10 (x64)  | 10.10.75.124 | 64 bit   |

[Dispatch (F)]

2. When you select a software package, the managed devices you can dispatch the selected software package to will be displayed in the Devices List. Select the managed devices to dispatch the software package to from the Device List, then click **Dispatch**.

ASUS Control Center 18:00 Administrator

Software Dispatch > Software Dispatch Task

Package List

Press 'Enter' key to search. [Clear] [All OS] [All Platform]

| Name      | Version   | Platform | OS Type | File Info | Description                                        | Time Created     |
|-----------|-----------|----------|---------|-----------|----------------------------------------------------|------------------|
| 7-Zip     | 16.04.0.0 | 64 bit   | Windows | 1.59 MB   | 7-Zip is a free and open-source file archiver.     | 2019-03-26 15:50 |
| FileZilla | 3.16.1    | 64 bit   | Windows | 9.71 MB   | FileZilla is a free software, cross-platform FT... | 2019-03-11 12:17 |
| IPMTool   | 1.8.15    | 64 bit   | Linux   | 401.26 KB | IPMTool provides a simple command-line int...      | 2019-03-11 12:18 |

Selected package: 7-Zip\_16.04.0.0

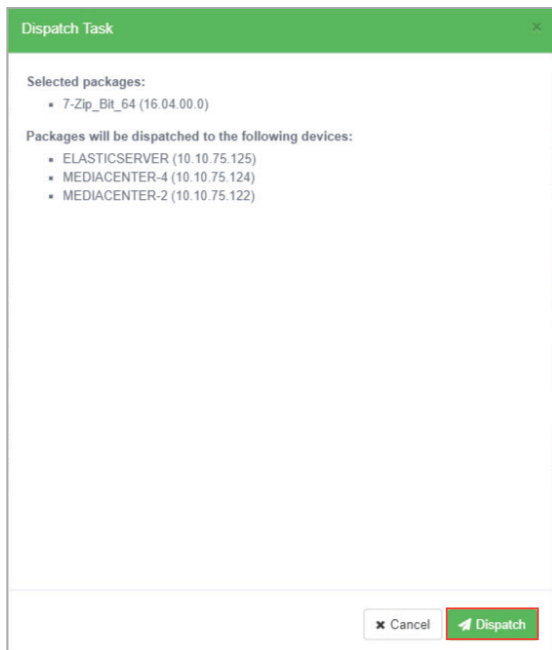
Device List

Press 'Enter' key to search. [Clear] [Options]

| Connection | Host Name     | OS Information    | IP Address   | Platform |
|------------|---------------|-------------------|--------------|----------|
| Online (3) | ELASTICSERVER | Server 2016 (x64) | 10.10.75.123 | 64 bit   |
| Online     | MEDIACENTER-2 | Windows 10 (x64)  | 10.10.75.122 | 64 bit   |
| Online     | MEDIACENTER-4 | Windows 10 (x64)  | 10.10.75.124 | 64 bit   |

[Dispatch (F)]

3. Confirm that the correct software package and managed devices are selected in the pop-up window, then click **Dispatch** to start dispatching the software to the managed devices.



4. After the software packages have been dispatched, you will be redirected to the Software Dispatch Task Report screen.

---

**NOTE:** For more details on the Software Dispatch Task Report, refer to the **Software Dispatch Task Report** section.

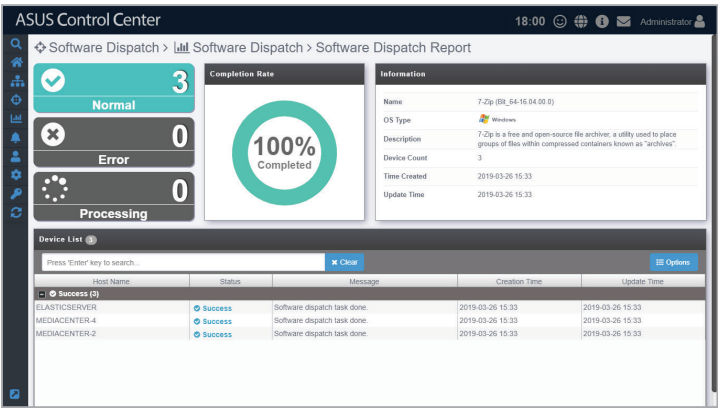
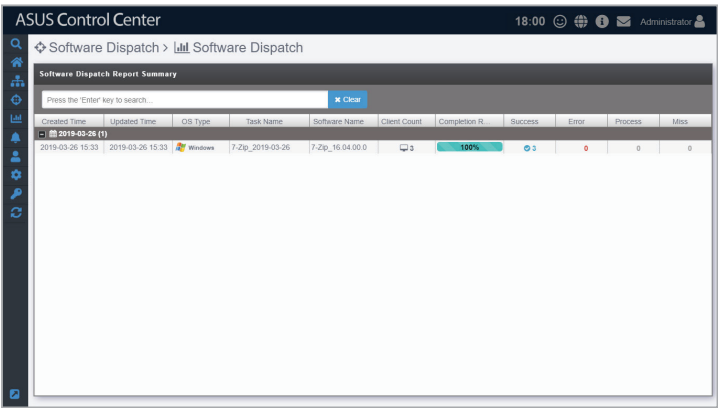
---

### 4.4.3 Software Dispatch Task Report

The **Software Dispatch Task Report** function will display a history of all software dispatch tasks performed using ASUS Control Center.

Selecting a software dispatch task listed in the Software Dispatch Report Summary will allow you to view information on the software, which devices the software was dispatched to, and also the status of the software dispatch to managed devices.

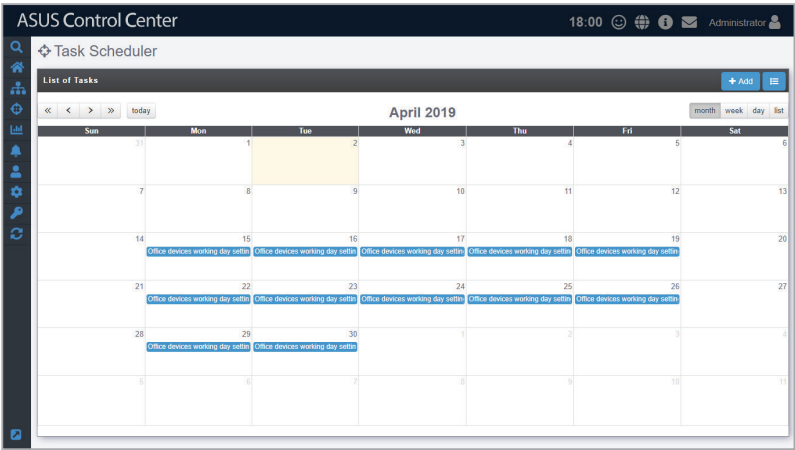
This provides you with a quick overview of your software dispatch tasks and also help you pinpoint failed software dispatches.



# 4.5 Task Scheduler

Schedule tasks for managed devices using the Task Scheduler. The tasks set can be executed automatically at specific times, or set to repeat periodically, which allows you to schedule tasks before hand or periodic tasks such as periodic reboot of managed devices.

To access **Task Scheduler**, click  > **Task Scheduler** in the left menu.



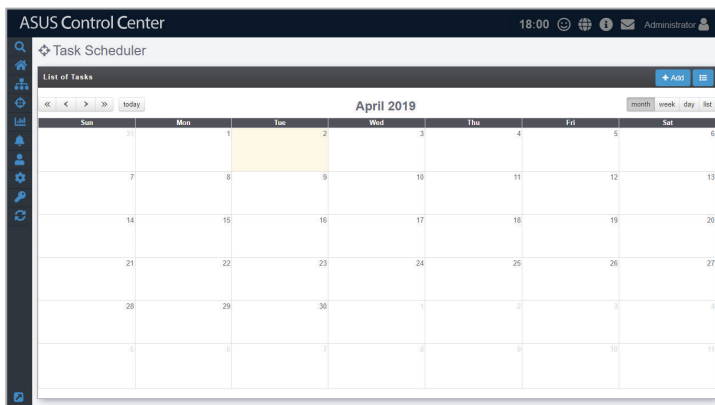
## Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

## Task Scheduler Overview

Toggle between the different Task Scheduler views by clicking on the  /  icon. You can click on any task displayed to view more details on the task.

 : Calendar view displays the tasks and the dates when they will be executed.



You can switch the time period displayed in Calendar view by using the following:



View previous year



View next year



View previous month / week / day



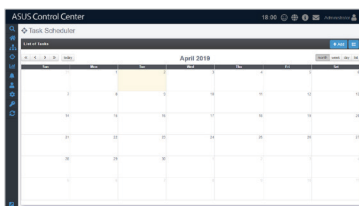
View next month / week / day



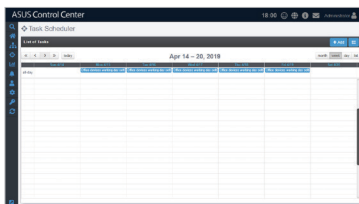
Move to the current day. The current day will be highlighted on the calendar.



Display month view



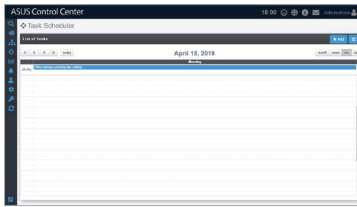
Display week view





day

Display day view

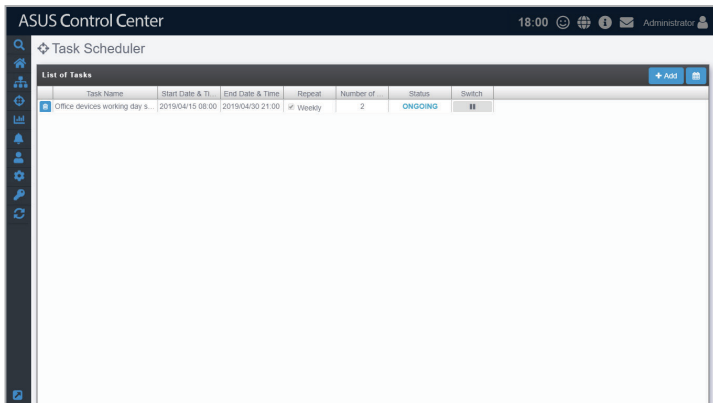


list

Display list of all tasks in the selected month and year.

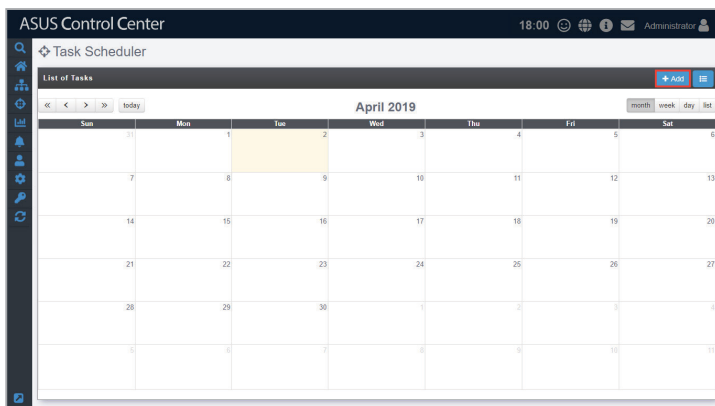


:History list of all tasks, including Task Name, Start Date & Time, End Date & Time, Repeat, Number of Clients, Status, and Switch.

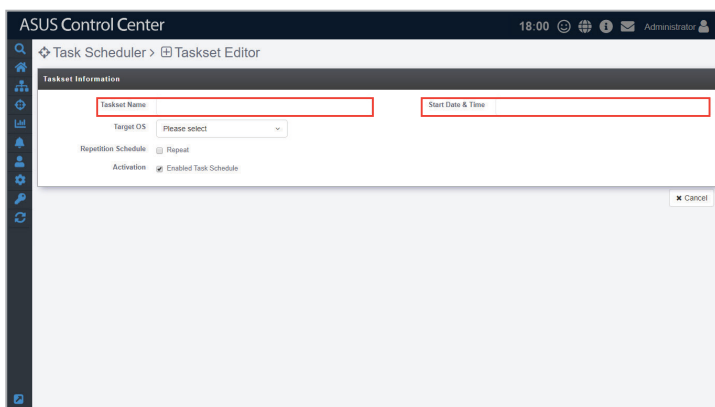


## Adding a scheduled task

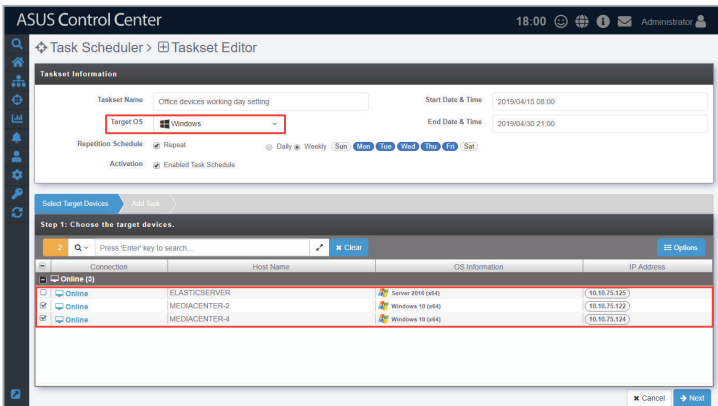
1. Click on **Add**.



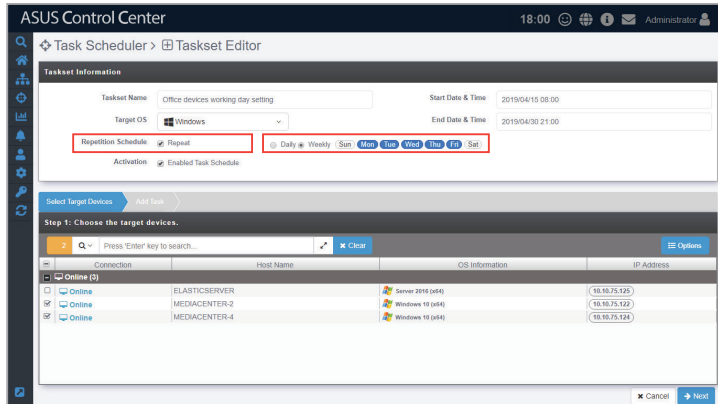
2. Enter the **Taskset Name**, then select a **Start Date & Time**.



3. Select **Windows** or **Linux** in the **Target OS** field to filter the target devices.



4. (optional) If you want to repeat the task, check **Repeat** in the **Repetition Schedule** field, then select **Daily** to repeat the task daily, or **Weekly** to repeat the task weekly. When you select **Weekly**, remember to select which days of the week you wish to repeat the task.



5. (optional) You may select an end date and time.

**NOTE:** The **End Date & Time** option only appears when **Repeat** has been checked.

ASUS Control Center 18:00 Administrator

Task Scheduler > Taskset Editor

**Taskset Information**

Taskset Name: Office devices working day setting

Target OS: Windows

Start Date & Time: 2019/04/15 08:00

End Date & Time: 2019/04/30 21:00

Repetition Schedule: ☒ Repeat ☐ Daily ☐ Weekly ☐ Monthly ☐ Yearly

Activation: ☒ Enabled Task Schedule

Select Target Devices Add Task

Step 1: Choose the target devices.

Press 'Enter' key to search... Clear Options

| Connection | Host Name     | OS Information    | IP Address   |
|------------|---------------|-------------------|--------------|
| Online (3) |               |                   |              |
| Online     | ELASTICSERVER | Server 2016 (x64) | 10.10.75.125 |
| Online     | MEDACENTER-2  | Windows 10 (x64)  | 10.10.75.122 |
| Online     | MEDACENTER-4  | Windows 10 (x64)  | 10.10.75.124 |

Cancel Next

6. **Enabled Task Schedule** is enabled by default, if you wish to disable the task, uncheck **Enabled Task Schedule** in the **Activation** field.

ASUS Control Center 18:00 Administrator

Task Scheduler > Taskset Editor

**Taskset Information**

Taskset Name: Office devices working day setting

Target OS: Windows

Start Date & Time: 2019/04/15 08:00

End Date & Time: 2019/04/30 21:00

Repetition Schedule: ☒ Repeat ☐ Daily ☐ Weekly ☐ Monthly ☐ Yearly

Activation: ☒ Enabled Task Schedule

Select Target Devices Add Task

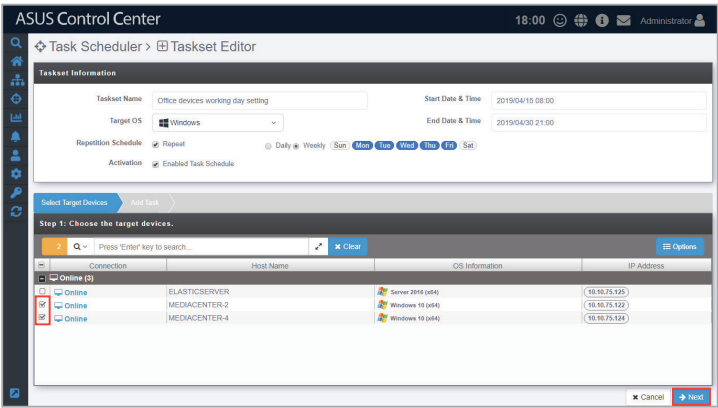
Step 1: Choose the target devices.

Press 'Enter' key to search... Clear Options

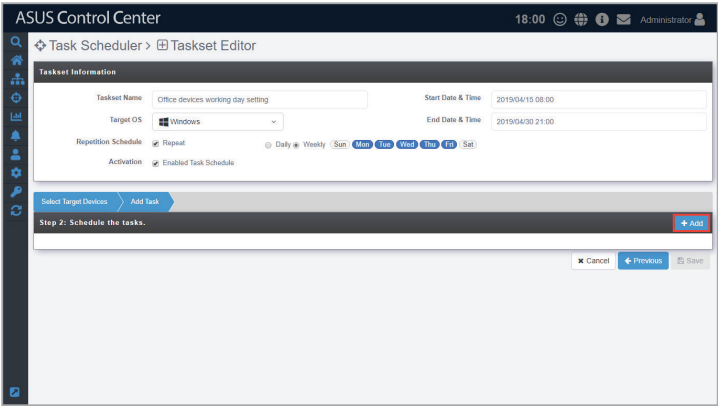
| Connection | Host Name     | OS Information    | IP Address   |
|------------|---------------|-------------------|--------------|
| Online (3) |               |                   |              |
| Online     | ELASTICSERVER | Server 2016 (x64) | 10.10.75.125 |
| Online     | MEDACENTER-2  | Windows 10 (x64)  | 10.10.75.122 |
| Online     | MEDACENTER-4  | Windows 10 (x64)  | 10.10.75.124 |

Cancel Next

7. A list of all managed devices matching the **Target OS** selected will be displayed. Select the managed devices to apply the task to, then click **Next**.



8. Click on **Add** in the middle-right of the screen to add a new task.



9. Select an **Action Type**. Each action type contains different options, see below for a list of the action types and the options available.

**NOTE:** Linux only supports **Power Control** and **Security** action types.

Power Control:

Add Task

Action Type

Power Control

Delay Time

0

Minute

The time that the task execution is delayed.

Power Action

Power On

Power Off

Power Reboot

Cancel

Save

| Action Type   | Options       | Description           |
|---------------|---------------|-----------------------|
| Power Control | Power On:     | Power on the device.  |
|               | Power Off:    | Power off the device. |
|               | Power Reboot: | Reboot the device.    |

Service Control:

Add Task

Action Type

Service Control

Delay Time

1

Minute

The time that the task execution is delayed.

Service Name

SNMPTRAP

Service Action

Start

Stop

Restart

Cancel

Save

| Action Type     | Options       | Description                                                                                                        |
|-----------------|---------------|--------------------------------------------------------------------------------------------------------------------|
| Service Control | Service Name: | Enter the name of the service. If you are unsure of the name of the service, refer to the <b>Software</b> section. |
|                 | Start:        | Activate the service.                                                                                              |
|                 | Stop:         | Stop the service.                                                                                                  |
|                 | Restart:      | Restart the service.                                                                                               |

Software Dispatch:

Add Task

Action Type

Software Dispatch

Delay Time

3

Minute

The time that the task execution is delayed.

Platform Type

32Bit64Bit32\_64Bit

Package Name

7-Zip

Cancel

Save

| Action Type       | Options        | Description                                                                                                                                      |
|-------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Software Dispatch | Platform Type: | Select from <b>32Bit</b> , <b>64Bit</b> , or <b>32_64Bit</b> to filter the software options.                                                     |
|                   | Package Name:  | Select an item from the <b>Software Pool</b> to be installed. The options will vary according to the Bit type selected in <b>Platform Type</b> . |

Security Control:

Add Task

Action Type

Security Control

Delay Time

1

Minute

The time that the task execution is delayed.

Security Type

USB Control

Status

EnableDisableRead Only

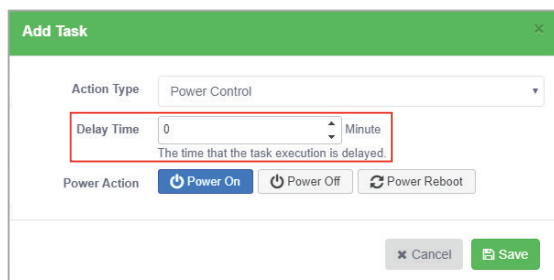
Cancel

Save

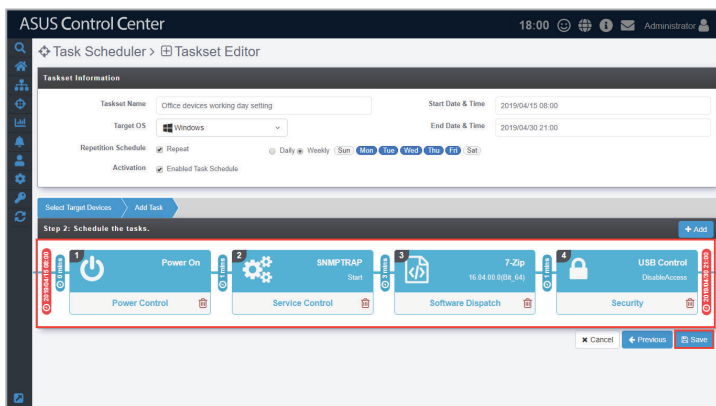
| Action Type      | Security Type     | Options        | Description                                       |
|------------------|-------------------|----------------|---------------------------------------------------|
| Security Control | USB Control       | Enable Access  | Allows USB ports to be accessed.                  |
|                  |                   | Disable Access | Do not allow USB ports to be accessed.            |
|                  |                   | Read Only      | Files on the USB storage device can only be read. |
|                  | WatchDog Function | Enable         | Enables Watchdog timer.                           |
|                  | Registry Tool     | Disable        | Disables Watchdog timer.                          |
|                  |                   | Enable         | Enable access to Regedit Tool.                    |
|                  |                   | Disable        | Disable access to Regedit Tool.                   |

- Set the **Delay Time** (in minutes). This function is used to set a delay time before the task is executed.

**CAUTION:** When adding multiple tasks, ensure to set a Delay Time for each task to ensure the tasks are executed properly.



- Once you have finished with setting the task, click on **Save**. The newly added task will be displayed in a timeline, you may click and drag the items in the timeline to rearrange the scheduled tasks. Clicking on  will delete the task.
- When you are finished, click on the **Save** at the bottom of the screen.





## **Editing a scheduled task**

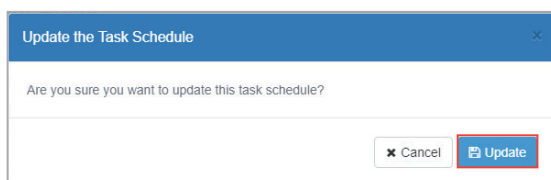
1. Click on the task you wish to edit on the calendar in Calendar view.  
OR  
Click on the task you wish to edit from the list in History view.
2. Edit the details then click **Update** at the bottom of the screen when you have finished editing.

---

**NOTE:** You can refer to step 2 to 12 of the **Add Scheduled task** under the **Task Scheduler** section for the steps on editing a task; the steps are the same.

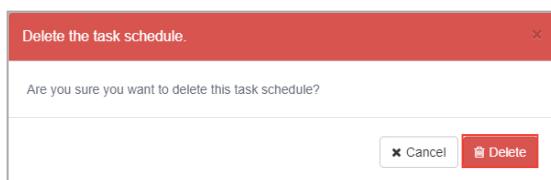
---

3. Click **Update** on the pop-up window to confirm the changes made.



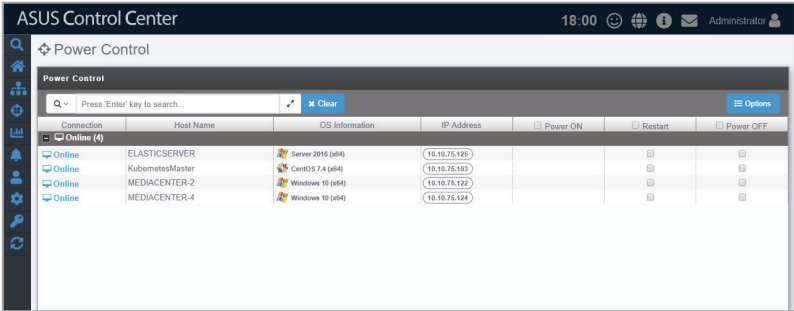
## **Deleting a scheduled task**

1. Click on the task you wish to edit on the calendar in Calendar view.  
OR  
Click on the task you wish to edit from the list in History view.
2. Click **Delete** at the bottom of the screen, then click **Delete** on the pop-up window to delete the scheduled task.



## 4.6 Power Control

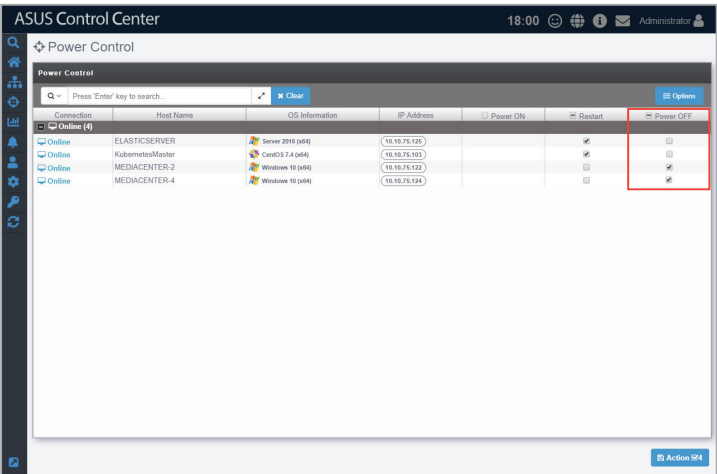
Power Control allows you to control the power settings of managed devices all from a centralized location. The centralized control over the power settings for managed devices makes it so that you do not have to manually power off, power on, or restart each managed device individually.



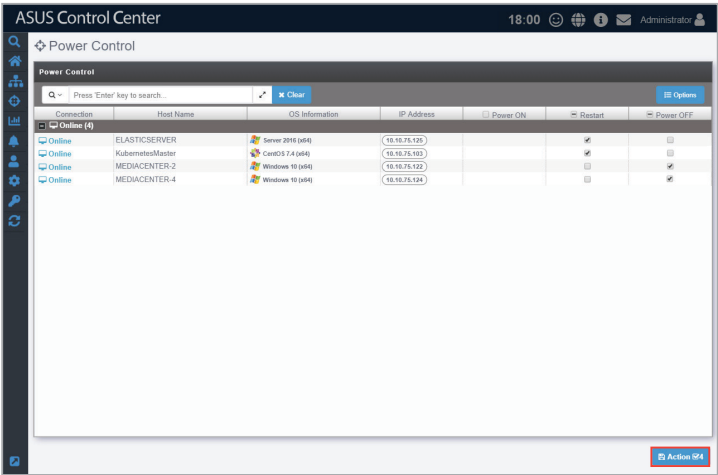
To power on / power off / restart device(s):

1. Check the **Power ON** / **Power OFF** / **Restart** check boxes of devices you would like to power on / power off / restart, or you may check the column title to check all devices eligible for the chosen action.

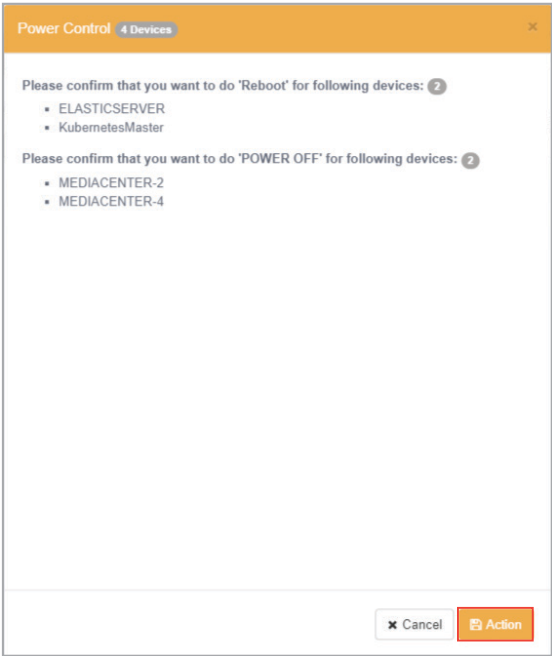
**NOTE:** The availability of the **Power ON**, **Power OFF**, and **Restart** check boxes will vary according to the current power status of the managed device.



2. Click **Action** in the lower right of the screen to perform the chosen action(s).



3. Click **Action** when prompted.



## 4.7 Firmware Management

Firmware Management allows you to manually update the BIOS, NIC, or DPU firmware of managed Redfish devices.

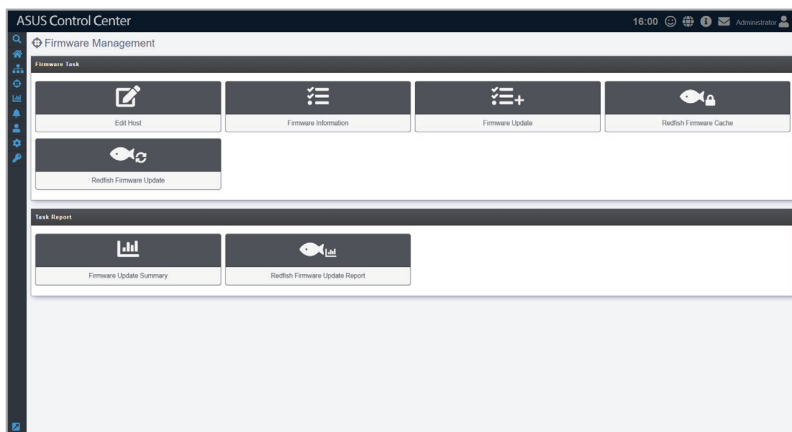
The **Redfish Firmware Cache** and **Redfish Firmware Update** functions allow you to initiate out-of-band firmware updates using Redfish.

The **Edit Host**, **Firmware Information**, and **Firmware Update** functions allow you to initiate firmware updates via the operating system, in cases where the firmware cannot be updated using Redfish.

---

**NOTE:** Firmware Management supports Redfish devices running Linux-based operating systems. Refer to the **System Requirements** section of the **Appendix** chapter for more information.

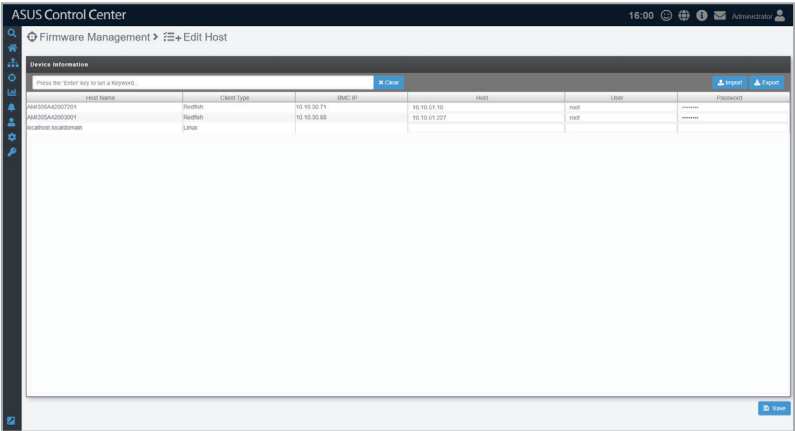
---



# 4.7.1 Edit Host

This page allows you to edit the host list for firmware management.

**NOTE:** Redfish devices must be added using the **Add Redfish** function in order to be displayed here. Refer to the **Add Redfish** section of the **Deployment** chapter for more information.



## Scanning for devices

**NOTE:** You can also click **Export** to export the host list as a .csv file, edit the host list in an external program, then click **Import** to load the edited .csv file.

1. In the Host, User, and Password columns, enter the IP address, username, and password of the Linux OS host.
2. Click **Save**.
3. Check the **Firmware Update Summary** page to see if the scan was successful.

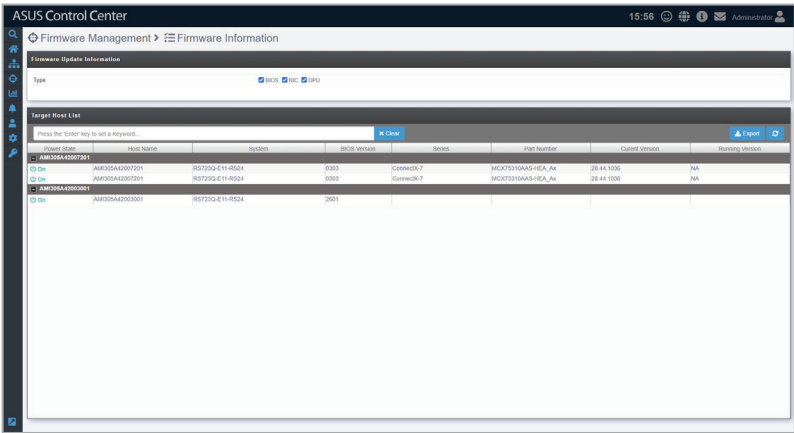
## Adding groups

Click **Add Group**, then enter a group name and click **Add**.

## 4.7.2      Firmware Information

This page shows the firmware information of devices that have been successfully scanned using the **Edit Host** page.

**NOTE:** To scan for additional devices, refer to the **Edit Host** section.



### **Filtering the firmware information list by firmware update type**

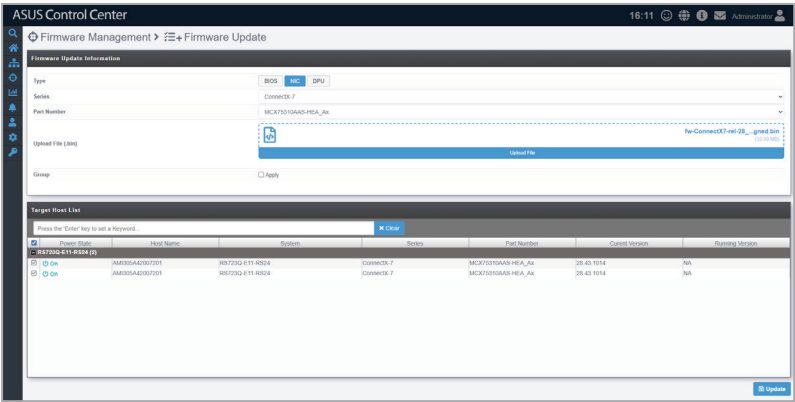
Use the checkboxes in the **Firmware Update Information** block to only show entries matching the selected firmware update types.

### **Using the search bar and search options**

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

### 4.7.3      Firmware Update

This page allows you to upload BIOS, NIC, and DPU firmware packages and manually update device firmware.

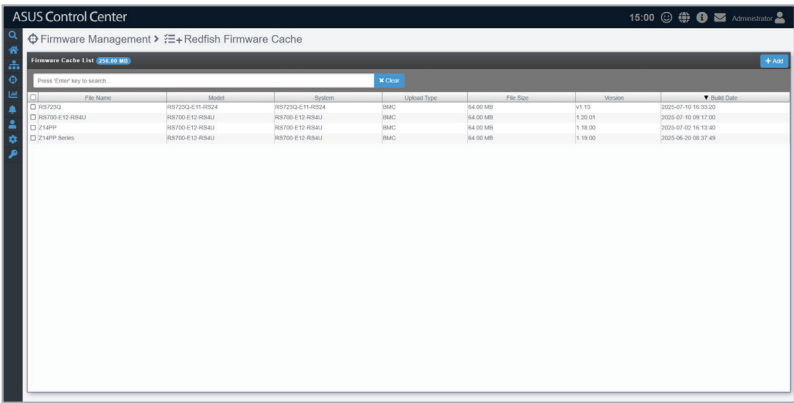


#### Initiating a firmware update

1. Fill in the fields in the **Firmware Update Information** block and upload a firmware package.
2. Select one or more devices from the **Target Host List** block.
3. Click **Update**, then type “Yes” when prompted.

### 4.7.4 Redfish Firmware Cache

This page allows you to upload BIOS and BMC firmware packages for use with the **Redfish Firmware Update** function.



#### Uploading a firmware package

1. Click **Add** and fill in the Name, Type, System, Version, and Description fields, then click **Next**.
2. Upload the Update/OEM parameters (as JSON files) and firmware package files, then click **Add**.

Add Firmware Package

Name

R72324113\_1

Type

☒ BMC

☐ BIOS

System

RS723Q-E11-RS24

Version

1

Description

Cancel

Next

Add Firmware Package

UpdateParameters

parameters.json

(73 bytes)

Upload JSON File

OemParameters

oem\_parameters.json

(22 bytes)

Upload JSON File

UpdateFile

R72324113\_1.ima

(84.00 MB)

Upload File

Cancel

Add

#### Removing a firmware package

1. Select one or more firmware packages and click **Remove**, then confirm the removal when prompted.

4-54



## 4.7.5 Redfish Firmware Update

This page allows you to initiate an out-of-band firmware update using Redfish.

ASUS Control Center

15:12

Firmware Management > Redfish Firmware Update

Firmware Update Information

Type: **BMC** | BIOS

System: R200TA-E12-R200U

Upload Type: **Locally** | Remotely

Firmware Cache List: Please Select...

Preserve Configuration: ☐ Enable ☒ Disable

Target Host List

Enter the "Host" key to set a keyword

Update

| Host Name          | Client Type | Model Name       | System           | BMC Version |
|--------------------|-------------|------------------|------------------|-------------|
| <b>Online (2)</b>  |             |                  |                  |             |
| JAN1070261000000   | Redfish     | R200TA-E12-R200U | R200TA-E12-R200U | 1.02.29     |
| JAN1070261000000   | Redfish     | R200TA-E12-R200U | R200TA-E12-R200U | 1.02.29     |
| <b>Offline (1)</b> |             |                  |                  |             |
| JAN1070261000000   | Redfish     | R200TA-E12-R200U | R200TA-E12-R200U | 1.02.29     |

### Updating BMC firmware

1. Select **BMC** in the **Firmware Update Information** block, then select a system and upload type.
2. If the **Upload Type** is set to **Remotely**, select a protocol and enter the address of the image in the **Protocol** and **Image URI** fields.
3. Select an update package from the **Firmware Cache List** dropdown menu.
4. To preserve existing configuration settings, tick the **Preserve Configuration** checkbox and the individual checkboxes for each type of configuration setting.
5. Select one or more devices in the **Target Host List** block and click **Update**.
6. Check the **Redfish Firmware Update Report** page to see if the scan was successful.

### Updating BIOS firmware

1. Select **BIOS** in the **Firmware Update Information** block, then select a system and upload type.
2. Select an update package from the **Firmware Cache List** dropdown menu.
3. Select one or more devices in the **Target Host List** block and click **Update**.
4. Check the **Redfish Firmware Update Report** page to see if the scan was successful.

### 4.7.6      Firmware Update Summary

This page allows you to view the firmware update history.

ASUS Control Center

16:30

Firmware Management > Firmware Update Summary

Firmware Update Summary

Please the Enter key to search.

Clear

Export

| Start Time          | End Time            | Action | Firmware Type | Completion Rate | Success | Error | Processing |
|---------------------|---------------------|--------|---------------|-----------------|---------|-------|------------|
| 2025-03-14 (3)      |                     |        |               |                 |         |       |            |
| 2025-03-14 15:12:51 | 2025-03-14 16:16:01 | Update | BIOS          | 100%            | 1       | 0     | 0          |
| 2025-03-14 16:06:00 | 2025-03-14 16:06:00 | Update | BIOS          | 100%            | 1       | 0     | 0          |
| 2025-03-11 (1)      |                     |        |               |                 |         |       |            |
| 2025-03-07 (4)      |                     |        |               |                 |         |       |            |
| 2025-03-06 (3)      |                     |        |               |                 |         |       |            |
| 2025-03-04 (20)     |                     |        |               |                 |         |       |            |
| 2025-03-04 (17)     |                     |        |               |                 |         |       |            |

#### Viewing detailed firmware update information

Click an entry in the **Firmware Update Summary** block to view detailed information about the selected firmware task.

### 4.7.7      Redfish Firmware Update Report

This page allows you to view the firmware update history.

ASUS Control Center

16:50

Firmware Management > Redfish Firmware Update Report

Redfish Firmware Update Summary

Please the Enter key to search.

Clear

Export

| Created             | Update Time         | Type | Client Count | Completion Rate | Success | Error | Processing |
|---------------------|---------------------|------|--------------|-----------------|---------|-------|------------|
| 2025-07-22 (3)      |                     |      |              |                 |         |       |            |
| 2025-07-22 15:32:34 | 2025-07-22 15:35:20 | BIOS | 1            | 100%            | 1       | 0     | 0          |
| 2025-07-22 15:31:24 | 2025-07-22 15:34:10 | BIOS | 1            | 100%            | 1       | 0     | 0          |
| 2025-07-16 (7)      |                     |      |              |                 |         |       |            |
| 2025-07-16 09:32:03 | 2025-07-16 09:34:06 | BIOS | 1            | 100%            | 0       | 1     | 0          |
| 2025-07-16 09:16:36 | 2025-07-16 09:16:36 | BIOS | 1            | 100%            | 0       | 1     | 0          |
| 2025-07-16 09:17:45 | 2025-07-16 09:17:45 | BIOS | 1            | 100%            | 0       | 1     | 0          |
| 2025-07-16 09:18:29 | 2025-07-16 09:18:29 | BIOS | 1            | 100%            | 0       | 1     | 0          |
| 2025-07-16 09:21:00 | 2025-07-16 09:21:00 | BIOS | 1            | 100%            | 0       | 1     | 0          |
| 2025-07-16 16:34:34 | 2025-07-16 16:34:34 | BIOS | 1            | 100%            | 0       | 1     | 0          |
| 2025-07-16 16:37:19 | 2025-07-16 16:48:09 | BIOS | 1            | 100%            | 1       | 0     | 0          |
| 2025-07-15 (1)      |                     |      |              |                 |         |       |            |
| 2025-07-02 16:14:23 | 2025-07-02 16:15:36 | BIOS | 1            | 100%            | 0       | 1     | 0          |
| 2025-06-26 (2)      |                     |      |              |                 |         |       |            |

#### Viewing detailed firmware update information

Click an entry in the **Redfish Firmware Update Summary** block to view detailed information about the selected firmware task.

# Chapter 5

This chapter describes the various reports ASUS Control Center generates from tasks, software, and hardware related subscriptions.

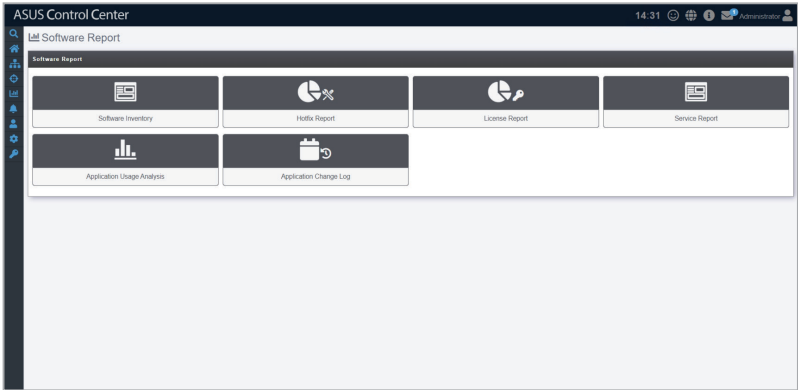
# Report

# 5.1 Software Report

**NOTE:** The information entered in this section is for reference only.

Software Report allows you to manage your report subscriptions on the applications installed on added devices. You may also customize which applications to receive reports on, as well as pinpoint applications which meet the rules you set, allowing you to efficiently manage high-priority applications and ignore applications which may not require much maintenance.

To access **Software Report**, click  in the left menu, then click on **Software Report**.



## Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

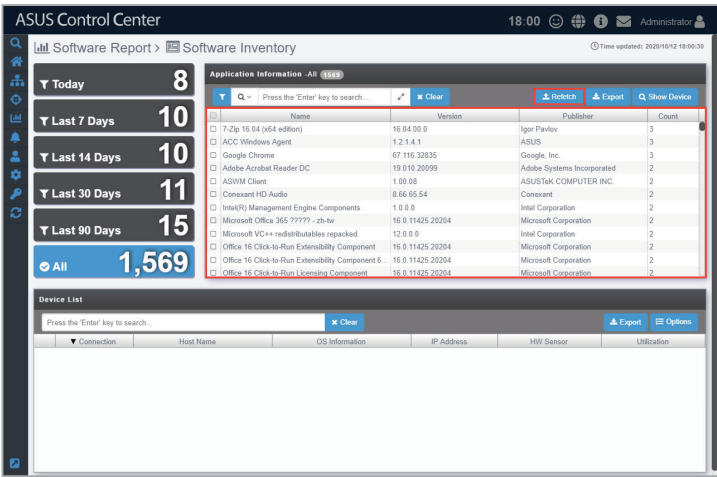
### 5.1.1 Software Inventory

Through **Software Inventory** you may view all the installed applications on all managed devices or filter through the applications installed on managed devices, providing you with a quick way to periodically keep track of new applications installed and the devices they are installed on.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.

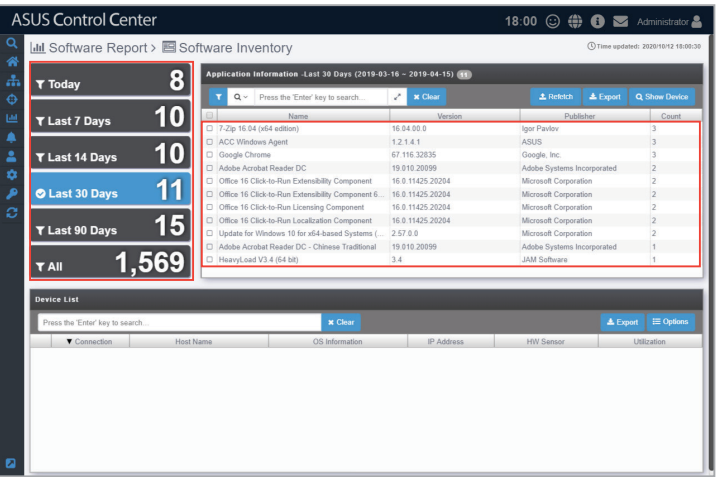
**Refetch Application**

Click on **Refetch** to request agents to return an immediate update the list of installed applications on all managed devices, making sure all the information displayed is up to date.



**Filter newly installed applications**

To quickly filter newly installed applications within a time period, click on the **Today**, **Last 7 Days**, **Last 14 Days**, **Last 30 Days**, **Last 90 Days** or **All** time period filters located on the left of the screen. This will help you in periodically reviewing the applications installed within a selected time period.



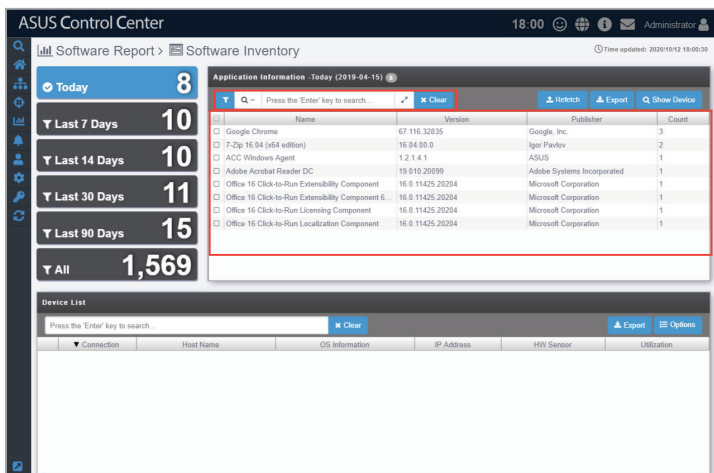
## Search for applications using keywords

Entering keywords into the search bar will display all installed applications which contain the keywords entered, allowing you to pinpoint certain applications and help you keep track of the amount of devices these applications are installed on as well as view which devices the applications are installed on. You may also view the device information as well as view all applications on the device to make sure your application information is correct.

1. Enter the keywords you wish to search for using the following methods:

- Directly entering the keywords

Enter the keyword(s) you wish to search with into the search bar and press <Enter>. Click on  to toggle between searching with the **AND** operator or **OR** operator. Searching using **AND** will search for items which contain all keywords entered, whilst searching using **OR** will search for items which contain at least one of the keywords entered.



ASUS Control Center

18:00 Administrator

Software Report > Software Inventory

Time updated: 2020/10/12 18:00:30

Application Information - Today (2019-04-15)

Search:  

| Name                                                | Version          | Publisher                  | Count |
|-----------------------------------------------------|------------------|----------------------------|-------|
| Google Chrome                                       | 67.116.320.35    | Google, Inc.               | 3     |
| 7-Zip 16.04 (64 edition)                            | 16.04.00.0       | Igor Pavlov                | 2     |
| ACC Windows Agent                                   | 1.2.1.4.1        | ASUS                       | 1     |
| Adobe Acrobat Reader DC                             | 19.010.20099     | Adobe Systems Incorporated | 1     |
| Office 16 Click-to-Run Extensibility Component      | 16.0.11425.20204 | Microsoft Corporation      | 1     |
| Office 16 Click-to-Run Extensibility Component 6... | 16.0.11425.20204 | Microsoft Corporation      | 1     |
| Office 16 Click-to-Run Licensing Component          | 16.0.11425.20204 | Microsoft Corporation      | 1     |
| Office 16 Click-to-Run Localization Component       | 16.0.11425.20204 | Microsoft Corporation      | 1     |

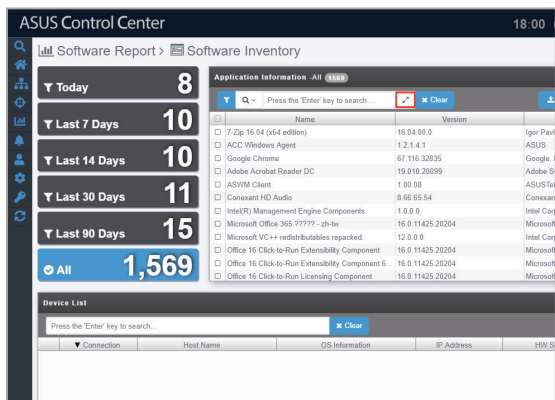
Device List

Press the Enter key to search.

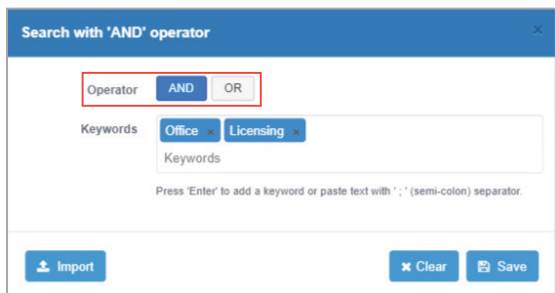
| Connection | Host Name | OS Information | IP Address | HW Sensor | Utilization |
|------------|-----------|----------------|------------|-----------|-------------|
|------------|-----------|----------------|------------|-----------|-------------|

- Importing multiple keywords from a .csv file

a. Click on  to bring up the search condition pop-up window.



b. Select the operator you wish to use. **AND** will search for items which contain all the keywords entered, whilst **OR** will search for items which contain at least one of the keywords entered.



- c. Enter the keyword(s) you wish to search with into the **Keywords** field and press <Enter>.

Search with 'AND' operator

Operator: **AND** OR

Keywords: **Office**, **Licensing**

Keywords

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import Clear Save

Import multiple keywords using a .csv file by click on **Import**, selecting the .csv file you wish to import, and then selecting the column in the .csv file you would like to import.

Search with 'OR' operator

Operator: **AND** OR

Keywords: Keywords

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import Clear Save

Open

File name: Software Inventory Keyword.csv

Open Cancel

Import

Please select the field that you want to import from the csv file.

Name

Cancel OK



- d. Click on **Save** once you have finished setting the search conditions.

Search with 'AND' operator

Operator: **AND** OR

Keywords: Office Acrobat

Keywords

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import Clear Save

2. If you wish to view the devices an application is installed on, check the application, then click on **Show Device**. The list of devices the selected application is installed on should be displayed in the **Device List** window

ASUS Control Center 18:00 Administrator

Software Report > Software Inventory Time updated: 2020/10/12 18:08:38

Today 8

Last 7 Days 10

Last 14 Days 10

Last 30 Days 11

Last 90 Days 15

All 1,569

Application Information - Today (2019-04-15)

Press the Enter key to search...

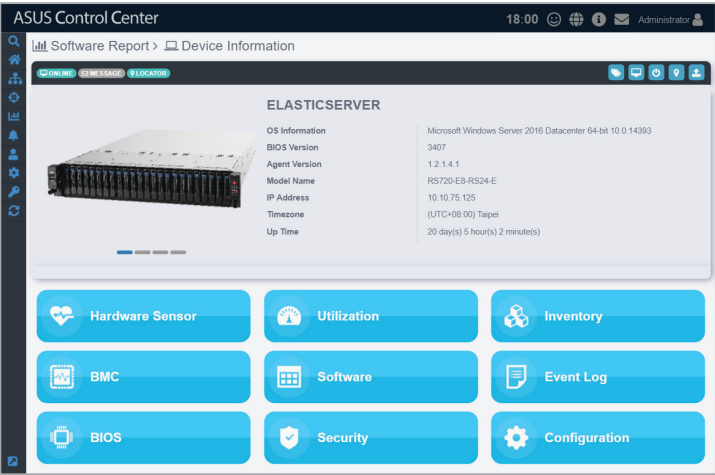
| Name                                             | Version          | Publisher                  | Count |
|--------------------------------------------------|------------------|----------------------------|-------|
| Google Chrome                                    | 73.0.3683.103    | Google, Inc.               | 3     |
| 7-Zip 16.04 (64-bit edition)                     | 16.04.00.0       | Igor Pavlov                | 2     |
| ACC Windows Agent                                | 1.2.1.4.1        | ASUS                       | 1     |
| Adobe Acrobat Reader DC                          | 19.010.20099     | Adobe Systems Incorporated | 1     |
| Office 16 Click-to-Run Extensibility Component   | 16.0.11425.20204 | Microsoft Corporation      | 1     |
| Office 16 Click-to-Run Extensibility Component 6 | 16.0.11425.20204 | Microsoft Corporation      | 1     |
| Office 16 Click-to-Run Licensing Component       | 16.0.11425.20204 | Microsoft Corporation      | 1     |
| Office 16 Click-to-Run Localization Component    | 16.0.11425.20204 | Microsoft Corporation      | 1     |

Device List

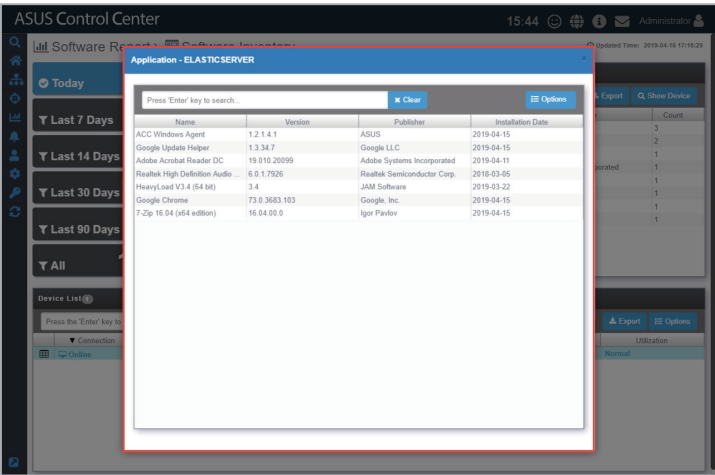
Press the Enter key to search...

| Connection | Host Name     | OS Information    | IP Address  | HW Sensor | Utilization |
|------------|---------------|-------------------|-------------|-----------|-------------|
| Online     | ELASTICSERVER | server 2019 (x64) | 10.10.10.10 | Normal    | Normal      |

3. (optional) Clicking on  next to each device in the **Device List** will allow you to view the Device Information.



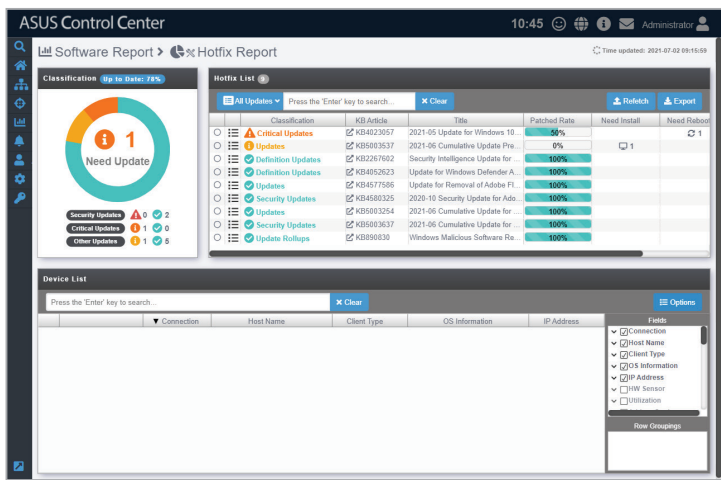
4. (optional) Clicking on the device will display all applications on the selected device.



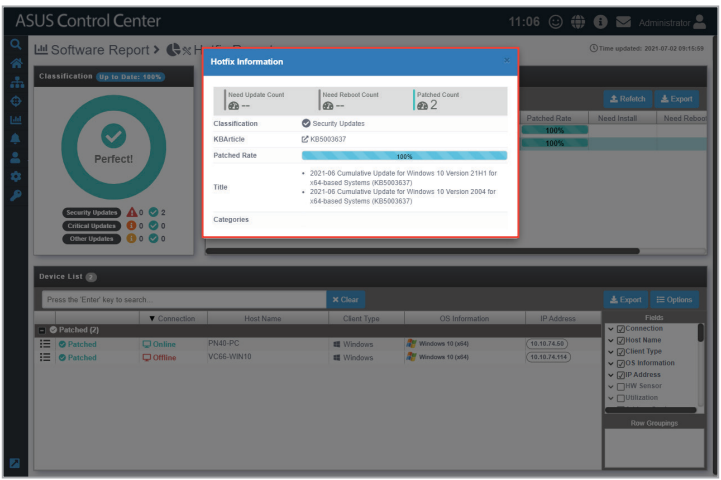
### 5.1.2 Hotfix Report (Windows only)

**Hotfix Report** allows you to view or filter through hotfix updates on all managed Windows devices, helping you pinpoint managed Windows devices that require an immediate hotfix update.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.

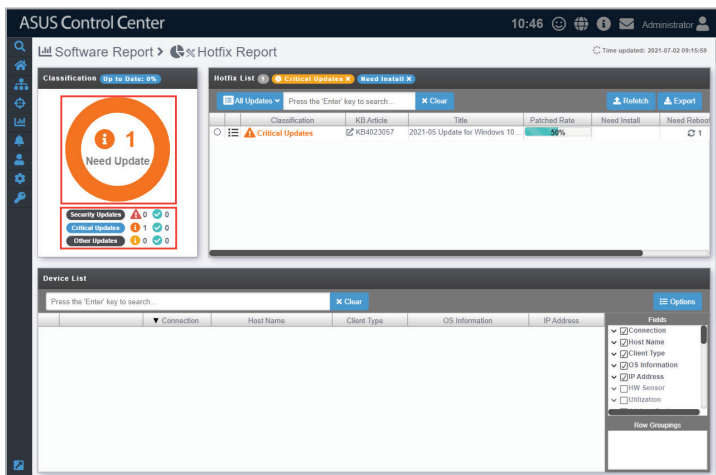


Clicking on  next to a hotfix update in the Hotfix List will allow you to view more details on the hotfix.



## Filtering hotfixes using Classification

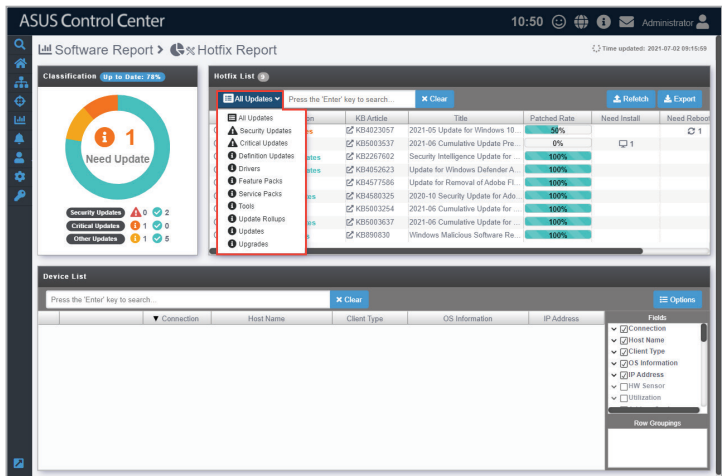
You can quickly filter hotfixes according to **Security Updates**, **Critical Updates**, or **Other Updates** by clicking on the respective item in the **Classification** block. This allows you to view the update statuses for the selected classification at a glance and give your attention to the hotfixes that still need to be updated. Alternatively, you can also filter the hotfixes by clicking on the overview circle allowing you to filter by hotfix updates successfully installed and those that still require your attention.



To clear the filter results, click on **Clear** in the Hotfix List block.

### Filtering hotfixes using Hotfix List

You can filter the Hotfix List according to the different categories provided in the drop down menu. To select a filter, click on the **All Updates** drop down menu, then select a category to filter by.



To clear the filter results, click on **Clear** in the Hotfix List block.

## Viewing devices the hotfix was applied to

Clicking on a hotfix update in the Hotfix List will list the managed devices the hotfix was applied to in the Device List below. This will allow you to better manage hotfix updates, and also manage issues with hotfix updates on managed devices, such as unsuccessful or pending hotfixes for individual devices.

The screenshot shows the ASUS Control Center interface. The top navigation bar includes 'Software Report' and 'Hotfix Report'. The 'Hotfix Report' section displays a 'Classification' summary on the left with a 'Perfect!' status and a 'Hotfix List' table on the right. The table lists security updates with columns for Classification, KB/Article, Title, Patched Rate, Need Install, and Need Reboot. Two updates are listed, both with a 100% patched rate. Below the Hotfix List is the 'Device List' section, which shows a table of managed devices with columns for Patched (P), Connection, Host Name, Client Type, OS Information, and IP Address. Two devices are listed: PN40-PC and VC66-WIN10. A sidebar on the right contains a 'Filter' menu with options like Connection, Host Name, Client Type, OS Information, IP Address, and Utilization. The bottom of the interface shows a 'Device Information' section for the selected device, PN40-PC, displaying OS Information, BIOS Version, Agent Version, Model Name, IP Address, Timezone, and Up Time. Below this are several blue buttons for 'Hardware Sensor', 'Utilization', 'Inventory', 'Software', 'Event Log', 'BIOS', 'Security', and 'Configuration'.

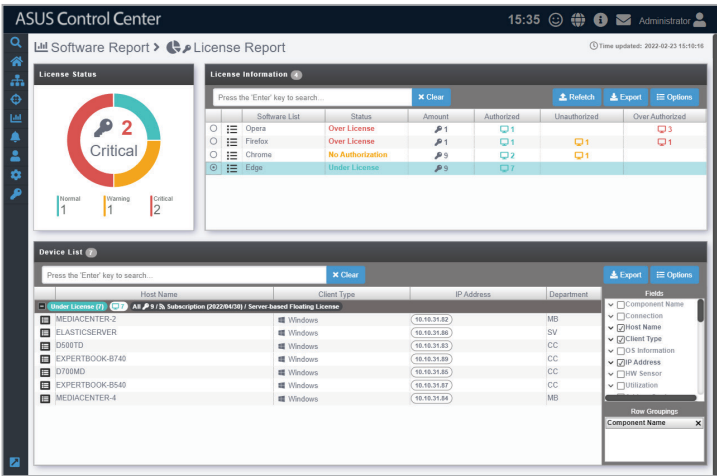
You may also click on  next to each device in the **Device List** to view the Device Information.

The screenshot shows the ASUS Control Center interface with the 'Device Information' section selected. The top navigation bar includes 'Software Report' and 'Device Information'. The 'Device Information' section displays a 'PN40-PC' device with a status of 'ONLINE'. The device information is organized into two columns: 'OS Information' and 'Microsoft Windows 10 Pro 64-bit 10.0.19043'. The 'OS Information' column lists BIOS Version, Agent Version, Model Name, IP Address, Timezone, and Up Time. The 'Microsoft Windows 10 Pro 64-bit 10.0.19043' column lists the OS version, build number, and release date. Below the device information are several blue buttons for 'Hardware Sensor', 'Utilization', 'Inventory', 'Software', 'Event Log', 'BIOS', 'Security', and 'Configuration'.

### 5.1.3 License Report

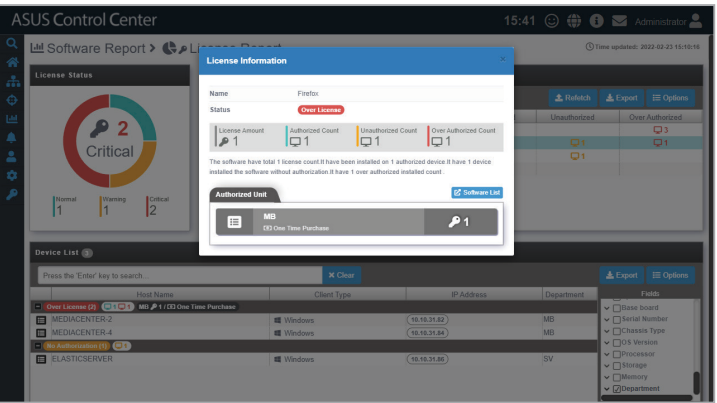
**License Report** allows you to view the total amount of licenses for each software and on which managed devices they are installed on. This allows you to compare and ensure that the number of licenses authorized and the amount of total licenses match up.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.



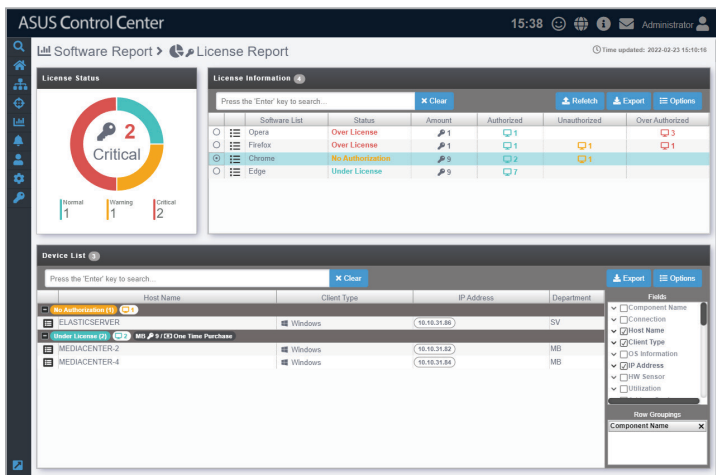
### Viewing information on the license

Click on  next to a selected license to view more information about the license.



### Viewing devices the software was installed on

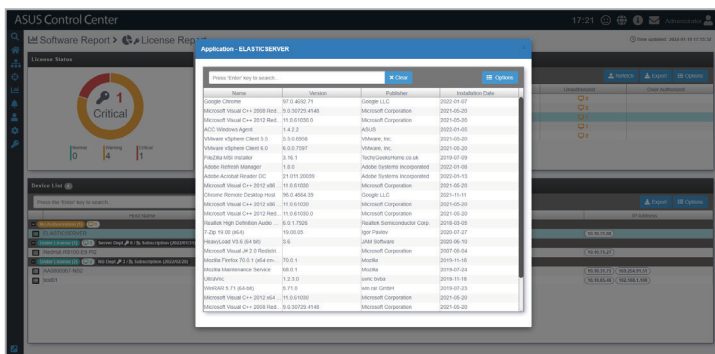
Clicking on a software in the License Information list will display all the managed devices the software is installed on, and also allows you to check which managed devices have the software installed without authorization, as well as the managed devices which have the appropriate license for the software.



**NOTE:**

- **Under License:** Sufficient licenses available and all software uses are authorized.
- **No Authorization:** Sufficient licenses available but some software uses are unauthorized.
- **Over License:** Insufficient licenses and some software uses are unauthorized.

You may also click on  next to each device in the **Device List** to view all the softwares installed on the selected device.

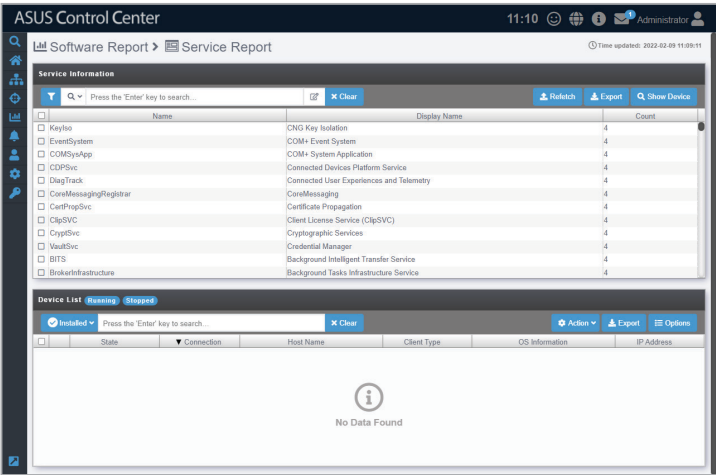




### 5.1.4 Service Report

**Service Report** allows you to view the services currently running on all managed devices, and also allows you to view the managed devices running a specific service.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.



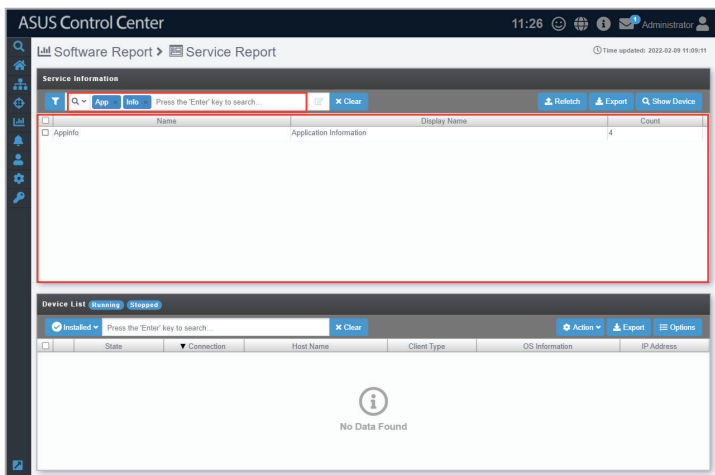
## Search for services using keywords

Entering keywords into the search bar will display all services which contain the keywords entered, allowing you to pinpoint certain services and help you keep track of the amount of devices these services are available on as well as view these devices.

1. Enter the keywords you wish to search for using the following methods:

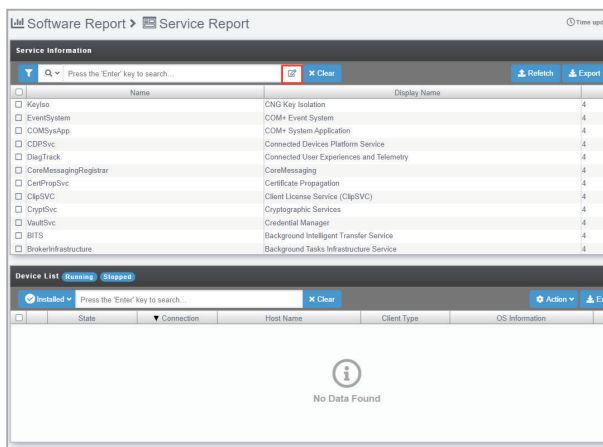
- Directly entering the keywords

Enter the keyword(s) you wish to search with into the search bar and press <Enter>. Click on  to toggle between searching with the **AND** operator or **OR** operator. Searching using **AND** will search for items which contain all keywords entered, whilst searching using **OR** will search for items which contain at least one of the keywords entered.

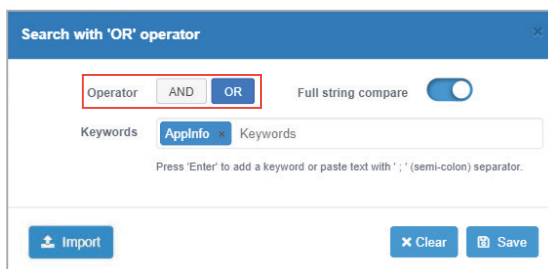


- Importing multiple keywords from a .csv file

- a. Click on  to bring up the search condition pop-up window.



- b. Select the operator you wish to use. **AND** will search for items which contain all the keywords entered, whilst **OR** will search for items which contain at least one of the keywords entered.



- c. Enter the keyword(s) you wish to search with into the **Keywords** field and press <Enter>.

Search with 'OR' operator

Operator: AND OR Full string compare: ☒

Keywords: AppInfo Keywords

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import Clear Save

Import multiple keywords using a .csv file by click on **Import**, selecting the .csv file you wish to import, and then selecting the column in the .csv file you would like to import.

Search with 'OR' operator

Operator: AND OR Full string compare: ☒

Keywords: AppInfo Keywords

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import Clear Save

Import

Please select the field that you want to import from the csv file.

Name

Cancel OK

- d. Click on **Save** once you have finished setting the search conditions.

Search with 'OR' operator

Operator

ANDOR

Full string compare

Keywords

AppInfo

Keywords

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import

Clear

Save

2. If you wish to view the devices a service is available on, check the service, then click on **Show Device**. The list of devices the selected service is available on should be displayed in the **Device List** window.

**NOTE:** You can also click on  to quickly deselect services already selected.

ASUS Control Center

11:38

Administrator

Software Report

Service Report

Service Information

1 AppInfo

Press the 'Enter' key to search...

Clear

Refresh

Export

Show Device

| ID | Name    | Display Name            | Count |
|----|---------|-------------------------|-------|
| 1  | AppInfo | Application Information | 4     |

Device List

Installed

Press the 'Enter' key to search...

Clear

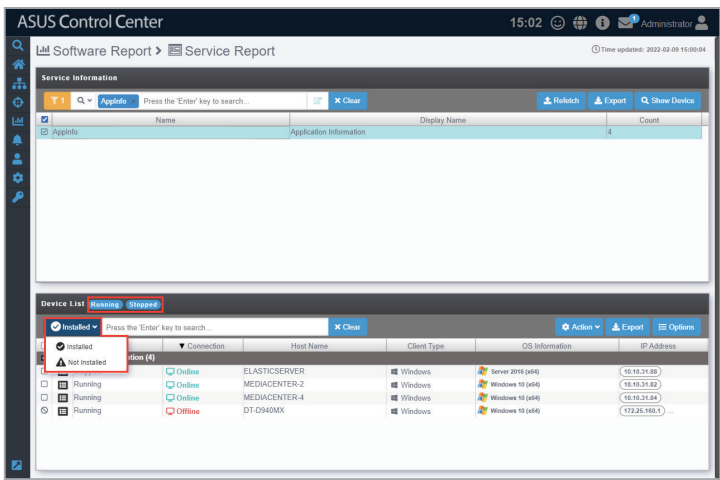
Action

Export

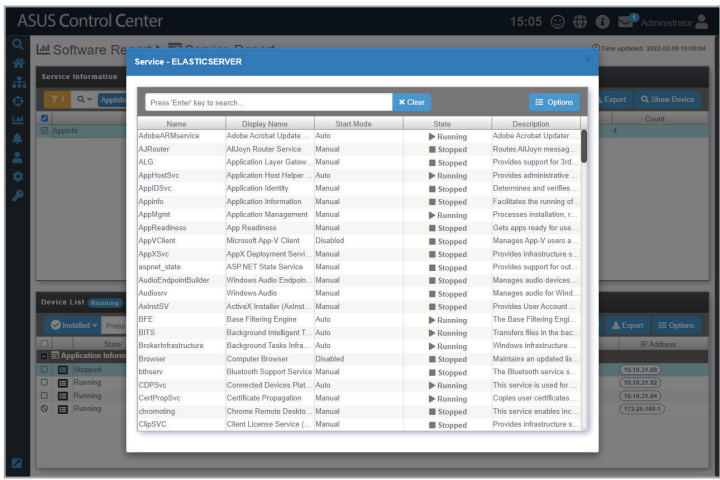
Options

| ID | State   | Connection | Host Name     | Client Type | OS Information    | IP Address       |
|----|---------|------------|---------------|-------------|-------------------|------------------|
| 1  | Stopped | Online     | ELASTICSERVER | Windows     | Server 2012 (x64) | 10.10.35.40      |
| 2  | Running | Online     | MEDIACENTER-2 | Windows     | Windows 10 (x64)  | 10.10.35.82      |
| 3  | Running | Online     | MEDIACENTER-4 | Windows     | Windows 10 (x64)  | 10.10.35.84      |
| 4  | Running | Offline    | DT-D940MX     | Windows     | Windows 10 (x64)  | 172.25.546.1 ... |

3. (optional) You may filter through the devices by clicking on the tags next to the Device List title, or filter by **Installed** or **Not Installed** by clicking on the drop down menu next to the search bar.

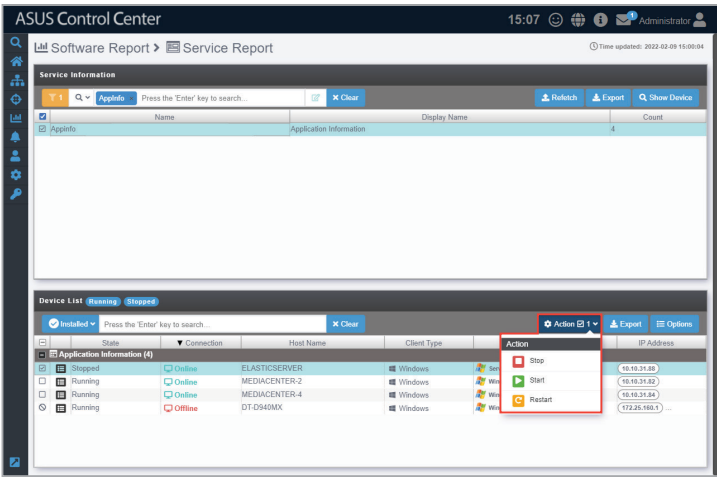


4. (optional) Clicking on  next to each device in the **Device List** will allow you to view all services on the selected device.



**Starting, stopping or restarting a service**

You can start, stop, or restart a selected service on a device by selecting the device in the Device List and clicking on the **Action** drop down menu to select your action.

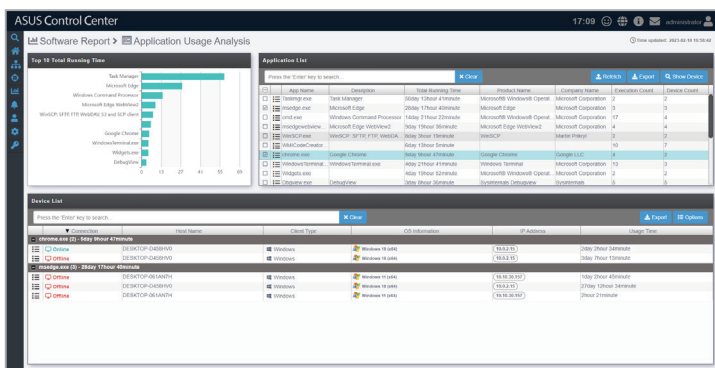


Starting, stopping or restarting the service may take up to two minutes to be completed. Once the process is completed, check if the count is correct, if not, you can click the **Refresh** button to refresh the service information.

## 5.1.5 Application Usage Analysis

**Application Usage Analysis** allows you to view the top ten most used applications, the execution count of each application, and other application usage information for all managed devices.

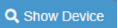
**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.



### Viewing application hash values

Click on  next to a selected application in the Application List to view more information about the application, such as the hash value. If there are multiple versions of an application, the hash value for each version will be shown.

### Viewing devices that have used a specified application

Select one or more application(s) in the Application List, then click  to display a list of all the managed devices that have used the selected application(s) and allows you to view additional information for each device.

Click  next to a selected device to view more information about the device.

### Refetching application usage information

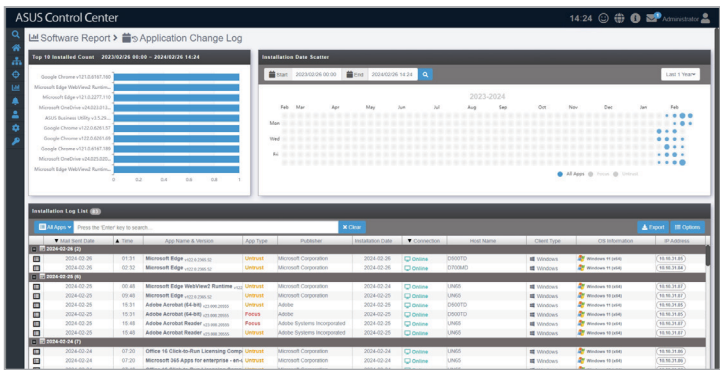
Click on  to request agents to immediately return updated application usage information for all managed devices, making sure all the information displayed is up to date.



## 5.1.6 Application Change Log

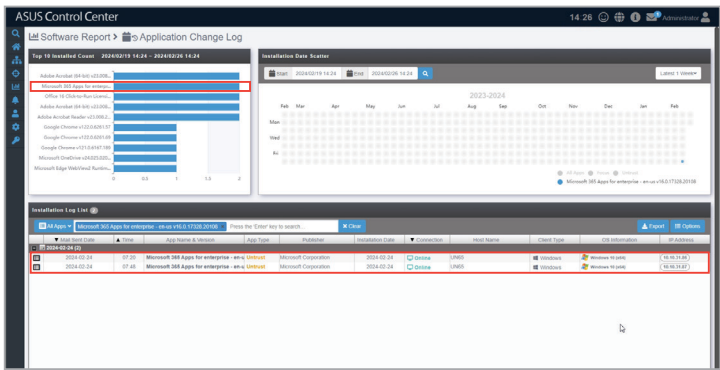
**Application Change Log** allows you to view application installation information for all managed devices.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.



### Filtering by application

Click an application in the **Top 10 Installed Count** block to only show devices with the specified application installed.



## Filtering by time period

Select a time period using the **Start** and **End** fields to only show records within the specified time period.

The screenshot shows the ASUS Control Center interface. The top navigation bar includes 'Software Report' and 'Application Change Log'. The 'Top 10 Installed Count' section displays a bar chart for various applications. The 'Installation Date Distribution' section shows a calendar for 2023-2024 with a date range filter set to '2023-05-01' to '2024-05-01'. The 'Change Log List' table below shows a list of applications with columns for 'App Name & Version', 'App Type', 'Publisher', 'Installation Date', 'Client Type', 'OS Information', and 'IP Address'.

| App Name & Version                                  | App Type | Publisher             | Installation Date | Client Type | OS Information | IP Address  |
|-----------------------------------------------------|----------|-----------------------|-------------------|-------------|----------------|-------------|
| Microsoft Word (Microsoft Word (Threading)) 2109    | Office   | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Edge for Business Web (Chrome) (1st)      | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Publisher Web (Chrome) (Threading) (1st)  | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft PowerPoint Web (Chrome) (Threading) (1st) | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Outlook Web (Chrome) (Threading) (1st)    | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Word Web (Chrome) (Threading) (1st)       | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Publisher Web (Chrome) (Threading) (1st)  | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft PowerPoint Web (Chrome) (Threading) (1st) | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Outlook Web (Chrome) (Threading) (1st)    | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Word Web (Chrome) (Threading) (1st)       | Web      | Microsoft Corporation | 2024-05-01 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |

Select a time period from the **Period** drop down menu to only show records within the specified time period.

The screenshot shows the ASUS Control Center interface. The top navigation bar includes 'Software Report' and 'Application Change Log'. The 'Top 10 Installed Count' section displays a bar chart for various applications. The 'Installation Date Distribution' section shows a calendar for 2023-2024 with a date range filter set to '2023-05-01' to '2024-05-01'. The 'Change Log List' table below shows a list of applications with columns for 'App Name & Version', 'App Type', 'Publisher', 'Installation Date', 'Client Type', 'OS Information', and 'IP Address'.

| App Name & Version                      | App Type | Publisher             | Installation Date | Client Type | OS Information | IP Address  |
|-----------------------------------------|----------|-----------------------|-------------------|-------------|----------------|-------------|
| Google Chrome (112.0.5615.135)          | Web      | Google LLC            | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Edge (112.0.1713.64)          | Web      | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Word (16.0.15224.10001)       | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Publisher (16.0.15224.10001)  | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft PowerPoint (16.0.15224.10001) | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Outlook (16.0.15224.10001)    | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Word (16.0.15224.10001)       | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Publisher (16.0.15224.10001)  | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft PowerPoint (16.0.15224.10001) | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |
| Microsoft Outlook (16.0.15224.10001)    | Office   | Microsoft Corporation | 2024-02-28 10:12  | Windows     | Windows 10 x64 | 192.168.1.1 |

Select All Apps, Focus, or Untrust to only show records matching the specified app type.

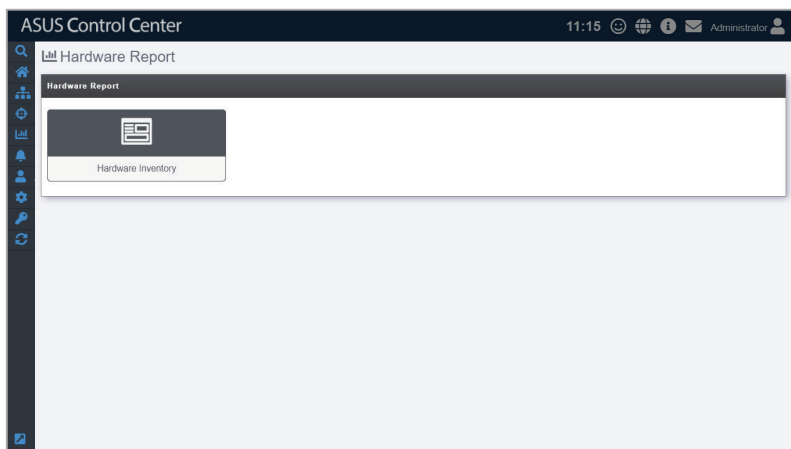


## 5.2 Hardware Report

**NOTE:** The information entered in this section is for reference only.

Hardware Report allows you to view a count of system models or hardware components of all managed devices, as well as rankings for each of these categories. For example you can view the top three storage components used in all managed devices.

To access **Hardware Report**, click  in the left menu, then click on **Hardware Report**.



### Using the search bar and search options

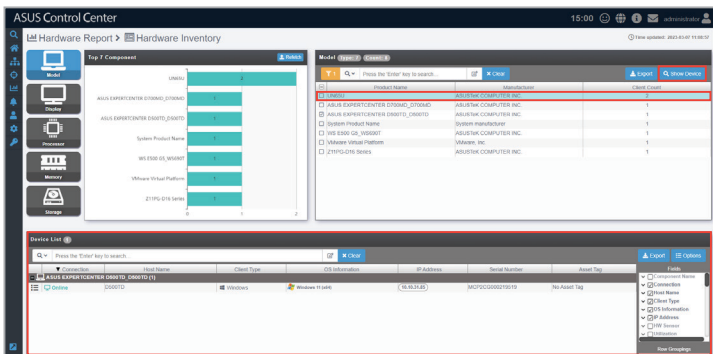
Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

### 5.2.1 Hardware Inventory

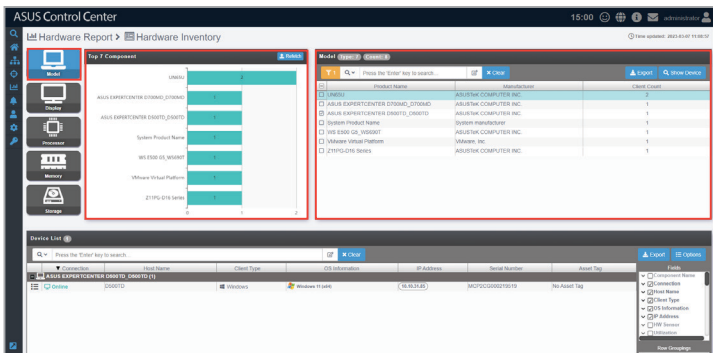
**Hardware Inventory** allows you to view the count for models, displays, processor, memory, or storage hardware components of all managed devices or filter through managed devices or hardware component.

Checking a component, then clicking on the **Show Device** button will display devices which have the selected components in the **Devices List**, allowing you to quickly locate managed devices with expensive hardware components or components which need to be replaced.

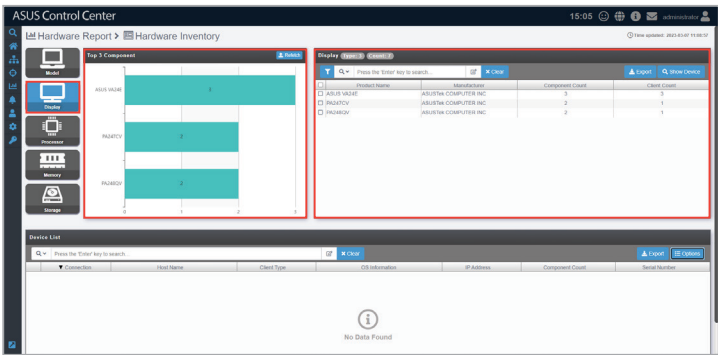
**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.



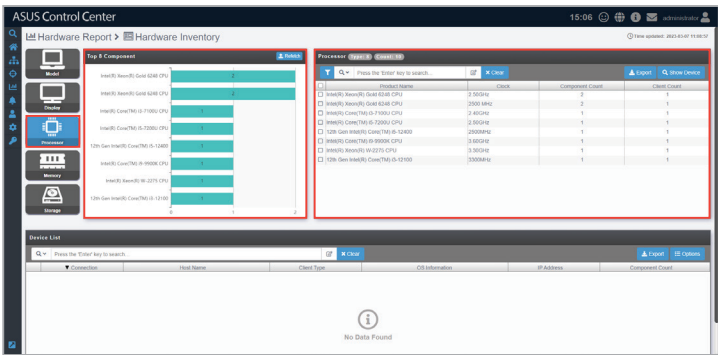
### View Model component type and count



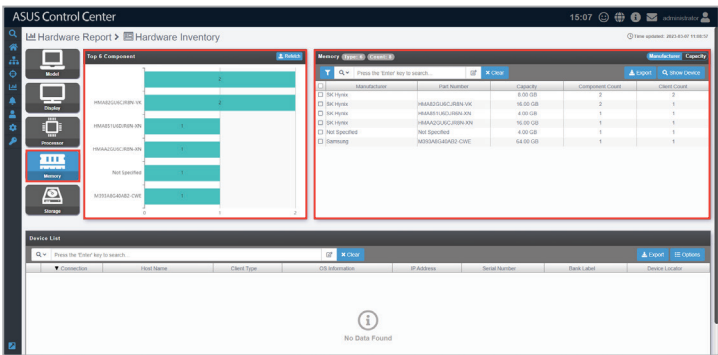
View Display component type and count



View Processor component type and count



View Memory component type and count



## View Storage component type and count

The screenshot shows the ASUS Control Center interface. The 'Hardware Inventory' tab is active, displaying a list of components under 'Top 10 Component'. The 'Storage' component is highlighted, showing a list of storage devices with columns for Product Name, Media Type, Size, Component Count, and Client Count.

| Product Name                      | Media Type            | Size      | Component Count | Client Count |
|-----------------------------------|-----------------------|-----------|-----------------|--------------|
| WESTERN DIGITAL WDC WDCW10000-400 | Fixed hard disk media | 224.41 GB | 1               | 1            |
| WESTERN DIGITAL WDC WDCW10000-400 | Fixed hard disk media | 880.76 GB | 1               | 1            |
| WESTERN DIGITAL WDC WDCW10000-400 | Fixed hard disk media | 224.41 GB | 1               | 1            |
| INTEL WDCW10000-400               | Fixed hard disk media | 476.34 GB | 1               | 1            |
| INTEL WDCW10000-400               | Fixed hard disk media | 476.34 GB | 1               | 1            |
| STORAGEDIGITAL-20000              | Fixed hard disk media | 800.00 GB | 1               | 1            |
| STORAGEDIGITAL-20000              | Fixed hard disk media | 1.82 TB   | 1               | 1            |
| STORAGEDIGITAL-20000              | Fixed hard disk media | 110.34 GB | 1               | 1            |
| WDC WDCW10000-400                 | Fixed hard disk media | 5.64 TB   | 1               | 1            |
| STORAGEDIGITAL-20000              | Fixed hard disk media | 800.00 GB | 1               | 1            |
| Virtual_disk                      | Fixed hard disk media | 32.00 GB  | 1               | 1            |

The 'Device List' section below shows a table with columns for Connection, Host Name, Client Type, OS Information, IP Address, Serial Number, and Password. It currently displays 'No Data Found!'.

## Refetch hardware component

Click on **Refetch** to request agents to return an immediate update the list of Model, Processor, Memory, or Storage components of all managed devices depending on the component category selected, making sure all hardware components, including newly added hardware components are counted for.

The screenshot shows the ASUS Control Center interface. The 'Hardware Inventory' tab is active, displaying a list of components under 'Top 7 Component'. The 'Model' component is highlighted, showing a list of models with columns for Product Name, Manufacturer, and Client Count.

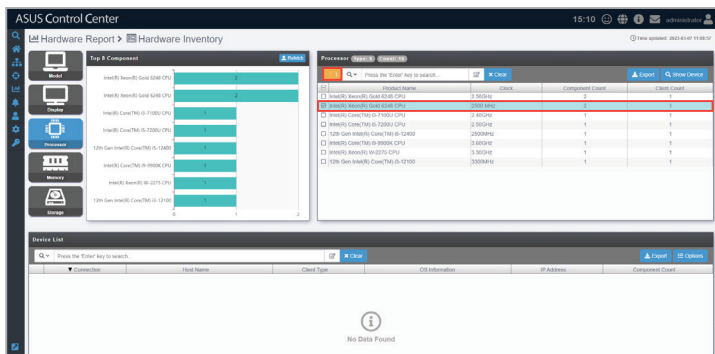
| Product Name                    | Manufacturer          | Client Count |
|---------------------------------|-----------------------|--------------|
| ASUS EXPERTCENTER CT0000_000000 | ASUSTEK COMPUTER INC. | 1            |
| ASUS EXPERTCENTER CT0000_000000 | ASUSTEK COMPUTER INC. | 1            |
| System Product Name             | System Manufacturer   | 1            |
| System Product Name             | System Manufacturer   | 1            |
| System Product Name             | System Manufacturer   | 1            |
| System Product Name             | System Manufacturer   | 1            |
| System Product Name             | System Manufacturer   | 1            |

The 'Device List' section below shows a table with columns for Connection, Host Name, Client Type, OS Information, IP Address, Serial Number, and Asset Tag. It currently displays 'No Data Found!'.

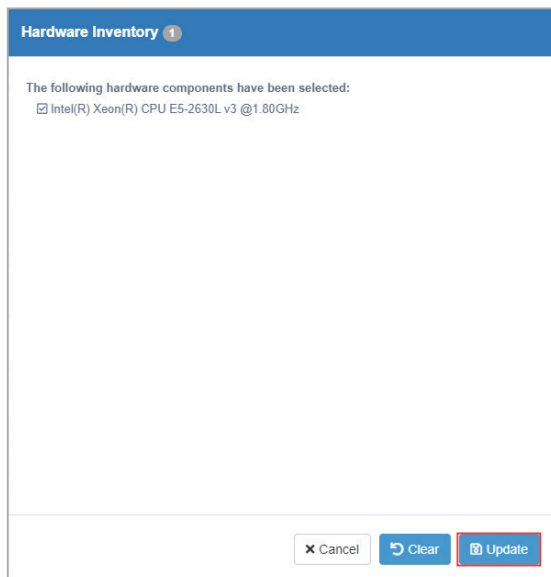
## Filter by component name

You can filter the components by the selected components.

1. Check the components you want to filter by then click on .



2. Confirm that the components displayed match the ones you checked, then click **Update**.



3. The component list should only display the selected components.



### Search for components using keywords

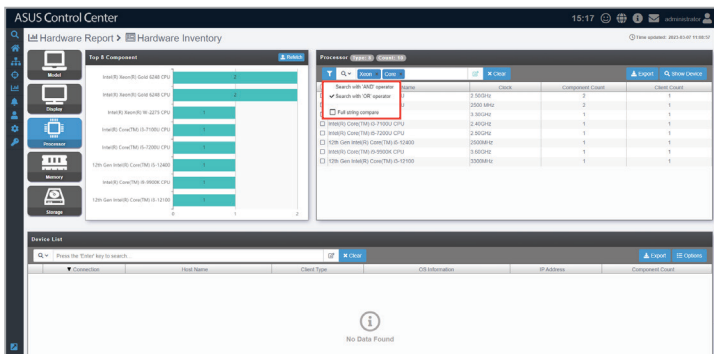
Entering keywords into the search bar will display all components which contain the keywords entered, allowing you to pinpoint certain hardware components and help you keep track of the amount of devices these hardware components are installed on.

1. Enter the keywords you wish to search for using the following methods:

- Directly entering the keywords

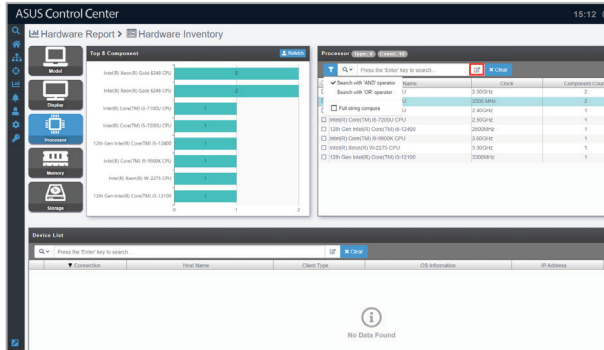
Enter the keyword(s) you wish to search with into the search bar and press <Enter>. Click on  to toggle between searching with **Search with 'AND' operator** or **Search with 'OR' operator**. **Search with 'AND' operator** will search for items which contain all keywords entered, whilst **Search with 'OR' operator** will search for items which contain at least one of the keywords entered.

Checking the **Full string compare** option will only return search results of items which have a string with an exact match to the keywords, and can be applied to any of the above search operators selected.



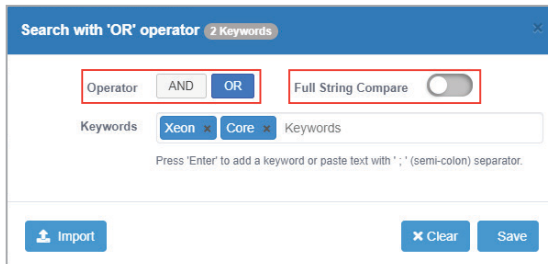
- Importing multiple keywords from a .csv file

- a. Click on  to bring up the search condition pop-up window.



- b. Select the operator you wish to use. **AND** will search for items which contain all the keywords entered, whilst **OR** will search for items which contain at least one of the keywords entered.

Enabling the **Full string compare** option will only return search results of items which have a string with an exact match to the keywords, and can be applied to any of the above search operators selected.



- c. Enter the keyword(s) you wish to search with into the **Keywords** field and press <Enter>. You may also Import multiple keywords using a .csv file by clicking on **Import**, selecting the .csv file you wish to import, and then selecting the field in the .csv file you would like to import.

Search with 'OR' operator 2 Keywords

Operator AND OR Full String Compare ☐

Keywords Xeon Core Keywords

Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import Clear Save

Import

Please select the field that you want to import from the csv file.

Name

Cancel OK

- d. Click on **Save** once you have finished setting the search conditions.

Search with 'OR' operator 2 Keywords

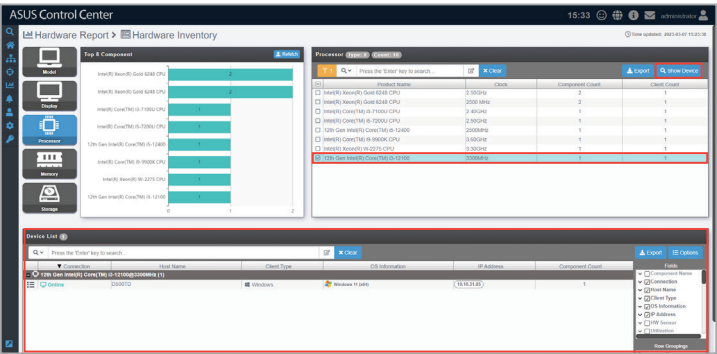
Operator AND OR Full String Compare ☐

Keywords Xeon Core Keywords

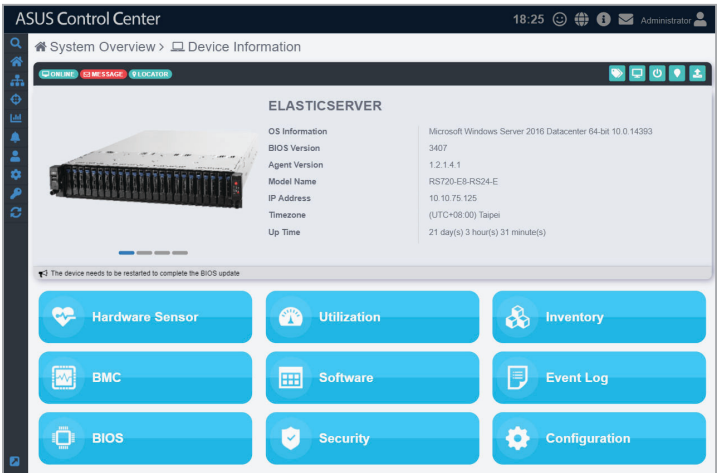
Press 'Enter' to add a keyword or paste text with ';' (semi-colon) separator.

Import Clear Save

- If you wish to view the devices a hardware component is installed on, check the application, then click on **Show Device**. The list of devices the selected application is installed on should be displayed in the **Device List** window



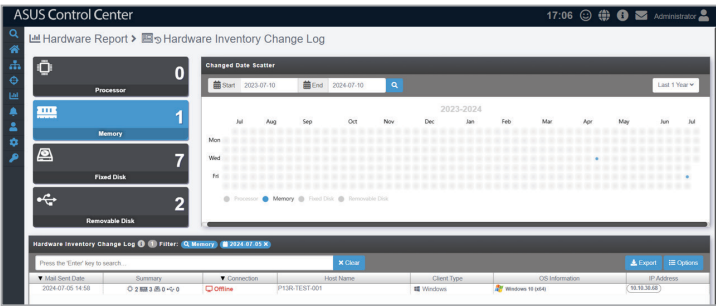
- (optional) Clicking on  next to each device in the **Device List** will allow you to view the Device Information.



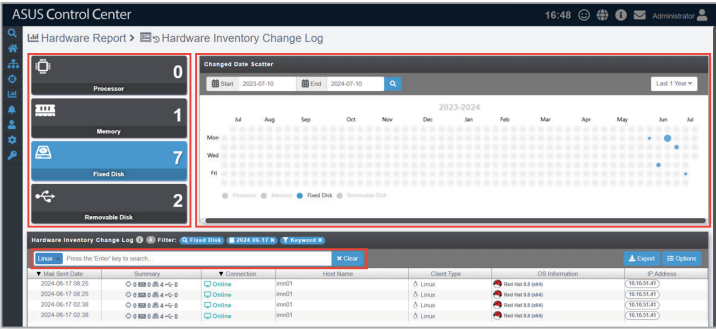
## 5.2.2 Hardware Inventory Change Log

This page allows you to view the hardware inventory change log.

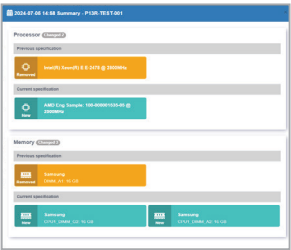
**NOTE:** Before using this function, ensure that hardware inventory change notifications and SMTP settings are properly configured. For more information, refer to the **Hardware Asset** section of the **Notification** chapter and the **SMTP Settings** section of the **Options** chapter.



1. Filter the hardware inventory change log by hardware type, date, or keyword.



2. Click an entry to view detailed information about the hardware inventory change.



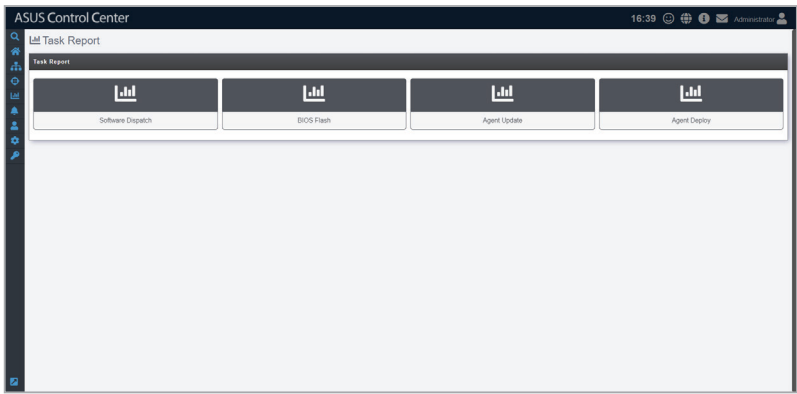
| <ul style="list-style-type: none"><li>Host Name: P13R</li><li>Login User: P13R\Administrator</li><li>IP Address: 10.10.30.68</li></ul> |                                   |                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                                                                                                                                   | Previous specification            | Current specification                                                                                                                                            |
| 1 Processor                                                                                                                            | Intel(R) Xeon(R) E-2478 @ 2800MHz | AMD 100-000001515-05 @ 2500MHz                                                                                                                                   |
| 2 Memory                                                                                                                               | Samsung CPU1 DIMM-A2 16GB         | Samsung CPU1 DIMM-A2 16GB                                                                                                                                        |
| 3 FixedDisk                                                                                                                            |                                   | INVMs SAMSUNG MZVL270HCL8-0B0B0 (New) <ul style="list-style-type: none"><li>SN: 0025_38BA_1101_5F99</li><li>Size: 953.96 GB</li><li>Partitions: ( C: )</li></ul> |

## 5.3 Task Report

**NOTE:** The information entered in this section is for reference only.

**Task Report** provides you with information on **Software Dispatch**, **BIOS Flash**, **Agent Update**, and **Agent Deploy**. These reports allow you to view when applications, BIOS, or agents were deployed, where they were deployed and their process statuses, helping you track all application, BIOS, and agent activity.

To access **Task Report**, click  > **Task Report** in the left menu.



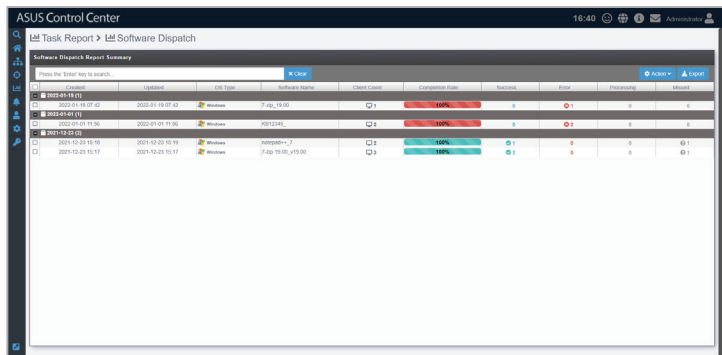
### Using the search bar and search options

Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

### 5.3.1 Software Dispatch Report

The **Software Dispatch Report** gives you an overview of all activities of application deployment. On the Software Dispatch report screen you can view information such as the date an application was dispatched, the last time its status was updated, the completion rate, how many clients the application was dispatched to, and also the status of the dispatch. You can refer to the **Software Dispatch Task Report** section for more details.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.



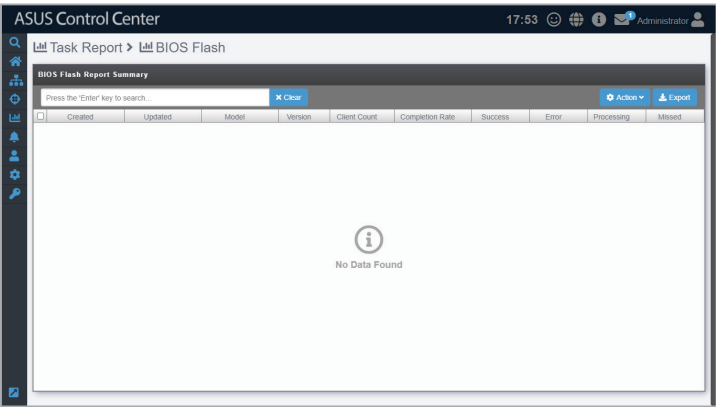
The screenshot shows the 'Software Dispatch Report Summary' interface in the ASUS Control Center. It features a table with columns for 'Application', 'Dispatched', 'Last Time', 'Software Name', 'Client Count', 'Completion Rate', 'Success', 'Error', 'Processing', and 'Message'. The table contains three data rows, each with a summary bar at the top showing the application name, dispatch time, and completion status. The first row is for 'HDD-45-18 (1)', the second for 'HDD-45-18 (1)', and the third for 'HDD-45-18 (1)'. Each row has a '100%' completion rate and a '0' success count. The table is filtered by 'All' and has a 'Clear' button. The interface also includes a search bar and a 'Filter' button.

| Application   | Dispatched          | Last Time           | Software Name | Client Count | Completion Rate | Success | Error | Processing | Message |
|---------------|---------------------|---------------------|---------------|--------------|-----------------|---------|-------|------------|---------|
| HDD-45-18 (1) | 2023-12-18 10:45:18 | 2023-12-18 10:45:18 | HDD-45-18 (1) | 0            | 100%            | 0       | 0     | 0          | 0       |
| HDD-45-18 (1) | 2023-12-18 11:05:18 | 2023-12-18 11:05:18 | HDD-45-18 (1) | 0            | 100%            | 0       | 0     | 0          | 0       |
| HDD-45-18 (1) | 2023-12-18 15:18:18 | 2023-12-18 15:18:18 | HDD-45-18 (1) | 0            | 100%            | 0       | 0     | 0          | 0       |

### 5.3.2 BIOS Flash Report

The **BIOS Flash Report** will display a history of BIOS flashes performed using ASUS Control Center. Each item will display the information on the BIOS, the device flashed, and status of the BIOS flash. You can refer to the **BIOS Flash Task Report** section for more details.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.

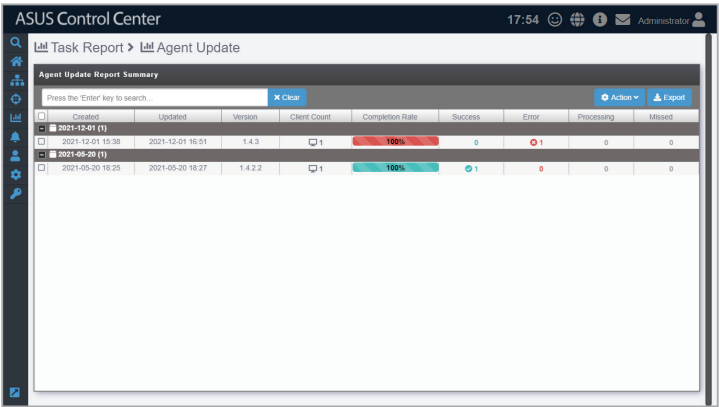




### 5.3.3 Agent Update Report

The **Agent Update Report** displays information on each upgrade to the deployed Windows and Linux agents. Each item showed on the Agent Update Report represents a single batch of agent updates. You can refer to the **Agent Update Report** section for more details.

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.



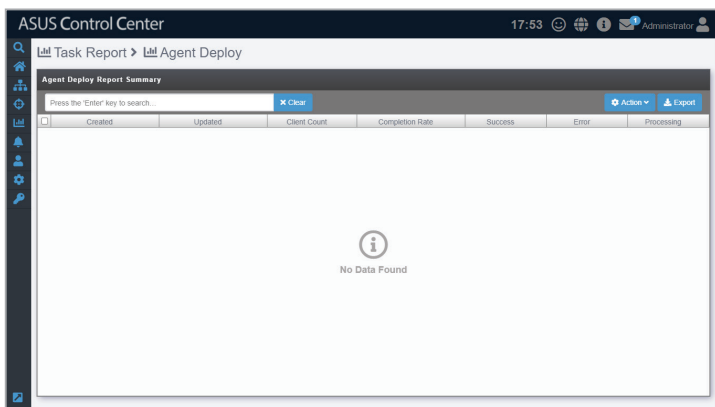
## 5.3.4 Agent Deploy Report

The **Agent Deploy Report** will display information on each time agent(s) are deployed onto managed devices. The list of agent deployment results are grouped by each batch of agent deployments. You can refer to the **Agent Deploy Report** section for more details.

---

**NOTE:** To export the information of a block click the **Export** button in that block, enter a filename, then click **OK**.

---



# Chapter 6

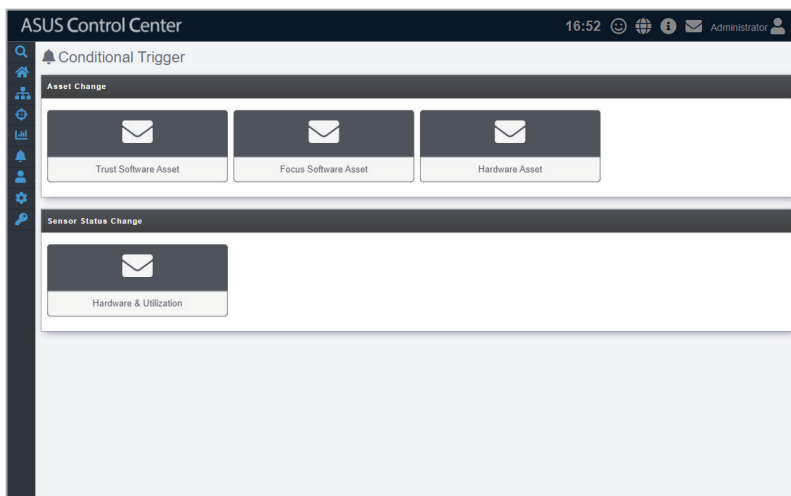
This chapter describes notification rules and asset report options.

# Notification

## 6.1 Conditional Trigger

Conditional Trigger allows you to set notifications for software changes, or hardware changes on managed devices. Notifications are sent when software not on the Trust or Focus list have been installed on managed devices, or if hardware such as CPUs or DIMMs that are removed or do not comply to company specifications are installed onto managed devices. This function will keep you alerted of potential risks to managed devices.

To access **Conditional Trigger**, click  in the left menu, then click on **Conditional Trigger**.



### Using the search bar and search options

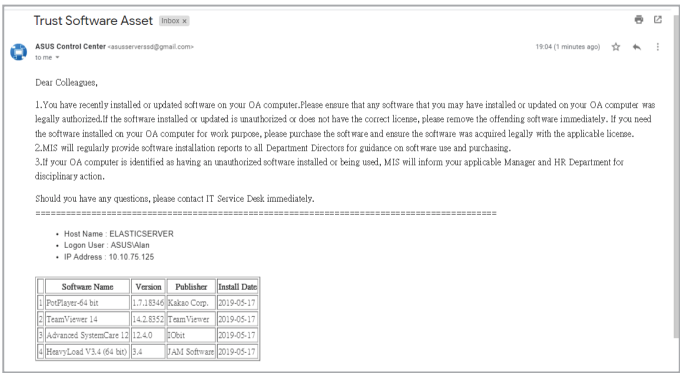
Refer to the **Search Options** and **Search and Filter Devices** sections of the **Monitor** chapter for more information.

### 6.1.1 Trust Software Asset

This function allows you to send notifications when the following events occur:

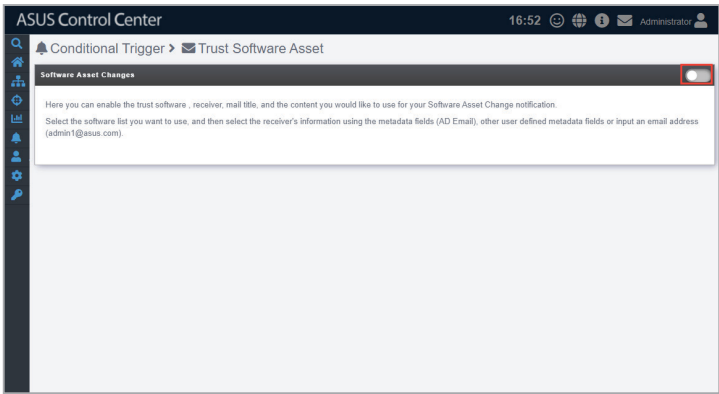
- Applications not in the Trust Software Asset are installed on managed devices

These notifications will be sent immediately to the owner of the managed device and their superior. Below is an example of a notification sent when an application not in the Trust Software Asset is installed on the managed device.



To enable Trust Software Asset :

1. Click on the button to configure and enable Software Asset Changes notifications.



2. Select software from the software list to be applied as a Trust Software Asset. Notifications will be sent when new software is installed on managed devices which do not appear on the Trust Software Asset.

**NOTE:** For more information on Software List, please refer to the **Software List** section of this manual.

3. Select the Compare feature fields **Software Name** and **Publisher**, as these two compare feature fields are required. **Version** and **Installed Date** are optional.
4. Enter the recipients of the notification email.
5. Click on **Save** after composing the title and content of the notification email.

**NOTE:** Ensure SMTP settings have been set and that a test email can be successfully sent to ensure notifications can be properly sent and received. For more information on SMTP settings and sending a test email, please refer to the **SMTP Settings** section.

ASUS Control Center 17:00 Administrator

Conditional Trigger > Trust Software Asset

**Software Asset Changes**

Here you can enable the trust software, receiver, mail title, and the content you would like to use for your Software Asset Change notification.

Select the software list you want to use, and then select the receiver's information using the metadata fields (AD Email), other user defined metadata fields or input an email address (admin1@asus.com).

**Trust Software**

|                       |                   |                           |                           |                       |                    |                  |             |
|-----------------------|-------------------|---------------------------|---------------------------|-----------------------|--------------------|------------------|-------------|
| Intel                 | AI Update         | MSP Office                | Drivers                   | Intel Corporation     | Nvidia Corporation | ASUS Corporation | Intel Corp. |
| Qualcomm Inc.         | Firmware          | AI Drivers                | Epson Utility             | Microsoft Corporation | Custom             | Google Chrome    |             |
| Microsoft Default App | Drivers - HP Inc. | Epson Utility - Publisher | Select from software list |                       |                    |                  |             |

**Compare Feature Fields**

| Software Name                                                                                      | Publisher | Version | Installed Date |
|----------------------------------------------------------------------------------------------------|-----------|---------|----------------|
| Software name and software publisher are required. Version and installed date fields are optional. |           |         |                |

**To:**  Select a metadata field or input an email address

**CC:**  Select a metadata field or input an email address

**BCC:**  Select a metadata field or input an email address

**Mail Title:** Trust Software Asset

**Mail Content:**

Dear Colleagues,

1. You have recently installed or updated software on your OA computer. Please ensure that any software that you have installed or updated on your OA computer was legally authorized.  
**If the software installed or updated is unauthorized or without legitimate license, please remove the software immediately.** If you need the software installed on your OA computer for work purpose, please apply for duty authorization or apply to Request for purchase of the software.
2. MIS will periodically provide software installation reports to all Department Directors for guidance on software use and purchasing
3. If your OA computer is identified as having unauthorized software installed or used, according to Work Rules "AD1-047" MIS will inform HR Department for disciplinary action.

**Save**

### 6.1.2 Focus Software Asset

This function allows you to send notifications when the following events occur:

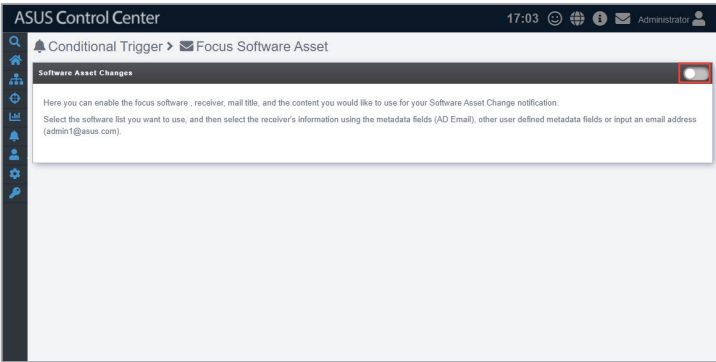
- Applications in the Focus Software Asset are installed on non-authorized managed devices

These notifications will be sent immediately to the owner of the managed device and their superior. Below is an example of a notification sent when an application in the Focus Software Asset is installed on a non-authorized managed device.



To enable Focus Software Asset :

1. Click on the button to configure and enable Software Asset Changes notifications.



2. Select software from the software list to be applied as a Focus Software Asset. Notifications will be sent when new software is installed on managed devices which do not appear on the Focus Software Asset.

---

**NOTE:** For more information on Software List, please refer to the **Software List** section of this manual.

---

3. Select the Compare feature fields **Software Name** and **Publisher**, as these two compare feature fields are required. **Version** and **Installed Date** are optional.
4. Enter the recipients of the notification email.
5. Click on **Save** after composing the title and content of the notification email.

---

**NOTE:** Ensure SMTP settings have been set and that a test email can be successfully sent to ensure notifications can be properly sent and received. For more information on SMTP settings and sending a test email, please refer to the **SMTP Settings** section.

---

**ASUS Control Center** 17:09 Administrator

Conditional Trigger > Focus Software Asset

**Software Asset Changes**

Here you can enable the focus software , receiver, mail title, and the content you would like to use for your Software Asset Change notification.  
Select this software list you want to use, and then select the receiver's information using the metadata fields (AD Email), other user defined metadata fields or input an email address (admin1@asus.com).

**Focus Software:** Autodesk Autodesk CorelDraw CorelDraw Systems Microsoft ADO Keyshot PTC CloudStream Lusion  
Milestone Graphics Siemens ANSYS Thin Matrix Select from software list

**Compare Feature Fields:** Software Name Publisher Version Installed Date  
Software name and software publisher are required. Version and installed date fields are optional.

**To:** AD Mail Select a metadata field or input an email address

**CC:** Microsoft Select a metadata field or input an email address

**BCC:** admin1@asus.com Select a metadata field or input an email address

**Mail Title:** Focus Software Asset

**Mail Content:**

Dear Managers,

In response to legally licensed use of software and to give department managers better control of software license information, MIS will assist in providing the notifications of software changes (add/remove) on QA computers, please review the list of employee-installed software in below EMAIL.

All departments must ensure all the software they use is properly licensed. MIS only provides the results of the survey, but it cannot determine whether the software installed by employees is legal or not.

Focussat.

**Save**

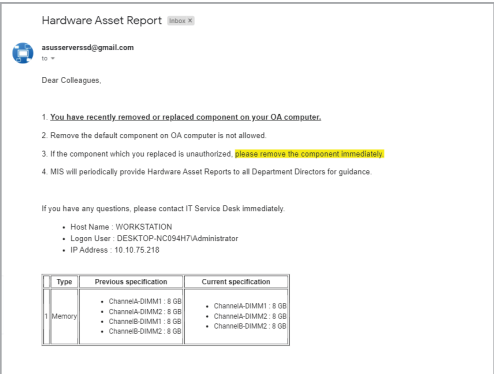


### 6.1.3 Hardware Asset

This function allows you to send notifications when the following events occur:

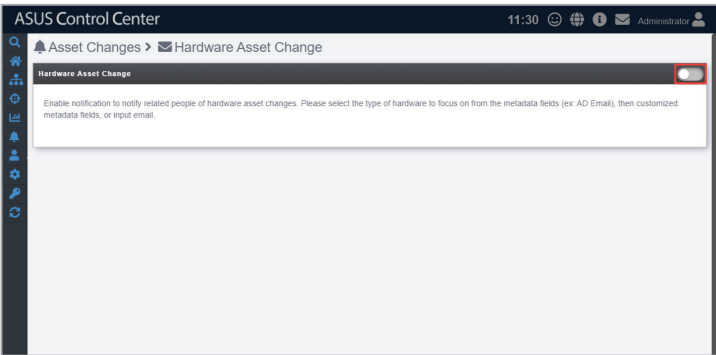
- Components which do not comply to company specifications are installed on managed devices
- Specified components are removed from managed devices

These notifications will list the hardware changes and be sent immediately to the owner of managed device and their superior. Below is an example of a notification sent when a DIMM is removed from a managed device.



To enable Hardware Asset :

1. Click on the button to configure and enable Hardware Asset change notifications.



2. Select which hardware component types (**Processor, Memory, Fixed Disk, Removable Disk**) you wish to receive notifications for.
3. Enter the recipients of the notification email.
4. Click on **Save** after composing the title and content of the notification email.

**NOTE:** Ensure SMTP settings have been set and that a test email can be successfully sent to ensure notifications can be properly sent and received. For more information on SMTP settings and sending a test email, please refer to the **SMTP Settings** section.

ASUS Control Center 11:00 Administrator

Asset Changes > Hardware Asset Change

**Hardware Asset Change**

Enable notification to notify related people of hardware asset changes. Please select the type of hardware to focus on from the metadata fields (ex: AD Email), then customized metadata fields, or input email.

Hardware Focus Type: **Memory** Select from the list of hardware types

To: **AD Mail** Select from the metadata fields or input an email

CC: **Director** Select from the metadata fields or input an email

BCC: **admin@asus.com** Select from the metadata fields or input an email

Subject: Hardware Asset Change

Mail content

Dear Colleagues,

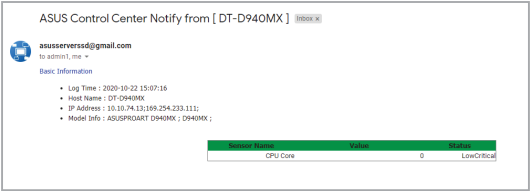
1. You have recently removed or replaced components on your OA Computers.
2. Remove the default component on the OA computer is not allowed.
3. If the component which you replaced is unauthorized, **please replace the component immediately.**
4. MIS will periodically provide Hardware Asset Reports to all Department Directors for guidance.

If you have any questions, please contact the IT Service Desk immediately.

**Save**

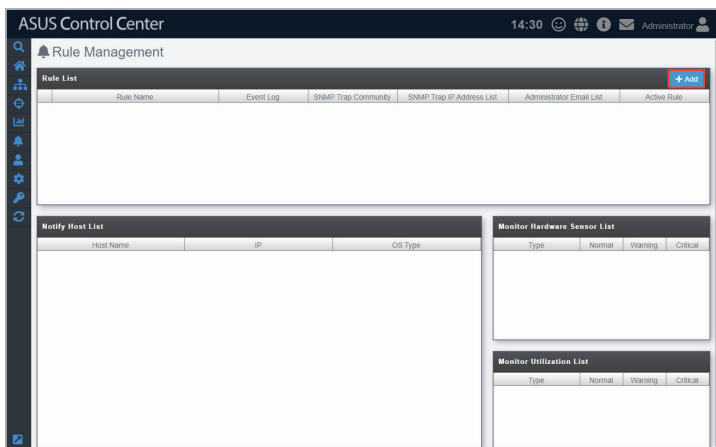
# 6.1.4      Hardware & Utilization

**Hardware & Utilization** allows you to add or delete rules on notifications. When a managed device's hardware sensor or utilization status changes to one that you have set a notification for, a notification will be sent to the system administrator. Below is an example of a notification sent when the CPU status of a managed device changes from **Normal** to **LowCritical**.

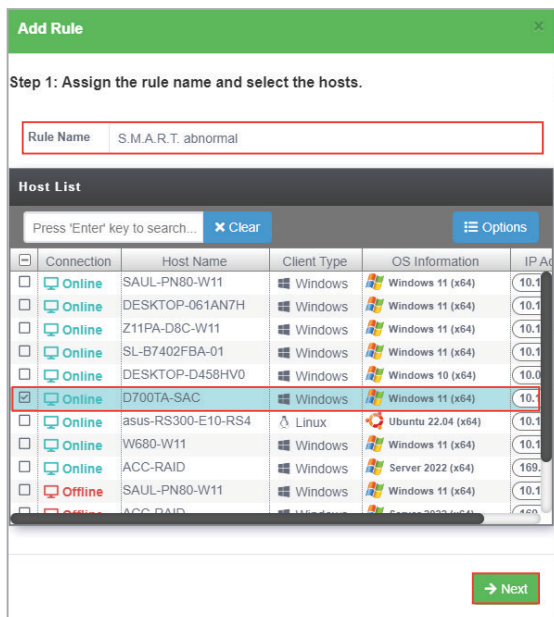


## Adding a new rule

1. Click **Add**.



2. Enter a rule name, then select the devices to apply the rule to. Click **Next**.



3. Select conditions (type and status of hardware sensors or utilization) to send notifications, then click **Next**.

**NOTE:**

- The checkbox checked when selecting the hardware sensor or utilization type and status will send notifications when the status shifts from the other two statuses to the status checked. For example, checking **Normal** will send notifications when the status changes from **Warning** or **Critical** to **Normal**.
- To set the status thresholds for the Utilization Type, please refer to the **Utilization** section.

Add Rule

Step 2: Select the hardware sensor or utilization type and status.

| Hardware Sensor type | <input type="checkbox"/> Normal | <input type="checkbox"/> Warning    | <input type="checkbox"/> Critical   |
|----------------------|---------------------------------|-------------------------------------|-------------------------------------|
| Fan                  | <input type="checkbox"/>        | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Temperature          | <input type="checkbox"/>        | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Voltage              | <input type="checkbox"/>        | <input type="checkbox"/>            | <input type="checkbox"/>            |
| S.M.A.R.T.           |                                 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Power Supply         | <input type="checkbox"/>        | <input type="checkbox"/>            | <input type="checkbox"/>            |

| Utilization Type | <input type="checkbox"/> Normal | <input type="checkbox"/> Warning | <input type="checkbox"/> Critical |
|------------------|---------------------------------|----------------------------------|-----------------------------------|
| CPU              | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |
| DIMM             | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |
| Partition        | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |
| Network          | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |

← Previous

→ Next

4. Select the notification method between the following options (multiple notification methods may be selected):

- Event Log

The notification will be displayed on the device's event log and system overview.

Add Rule

Step 3: Select at least one notification method.

Event Log

☒

SNMP Trap

Community

ASUS

Receiver's IP address

192.168.0.1

EX: 192.168.0.1

Email

Device administrator's email address

admin@asus.com

EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semi-colon.

Previous

Save

- SNMP Trap

The notification is recorded in the SNMP Trap Receiver, ensure to enter the corresponding information into the **Community** and **Receiver's IP address** fields.

**Add Rule** [Close]

**Step 3: Select at least one notification method.**

Event Log ☒

---

**SNMP Trap**

Community  
ASUS

Receiver's IP address  
192.168.0.1 EX: 192.168.0.1

---

**Email**

Device administrator's email address  
admin@asus.com  
EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semi-colon.

← Previous Save

- Email

The notification is sent to the entered email addresses of the IT department as well as all people associated with the device.

---

**NOTE:**

- Ensure to set up the SMTP server settings before using the email function. For more information please refer to the **SMTP Settings** section.
  - When entering multiple emails, use a semicolon ';' to separate the emails.
- 

**Add Rule** [X]

**Step 3: Select at least one notification method.**

Event Log ☒

SNMP Trap

Community  
ASUS

Receiver's IP address  
192.168.0.1 [X] EX: 192.168.0.1

Email

Device administrator's email address  
admin@asus.com [X]  
EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semi-colon.

← Previous Save



5. Click on **Save** after finished selecting your notification method(s).

Add Rule

Step 3: Select at least one notification method.

Event Log

☒

SNMP Trap

Community

ASUS

Receiver's IP address

192.168.0.1

EX: 192.168.0.1

Email

Device administrator's email address

admin@asus.com

EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semi-colon.

Previous

Save

Your newly added rule should appear in the main Hardware & Utilization screen, under **Rule List**, this displays the rule name and details of your selected notification method. Clicking on the newly added rule will display the devices associated with the rule in the **Notify List**, and the list of hardware and utilizations being monitored in the **Monitor Hardware Sensor List** and **Monitor Utilization List**.

**NOTE:** Ensure SMTP settings have been set and that a test email can be successfully sent to ensure notifications can be properly sent and received. For more information on SMTP settings and sending a test email, please refer to the **SMTP Settings** section.

ASUS Control Center

11:08

Conditional Trigger > Hardware & Utilization

Rule List

| Rule Name       | Event Log | SMTP Trigger Command | SMTP Trigger IP Address List | Authentication Email List |
|-----------------|-----------|----------------------|------------------------------|---------------------------|
| CPU Temp. alert | 02        | ASUS                 | 192.168.0.01                 |                           |

Notify Host List

| Host Name       | IP           | OS Type             |
|-----------------|--------------|---------------------|
| 192.168.0.01    | 192.168.0.01 | Windows 10 (64-bit) |
| DESKTOP-P00L3M8 | 192.168.0.01 | Windows 10 (64-bit) |

Monitor Hardware Sensor List

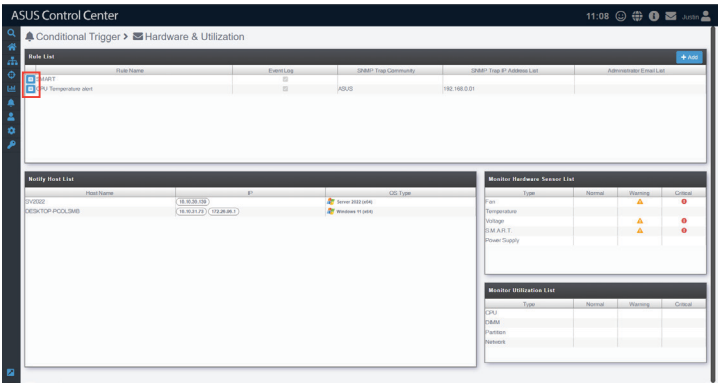
| Type         | Normal | Warning | Critical |
|--------------|--------|---------|----------|
| Fan          |        |         |          |
| Temperature  |        |         |          |
| Voltage      |        |         |          |
| SMART        |        |         |          |
| Power Supply |        |         |          |

Monitor Utilization List

| Type    | Normal | Warning | Critical |
|---------|--------|---------|----------|
| CPU     |        |         |          |
| RAM     |        |         |          |
| Network |        |         |          |

## Editing an existing rule

1. Click on  next to the rule you wish to edit.



2. You can edit the rule name and select the hosts to apply the rule to. Click **Next**.

Edit Rule

Step 1: Assign the rule name and select the hosts.

Rule Name

Notification\_2

Host List

Press 'Enter' key to search... Clear Options

|                                     | Host Name           | Client Type | OS Information     | IP Address    |
|-------------------------------------|---------------------|-------------|--------------------|---------------|
| <input checked="" type="checkbox"/> | ELASTICSERVER       | Windows     | Server 2016 (x64)  | 10.10.31.88   |
| <input type="checkbox"/>            | gpuforal-ESC4000-G4 | Linux       | Ubuntu 18.04 (x64) | 10.10.30.122  |
| <input checked="" type="checkbox"/> | LAPTOP-OHMO4NT5     | Windows     | Windows 10 (x64)   | 192.168.1.235 |
| <input checked="" type="checkbox"/> | AA0800987-NB2       | Windows     | Windows 10 (x64)   | 10.10.31.75   |
| <input checked="" type="checkbox"/> | VC66-WIN10          | Windows     | Windows 10 (x64)   | 10.10.30.142  |
| <input type="checkbox"/>            | Z11PA-D8C           | Windows     | Windows 10 (x64)   | 10.10.30.113  |
| <input type="checkbox"/>            | DT-D940MX           | Windows     | Windows 10 (x64)   | 192.168.120.1 |
| <input type="checkbox"/>            | test01              | Linux       | SLES 15 SP2 (x64)  | 10.10.65.46   |
| <input type="checkbox"/>            | LAPTOP-TU0JT9NL     | Windows     | Windows 11 (x64)   | 10.8.60.37    |
| <input type="checkbox"/>            | RedHat-RS100-E9-PI2 | Linux       | Red Hat 8.0 (x64)  | 10.10.75.27   |

Next

3. Select conditions (type and status of hardware sensors or utilization) to send notifications, then click **Next**.

**NOTE:**

- The checkbox checked when selecting the hardware sensor or utilization type and status will send notifications when the status shifts from the other two statuses to the status checked. For example, checking **Normal** will send notifications when the status changes from **Warning** or **Critical** to **Normal**.
- To set the status thresholds for the Utilization Type, please refer to the **Utilization** section.

Edit Rule

Step 2: Select the hardware sensor or utilization type and status.

| Hardware Sensor Type | <input type="checkbox"/> Normal | <input type="checkbox"/> Warning    | <input type="checkbox"/> Critical   |
|----------------------|---------------------------------|-------------------------------------|-------------------------------------|
| Fan                  | <input type="checkbox"/>        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Temperature          | <input type="checkbox"/>        | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Voltage              | <input type="checkbox"/>        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| S.M.A.R.T.           |                                 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Power Supply         | <input type="checkbox"/>        | <input type="checkbox"/>            | <input type="checkbox"/>            |

| Utilization Type | <input type="checkbox"/> Normal | <input type="checkbox"/> Warning | <input type="checkbox"/> Critical |
|------------------|---------------------------------|----------------------------------|-----------------------------------|
| CPU              | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |
| DIIMM            | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |
| Partition        | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |
| Network          | <input type="checkbox"/>        | <input type="checkbox"/>         | <input type="checkbox"/>          |

← Previous

→ Next

4. Select the notification method (multiple notification methods may be selected).

**NOTE:** For more details on the notification methods, please refer to the **Adding a new rule** section

Edit Rule

Step 3: Select at least one notification method.

Event Log

☒

SNMP Trap

Community

ASUS

Receiver's IP address

192.168.0.01

EX: 192.168.0.1

Email

Device administrator's email address

admin@asus.com

EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semi-colon.

Previous

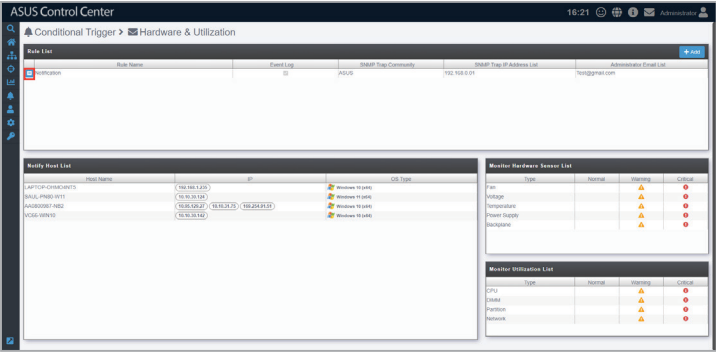
Delete

Update

5. Click on **Update** once you have finished editing the rule.

## Deleting a notification rule

1. Click on  next to the rule you wish to delete.



2. Click **Next**, then **Next** again until you reach the following window, then click **Delete**.

Edit Rule

Step 3: Select at least one notification method.

Event Log

☒

SNMP Trap

Community

ASUS

Receiver's IP address

192.168.0.01 EX: 192.168.0.1

Email

Device administrator's email address

admin@asus.com EX: admin1@asus.com;admin2@asus.com;

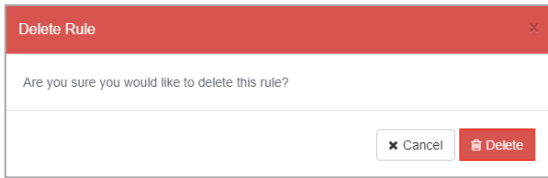
Tip: Press <Enter> to add another email address separated by a semi-colon.

Previous

Delete

Update

3. Click **Delete** on the pop up window to delete the rule.

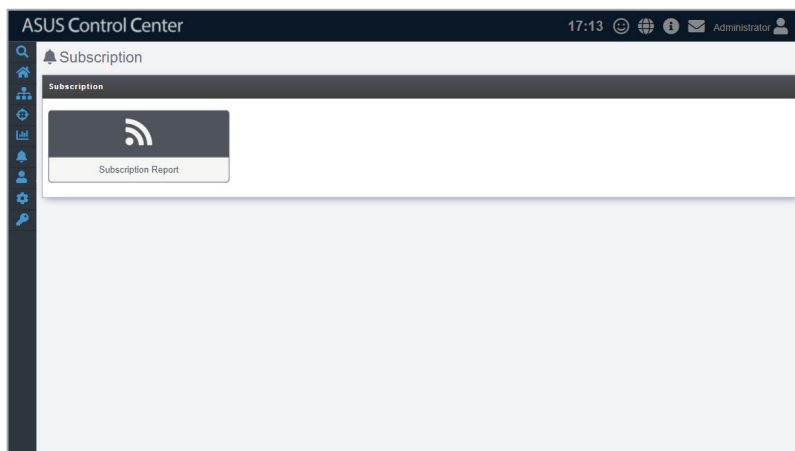


## 6.2 Subscription

**NOTE:** The information entered in this section is for reference only.

Subscription allows you to set a periodic report on the hardware or software of managed devices. The reports are then sent to the department's director, allowing them to easily manage the department's software and hardware.

To access **Subscription**, click  in the left menu, then click on **Subscription**.





## 6.2.1 Subscription Report

**Subscription Report** allows you to manage your Software Reports such as which list set to apply (Trust Software or Focus Software), the receiver of the report, which devices to create reports on and when to receive the reports. This gives you the flexibility to tailor each subscription report according to your needs and focus on the device and applications you want to focus on.

**NOTE:** The report mail sender information can be set at the SMTP settings section, please refer to **SMTP Setting** section in this manual.

- Below is an example of a monthly Trust Software Asset report on the softwares of a department's managed devices.

Software Report by Trust List ✖

ASUS Control Center -asususeresad@gmail.com-  
to me +

16:28 (2 minutes ago) ☆ ↻ ⋮

Dear Directs,

Your department's software report as below, please ensure these application are followed company's policy.

|    | Software Name                            | Version          | Publisher          | Install Date | Host Name        | Login User               | Work ID   | Phone | Department |
|----|------------------------------------------|------------------|--------------------|--------------|------------------|--------------------------|-----------|-------|------------|
| 1  | HeavyLoad v3.5.1 (64 bit)                | 3.5.1            | JAM Software       | 2019-05-10   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 2  | Concertant VIO Audio                     | 0.66.05.54       | Concertant         | 2019-05-11   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 3  | Intel(R) Management Engine Components    | 12.0.0.0         | Intel Corporation  | 2019-05-12   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 4  | Microsoft VC++ redistributables repacked | 12.0.0.0         | Intel Corporation  | 2019-05-12   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 5  | Vulkan Run Time Libraries 1.0.65.1       | 1.0.65.1         | LunarG, Inc.       | 2019-05-13   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 6  | NetBeans IDE 8.2                         | 8.2              | NetBeans.org       | 2019-05-14   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 7  | MySQL Workbench 6.3 CE                   | 6.3.10           | Oracle Corporation | 2019-05-15   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 8  | PyTTY release 0.71 (64-bit)              | 0.71.0.0         | Simon Tatham       | 2019-05-15   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 9  | Python 3.6.4 pip bootstrap (32-bit)      | 3.6.4150.0       | Python Foundation  | 2019-05-16   | ELASTICSERVER    | ELASTICSERVER\ain        | AA1600050 | 29631 | SW         |
| 10 | iboveap                                  | 0.3.0            | CentOS             | 2019-05-17   | KubernetesMaster | KubernetesMaster\Charles | AA1600053 | 29768 | SW         |
| 11 | weblogic4-plugin-process-gb2             | 2.14.7           | CentOS             | 2019-05-18   | KubernetesMaster | KubernetesMaster\Charles | AA1600053 | 29768 | SW         |
| 12 | ganglia-web                              | 16.0.11425.20244 | CentOS             | 2019-05-18   | KubernetesMaster | KubernetesMaster\Charles | AA1600053 | 29768 | SW         |
| 13 | packaged-jenkins-plugin                  | 1.1.5            | CentOS             | 2019-05-19   | KubernetesMaster | KubernetesMaster\Charles | AA1600053 | 29768 | SW         |
| 14 | python-decorator                         | 3.4.0            | CentOS             | 2019-05-20   | KubernetesMaster | KubernetesMaster\Charles | AA1600053 | 29768 | SW         |
| 15 | gnome-shell-extension-common             | 3.22.2           | CentOS             | 2019-05-20   | KubernetesMaster | KubernetesMaster\Charles | AA1600053 | 29768 | SW         |

- Below is an example of a monthly Focus Software Asset report on the software applications of a department's managed devices.

Software Report by Focus List Help

ASUS Control Center - asusserverstd@gmail.com 17:45 (3 minutes ago)

to me

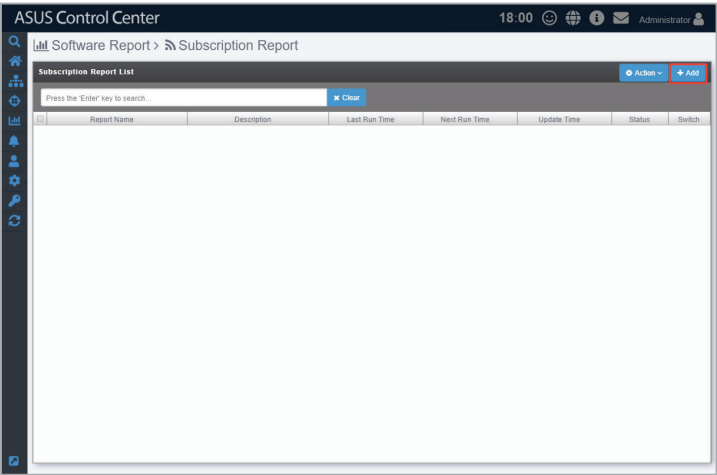
Dear Directs,

Your department's software report as below, please ensure these application's license are enough.

|   | Software Name                | Version          | Publisher             | Install Date | Host Name     | Login User        | Work ID   | Phone | Department |
|---|------------------------------|------------------|-----------------------|--------------|---------------|-------------------|-----------|-------|------------|
| 1 | Adobe Acrobat Reader DC      | 19.010.20090     | Adobe Systems Inc.    | 2019-05-15   | ELASTICSERVER | ELASTICSERVER\Aan | AA1600050 | 29631 | SW         |
| 2 | Microsoft Office 2016 - 29-N | 16.0.11425.20244 | Microsoft Corporation | 2019-05-18   | ELASTICSERVER | ELASTICSERVER\Aan | AA1600050 | 29631 | SW         |

### To create a Subscription Report:

- Click on **Add** on the Subscription Report main screen to create a new report subscription.



2. Enter the Report name as well as a brief description of the report into their respective fields. Then select which list to apply to the report, Trust Software or Focus Software, and select the specific list(s) you wish to apply.

**NOTE:**

- Selecting the **Trust Software** option will exclude applications on the trust list when a report is generated. For more information please refer to the **Trust Software Asset** section of this chapter.
- Selecting the **Focus Software** option will only include applications on the focus list when a report is generated. For more information please refer to the **Focus Software Asset** section of this chapter.

ASUS Control Center 18:00 Administrator

Software Report > Subscription Report > Subscription Report Information

**Subscription Report Information**

|             |                                                                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Report Name | Software Report by Trust List                                                                                                           |
| Description | Show all application but ignore known application from trust list                                                                       |
| Apply List  | <input checked="" type="radio"/> Apply Trust List <input type="radio"/> Apply Focus List                                                |
|             | <input checked="" type="checkbox"/> Google Chrome <input checked="" type="checkbox"/> ACC Windows Agent Select from software trust list |
| Enable      | <input checked="" type="checkbox"/> Enable Report                                                                                       |

**Mail Template** > Mail Settings > Mail Time

**Step 1: Set up the mail template**

|               |                                                                                                |
|---------------|------------------------------------------------------------------------------------------------|
| Mail Receiver | <input checked="" type="checkbox"/> Director Select a metadata field or input an email address |
| Mail Title    | Software Report by Trust List                                                                  |

3. Check **Enable Report** to enable this report.

ASUS Control Center 18:00 Administrator

Software Report > Subscription Report > Subscription Report Information

**Subscription Report Information**

|               |                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Report Name   | Software Report by Focus Software                                                                                                               |
| Description   | Show specific application from focus list and ignore the other application                                                                      |
| Apply List as | <input checked="" type="radio"/> Trust Software <input type="radio"/> Focus Software                                                            |
|               | <input checked="" type="checkbox"/> Adobe Application <input checked="" type="checkbox"/> Microsoft Application Select from software focus list |
| Enable        | <input checked="" type="checkbox"/> Enable Report                                                                                               |

**Mail Template** > Mail Settings > Mail Time

**Step 1: Set up the mail template**

|               |                                                                                                |
|---------------|------------------------------------------------------------------------------------------------|
| Mail Receiver | <input checked="" type="checkbox"/> Director Select a metadata field or input an email address |
| Mail Title    | Software Report by Trust Software                                                              |

4. Select a metadata tag or enter an email address into the **Mail Receiver** field, then enter your mail title and mail content.

---

**NOTE:** The metadata tag allows you to use customized groups as your mail recipients. For more details on metadata, please refer to the **Metadata Management** section in this manual.

---

5. Select **Only Mail Content** to only include the mail content entered when the report is sent. Select **Mail Content with Details** to also include a software list in the mail content when the report is sent.

The screenshot displays the ASUS Control Center interface. The top navigation bar shows the path: Software Report > Subscription Report > Subscription Report Information. The main section is titled "Subscription Report Information" and contains fields for Report Name, Description, Apply List as (Trust Software, Focus Software), and Enable (checked). Below this, the "Mail Template" section is active, showing "Step 1: Set up the mail template". The "Mail Receiver" field is set to "Director" with a dropdown menu. The "Mail Title" field is set to "Software Report by Trust Software". The "Mail Content" field contains a placeholder text: "Dear Directors: Your department's software report as below, please ensure these application's license are enough". At the bottom of the Mail Content field, there are two radio buttons: "Only Mail Content" (selected) and "Mail Content with Details". The interface also shows a "Cancel" button and a "Next" button.

6. In the **Rule Settings** step, you have to filter out the managed devices you wish to generate this report on. You can either select Custom rules or Grouping by selected metadata field.

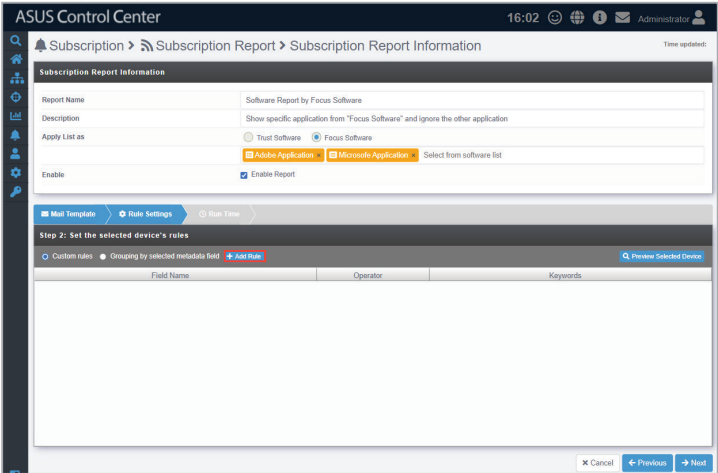
---

**NOTE:**

- Selecting the **Custom rules** option will allow you to select the rules to filter by.
  - Selecting the **Grouping by selected metadata** option will filter by the metadata tag selected. To use the **Grouping by selected metadata** option ensure you have added a metadata tag as the **Mail Receiver** in step 4.
-

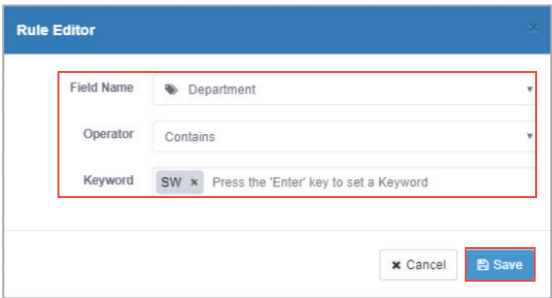
7. If you selected the **Custom rules** option, Click on **Add Rule**.

**NOTE:** Follow this step only if you selected the **Custom rules** option.

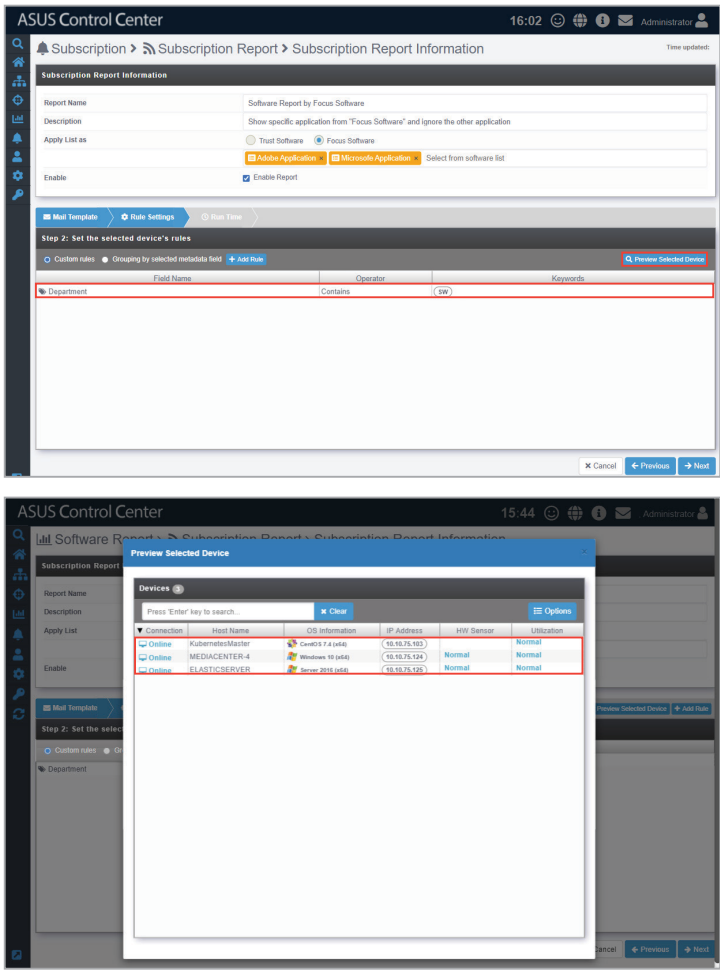


8. Enter the information required on the Rule Editor pop-up window. Once you have finished editing the rule on which to filter devices, click on **Save**.

**NOTE:** Follow this step only if you selected the **Custom rules** option.



9. Your new rule will appear in the window below. Click on **Preview Selected Device** to view the device(s) results of your newly added rule.



10. Repeat steps 6 to 8 to add another rule.

11. (optional) You may also edit or delete a rule by clicking on the rule, then repeat steps 4 to edit the rule, or click on **Delete** to delete the rule.

**Rule Editor**

Field Name: Department

Operator: Contains

Keyword: SW

Press the 'Enter' key to set a Keyword

Cancel Delete Save

12. Click on **Next** once you are finished.

**ASUS Control Center** 18:00 Administrator

Software Report > Subscription Report > Subscription Report Information

**Subscription Report Information**

Report Name: Software Report by Focus List

Description: Show specific application from focus list and ignore the other application.

Apply List: ☐ Apply Trust List ☒ Apply Focus List

Enable: ☒ Enable Report

Adobe Application Microsoft Application Select from software focus list

Step 2: Set the selected device's rules

| Field Name | Operator | Keywords |
|------------|----------|----------|
| Department | Contains | SW       |

Cancel Previous **Next**

13. Select a **Send Date** from the drop down menu to specify when the report will be sent. The **Send Date** options are as below:
- **Every Day**: Send a report every day.
  - **Every Week**: Send a report every week on a selected weekday.
  - **First day of the month**: Send a report on the first day of every month.
  - **Nth day of the month**: Send a report on the selected day of each month.
  - **Last day of the month**: Send a report on the last day of each month.

The screenshot shows the ASUS Control Center interface. The top navigation bar includes the title 'ASUS Control Center', the time '18:00', and user information 'Administrator'. The breadcrumb trail is 'Software Report > Subscription Report > Subscription Report Information'. The main section is titled 'Subscription Report Information' and contains fields for 'Report Name' (Software Report by Focus List), 'Description' (Show specific application from focus list and ignore the other application), 'Apply List' (with radio buttons for 'Apply Trust List' and 'Apply Focus List'), and 'Enable' (checked 'Enable Report'). Below this is a 'Mail Template' section with tabs for 'Mail Template', 'Mail Settings', and 'Run Time'. The 'Run Time' tab is active, showing 'Step 3: Set the Run Time'. In this step, the 'Send Date' is set to 'Nth day of the month' with a value of '10'. The 'Data Period' is set to '1' month, with options for 'Entire month' and 'Depend on send date'. A 'Next Run Time' box indicates the report will be mailed on '2019/06/10 00:00' containing data from '2019/05/10 ~ 2019/06/09'. At the bottom, there are buttons for 'Cancel', 'Previous', 'Send Now', and 'Save'.

ASUS Control Center 18:00 Administrator

Software Report > Subscription Report > Subscription Report Information

Subscription Report Information

Report Name: Software Report by Focus List

Description: Show specific application from focus list and ignore the other application.

Apply List: ☐ Apply Trust List ☒ Apply Focus List

Enable: ☒ Enable Report

Mail Template Mail Settings Run Time

Step 3: Set the Run Time

Send Date: Nth day of the month 10

Days: Days Months All

Data Period: 1 Months

☐ Entire month ☒ Depend on send date

Next Run Time  
The report will be mailed on: 2019/06/10 00:00  
Containing data from the following period.  
2019/05/10 ~ 2019/06/09

Cancel Previous Send Now Save



14. In the date period field, select the period of time the report will be generated on. The report will be generated on the information prior to the day the report is mailed, including the day it will be mailed.

The different **Date Period** options are as below:

- **Days:** The report generated will be based on information from your selected number of days before the day the report is mailed.
- **Months:** The report generated will be based on information from your selected number of months before the day the report is mailed. Additional options are available if you selected **Months**.
  - **Entire Month:** This will generate information starting on the **Send Date's** previous month, with each month calculated from start of the month till the last day of the month.
  - **Depend on send date:** This will generate information starting on the **Send Date**, with each month calculated as the previous day of the send date till the day of the send date.

ASUS Control Center 18:00 Administrator

Software Report > Subscription Report > Subscription Report Information

**Subscription Report Information**

Report Name: Software Report by Focus List

Description: Show specific application from focus list and ignore the other application.

Apply List: ☐ Apple Trust List ☒ Apple Focus List ☒ Adobe Application ☒ Microsoft Application Select from software focus list

Enable: ☒ Enable Report

**Step 3: Set the Run Time**

Send Date: 10th day of the month 10

Data Period: Days Monthly All 1 Months

☐ Entire month ☒ Depend on send date

**Next Run Time**  
The report will be mailed on: 2019/06/10 00:00  
Containing data from the following period:  
2019/05/10 - 2019/06/09

Cancel Previous Send Now Save

15. You can view information on when you will receive the next report, and the time period the report is based on in the window below. Once you finished editing the Run Time, you may click on **Send Now** to immediately receive a report, then click on **Save** to save your settings.

**IMPORTANT:** Ensure SMTP settings have been set and that a test email can be successfully sent to ensure notifications can be properly sent and received. For more information on SMTP settings and sending a test email, please refer to the **SMTP Settings** section.

ASUS Control Center 18:00 Administrator

Software Report > Subscription Report > Subscription Report Information

**Subscription Report Information**

Report Name: Software Report by Focus List

Description: Show specific application from focus list and ignore the other application.

Apply List: ☐ Apply Trust List ☒ Apply Focus List

Enable: ☒ Enable Report

**Step 3: Set the Run Time**

Send Date: 10th day of the month

Days: ☒ Days ☐ Months ☐ All

Data Period: 1 Months

☐ Entire month ☒ Depend on send date

**Next Run Time**  
The report will be mailed on: 2019/06/10 00:00  
Containing data from the following period:  
2019/05/10 ~ 2019/06/09

Cancel Previous **Send Now** Save

- Report as a result of applying **Trust Software Asset**. (Does not show white listed applications)

Software Report by Trust List

ASUS Control Center - asusserverssd@gmail.com

Dear Directs,

Your department's software report as below, please ensure these application are followed company's policy.

|   | Software Name                         | Version    | Publisher          | Install Date | Host Name     | Login User        | Work ID   | Phone | Department |
|---|---------------------------------------|------------|--------------------|--------------|---------------|-------------------|-----------|-------|------------|
| 1 | HeavyLoad V3.5.1 (64 bit)             | 3.5.1      | JAM Software       | 2019-05-10   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |
| 2 | Concavent HD Audio                    | 8.66.65.54 | Concavent          | 2019-05-11   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |
| 3 | Intel(R) Management Engine Components | 1.0.0.0    | Intel Corporation  | 2019-05-12   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |
| 4 | Microsoft VC++ redistributables x64   | 12.0.0.0   | Intel Corporation  | 2019-05-12   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |
| 5 | Yulan Run Time Libraries 1.0.05.1     | 1.0.05.1   | Lunard, Inc.       | 2019-05-13   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |
| 6 | NetBeans IDE 8.2                      | 8.2        | NetBeans.org       | 2019-05-14   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |
| 7 | MySQL Workbench 6.3 CE                | 6.3.10     | Oracle Corporation | 2019-05-15   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |

- Report as a result of applying **Focus Software Asset**. (Only shows applications on the focus list)

Software Report by Focus List

ASUS Control Center - asusserverssd@gmail.com

Dear Directs,

Your department's software report as below, please ensure these application's license are enough.

|   | Software Name                 | Version          | Publisher             | Install Date | Host Name     | Login User        | Work ID   | Phone | Department |
|---|-------------------------------|------------------|-----------------------|--------------|---------------|-------------------|-----------|-------|------------|
| 1 | Adobe Acrobat Reader DC       | 19.010.20099     | Adobe Systems Inc.    | 2019-05-16   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |
| 2 | Microsoft Office 2016 - zh-tw | 16.0.11425.20244 | Microsoft Corporation | 2019-05-18   | ELASTICSERVER | ELASTICSERVERAian | AA1600050 | 29631 | SW         |

16. Your new report subscription should appear in the Subscription Report List on the main screen of **Subscription Report**.

ASUS Control Center 17:13 Administrator

Subscription Subscription Report

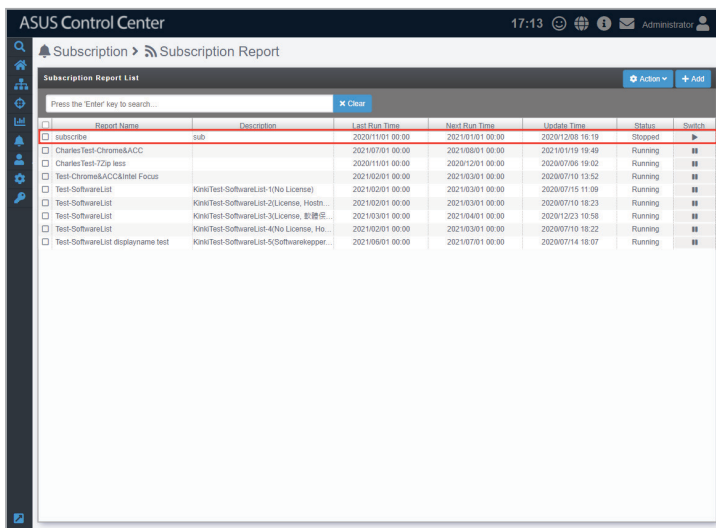
Subscription Report List Action Add

Press the 'Enter' key to search... Clear

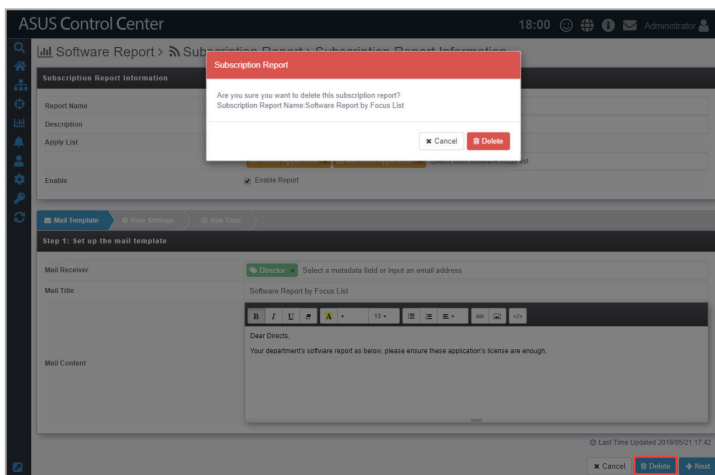
|                          | Report Name                        | Description                                | Last Run Time    | Next Run Time    | Update Time      | Status  | Switch |
|--------------------------|------------------------------------|--------------------------------------------|------------------|------------------|------------------|---------|--------|
| <input type="checkbox"/> | subscribe                          | sub                                        | 2020/11/01 00:00 | 2021/01/01 00:00 | 2020/12/08 16:19 | Stopped | ▶      |
| <input type="checkbox"/> | CharlesTest-Chrome&ACC             |                                            | 2021/07/01 00:00 | 2021/08/01 00:00 | 2021/01/19 19:49 | Running | ⏏      |
| <input type="checkbox"/> | CharlesTest-7Zip-less              |                                            | 2020/11/01 00:00 | 2020/12/01 00:00 | 2020/07/06 19:02 | Running | ⏏      |
| <input type="checkbox"/> | Test-Chrome&ACC&Intel Focus        |                                            | 2021/02/01 00:00 | 2021/03/01 00:00 | 2020/07/10 13:52 | Running | ⏏      |
| <input type="checkbox"/> | Test-SoftwareList                  | KinkiTest-SoftwareList-1[No License]       | 2021/02/01 00:00 | 2021/03/01 00:00 | 2020/07/15 11:09 | Running | ⏏      |
| <input type="checkbox"/> | Test-SoftwareList                  | KinkiTest-SoftwareList-2[License, Hosts... | 2021/02/01 00:00 | 2021/03/01 00:00 | 2020/07/10 18:23 | Running | ⏏      |
| <input type="checkbox"/> | Test-SoftwareList                  | KinkiTest-SoftwareList-3[License, 軟體保...   | 2021/03/01 00:00 | 2021/04/01 00:00 | 2020/12/23 10:58 | Running | ⏏      |
| <input type="checkbox"/> | Test-SoftwareList                  | KinkiTest-SoftwareList-4[No License, Ho... | 2021/02/01 00:00 | 2021/03/01 00:00 | 2020/07/10 18:22 | Running | ⏏      |
| <input type="checkbox"/> | Test-SoftwareList displayName test | KinkiTest-SoftwareList-5[Softwarekeeper... | 2021/06/01 00:00 | 2021/07/01 00:00 | 2020/07/14 18:07 | Running | ⏏      |

## To edit or delete a subscription report:

1. Click on the subscription report you wish to edit.

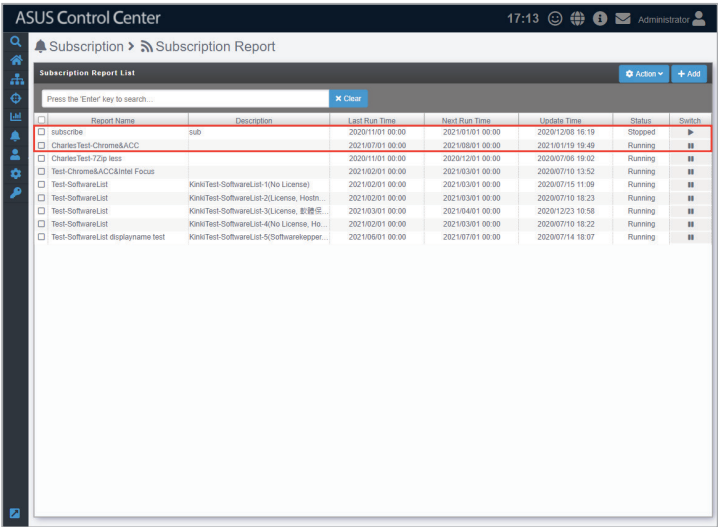


2. Repeat steps 2 to 14 of the **To create a Subscription Report** section to edit a subscription report, or click on **Delete** to delete the subscription report.

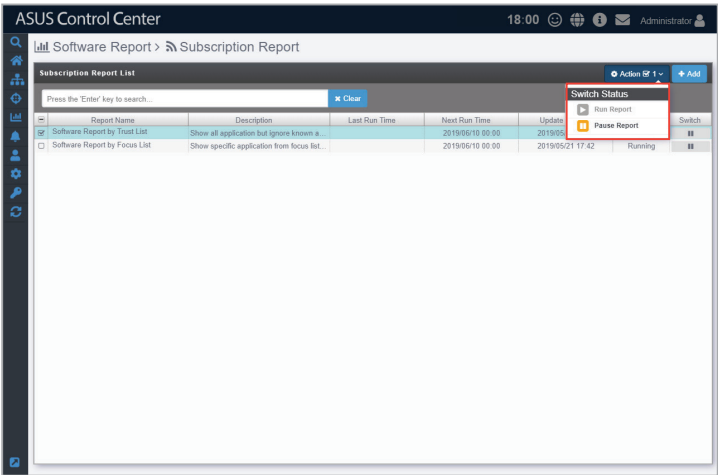


Switching the status of a subscription reports:

- 1. Click on the subscription reports you wish to switch the subscription status of.



- 2. Click on **Action**, then select if you want to pause or run the report.





# Chapter 7

This chapter describes how to add and edit accounts and roles for different users.

# Account Management

## 7.1 Role Privilege Management

**Role Privilege** will allow you to create roles with different permissions which gives you control over the functions and information accessible to each role created.

A **Viewer** role privilege is available by default, which only allows accounts assigned with this role privilege to view all the functions, but cannot edit customized roles.

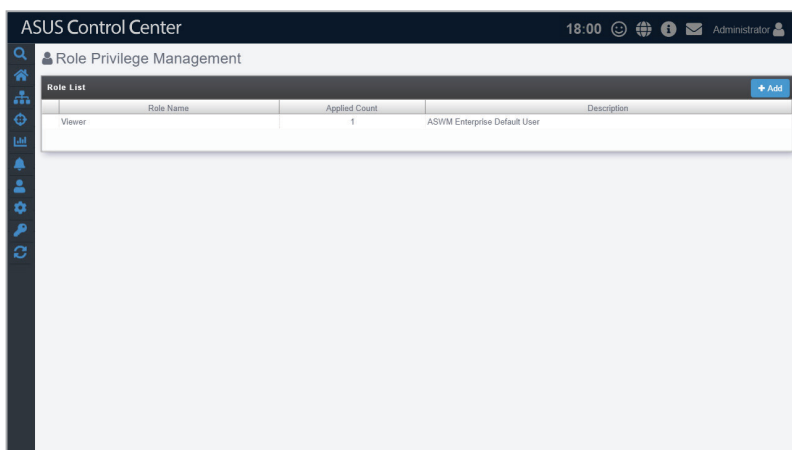
There is no Administrator role in the **Role List** by default, but you can create one by enabling all permissions when creating a new role, this will allow accounts assigned with this role to add, edit, or delete when using any function, and also allows you to customize roles.

---

**NOTE:** The **Admin** role assigned to the default Administrator account of ASUS Control Center will not appear in the **Role List** and cannot be edited.

---

To access **Role Privilege Management**, Click  in the left menu, then click on **Role Privilege**.

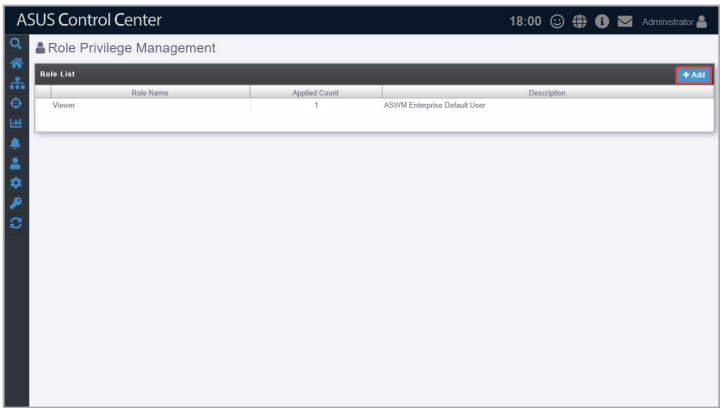




**Adding a new role**

You can add new roles and set the permissions of this role. For example, assigning an account with Software User role which is customized to only allow users with this role access to ASUS Control Center software related functions, or creating an account with BIOS User role which is customized to only allow users access to ASUS Control Center BIOS related functions.

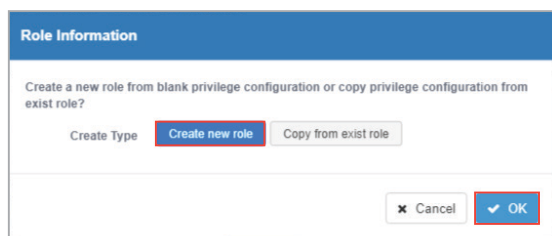
- 1. Click on **Add**.



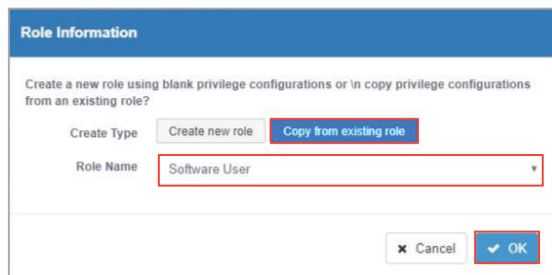
2. Select between **Create new role** and **Copy from exist role**, then click **OK**.

**NOTE:**

- **Create new role:** Create a new role with no permissions enabled in **Privilege Configurations**.
- **Copy from exist role:** Select from an existing role (including the Admin role assigned to ASUS Control Center's default administrator account), this will load the **Privilege Configurations** of the selected account into the new role.



The screenshot shows a dialog box titled "Role Information". The text inside says "Create a new role from blank privilege configuration or copy privilege configuration from exist role?". Below this text are two buttons: "Create new role" (highlighted with a red box) and "Copy from exist role". At the bottom right, there are two buttons: "Cancel" and "OK" (highlighted with a red box).

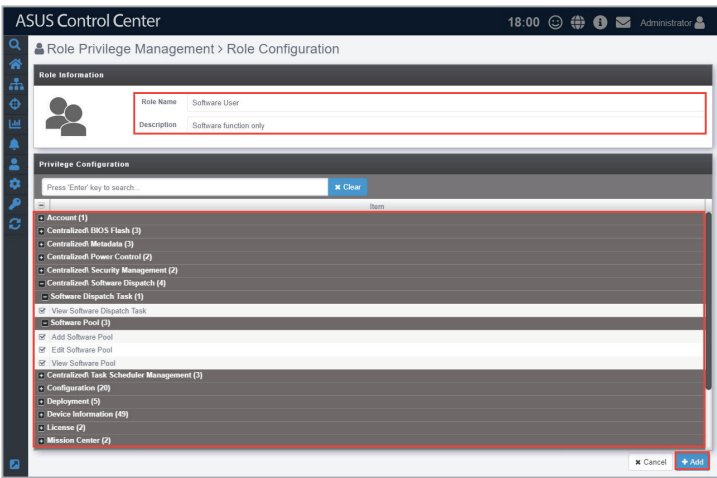


The screenshot shows the same "Role Information" dialog box. The text inside says "Create a new role using blank privilege configurations or 'n copy privilege configurations from an existing role?". Below this text are two buttons: "Create new role" and "Copy from existing role" (highlighted with a red box). Below the buttons is a text field labeled "Role Name" containing the text "Software User" (highlighted with a red box). At the bottom right, there are two buttons: "Cancel" and "OK" (highlighted with a red box).

3. Enter the Role Name and Description of the new role.
4. Select and check / uncheck the permissions to enable / disable for the role in the **Privilege Configuration** block.

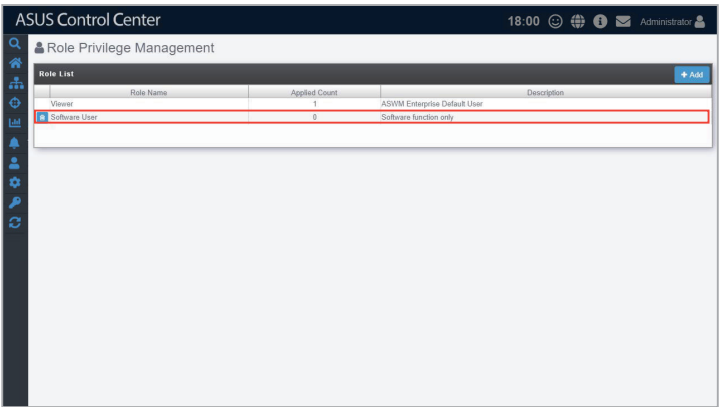
**NOTE:**

- If you chose **Copy from exist role** in step 2, your **Privilege Configurations** list should be the same as the role you selected to copy from. You can still customize the permissions for this new role.
  - You can click on  /  next to each permission category to expand / collapse the category to view / hide the permissions available for that permission category.
  - You can use the Search Bar to search and filter through the permission items in the **Privilege Configurations** list.
5. Click **Add** once you have finished.

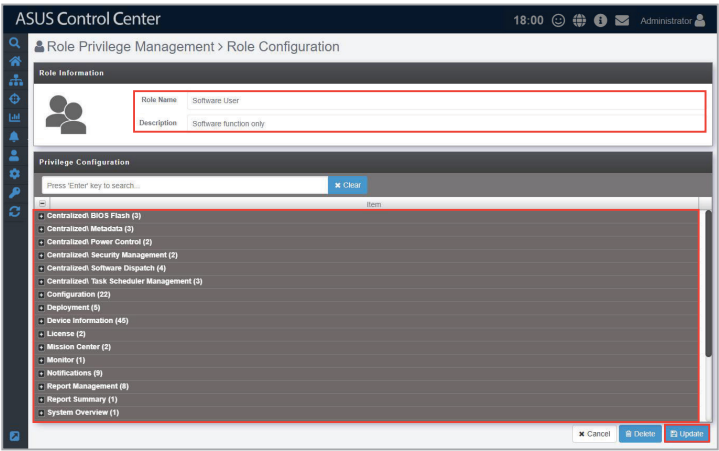


## Editing a role

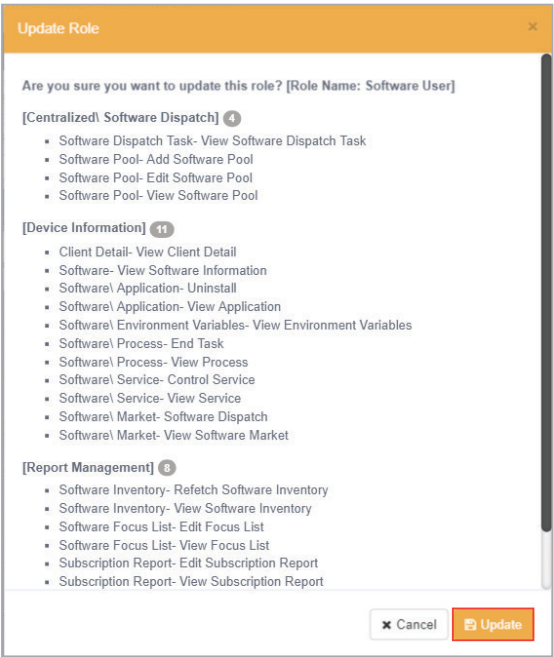
1. Click on the role you wish to edit from the Role List block.



2. You can edit the **Role Name** and **Description**, and also configure the permissions in the Privilege Configuration list. Once you are finished click on **Update**.



3. A pop-up window should appear and allow you to check the changes made to the role, click on **Update** to confirm these changes.



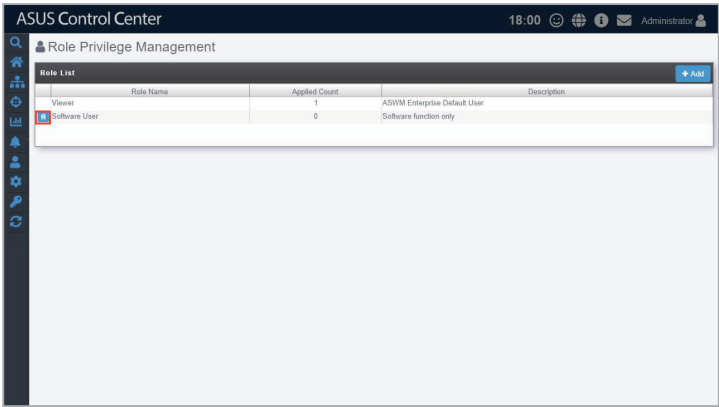
## Deleting a role

**CAUTION:** Account(s) associated with a role will be deleted too when you delete a role. You can check how many accounts are associated with the role in the Applied Count column. For more information on managing accounts, please refer to the **Accounts Management** section.

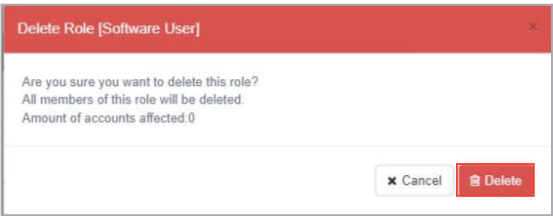
You can delete a role using the following methods:

- Deleting the role from the Role List

1. Click on  next to the role you wish to delete.

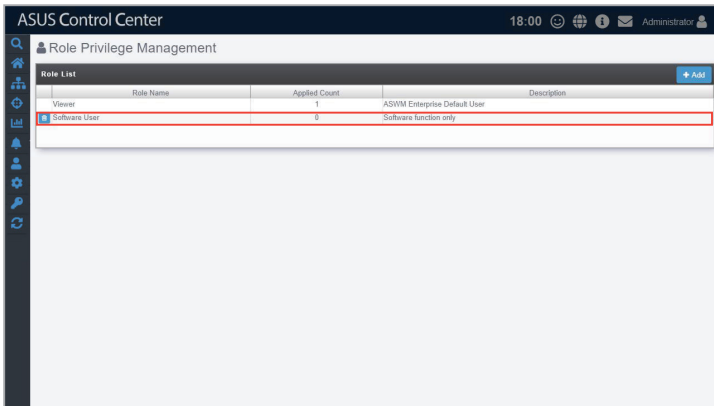


2. Click Delete to delete the role.

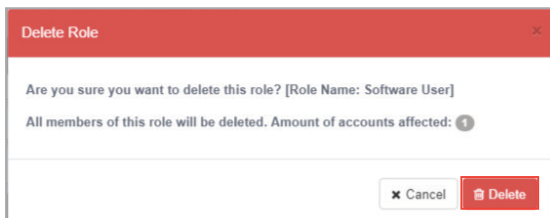
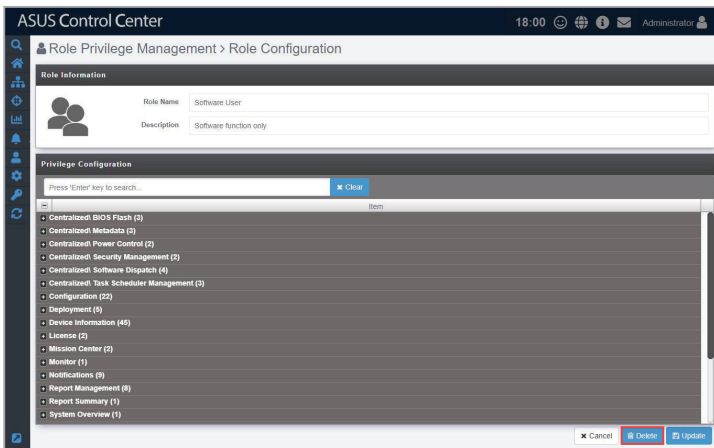


- Deleting the role from Role Configuration

1. Click on the role you wish to delete from the **Role List** block.



2. Click Delete to delete the role.

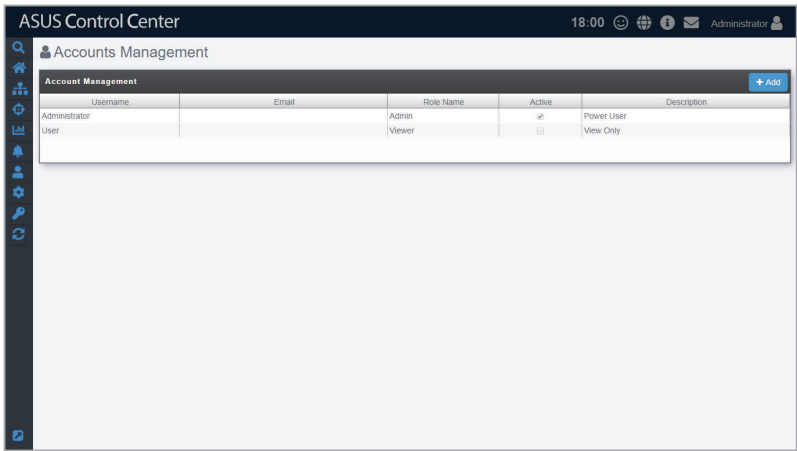


## 7.2 Accounts Management

**Accounts Management** displays all user accounts on ASUS Control Center, and allows you to add, edit, or delete accounts. ASUS Control Center comes with a default Administrator account with Admin role privileges, and a User account with Viewer role privileges.

To access **Accounts Management**, you can use the following methods:

- Click  in the left menu, then click on **Accounts Management**.
- Click  (**Account Information**) in the top right corner, then select **Settings**.



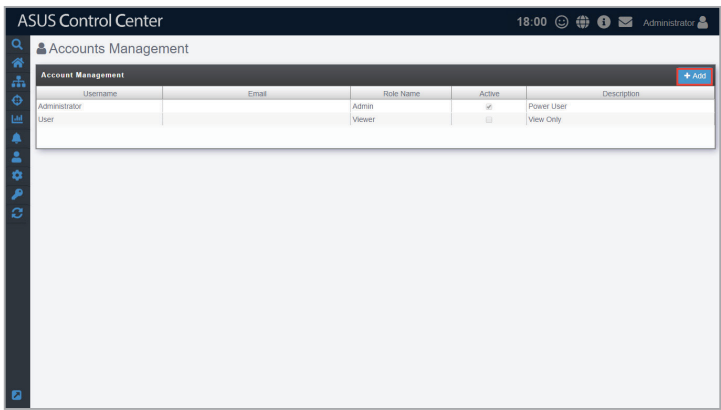


### Adding a new account

You can add new accounts and apply customized roles to them, allowing you to and control the functions and information each account can access with ease. For example, assigning an account with Software User role which is customized to only allow users with this role access to ASUS Control Center software related functions, or creating an account with BIOS User role which is customized to only allow users access to ASUS Control Center BIOS related functions.

**NOTE:** For more details on role privileges, please refer to the **Role Privilege Management** section.

1. Click on **Add**.



2. Enter the username, password, and email of the new account.
3. Select a role in the **Role Name** field.

---

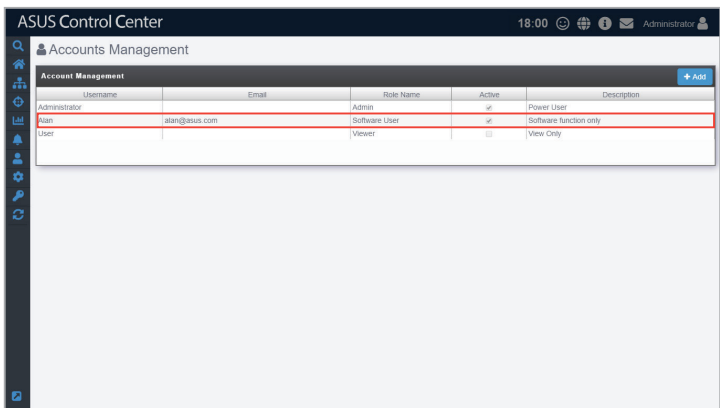
**NOTE:** For more details on adding new roles, please refer to **Add Role** under the **Role Privilege Management** section.

---

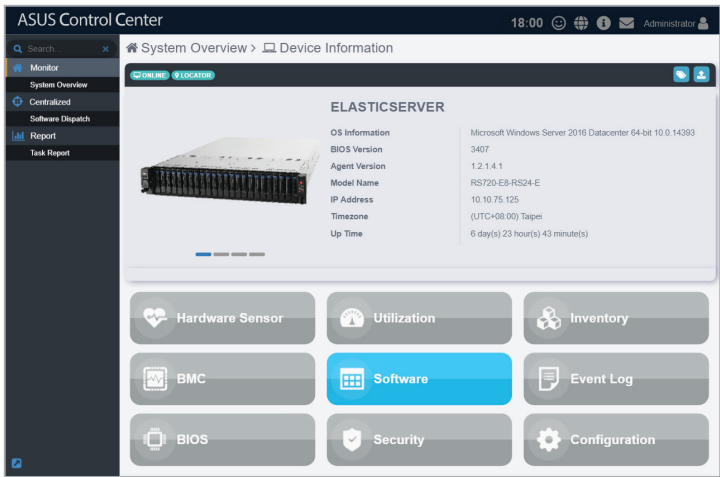
4. Enter a brief description for the account.
5. (optional) Check or uncheck **Enable the account** in the **Active** field to enable or disable the newly created account.
6. Click on **Save** once you have finished.

The screenshot shows a web form titled "Add New Account" with a green header bar. The form contains several input fields and a checkbox, all of which are highlighted with red rectangular boxes. The fields are: Username (text input with "Alan"), Password (password input with "••••••••"), Confirm Password (password input with "••••••••"), Email (text input with "alan@asus.com"), Role Name (dropdown menu with "Software User" selected), Description (text input with "Software function only"), and Active (checkbox labeled "Enable the account" which is checked). At the bottom right of the form are two buttons: "Cancel" and "Save".

7. Your newly created account should appear in the **Account Management** list.

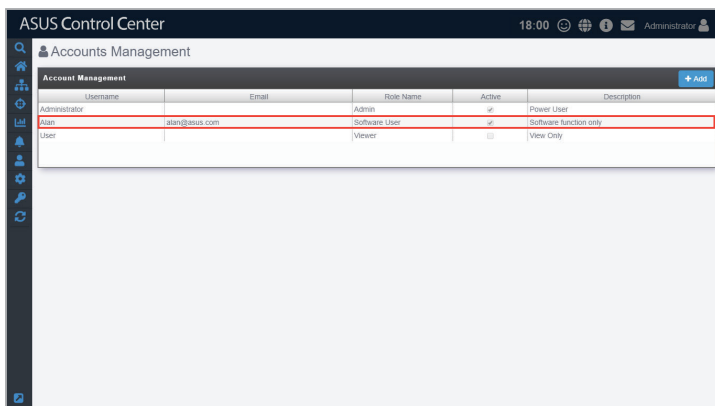


Logging in to ASUS Control Center using different accounts with different roles assigned will affect the items the account can gain access to, depending on the permissions assigned to the role selected. For example, logging in an account which you have set to a role with access only to Software related functions will result in the following screenshot.



## Editing an account

1. Click on the account you wish to edit.



2. You can edit the **Password**, **Email**, **Role Name**, **Description**, and **Active** fields. Once you have finished editing click on **Save** to save the changes made.

The 'Edit Account' dialog box is shown with the following fields and options:

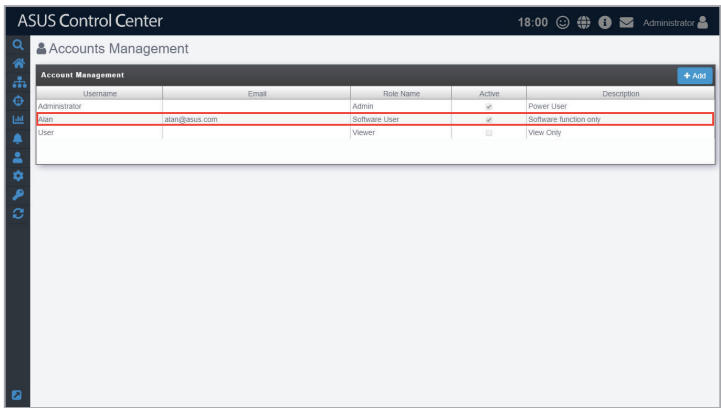
- Username:** Alan
- Password:** e.g., \*\*\*\*\* (with an eye icon to toggle visibility)
- Confirm Password:** e.g., \*\*\*\*\* (with an eye icon to toggle visibility)
- Email:** alan@asus.com
- Role Name:** Software User (dropdown menu)
- Description:** Software function only
- Active:** ☒ Enable the account

At the bottom, there are three buttons: 'Cancel', 'Delete', and 'Save'.

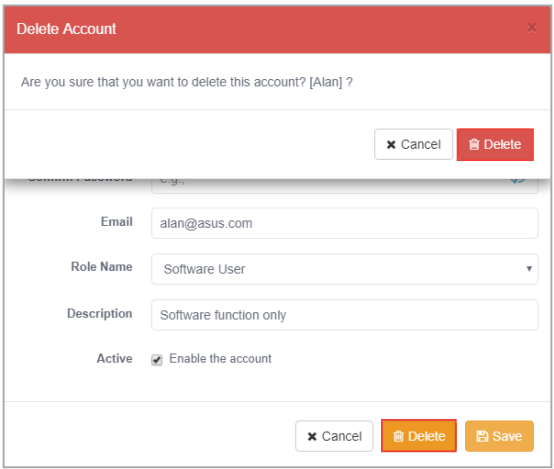
## Deleting an account

**NOTE:** The default **Administrator** and **User** accounts cannot be deleted.

1. Click on the account you wish to delete.



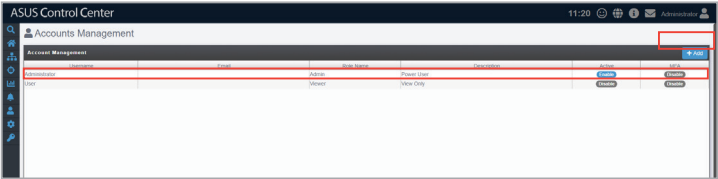
2. Click on **Delete**, then click on **Delete** again on the confirmation pop-up to delete the account.



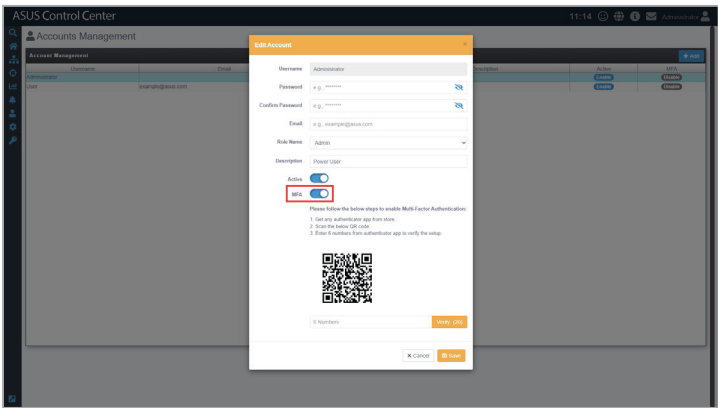
## Enabling multi-factor authentication (MFA)

**NOTE:** It is only possible to enable or disable MFA for currently logged in account.

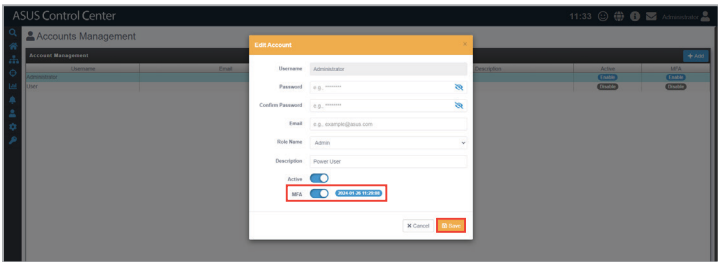
1. Click on the currently logged in account.



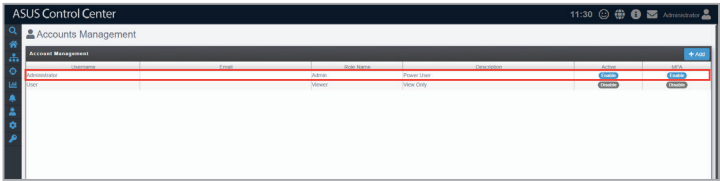
2. Enable the **MFA** option, then scan the QR code using an authenticator app and enter the 6-digit passcode to verify the multi-factor authentication setup.



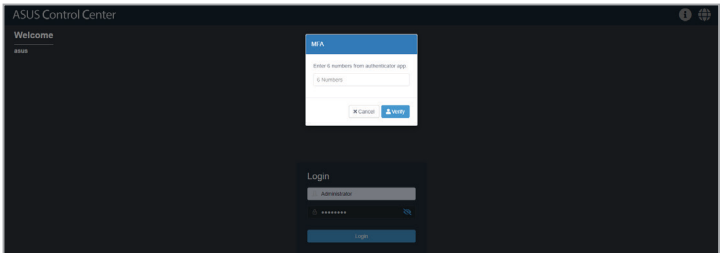
3. Once MFA is enabled, the MFA field will show when MFA was enabled for this account. Click **Save**.



4. Click on the currently logged in account again.



5. Enter the 6-digit passcode from the authenticator app, then click **Verify**.

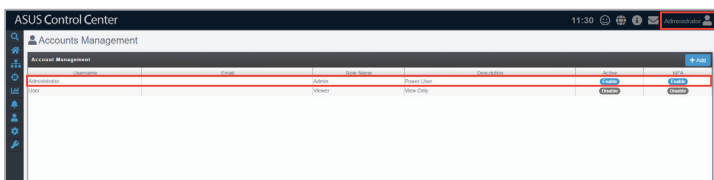


## Disabling multi-factor authentication (MFA)

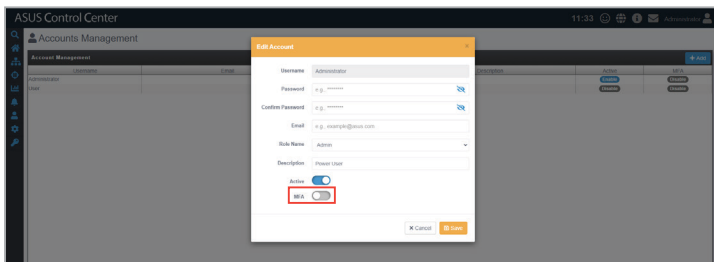
### NOTE:

- It is only possible to enable or disable MFA for the currently logged in account.
- Only the default Administrator account can view the MFA status of other accounts.

1. Click on the currently logged in account.



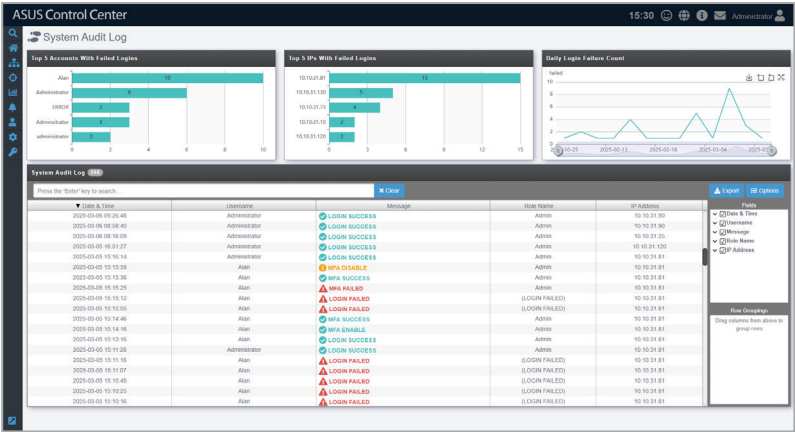
2. Disable the **MFA** option.





## 7.3 System Audit Log

This page allows you to view the system audit log.



### Filtering the system audit log

To filter the system audit log, click a user, IP address, or date in the bar graphs or time series chart. You can also use the search field and search options in the **System Audit Log** block to manually define search criteria.

**NOTE:**

- Only the Administrator account can access the system audit log.
- The **Role Name** column may display **(LOGIN FAILED)** in cases where the account name is unknown.

### 7.3.1 System audit log events

The following events will be logged in the system audit log:

| Event         | Description                                                |
|---------------|------------------------------------------------------------|
| LOGIN SUCCESS | Successful login attempt with MFA disabled.                |
| LOGIN FAILED  | Failed login attempt due to incorrect account credentials. |
| MFA ENABLE    | MFA was enabled for this account.                          |
| MFA DISABLE   | MFA was disabled for this account.                         |
| MFA SUCCESS   | Successful login attempt with MFA enabled.                 |
| MFA FAILED    | Failed login attempt due to incorrect MFA response.        |



# Chapter 8

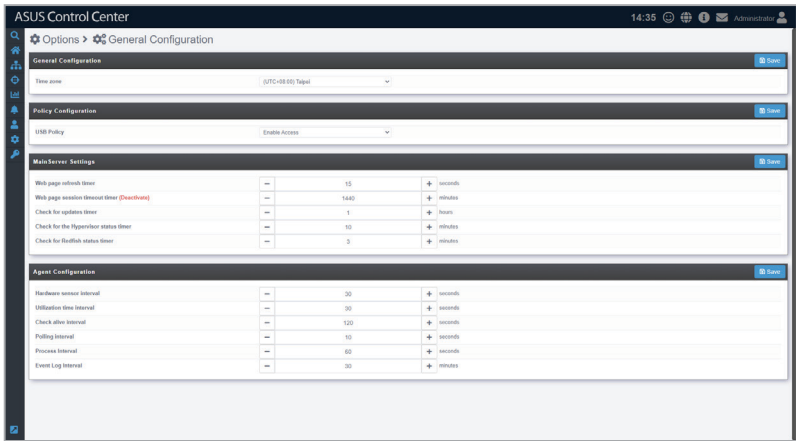
This chapter describes system, network, appearance, security, SMTP, backup and restore, maintenance, DBExpose, update, access control, sensor threshold, and software list configuration options.

# Options

# 8.1 General Configuration

The **General Configuration** allows you to configure different settings for the main ASUS Control Center server and agents, as well as set the time zone.

To access **General Configuration**, click  in the left menu, then click on **General Configuration**.



## Adjusting items on the General configurations page

Configure the items in the **General Configurations** block, **MainServer Settings** block, and **Agent Configuration** block, then click on **Save** to save the changes made. For more details on the different configuration options available, please refer to the tables below:

| General Configuration |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Zone             | <p>Adjust the time zone of the underlying Linux system the ASUS Control Center's main server is installed on.</p> <p>* The time zone set here should match the time zone of the system of the VM with ASUS Control Center installed.</p> <p>** Adjusting this item will only affect the initialization of ASUS Control Center, and will not affect the time displayed in the top right of ASUS Control Center, nor will it affect the Agent and Event Log response times.</p> |

| Policy Configuration |                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------|
| USB Policy           | <p>Set the default USB policy to enable or disable USB devices on new managed devices.</p> |

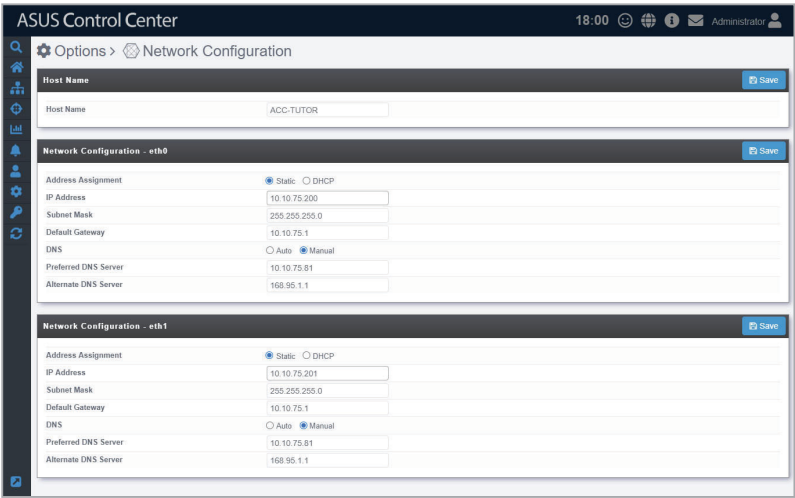
| Main Server Settings                  |                                                                                                                                                                                                                                                                                        |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web page refresh timer                | <p>Set the time interval in seconds between each refresh of data on all webpages of the main server.</p> <p>* This setting will affect the response time for items such as System Overview and Event Log.</p>                                                                          |
| Web page session timeout timer        | <p>Set the time interval in seconds for the web page session timeout timer, which causes web sessions to be logged out after no activity is detected for the specified amount of time. The default setting of 1440 minutes (24 hours) disables the web page session timeout timer.</p> |
| Check for updates timer               | <p>Set the time interval in hours for the main server and agent update check.</p> <p>* This setting will affect the main server and agent version check timer in the Updates page, and may require an Internet connection.</p>                                                         |
| Check for the Hypervisor status timer | <p>Set the time interval in minutes ASUS Control Center should perform a status check on managed vSpheres.</p> <p>* This setting will affect the response times for items in the VM Overview page such as vSphere hardware sensors and utilization .</p>                               |
| Check for Redfish status timer        | <p>Set the time interval in minutes ASUS Control Center should perform a status check on managed Redfish devices.</p>                                                                                                                                                                  |

| Agent Configuration       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware sensor interval  | Set the time interval in seconds for the agents of all managed devices to return <b>Hardware Sensor</b> values. The default setting is 30 seconds, which means that the agents need to report <b>Hardware Sensor</b> values and status every 30 seconds. For example, if a fan was removed from a device, ASUS Control Center's web interface should receive and update the status for fan abnormality within 30 seconds (Web page refresh time could affect the update time). |
| Utilization time interval | Set the time interval in seconds for the agents of all managed devices to return <b>Utilization</b> values. The default setting is 30 seconds, which means that the agents need to report Utilization values and status every 30 seconds. For example, if a stress test was performed on a CPU, ASUS Control Center's web interface should receive and update the status for CPU abnormality within 30 seconds (Web page refresh time could affect the update time).           |
| Check alive interval      | Set the time interval in seconds for the agents of all managed devices to return the connection status. The default setting is 120 seconds, which means that the agents need to report the connection status every 120 seconds. For example, if a device loses connection, ASUS Control Center's system overview should display it as "Offline" after 120 seconds (Web page refresh time could affect the update time).                                                        |
| Polling interval          | Set the time interval in seconds for the agents of all managed devices to query tasks from ASUS Control Center. The default setting is 10 seconds, which means that the agents need to query ASUS Control Center if there is a task for that device every 10 seconds. For example, the device should perform a task of disabling the registry, locally, within 10 seconds of disabling the registry of that device on the ASUS Control Center web interface.                   |
| Process interval          | Set the time interval in seconds for the agents of all managed devices to return PID (Process ID) values. The default setting is 60 seconds, which means that the agents need to report PID values every 60 seconds.<br><br>* To view process information, refer to Software under the Device Information section.                                                                                                                                                             |
| Event log interval        | Set the time interval in seconds for the agents of all managed devices to return Event Log entries. The default setting is 30 minutes, which means that the agents need to provide an updated Event Log every 30 minutes.<br><br>* To view event logs, refer to Event Log under the Device Information section.                                                                                                                                                                |

## 8.2 Network Configuration

The **Network Configuration** allows you to configure the network for the ASUS Control Center main server. When the device with ASUS Control Center or a hypervisor features multiple network cards, you can configure multiple networks to allow ASUS Control Center to manage different network segments.

To access **Network Configuration**, click  in the left menu, then click on **Network Configuration**.



ASUS Control Center 18:00 Administrator

Options > Network Configuration

**Host Name** Save

Host Name ACC-TUTOR

**Network Configuration - eth0** Save

Address Assignment ☒ Static ☐ DHCP

IP Address 10.10.75.200

Subnet Mask 255.255.255.0

Default Gateway 10.10.75.1

DNS ☐ Auto ☒ Manual

Preferred DNS Server 10.10.75.81

Alternate DNS Server 168.95.1.1

**Network Configuration - eth1** Save

Address Assignment ☒ Static ☐ DHCP

IP Address 10.10.75.201

Subnet Mask 255.255.255.0

Default Gateway 10.10.75.1

DNS ☐ Auto ☒ Manual

Preferred DNS Server 10.10.75.81

Alternate DNS Server 168.95.1.1

### Adjusting the Network configurations

Configure the items in the **Host Name** block and **Network Configuration** block then click on **Save** to save the changes made. For more details on the different configuration options available, please refer to the tables below:

| Host Name |                                                                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name | <p>The name of the ASUS Control Center main server.</p> <p>* You will need to refer to the Host Name set here when manually installing Windows agents to devices.</p> |

| Network Configuration |                                                                                                                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address Assignment    | Select <b>DHCP</b> to automatically set the <b>IP address</b> and <b>Subnet Mask</b> . Select <b>Static</b> to enter the <b>IP address</b> and <b>Subnet Mask</b> manually. |
| IP Address            | Enter the IP address for this network card.<br>* You can only set the IP Address manually if you selected Static in the Address Assignment field.                           |
| Subnet Mask           | Enter the Subnet Mask for this network card.<br>* You can only set the Subnet Mask manually if you selected Static in the Address Assignment field.                         |
| Default Gateway       | Enter the default gateway for this network card.                                                                                                                            |
| DNS                   | Select <b>Auto</b> to automatically set the <b>DNS Server</b> , or select <b>Manual</b> to manually configure the <b>DNS Server</b> .                                       |
| Preferred DNS Server  | Enter the Preferred DNS Server for this network card.<br>* You can only set the Preferred DNS Server manually if you selected Manual in the DNS field.                      |
| Alternate DNS Server  | Enter the Alternate DNS Server for this network card.<br>* You can only set the Alternate DNS Server manually if you selected Manual in the DNS field.                      |

**NOTE:**

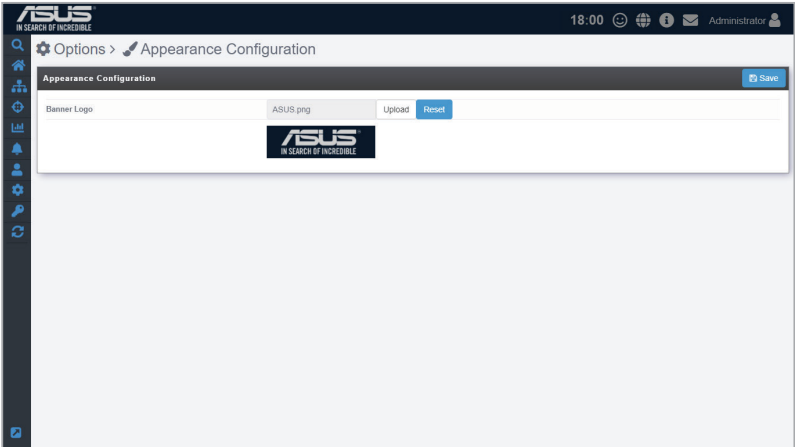
- The amount of **Network Configuration** blocks available will depend on the amount of network cards available.
- You will be logged out of ASUS Control Center when you save the changes made to the **Network Configuration** block(s). If you changed the IP address, you will need to enter the new IP address when logging in.



### 8.3 Appearance Configuration

The **Appearance Configuration** allows you to customize and personalize your ASUS Control Center's top left banner logo.

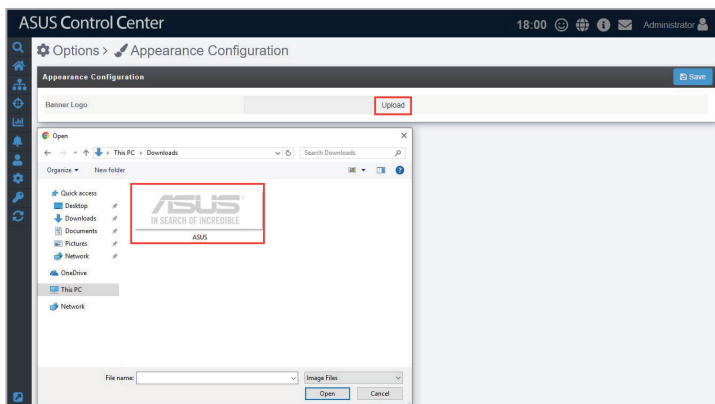
To access **Appearance Configuration**, click  in the left menu, then click on **Appearance Configuration**.



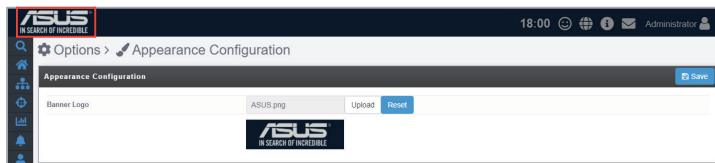
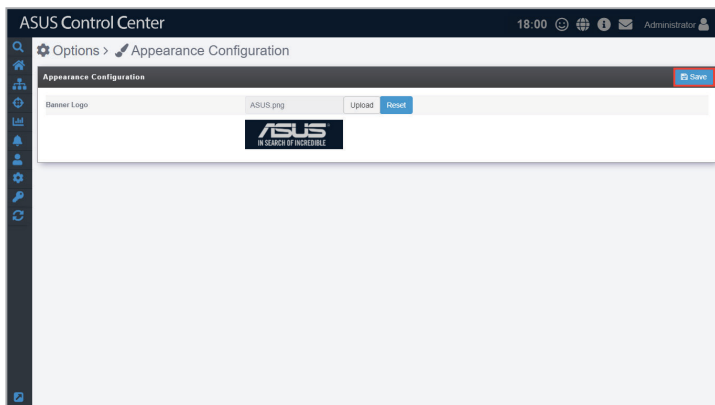
## Setting a custom banner logo

1. Click on **Upload**, then select your new banner logo.

**NOTE:** The height dimension of the logo image file should be 56 pixels.

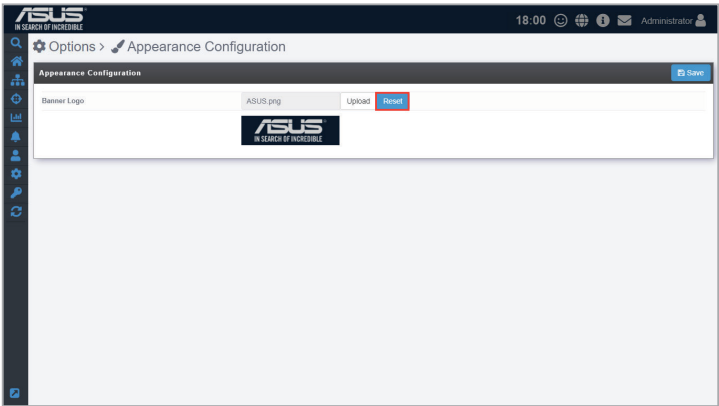


2. Once you have finished uploading the new banner logo, click on **Save**.

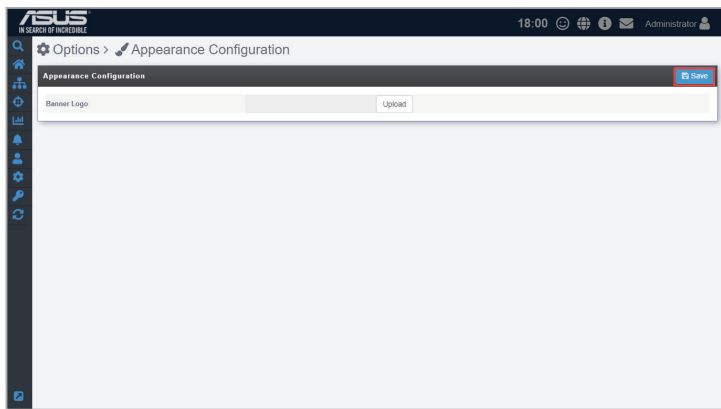


**Resetting the banner logo**

- 1. Click on **Reset** to reset your banner logo to the default banner logo.



- 2. Click on **Save** to save the changes made.



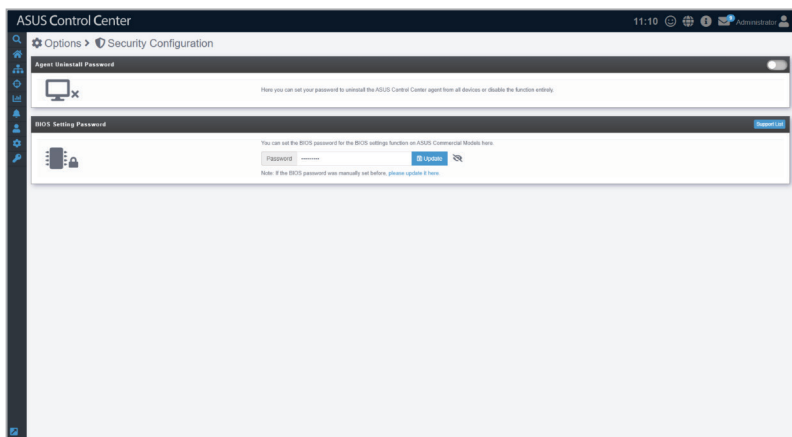
## 8.4 Security Configuration

**NOTE:** This function is only available for Windows® OS managed devices.

The **Security Configuration** allows you to set a password as a method to prevent users from removing the agents themselves. This enables a more centralized control over all managed Windows® devices.

This password is separate from the agent uninstall password on individual devices (**Device Information > Configuration**), and setting this password will not override the individual agent uninstall passwords.

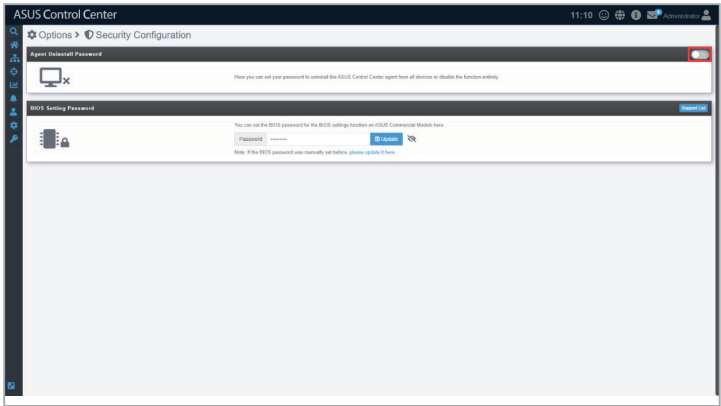
To access **Security Configuration**, click  in the left menu, then click on **Security Configuration**.



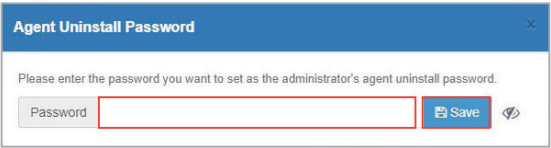
# 8.4.1 Agent Uninstall Password

## Setting a new password

1. Toggle the slider to bring up the pop-up window to set the Administrator's Agent Uninstall Password.

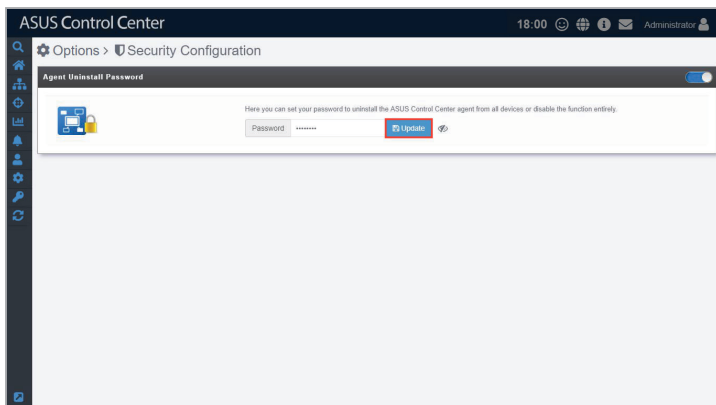


2. Enter the password you wish to set as the Administrator's Agent Uninstall Password, then click **Save** to set the new password.



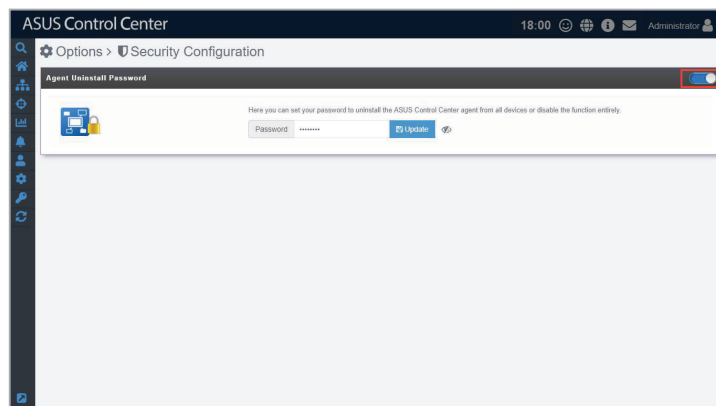
## Editing the password

Click on the **Update** button, then re-enter your new password and click on **Save** to save your new password.



## Disabling the password

Click on the button located at the top right to disable the Administrator's Agent Uninstall Password.



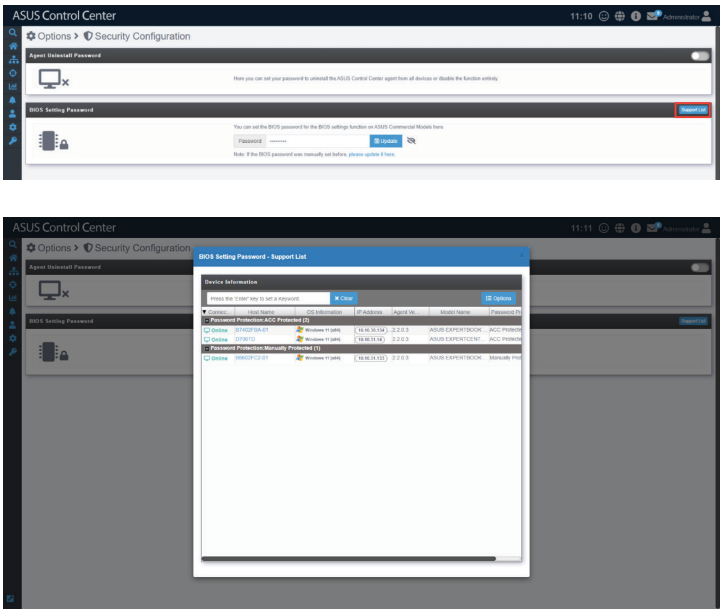
### 8.4.2 BIOS Setting Password

When an agent is installed onto a device without a BIOS password, ASUS Control Center will automatically enable BIOS Password Protection and set a BIOS password that meets complexity requirements. In such cases, the client's BIOS password protection status will be defined as "ACC Protected".

BIOS Password Protection cannot be automatically enabled if the device has an existing BIOS password. In such cases, the client's BIOS password protection status will be defined as "Manually Protected".

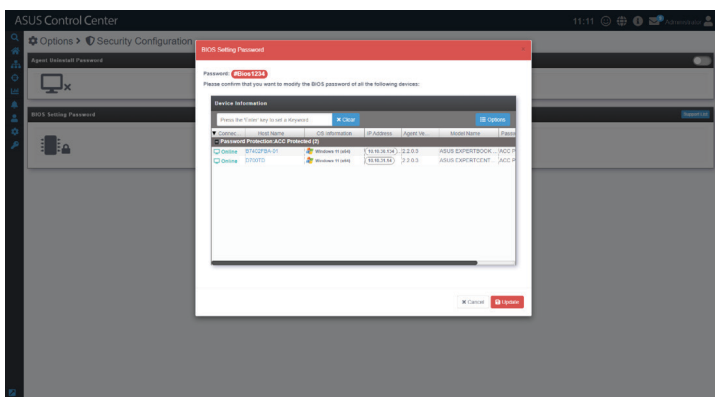
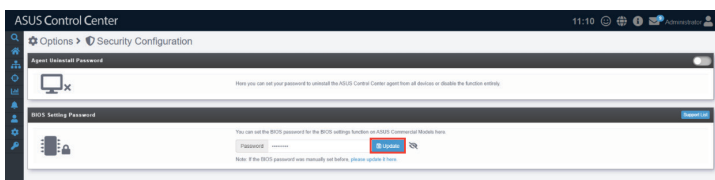
#### Viewing the BIOS password protection status

Click **Support List** to view the BIOS password protection status for all devices.



## Updating ACC Protected BIOS passwords

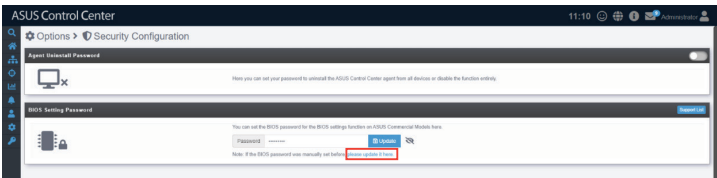
Click on the **Update** button to open a list of ACC Protected devices, then click **Update** in the popup window to update the BIOS password.





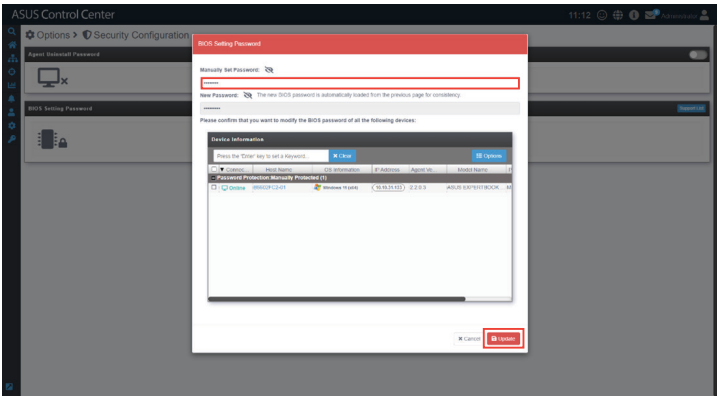
## Updating manually protected BIOS passwords

1. Click **Please update it here** to open a list of manually protected devices.



2. Enter the device's existing BIOS password, then click **Update** to update the BIOS password. BIOS Password Protection will automatically be enabled and the device's status will change to "ACC Protected".

**NOTE:** For security reasons, the existing BIOS password is required to make any changes. This protects the client devices from malicious attacks that may compromise the BIOS.



# 8.5 SMTP Settings

**NOTE:** The information entered in this section is for reference only.

Set up the SMTP (Simple Mail Transfer Protocol) for ASUS Control Center to allow feedback on system failures and alerts to be sent via email to the system administrator.

To access **Software Report**, click  in the left menu, then click on **SMTP Settings**.

ASUS Control Center

18:00

Administrator

SMTP Settings

Display Name

ASUS Control Center SMTP

SMTP Server

smtp.gmail.com

SMTP Port

587

Sender Address

asusserverssd@gmail.com

Sender Password

\*\*\*\*\*

Enable SSL

☒ Yes, I want to enable SSL

Send From

☒ Send by Server ☒ Send by Client

Send Test Mail

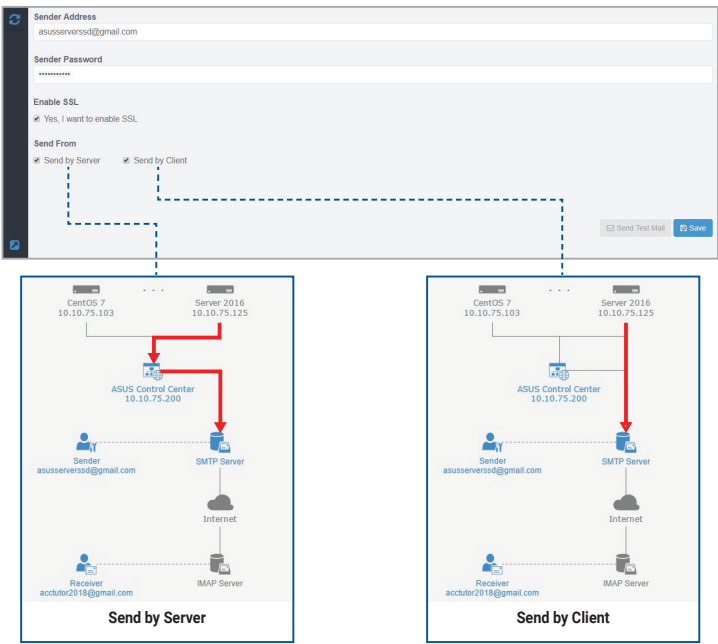
Save

**To set up the SMTP Server:**

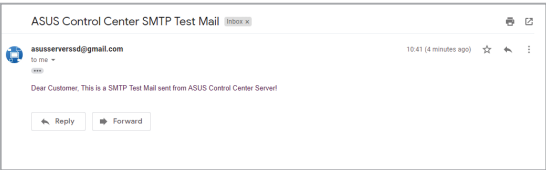
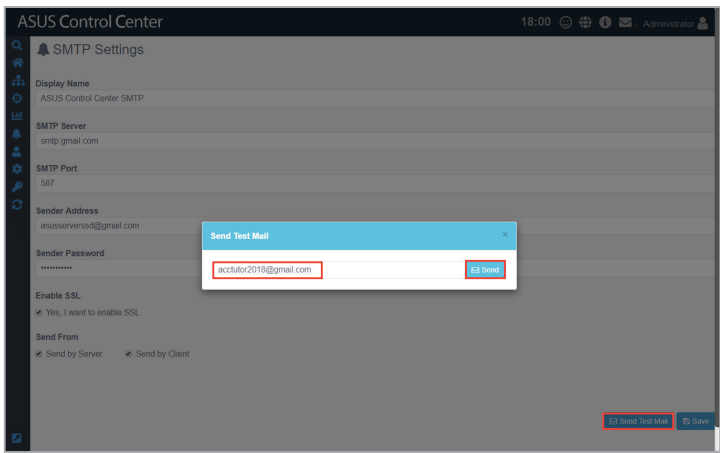
1. Fill in or check the following fields:

|                        |                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Display Name</b>    | The name of this SMTP setting. The display name will not appear on sent emails.                                                            |
| <b>SMTP Server</b>     | The SMTP server responsible for collecting and sending emails                                                                              |
| <b>SMTP Port</b>       | Service port for SMTP. Common ports used are 25 (SMTP former default port), 465 (encrypted SMTP), and 587 (new SMTP default)               |
| <b>Sender Address</b>  | The email of the ACC notification sender. This email address must exist within the SMTP Server service                                     |
| <b>Sender Password</b> | The password for the ACC notification email sender                                                                                         |
| <b>Enable SSL</b>      | Enables mail sent or forwarded through this SMTP server are SSL encrypted                                                                  |
| <b>Send by Server*</b> | When there are issues with managed devices whilst within the same domain as ACC, ACC will send emails using the SMTP server                |
| <b>Send by Client*</b> | When there are issues with managed devices whilst not in the same domain as ACC, the managed device will send emails using the SMTP server |

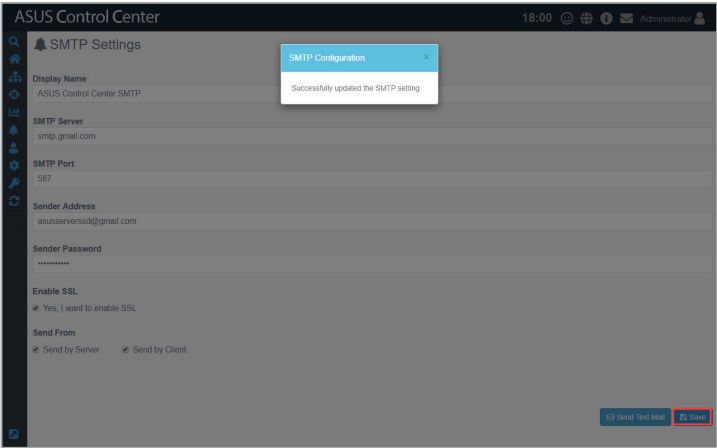
**NOTE:** Refer to the flow chart for more details on the difference between Send by Server and Send by Client.



2. (optional) Click on **Send Test Mail**, then enter an email and click **Send** to receive the test mail to check the status of the SMTP. If the SMTP is functioning properly, you should receive an email.



3. Click **Save** to save the changes made.

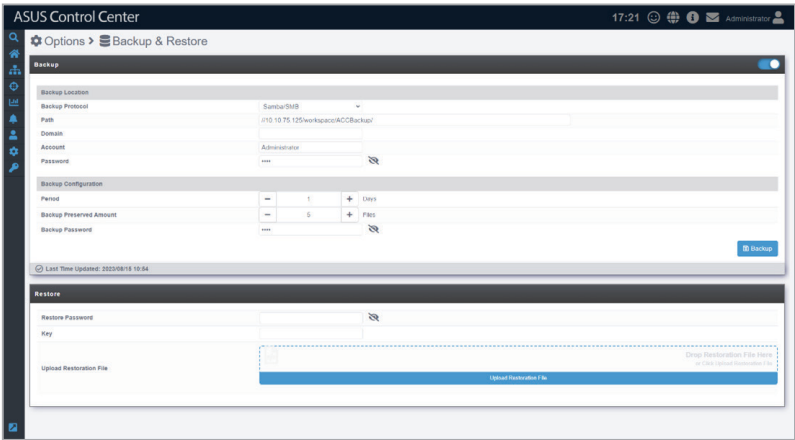


# 8.6 Backup & Restore

**NOTE:** This function is only available for ASUS Control Center Enterprise edition.

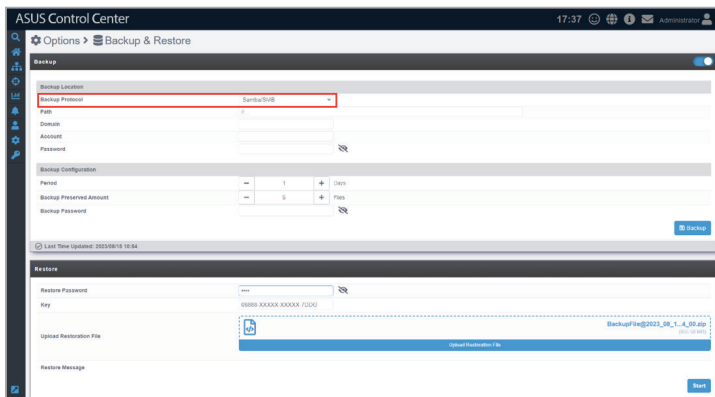
The **Backup & Restore** function allows you to set a periodic backup of the settings and configurations of ASUS Control Center to another backup device, allowing you to easily restore the backup settings and configurations if something were to happen to the ACC VM.

To access **Backup & Restore**, click  in the left menu, then click on **Backup & Restore**.



## Enabling periodic backup

1. Select a Backup Protocol (currently only supports Samba / SMB protocols).



If you wish to back up your ACC to a Linux OS device's SMB folder, do the following:

- Close SELinux
  - For RHEL, CentOS, Scientific Linux
    - a. Open `/etc/sysconfig/selinux`.
    - b. Set `SELINUX=enforcing` to `SELINUX=disabled`.
    - c. Reboot the system.
  - For Debian, Ubuntu

SELinux is not installed by default in Debian and Ubuntu.
- Adding to the Firewall whitelist
  - For RHEL, CentOS, Scientific Linux
    - If you are using **iptables**:
      - a. Input the following command to allow 137, 138, and 139 ports:

```
-A INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
```

- b. Restart the service for the changes to take effect by using the following command:  
`systemctl restart iptables.`

- If you are using **firewalld**:

Enter the following commands to add Samba access privileges: `firewall-cmd --permanent --zone=public --add-service=samba.`

- For Debian, Ubuntu

If you are using **ufw**, the system has already added `nf_conntrack_netbios_ns` to `IPT_MODULES` under `/etc/default/ufw` by default, so access should already be allowed.

- Enable write permissions for the destination folder

The “Write” permission should be enabled for “other(O)” in the folder you wish to back up to. You can use the following command:

`chmod -R 755 /home/acc/backup.`

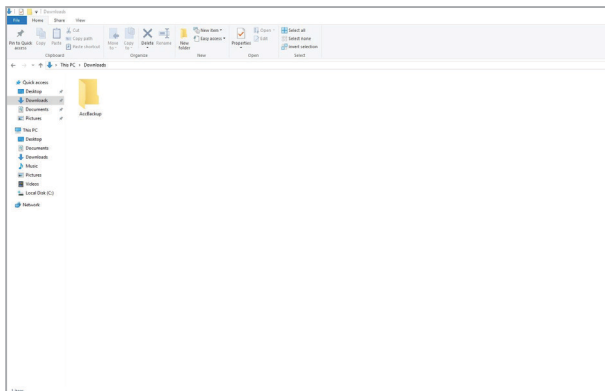
- Modify the Samba configuration file

- a. Open `/etc/samba/smb.conf`.
- b. Set the **security** variable in **Global Setting** to “user”.
- c. Set the **writable** variable in **Share Definitions** to “yes”.

If you wish to back up your ACC to a Windows OS device’s SMB folder, do the following on the Windows OS device you wish to backup to:

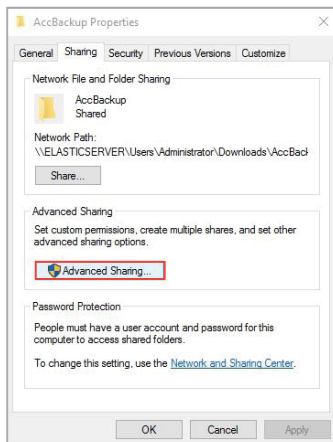
- Create, share, and enable permissions for the destination folder

- a. Create a new folder and enter a name for it, for example **AccBackup**.

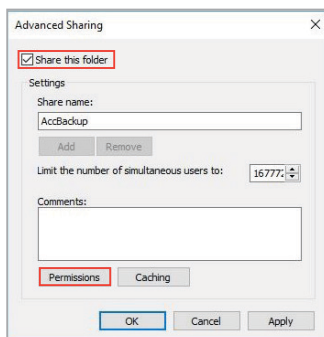




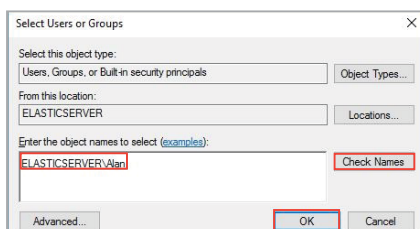
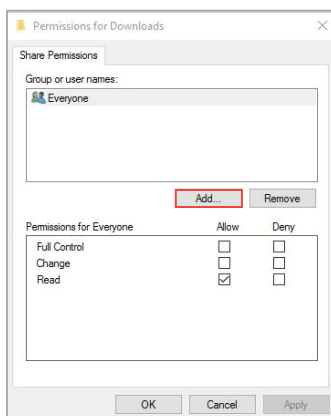
- b. Right click on the newly created folder and select **Properties > Sharing > Advanced Sharing...**



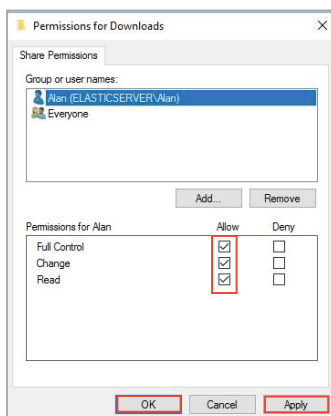
- c. Check **Share this folder**, then click on **Permissions**.



- d. Click on **Add...**, then enter the users you would like to allow permissions for, click on **Check Names** and click **OK**.



- e. Select the newly added group or username and check the **Full Control** permission. Ensure the **Full Control**, **Change** and **Read** permissions are all checked, click **Apply**, then click **OK**.



- f. Return to your ASUS Control Center main server.

2. Fill in the **Path**, **Domain**, **Account**, and **Password** fields.

**NOTE:**

- The **Account** and **Password** fields refer to the credentials used to access the backup location, not the credentials used to log into ASUS Control Center.
- The folder should be set as a shared folder and discoverable by the system you wish to back up, and should have read and write permissions enabled.
- Take note of the syntax of the path. Ensure that the syntax of your selected protocol from the previous step is correct.

ASUS Control Center 17:37

Options > Backup & Restore

Backup

Backup Location

Backup Protocol: Samba (SMB)

Path: /

Domain:

Account:

Password:

Backup Configuration

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password:

Last Time Updated: 2023/09/18 10:34

Restore

Restore Password:

Key: 0000 XXXXX XXXXX /0000

Upload Restoration File:

Restore Message:

3. Select the **Period** and **Preserved Backup** numbers. **Period** determines the amount of days each periodic backup should be done. The **Preserved Backup** amount determines how many backup files should be saved, when the amount of files exceed the **Preserved Backup** number, the backup file with the earliest date will be deleted.

ASUS Control Center 17:37

Options > Backup & Restore

Backup

Backup Location

Backup Protocol: Samba (SMB)

Path: /

Domain:

Account:

Password:

Backup Configuration

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password:

Last Time Updated: 2023/09/18 10:34

Restore

Restore Password:

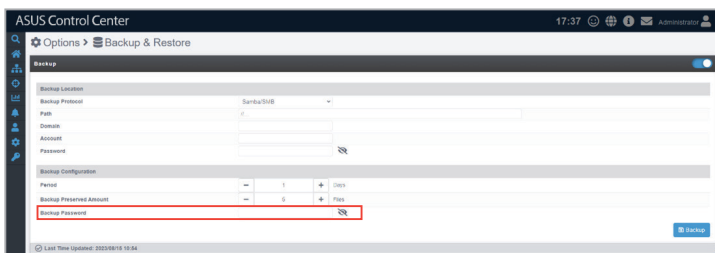
Key: 0000 XXXXX XXXXX /0000

Upload Restoration File:

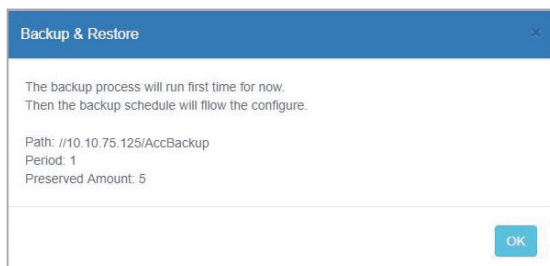
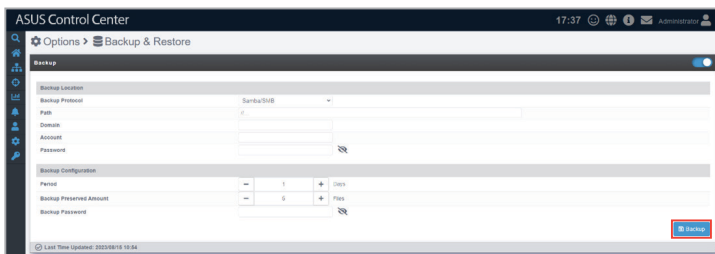
Restore Message:

4. Enter a backup password. This password is required when you use the **Restore** function.

**NOTE:** Store the backup password in a safe place. If the backup password is lost, you will not be able to restore from the backup file.



5. Click **Backup** to save the backup settings and start the initial backup.



## Restoring the backup file

1. Enter the **Backup Password** previously set when enabling periodic backup into the **Restore Password** field.

The screenshot shows the ASUS Control Center interface for Backup & Restore. The 'Backup' section is at the top, and the 'Restore' section is below it. In the 'Restore' section, the 'Restore Password' field is highlighted with a red rectangle. The 'Key' field contains the license key '0000 XXXXX XXXXX 0000'. The 'Upload Restoration File' section shows a file named 'BackupFile@2023\_08\_1\_4\_00.zip' with a size of 10.0 MB. The 'Restore Message' field is empty.

2. Enter the license key in the **Key** field.

The screenshot shows the ASUS Control Center interface for Backup & Restore. The 'Backup' section is at the top, and the 'Restore' section is below it. In the 'Restore' section, the 'Key' field is highlighted with a red rectangle. The 'Restore Password' field is empty. The 'Upload Restoration File' section shows a file named 'BackupFile@2023\_08\_1\_4\_00.zip' with a size of 10.0 MB. The 'Restore Message' field is empty.

3. Drag a backup file you wish to restore into the **Upload Restoration File** field, or click on **Upload Restoration File** and select the backup file you wish to use to restore.

ASUS Control Center 17:37 Administrator

Options > Backup & Restore

**Backup**

Backup Location: Samba/1916

Backup Protocol: S

Path: /

Domain:

Account:

Password:

Backup Configuration

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password:

Last Time Updated: 2023/08/16 10:34

**Restore**

Restore Password:

Key: 0000 XXXXX XXXXX (0000)

Upload Restoration File: BackupFile@2023\_08\_1\_4\_00.apk

Restore Message:

Start

4. Click **Start** to restore from the selected backup file.

ASUS Control Center 17:37 Administrator

Options > Backup & Restore

**Backup**

Backup Location: Samba/1916

Backup Protocol: S

Path: /

Domain:

Account:

Password:

Backup Configuration

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password:

Last Time Updated: 2023/08/16 10:34

**Restore**

Restore Password:

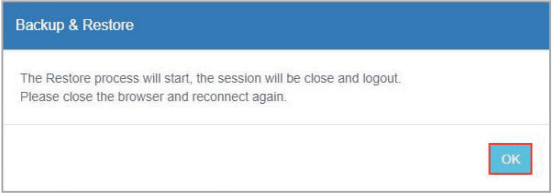
Key: 0000 XXXXX XXXXX (0000)

Upload Restoration File: BackupFile@2023\_08\_1\_4\_00.apk

Restore Message:

Start

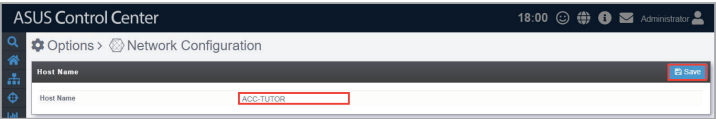
5. The session will expire and you will be logged out of ACC when the restore process begins, please restart the browser and log in again once the restore process is complete.



6. Once you've logged into the restored ACC, you will need to configure the network settings such as the Host Name and IP Address of the restored ACC, for managed devices to return and display the correct information and data.

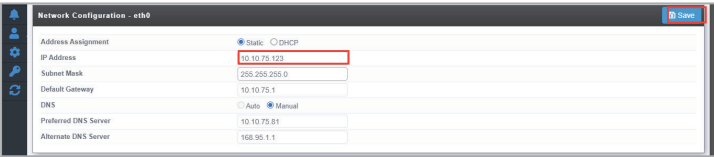
Navigate to  > **Network Configuration**, and change the **Host Name** of the restored ACC to the same host name as the backed up ACC, then click **Save**.

For example, if the backed up ACC's host name was ACC TUTOR, then after restoring it to an ACC main server with the host name ACC NWONE, change the host name ACC NWONE to ACC TUTOR.



7. Change the IP Address of the restored ACC to the same IP address as the backed up ACC, then click Save.

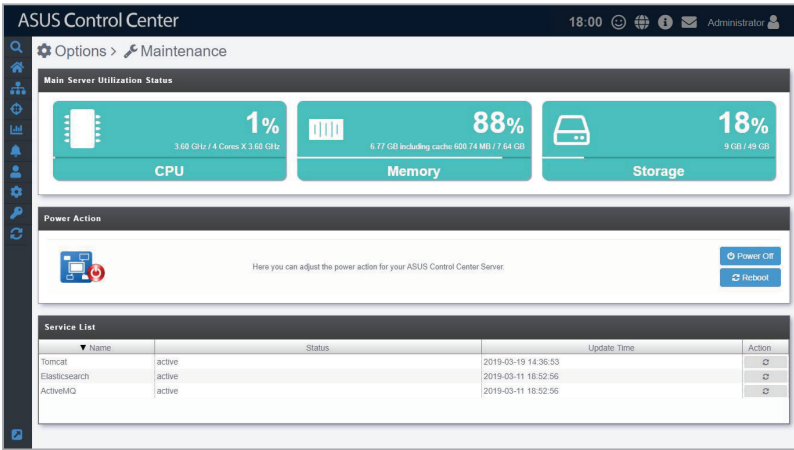
For example, if the backed up ACC's IP address was 10.10.75.123, then after restoring it to an ACC main server with the IP address 10.10.75.235, change the IP address 10.10.75.235 to 10.10.75.123.



## 8.7 Maintenance

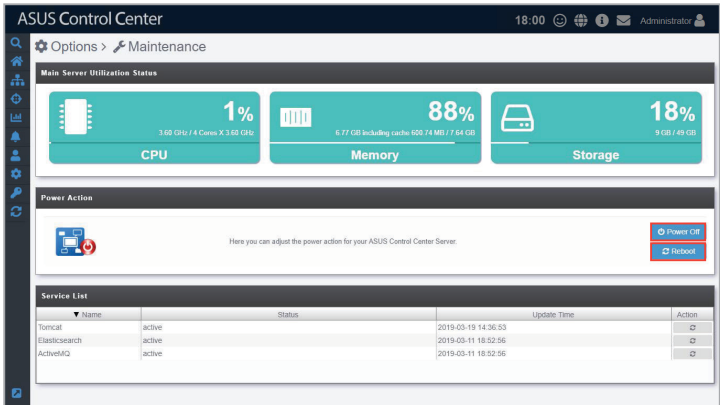
The **Maintenance** function allows you view the information such as the CPU, memory, and storage of the ACC VM. It also allows you to configure the power options and services running on the ACC VM remotely from the ASUS Control Center. This helps you save time when managing hypervisors, as you can control and configure them all from the ASUS Control Center.

To access **Maintenance**, click  in the left menu, then click on **Maintenance**.



### Configuring the power option of Hypervisors

1. Click on **Power Off** or **Reboot** to power off or reboot the hypervisor.





2. Enter the password of an account with a role that has Power Control enabled, then click on **Confirm** to execute your selected power option.

**NOTE:** For more information on Accounts and Roles, please refer to the **Account Management** chapter.

Administrator's Password

Please enter the administrator's password to authenticate your power action.

Password

\*\*\*\*\*

Confirm

**Restarting the Services**

Click on the restart button next to the service you wish to restart.

ASUS Control Center

18:00

Administrator

Options > Maintenance

Main Server Utilization Status

CPU

3.68 GHz / 4 Cores X3.68 GHz

1%

Memory

6.77 GB Inbuilt cache: 6GB / 4 MB / 7.64 GB

88%

Storage

9 GB / 49 GB

18%

Power Action

Here you can adjust the power action for your ASUS Control Center Server.

Power Off

Reboot

Service List

| Name          | Status | Update Time         | Action             |
|---------------|--------|---------------------|--------------------|
| Tomcat        | active | 2019-03-19 14:36:53 | <div>Restart</div> |
| Elasticsearch | active | 2019-03-11 18:52:56 | <div>Restart</div> |
| Activemq2     | active | 2019-03-11 18:52:56 | <div>Restart</div> |

This will end your session and you will be logged out of ASUS Control Center. Please login again once the restoration is complete.

Information

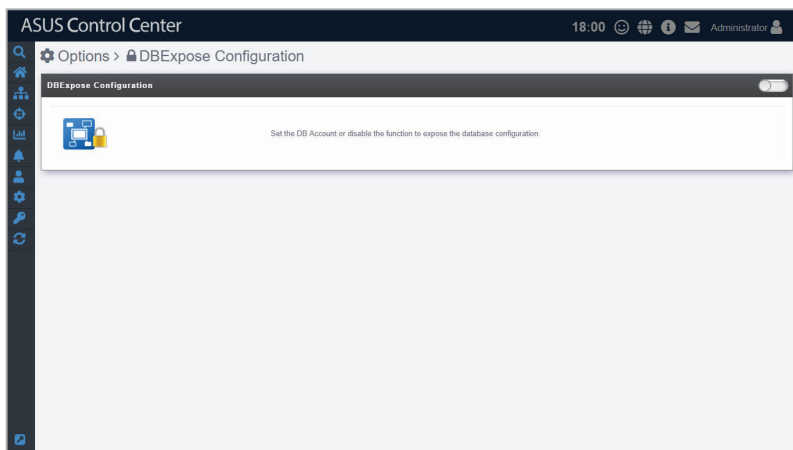
Restart successfully, please wait a moment and refresh website.

OK

## 8.8 DBExpose Configuration

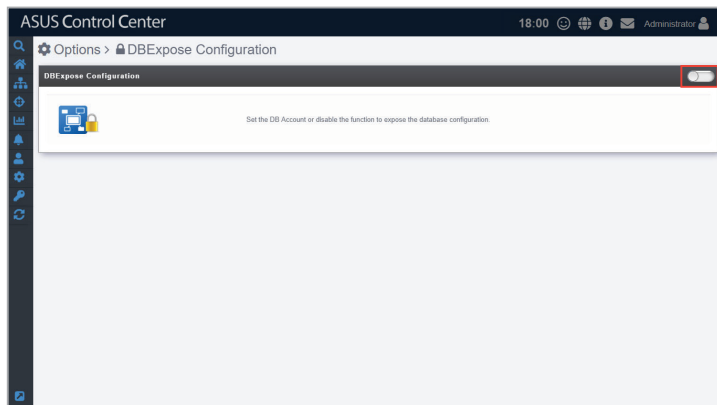
The **DBExpose Configuration** allows you to set an account and password which allows users to use third-party software, such as MySQL Workbench to access data on ASUS Control Center, such as device information or metadata. This information is read-only and cannot be edited.

To access **DBExpose Configuration**, click  in the left menu, then click on **DBExpose Configuration**.

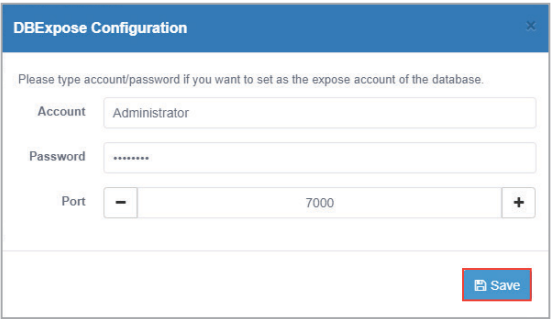


### To set the DBExpose account and password

1. Click on the slide button on the top right of the main screen.



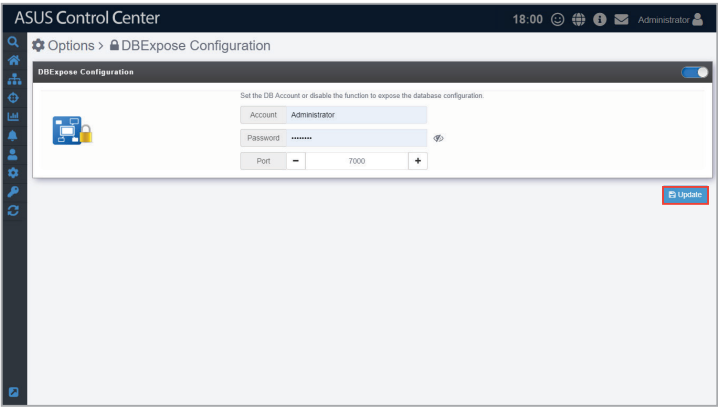
2. Enter an account and password, then enter a port (between 7000-7999) which is not being used. Once you have finished entered the required fields, click on **Save**.



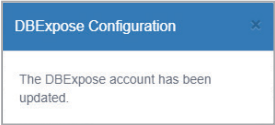
The image shows a 'DBExpose Configuration' dialog box. It has a blue header with the title and a close button. Below the header, there is a text prompt: 'Please type account/password if you want to set as the expose account of the database.' The form contains three fields: 'Account' with the value 'Administrator', 'Password' with masked characters '\*\*\*\*\*', and 'Port' with a spinner control set to '7000'. At the bottom right, there is a red 'Save' button.

**To edit the DBExpose account information**

Edit the account, password, and port information then click on **Update** to save the changes made.



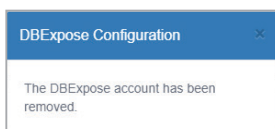
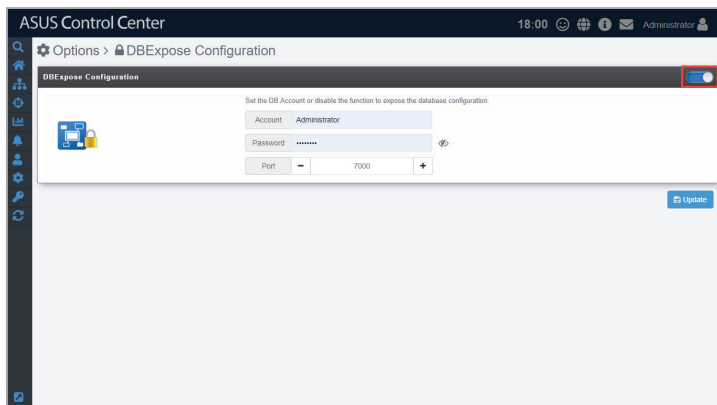
The image shows the 'ASUS Control Center' interface. The top bar displays 'ASUS Control Center', the time '18:00', and the user 'Administrator'. The main area shows 'Options > DBExpose Configuration'. A 'DBExpose Configuration' window is open, featuring a toggle switch, a text prompt 'Set the DB Account or disable the function to expose the database configuration', and fields for 'Account' (Administrator), 'Password' (masked), and 'Port' (7000). An 'Update' button is at the bottom right.



The image shows a small 'DBExpose Configuration' dialog box with a blue header. The message inside reads: 'The DBExpose account has been updated.'

## **To delete the DBExpose account information**

Click on the slide button on the top right to disable and delete the DBExposure Configuration settings.

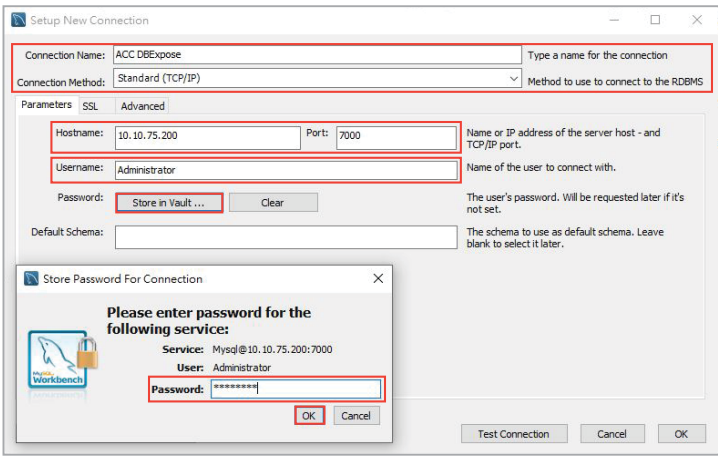


### Access ASUS Control Center with third-party software

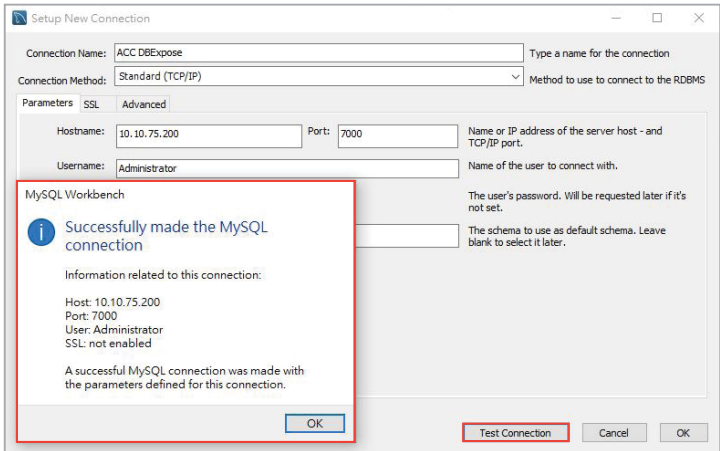
**NOTE:** The example in this section is for reference only.

You can use a third-party software such as **MySQL Workbench** to access information such as the metadata and device information of your ASUS Control Center.

1. Load MySQL Workbench, then set up a new connection and enter the required information.
2. Enter the ip and port of the ASUS Control Center server into the **Hostname** and **Port** field.
3. Next, enter the DBExposure account created into the **Username** field.
4. Click on **Store in Vault...** then enter the DBExposure password you created into the password field and click **OK**.

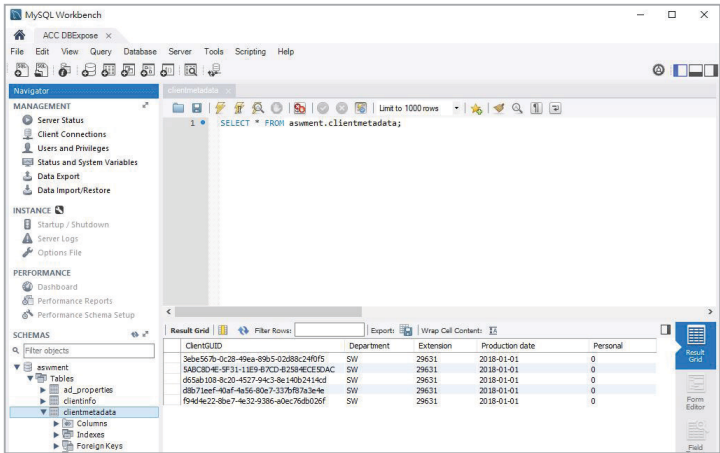


5. Click on **Test Connection** to test if the connection to ASUS Control Center was successfully created.



6. Save the connection settings, now when using MySQL Workbench, you should be able to access some of the data on ASUS Control Center.

**NOTE:** The screenshot below is an example of accessing the metadata of ASUS Control Center.

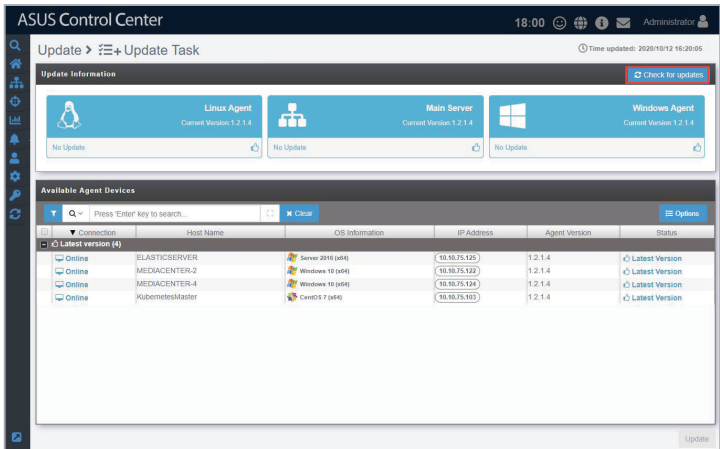


# 8.9 Update

The **Update Task** screen will display available updates for the Linux Agent, Windows Agent, and Main Server, you may manually refresh the updates screen by clicking on **Check for updates**.

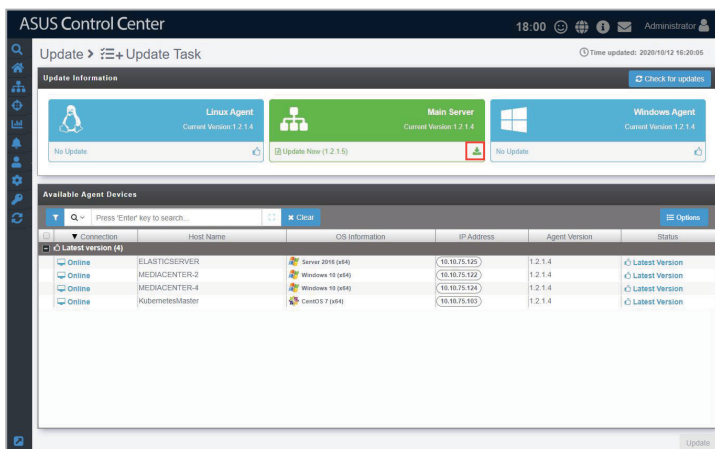
**NOTE:**

- Ensure to add `asuscontrolcenter.asus.com/*` to your firewall exceptions list to enable update checks.
- Ensure you have a stable Internet connection.

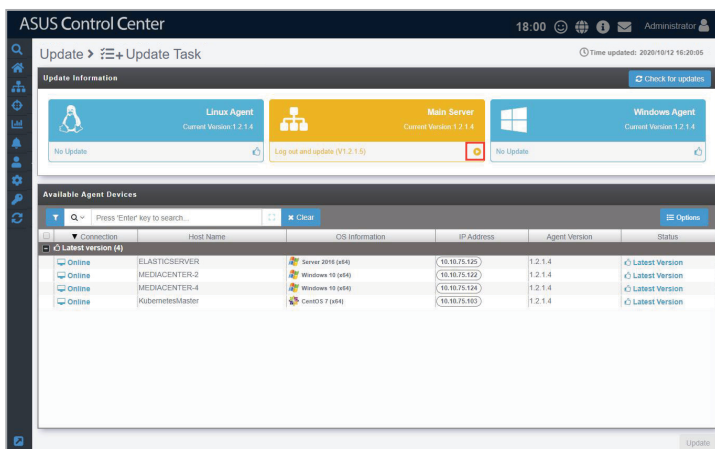


## Updating ASUS Control Center main server

1. When an update is available for the main server, it will be displayed under **Update Information** and the **Main Server** block will be displayed in green. Click on  in the **Main Server** block to download the update files.



2. Once the update files are successfully downloaded, the **Main Server** block should be displayed in orange. Now click on  to update the ASUS Control Center main server. You will also be logged out of ASUS Control Center when the main server is updating.

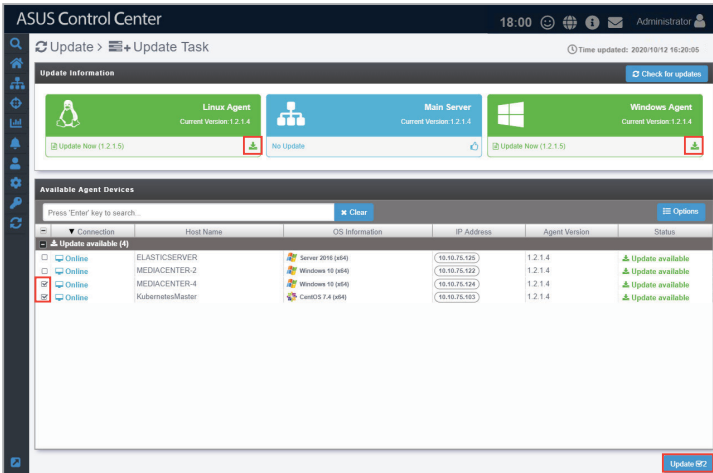


3. Log into ASUS Control Center again after the update is completed.



## Updating Windows and Linux agents

1. When an update is available for Linux and/or Windows Agents it will be displayed under **Update Information**, and the **Linux Agent** and/or **Windows Agent** block will be displayed in green.
2. Click on  in the **Linux Agent** and/or **Windows Agent** block to download the agent. Once the download is complete, the **Linux Agent** and/or **Windows Agent** block will be displayed in blue.
3. Select the device(s) you wish to update agents for in the **Available Agent Devices** list.
4. Click on **Update**.

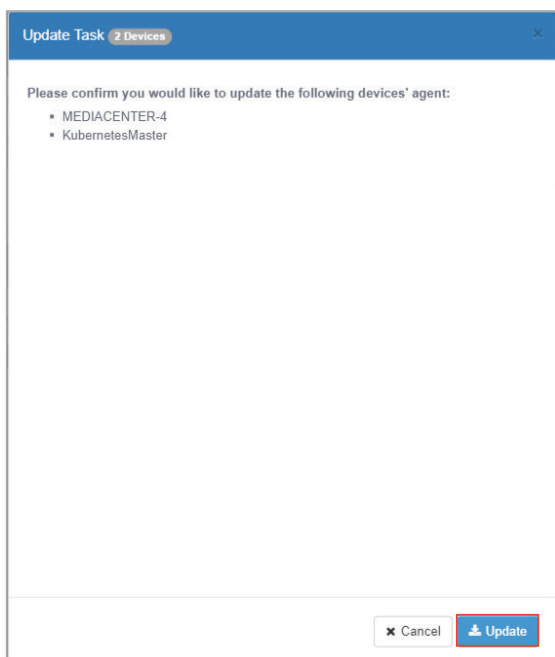


5. Click **Update** on the confirmation pop-up window to start the update process.

---

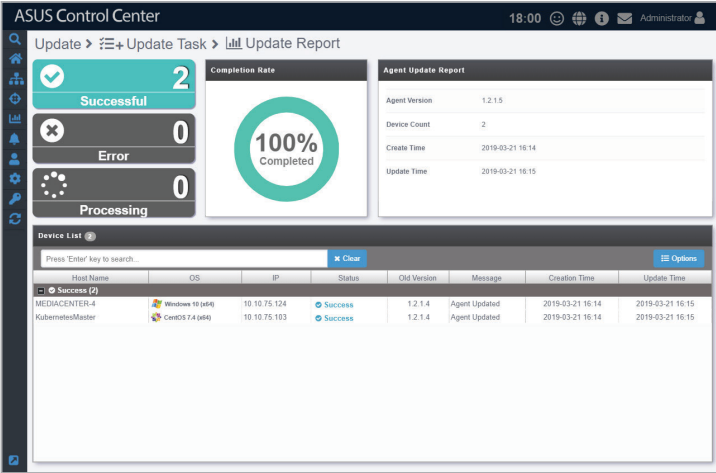
**NOTE:** You do not need to uninstall the agents on the selected devices before updating.

---



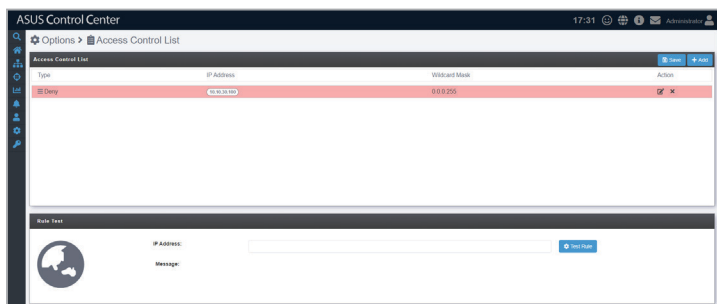
6. After the agent updates have been completed, you will be redirected to the Agent Update Report screen.

**NOTE:** For more details on the Agent Update Report, refer to the **Agent Update Report** section.



## 8.10 Access Control List

The **Access Control List** allows you to configure rules to permit or deny access to ASUS Control Center from specified IP addresses.



**Add New Access Control List Rule**

Type: ☐ Permit ☒ Deny

IP Address: 10.10.30.100

Wildcard Mask: 0.0.0.255

### To add an access control rule

1. Click **+ Add** to start adding a new access control rule.
2. Select **Permit** or **Deny** in the popup window, then enter an **IP address** and **Wildcard Mask**.

#### NOTE:

- For example, to deny access from a Class C IP range, set the **Type** to Deny, **IP address** to 10.10.30.100, and the **Wildcard Mask** to 0.0.0.255. The resulting access control rule will deny access from any IP address from 10.10.30.1 to 10.10.30.254.
- For example, to permit access from a specific IP address, set the **Type** to Permit, **IP address** to 10.10.30.123, and the **Wildcard Mask** to 0.0.0.0. The resulting access control rule will permit access from 10.10.30.123.

3. Click **Save** to save the access control rule.

### To adjust the priority of an access control rule

1. Click and drag an access control rule up or down to adjust its priority.
2. Click  **Save** to save changes to the access control rule list, then click **OK** in the popup window to confirm your changes.

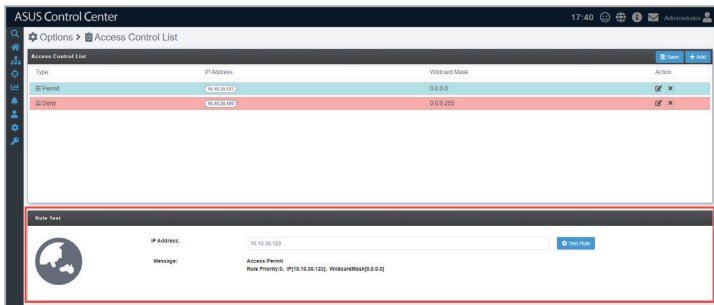
---

**NOTE:** The access control rules are applied in descending order.

---

### To test an access control rule

1. Enter an IP address under **Rule Test**.
2. Click  **Test Rule** to view if the specified IP address will be permitted or blocked based on the existing access control rules.



### To edit an access control rule

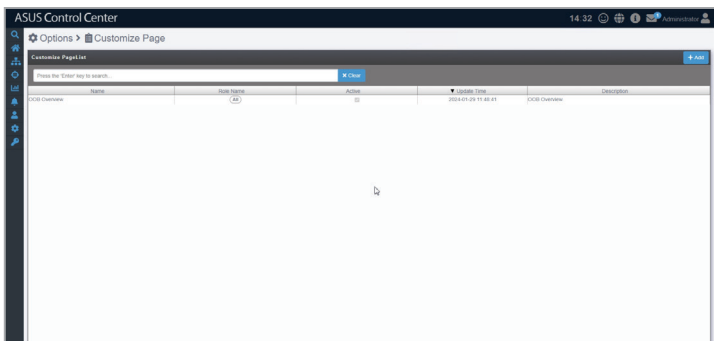
1. Click  to start editing a new access control rule.
2. After making the desired changes, click  **Save** to save the access control rule, then click **OK** in the popup window to confirm your changes.

### To delete an access control rule

1. Click  to delete an access control rule, then click **Delete** in the popup window to confirm deletion.
2. Click  **Save** to save changes to the access control rule list.

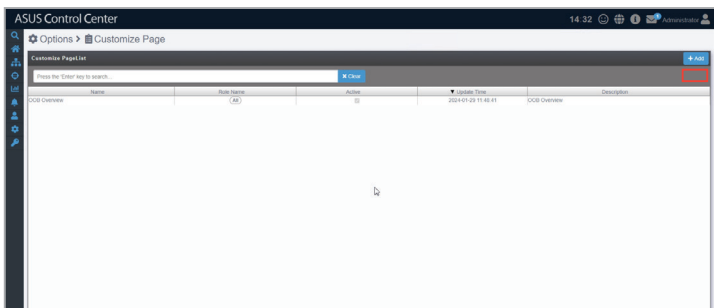
## 8.11 Customize Page

**Customize Page** allows you to create and edit custom pages.



### Adding a blank custom page

1. Click **Add** to open the custom page editor and create a blank custom page.



2. Fill in the **Name** and **Description** fields.

Information

Create Type: ☒ Role ☐ Page List

Name:

Description:

Apply page: ☒ All ☐ Role List ☐ Enable the page

Action: ☐ Enable the page

3. Select the **Role List** option in the **Apply page** field, then select a role from the drop down menu to specify which roles should have access to the custom page (optional).

Information

Create Type: ☒ Role ☐ Page List

Name:

Description:

Apply page: ☒ All ☐ Role List ☐ Enable the page

Action: ☐ Enable the page

Role List:

- ☒ Admin
- ☐ Editor
- ☐ Viewer

4. Tick **Enable this page** to enable the custom page.

Information

Create Type: ☒ Role ☐ Page List

Name:

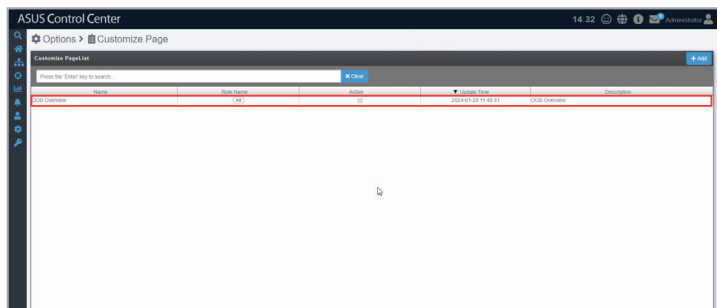
Description:

Apply page: ☒ All ☐ Role List ☐ Enable the page

Action: ☒ Enable the page

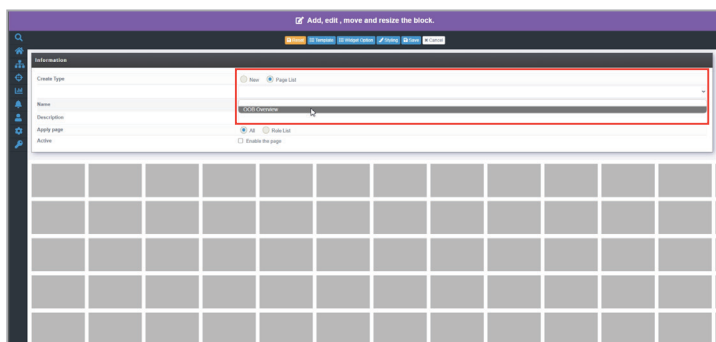
## Editing an existing customized page

Select an existing custom page to open the custom page editor.



## Using an existing custom page as a template

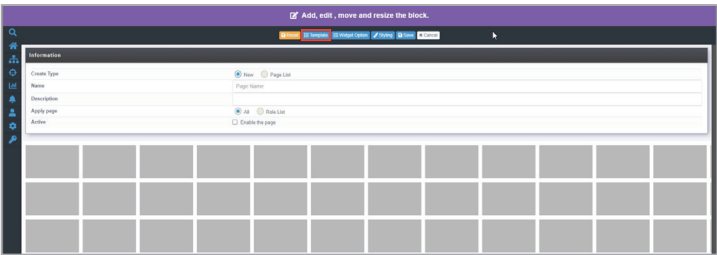
In the custom page editor, select the **Page List** option in the **Create Type** field, then select a custom page from the drop down list to use as a template.



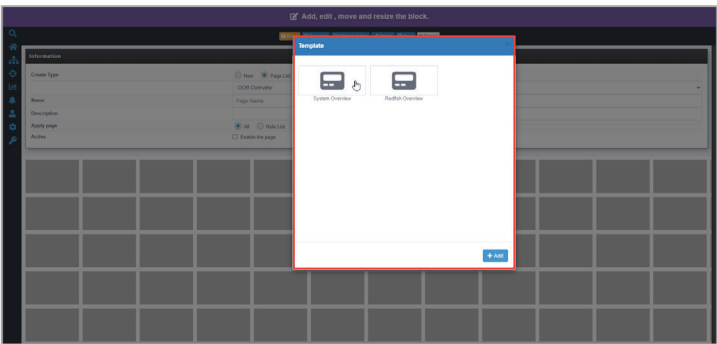


**Loading a custom page template**

- 1. In the custom page editor, click **Template**.

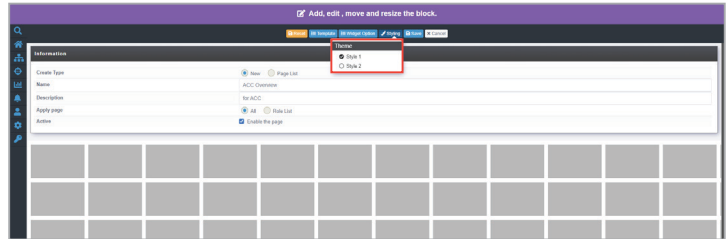


- 2. Select a template, then click **Add**.



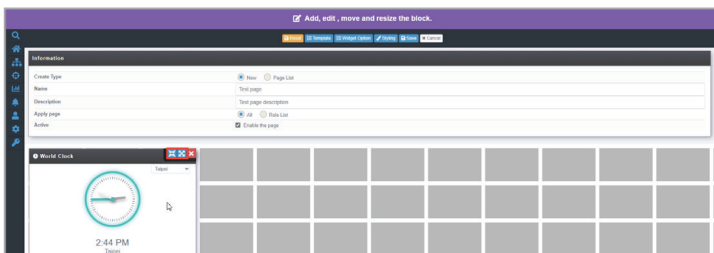
**Changing the theme of the custom page**

In the custom page editor, click **Styling**, then select a theme from the drop down menu.



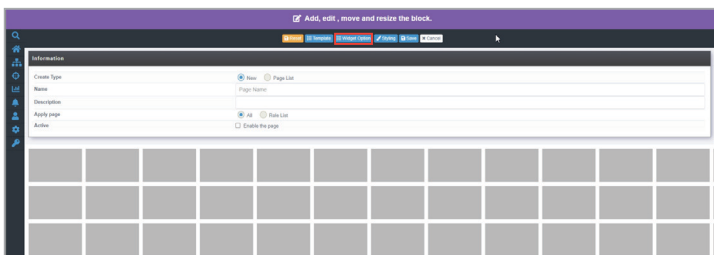
## Changing the size of widgets

Click the enlarge or shrink button in the title bar of the widget.

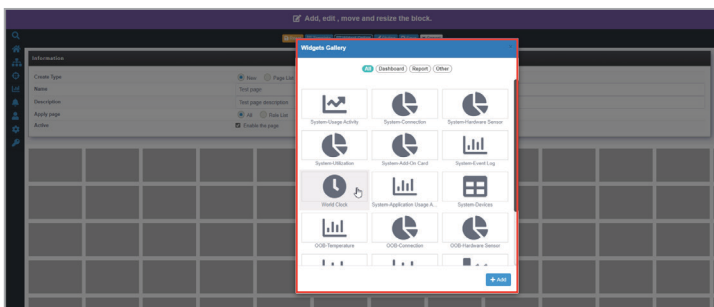


## Adding a widget using the widget gallery

1. In the custom page editor, click **Widget Option**.

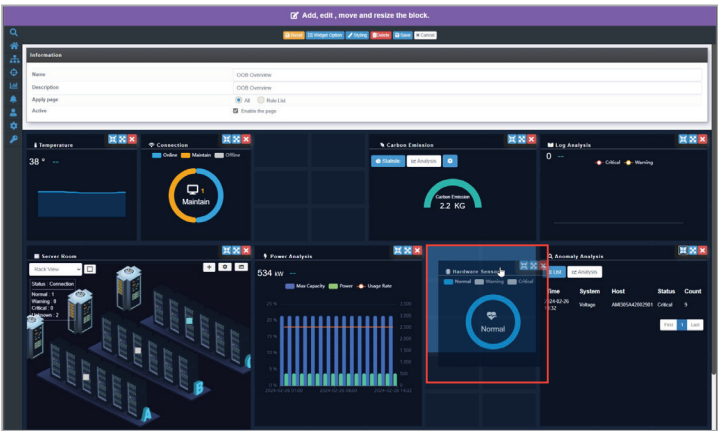


2. Select a widget from the Widget Gallery, then click **Add**.



# Changing the location of widgets

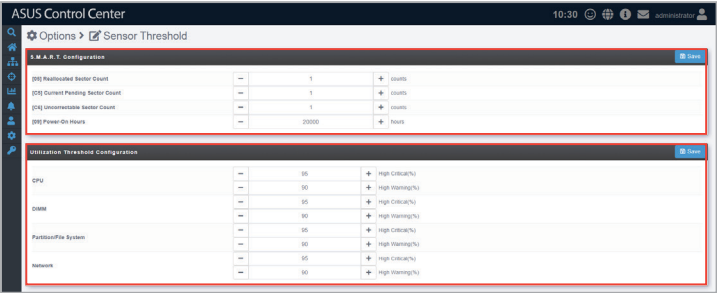
Drag and drop a widget to the desired location.



## 8.12 Sensor Threshold

The **Sensor Threshold** allows you to centrally configure the threshold values of all managed devices, providing you with an effortless method of setting threshold values of all managed devices, instead of having to configure each device's threshold values individually.

To access **Sensor Threshold**, click  in the left menu, then click **Sensor Threshold**.



### Adjusting the Disk S.M.A.R.T. status configurations

Adjust the disk S.M.A.R.T. status configurations, then click **Save** to save and apply the changes made to all managed devices.

### Adjusting the Utilization Threshold configurations

Adjust the threshold at which warnings and critical warnings will be shown, then click **Save** to save and apply the changes made to all managed devices.

---

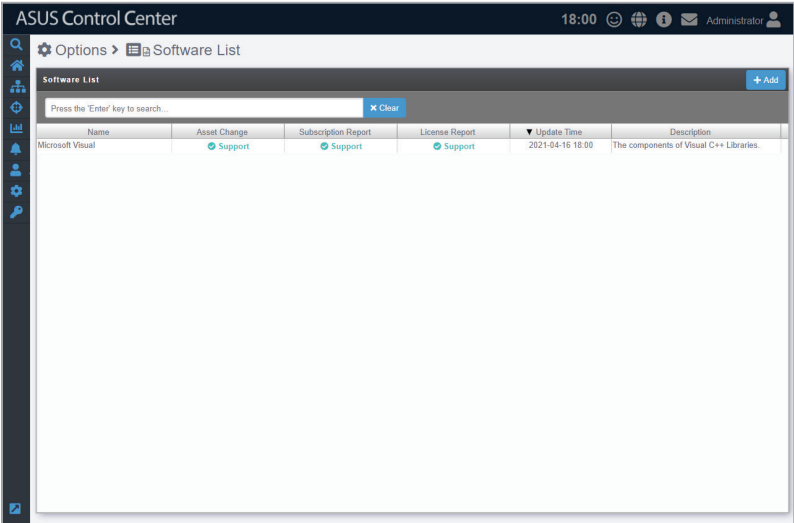
**NOTE:** To adjust the threshold for a single managed device, refer to **Utilization** under the **Device Information** section.

---

# 8.13      Software List

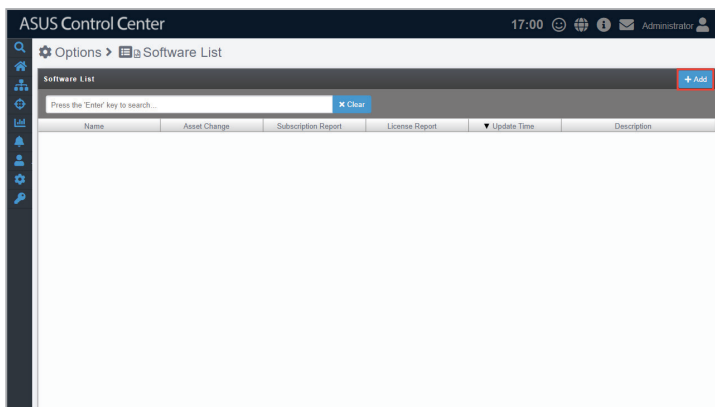
The **Software List** allows you to view and manage rules of the installed software of all managed devices. You can use the Search Bar at the top of the page to search and filter through added software lists in the Software List.

To access **Software List**, click  in the left menu, then click on **Software List** in the Definition block.

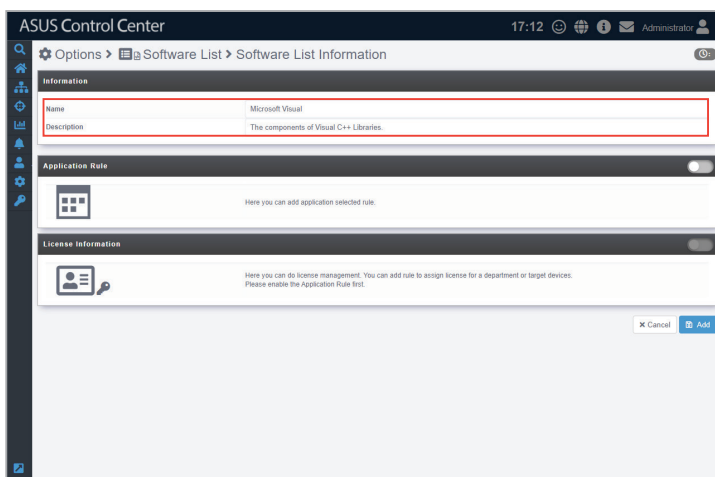


## Adding a software list

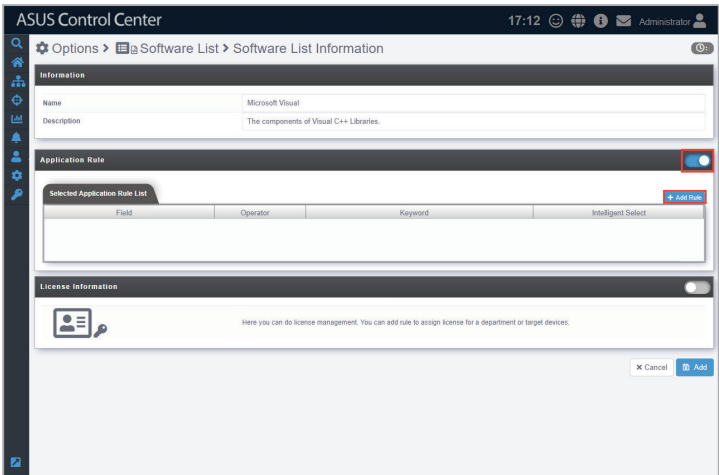
1. Click on **Add**.



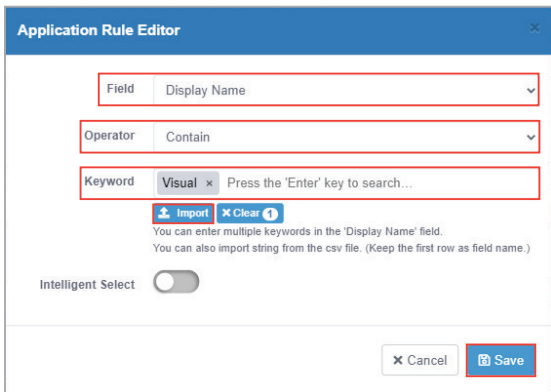
2. Enter the **Name** and **Description** of the software list.



3. Click on the slide button in the **Application Rule** block, then click on **Add Rule**.



4. You may add a rule from each filter field (**Display Name**, **Publisher**, **Version**). Please refer to the following on methods of adding each filter field.
- Using Conditions (Display Name, Publisher, Version)
    - Select a **Field**.
    - Select the Operator (**Equal**, **Contain**, **Not Contain**), this will allow you to set the conditions for the keywords you enter.
    - Enter keyword(s) or use the **Import** button to import keywords from a .csv file.
    - Click on **Save** once you are finished adding keywords.



- Using Intelligent Select (Display Name)

Intelligent Select will group softwares with slight differences in software name, publisher or version. For example the *Microsoft Visual Studio* Application Collection will include both *Microsoft Visual Studio 2016* and *Microsoft Visual Studio 2019*.

---

**NOTE:** This option is only available for when **Display Name** is selected as the **Field**.

---

- a. Select **Display Name** as the **Field**.
- b. Select the Operator (**Equal, Contain, Not Contain**), this will allow you to set the conditions for the items selected in Intelligent List.
- c. Click on the slide button **Intelligent Select**, then click **Add From Intelligent List**.

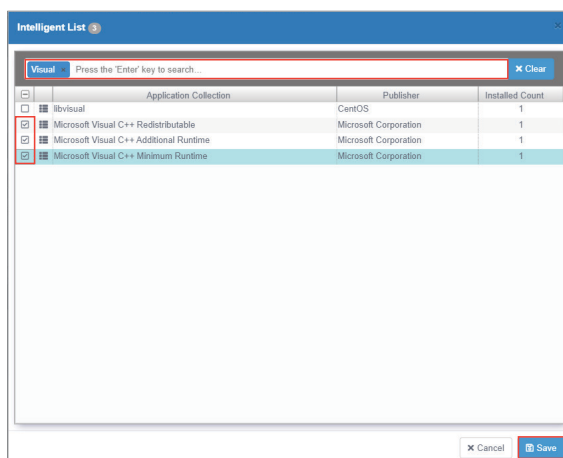
The screenshot shows the 'Application Rule Editor' dialog box. It has a blue header bar with the title 'Application Rule Editor' and a close button. The main area contains several fields and controls:

- A 'Field' dropdown menu with 'Display Name' selected.
- An 'Operator' dropdown menu with 'Contain' selected.
- A 'Keyword' text input field with the placeholder text 'Press the 'Enter' key to search...'. Below it is an 'Import' button with a download icon. A note below the 'Import' button states: 'You can enter multiple keywords in the 'Display Name' field. You can also import string from the csv file. (Keep the first row as field name.)'
- An 'Intelligent Select' section with a toggle switch that is currently turned on (blue) and a button labeled '+ Add From Intelligent List'.
- A table with two columns: 'Application Collection' and 'Publisher'. The table is currently empty.
- At the bottom right, there are 'Cancel' and 'Save' buttons.



- d. Check Application Collections to add them to the Intelligent List, then click on **Save**. You may also use the search bar to search for Application Collections.

**NOTE:** Click on  next to the Application Collection name to view all applications included in the Application Collection.



e. Click on **Save** when you are finished.

**NOTE:** Click on **Clear** to clear all Application Collections added.

Application Rule Editor

Field

Display Name

Operator

Contain

Keyword

Press the 'Enter' key to search...

Import

You can enter multiple keywords in the 'Display Name' field.  
You can also import string from the csv file. (Keep the first row as field name.)

Intelligent Select

Add From Intelligent List

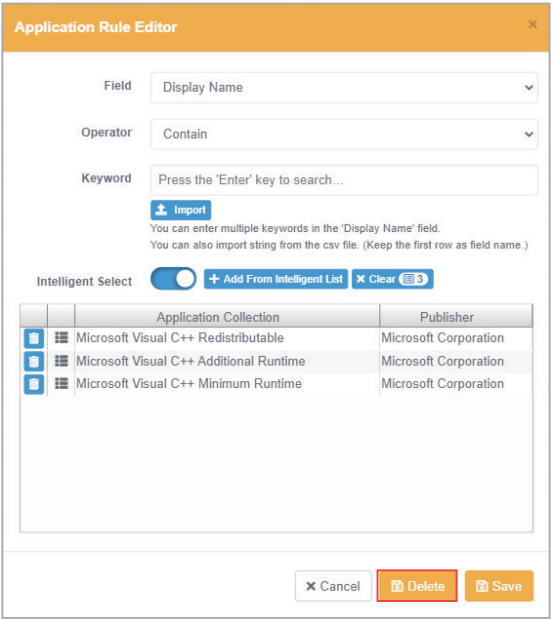
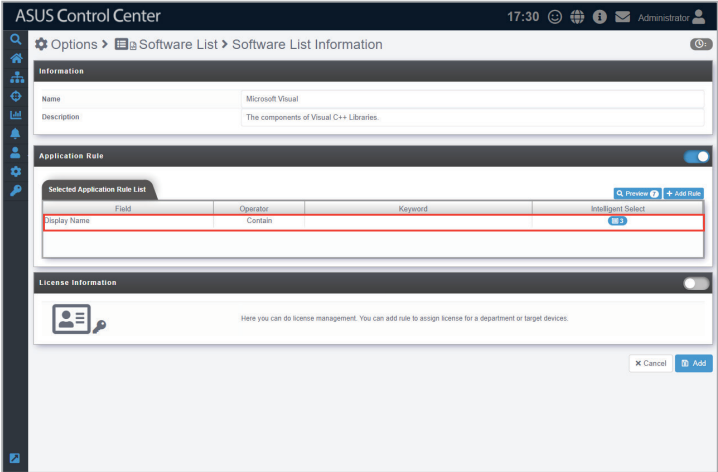
Clear

|                                                                                   | Application Collection                  | Publisher             |
|-----------------------------------------------------------------------------------|-----------------------------------------|-----------------------|
|  | Microsoft Visual C++ Redistributable    | Microsoft Corporation |
|  | Microsoft Visual C++ Additional Runtime | Microsoft Corporation |
|  | Microsoft Visual C++ Minimum Runtime    | Microsoft Corporation |

Cancel

Save

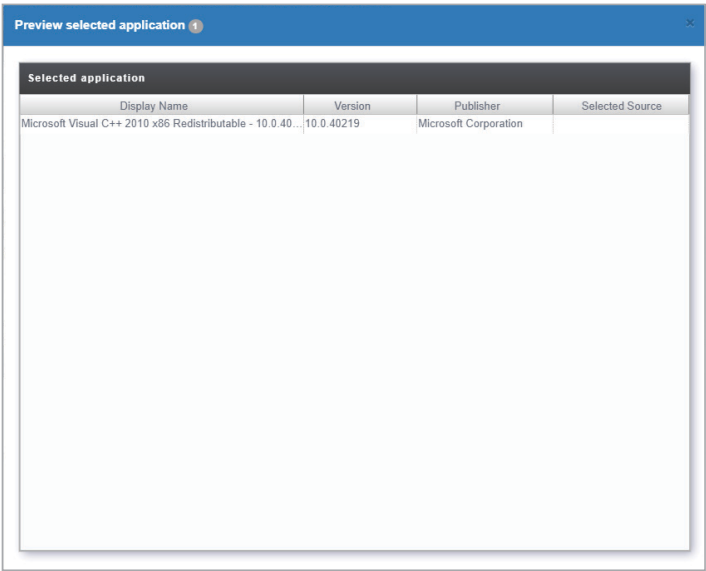
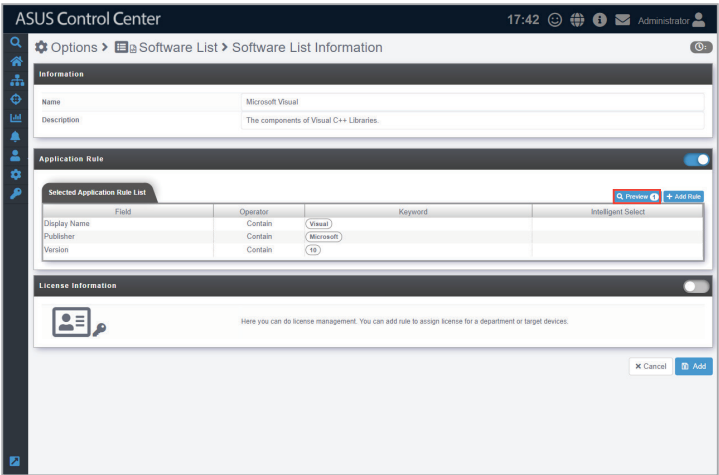
5. (optional) You may also edit or delete an application rule by clicking on the rule, then following step 4 to edit the rule, or click on **Delete** to delete the application rule.



6. Repeat step 3 to step 5 to add more Application Rules.

**NOTE:** You may only add one Application Rule per **Field** (**Display Name, Publisher, Version**).

7. Click on **Preview** to view the filter results based on the Applications Rules added.



**NOTE:** Adding License Information is optional, if you do not wish to add License Information, skip steps 8 to 17.

8. Click on the slide button in the **License Information** block.

ASUS Control Center 17:50 Administrator

Options > Software List > Software List Information

**Information**

Name: Microsoft Visual  
Description: The components of Visual C++ Libraries.

**Application Rule**

Selected Application Rule List

| Field        | Operator | Keyword     | Intelligent Select |
|--------------|----------|-------------|--------------------|
| Display Name | Contain  | (Visual)    |                    |
| Publisher    | Contain  | (Microsoft) |                    |
| Version      | Contain  | (10)        |                    |

**License Information**

Authorized ☒ Authorization Details [Assign License](#)

| Description | License Type | Server-based Floating License | License Amount | Due Date |
|-------------|--------------|-------------------------------|----------------|----------|
|-------------|--------------|-------------------------------|----------------|----------|

[Cancel](#) [Add](#)

9. (optional) Click on the **Authorization Details** slide button to add authorization details to the License you are about to add.

**NOTE:** Toggling this option when there are already items in the **Authorized** list will clear the **Authorized** list.

ASUS Control Center 17:50 Administrator

Options > Software List > Software List Information

**Information**

Name: Microsoft Visual  
Description: The components of Visual C++ Libraries.

**Application Rule**

Selected Application Rule List

| Field        | Operator | Keyword     | Intelligent Select |
|--------------|----------|-------------|--------------------|
| Display Name | Contain  | (Visual)    |                    |
| Publisher    | Contain  | (Microsoft) |                    |
| Version      | Contain  | (10)        |                    |

**License Information**

Authorized ☒ Authorization Details [Assign License](#)

| Description | License Type | Server-based Floating License | License Amount | Due Date |
|-------------|--------------|-------------------------------|----------------|----------|
|-------------|--------------|-------------------------------|----------------|----------|

[Cancel](#) [Add](#)

10. Click on **Assign License**.

ASUS Control Center

Options > Software List > Software List Information

17:50 Administrator

**Information**

Name: Microsoft Visual  
Description: The components of Visual C++ Libraries.

**Application Rule**

Selected Application Rule List

| Field        | Operator | Keyword     | Intelligent Select |
|--------------|----------|-------------|--------------------|
| Display Name | Contain  | (Visual)    |                    |
| Publisher    | Contain  | (Microsoft) |                    |
| Version      | Contain  | (15)        |                    |

**License Information**

Authorized ☒ Authorization Details [Assign License](#)

| Description | License Type | Server-based Floating License | License Amount | Due Date |
|-------------|--------------|-------------------------------|----------------|----------|
|-------------|--------------|-------------------------------|----------------|----------|

Cancel Add

11. Enter a **Description** for the License.

12. Select the **License Type**.

**NOTE:**

- **One Time Purchase:** Softwares that are a one time purchase and require no other subscription fees.
- **Subscription:** Softwares that require a periodic subscription fee.

**License Rule Editor**

Description: Server department only

License Type: ☒ One Time Purchase ☒ Subscription

Server-based Floating License: ☒ Yes ☐ No

License Amount: 1 Due Date: 2021/04/30

Authorization Details: ☒ AD Department

Server x Add a tag

Import Clear

Press 'Enter' to add a full comparison string or paste text with ';' (semi-colon) separator.  
You can also import string from the csv file. (Keep the first row as field name.)

Cancel Save

13. Select if the License is a **Server-based Floating License**. A floating license is a licensing approach in which a limited number of licenses for the software is shared among users, and only allows a user to use the software if a license is available.
14. Set the amount of licenses available for this software.
15. Set the **Due Date** for the License if you selected **Subscription** as the **License Type**.

---

**NOTE:** This option is only available when **Subscription** is selected as the **License Type**.

---

The screenshot shows the 'License Rule Editor' window. The 'Description' field contains 'Server department only'. The 'License Type' section has 'One Time Purchase' and 'Subscription' buttons, with 'Subscription' selected. Below this, the 'Server-based Floating License' section is highlighted with a red box and contains 'Yes' and 'No' radio buttons, with 'Yes' selected. The 'License Amount' section, also highlighted with a red box, shows a numeric input set to '1' with minus and plus buttons. The 'Due Date' field, highlighted with a red box, contains '2021/04/30'. The 'Authorization Details' section shows a dropdown menu set to 'AD Department', a 'Server' tag, and an 'Add a tag' button. Below this are 'Import' and 'Clear' buttons. A note at the bottom of this section reads: 'Press 'Enter' to add a full comparison string or paste text with ';' (semi-colon) separator. You can also import string from the csv file. (Keep the first row as field name.)' At the bottom right of the window are 'Cancel' and 'Save' buttons.

16. Select the Authorization Details from the drop down menu.

**NOTE:**

- This option is only available if **Authorization Details** was enabled.
- The drop down menu consists of existing metadata items. For more information on adding, editing or deleting metadata, please refer to the **Metadata Management** section.

17. Add keyword tags to the **Authorization Details** selected to help provide more information on the **Authorization Details** item selected. You may also Import multiple keywords using a .csv file by clicking on Import, selecting the .csv file you wish to import, and then selecting the field in the .csv file you would like to import.

**NOTE:**

- This option is only available if **Authorization Details** was enabled.
- Click on **Clear** to clear all Application Collections added.

18. Click on **Save** once you are finished.

**License Rule Editor**

Description: Server department only

License Type: ☒ One Time Purchase ☒ Subscription

Server-based Floating License: ☒ Yes ☐ No

License Amount:  1  Due Date: 2021/04/30

**Authorization Details**

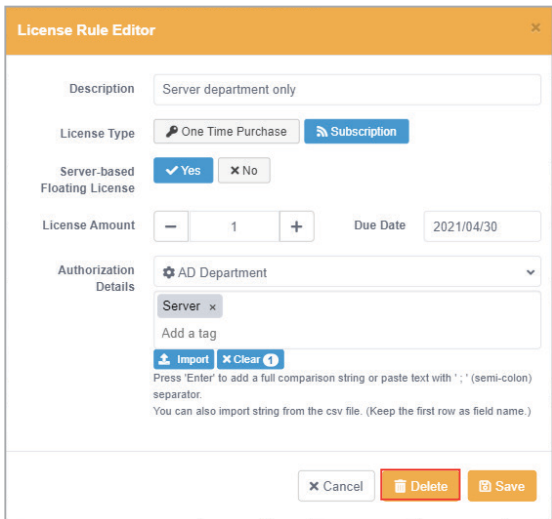
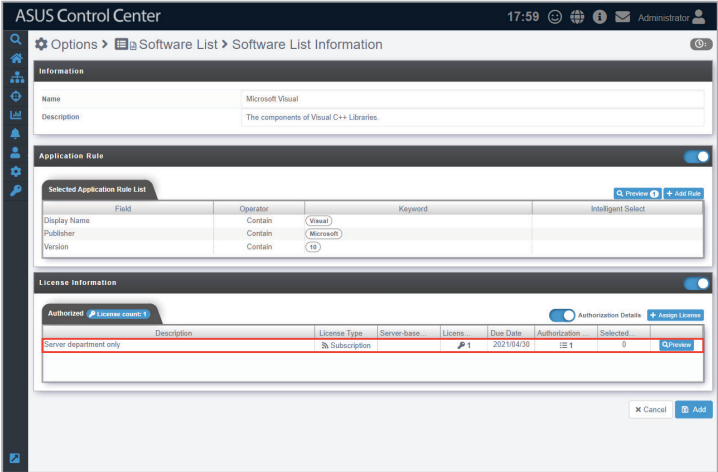
AD Department

Server x Add a tag

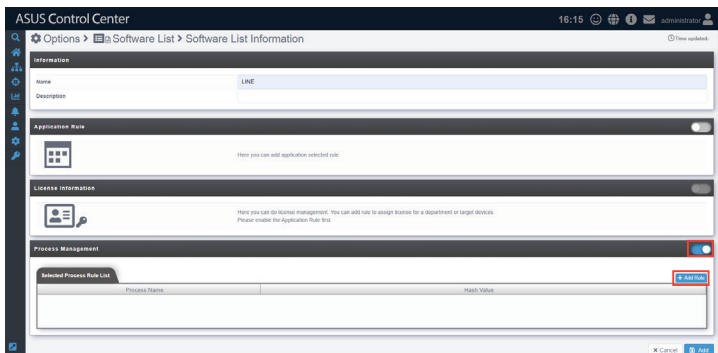
Press 'Enter' to add a full comparison string or paste text with ';' (semi-colon) separator.  
You can also import string from the csv file. (Keep the first row as field name.)



19. (optional) You may also edit or delete a License by clicking on the License, then follow step 8 to 17 to edit the License, or click on **Delete** to delete the application rule.



20. (optional) Click on the slide button in the **Process Management** block, then click **Add Rule**.



21. Enter the **Process Name** and **Hash Value** of the process, then click **Save**.

**NOTE:** To get the hash value of a process, refer to **Application Usage Analysis** under the **Software Report** section of the **Report** chapter.

The screenshot shows the 'Process Rule Editor' dialog box. It has two input fields: 'Process Name' with the value 'LINE' and 'Hash Value' with the value 'C769FE683BDF9421BACD4FD1E6254CBB'. At the bottom right, there are two buttons: 'Cancel' and 'Save'. The 'Save' button is highlighted with a red box.

22. Click on **Add** once you have finished editing the software list.

ASUS Control Center 17:59 Administrator

Options > Software List > Software List Information

**Information**

Name: Microsoft Visual  
Description: The components of Visual C++ Libraries.

**Application Rule**

Selected Application Rule List

| Field        | Operator | Keyword   | Intelligent Select |
|--------------|----------|-----------|--------------------|
| Display Name | Contains | Visual    |                    |
| Publisher    | Contains | Microsoft |                    |
| Version      | Contains | 10        |                    |

**License Information**

Authorized License Details

| Description            | License Type | Server base | Licenses | Due Date   | Authorizations | Selected |
|------------------------|--------------|-------------|----------|------------|----------------|----------|
| Server department only | Subscription |             | 1        | 2021/04/30 | 1              | 0        |

Cancel Add

Your newly added software list should appear in the main Software List screen. For more information on applying the software list, please refer to the **Trust Software Asset** or **Focus Software Asset** sections.

ASUS Control Center 18:00 Administrator

Options > Software List

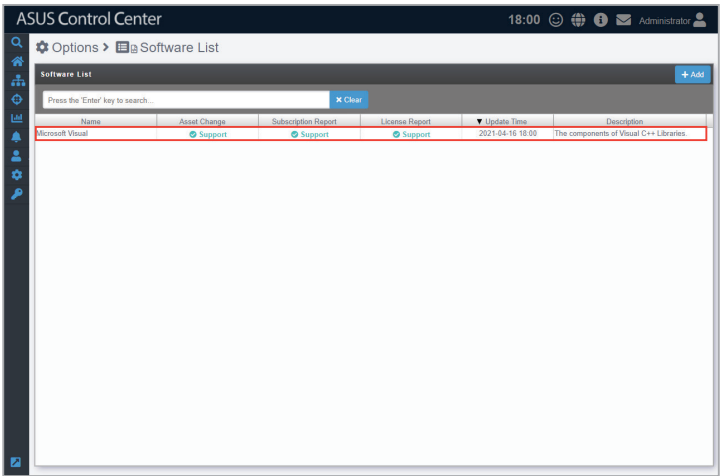
Software List

Press the Enter key to search. Clear

| Name             | Asset Change | Subscription Report | License Report | Update Time      | Description                             |
|------------------|--------------|---------------------|----------------|------------------|-----------------------------------------|
| Microsoft Visual | Support      | Support             | Support        | 2021-04-16 18:00 | The components of Visual C++ Libraries. |

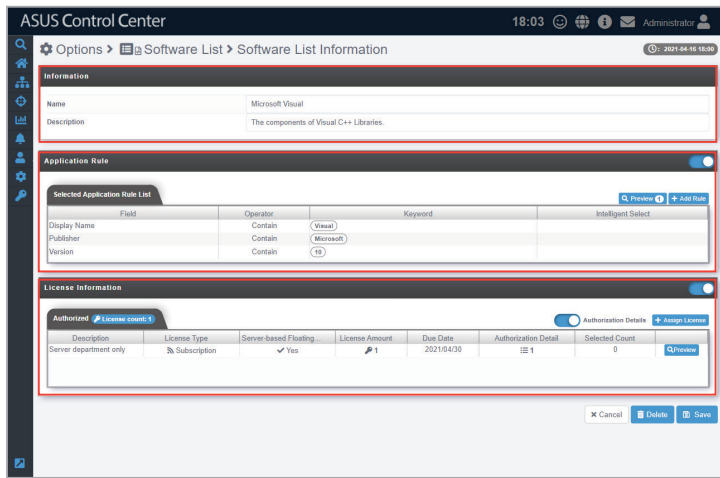
### Editing a software list

1. Click on the software list you would like to edit from the **Software List**.



2. You can edit the items in the Information, Application Rule and License Information blocks. For more information on the items in these blocks please refer to the **Adding a software list** section.

**NOTE:** You can see the date and time of the last time this software list was updated in the top right corner.



3. Click on **Save** once you are finished editing the software list.

ASUS Control Center 18:03 Administrator

Options > Software List > Software List Information

Information

Name: Microsoft Visual  
Description: The components of Visual C++ Libraries.

Application Rule

Selected Application Rule List

| Field        | Operator | Keyword     | Intelligent Select |
|--------------|----------|-------------|--------------------|
| Display Name | Contain  | (Visual)    |                    |
| Publisher    | Contain  | (Microsoft) |                    |
| Version      | Contain  | (16)        |                    |

License Information

Authorized License counts

| Description            | License Type | Server-based Floating | License Amount | Due Date   | Authorization Detail | Selected Count |
|------------------------|--------------|-----------------------|----------------|------------|----------------------|----------------|
| Server department only | Subscription | ✓ Yes                 | 1              | 2021/04/30 | 1                    | 0              |

Cancel Delete Save

### Deleting a software list

1. Click on the software list you would like to delete from the **Software List**.

ASUS Control Center 18:00 Administrator

Options > Software List

Software List

Press the 'Enter' key to search. Clear

| Name             | Asset Change | Subscription Report | License Report | Update Time      | Description                             |
|------------------|--------------|---------------------|----------------|------------------|-----------------------------------------|
| Microsoft Visual | Support      | Support             | Support        | 2021-04-16 18:00 | The components of Visual C++ Libraries. |

2. Click on **Delete** to delete the software list.

ASUS Control Center 18:03 Administrator

Options > Software List > Software List Information

Information

Name: Microsoft Visual  
Description: The components of Visual C++ Libraries.

Application Rule

Selected Application Rule List

| Field        | Operator | Keyword   | Intelligent Select |
|--------------|----------|-----------|--------------------|
| Display Name | Contain  | Visual    |                    |
| Publisher    | Contain  | Microsoft |                    |
| Version      | Contain  | 10        |                    |

License Information

Authorized License count: 1

| Description            | License Type | Server-based Licensing | License Amount | Exp. Date  | Authorization Detail | Selected Count |
|------------------------|--------------|------------------------|----------------|------------|----------------------|----------------|
| Server department only | Subscription | ✓ Yes                  | 1              | 2021/04/30 | 1                    | 0              |

Cancel Delete Save

# Chapter 9

This chapter describes the license settings.

# License





## Importing a License key

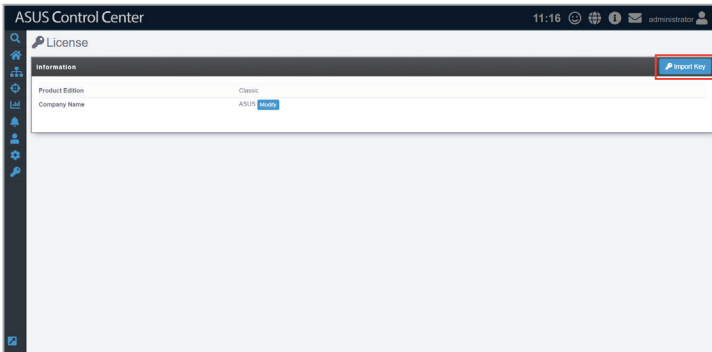
If you are using ASUS Control Center (Classic) or the CSM edition, and have a license key to upgrade to Enterprise edition, you can follow the steps below to import your Enterprise edition license key.

---

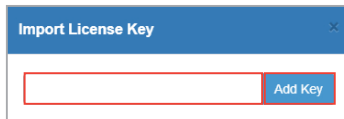
**NOTE:** A working Internet connection is required when verifying the upgrade License key.

---

1. Click on **Import Key**.



2. Enter your license key and click **Add Key**.



3. After entering the license key, you should be prompted with a message, then automatically logged out of ASUS Control Center. Please log into ASUS Control Center again.
4. Navigate to the License screen to see the details of your license displayed.



# Appendix

This appendix includes additional information on system requirements and contact information.

# Appendix

# System Requirements

## Hardware host server requirements

|                                                        |                        |                                                                                               |
|--------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------|
| Virtual machine hypervisors                            |                        | Oracle VirtualBox 5.1.x<br>VMware ESXi 5.x                                                    |
| Virtual machine resources<br>(3000 clients capability) | vCPU (Cores)           | 12 cores                                                                                      |
|                                                        | Memory (GB)            | 128 GB memory                                                                                 |
|                                                        | Disk (GB)              | 500 GB disk space                                                                             |
|                                                        | Hypervisor recommended | VMware                                                                                        |
| Virtual machine resources<br>(1000 clients capability) | vCPU (Cores)           | 12 cores                                                                                      |
|                                                        | Memory (GB)            | 64 GB memory                                                                                  |
|                                                        | Disk (GB)              | 200 GB disk space                                                                             |
|                                                        | Hypervisor recommended | VMware                                                                                        |
| Virtual machine resources<br>(500 clients capability)  | vCPU (Cores)           | 8 cores                                                                                       |
|                                                        | Memory (GB)            | 32 GB memory                                                                                  |
|                                                        | Disk (GB)              | 200 GB disk space                                                                             |
|                                                        | Hypervisor recommended | Virtual Box, VMware                                                                           |
| Virtual machine resources<br>(200 clients capability)  | vCPU (Cores)           | 4 cores                                                                                       |
|                                                        | Memory (GB)            | 16 GB memory                                                                                  |
|                                                        | Disk (GB)              | 200 GB disk space                                                                             |
|                                                        | Hypervisor recommended | Virtual Box, VMware                                                                           |
| Networking                                             |                        | HTTP / HTTPS<br>SMTP<br>SNMP<br>Connection among devices                                      |
| Supported Internet browsers                            |                        | Browsers with HTML5 support<br>Google Chrome<br>Firefox<br>Apple Safari<br>ASUS ZenUI browser |

**NOTE:** We do not recommend using Virtual Box as a hypervisor for client capabilities above 500 clients.

Managed client requirements

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported client operating systems      | <div>Windows</div> <div><ul style="list-style-type: none"><li>Windows 7, 10, 11</li><li>Windows Server 2025, 2022, 2019, 2016, 2012, 2012 R2, 2008 R2 SP1</li></ul></div> <div>Linux</div> <div><ul style="list-style-type: none"><li>RedHat 7.0~/8.0~/9.0~</li><li>CentOS 7.0~/8.0~</li><li>SUSE 12 SP3~/15~</li><li>Ubuntu 16.04~</li><li>Debian 9~</li><li>Rocky Linux 8.0~/9.0~</li><li>Scientific Linux 6.0~/7.0~</li></ul></div> |
| Additional client software requirements | <div>Windows</div> <div>.NET Framework 4.8</div> <div>Linux</div> <div>sysstat, smartmontools, ethtool, curl, ipmitool, OpenIPMI-libs, OpenIPMI-tools, pciutils, net-tools, ssh</div> <div>RHEL 8~, CentOS 8~</div> <div>libnsl</div> <div>SLES 15~</div> <div>insserv-compat</div>                                                                                                                                                    |
| Firmware management requirements        | <div>Firmware management requires Redfish, which is only supported on devices with Linux-based operating systems</div> <div>* BIOS firmware updates via firmware management require Z13/ K14 series motherboards or newer</div> <div>** NIC/DPU firmware updates via firmware management support NVIDIA NIC/DPU devices only</div>                                                                                                     |

## Service and Support

Visit our multi-language website at <https://www.asus.com/support>.

